NTNU

Norwegian University of
Science and Technology

Resilience in emergency management teams

Hanne Wilhelmsen

Safety, Health and Environment
Submission date: June 2011
Supervisor: Eirik Albrechtsen, IØT

Norwegian University of Science and Technology
Department of Industrial Economics and Technology Management

Resilience in emergency management teams

By Hanne Wilhelmsen

06.06.2011

Department of Industrial Economics and Technology Management

Faculty of Social Sciences and Technology Management

The Norwegian University of Science and Technology

Spring 2011

NTNU
Det skapende universitet

MASTERKONTRAKT
- uttak av masteroppgave

1. Studentens personalia

Etternavn, fornavn **Wilhelmsen, Hanne**	Fødselsdato **17. nov 1985**
E-post **hannewil@stud.ntnu.no**	Telefon **99515081**

2. Studieopplysninger

Fakultet **Fakultet for Samfunnsvitenskap og teknologiledelse**	
Institutt **Institutt for industriell økonomi og teknologiledelse**	
Studieprogram **Helse, miljø og sikkerhet**	
E-post **hannewil@stud.ntnu.no**	Telefon **99515081**

3. Masteroppgave

Oppstartsdato **17. jan 2011**	Innleveringsfrist **13. jun 2011**
Oppgavens (foreløpige) tittel **Emergency management and distributed teams**	
Oppgavetekst/Problembeskrivelse 1. Literature review on trust among distributed actors related to emergency management. 2. Map distributed actors in situations of emergency handling in the petroleum industry. 3. Study different actors' experiences on and expectation to interaction by use of collaboration technology in situations of emergency. 4. Develop general advices regarding planning and collaboration in different phases of emergency management.	
Hovedveileder ved institutt **Førsteamanuensis II Albrechtsen Eirik**	Biveileder(e) ved institutt
Merknader **1 uke ekstra p.g.a påske.**	

4. Underskrift

Student: Jeg erklærer herved at jeg har satt meg inn i gjeldende bestemmelser for mastergradsstudiet og at jeg oppfyller kravene for adgang til å påbegynne oppgaven, herunder eventuelle praksiskrav.

Partene er gjort kjent med avtalens vilkår, samt kapitlene i studiehåndboken om generelle regler og aktuell studieplan for masterstudiet.

Trondheim 14-01-2011
Sted og dato

Hanne Wilhelmsen
Student

Eirik Albrektsen
Hovedveileder

Originalen oppbevares på fakultetet. Kopi av avtalen sendes til instituttet og studenten.

Abstract

This thesis is an explorative study of resilience in emergency management, including different actors' experiences with, and expectations to, interaction by use of collaboration technology in situations of emergency. The study is comprised of interviews with important actors within the Norwegian petroleum industry, i.e. operators, contractors, authorities, and other relevant informants. Further, a literature review is presented upon the theme trust among distributed actors.

The findings in this study show that there is a small degree of IO (Integrated Operations) concepts between the different external actors within emergency management. However, there is a somewhat higher utilization of these concepts between the company's internal actors. This study recommends that the operator companies should turn to the organizations which offer to handle the 2nd line emergency management, and analyze what kind of collaboration technologies they utilize with respect to information sharing during an emergency. It is not possible to anticipate every possible scenario, meaning that the actors should focus on being prepared to be unprepared and thereby rely on their improvisation skills. Further, in order to make the emergency management more resilient, it is necessary to implement more of the IO concepts which are available today while, at the same time, trusting the technology to a greater extent. Another important factor is that the contractor companies wants to be more involved at the operator's emergency management planning and training events. As mentioned in this thesis, my opinion is that the inclusion of contractor companies is something which the industry should take into consideration. Such a contribution may, along with implementation of IO concepts, make the emergency management more resilient and render possible to react on early warnings such that emergencies could be avoided.

Preface

The 10th and final semester of the Masters' degree programme in Health, Safety and Environment, at the department of Industrial economics and technology management at NTNU consists of a compulsory Master thesis. Majoring in Safety-related themes, I chose to focus on the field of emergency management and the use of integrated operations in the Norwegian petroleum industry. I have a diverse academic background covering topics such as safety management, ecotoxicology, spreading of pollution, occupational hygiene, hydrogeology, flow in porous media and environmental management. In this study, it has been an excellent opportunity for me to utilize my diverse background to acquire new knowledge in a fast manner and also use the platform of knowledge which is acquired in advance, to be able to solve intricate problems.

I am very grateful for the sessions and discussions I have had with my teaching supervisor Eirik Albrechtsen, Senior Researcher at SINTEF and Associate Professor II at my institute at NTNU and also the help I have received from Irene Wærø and Camilla K. Tveiten both at SINTEF. They have been robust guides for me during my ups, downs and frustrations throughout the semester.

I would also like to thank all the informants who gave me the information needed to make this study possible.

I take full responsibility for any mistakes or incorrect representations in this report.

Hanne Wilhelmsen

Trondheim, 06 June 2011

Table of contents

Table of tables

Table of figures

Abbreviations

Abbreviation	*Full name*
NOFO	Norwegian Clean Seas Association
PSA	Petroleum Safety Authority
JRCC	Joint Rescue Coordination Centre
SAR	Search and Rescue
IUA (Interkommunalt utvalg mot akutt forurensning)	Intermunicipal committee against acute pollution
KLIF	Climate and pollution agency
ODC	Onshore Drilling centre
NOTAM	Notice to Air Men
DSHA	Defined Situations of Hazard and Accident
IO	Integrated Operations
DSB	Directorate for Civil Protection and Emergency Planning
ICT	Information and communication technology

1 Introduction

In the autumn of 2010 I wrote a project in TIØ 4521 on the use of IO (Integrated operations) concepts in emergency management in light of resilience engineering. I found writing this project very interesting, and it founded the basis for this study. There exists few studies on the use of IO concepts in emergency management, and I feel that this is a field which deserves more focus than it has today. A greater focus on this field is a prerequisite to make sure that this is not only a research area which turns up when an accident happens (reactive), but that it may also be included in the early warning phase and in this way give the emergency management field a view of being proactive (i.e. preventing accidents from happening in the first place). Hopefully, this study may give insight into which challenges and possibilities that exists within the field of emergency management. Further, the study may help in evolving this research area regarding sharing of information, development of trust and the use of IO concepts between internal and external actors in the emergency management.

In the early phase of IO, emergency management were one of the fields in which IO were shown as a useful concept (Albrechtsen, et al., 2009). In spite of this, the field has not shown the same development within IO as many of the other fields (e.g. drilling). The explanation for this may be that emergency management is a field where you cannot afford mistakes; it is not acceptable to experiment with emergency management, and everything has to work when an accident/ incident is occurring. Since the composition of the emergency organisation is different for every accident, the solutions developed in emergency management must not be too complex, the framework that the organisation has to work in must be simple, create trust, and be user-friendly. This master thesis focuses on the different actors who are involved in an emergency and their experiences with and expectations to interaction by the use of collaboration technology. Different actors within the emergency management area are interviewed and through the theory of resilience engineering the results are discussed, and finally different measures are suggested which may be implemented to be able to handle the emergency management in a more resilient way.

The following sub chapters will further introduce the scope within emergency management which this study will focus on.

1.1 Integrated operations and emergency management case description

In this chapter two sub-chapters will be introduced which explain the general concepts of integrated operations and emergency preparedness; the latter is introduced because it is regarded as an essential part of emergency management. The introduction will function as a fundament for the scope and limitations of this study.

1.1.1 Integrated operations

Integrated operations (IO) is a concept where information technology is being used to alter work processes, improve decision making, implement remote control equipment and processes and relocate functions and personnel from offshore to onshore (Tveiten, et al., 2008). IO is comprised of new work processes which use real-time data to improve the collaboration between organizations, disciplines, companies and locations to achieve faster, better and safer decisions (Albrechtsen, 2010; Statoil, 2008). The backbone of the development in IO is ICT-tools, e.g. fiber-optic broadband networks and computer systems which have the possibility to communicate together in real-time (Statoil, 2008).

There are many different names for the concept of integrated operations e.g. eOperation, Intelligent fields, Smart field (Shell), Field of the future (BP), iField (Chevron). Further, there are many different degrees of IO (Johnsen & Lundteigen, 2008):

- Remote support: Possibility for assistance from onshore, but direct interventions are not executed.
- Remote surveillance: An onshore operation department are monitoring operational parameters, and making schedules for well optimization. The responsibility regarding the daily operation is still on the offshore installation.
- Remote management: The total operation or parts of the operation is removed to another location.
- Remote operation: All the responsibility for the operation is moved to another location.

The implementation of IO with ICT-tools to enhance the interaction, and in some cases remove functions has two immediate effects; the work processes and role distribution are adjusted to the new form for operation; second, is to have a greater focus on information security in operations (Johnsen & Lundteigen, 2008).

1.1.1.1 Benefits with IO

Some of the benefits of IO are: improved HSE; increased regularity (uptime); better utilization of resources ; better monitoring of equipment and more efficient maintenance; better reservoir and production control; increased recovery; production optimization; more efficient drilling operations and better placement of wells (Statoil, 2008). In Table 1 you see how IO changes the ways of working in the petroleum companies. Each of the elements on the right side of Table 1 will be further elaborated in the text below the table.

Table 1: Change in the ways of working in petroleum companies (Ringstad & Andersen, 2006).

Traditional way of working	***IO way of working***
Serial	Parallel
Single discipline	Multi discipline
Dependence of physical location	Independence of physical location
Decisions are made based on historical data	Decisions are made based on real-time data
Reactive	Proactive

1.1.1.1.1 Parallel

A greater deal of the work can be performed in a parallel fashion with IO which challenges the old assembly line work mode, and could reduce the total time-consumption on the tasks. When focusing on parallel working in a decision making perspective, it could imply a more iterative and relational process. This results in problems being solved in a broader context and that more alternatives may be evaluated before a decision is taken (cf. chapter 1.1.1.1.2 below), along with the fact that the decisions are also more flexible (Ringstad & Andersen, 2007).

1.1.1.1.2 Multidiscipline

The multidisciplinary teamwork increases in importance as the availability of real-time data increases, along with the fact that work is being performed in a parallel fashion to a greater or lesser degree independent of physical location. The multidisciplinary team composition means that further factors are being considered in the decision process, and also that more solutions are being evaluated. A successful multidisciplinary team has the ability to focus on general goals at the expense of each of the member's diverse professional ambitions (Ringstad & Andersen, 2007).

1.1.1.1.3 Independence of physical location

The work may be performed independent of each task's physical location. E.g., the use of videoconferencing and an easy access to data and software tools reduces the requirement for the experts to be physically present at the location. This leads to an increased availability of expert knowledge for the different operational units and decreases the time that is needed to gather the experts. This means that decision making will be improved along with reduced time consumption (Ringstad & Andersen, 2007).

1.1.1.1.4 Decisions based on real-time data

The availability of real-time data makes it possible for the persons at different locations to cooperate on the basis of shared and up-to-date descriptions of the situation. The increasing amount of real-time data gives us the opportunity to construct a more detailed and accurate understanding of the situation, which brings along more precise predictions (Ringstad & Andersen, 2007).

1.1.1.1.5 Proactive focus

By the use of a proactive focus, professionals with expert knowledge in a field will be more involved in the early detection of the possible problems and further in the development of countermeasures. The experts do not have to rely on old and outdated information of the petroleum-field or -well, and are involved more actively in collaboration with the different people on location. By predefined scenarios it would be easier to interpret the information and by this enhance the remote collaboration (Ringstad & Andersen, 2007).

Other benefits of IO are that it render possible to make decisions over long distances, between companies, across time zones and over different cultural boundaries. The interactions between many of the actors inside and outside of an operating company can have positive effects on decreasing the risk for major accidents; an example on this may be the improved awareness and access to expert support (Mostue & Albrechtsen, 2010).

1.1.1.2 Drawbacks with IO

The IO concept is not completely as superior as theory might present it; there are some drawbacks. For example, it is also possible that team-based and distributed decisions could create confusion around who has the main responsibility. The extended fragmentation of companies and the specialization might result in a group of people with a lack of knowledge over the system in total. The system may have too many specialists and too few generalists (Mostue & Albrechtsen, 2010).

Another aspect in IO is that the decision makers/ expertise should be relocated away from the hazard, in to the control rooms, which may lead to a lack of belonging to any specific installation, and so the decisions are being made by "nomad life"- personnel. This means that the decision takers are semi-skilled workers which do not "belong" to any installation. The processes of distributed decision-making will depend upon the situational awareness; how people work together in networks (power/influence, confidence and relations), how the interaction between actors are (management, learning, collaboration, communication) and the different cultures of people (identity, knowledge, values, norms) (Mostue & Albrechtsen, 2010).

Another issue with IO is the possibility for information overload. There are vast amounts of data which has to be analyzed and then presented in a good and informative manner both for the people at the operation centres, and for the people at the installations (Mostue & Albrechtsen, 2010). There will also be heightened complexity and interactivity that can make it difficult for decision-makers to maintain an overview during an accident (Ringstad & Andersen, 2007).

Another issue is with the security of the data flow by the use of IO. This problem may come from hostile hacking of the system, sabotage and virus infections. There is also a possibility for lack of communication and information transfer offshore – onshore due to, for example, cable rupture. Further, there is also a chance of a total power failure, which leads to a total information drop out. Such an event may be due both to an accident and to malicious acts (Albrechtsen, 2010).

The possibility for communication problems between ICT personnel and process-control personnel may be due to trust issues between the different parties. Overall, information security will be an essential part of the new problems that emerges with the increased use of IO (Albrechtsen, 2010).

During the implementation of IO the need for deep organizational changes will and is frequently met with resistance from those which is exposed to the change, and it is also very probable that the people that are responsible for the changes will make mistakes, something which will reinforce the scepticism (Ringstad & Andersen, 2007).

1.1.1.3 Implementation of IO

In Figure 1 below we see how the Norwegian Oil Industry Association (OLF) predicts in which way the content of IO will change over time, and emphasizes two IO generations. In the first generation there will be a focus on integration of the work process between the staff onshore and staff offshore by the use of ICT, and in total this generation will improve the onshore staff's capability to support the staff offshore. This implies that the decisions are made in real-time collaboration among onshore and offshore employees. In the second generation there is a need for integration across the companies. That is, a closer integration between vendors and operators, which is important to be able to lighten the efficient exploitation of the vendor's expertise and services by the operator. In this generation there will be more automated processes, digital services and 24/7 operations (Skjerve, et al., 2008).

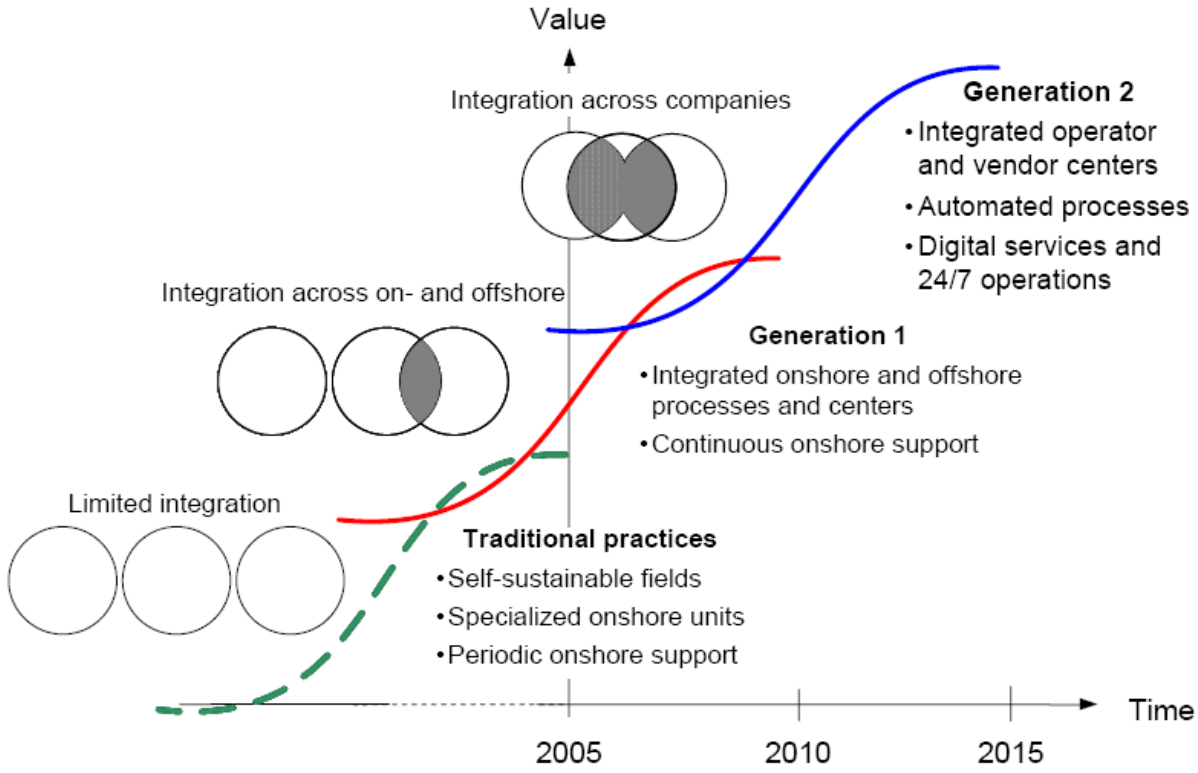

Figure 1: The integration steps of IO (OLF, 2005).

An important factor according to the use of ICT is that the people that are going to use it actually trust the technology in itself. Another important factor concerning the use of ICT is that it should be so simple to use, that the user do not have to concern about how to use the ICT, but only on how to carry out the job in the best way (Büscher, et al., 2008).

Emergency preparedness is regarded as an essential part of emergency management, and due to this the following chapter will deal with this theme.

1.1.2 Emergency preparedness

According to the homepage of the Norwegian Petroleum Safety Authorities (Ptil, 2008) the main goal with the use of emergency preparedness is to prevent or limit the consequences of accidents or incidents. This is why the ability to enhance the technology, organisation and personnel at all levels in the organisation would be a key factor for emergency preparedness. According to Petroleumsloven (§ 9-2, 1996) shall "*The licensee and other participants in the petroleum activities at all times maintain efficient emergency preparedness with a view to dealing with accidents and emergencies which may lead to loss of lives or personal injuries, pollution or major damage to property*" (Ptil, 2008). In NORSOK standard Z-013 'Risk and emergency preparedness analysis' (NTS, 2001), the definition of emergency is "… *technical, operational and organizational measures that are planned to be implemented under the management of emergency organizations in case hazardous or accidental situations occur, in order to protect human and environmental resources and assets*". The requirements for handling risks in the oil and gas sector at the Norwegian continental shelf are set by the NORSOK Standard Z- 013 (NTS, 2001). The requirements follow the ALARP (as low as reasonable possible) principles. The basis for the planning and execution of the risk- and emergency preparedness analyses are from defined situations of hazard and accident (DSHA). The establishment of the emergency preparedness plan is in the installation's design and building phase, and is further carried out at e.g. manning and training purposes in the operation. The oil and gas companies may follow the proposed structure of the NORSOK standard for establishing their emergency management and for training (Tveiten, et al., 2010b). Within the relevance of the individual operation, there should be established measures for all the five emergency preparedness phases (Vinnem, 2009):

1. Notification
2. Combating
3. Rescue
4. Evacuation
5. Normalization

In addition to these there is also the emergency preparedness for the reduction of, or the counteraction against the environmental consequences of an acute pollution if that should happen.

The operator has the responsibility for securing an immediate and coordinated warning of hazard and accidental situations to the authorities. Hazardous and accidental situations that can cause damage or pollution should also be reported and investigated to be able to prevent a repetition. Those situations which occur at a frequent basis, or that have great actual or potential consequences, should be investigated by the operator. The emergency preparedness shall be coordinated, also with the public emergency preparedness resources. To be able to handle hazardous and accidental situations on an effective manner, the emergency preparedness organization has to be a robust organization (Ptil, 2008).

The operator is responsible for ensuring that activities are done in a careful manner and that it is in accordance with the regulatory requirements. The number of small actors has been expanding to a large degree in the last couple of years. The regulations regarding HSE in the petroleum industry place

demands on the operator that it shall have an organization in Norway, which on an independent basis has the possibility to ensure that the petroleum activity is done according to the regulations. In this regulation the operator is given a large degree of freedom to organize its activity, e.g. to use external resources to carry out activities. For the operator to safeguard its own responsibility, it must as a minimum, perform assessments and make decisions at a strategic level. The 3rd line emergency preparedness is a good definition of this border, due to the fact that it is defined as; handling strategic level matters; seeing the big picture; communication to the media; owner/ board level; and business decisions. All of these tasks give an indication of which tasks the operator has to do itself. The operator is also responsible for keeping the supervisory authorities updated on a continually basis on the development and about which measures that are planned to be implemented, though some of this communication may be delegated to external actors, and in this way give the actors formal and real competence to carry out some tasks on the operator's behalf (Ptil, 2010).

According to the Regulations relating to health, safety and the environment in the petroleum activities and at certain onshore facilities (Rammeforskriften) the operator shall cooperate with operators of other production licenses to ensure necessary emergency preparedness in the areas of health, safety and environment. Under special circumstances the Petroleum Safety Authority Norway and the Climate and Pollution Agency may set the requirements and the terms for such collaboration, including an order to the effect that the financing shall be a joint responsibility. There shall be established regions that have joint emergency preparedness plans and joint emergency preparedness resources (Rammeforskriften § 21, 2010).

The different emergency handling units are (Tveiten, et al., 2010a; Tveiten, et al., 2010b ; With, 2010):

- The 1st line emergency team is the local emergency team that is operating at the place of the accident.
- The 2nd line emergency team works as a decision support for the 1st line, they handle e.g. the next of kin, the press and they are the information feeder to the 3rd line. This line is the information processing unit, this is the node in the emergency handling network in which all information gathers and spreads out to the other actors in the emergency management network.
- The 3rd line emergency team is the companies' face seen from outside the organisation. This line is most often located at the companies head office.

1.2 Scope and limitations

The scope of this master thesis is to do an explorative study of the different actors' experiences with and expectations to interaction by use of collaboration technology in situations of emergency in the Norwegian petroleum industry. The aspect of trust both between humans and between human and machine is also an important part of this thesis, since trust is an all-important element of IO. When regarding the trust between humans, the main goal is to see what kind of trust which exists between them, e.g. is swift trust the main category or are there any other dominating kinds of trust within emergency management? Due to poor response on the interview requests from many of the contractors, the number of interviews with this kind of informants are not as many as was initially wanted, but in return interviews with many of the governmental actors within the emergency management was carried out. Lately, several new small operator companies have evolved and due to this there has also evolved external 2nd line emergency management organizations. These organizations handle the 2nd line emergency management for the smaller operator companies; some focus is dedicated in the thesis towards the new organization of the emergency management field.

A part of this study was to map the different actors who participated during different DSHAs. The two different DSHAs which were chosen were;

1. Ship on collision course.
2. Acute oil spill.

During the mapping phase it turned out that the actors involved within these two DSHAS was so similar that there was no use in making two different maps, and due to this only the map over acute oil spill is drawn. The last part of this study is dedicated to development of recommendations regarding planning and collaboration in different phases of emergency management.

1.3 Research questions

This chapter presents the main purpose along with the five research questions which I seek to address in this thesis, with regard to affiliated theory and empirical data.

The main purpose of this master thesis is to do an explorative study of resilience in emergency management, including different actors' experiences with, and expectation to, interaction by use of collaboration technology in situations of emergency.

The research questions below are a concretization of the problem description in the master contract. Compared to the contract, number 4) is new. Still, its content belongs under point four in the master contract.

1) How and why do trust issues influence the collaboration between the different actors during an emergency?
2) How have the map of actors who are involved in situations of emergency handling in the petroleum industry changed with the implementation of IO concepts? What is the degree of complexity on the actor map?
3) What kind of possibilities do the informants see by use of collaboration technology?
4) Which factors has to be in place to enable a resilient emergency management organization?
5) What recommendations, based on the findings of the study, may be developed regarding planning and collaboration in different phases of emergency management?

1.4 Central notions

Emergency management – Is defined by Haddow & Bullock (2003) as: *.."the generic name of an interdisciplinary field dealing with the strategic organizational management processes used to protect critical assets of an organization from hazard risks that can cause disasters or catastrophes, and to ensure the continuance of the organization within their planned lifetime".*

External 2nd line emergency management - This is the expression used for the new organizations which offers to handle the operator companies 2nd line emergency management. This external 2nd line emergency management handles the emergency management for several different operators, and have their own emergency preparedness centrals where they perform the activity which is delegated upon the 2nd line emergency management. To a great degree this concerns coordination of action, resources and services in the handling of emergency situations and unwanted incidents within the operator companies' emergency organization.

Resilience engineering - The essence of resilience is the inner capability of an organization / system to maintain or regain a dynamically stable state, which permits the system to continue operations after a major accident and / or in the existence of continuous stress (Hollnagel & Woods, 2006)

Trust – The term is defined as: *"... the willingness of a party to be vulnerable to the actions of another party based on the expectations that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party"* (Mayer, et al., 1995).

1.5 Structure of the thesis

This thesis is built up according to Figure 2 as shown below. In chapter 2 theory around resilience engineering, complex interactions and tight couplings, and trust are described. Further, in chapter 3, previous research regarding DSHAs, emergency management in today's new work environment and different findings from the project carried out on emergency management in the autumn of 2010 are described. The methodology chapter (chapter 4), explains which kind of methods that are used, and the pros and cons with these methods. Chapter 4.3, contemplates the interviews, a detailed table over the informants is shown there. The results and analysis of the interviews are written in chapter 5. The discussion in chapter 6 is constructed by connecting the theory in chapter 2, the previous research in chapter 3, and the results and analysis in chapter 5. Further recommendations regarding planning and collaboration in different phases of emergency management are written in chapter 6.6. The conclusion of the study which answers the research questions is located in chapter 7, and propositions for further work in chapter 8. The transcriptions from the interviews are located in Appendix B and the interview guide is located in Appendix A.

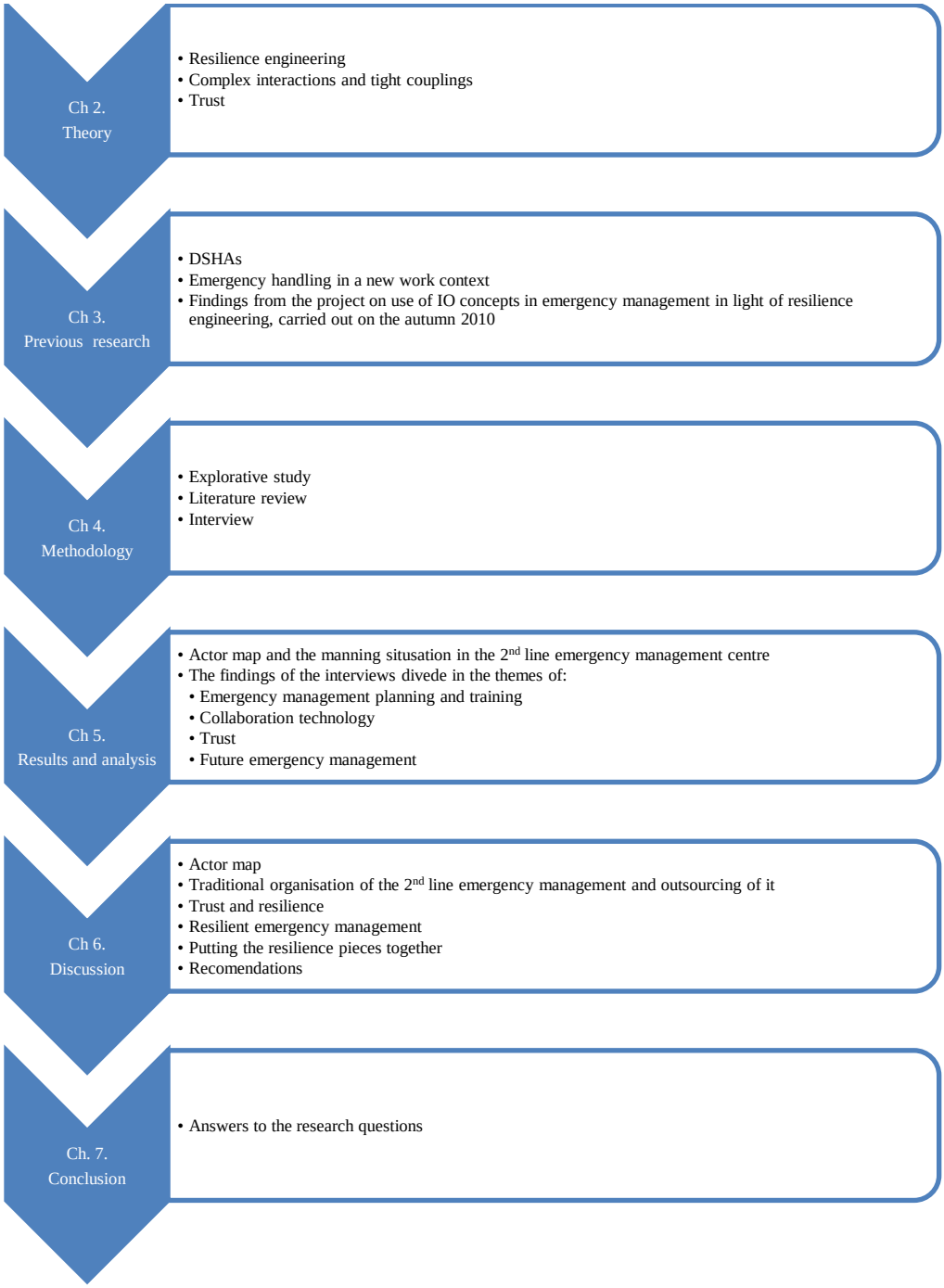

Figure 2: Structure of the thesis

2 Theory

In this theory chapter relevant theory regarding this study will be presented. As mentioned in chapter 1.5 Structure of the thesis, the main theoretical foundation which will be explained in the following chapter is: Resilience engineering, Complex interactions and tight couplings, and Trust.

2.1 Resilience engineering

According to (Hollnagel & Woods, 2006, p. 6) resilience engineering is;"… *a paradigm for safety management that focuses on how to help people cope with complexity under pressure to achieve success*". A resilient organization is an organization that treats safety as a core value, and not as an item that can be counted. The most accurate way to display safety is by counting the events that did not happen. The essence of resilience is the inner capability of an organization / system to maintain or regain a dynamically stable state, which permits the system to continue operations after a major accident and / or in the existence of continuous stress (Hollnagel & Woods, 2006). In other words, Hollnagel also states that the resilience engineering perspective in safety is about how it is possible to make sure that systems remain safe and productive in both unexpected and expected situations (Hollnagel, et al., 2006; Hollnagel, et al., 2008; Nemeth, et al., 2009; Hollnagel, et al., 2011).

In resilience engineering success and fiasco are treated as two very similar phenomenons. The factor that defines a resilient system is its ability to efficiently adjust its functions before, during and after changes or disturbances. To be able to be resilient it is important to know what has happened (the past), to know what is happening (the present) and what may happen (the future), along with knowledge of how to react during different situations (Hollnagel, 2010). Hollnagel defines four foundation pillars in resilience, where each represents an important property of the system (Hollnagel, 2010).

1. Responding – To know what to do, and to be able to do it.
2. Monitoring – To know what to look for, and to find it by the use of special indicators.
3. Anticipating – To find out, and to be able to know what to expect.
4. Learning – To learn from past events by understanding exactly what happened and why.

These pillars can also be found in Figure 3 which is an older figure made by Hollnagel & Woods in 2006. Notice that in today's theory about resilience engineering, learning has also achieved its own pillar as shown above. Figure 3 shows how a resilient mindset/work method has to have continuous improvement to be able to work in an optimal way in dynamic environments. Here the possibility for learning and updating of knowledge comes from the dynamic developments which are present in a continuous manner in the upper part of the figure.

Time, or lack of it, is often a consequence of lack of foresight, since it shoves the system into a mode of reactive response. Knowledge regarding what is to happen and the capability to respond is not enough to ensure control; this is due to that a system without anticipation is constrained towards a purely reactive behavior. Knowledge is an important quality for the anticipation pillar. Knowledge is more than having experience; it also includes the ability to look for more than just the obvious and to expect the unexpected. For the system to be able to respond rationally, both competence and resources are important. Competence concerns the fact of knowing what to do, and how to do it. Resources are needed because it is easy to lose control of the system if the required resources are missing. Together, knowledge, competence, and resources are the three qualities which a system must have in order to remain in control and be resilient. Time is the fourth and dependent quality, and together with the

three aforementioned qualities, they all have to be present to have a resilient system (Hollnagel & Woods, 2006).

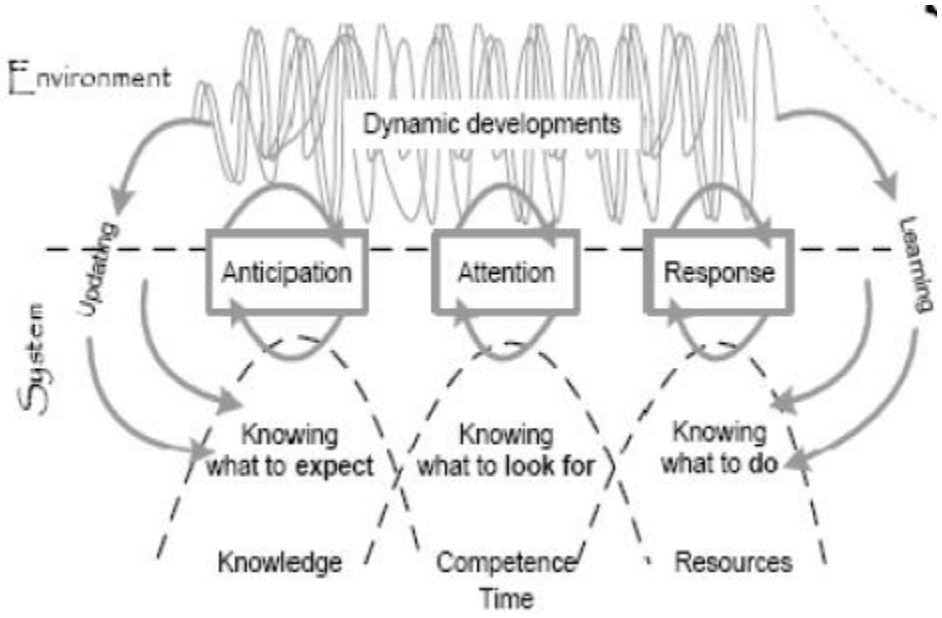

Figure 3: Required qualities of a resilient system (Hollnagel & Woods, 2006).

2.2 Complex interactions and tight coupling

The petroleum industry today may be classified according to Charles Perrow (1984) as a system that consists of complex interactions and tight couplings. A system with complex interactions can be described by: a tight spacing of equipment; proximate production steps; the existence of many common-mode connections of components that is not in the production sequence; there may also be a limited isolation of the failed components; a high degree of specialisation which limits the awareness of the interdependencies; feedback loops that may be unfamiliar and unintended; and some parts of the process that may have a limited understanding. While the tight couplings means that: any delays in the process is not possible; non-changeable sequences; only one correct method to achieve the goal; no room for slack in the equipment, personnel and supplies; and also the limited substitutions of the equipment, personnel and supplies. To be able to manage such a system you should both centralise the system to be able to handle the tight couplings, but also de-centralise the system to be able to handle unexpected interactions between failures (Perrow, 1984).

According to the text above it is theoretically impossible for today's petroleum industry to exist, but in practice it does, which is mostly due to the concept of organisational redundancy. Organisational redundancy may be built by the means that more people have knowledge about the same things, more people know what other people do, and more people are able to challenge a bad idea or to detect a mistake before it turns in to a failure. The aim of building this kind of redundancy even more redundant may be enhanced by the use of ICT, because it enhances more people to see what is going on at the same time (Tveiten, et al., 2008).

2.3 Trust

During an emergency situation the different distributed actors may not have met and / or worked together before. In an emergency scenario a temporary group that consists of distributed actors can be put together to solve the emergency. For the different actors to be able to work together, it is important that each of the actors trust each other, and further trust the collaboration technology which is in use

by the different actors. There is no time to learn a new system during an emergency; this has to be learnt in advance.

2.3.1 Trust between humans

Trust is a very important parameter in the use of ICT in emergency management. The term trust is defined by Mayer et al. (1995): *"... the willingness of a party to be vulnerable to the actions of another party based on the expectations that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party".* It is very important that there exist trust between the different organisations and within an organisation during an emergency situation. This is especially important due to the need for collaboration under an emergency. Creation of this form of trust is also important before the emergency emerges, by working together and building relationships in a normal operational setting (Foulquier & Caron, 2010).

The amount of trust in a partner may be influencing how great degree of freedom you allow your partner, without executing continuous monitoring, interrogation and suspiciousness (Strand, 2001). The sharing and dispersion of information is both problematic and critical, it all begins with whom to trust in unacquainted settings. Even after there is established a level of trust, security issues must still be emphasized. Another very important factor is the emotional feelings of the potential victims in the situation; stress and fear are worsening by the shortage of information, and it is therefore very important with periodic updates (Manoj & Baker, 2007). When a disaster happens, different actors have to collaborate on a short notice; they have to make this collaboration happen from wherever they are placed at that striking point in time. To a large degree this need for collaboration results in electronic communication as being the primary interaction mode (Altschuller & Benbunan, 2008).

In a daily working situation both the formal (e.g. people's hierarchically placement in the organization, job descriptions, and steering documentation) and the informal (e.g. relations to colleagues, leaders, and subordinates) personnel characteristics of the organization plays an important role. The informal personnel characteristic may be characterized by trust, distrust or friendship. As seen in the casual analysis of the accident at Snorre A (see Schiefloe, et al., 2005), an explanation of why the situation was stabilized and not evolved into a disaster, was (to a great degree) due to the trust that was established between the personnel at the platform. Of the 216 people at Snorre A at the time of the gas leakage, 181 got evacuated and 35 stayed behind to handle the leakage and prevent a possible disaster. To be able to take this decision regarding who should stay behind and handle the situation at the platform, is was crucial that the personnel at Snorre A knew each other. They had worked together for many years, had a great degree of technical expertise, local knowledge, capability of efficient communication, and a high degree of trust between each other. As one of the employees at the platform said (translated freely to English): *"The outcome of the situation would have been different if the people onboard were not familiar with the platform or with each other. Everybody trusted each other and knew what to do"* (Schiefloe, et al., 2005, p. 32).

2.3.1.1 Different kinds of trust

The first theoretical description of *swift trust* is performed by Meyerson et al. (1996). The term swift trust emerged to be an explanation for the kind of surprising finding that some teams seems to be immediately adapted in situations with high risk and high vulnerability, to show high levels of trust. Swift trust was primarily identified in temporary teams that were formed to handle a common assignment within a limited amount of time. These kind of teams have been observed to be consisting of members that have dissimilar skills, which may not have worked together earlier (or just to a limited degree), and it is not very likely that they are going to work together again in the future. This means that there is little or no time for relationship building in these kinds of teams due to the tight

deadlines the teams work under (Adams, et al., 2007). This resembles the case within an emergency management setting, where different actors from different distributed organizations come together either face to face or by technological devices to solve the emergency.

Due to the fact that lack of time stops the team members from making expectations of the other members on the team based on first hand information, members do import their expectations of trust, partly based on information from categorical sources such as role and reputation. Within these teams swift trust is also stated on a clear division of roles with well-defined specialties among members. The clue here is that each member understands and knows their own role and the team member's roles; if the role behaviour is inconsistent and there exist a "blurring" of roles, this may lead to a heightened uncertainty and further a lower degree of swift trust. Some other social and "cognitive" mechanisms, like unrealistic optimism and positive illusions may advance the appearance of swift trust by the reduction of feelings of vulnerability (Meyerson, et al., 1996).

When trust between two or more interdependent actors increases or decreases as a function of their cumulative interaction this is called *history-based trust*. Histories of interaction give the decision-makers information that is useful in assessing other people's motives, dispositions and intentions. This kind of trust influences people's trust towards other people by letting their a priori expectations about the other's behaviour decide to what degree you trust this person. But, it is also important to take account of the fact that the current experience you have with the person either will validate or discredit your earlier experiences (Kramer, 1999).

Category-based trust refers to the trust which is predicated on information regarding a trustee's membership in a social organizational category. This is information which, when it is pronounced to a great degree, often will influence other people's judgments about their trustworthiness. Memberships in a salient category may give a basis for presumptive trust; this may be due to the fact that you do not need to have personal knowledge towards the person which whom you shall trust. Further, because of the cognitive consequences of in-group bias and categorization of the different individuals seem to give positive characteristics such as honesty, trustworthiness and cooperativeness to other members in the group. As a consequence of this, the different individuals may transfer a kind of de-personalized trust to other members in the group, which has its only basis on their shared category membership (Kramer, 1999).

Role-based trust is another kind of presumptive trust which is found within organizations. In the same way as category-based trust also role-based trust is based upon a form for de-personalized trust, since it is based upon the knowledge that a person has a special role in the organization, rather than having specific knowledge about the person's motives, dispositions, capabilities and intentions. Strong expectations regarding technically competent role performance are often aligned with roles within the organization, and also expectations that the role-occupants will fulfil their responsibility and obligations which is associated with the roles they have. This leads to the extent that people within an organization have confidence towards the role-occupants who signal that they have the intention and competence to fulfil and carry out their obligations. Further, individuals may adopt some sort of presumptive trust, which is based upon the knowledge of role relations, even if there is an absence of personal knowledge and history due to prior interaction. This kind of trust is developed and maintained by people's common knowledge regarding the different barriers that has to be crossed to be able to entry the different organizational roles. In these barriers there are presumptions about the training and the socialization processes that the different role-occupants have to go through. There are also perceptions about the assurance processes that the different role-occupants have to go through, to ensure the role compliance. In this kind of trust it is not as much the person in the role that the trust is

based upon, but rather the verification system which is established around the role, to be sure that the role-occupant fulfils its role (Kramer, 1999). This may be illustrated with this quotation from Dawes (1994, p. 24, in Kramer, 1999):

"We trust engineers because we trust engineering and believe that engineers are trained to apply valid principles of engineering; moreover, we have evidence every day that these principles are valid when we observe airplanes flying. We trust doctors because we trust modern medicine, and we have evidence that it works when antibiotics and operations cure people".

Role-based trust functions to reduce the uncertainty regarding the role-occupant's relations according to trust-related intentions and capabilities. This means that roles lessen the need for and cost around negotiating trust when interacting with others. But, this kind of trust may also be fragile and has the possibility to create catastrophic failures of cooperation and coordination. This is mainly during different organizational crises or when different novel situations arise which in return blurs the roles or break down the role-based interaction (Kramer, 1999).

2.3.1.2 Trust in organizations

Trust is not only considered as one person's expectations for another person, it may also be the norms and values within certain institutions or cultures. It is periodically claimed that certain nations, organizations and groups have higher or lower levels of trust than others (Julsrud, 2008). Organizations may serve as objects of trust for others, organizations may also come in to sight as trusting subjects (i.e. organizations that have trust in other organizations) (Sydow, 2006, in Julsrud, 2008). The construction of trust is done within the organizations, but at the same time, the institutions also become the recipients of trust. In today's modern society it is crucial to be able to trust formal institutions and due to this there has been a development of a greater degree of impersonal and institutional anchored trust has come into place (Julsrud, 2008).

Temporary groups make an organizational analogue of a "one night stand". They have a finite life-span, they form around a shared and relatively clear goal or intention, and the success of the temporary groups depends on a steady and coordinated connection of activity (Meyerson, et al., 1996). To be able to trust the different actors in an inter-organizational virtual organization (i.e. an organization which communicates by the use of ICT), it is important that the technology is standardized between the interacting organizations. That is, the different actors have to trust the technology before an inter-organizational virtual organization can be successful (Kasper- Fuehrer & Ashkanasy, 2001).

Boin (2009, p. 372), describes the crisis response in the modern society in this way: "*In fact, the crisis response in modern society is best characterized in terms of a network compromising a wide variety of response organizations that usually do not work together during 'normal' times*". This means that during an emergency, the emergency handling organization is a distributed organization which has to co-work in a perfect manner (to be able to handle the emergency in an optimal manner) during an emergency despite the fact that they may not have worked together on an earlier basis. This shows the importance of training on different DSHAs with all the different kinds of actors. Further in the work done by Boin (2009) the development of swift trust is not enough to attain an effective response in an emergency. In order to get the desired response it is crucial that there exist variables such as previous interaction and trust between the network parties

2.3.1.3 Collaboration and distance

In a study by Bradner & Mark (2002) they examined how the geographic distance affects collaboration when they used computer-mediated communication technology. They investigated the effects of cooperating partners who were in the same or in a distant city on three behaviours: cooperation,

persuasion, and deception by the use of video-conferencing and instant messaging. The results from the study showed that subjects are more likely to deceive, be less persuaded by, and cooperate less, with someone that they believe is in a distant city, as opposed to in the same city as themselves.

In the use of remote working today, there are both successes and failures. An example of a success story is the collaboration of space physicists. The collaboration in itself focused on the possibility for simultaneous access to real-time data from instruments which is positioned around the world. This makes it possible for space physicists from all over the world to discuss the phenomena while it is happening. The evolving use of technology is a good way to utilize it; to be able to use the technology in the same way within the field of emergency management would maybe have lead to enormous improvements in efficiency and faster problem solving (Olson & Olson, 2000).

People will achieve trust from others, when they do a sincere contribution to fulfil commitments, do not take advantage of others when an opportunity rises, and are honest in negotiating commitments. Shared experiences and norms increase the growth of trust. Face-to-face teams have been reported to be more effective and reliable than remote teams, this is stated on the observation of "trust needs touch" (Handy, 1995 in Olson & Olson, 2000). Trust is an important property when teams participate in risky activities, especially when they lack the ability to monitor and see each other's behaviour. An advice often given when the goal is to build trust in a team is to let the teammates get to know each other, but this is often costly and time consuming especially when the members are spread out over a large area. This may be the case when a team is constructed during an emergency situation, but it is also important to remember that the people in these teams may not work together more than this one time, and do not have time to develop trust in advance of the teamwork.

2.3.2 Trust between human and machine

Trust between human and technology is also an important issue during an emergency management context, due to the fact that for IO to be a fruitful part of the emergency management process, the actors involved in the process have to have trust to the technology utilized in IO. A definition of trust is proposed by Moray & Inagaki, which also cover trust in technology (1999, p. 204):

"[Trust is] an attitude towards an agent with whom a human operator is collaborating. The agent may be another human or a machine (automated sensor, automated controller, computer hardware, software programs or software agents, etc.). By trust we mean an attitude which includes the belief that the collaborator will perform as expected, and can, within the limits of the designer's intention, be relied on to achieve the design goals."

Rempel et al. (1985) suggest a model of trust made up of three fundamental dimensions:

- Predictability
- Dependability
- Faith

Rempel's model focused on human-human relationships, while Strand (2001) extended this model to the context of human-machine interface. In a human-human context predictability is based on the knowledge and experience with your previous experience and knowledge of the person. Here it is important that your earlier experience has been stable and consistent for this element to be fulfilled. Seen in a human–machine context, predictability will be determined by the operator as if he has the possibility to predict the future actions of the machine, based on the evaluations of the machines regularity. The predictability is also depending on the constraints of the system, as when a higher

degree of constraints is in use, it is easier to predict its outcome. The transparency of the system will also be influencing the predictability of the system. If there is a good possibility to be able to unveil the system, it has to be observable to some degree and to give the opportunity to be able to observe and understand what happens in the system. It will also be easier for the operator to foresee the system's actions if they have a high degree of control, than if it is the system which has the highest degree of control. That the operator has good decision making abilities and experience will also influence the possibility of predictability (Strand, 2001).

Dependability is the second factor in the concept of trust. This concept goes further than the predictability concept since it also emphasizes that the predictability of behaviour is considering characteristics and qualities of the person (Strand, 2001). In Rempel et al. (1985), it is emphasized that a prerequisite for dependency is the existence of risk and the possibility of personal vulnerability. This means, that for someone to state that a person is not trustworthy the person must have had the chance to show that he / she has not earned the decision maker's trustworthiness. Used in a human-machine area, probable personal vulnerability and risk must be present in order to develop trust. This may be done by challenging the machine beyond its designed limits to be able to confirm or disconfirm its dependability in challenging / unexpected situations (Strand, 2001).

The last factor that builds the concept of trust is faith. According to Rempel et al. (1985) faith depends on evaluations of trustworthiness, which is more wide-reaching than the evidence of experience. In this factor, the focus is on the fact that not everything reflects the past, and since both personnel and circumstances change, the use of the past as an indicator for future events may not be reliable. But Rempel et al. (1985) also says that experience is a relevant factor, due to the fact that earlier experience of dependability and predictability of the partner may be an important basis for the development of this dimension, although the most important factors for the development of faith is the person's internal motivation to maintain the relationship. In a human–machine relationship it is important to have faith, but due to the complexity of the system it is often hard to unveil and predict its entire behavioural pattern and to hold trust to the systems unacquainted future actions (Strand, 2001). Definition of trust in the human-machine interface: *"... an attitude reflecting an expectation that the actions of the automatic system will be predictable, dependable and providing faith in the future well-functioning of its actions"* (Strand, 2001, p.18).

To be able to use IO concepts in an emergency situation, one important factor is that the personnel who are going to use the equipment actually know how to use it, e.g. how to turn it on, how to turn up the volume, how to adjust the screen, etc. All of these factors are critical towards which degree of trust you dedicate to the technology. In the study by Olson & Olson (2000), it appeared that people involved in using new technology without having thoroughly training, adapted their behaviour to the technology itself rather than to fix the technology (i.e. the technology was not adapted to the people, but the people adapted to the technology).

People may see the technological system as trustworthy even if they have no earlier experience with it, i.e. where there is no indication of its predictability or dependability. This implies that the level of trust is only depending on the factor of faith (Strand, 2001). This is contradictory to the findings by Zuboff (1988, in Strand, 2001) where it is revealed a great resistance and distrust / lack of faith in new technology. Zuboff's study was performed with workers who had experience with the "old" system in advance and had to learn new ways of working to be able to master the new technology. A person with no earlier experience with the system may not lack faith in the new technology, mainly due to the fact that he has no earlier experience with the older system and therefore has no reason to lack faith in situations of altering of the system.

Today, the idea of being perfectly reliable is not yet achieved by the design and development of automatic systems. Due to this, most operators will experience malfunctions in the system at some time. The degree of reliability of the system is thought of as being a factor which is strongly affecting the level of operator trust (Strand, 2001).

The increasing complexity that follows new technology is evident through the great degree of coupling or linking parts of the system. This implies an increased possibility for combining multiple functions and qualities into a single physical device, making it possible to apply the same device when exerting a variety of things depending on mode, and that several displays appears on the same physical viewport. This might seem as a simplification of the work, but if the system gives insufficient feedback to the operator, this makes it difficult for the operator to understand and predict what the system does and why it does it (Woods, 1996, in Strand, 2001). Often, users of systems only have a small degree of information about the computerized systems they work with, and due to this they have little understanding of the system's actual functions (Maass, 1983, in Strand, 2001).

Familiarity is an important aspect to predictability (Rempel, et al., 1985). When there is a good feedback mechanism and some degrees of experience, this will most likely enhance both the understanding and the familiarity of the system. Dependability, which is the second dimension of trust described by Rempel et al. (1985), is in part related to predictability. It is therefore reasonable to expect that if feedback gives a better opportunity to predict the system, it will also lead to an increased understanding of the stable, dispositional attributes of the system (Strand, 2001).

Feedback also seems to influence the third level of trust, namely faith. Now the focus is no longer on the specific behaviour of the system, but the first two dimensions is an important basis for the development of faith. Due to this, the amount of feedback will most likely still be of importance. But, as mentioned earlier, faith may also arise with workers that have no earlier experience with the system. This is an important part of faith which refers to the operator's belief on the intrinsic intentions/ motivations of the system (Strand, 2001), this is also shown by Sheridan (1992) where he underlines that an elucidation of the systems intention increases the operators trust.

The interface between human and computer is an important device, which may give different amounts of feedback; it is shown by Milewsky & Lewis (1997) that interface design has a profound impact on operator trust. They emphasize the important points that the operator has the chance to observe the behaviour of the system (increase the predictability), get experience with the system during risky tasks (increase the dependability) and to have training to be able to understand the internal functioning of the system (increase faith). According to Milewsky & Lewis (1997) these three aspects may be fulfilled by using the proper design of the interface between human and machine.

An important factor is not to make the amount of feedback too detailed. A study by Yeh & Wickens (2001) showed that displays with a high degree of detail resulted in lower levels of operator trust than displays with a lower degree of detail. They suggested that the detailed display increased the visual noise and reduced the conspicuity of the targets. The possible effect of too much feedback may lead to an information overload and an increased operator workload (Strand, 2001). It is important to have in mind that the development of good feedback and high levels of operator trust is useless without simultaneously monitoring the actual reliability of the system. In a complex system with poor feedback, errors may hide in the system for a while, and in this fashion bring along other errors which is a problem because the severity of errors often enhance in these error finding processes.

3 Previous research

In this chapter, previous research upon the field of DSHAs and emergency management will be presented. This is done in order to see whether the results in this study are congruent with the results of earlier studies. The search for previous research is confined against IO in emergency management, there could have been possible to look at use of IO in other fields, but this is not done in this study.

3.1 DSHAs

The concept of Defined situations of hazard and accident (DSHA) is in use by the petroleum companies that are operating on the Norwegian Continental Shelf. This concept is being used to specify an assortment of hazardous and accidental events on which establishment of emergency preparedness can be done (NTS, 2001).

The DSHAs in Table 2 are connected to the potential for major accidents, while the DSHAs in Table 3 are not connected to this potential (Ptil, 2009).

Table 2: DSHAs for major accidents (Ptil, 2009).

No	DSHA description
1	Non-ignited hydrocarbon leaks.
2	Ignited hydrocarbon leaks.
3	Well kicks / loss of well control.
4	Fire / explosion in other areas, flammable liquids, non hydrocarbon.
5	Vessel on collision course (towards the installation).
6	Drifting object (on collision course towards the installation).
7	Collision with field related vessel / installation / anchoring (towards the installation).
8	Structural damage to platform / stability / anchoring / position failure.
9	Leaking from subsea production systems / pipelines / risers / flow lines / loading buoy / loading house.
10	Damage to subsea production equipment / pipeline systems / diving equipment due to fishing equipment.
11	Evacuation. (Ex-ant evacuation / emergency evacuation).
12	Helicopter occurrence.

Table 3: Other DSHAs (Petroleumstilsynet, 2009; Skjerve, et al., 2008).

No	DSHA description.
13	Man overboard.
14	Serious injury to personnel.
15	Occupational illness.
16	Total power failure.
17	*Control room out of service.*
18	Diving accident.
19	H_2S emission.
20	*Lost control of radioactive source.*

21	Falling object.
22	*Acute pollution.*
23	*Production halt.*
24	*Transport system halt.*

The DSHAs which are in italics in Table 3 were not among the DSHAs that were in use during the RNNP 2009 (Risk level on the Norwegian shelf 2009).

These DSHA's were established based on the risk analyses of hazards associated with petroleum production in a traditional operational environment, that is, before the introduction of IO so there might be some need for an extension of the list of DSHAs. However, according to a report by Skjerve et al. (2008) concerning this special case, they did not find any new problems that needed a new DSHA on basis of the implementation of IO concepts. This revealed itself in a good manner during one of their interviews:"*IO or not IO - the crisis is the same. DSHAs are death and troubles that can strike an installation. The crises are the same, but the emergency handling is different in IO*". This study was carried out in 2008, so the answers might not be the same today since the introduction of IO now has come further. Some IO-related DSHAs might be (Skjerve, et al., 2008):

- The lack of communication and information transfer offshore-onshore, e.g. cable rupture. However, there are radio and satellite systems that may function as backup systems.
- Incidents that are created by malicious acts (virus infections, sabotage, hacking, etc.).
- The possibility of a total power failure and total information drop out. This may be both due to accidental events and malicious acts.

In the study of (Skjerve, et al., 2008) they found some new challenges and possible opportunities for the use of IO concepts in emergency handling:

- The transition from the normal integrated operation to crisis handling will be different from traditional operation. New actors will be involved, and the interactions between actors will be changed. There is an issue according to whether the operation room also should be used as the emergency handling room. A large counterargument for this is that if you physically change your location from the collaborating room to the emergency room, you will also psychologically change your operating mode. This change in mode is not so likely to happen if the crisis is being dealt with from your ordinary workplace. In an emergency context there are also other people that daily work in other operational modes which are being called upon. This is an issue related to the 2nd line emergency resource.
- The awareness of the situation. The use of IO concepts provides more information about the situation / crisis, which may have two positive outcomes; 1) make a better understanding of the situation, and 2) to get a better overview of and to give the 1st line of emergency an improved overview of the distribution of resources.
- The change of location for the 1st line of emergency, from offshore to onshore.
- When working together in a group to solve a problem, there will always be challenges according to composition and power mechanisms of the group. The group may define preferred settings that may work in some situations but not in all. Another important point is whether the person with the best competence or the person with the most authority is the one the rest of the group are listening to in group decisions.

- As IO enables the integration of contractors in many aspects of the petroleum industry, there will be a requirement that the contractors and not only the operating company are engaged in the control of the emergency training and DSHAs. In this way the contractors will be engaged in thinking about new approaches.
- The coordination of different actors is important in e.g. the emergency handling of a costal oil spill. In such situations it is very important with a good overview of the available resources and the coordination of these. IO has tools that may contribute to this coordination.

3.2 Emergency handling in a new work context

In the paper by Tveiten et al. (2010a) they observed two different emergency handling training sessions;

1) Loss of control of a well, and the subsequent oil spill.
2) Loss of control of a well, the subsequent oil spill, and a personal injury.

In this study there were also a workshop with representatives from three operating companies and one contractor company. Further, consultants and researchers who work within the emergency handling field were also present. The fundamental question which was challenged to the participants in the workshop was: "*Which opportunities and challenges do you foresee related to emergency handling in 2015?*". The results from this study were defined in three main findings: early warning, sharing of information, and interfaces between actors. Each of these will be outlined below, together with other relevant research upon these themes.

3.2.1 Early warning

Early warning implies shifting focus toward handling deviant situations at an earlier stage rendering possible to handle the situation before it generates in to a severe accident. Through the workshop mentioned above it became clear that there is a need to get more focus on handling deviant situations at an earlier stage. The industry has primarily two states; normal operation and emergency. However, in the workshop there were also revealed a third state, the transition state, where the normal operation is abandoned, but at the same time the operation group will handle the situation and not the emergency team (Tveiten, et al., 2010a).

There is a difference between the emergency and the normal operation teams according to how the risks are assessed. In normal operation the "worst case scenario" is normally not considered, but it is the common scenario of the situation for the emergency handling team. In the workshop it was revealed that offshore site teams are more preoccupied with being prepared for the worst and looking ahead, and that this attitude should be transferred to the onshore groups, as the onshore groups would be more in to the daily operation offshore (Tveiten, et al., 2010a).

Onshore possess very much information covering boats, logistics and elements of hazard, and with the use of IO concepts this may contribute to an earlier detection of a deviation with the potential for a serious accident. The contractors may also be a part of the team of discovering the accidents at an earlier stage. When using IO concepts it is possible to possess huge amounts of information, the challenge is to classify the information, to be able to see deviations at an earlier stage, and in this way have the opportunity to prevent incidents from happening (Albrechtsen, et al., 2009).

3.2.2 Sharing of information

Vast amounts of information is being collected, shared and visualized among different actors in emergency handling. Information has a very central role within the coordination of the different

activities at the horizontal and vertical levels of an emergency handling situation. Here there is use of both lean and rich communication forms (Tveiten, et al., 2010a).

In an emergency, the emergency handling log system is a very important tool for sharing of information. In this log, all decisions and actions that are made by the different actors are written. The emergency log system share information about lost and wounded persons, information on vessel, SAR (search and rescue) helicopter requests and information on handling of personnel. Specific information about the wells and installation, and the state of production and historical data is not shared if they are not asked for (the historical data is very difficult, if not impossible, to get a hand of). The log system is usually only open for the 1st and 2nd line, and occasionally also for the 3rd line emergency management. Information overload and an excess information demand by the 3rd line is a possible stressful problem for the 1st and 2nd line emergency management teams. For example, it may be a situation where the 3rd line feels like not getting enough information, while the 2nd line feels that the 3rd lines constant demand for information may be an obstacle for them in concentrating on their work situation, namely handling the emergency (Tveiten, et al., 2010a).

In an Emergency Operations Centre (EOC), similar to the one manned by the 2nd line emergency personnel, the first responders need to do different things, such as; monitoring and analyzing data, deal with the communication of the situation to others, determine what to do, and also collaborate with other workers in the EOC and in the field. These aspects turn into five challenges when working with EOC: high stress, information overload, intense collaboration, irregular work pattern and diverse experience (Landrigan, et al., 2010).The challenges of psychological stress such as frustration and anxiety may be a problem in emergency management, since when people are stressed, they seem to underperform in their tasks and more frequently make mistakes. Psychological stress may also reduce the ability of individuals to be able to improvise on issues that are not routine procedures, e.g. when an emergency is not defined in one of the DSHAs and the emergency team do not have any specific rules to follow (Chen, et al., 2010).

In the study by Tveiten et al. (2010a) it was shown that the information flow between the different actors in an emergency handling situation not is optimal. The groups that were located outside the 2nd line emergency rooms, but also individuals inside the rooms, were all stressed by the lack of information. Often the only way to get information was to be at the spot where people exchanged information. During an emergency situation there are many actors that possess different kinds of information; it is a crucial issue not only to construct new information with the information technology, but also to utilize the information that is available. The focus on technology should be altered from looking at technology as something that collects information, to look at it as a tool that creates information in situ (Albrechtsen, et al., 2009). In an emergency situation the communication channels that are in use between the different teams and actors are mainly lean, for instance e-mail and telephone. The main challenge regarding the information flow for the emergency response organization is the possibility for having too many resources available and receiving too much information (i.e. information overflow), which in return may strain the management's capacity and the information system itself (Manoj & Baker, 2007). A very important factor in emergency management is that you should only have the information that you need, not more or less. Other important factors may be that the tools being used in an emergency situation have to be adjusted to the organization which shall handle the emergency. This statement implies that if you do not have an emergency staff that work with emergency preparedness on a daily basis and are thoroughly known with the tools that are being used, it may be difficult to introduce advanced tools for use in an emergency setting. The emergency system's criteria are that they are user-friendly and easy to use in an emergency situation (Albrechtsen, et al., 2009).

During the workshop it emerged that there is an ambiguous view on the need for richer communication channels in emergency situations. On one hand it is not desirable to have videoconference equipment in an emergency situation, as this may lead to an interruption that is not desirable in this kind of situation. This especially regards the 1st line of emergency. On the other hand, if the 2nd line has the same situational data as the 1st line, that includes pictures, the situational awareness will also increase. Another improvement area is the possibility for video-communication between the 2nd and the 3rd line to also create an enhanced situational awareness between these lines (Albrechtsen, et al., 2009).

3.2.3 Interfaces between different actors

The use of collaboration technology and new ways of working within IO implies that there exist many different actors with different responsibilities, different proximity to hazards and resources, and different interests that are involved in the emergency handling. In today's emergency management there are many interfaces. The interfaces are both across the organizational boundaries and within the organization (i.e. inter- and intra-organizational boundaries). The number of involved actors will vary according to the accident and hazard that is being handled. The map of actors involved in an emergency response is becoming more and more complex due to the changes brought by IO, e.g. IO render possible a greater involvement of contractors and internal support groups. As mentioned above, all actors are different with respect to their responsibilities, proximity to hazard, interests and resources. Therefore, it is necessary to focus on new forms of coordination, cooperation and awareness during the planning and handling of emergencies. To be able to do this there is necessary to draw the actor maps all over again. It may also be necessary to involve some of these actors at an earlier stage in the normal operation and by this to develop new ways of working; including these actors in emergency management could be a step in the right direction towards the earlier detection of deficiencies or drift from normal operation to incident or accident situations (Tveiten, et al., 2010a; Tveiten, et al., 2010b).

Often when the emergency handling starts, the groups involved have not worked together in an earlier emergency situation. This is because the people in the emergency handling teams are gathered only when they are needed in a specific emergency situation. The degree of earlier co-work between the team members is often dependent on which expertise the current and earlier situations have needed (Tveiten, et al., 2010a).

3.3 Emergency preparedness training

Training is a very important part of emergency preparedness. It is important to keep on training on DSHAs, but it is also important to train on the interaction across interfaces between different actors; this means both the external and the internal actors who are distributed geographically. A very common statement in training is that the emergency "*is over before it has started*", which implies that the 1st line will be involved in the emergency exercise, while the 2nd and the 3rd line are only practising the situation of normalisation. There are different needs for information during a normal vs. an emergency situation. Therefore, it is important that the organizations define their need for information in advance, and at the same time considering the importance that the information is comprehensible for the receiver. This task may be demanding, but it is very important, since you have to be certain that you are not getting too much or too little information in a stressed situation with respect to the decisions that are going to be made (Albrechtsen, et al., 2009). It is important that the organizations have been training on the handling of possible disasters, but what kind of disasters that may appear are not always as easy to know. This leads us to an issue with respect to the use of ICT in emergency management: what kind of ICT should be used? Should one use different ICT equipment at each task? And how should one select what kind of equipment to use? (Mendonca, et al., 2007). Due to the

increased degree of interaction among both internal and external actors along with better access to and visualisation of real-time data and information, it will be important that the training not only concerns the handling of the incident, but also considers interaction and sharing of information, as mentioned above by Mendonca et al. (2007). There may also be a need to train on situations where the ICT-systems, which the emergency organization is based upon, will fail (e.g. due to computer problems, power failure, or loss of communication onshore and offshore). In those cases, it is important to have whiteboards and post-its available to be able to handle the emergency in an efficient way. It is also important to establish a forum where the different parties have the opportunity to discuss issues regarding the emergency preparedness. This should be fairly easy to establish, since emergency preparedness is not something that you should compete for but collaborate in (Albrechtsen, et al., 2009).

3.4 Planning of the emergency preparedness

Recommendations on how to make an emergency preparedness plan can be found in the NORSOK standard Z-013 "Risk emergency preparedness analysis" (NTS, 2001). The plan should be based upon an emergency preparedness analysis, which includes an identification of DSHAs and also a process for risk analysis. Identification of the different actors who are involved in the emergency handling should be performed for each DSHA. Further, the actor map should be constructed once more based on the recent developments. This to be able to get an accurate view over the actors involved, the different authorities, and the other roles that have to be present to render possible good and efficient handling of the emergency. Every complex interaction between the different actors must be mapped, and it is also important to map how these actors communicate and collaborate (Tveiten, et al., 2010a). This is the theoretical reason why a part of this study is dealing with the mapping of actors during a DSHA, namely; acute pollution. In emergency preparedness it is important to remember that also the organizational challenges are strong. There are especially large challenges when groups that are used to work in hierarchical decision-making, suddenly find themselves working in a flat and more dynamic ad-hoc organization. There are advantages to both the flat and the hierarchical organizational decision-making. The use of e-mail, mobile applications, real-time data, etc., alleviates the effectiveness in cross-organizational communication. While, in the hierarchical organization, there may be information gaps between organizations, the flat organisations are not scalable. This implies that in an emergency situation a hybrid organizational model needs to be developed (Manoj & Baker, 2007).

Since the petroleum industry is moving their operations towards a harsher climate and areas that are less developed (e.g. the arctic areas), challenges concerning the different hardware and software solutions may appear as compatibility problems between the different groups and organizations that are cooperating in emergency handling situations in areas where the infrastructure for communication is not sufficient (Tveiten, et al., 2010b).

3.5 Resilient emergency management

According to the study by Wilhelmsen (2010) there are several factors that must be in place to make emergency management resilient by the use of IO concepts. Each of the pillars in resilience engineering includes processes and resources that have to be in place to make the system resilient. The pillar of anticipation needs real-time data to be able to give an earlier warning according to what things that may go wrong. During monitoring it is important not to get an information overflow, and to be able to extract the essential and critical elements from the information flow by e.g. indicators. In the responding phase it is important to be able to improvise. In order to improvise you need resources such as creativity, knowledge and skills. It is also important to trust the information from; the real-time data, your colleagues, and the company's external actors, in a way such that the handling of the

emergency is done fast and efficient. At last but not at least, the learning pillar of resilience engineering is essential for any further development within the use of IO concepts in emergency management. It is pivotal to have continuous learning from historical accidents, emergency management training sessions, and from audit deviations and improvement points set by The Petroleum Safety Authority in Norway. This learning works as input to what you should look for in the monitoring phase, what new areas that you have to look for in the anticipation phase, and how to respond to these kinds of problems. These resilient factors, and how they influence each other, are illustrated in Figure 4.

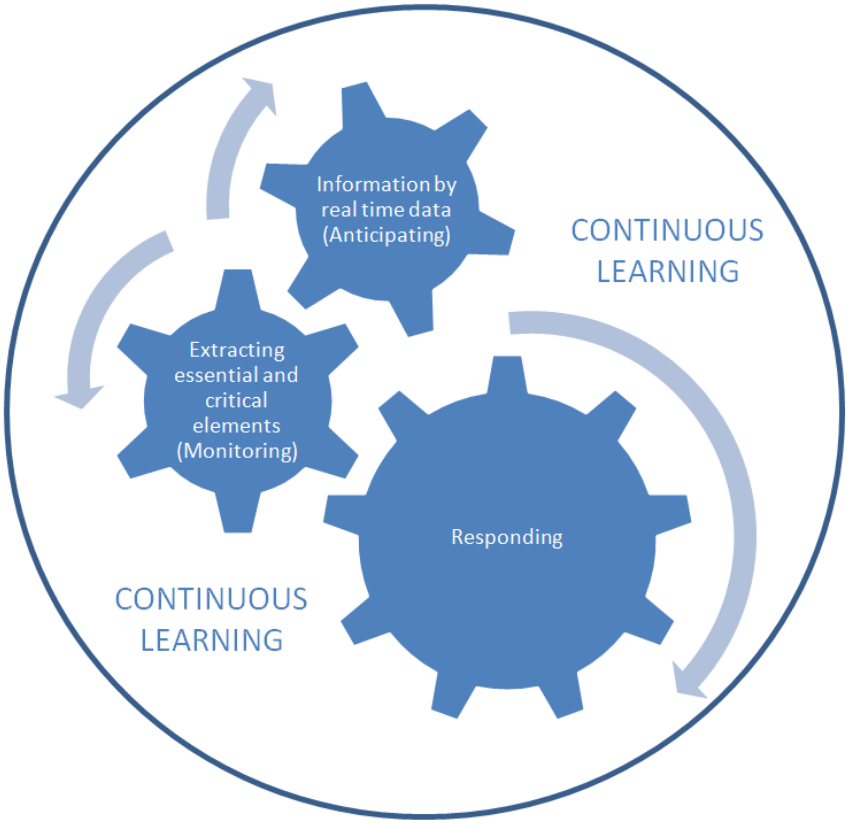

Figure 4: Resilient emergency management by the use of IO concepts (Wilhelmsen, 2010).

4 Methodology

This chapter presents the methodology utilized in this study, including strengths and weaknesses of the chosen methods.

4.1 Research design

A research design is a sketch of how a research study shall be performed. To be able to arrive at one design, it is necessary to do several choices. One of these choices is whether to do a qualitative or quantitative study. Here the qualitative design encompasses a thorough research of few units, while quantitative design often evolves measurements of several variables to a great extent. As a result the quantitative research gives data represented by numbers, while qualitative research gives its results in the form of text-based data (Ringdal, 2001). This study is performed as a qualitative study.

The research design in this study may be explained as consisting of explorative, describing and explanatory parts. I will first start with a description of these kinds of designs, and then follow with why I chose a research design consisting of these mixed methods for this study.

An explorative study is a study where the aim is to discover new things regarding the theme in question when the theme has not been investigated to a great extent in previous research. Due to this, it is important to be open for new information and to be able to see the research theme in several perspectives during the study. These kind of studies are seldom independent studies, but are often carried out as an pilot study / pre-study done in advance to more comprehensive studies describing or explaining the phenomenon explored in the explorative study. An explorative study may result in; knowledge to the field, definitions of central conceptions, and development of interesting research questions. In this study knowledge to the field is a central part, and it is the main focus of the exploratory part of the study. Due to the wide character and the proximity to the phenomenon that is being explored, the explorative study often uses qualitative techniques such as field research and a conversational interview as methods during the research (Ringdal, 2001). When the explorative study is carried out, the *describing* and the *explaining* part of the study are put into action. Mostly all of the scientific studies have a goal to describe the phenomenon which is studied and also to give an explanation of the study. As an example you may want to study the relation between the family background and level of education. The describing part of this study may be to prove such an relation in detail, while the explanatory part consists of trying to give answers to why it is often the case that children with background from the middle-class gets an higher education than children from the working class.

Since emergency management and the use of IO concepts in the Norwegian petroleum industry are not something which has been studied to a large degree earlier, there was a need to start with an explorative study to be able to get an overview over this field of the petroleum industry. This was performed by a literature review of emergency management, and further also about trust related to emergency management (which is a part of the study). After completing these literature reviews, informant interviews were performed to get more "in the field" information about the theme, at the same time as investigating whether the findings in the literature comprehend with the daily praxis in petroleum companies in Norway.

4.2 Literature review

The literature review was done as a narrative review which is defined in Bryman (2008, p. 696) as: *"An approach to reviewing the literature that is often contrasted nowadays with a systematic review.*

It tends to be less focused than a systematic review and seeks to arrive at a critical interpretation of the literature that it covers".

The literature review was performed to explore the existing literature on the themes of; emergency management, integrated operations, resilience engineering and trust. Most of the literature was discovered on the internet by the use of search engines at; Google, GoogleScholar, SINTEF, UBIT (NTNU University Library), ISCRAM (International Community on information systems for crisis response and management), and the homepages of petroleum companies. The search criteria for the searches that included emergency preparedness were: "emergency management", "emergency preparedness", "emergency preparedness ICT" and "crisis handling". While the searches that involved integrated operations had search criteria as "IO and the petroleum industry Norway", "integrated operations" and "integrated operations emergency management". When searching for literature about trust, some of the search criteria were: "swift trust", "trust", "trust in distributed teams" and "trust in organizations". The theory of resilience engineering is mainly extracted from Eirik Hollnagel's theory on this field. For each of the sources that were used in the project, an evaluation of objectivity was done.

4.3 Interview

In this study, eleven interviews were carried out together with one mail-correspondence to explore the theme of this study and to check if the literature findings also were the case in practice. The chosen sampling method was non-probability sampling. There exist three types of non-probability sampling: the convenience sample, the snowball sample, and the quota sample (Bryman, 2008). The selection of interviewee objects was done as a combination of these three sampling strategies. The mixed sampling strategy was used due to the fact that one needed different types of actors in the sample to be able to get the desired breadth of the study, while it was also necessary to perform interviews with the people who were available at the time the data collection phase was planned (and further, the people that were interviewed often gave tips on which personnel to contact for further interviews). Convenience sampling is defined in Bryman (2008, p. 692) as; "… *a sample that is simply available to the researcher by virtue of its accessibility*". While quota sampling is a sampling strategy where you in advance have decided what kind of groups, in this case what kind of organizations, you want to interview. Further, snowball sampling is a kind of sampling where "…*the researcher makes initial contact with a small group of people who are relevant to the research topic and then uses these to establish contacts with others*" (Bryman, 2008, p. 699). Snowball sampling is often defined as a form of convenience sampling. During the sampling phase in this study, all these methods were used and the resulting sampling strategy that was used was mixed methods. Quota sampling was used due to the fact that it was necessary in this study to have informants that had different roles in an emergency, e.g. operators, contractors, governmental instances etc. The selection of which kind of organizations that should be selected was decided in collaboration with my teaching supervisor. Here, the use of convenience sampling was utilized by selecting informants with whom my supervisor had been in contact with at an earlier phase and were defined as good and reliable sources of information. Further selection of informants where also extracted from random sources which were found e.g. on the different organizations homepages on the internet. Often, when talking to the informants, they had contact-information to other relevant informants in other organizations, and here the snowball sampling strategy was utilized.

The informants were requested if they could participate in the study preferably by telephone or by e-mail. The interviews in themselves were done over the telephone or in face-to-face meetings. The telephone meetings were selected due to the distance between the interviewer and the informant and that a telephone interview was the least time-consuming and costly solution for both the interviewer

and the interviewee. All the interviews were recorded on a digital voice recorder in order to focus on getting all the information necessary from the informants and not worrying about writing everything down. Also, it was important to be sure that the answers they gave really were the answers to the questions that were asked (i.e. focusing on the questions and the information received, rather than documenting what was said).

The interviews that were conducted can be explained as semi-structured interviews. In this kind of interviews there is an interview guide concerning questions or topics which have to be covered, but the interviewee has great freedom with respect to replying (Bryman, 2008). In this study, an interview guide (cf. Appendix A) was prepared before the interview, based on the knowledge gained in the literature review. The interview guide was modified during the sampling phase, to fit the different actors in each of the interviews, but the main structure within the guide was the same for all the actors. Some of the interviewees received the interview guide in advance to be able to prepare for the questions; this was mainly done for the interviewees who asked for the guide to be able to prepare themselves and to some of the interviewees in the starting phase of the data collection. During the interview, notes were taken as a backup solution if the voice recorder failed, or if I should forget to turn it on during the interview. All the interviews were done over a period of three weeks. A description of the different interviewees is given in Table 4. In some of the interviews there were two participants who attended the interview; this is stated in Table 4. Further in the text, there is not made a separation between which participants that said what during the interview. Some of the informants wanted to be anonymous and are therefore given different letters; mainly, no referrals will be made directly to the letters of the actors who are anonymous in the text. The interviews conducted with A and I were mainly done to be able to map the different actors who are participating in an emergency handling incident. The interview with I was done by a face-to-face interview, and the data collected from the Joint Rescue Coordination Centre were done by e-mail correspondence. The rest of the interviews were done by use of the telephone.

Table 4: Informants in the study.

Actor	***Information about the actor***	***Position of the informant***
A	Large operator company in Norway.	Planner of emergency preparedness in A, including emergency preparedness analysis, plans and exercises.
B	Contractor company in Norway, which among other delivers services as maintenance and modifications.	HSE & Q leader, who also has a position in the emergency preparedness group.
C	Consultant company in Norway with one of their special fields being emergency preparedness establishment, development and revisions of emergency preparedness plans. Training of emergency management teams. Emergency handling on top management level. Emergency preparedness training.	Safety engineer, working as a consultant within emergency preparedness.
D	2nd line emergency management organization which handles the 2nd line emergency management for different operators.	Emergency preparedness leader for one of the emergency preparedness teams.

E	2nd line emergency management organization which handles the 2nd line emergency management for different operators.	Consultant within emergency management.
F	Contractor company in Norway which, among other things, delivers services as maintenance and modifications.	HSE manager for one installation and one location.
G	Little operator company in Norway.	Informant 1: drilling engineer. Informant 2: Responsible for the emergency management.
I	Large operator company in Norway.	Informant 1: Planned and been responsible for many large emergency preparedness trainings. Informant 2: Working with emergency management up against the 1st line in the emergency management organization.
Petroleum Safety Authority Norway (PSA)	PSA has the governmental responsibility for the technical and operational safety, among this emergency preparedness and working environment. PSA supervises how the operator handles an ongoing incident during an emergency situation (Ptil, 2011).	Works within the field of emergency preparedness and logistics.
Norwegian Clean Seas Association (NOFO)	Keeps the operating companies' oil spill preparedness, which is associated with exploration for and production of oil and gas on the Norwegian Continental Shelf. The objective of NOFO is to keep the oil spill preparedness organization in order, and in such a manner be able to prevent acute oil spills and to have extensive oil spill response resources available. NOFO is responsible for the organization of personnel, equipment and vessels, against acute oil spills. Combined with regional and governmental resources, NOFOs resources will mitigate environmental damage that may be caused by a possible oil spill from petroleum activity (NOFO, 2011).	Emergency preparedness advisor.
Joint Rescue Coordination Centre (JRCC)	JRCCs areas of responsibility is to perform an operative coordination of rescue operations, receive SOS calls, evaluate the situation in a fast manner, put countermeasures into action and lead the following search and rescue operation. Their focus area is to save human lives (HRS, 2003).	Rescue inspector.
The Norwegian Coastal Administration	Is a department of Ministry of Fisheries and Coastal Affairs for sea transport, maritime safety, ports and emergency preparedness against acute pollution. The Norwegian Coastal Administration works among others to prevent and limit the harming effect that	Senior advisor.

	comes with acute pollution, and they also aid in generating a sustainable development of the coastal zone (Kystverket, 2011).	

4.4 Analysis of the results

Due to the fact that the interviews were performed over three weeks, the transcriptions of the interviews were done in parallel with the execution of them. A main point of separation in a qualitative analysis is between studies which focus on the significance of how the informants are expressing themselves and studies of the content in the text. In this study, the focus of the analysis is on the content in the text. The qualitative research process has kind of a floating transition phase between collection and analysis. The analysis and interpretation already starts during the contact with the informants (Thagaard, 2003). This was also the case in this study, and much of the analysis was already done before the actual analysis phase begun.

The strength with qualitative interviews is the possibility to follow up on themes which emerges during the interview, and that the interviewer has not been thinking of in advance. This specific characteristic makes the interview very suitable for explorative studies, such as this study was (Rosness, et al., 2010). This was experienced in this study, due to the fact that the informants brought up information on areas which were not thought of in advance. Because of this, there were done some adjustments in the interview guides after these interviews to be able to discuss the new concepts in the remaining interviewees.

During the analysis the transcribed data was coded into the same categories as was on the interview guide, some of the questions on the interview guide had very similar answers, and on the basis of this fact these categories were decreased into one category. This coding was done in Exel, to be able to compare the answers from the different informants in a quick and simple manner.

4.5 Evaluation of methodology

Asking questions about validity, reliability and generalizability are important in order to check the quality of the study. The validity of the study is often connected to the fact that the research is done with a great deal of confidence. The validity may be connected to the quality of the information in which the project is based on, and also to evaluations of how the researcher uses and develops information from the field. Using both voice-recording and video enhances the validity of the study, since this kind of information gives basis for constructing data which is more independent on the researcher's understanding than documented notes where the researcher reconstructs happenings and statements (Thagaard, 2003). Since eleven of twelve interviews were voice-recorded in this study the analysis was performed mostly by the help of voice recording, and therefore this part of the validity criterion is fulfilled. Reliability is explained by which degree the study may be duplicated; this is generally a hard criterion to fulfil in qualitative research, since the social setting may be different from one study to the other (Bryman, 2008). The third measure to check the study's quality is the generalizability, namely to what degree the findings may be generalized across social settings. This concept is often a problem for qualitative studies due to the fact that a qualitative study is often based on case studies and small samples (Bryman, 2008). The petroleum industry in Norway is not so large, and since many of the important actors who are participating during an emergency were actually interviewed in this study, the results may be generalizable for some of the organizations within the petroleum industry in Norway.

The interviews were carried out over a timeframe consisting of three weeks. This implied that most of the transcription was finished at the same time as the interviews were finished. This gave room to see what kind of information which was missing, and what kind of information that should be the main focus to get a hold of from the next informant that was to be interviewed. The first interview which was performed was done in order to check if the interview guide functioned to its purpose. My conclusion is that the interview guide functioned, and only minor alterations were implemented to the guide when interviewing the rest of the actors. The timeframe of the interviews spanned from thirty minutes to one hour and forty minutes, mostly the duration of the interviews were within one hour. As mentioned earlier, most interviews were done by telephone; there are mainly two drawbacks with the use of telephone interviews (Bryman, 2008):

1. It is unlikely to function very well with long interviews.
2. It is not possible to observe body language; i.e. to see how the interviewees react physically to certain types of questions.

Most of the telephone-based interviews only lasted for an hour, but one lasted for one hour and forty minutes. During the prolonged interview the semi-qualitative interviewing technique got a little out of hand, and the interviewee talked about themes which were far from the interview guide. Further, as Bryman mentions, during many of the interviews one did not have the possibility to see the interviewees' body language and also they did not have the possibility to physically sketch a picture over what they wanted to explain. During the interview with I (the face-to-face meeting), these drawbacks were avoided.

The use of telephone interviewing has some benefits when compared to face-to-face interviewing; one of these is the cost issue, since it will be much cheaper to perform qualitative interviews over the telephone. This was also the case in this study, since many of the interview objects were located in other areas of the country than the interviewer.

Since interviews are seldom analyzed directly from tape recordings, the usual procedure for analyzing is to have the taped interviews transcribed into written texts. This transcription involves a series of methodical and theoretical problems. One of these problems may be that once the interview transcriptions are made, they could be viewed as the solid empirical data in the interview project. However, they are not that; they are only artificial constructions from a verbally to a written communication mode. The determination about what style the transcription should be in depends on what kind of use which was meant with the transcription from the start (Kvale, 1996). Since this analysis of the transcription was not going to be of a socio-linguistic or psychological type, there was no need for transcribing in a detailed and verbatim way. That is why the transcriptions were written as a summary of each interview (cf. Appendix B). Some citations were also withdrawn from the interviews which were used in this report. To be able to check the reliability of the transcription one may make two different people transcribe the same interview, and afterwards have a computer program to list and count the differing parts of the two transcriptions, and in this way provide a quantified reliability check. In this study, this was not done, and due to this, the reliability of the data may not be proven and may therefore be a source of error. Further, to prove the validity of the data is an even more complex exercise than to prove the reliability. When transcribing the data, one is translating from an oral language, with its own set of rules, into a written language with another set of rules. Transcripts are interpretative constructions which are useful tools within some given purposes (Kvale, 1996). Due to this, there exists no correct transcription form, i.e. there exists no true objective transformation from an oral to a written mode. A good question to ask oneself when transcribing interviews are, as stated in Kvale (1996, p. 166): *"What is a useful transcription for my research*

purpose?". Based on this, it was concluded that writing summaries of each of the interview was the best solution within this research purpose.

5 Results and analysis

In this chapter the results from the interviews and an analysis of these results will be presented. The chapter is divided into sub-chapters covering the themes of the 2nd line emergency management centre, information flow between the different actors during an emergency, emergency management planning and training, collaboration technology, trust and future emergency management.

5.1 The 2nd line emergency preparedness centre

In this study the main focus is on what kind of information sharing that is done from the 2nd line emergency management centre. This is due to the fact that it is this centre which has the greatest responsibility for notifying the different actors during an emergency, along with the responsibility towards achieving and coordinating the information. Due to this they most likely also have the greatest possibility towards use of different IO concepts, as video-conference and other web-based forms of information sharing technology.

According to the information achieved from the informants in this study a 2nd line emergency management centre most often consists of the positions that are mentioned in Table 5.

Table 5: 2nd line emergency management room.

	Name of position	***Role and responsibility***
1.	Emergency response leader/ coordinator	Has the main authority in the emergency handling room.
2.	HSE representative	Follows up HSE problems, has the main authority in the emergency handling room when the emergency response leader/ coordinator is not in the room.
3.	Logistics (sea and air)	Responsible for mapping and acquisition of resources in sea and air. This position may consist of one or two persons. When two persons are employed one is handling logistics in the air, and the other is handling sea logistics.
4.	Operations / rig coordinator	Person with a great degree of knowledge about the installation. In drilling rigs this position is often held by drilling leaders.
5.	Next of kin	Handles the personnel issues
6.	Media handling	Writes press releases, and keeps track of the development of the situation.
7.	Log writer	Has the responsibility for keeping the log updated.
8.	Medical doctor	Medical resource, which may help wounded at the installation by the use of telemedicine.

In the 2nd line emergency management centre only a specific predefined group of personnel are allowed, e.g. the personnel shown in Table 5; if other personnel want to get into the room they have to get an approval from the emergency response leader/ coordinator. There may be guards that are placed in front of the door to secure that only the personnel who are approved are able to enter. The person communicating with the rig is the person with the position as operations / rig coordinator (role number 4). The HSE representative (role number 2) has the responsibility to notify the authorities together with the overall environmental responsibility during an incident. The HSE representative position may also be divided into two separate positions, namely "Authority response" and "Environment handling". In some of the companies that offers the service of 2nd line emergency management handling to different operator companies, there is no personnel in the 2nd line emergency management room who has role number 4 (i.e. operations / rig coordinator). According to one of the external 2nd line emergency management organizations, all information which regards the well-technical and other installation-specific elements must, according to the emergency preparedness plan, be handled by the support groups within the operator companies. The other interviewed organization which is offering the service of 2nd line emergency management handling (cf. chapter 1.4) sees this as a negative factor in order to maintain an effective communication with the installation during an emergency. This because the operations / rig coordinator knows the installation very well, and knows the jargon and technical terms which are used on the installations. As a result of this, not having an operations/ rig coordinator will be a factor which according to this organization will lessen the possibilities for site specific action from the 2nd line emergency management centre.

5.2 Information flow between different actors during an emergency

The map which is shown in Figure 5 illustrates the different actors involved in a DSHA regarding an acute oil spill. The different abbreviations are listed and explained before chapter 1 earlier in this study. The map is based on information from two different operator companies which operates on the Norwegian Continental Shelf. All grey lines are direct communication patterns between the 2nd line emergency management centre and the different actors. Along these lines the information flow may go both ways, but mostly the information will go from the 2nd line emergency management centre towards the other actors. The red lines are the communication lines that do not go through the 2nd line emergency management centre. The information flow between the actors who are connected with the red directed lines may not always follow the direction of the arrow; sometimes the communication flows in both directions.

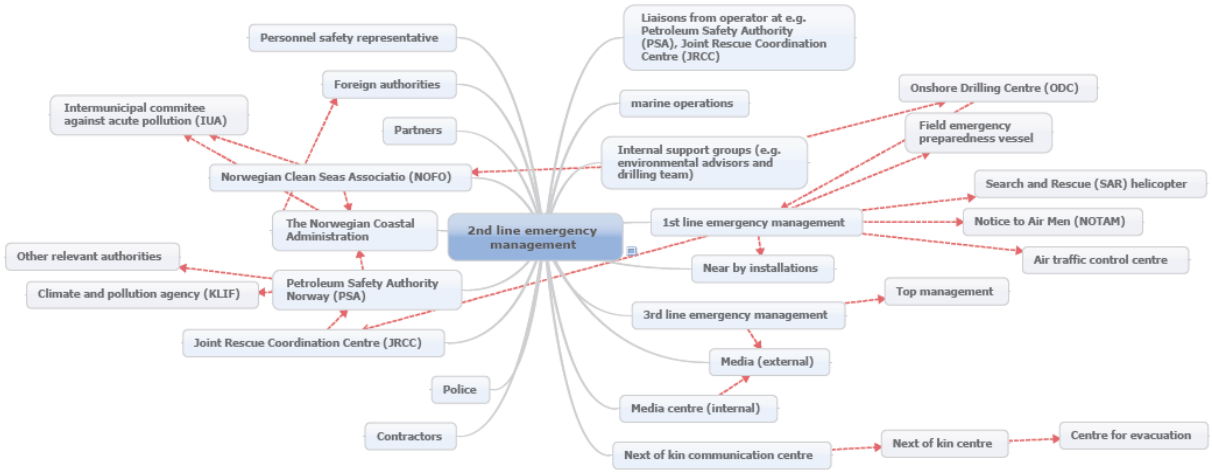

Figure 5: Actor map, acute oil spill.

Since there has often been a blow-out or other dangerous problems with the well in the period before an acute oil spill, actors such as JRCC (Joint Rescue Coordination centre) are notified to be able to help save lives at the installation before countermeasures to the oil spill are implemented. JRCC should be notified by the 1st line emergency management centre, and also by 2nd line emergency management centre when this team is established. This kind of dual notification is done in order to make sure that JRCC has received the notification and therefore has the opportunity to start preparing for a mission. In these cases, there is a possibility for liaison personnel to mobilize at the JRCC, in order to secure good communication between the 2nd line emergency management and the emergency operations centre at JRCC. Further, the person responsible for notifying the authorities at the 2nd line emergency management centre (HSE representative), shall notify PSA (Petroleum Safety Authority) as soon as possible after the 2nd line emergency management team has been mobilized; this notification shall also be confirmed in a written form. The HSE representative also notifies the police and other relevant authorities. The requirements for the operator to notify PSA is stated in The Management regulations § 29 (Styringsforskriften §29, 2011). As may be seen from Figure 5, the 1st line emergency management also notifies the SAR (Search and Rescue) helicopter, emergency preparedness vessel, NOTAM (Notice To Air Men) and the Air traffic control centre in the nearby area.

According to Figure 5, the 3rd line emergency management shall be notified by the 2nd line emergency management; the 3rd line further gives information to the top management which may be located abroad. All press releases shall be confirmed by the emergency response leader/ coordinator. In the companies which are outsourcing their 2nd line emergency management, the press releases most often has to be approved by the 3rd line emergency management. If there are very critical accidents, the media handling may be carried out by the 3rd line which also handles the media in the companies which has "their own" 2nd line emergency management centre (i.e. no outsourcing). The internal media centre has the function of giving information to the media. It is important for the 2nd line emergency management centre to notify the operator's partners about what has happened, distributing knowledge about the incident before it gets to the media. The different relevant contractors, the police and the Personnel safety representative are notified, by the 2nd line emergency management centre.

The installations which are nearby the incident may be notified by the 2nd line emergency management or immediately by the 1st line emergency management, this is very dependent upon the seriousness of

the incident. The 2nd line emergency management centre shall also notify the internal support groups. In the case of an acute oil spill these groups may be, among others, the drilling team and environmental advisors. If the ODC (onshore drilling centre) is not on duty, a task for one of these support groups is to get that centre manned. The 2nd line emergency management centre establishes contact with NOFO (Norwegian Clean Seas Association). The environmental advisors in the internal support groups may be the main point of contact between the operator and NOFO later in the course of events. NOFO notifies the IUA (Inter municipal committee against acute pollution), and keeps in contact with them during the event. If NOFO needs assistance during an event they may get this from The Norwegian Coastal Administration. The Norwegian Coastal Administration also has contact with the IUA in order to have a good way of cooperation with the local oil spill resources near the spill scene, and further to be able to borrow oil protection equipment from the depots of IUA. These connections are all shown in Figure 5. If The Norwegian Coastal Administration feels that the operator does not handle the accident in a good manner, they may, according to the informant from the Norwegian Coastal Administration, take over the operational activity of an accident as stated in the Law against pollution §46 (Forurensningsloven §46, 2009).

The "Plan for implementation of action", which is a action plan according to how the operator plans to handle the spill, shall be constructed by the 2nd line emergency management personnel and delivered to the Norwegian Coastal Administration within an hour after the 2nd line emergency management team is established. This plan shall be continuously updated through all phases of the operation; as stated in The Activities Regulations § 79 (Aktivitetsforskriften § 79, 2011). KLIF (Climate and Pollution Agency), the Ministry of Health and PSA have an arrangement which states that the operator only has to notify PSA during an incident; PSA does the further notification which is necessary in the specific situation. JRCC, which is one of the first actors who is notified from 1st line emergency management, notifies PSA such that PSA often already knows about the incident before they are being notified by the operators at the 2nd line emergency management centre. Further, PSA notifies The Norwegian Coastal Administration; the 2nd line emergency management personnel also notifies this actor. PSA are also responsible for notifying KLIF and other relevant authorities during an incident.

In the case of an acute spill where other countries may be affected, the 2nd line emergency management contacts these countries' authorities. According to The Norwegian Coastal Administration they are the authority which will have the responsibility for notifying and further communication with the foreign authorities. "Marine operations" is a surveillance system of the Norwegian coast. This system consists of three radar-sources along the coast which together gives a good picture of all activity happening on the Norwegian Continental Shelf. This system may give information to the personnel who are handling the logistics within the 2nd line emergency management centre about where different vessels are located at any given time.
The next of kin person (role number 5) in the 2nd line emergency preparedness centre works in close connection with the next of kin communication centre, such that all the information which the next of kin person in the 2nd line emergency preparedness centre has are being transferred to the next of kin communication centre where the next of kin to the operator employees calls, to check up on the status about their loved ones.

5.3 Emergency management planning and training

The emergency management planning seems to happen in the same manner among the operator companies; this because the emergency preparedness standards suggested by the authorities give a relatively specific explanation of how the risk and preparedness assessment should be carried out. In the companies which have outsourced their 2nd line emergency management to one of the external 2nd line emergency management organizations, the companies have a forum of collaboration where the

different actors have the possibility to get involved. By joining this forum they may share their different emergency preparedness plans, and try to construct similar plans. When the plans are reasonably similar it is easier for both the external 2nd line emergency management organization and for the different external actors, who shall be notified during an incident, to know how the handling of the incident is going to happen. The external 2nd line emergency management organization participates in making the bridging documents against each new well for the operator, since the operator have to have a new emergency preparedness plan for each new well they are planning to make. The Norwegian Coastal Administration base their emergency planning on environmental risk analyses and an emergency preparedness analysis. Often, the Norwegian Coastal Administration's need for emergency equipment is administrated by the government. For example, after the Full City accident in 2009 the government allocated money to a new towboat in the south of Norway, even if this accident did not have the need for a towboat. The Norwegian Coastal Administration had already stated the need for such a boat in this area in 2006.This is a good example of the reactivity which exists in the field of emergency management.

The identification of the different actors during the planning phase of emergency management is done by identifying what kind of role they have. That is, if they have a central role in the emergency preparedness work, they will be identified by their function and other actors will be identified due to the fact that it is stated in the law that they should be notified during an emergency. At the consultant companies, the different actors are given by the operator they are doing the analysis for. Overall, it does not seem to be any new form for identification of actors involved during an emergency due to the implementation of collaboration technology. The implementation of collaboration technology seems to only be in the starting phase among the informants. Even if they see the benefits of using collaboration technology and IO concepts to a greater degree in their work, it seems like there is a great degree of conservatism and scepticism towards e.g. the up-time of the network, which is one of the main factors towards why they want to hold on to their old methods.

The contractor companies are placed under the operator's 1st line emergency management system when they work offshore, but onshore they have to have their own 2nd line emergency management system. In each of their projects, they make emergency preparedness plans which, among others, show which people that shall be notified during an incident. The contractor companies is not involved in the emergency preparedness planning that the operator does, but they are involved in exercises and drills which the operator arranges. During each of the offshore shifts there is an evacuation alarm, where all employees on the installation have to put on their survival suit and get into the lifeboats. This was also mentioned by one of the operator companies during the interviews. The operators may also run larger exercises where they are testing the whole emergency management system. During these exercises, the contractors at the 2nd line emergency management are also involved; these kind of exercises happens precisely every other year.

According to one of the operator companies, all the different DSHAs shall be trained on by all the shifts on the installation during a time period of two years. In addition to these exercises, the personnel within the specific emergency response teams shall practice on their function once each shift. The personnel who possess an emergency function must join a refreshment course once every other year. Emergency preparedness drills are also performed each year. These drills involve multiple systems, helicopters, boats, etc. The operator company emphasizes the difference between exercises and verification exercises, where exercises means that you train on a specific event, while the verification exercises are exercises carried out to check if you reach your performance requirements. The verification exercises are performed from the 2nd line emergency management, while the regular exercises are managed by the 1st line emergency management. After the Scandinavian Star accident, there has been an increased focus on proactive emergency management. This means, among other

elements in practice, that during the status meetings the emergency response leader/ coordinator puts the focus points up on a board such that everybody works towards the same goal.

One of the contractor companies stated that they wanted to be involved in the operator's emergency preparedness work. The informant feels that the resources they hold could come in handy for the operator during an emergency. The 2nd line emergency management at the contractor company has not been involved in exercises that the operator has performed (but it is important to remember that the informant only has been working at this contractor company for 2,5 years). The contractor feels that the lines of responsibility between the operator and the contractor should have been drawn more thoroughly. This is because that during an emergency everybody have clear lines of responsibility and, due to this, knows what to do and have access to the information they need (e.g. access to the operator's status board). The contractor also wants to have a person from their company present at the operator, to be able to be continuously updated on the status of the emergency at all times. One fact that the contractor companies mentioned as important to point out, is that emergency management is not something which is meant for everybody to be able to handle; this discipline demands a great deal of experience in order to know what to do under a stressful situation.

One of the operators emphasizes that if you do not exercise and train on all the functions in an emergency preparedness organization, the whole organization will fall down as a house of cards if something goes wrong one place within the organization. The operator also focuses on that the emergency response leader/ coordinator has to have a proactive view into the organization, i.e. to be able to predict what is going to happen in the next phase in the emergency management process. The operator also emphasizes, in the same way as the external 2nd line emergency management actors, the importance of no interference between the 3rd line emergency management and the 2nd line emergency management's handling of the situation.

5.4 Collaboration technology

The utilization of technology within companies during an emergency situation, most often consist of a log system (usually CIM or Crisis manager), telephone and e-mail. In one of the external 2nd line emergency management organizations, the communication towards the internal support groups is also done by the use of videoconference. The Norwegian Coastal Administration uses, among others, "kystinfo" which is a map that shows where the different resources are at any given time. This map is in use both among internal and external actors. In their handling of "Godafoss", The Norwegian Coastal Administration used "Projectplace" to manage and plan what to do during all the phases of their emergency management. Still, the technology used for the transfer of information between external actors, e.g. the operator and the contractor, and the operator and PSA is mainly done by telephone.

There were many different opinions about which factors which were considered the most important in order to collaborate in a good manner during an incident; these are shown in Figure 6.

Figure 6: Collaboration factors.

The most important factor in order to collaborate in a good fashion mentioned most often by the informants was to have a clear role clarification and role distribution. One of the external emergency management organizations focused on the importance of trust to the person who is handling the incident; this person must have the knowledge, training and authority to fulfil its role. The development of this trust is achieved trough co-training, and in this way showing the operator, authorities and other relevant actors that the external actor manages to do their job. This is also what PSA focuses on, something they feel that they have achieved by years with dialogue, discussions and exercises with the operators. The Norwegian Coastal Administration focuses on the involvement, which is a close dialogue between the different parties during an incident, in a way such that all parties may give their contribution when a new operational command shall be put into action. The Norwegian Coastal Administration also puts a great deal of emphasis on training, education and understanding such that the possessors of the roles know what their own role is all about. The informant often sees people who misunderstand their own role, a factor that contributes to a great deal of confusion both for themselves and for others. At one of the external 2nd line emergency management organizations, the most important factor is the role declaration between the 2nd line emergency management and the 3rd line emergency management. This because many of the people who now has positions in the 3rd line emergency management earlier had positions in the 2nd line emergency management, and they often do not manage to keep to their own business (i.e. they also want to know in detail what is going on in the 2nd line). This is why one of the external 2nd line emergency management organizations wants to focus further on the role division by involving the 3rd line emergency management in a greater degree during training. One of the contractor companies states the most important factor as having plans which are well known, such that everybody knows what has to be done. To have the emergency preparedness plans in folders or on a server are not good enough to establish a robust organization. It is important that the people know the emergency preparedness plans and participates in exercises to be able to imagine situations of "worst case scenario", and further to get a hold on what their roles and responsibilities are and how to handle them during emergency situations.

The informants in one of the operator companies, NOFO, and the Norwegian Coastal Administration all feel that there is an information overflow during an emergency, especially when concerning the log.

It is also important to remember that the log may not be better than the person who writes it. One of the contractor companies feels, on the other hand, that they get far too little information and therefore wants an increasing amount of information from the operator during an emergency. The new 2nd line emergency management organizations feel that the information flow functions very well. One of the external 2nd line emergency management organizations mentions that the information flow is great between all three emergency management lines, and also between the operators internal support groups and the 2nd line emergency management. One of the external 2nd line emergence management organizations mentions that during exercises, personnel in the 2nd line emergency management centre has started to work on the wrong incident on the logging system which they use, and that it took some time before this mistake was detected. One of the operator companies emphasizes that the log system they use today is not optimal, but it is the best system available and there will always be a focus on further development of this system. It seemed clear that the forms of communication which the outsourced 2nd line emergency management centres use, were based much more upon utilization of IO concepts compared to the internal 2nd line emergency management centres use as communication device.

The different actors saw different possibilities for use of collaboration technology in emergency management. Some were very open for the use of video conferences and generally for the use of technology in a greater extent than today; specially the new organizations which handle the 2nd line emergency management for the operators. These actors have to use this kind of technology to be able to cooperate with the operator companies. They utilize the IO concepts to be able to talk to each other even if they are located in different areas. This may be illustrated by a statement which an informant from one of the external 2nd line emergency management organizations had:

"It does not matter for me if the contact person / rig coordinator sits in his own office or at our office, the main focus point is that this person is located at the place where he has the best surroundings to perform his job".

Also one of the contractors was very positive towards the use of more collaboration technology in their cooperation with the operator companies. According to one of the contractors, one of the operators and one of the external 2nd line emergency management organizations one would, by implementing a greater degree of collaboration technology (e.g. video conference and pictures), make the different actors be more up to date on the situational picture during an emergency situation. Use of collaboration technology facilitates interaction between the different actors in a greater degree, since by using this kind of technology it is possible for all parties to possess the same picture of the situation, and the different actors may come with their kind of special expertise to help handle the incident. One of the contractors also see the possibility of getting more information from the operator with respect to what they can tell the next of kin, media and the rest of the stakeholders. During an emergency, the next of kin to the contractor's employees will call the contractor to get status updates; the contractor do not always feel that they have enough updates, and due to this they feel that there is a need for a closer collaboration between the operator's next of kin centre and the contractor's next of kin centre.

At one of the external 2nd line emergency management organizations, the 1st line emergency management do not have access to the same log system as the 2nd and the 3rd line emergency management, but they clearly see the potential for an increased degree of efficiency in the sharing of information by implementing the same log system. By giving the 1st line emergency management access to the log, they have the possibility to see what resources the logistic person in the 2nd line emergency management has allocated (with regard, to among others, their placing and arrival times). Today, this kind of information is brought forward by telephone. It is also possible for the public

actors (e.g. PSA) to be able to have access to the status board of the log during an incident. In this way, PSA and the 2nd line emergency management would have avoided the telephone dictate which they have to perform today. Further, PSA would be able to be continuously updated regarding the handling of the incident. One of the external 2nd line emergency management organization stated:

"*… the technology, the possibilities and the screens are present. The only thing missing is that someone grabs the opportunity and uses this technology.*"

When talking with PSA, they mentioned that they wanted to be updated by telephone; this because PSA is a regulatory authority, and during an incident and they want to ask the operator / the 2nd line emergency management questions about e.g. their action plan regarding handling of the incident. PSA feels that, by receiving the information online, they will lose their possibility to ask follow up questions about the action plan. Further, they feel that the operator may put some of the responsibility about identifying the needed countermeasures over to PSA. Said in another way; you decrease the quality of the transferred information by using IO technology. PSA and JRCC tried to connect their log systems, such that each part could see each other's log. This connection was, after a short period of time, deactivated because both PSA and JRCC felt that they got information overflow. This is also something they feel may be an issue if they should share the log system with the operator.

According to NOFO, other possible problems by the use of collaboration technology may be that the systems, in which the different actors are using, are not compatible with each other. This is because the companies that create the systems often make them exclusive, i.e. in a way such that they are not necessarily easy to connect to other systems. This may be due to the functional requirements that the user has to the system, e.g. the Norwegian Armed Forces have stated requirements that imply that their system shall not be visible for others. This requirement is also put forth from the police and also the National Health Service in parts of their system, which result in the fact that these systems cannot "talk" with each other. One of the challenges in which NOFO are currently working on, is to develop common platforms and standards which make it possible for the systems to talk together. As an example of this concept, is that NOFO may easily "talk" with JRCC, since these two organizations have the same platform. NOFO also has a tight collaboration with the Norwegian Coastal Administration, such that when the Norwegian Coastal Administration is going to build their new information system, they most likely will build it on the same platform as NOFO and JRCC. NOFO has as a goal that all the actors who participate in an oil spill emergency preparedness situation shall build their collaboration technology on the same platform. It is also important according to NOFO that the system is well known, in a way such that the operator of the system may focus on the battle in the field and not "the battle" with the computer. Another factor is not to develop a too large dependence upon the system, such that in case of a system break-down or with loss of power, the personnel still knows what to do. This is also something which one of the contractors, both the external 2nd line emergency management organizations, and the Norwegian Coastal Administration, mentions as important focus areas. Further, one of the informants also tells that with their use of the log system, one of their 2nd line emergency management personnel started working on an old event and not on the event which were established for the event they were training on at that time. The problems which were mentioned by the informants within the use of collaboration technology are mapped in Figure 7.

Figure 7: Problems with the use of collaboration technology within emergency management.

The implementation of new technology has, to a certain degree, resulted in a change among which kind of actors that are involved in an emergency handling situation. As mentioned in chapter 1.2, there exists now a much higher degree of small operator companies which does wildcat-drilling on the Norwegian Continental Shelf. These companies are so small that they do not have the possibility to run a good and up to date 2nd line emergency management organization; because of this, some companies are now offering to handle the 2nd line emergency management for these small operator companies. This is also what the different informants mentioned as the new actors who have evolved in an emergency situation; as PSA mentions:

"... the only way the outsourcing of the 2nd line emergency management is possible, is by using collaboration technology".

Along with this, one of the external 2nd line emergency management organizations says that they are only waiting for the larger operator companies to realize that this form of outsourcing of the 2nd line emergency management is the most sustainable way to perform these activities; this regards expenses, professionalism and use of time.

NOFO feels that the implementation of new technology has led to a greater degree of decision-making support. This because that you may sit onshore and have the same picture in front of you on the screen as the personnel offshore has. This enhances the situational awareness of the personnel onshore, and further increase the possibility to make a right decision at the right time. The Norwegian Coastal Administration feels that by using e-mail and "Projectplace" in the emergency handling, their telephone usage has decreased to a large degree, and made it possible:

"*… to use the leftover time and the remaining degree of brain capacity to think ahead around the expected development, and about how to reduce the extent of the negative development*".

5.5 Trust

There are different understandings among the informants of how trust is established among the actors during an emergency, both internal and external. However, the major share of the informants mentions trainings and drillings as the best way to create trust. NOFO especially mentions that you have to train

and create fellowship and collaboration in "times of peace". By training together, one gets an approval regarding that the collaboration works, and if it do not work one has to implement efforts to make it work. NOFO also mentions that trust establishes itself when you are in social gatherings, e.g. when you grab a cup of coffee together with the captain on the bridge. One of the external 2nd line emergency management organizations mentions that trust is something which shall emerge as a result of an efficient organization. For them it is very important that the people who has specific roles in an emergency management setting, masters their role and has a good competence within their role area. They emphasize the importance of a large enough amount of training, such that the person who has the role is comfortable with its role. The other external 2nd line emergency management organization emphasizes the importance of getting to know each other on a social basis before trainings and drills starts. They also focus on performing an evaluation after each of the exercises in order to receive feedback regarding what was done right and which factors they have to improve on.

The answers regarding the question about whether the informants had trust to the different people and / or roles without actually knowing them, half of the informants which answered the question said that they trusted them, while the other half did not have this kind of trust. Both one of the operator companies and one of the contractor companies trusted the role that the person had. The contractor company said:

"When an operator calls you to inform about an emergency, you trust that this person give you the right information".

This operator company simply trusts that the education and training that the person has in order to possess a specific role is adequate. On the other hand, the Norwegian Coastal administration has, by experience, found that the title / role is not necessarily on par with the level of knowledge. As this informant said:

"*It is by action, and not by title, that you show if you are trustworthy"*.

The informant also mentioned that you cannot go in to a relationship with distrust towards the other party; i.e. you have to start a relationship with trust. The informant from NOFO feels that this trust issue is dependent upon which system you are in. For example, if you talk to the captain on a boat you know that this person must have performed a special education to be able to hold this title. On the other hand if you work with a person who tells you that he is an accident scene leader it is difficult to understand what kind of knowledge this person has. That is why DSB (Directorate for Civil Protection and Emergency Planning), The Norwegian Coastal Administration, and NOFO have been cooperating to develop a system within a general education, where certain demands shall be fulfilled to be able to hold a title. In this way, all the people who hold a title would have the same basis education. The informant from NOFO has often experienced a loss of trust; this mistrust is mainly connected to individual people and not to organizations as a whole. Further, the informant from NOFO emphasizes the importance of the different levels of expectation which you have for the different organizations. There are different expectations for performance if you are contacting the public authorities (such as the JRCC, the Police, and the Norwegian Coastal Administration), one will expect that these authorities would handle the request in a respectable and honest way. These organizations usually have a predictable and uniform way of handling the situation. This concerns also the NGOs (Non Governmental Organizations), which are also highly trained and organized in such a situation (e.g. environmental organizations, etc). Still, you may find large local variations between the individual organizations. A supply vessel in the North Sea is subject to very different regimes and rules when it comes to safety than, say, a fishing vessel or other vessels. The informant also has different expectations to e.g. a gas tanker and a vessel transporting sand. This is due to the fact that you know that the gas tanker is used to work within strict safety regimes, safety regulations, etc., while a vessel

transporting sand may not follow as strict regimes since the cargo do not involve as great risk as the gas.

When questioning the informants about their trust towards the technology, everybody except one of the operator companies said that they had little trust towards the technology. This operator company has complete trust in that the right information is communicated to the right person. Among the informants, almost everybody emphasize the importance of verifying that a message / information is received and understood. PSA also emphasizes the fact that it is often the human in combination with the machine that fails (i.e. not the machine by itself). One of the external 2nd line emergency management organizations focuses on the small degree of redundancy in the communications infrastructure and the mobile network. Both NOFO and the external 2nd line emergency management organizations focus on the fact that you have to make room for a possible failure of the technology, as the external 2nd line emergency management organization says:

"You have to use a "what if" mindset, to be able to handle an emergency in a good way".

As mentioned above, only one of the operator companies had a great degree of trust that the right information reached the right person. The other informants did not have trust in this area, and due to this they demanded some kind of verification to be sure that the information reached the right person. One of the contractor companies wants to have a person in the operator's observation room to be sure that they get all the information that they need, something that may not reflect their trust towards the technology (but rather their trust towards the operator). In Figure 8 you see a summary of the most important issues the informants gave around the concept of trust in an emergency situation.

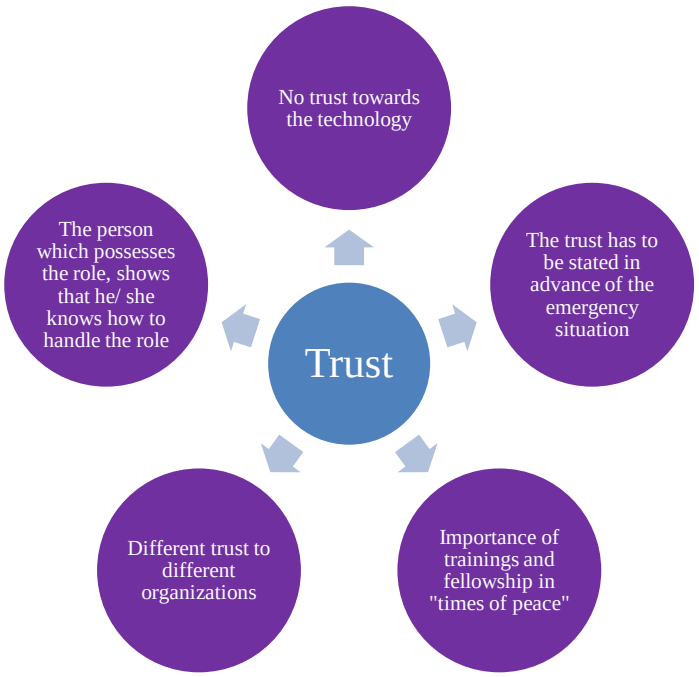

Figure 8: Summary around issues within trust in an emergency management situation.

5.6 Future emergency management

When asking informants about how they saw the possibilities for IO technology to be able to be useful in a proactive way during an incident, they answered that it may be useful due to the fact that it could trigger the emergency preparedness situation on a much earlier time. Due to this one may introduce the different countermeasures into the incident at an earlier time and prevent the incident from escalating.

According to one of the operator companies, this is dependent upon when you define the emergency management phase to start; is it when the deviation happens?; or is it when the accident already has happened? In a big picture, it is the IO technology which makes it possible to intervene earlier in the process when a deviation has occurred. One may therefore have to redefine the emergency preparedness concept to be able to be proactive in a greater degree.

On the other hand, The Norwegian Coastal Administration belongs to the group which feels that the emergency management situation is when the accident has happened. The way that they see the IO technology to be useful, is for monitoring and sharing of information before an accident happens. One concern the informant has, is that the emergency management organization builds its capacity in connection with the mobile network. This network is not built to be able to handle an emergency situation, and one should therefore not build the emergency management organization around it.

By the use of IO technology, one of the contractors feels that it is easier to share information, and also to get the right kind of information to the right kind of people. By not only receiving information verbally, but also in writing and / or in pictures, does it much easier to mediate the right information. NOFO feels that IO technology may be useful in making things proactive in a situation of deviation, but it is very important that the human in the "human-machine"-relation knows what they are doing, since the systems may not tell you that something is wrong. This is why it is so important that the human in these systems knows what is going on in the system, or else it may never be proactive. One may get a few simple warnings from the system; in a way such that you get a "heads up" before a barrier is broken. These "heads up" functions are based on very simple presumptions, while "the long and important lines" will, in such a system, not be revealed. It is important to emphasize that some of the systems which uses IO concepts, are very detailed with checklist, etc. In this fashion, the operator will "walk through" the system by the checklist; this kind of IO technology utilization may be very extreme. Another way of using this technology is something which the informant calls the "Clint Eastwood method". The method bases itself on the concepts of: "adapt, improvise, and overcome". This means that there is no simple plan for finding the right solution, but you solve the problems along the way. The informant's way of solving problems goes in the direction of the "Clint Eastwood method", due to the fact that the informant knows his profession very well. But, if one is to build an emergency preparedness organization around an organization which does not work with emergency management on a daily basis, you may need to use checklists and other kinds of support equipment in a greater degree. In practice, this means that you need a totally different kind of management system for actors such as the police, JRCC and the Norwegian Coastal Administration, than you would need for operators who handles an emergency at a seldom basis. The informant from NOFO feels that the use of IO technology is best used by giving the right situational picture over the event. The informant is not confident enough on the technology such that the technology may make decisions for the informant during an accident; put in the informants own words:

"*The more involved the system is in taking decisions for a person, the more my stomach hurts*".

According to NOFO, training and exercises are also very important factors to be able to handle an incident. By the use of training and exercises you prepare yourself for the situation to come, and when the situation happens you know what to do, and also have the possibility to think in a proactive manner during the handling of the incident. One of the external 2nd line emergency management organizations and one of the contractor companies also think that the only way to make organizations think proactive is by repeatedly trainings and exercises. According to the external 2nd line emergency management organization, one way to be proactive during an incident is by dividing the status board into two pieces. One piece will contain what is done and the current status, while the other half contains proactive measures about how to impede things to go wrong. By dividing the status board in

two pieces the personnel, who are not present in the room when the meeting is held, get a hold of the possible proactive measures that may be implemented in the future phases of the emergency handling.

The consultant company's (C) evaluation of the 1st line emergency management situation at the different operators is that the connection between the offshore control room and the emergency room offshore is very good; there exists short and clear communication lines. Still, a concern which C possesses is that these communication lines will not be so good when the control room is moved onshore. The informant has doubts about maintaining this kind of efficient contact.

A problem one of the external 2nd line emergency management organizations notices with respect to the use of IO technology is the willingness of the personnel offshore to be constantly monitored. Still, they also see the benefits of monitoring since the onshore personnel have high situational awareness at once the incident has happened, without having to go through the reporting phase. The faster you get situational awareness onshore, the faster you will be able to start a proactive mindset to be able to help the installation.

According to what that may be done to improve today's emergency management, the Norwegian Coastal Administration feels that there has to be an increased focus on an improvement regarding research and innovation in the development of new methods for mapping the different areas of risk.

Figure 9, shows some of the different actors' meanings about the use of IO concepts.

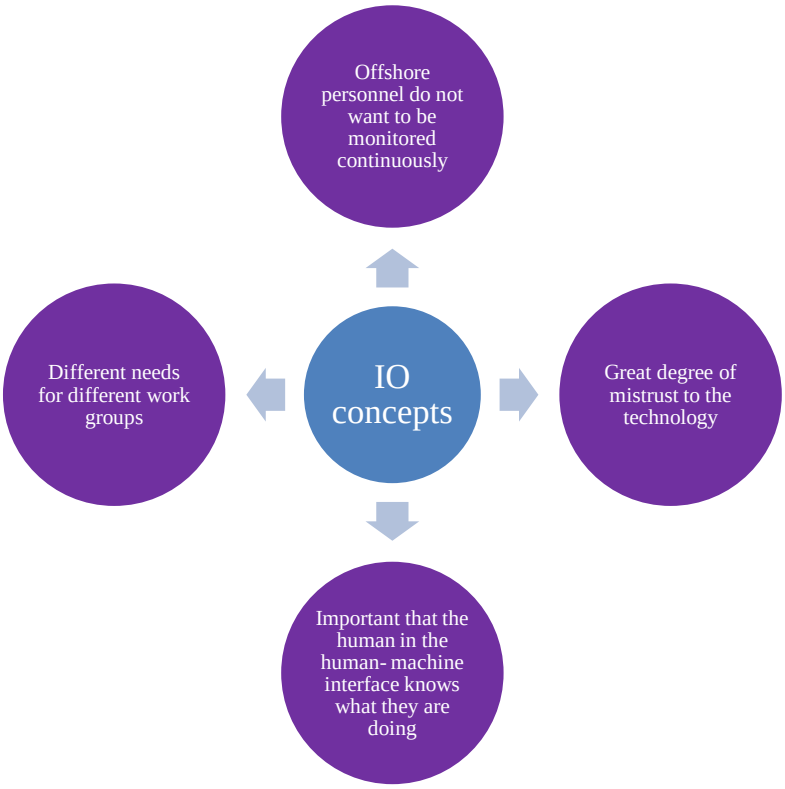

Figure 9: Challenges related to IO concepts.

The informants' answers around a question that has received a lot of media attention lately, namely if we are able to prevent a disaster like the Deepwater Horizon in Norway, were not clear. NOFO states that they have the equipment to prevent the accident to become as great as was the case in the Gulf of Mexico, but there are very many parameters which may make the emergency management extremely difficult to handle. For example, if it is sleeting, a lot of the technological equipment will lose much of

their function; this may regard radars and other communication systems. Further, C thinks that it is not the emergency management which may prevent a catastrophe like the Deepwater Horizon to happen in Norway, but that there has to be a greater focus on the underlying causes that leads to an incident, in order to be able to be better prepared for it. The Norwegian Coastal Administration states that there is no emergency preparedness in the whole world which is dimensioned for such an accident as the Deepwater Horizon. The emergency preparedness is dimensioned on basis of risk analyses, but according to the informant it should be dimensioned according to worst case scenarios.

6 Discussion

In this chapter the main results from the interviews will be discussed with regard to the research questions in chapter 1.3. Further, the information presented in the chapters 2, 3, and 5 will be used in this discussion. The discussion is divided into five parts focusing on: the Actor map; Traditional organisation of the 2nd line emergency management and outsourcing of it; Trust and resilience; Resilient emergency management; Putting the resilience pieces together; and Recommendations.

Before contemplating the research questions, the most important findings in this study are:

- The use of IO concepts for collaboration between the different actors involved in an emergency is found to be greater at the external 2nd line emergency management organizations than at the traditional 2nd line emergency organizations.
- There are many opportunities within emergency management in which IO concepts could be used today (e.g. video conference). Still, such concepts are not highly utilized, which may be explained by some degree of fear that the technology at hand is not reliable enough during an emergency.
- On the other hand, NOFO, the Norwegian Coastal Administration, one of the operator companies, one of the contractor companies, and both the external 2nd line emergency management organizations are interested in, and positive towards, the use of new technology for sharing of information in emergency management.
- By implementing and using other technological devices than telephone to distribute information during an emergency, the PSA feels that the operator may give too much responsibility upon PSA and further that PSA lose a part of their supervising authority.
- The different actors within emergency management often knows each other in advance, and due to this the degree of swift trust is low; i.e. trust between the actors are most often built in advance of an emergency setting because the actors often knows each other from before.

Some of these findings are considered as so important for this study (cf. chapter 1.3) that they are considered as essential elements of the following discussion.

6.1 Actor map

The actor map constructed with information from the informants (cf. Figure 5) indicates that the connections between the different actors during an emergency are very complex. Many actors are to be notified during an emergency, and in some of the connections the information sharing is exceeding one-to-one complexity. There may be connections between the different actors which are not found in this study, and it may also be actors missing in the map in Figure 5. Due to the great degree of actors involved during an emergency, it may be useful to implement a common log system for all the actors involved in an emergency situation (as mentioned by one of the external 2nd line emergency management organizations). As Figure 5 shows, there are many actors and it is possible that some of them may be forgotten (or "feels forgotten") due that they do not receive an update as often as desirable during a stressed emergency situation. The empirical data indicates that one of the contractor companies wants more information regarding the status of the situation. If one has an emergency management log system which enables all the involved actors to receive the information they need regarding the situation, the issue of not giving information to the right person at the right time would be decreased. However, since no person or technology is infallible, it will always be possible that the information is not communicated when it should. All in all, a more accessible information system

would most likely result in more efficient information sharing and maybe more efficient problem solving because the right people receive the information they need faster. NOFO mentioned that the utilized systems must not result in the system's operator using their time battling with the computer and not being able to focus one hundred percent on the battle in the field. In order to avoid such situations, it is necessary with a great degree of training on the system.

As mentioned in chapter 3.2.3, Tveiten et al. (2010a) stated that the "new methods of working" (i.e. the implementation of IO concepts) had led to a different actor map during an emergency today in contrast to earlier. Figure 5 illustrates the different actors involved during an acute oil spill; the interfaces between the different actors do not seem to have changed in a great degree from earlier. This may be explained by the fact that telephone still is the main communication tool which is utilized as an information channel by the different actors in an emergency setting. Further, the list that shows which actors that have to be notified has not changed to a great degree due to the implementation of more ICT in their daily work. Regarding the introduction of new actors, the informants mention two; namely the independent 2nd line emergency management organizations, and the small operator companies that use these independent 2nd line emergency management companies. In these operator companies there is a greater need for utilizing collaboration technology to be able to handle the emergency in an adequate manner. Due to this, the empirical data implies that the map over the different actors is still the same, but the 2nd line emergency management is now outsourced (it is not located on the premises of the operator company anymore). The 2nd line emergency personnel are now professionals within emergency management, and not personnel who only have this profession as an extra work-task (which is often the case within the large operator companies). When this kind of responsibility is viewed upon (only) as a secondary work position, the tasks may not necessarily receive the required attention and the tasks could therefore be branded as low-priority.

In Tveiten et al. (2010a) the difference in the actor map was directed towards the contractors and the internal support groups (cf. chapter 3.2.3). In this study only two contractors were interviewed and there were no interviews with the internal support groups. This means that there is not enough material in this study to state whether there is no change in the actor map (except for the new 2nd line emergency organizations and the small operator companies). In this study, it emerged that the contractor companies wants to be more involved in the operator's emergency management work. In the longer term, new and improved interfaces between the operator and the contractors may be constructed.

6.2 Traditional organisation of the 2nd line emergency management and outsourcing of it

The empirical data indicates that in the external 2nd line emergency management organizations there are a high degree of learning, because during all the different trainings the different operators learn from both the positive and the negative things which may happen. According to one of the external 2nd line emergency management organizations, feedback is highly focused upon after each exercise; feedback where they discuss what went right and what went wrong. All too often, the focus is on what went wrong during an incident, but it is also important to focus on and learn from the things which went well. This is one of the factors that Hollnagel (2011), emphasizes when discussing the resilience pillar that concerns learning. Hollnagel bases this fact on the argument that it is easier to learn from something which happens often than from something that happens seldom. One may witness this fact on the frequent trainings which are performed within the organizations that offer to handle the 2nd line emergency management for the operator companies. The external 2nd line emergency management organizations are then able to increase their training on emergency management handling, and also be more professional, since this is their "only" job. When these organizations get more and more clients,

they can construct a greater platform of experience and further have the possibility to see weaknesses and problems within their own and their clients' ways of handling an emergency. The experience may make it easier for them to see the early warning signs which may emerge during training, and further respond to these signs in order to prevent them from happening during a full scale event. It is also very important that the personnel who are manning the 2nd line emergency management centre always have a forward-looking focus. This means that they implement a proactive mindset in order to anticipate what might happen in the future, and construct monitoring mechanisms with indicators that are able to detect the anticipated events.

There may also be negative elements regarding outsourcing of the 2nd line emergency management. Since there are no in-house 2nd line emergency preparedness personnel anymore, the valuable information transfer from experts within emergency management to other personnel within the organization is lost. Another factor is that the 2nd line emergency management organizations have to set a limit on how many operator companies they have the capacity to work for. If several accidents happen at the same time, there may not be enough emergency management centrals and personnel available that are able to handle the emergency for each of the operators involved. So even if it is good to have experts on the field handling the emergency management (i.e. the 2nd line emergency management), the development within this field may stagnate due that the most time- and cost-efficient way of handling emergencies is to do it in one particular way for all the member companies. The cost factor is present because some of the companies which offers 2nd line emergency management are consulting companies; companies that may over-focus on profit. Emergency management is not an area where it is suitable to be "greedy"; it is necessary to put in your best and most experienced personnel. In a consultant's mindset this could mean that the best emergency management personnel are presented as the most expensive ones for the customer, which further may result with the operator companies wanting to save money on this field requesting cheaper personnel; the great degree of competence which the 2nd line emergency management personnel should possess may not be present. This may be avoided when having the 2nd line emergency management inside one's own organization, since the employees then belong to the organization, and the pressure on profit could be avoided since all the employees earn on avoiding an accident.

From the empirical data it seems that for the operator companies to be able to offer a 2nd line emergency management which are just as good as (or better than) the one that the outsourcing companies gives, the operator company has to be a reasonably large company in order to fill all the positions in which the 2nd line emergency management possesses. One relevant factor which were discovered during this study is that the operator companies which have their own 2nd line emergency management utilize, to a very little degree, IO- concepts for sharing of information, while the outsourced 2nd line emergency management units have to utilize IO-concepts in order to have a great enough contact with e.g. the internal support groups within the operator company. Since the internal support groups may be located in another part of the country, they have to use videoconferences and other equipment to be able to have the same picture over the situation. As mentioned in chapter 5.4, the informant from one of the external 2nd line emergency management organizations said*;*

" It does not matter for me if the contact person / rig coordinator sits in his own office or at our office, the main focus point is that this person is located at the place where he has the best surroundings to perform his job".

This may indicate that the organizations which are handling the 2nd line emergency management for the different companies are not as old-fashioned with their information-sharing as the operator companies which handle the 2nd line emergency management on their own. My own reflections about this theme is that the external 2nd line emergency management organizations witness, to a greater

degree, the usefulness of utilizing new technology, and they also utilize it to some degree within emergency handling. They see the possibilities within the technology, and are not as "afraid" of trying new things as some of the other actors interviewed in this study. Specially one of the 2nd line emergency management organizations mentioned the possibilities regarding the use of a log system which may give all the actors involved in an emergency management situation access to updated information about the status of the emergency. This concept is also mentioned in chapter 6.1, and seems (from my point of view) to be a very good device for information-sharing between the different actors within an emergency situation. It is important to consider the user interface, which should be designed and constructed in a way that *"it is not possible to do mistakes"* when the different users utilize it during an emergency. How to design and construct such a system is not in the scope of this study, and it will not be discussed any further. However, it is important to have in mind that the log systems used today in the external 2nd line emergency management organizations are not optimal. In chapter 5.4 it is explained about one incident when one of the personnel in the 2nd line emergency management organization started to work on the wrong incident in the logging system. This shows that the technological solutions used in this log system was not good enough; they were not build on a manner that were resilient enough to withstand the possible failures that may be done by stressed personnel during an emergency. During situations of stress there are many factors which add together towards the person's actual response upon the situation. This is mentioned in chapter 3.2.2 by Chen et al. (2010), and correlates in a good manner with the findings from the interviews which are shown above, namely that stressed persons often starts to underperform on their tasks and more often make mistakes. There may be many reasons why the particular person in the 2nd line emergency management started to work on the wrong incident, but it may be evident that the log system did not have good enough control mechanisms making sure that the personnel starts to work on the right incident. It is possible that an introduction of a checklist before handling of the emergency is a good solution towards avoiding these kinds of mistakes in the future. In chapter 5.4 some of the informants mentioned the possibility of being more up to date on the situational picture as an important factor which the implementation of collaboration technology may bring along. This may be done by e.g. having a log system which shares real time situational pictures of the emergency between the involved actors.

The most important collaboration factor mentioned by the informants was to have a clear role clarification and role distribution. During an emergency, tasks and activities must happen in a fast and correct manner. Because of this, people need to know what roles different people possess and also that the person or people that possesses the role knows which responsibilities and actions that are expected by the person possessing the role. One of the external 2nd line emergency management organizations explains this as:

"*... a person having the authority, knowledge and training to fulfil its role in a good manner*".

To be able to achieve such a role clarification and role distribution, training has to be an essential part of emergency management, since during training the personnel gets to know which kind of responsibilities and duties that follow their own and the other personnel's roles.

It is also important for the different actors who participate in an emergency management situation to build their collaboration technology on the same platform (i.e. that the different participants all uses systems which are compatible); this to render possible information-sharing between the organizations in a safe and efficient way. A compatible system is something which NOFO and HRS has implemented, and that is stated as well-functioning. With a common platform, it would be easier to communicate between the different actors during an emergency, and it would also be possible to

achieve a faster response phase when an emergency has happened. To have the same technological platform is stated as a necessary step towards creation of trust between external actors by Kasper-Fuehrer & Ashkenazy (2001). If the different actors could be updated upon the situation by for example checking the operator's log, the sharing of information would be done much faster. This would also imply that personnel who usually sat in the phone to update the different actors would be free to use the "phone free time" to think in a proactive manner and concentrate on how to solve the emergency in a best possible way. This is something which the Norwegian Coastal Administration experienced when they started to use e-mail and "Projectplace" to a greater degree when planning what measures to implement during an emergency.

As mentioned in chapter 3.5, emergency management has its basis in the ability to respond. The ability to respond mainly relies on two strategies, namely to anticipate the potential event, and to predefine the potential ready-for-use solutions (this may be emergency preparedness plans which are made due to the identification of the different DSHAs). When you have to make ad hoc and / or improvised solutions to a problem, the first strategy can be considered as the proactive and the second as the reactive. One problem with the strategies is how to establish and maintain a correct responding phase throughout the system's life-cycle. The degree of resilience lies in the operator's ability to anticipate, monitor, detect, accept, and decide that the system has breached its boundaries for potential variability. Many accidents may be understood as a result of a failure to recognize and / or accept a derogation of the situation outside the stated boarders of expected deviations from the basis which leads to a continued use of the current (de-adapted) strategies. Here, two versions of anticipation emerge, first the ability to anticipate future situations, but also the different personnel's capacity to cope when the system gets out of hand (Pariès, 2011).

In chapter 3.2 Landrigan et al. (2010) stated that the personnel in the 2nd line emergency management centre needs to:

- Monitor and analyze the data
- Communicate the situation to others
- Communicate with others about how to handle the situation
- Determine how to handle the situation

All the factors mentioned above may be seen as parts of the responding phase, since there is a need for monitoring and analyzing of the achieved data to be able to know how to respond. To communicate the situation to others and communicate with others about how to handle the situation is a big part of the responding phase. It is very unlikely that one person may handle the whole situation by himself / herself; the receiver of information needs to communicate with others about how to handle it in the best possible manner. Finally, the actor has to determine how to handle the situation, based on the findings and solutions achieved from the aforementioned bullet points. All this adds up to being part of the responding phase. Further, the responding phase results in an outcome comprised of five challenges: possibility for high stress; information overload; intense collaboration; irregular work patterns; and diverse experience. This correlates well with the statement put by one of the contractor companies, where the informant emphasized that emergency management is not a task which suits everyone and that it is important to have experience in order to handle an emergency in a good manner. If one lacks experience, it is easy to get stressed when a new and unforeseen situation arise. This is not stated to a great degree in the empirical data, but it is an issue most people experience when exposed for a new, time limited and challenging situation, as emergency management may be. In chapter 3.2, Chen et al. (2010) states that challenges of psychological stress such as anxiety and frustration may be a problem in emergency management, due to the fact that people underperform and

make mistakes when they are stressed. The same author also points out that people seem to reduce their ability to improvise when they are stressed, which may be problematic since one could need these kinds of capabilities during an emergency. The need to improvise is stated by Wilhelmsen (2010) in chapter 3.5 as one of the main factors necessary in order to handle the response phase of resilience engineering in a sufficient way. In order to improvise in a good manner, it is necessary with creativity, knowledge and skills. In the empirical data, this emerged to a great degree from the interview with NOFO. It is not necessary that everybody have the same kind of technology during an event; a person working with emergency management every day, do not need the same kind of system regarding checklists and other equipment as the personnel who are only handling emergency situations once every second year. The informant uses a methodology during an emergency which bases itself on the fact that there is no simple plan for finding the right solution – you must solve the problems along the way. This is what the informant calls the "Clint Eastwood method" and it bases itself on the concepts of; adapt, improvise, and overcome. In Pariès (2011), they emphasize the same fact, namely the concept of being prepared to be unprepared. You may never anticipate everything that may happen; the same as stated above by Wilhelmsen (2010) - it is necessary to be able to improvise when things, which are not anticipated, happens. Due to this, Pariès (2011) states that resilience implies that you have to have a combination of creativity, readiness, serendipity and anticipation. The same author also mentions other interesting issues; one is the fact that you have to train on unforeseen things, for example by training on generic team competencies rather than domain specific skills (which, to a great degree, contain pre-defined responses). The training may be what is necessary for personnel to be able to achieve the ability to improvise and to function well under stress, and in this manner become a more resilient employee during an emergency management situation.

6.3 Trust and resilience

Almost none of the informants showed trust towards the collaboration technology working as it is supposed to work. Many of the informants pointed out the low degree of reliability towards the mobile network as one of the main reasons to why they did not trust the technology. As one of the external 2nd line emergency management organizations said:

"*It does not seem like the mobile phone companies want to fulfil their promise around the up-time of the network*".

According to the theoretical foundation of Rempel et al. (1985) and Strand (2001) in chapter 2.3.2, the collaboration technology utilized today, such as telephone, e-mail, log systems, videoconferences, etc. do not present the user of the system with a great degree of predictability (i.e. the user may not see why the system behaves as it does in different situations). An explanation for this is that the systems are so complex that it requires specialist personnel to understand them, and in this manner the personnel are able to predict how the system may act. The dependability of the systems may be tested by exploring the system's boundaries and test how it will behave when presented with different kinds of challenges. Faith is another factor which is important in order to have trust towards a system. The factor of faith goes further than what you may prove by use of experience because the systems are so complex that one does not have the ability to unveil it and predict the entire behavioural pattern; one need to have faith in that the system handles what it should. From this theory, it is revealing that the informants in this study may feel a too high degree of dependability upon the system; they do not have any faith towards it since it breaks down regularly. Since this breakdown is not possible to predict, the informants would not have any trust towards the technology.

In work done by Zuboff (1988, in Strand, 2001), it was shown that in order for the personnel to be able to trust systems in an automated work environment, it is important that the employees have experience with the system. Further, it is also important that they have the opportunity to learn about the system

while working with it. This is something that can be directly used in emergency management, since it is often the case that during an emergency other systems are utilized than during normal operation. Due to the time pressure and other contributing stress factors (as mentioned by Chen et al. & Landrigan et al. (2010)), making mistakes, and thereby not taking the right decisions, is easy to do (cf. chapter 6.2). Because of this, it seems from the theory by Zuboff (1988, in Strand, 2001) that to be familiar with the equipment and the technology utilized during an emergency, it is crucial to be able to trust the technology. Another important factor which was stated by NOFO is the importance that the system is well-known for the user in such a way that the operator of the system may focus on the battle in the field and not "the battle" with the machine. In this case, a great degree of training with the system together with good and detailed feedback from the system would probably increase the user's knowledge according to present and former actions of the system, and might in this way also influence the future expectations (Rempel, et al., 1985). To hold on to this kind of knowledge would lead to a better understanding of what the system does and why, and further this may also enhance the operator's ability to predict the future actions of the system. With good feedback mechanisms and experienced personnel handling the technology, this will most likely enhance both the understanding and the familiarity of the system. This is important since familiarity is an important aspect to predictability. Dependability is also connected to predictability, and it is therefore possible to expect that feedback mechanisms give a better possibility to predict the system. Both dependability and predictability influences the third level of trust, namely faith (Strand, 2001). Many of the informants did not trust the technology and required a verification device / feedback device to be sure that the information got through. The human -machine interface is an important interface which may give different amounts of feedback. Milewsky and Lewis (1997) showed that interface design has a profound impact on operator trust. It is also important not to have a too detailed amount of feedback, as shown by Yeh & Wickens (2001), where displays with high degree of detail gave lower trust than displays with a lower degree of detail. This is an important factor to have in mind when constructing feedback mechanisms within emergency management, namely that you should receive the information you need either more or less. This implies that the systems which are in use during an emergency management handling process, to a great degree, have to be based on simple feedback mechanisms and configured with displays with not too much information. As Tveiten et al. (2010b) discovered as a point of improvement during their studies, logs with too much information and a little degree of sorting of information may lead to a slow detection of important information. This means that the interface between the human and the machine should be easy to handle and not possess too much information, in a way such that the personnel may create a trusting relationship towards these devices.

In Tveiten et al. (2010a), one of their findings were regarding the conservative attitude in which personnel within the field of emergency management have and that they did not want to change anything which worked. In this study, I would not say that it was the conservative attitude which struck me when interviewing the informants, rather it was the great degree of insecurity of the uptime of the network (as mentioned above), which seems to be the greatest issue regarding not using more of the new technological solutions which are available within the field of emergency management.

The use of IO concepts are viewed upon by the working force and their unions at the installations in the same manner as was mentioned by Zuboff (1988); the working force are afraid that the local knowledge, the feeling, and the competence are going to be lost and that there may be a high degree of new personnel onshore controlling the installations without ever actually being on an installation. As a result, it may lead to mistrust between the personnel onshore and offshore. This mistrust is felt by the offshore personnel as "not feeling safe" due to the lack of offshore experience of the personnel onshore (Grøtan & Albrechtsen, 2008). In this study it emerged that mistrust may also exist between the introduction of new technology and the personnel using the technology, due to the necessity to

learn new ways of working in order to use the new technology in the work-setting. Seen in an emergency management perspective, this could be some of the reasons why this line of the petroleum industry has not taken advantage of the possibilities shown with the use of IO. In an emergency setting, everything has to be familiar and known for the workers, which may be one of the explanations of why the use of IO concepts are not yet utilized here; the employees may not have enough faith to the use of new technology to be able to use it in these kinds of situations.

The informant from NOFO emphasized the different levels of trust which exists towards different organizations, e.g. the informant expects the following organizations to behave in a good manner: personnel within the JRCC; the Norwegian Coastal Administration; and the different NGOs. This kind of organizational based trust is also mentioned by Julsrud (2008). Further, this means that the informant has category-based trust (Kramer, 1999) towards these kinds of organizations. Having category-based trust indicates that the informant does not need to have personal knowledge towards the people who are to be trusted. It was also discovered a great deal of role-based trust (Kramer, 1999) within the organizations; the necessity of this kind of trust came clear when talking to NOFO. Performing a background-check of the personnel with whom you are working with is not always possible. Because of this, DSB, the Norwegian Coastal Administration, and NOFO now work together to create a system where certain requirements have to be fulfilled in order to hold a title. In this kind of trust, it is not as much the person in the role who the trust is based upon, but rather the system which is established around the role, which exists in order to make sure that the role occupant fulfils its role (Kramer, 1999). That is, one trusts the people and / or organizations that have made the certification system and not necessarily the person who is occupying the role.

The degree of swift trust which is defined in chapter 2.3.1.1 is not indicated to a great degree in the empirical data. Only the informants from one of the operator companies, one of the contractor companies, and the Norwegian Coastal Administration had this kind of trust against other actors. The rest of the informants focused on a greater degree of trust-building, and the need to actually know the person with whom you are cooperating with during an emergency. This corresponds with Boin's (2009) theory around the need for personal trust in order to have an efficient emergency response. The rest of the informants focused on the need for personal trust, this may be due that many of the people who are involved in such a situation knows each other in advance of the emergency. The reason for this is not easy to explain, but it may be that the different actors know each other from trainings and drills, and have already made their own understanding of the other people who are participating in an emergency. This is opposite to what Tveiten et al. (2010a) and Boin (2009) mentioned in their studies, where it is indicated that the personnel involved in an emergency situation do not know each other in advance. This may be the case to some degree, as mentioned above for one of the operator companies, one of the contractor companies, and the Norwegian Coastal Administration. One of the contractor companies that have personnel at the operator's installation offshore stated that:

"When an operator calls you to inform about an emergency, you trust that this person gives you the right information".

This person will then experience swift trust towards the operator. One of the operator companies simply trusts that the education and training that the person with a specific role has is adequate. The reason why the Norwegian Coastal Administration has swift trust towards the actors involved in an emergency is due to the fact that they want to give the other party the benefit of the doubt, before they decide in what manner to handle the actors in the future. Without swift trust, every action would be extremely time-consuming since you would have to double-check all information that you receive and send to be able to know if the correspondence is real. This seems to be a reasonable explanation towards their degree of swift trust against the other actors involved in an emergency. The contractors

wanted to be included in a greater degree in the planning and training phases of the operators' emergency management. This may enhance the resilience of emergency management, since the contractors may give the operator companies good contributions around indicators that the operator companies should respond to during the monitoring phase. The operators may have different views on the different factors which are present, and may, in this manner, make the emergency management organization more resilient, due that they may learn from each other's experience within emergency management.

6.4 Resilient emergency management

In this chapter the main empirical findings which emerged from this study will be discussed in light of resilience engineering. It is important to emphasize that the findings from the empirical qualitative data may not be generalizable for the whole industry. In chapter 3.5 a conceptual figure depicting the use of resilience engineering within emergency management was presented (Figure 4). The figure illustrates how the different abilities: monitor, respond, anticipate, and learn, all may be placed together in a cog wheel system in order to achieve a resilient system. In the following discussion the different empirical factors for a resilient emergency management system (as shown in Figure 10) will be discussed, and finally the conceptual model in Figure 4 will be compared with the empirical and theoretical findings in this study to see if there are any corresponding elements.

In order to construct a resilient system there are several basic qualities which must be in place (as shown in Figure 3), such as knowledge, competence, time, and resources. Together, with its different abilities, these basic qualities create a resilient system. In Figure 10 the most important findings from this study's empirical data are illustrated. These factors are looked upon as being essential towards the process of constructing a resilient emergency management, and they influence both the basic qualities and the abilities of a resilient emergency management system.

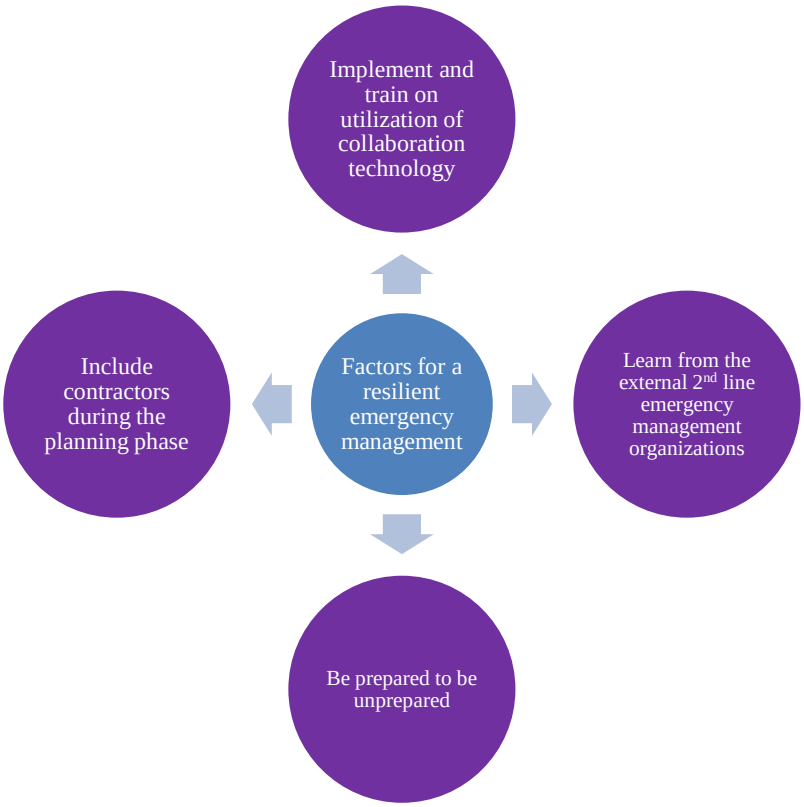

Figure 10: Most important factors for resilient emergency management identified in the empirical study.

In Figure 11, the concept of this resilient emergency management system is shown. It is indicated that the basic qualities are all a part of each of the four empirical factors (cf. Figure 10), i.e. all the basic qualities lies as the inner core for each of the four empirical factors in a resilient emergency management system. Further, all the empirical factors for a resilient emergency management system may influence each of the abilities for a resilient system. This also means that the basic qualities directly influence the abilities. In different words, this means that the basic qualities lies as an inner core in each of the empirical factors for a resilient emergency management, all the empirical factors influence all four abilities needed to have a resilient system, and as a result the emergency management system becomes more resilient.

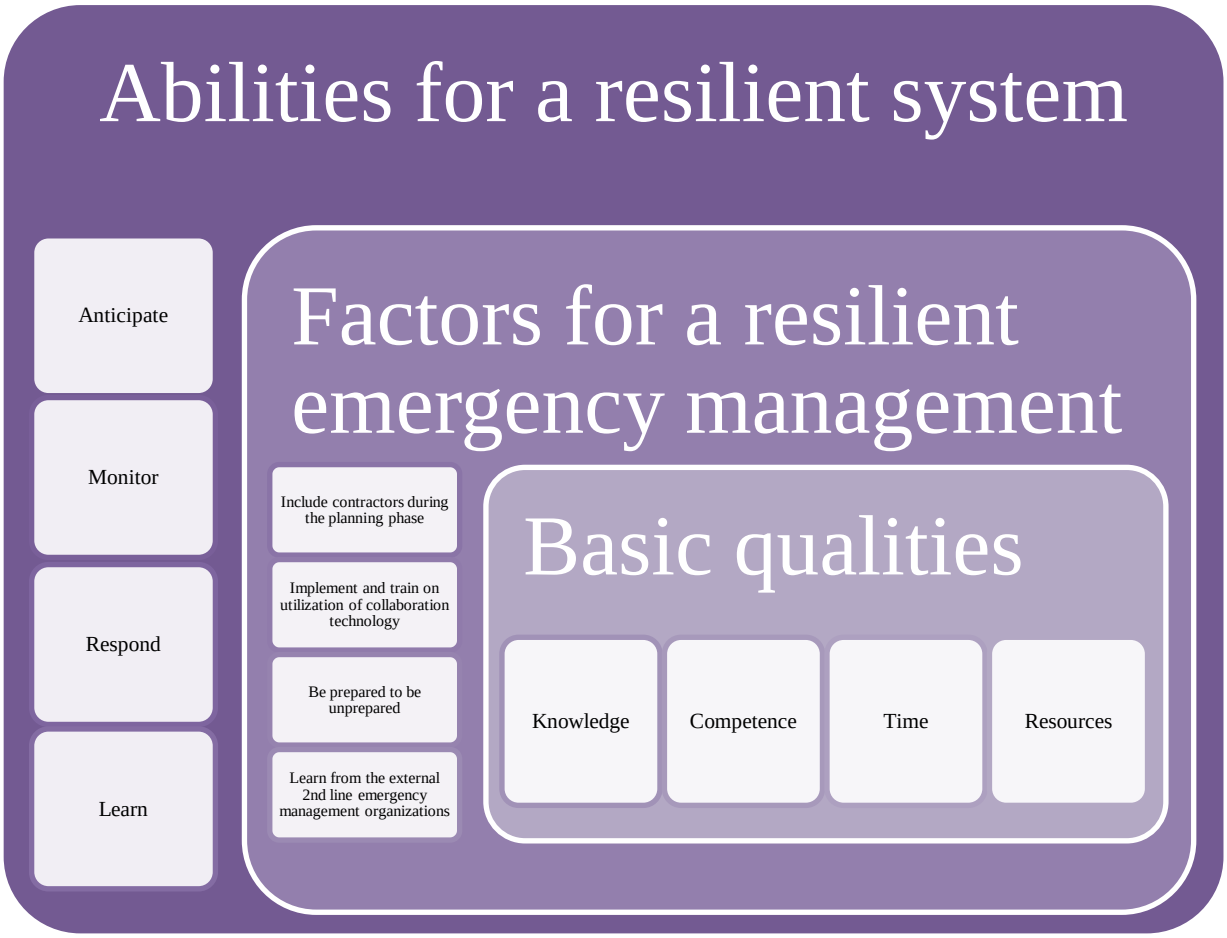

Figure 11: A conceptual model of a resilient emergency management system (all the boxes are mutually dependent).

In the following text, the discussion focuses on the necessity of the empirical factors and basic qualities in order to make a resilient emergency management.

To render possible a resilient emergency management it is, among other things, important to start implementing new forms of collaboration technology into the emergency management area. That is, in a way such that the technology which is utilized during daily operations also may be utilized during emergency situations. Further, it is important to emphasize a greater degree of training with these systems; to train on the systems may according to Zuboff (1988, in Strand, 2001) enhance the personnel's trust towards the system. In order to train on the system, you need all the basic qualities. For example, it is necessary to prioritize the time and resources to perform the training, i.e. that the

implementation of collaboration technology is taken seriously and given the required amount of time and resources in order to make it a part of each of the resilience engineering pillars. By training on use of the collaboration technology, the required competence and knowledge will most likely emerge, such that during an emergency the personnel knows how to use the technology and are able to handle the emergency in the most efficient way possible. By implementing and training on the use of collaboration technology the employees would most likely be able to anticipate to a greater degree how the technology will behave during an emergency, and also how to use real time data to anticipate what may happen. By implementing and training on the use of collaboration technology the employees will most likely have a greater possibility towards knowing which indicators to look for during an emergency, such that incidents may be stopped in the early warning phase. The ability to respond will most likely be increased, due to an enhanced degree of training on the use of collaboration technology the personnel will most likely know what to do, and thereby respond faster during an emergency. The learning pillar is prevalent within the implementation and training on utilization of collaboration technology, since learning is a desirable outcome of the training process. The capability to learn from both good and bad experiences during the training is a very important ability in order to make the system resilient (Hollnagel, 2011). During the trainings, it is also important to increase the focus on understanding each of the actors' roles during an emergency in order to avoid misunderstandings and confusions about responsibilities, tasks, and duties. Clearly defined roles and competencies are important in order to be certain that the person holding the title / role actually has the competence to do what the title / role states. This is emphasized in chapter 5.5, where it is mentioned that DSB, NOFO and the Norwegian Coastal Administration collaborates to construct a general education program within emergency management. Learning may not only come from exercises and drills, but may also originate from real incidents and the use of collaboration technology from both incidents happening within their own organization and in other organizations. An example was mentioned in chapter 5.4 regarding the person who started the log work in the wrong event, and as a result the work performed did not appear on the screen to the other personnel in the 2nd line emergency management centre. This is a problem that may easily be solved by implementing checklists or other verification mechanisms before the user starts to work on the log system.

The results in this study indicated that the external 2nd line emergency management use new forms of technology in a greater extent than the operators which are handling their own 2nd line emergency management. This is mainly because they have to use e.g. videoconferences and log systems in an extended degree in order to be in contact with the operator company. If the operator companies were able to learn from the external 2nd line emergency management organizations, it could increase their competence together with a general increase in the knowledge regarding the use of collaboration technology during emergency management. The external 2nd line emergency management organizations would be a great resource regarding the use of collaboration technology, since they have experience from this during their emergency management work.

Time is as always an important factor; if one lacks time for competence sharing between the external 2nd line emergency management and the operator companies handling their own emergency management, the competence sharing may not be fulfilling enough and the other basic qualities may suffer. However, when all the basic qualities are present the ability to learn from the external 2nd line emergency management organizations may also be present. When learning from other actors' emergency management, all the abilities needed in order to make a resilient system are also present (cf. Figure 11). Due to the knowledge transfer from the external 2nd line emergency management, anticipation will be present because the operator company may now, in a greater degree, know what to expect and therefore be more prepared for any potential "problems" with the utilization of the

collaboration technology. The operator company's ability to monitor will be enhanced, because their experience is transferred from the external 2nd line emergency management organizations. The transferral of experience results in the operator companies not having to find all the monitoring indicators on their own; the knowledge regarding early warning indicators will come from the external 2nd line emergency management organizations. Further, the response phase will also be influenced by learning from the external 2nd line emergency management organizations. By utilizing the resources the operator companies have in their external 2nd line emergency management, they may receive a lot of input with regard to how these companies handle the incidents which occurs. All in all, when the operator companies are learning from other actors' emergency management this is a mixture of the responding, anticipating, and monitoring abilities of the other actors. In this study, one of the external 2nd line emergency management organizations proposed that all the involved actors during an emergency may get access to the log system during the emergency handling (cf. chapter 5.4). Each of the actors' access to the log had to be predefined in a way such that they only got the information that they needed and were not able to access sensitive information. Access to a joint log system is something which also the operator companies handling their own emergency management organizations may think of as having potential. On the other hand, PSA do not see this being a good concept towards their need for information during emergencies. PSA want to be able to ask "follow-up" questions when they receive information regarding the operators' action plans according how to handle an emergency. Still, it may be possible to transmit "double information" to authorities such as PSA; giving them information both over telephone and by the log. This would give a degree of redundancy within securing the information sharing; securing that the information is transferred to the right people at the right time. In chapter 5.6, a suggestion was given by one of the external 2nd line emergency management organizations, namely to divide the status board into two pieces; one half showing the status while the other half showing which kind of measures that are planned to be implemented next. A log system that allows the different external actors to see this status board would render possible to get real-time updates about the situation. The actors may also efficiently submit other recommendations on how to prevent the emergency from escalating. Still, it is important to emphasize that it is the operator who has the legal responsibility for the emergency management handling; the log system should not be a device for the operator company to deprive its responsibilities.

The concept of being prepared to be unprepared (Pariès, 2011), is important within emergency management. The concept is a central part of the resilience engineering theory and will therefore be an important part to include in this discussion. The "Clint Eastwood method" justifies thinking in a resilient manner during emergencies; therefore there are indirect empirical data which shows that Pariès (2011) theory is carried out in praxis (cf. chapter 6.2). The accidents which happen are seldom only consisting of one DSHA, often there may be several different DSHAs mixed together during an emergency, and in such situations there are no easy solutions for solving the problem. One may have to mix different responding phases in order to achieve a suitable one, and further be able to improvise in order to achieve the best solution of the emergency.

To be prepared to be unprepared it is necessary to have the right resources available, e.g. having access to different personnel with a great degree of experience and knowledge. When an emergency happens (or during trainings) there must be enough resources with the right knowledge to be able to handle the emergency even if it is a complex matter. Further, the competence of the personnel and their knowledge about the field is important, such that the abilities of the resilient system may be fulfilled. As mentioned earlier, time is always important; with lack of time it may not be possible to gather the resources, competence, and knowledge necessary to be prepared to be unprepared. Being

prepared to be unprepared does not mean that it is possible to anticipate everything that may happen; as mentioned above an emergency may be a complex connection of many different DSHAs, in a way such that there may not be a single method of operation which is the right one. This is why it is necessary to have the possibility and capability to improvise in the responding phase of the situation. As stated by Mendonca et al. (2007), it is necessary to improvise in order to have a successful response during an emergency. This because an emergency will often require the staff to think in ways that differ from the original plan and in order to respond adequately, the staff may take on widen or totally new roles, adapt existing technology to unforeseen requirements, and develop new organizational structures. As stated by Pariès (2011), resilience implies that you have a combination of creativity, readiness, serendipity, and anticipation (here creativity will mean the same as improvisation). This means that, in the responding phase, it is important to be able to implement a great degree of improvisation since one cannot anticipate all incidents.

Training on being prepared to be unprepared also enhances the monitoring part of the emergency management system, since training will most likely enhance the ability to know what indicators you have to look for during the monitoring phase. The ability to learn is also present in the whole process; the concept of being prepared to be unprepared bases itself on a continuous learning process in order to be able to be prepared and not panic when an unforeseen thing happens.

The inclusion of different contractors during the planning phase will most likely improve the emergency management both at the contractor and the operator. This is only valid if the contractors are included in a good manner. Including contractors during the emergency management planning phase may function as a resource and contribute with valuable information regarding, for example, flaws and possibilities within today's emergency management, and also in which ways they want to work to make the emergency management even better. One of the contractor companies mentioned that they want to be more involved in the operator's planning. Both contractor companies want to increase the collaboration between the operator and the contractor with regard to how the emergency management should work in praxis. They see possibilities for using a collaboration system which may render this possible. The information lines have to be constructed before an emergency happens in order to be sure that the emergency management will be done in a resilient way. The contractors may for example construct connections to a log system, this to be continually updated about the situation and about which kind of information they may give their own workers' next of kin (as was mentioned as a focus point by one of the contractor companies in chapter 5.4). It is important that the operator prioritize time to listen and learn from the contractors' experiences and knowledge, and further use this knowledge by implementing it into the emergency management. The inclusion of the contractors may influence the anticipation phase of emergency management. This is because the contractors may have important knowledge and experience regarding risk factors which are important to follow up on during emergencies, and may assist in being prepared towards knowing what to expect. The monitoring phase is connected with the anticipation phase, since the contractor may have knowledge about which factors one should be aware of, and by utilizing this information new indicators which are important to look for before and during emergencies may be discovered. The response phase may also be improved since the contractors may contribute with a different approach and knowledge of how to respond in an emergency setting. The contractor companies may contribute to the operator company about how to solve the problem, and, due to this, give the contractor company a more efficient responding phase. The learning phase permeates the concept of including contractors during the planning phase; this is due to the great degree of competence, resources, and knowledge that may come from the contractors when cooperating with them.

6.5 Putting the resilience pieces together

In chapter 6.4 it is clear that the conceptual figure mentioned in chapter 3.5 corresponds with the factors in Figure 10 by making the emergency management system more resilient. Further, the different empirical factors were discussed together with Hollnagel & Woods' (2006) different basic qualities and abilities (as shown in Figure 3). Figure 12 depicts the findings in this study which influences the possibility towards making a resilient emergency management system; this includes both theoretical and empirical findings. Most of the findings also influence each other (at some level) in their way towards creating a resilient emergency management system. The red boxes show the needed abilities, the blue boxes the needed qualities, and the green boxes the empirical factors found within this study in order to enhance the resilience in emergency management. By implementing the basic qualities, abilities, and empirical factors into the emergency management it is likely that the emergency management organization will become more resilient. In the next chapter, recommendations will be given with regard to how to make the emergency management more resilient; the recommendations build upon the empirical findings of this study (the green boxes).

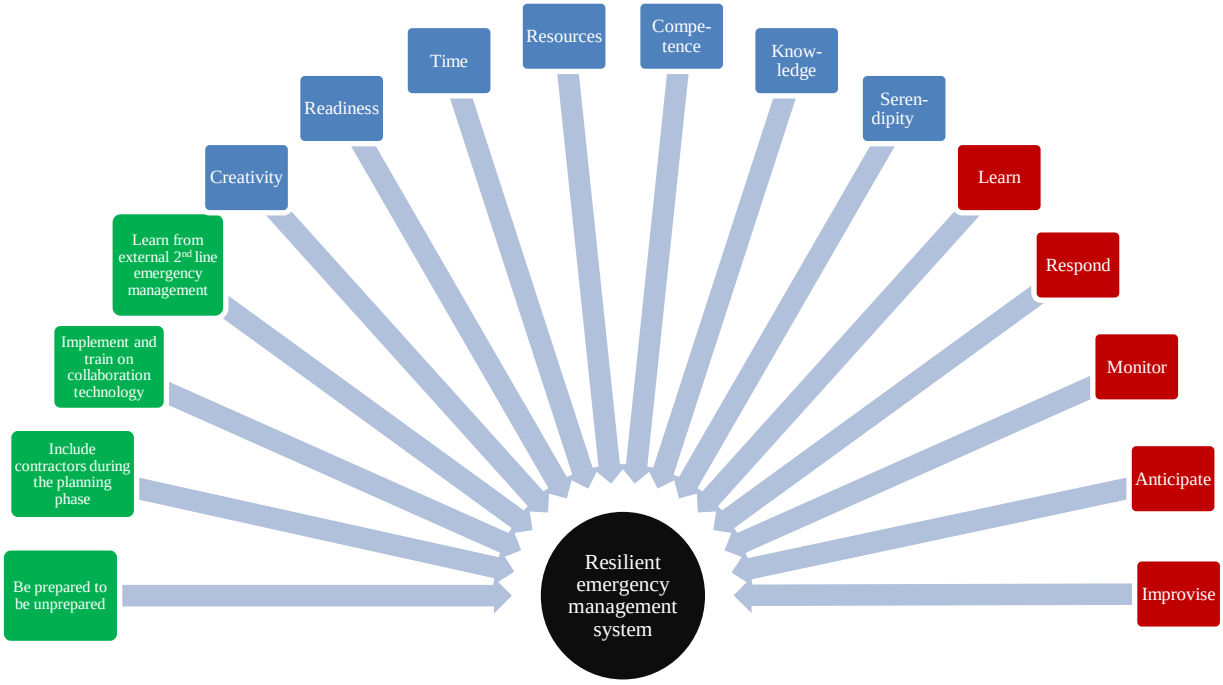

Figure 12: Basic qualities (in blue), abilities (in red), and factors identified in the empirical study (in green) for a resilient emergency management system (the factors are mutually dependent).

6.6 Recommendations

The main part of the recommendations made from the results and discussion of this study are shown in Figure 10. As discussed in chapter 6.4, these are all different empirical factors which could be implemented into the emergency management organizations to make it more resilient. It is important to emphasize that these are made from qualitative empirical data, and may not be generalizable for the whole industry. Below, the factors will be discussed further.

- *Implement and train on collaboration technology, and include contractors during the planning phase*

In order to increase the degree of trust between the different actors involved in the emergency management, it is necessary to train more together with the contractors and also to include the contractors and other external actors within the planning phase of the emergency management. As indicated by Boin (2009), the development of swift trust is not enough to attain an effective response in an emergency, and, due to this, the trust have to be built before the emergency happens. In order to increase the degree of trust towards the technology, it is necessary to start using new technology in emergency management; gaining experience with the different technologies and knowledge of their strengths and weaknesses. As mentioned by Zuboff (1988, in Strand, 2001), it is important that the personnel have experience with the system in order to trust systems in an automated work environment. Further, it is also important to define what kind of technology which is required within the specific organizations, and not to select a particular technology only because a competitor uses it. Still, as mentioned above, the devices each organization utilizes should be built on the same platform, such that they may be compatible with each other. To increase the information-sharing between the operator and the external actors involved during an emergency, one may grant access to a continually updated log system; with interfaces especially designed towards each of the actors such that they may receive the information they need, when they need it. However, with an increased use of web-based collaboration technologies, one must develop suitable methods for information security. These methods should provide certainty that e.g. only the people who should receive the information, have received it and actually acknowledged it. To implement this kind of technology would also need a great degree of training with all actors involved during an emergency, such that the collaboration technology becomes a tool to help solve the problem and not a problem in itself which has to be solved (especially since there is no time to start learning how to use a system during an emergency).

- *Be prepared to be unprepared*
  Flexibility is a key factor around the concept of being prepared to be unprepared. This flexibility may be acquired by performing more general training sessions of emergency management, which may teach the participants to handle things in general and not only how to handle a specific DSHA. This is mentioned by Pairès (2011) (cf. chapter 6.4) as a way to implement a greater degree of resilience into the organization. By introducing more general trainings, one will enhance the knowledge of which kind of indicators that you have to look out for during the monitoring phase. Anticipation is also important due to the fact that an emergency may change its shape during an event; spanning from an action plan which follows the specific guidelines of the given emergency (DSHA), to an emergency consisting of several DSHAs. Therefore, an improvisatory line of action has to be implemented. Further, all actors within the petroleum industry should build their technology on the same platform; having compatible information systems is a key element in fast and reliable exchange of information during an emergency. All in all, flexibility is a key factor of being prepared to be unprepared.

- *Learn from external 2nd line emergency management organizations*
  To learn from the external 2nd line emergency management organizations about their use of collaboration technology during an emergency is a possible gateway for transfer of experience. The large operator companies that handle their 2nd line emergency management on their own should look at the organizations which offer these kind of services to the small operator companies, and further investigate in what ways they use collaboration technology in emergency management. By learning from the external 2nd line emergency management

organizations, all the pillars within resilience engineering may be influenced (cf. chapter 6.4); as a result, it may make the emergency management more resilient.

The final recommendation concerns broadening the scope of the term "emergency preparedness"; according to Ptil (2008), "notification" is one of the phases of emergency preparedness. However, this phase is often handled by the personnel who handle the normal operation; they should also have a greater focus towards avoiding emergencies and be more critical when elements that may result in an incident are discovered. An increased focus towards worst-case thinking should be present, a focus which the emergency management personnel are good at. Implementation of a more proactive mindset in the normal operation may contribute towards avoiding emergencies to happen at all; IO concepts may be an enabler for a proactive mindset among the personnel handling the daily operation. Monitoring render it possible for different onshore experts to notice the early warnings regarding deviations and to further implement measures before the deviation develops into an accident.

7 Conclusion

In this study, the themes of emergency management, collaboration technology, trust, and resilience engineering have been explored. Further, the results from the interviews have been analyzed in the light of the theory and previous research (which was presented in chapter 2 and 3) in order to answer the research questions. In the following text an answer to each of the research questions are elaborated.

7.1 The actor map

The actor map in an emergency management handling situation has not been altered in a great degree after the introduction of IO technology. This may be because the communication channels utilized between the external actors are mainly still telephone and e-mail. However, within each organization there is a greater use of other communication forms such as a log system, e-mail, videoconferences, etc. According to the empirical data, the only noticeable changes which have evolved within the emergency management area are the implementation of the organizations which offers to handle the 2nd line emergency management at the operator companies together with an increased activity from small scale operator companies on the Norwegian continental shelf. As shown in Figure 5, the actor map has very complex connections. Due to this, there may be some actors which are forgotten (or which "feels forgotten") during an emergency since they may feel that they do not receive situational updates often enough. A good emergency management log system for all the involved actors would possibly decrease the issue of not being able to transmit the right information to the right people at the right time.

7.2 Trust

According to Rempel et al. (1985) and Strand (2001), the informants' low degree of trust towards the technology may be the result of low or non existing predictability, dependability, and faith. Different kind of roles leads to different kind of trust, e.g. NOFO has category-based trust against actors as JRCC, the Norwegian Coastal Administration, and the NGOs because they are regarded as professional organizations. Trust issues influence the collaboration between the different actors to a great degree; this study indicates that the trust which exists between the different actors are mostly based on personal knowledge and trust towards the other person – only three of the informants mentions swift trust as a basis for their collaboration during emergency handling. This indicates that to build a relationship based on trust with the other actors; the actors have to know each other in advance. This is also in accordance with the findings by Boin (2009), where it is indicated that swift trust is not enough to attain an effective response during emergencies. Further, there is a low degree of trust towards the utilization of new technology in an emergency setting; network coverage and the possibility for down-time are considered as inadequate. The actors mention trainings and drills as the best way of creating trust between the different actors during an emergency setting. During these exercises it would be necessary to implement IO concepts, such that the actors could analyze how this technology would function during an emergency situation. In such a way, they are prepared and know how to use the technology when a real emergency emerges, and further also generate trust towards the technology which is utilized during these training sessions. In the longer term, this may lead to a decreased degree of telephone use compared to today's use of this communication device.

7.3 Possibilities by use of collaboration technology

Overall, the external 2nd line emergency management organizations utilize more collaboration technology during an emergency than the other actors, mostly to be able to communicate with the operator company. The operator companies which handle their own 2nd line emergency management

could learn from how the external 2nd line emergency management organizations handle their emergency management. Further, the communication between actors involved in an emergency could be much more efficient by utilizing the technology available in a higher degree, e.g. by creating a log system which shares the information regarding the emergency with the actors involved. Implementation of a shared log system may update the different actors about the situation more efficiently, which may lead to a more efficient handling of the emergency in itself. This may also render possible that all actors involved in the emergency have the same situational picture over the emergency, and in this way implement a proactive mindset regarding further handling of the emergency. By building the different actors information systems on the same platform, compatibility issues may be avoided such that all effort is put towards solving the emergency.

7.4 Resilient emergency management

Resilience engineering may be a proactive contribution within today's emergency management, and increase the focus on stopping the emergency in an early phase (early warning phase). The most important factors which were indicated in this study in order to gain resilient emergency management are to:

- Be prepared to be unprepared
- Include contractors during the planning phase
- Implement and train on collaboration technology
- Learn from the external 2nd line emergency management organizations

In the text below each of the bullet points will be elaborated.

Be prepared to be unprepared

Since it is not possible to be prepared for every possible case, you have to be prepared to be unprepared in the emergency management responding phase. Here it is important to have all the other resilience engineering phases intact and to use IO concepts in a best possible manner in order to both prevent incidents from developing into accidents and even prevent early warnings from developing into incidents; where the latter could be resolved by having good monitoring indicators that capture and reveal these early warnings. Even though many of the informants looked upon emergency management as a reactive discipline which happens after an accident has happened, it may be necessary to widen the scope of emergency management. That is, including the early warning phase within the definition; something which requires a heightened focus on early warnings and in this way avoiding that incidents evolve into major accidents.

Include contractors during the planning phase

Including contractors during the planning phase of the emergency management would most likely improve the resilience of the emergency management both at the contractor and at the operator. The contractors may function as a supplier of competence and knowledge to the operator company; that is, information regarding troubles and opportunities within today's emergency management. Further, it would also give the contractor a better understanding of how the operator's emergency management system is constructed, and how the contractors fit best within this construction.

Implement and train on collaboration technology

The implementation of and training with collaboration technology would most likely make it possible for the different actors to see the potential in which the technology brings towards sharing of

information (e.g. a log system). It would also render possible for an increased efficiency of finding a suitable solution, since more of the actors possess the same picture over the situation (cf. chapter 7.3). Further, the employees may be more aware of which indicators to look for during emergencies, and may, due to this, prevent emergencies by implementing measures in the early warning phase of an emergency.

Learn from the external 2nd line emergency management organizations

An important factor for the operator companies which handles their own 2nd line emergency management is to analyze and learn from how the external 2nd line emergency management organizations handle their emergency management, which technology they use, and how they organize the different actors during an emergency. Learning from the external 2nd line emergency management organizations may render it possible for the operator companies which handles their own 2nd line emergency management to be more prepared (and more proactive) towards any potential problems that may emerge by the use of collaboration technology within emergency management.

There are many factors that may influence the degree of resilience for the emergency management organization. The empirical factors mentioned above are some of them, the other factors (basic qualities and abilities) are: creativity; readiness; time; resources; competence; serendipity; knowledge; improvisation; anticipation; learning; responding; monitoring. By implementing these factors in a suitable manner, the degree of resilience would most likely increase within the field of emergency management.

7.5 Recommendations

Below, the recommendations which emerged from this study to make an emergency management system more resilient are summarized.

1) *Be prepared to be unprepared*
   Flexibility is a key factor around the concept of being prepared to be unprepared. Making the training sessions more general (Pairès, 2011), may work as a device towards implementing a greater degree of resilience into the organization. More general trainings would most likely enhance the possibility to know which kind of indicators one should look out for during the monitoring phase. Also, it is important to anticipate that things may not play out exactly as planned. Even if you start out with a situation which is only comprised of one DSHA, the situation may escalate and become more complex in the course of events. This may in return require a greater degree of improvisation and flexibility in handling of the emergency, than in the start phase of the emergency.

2) *Implement and train on collaboration technology, and include contractors during the planning phase*
   By including the contractors in a well-functioning manner during the planning phase may lead to a great degree of trust between the operator and the contractors involved in an emergency. If the contractor and the operator were executing more exercises together, it may increase the degree of trust between these actors since swift trust is not enough to be able to attain an effective response during an emergency (Boin, 2009). In order to increase the degree of trust towards the technology, it is necessary to start using new technology in emergency management and to gain experience regarding the different technologies' strengths and weaknesses. According to Zuboff (1988, in Strand, 2001), it is important that the personnel have experience with the system in order to trust systems in an automated work environment;

the actors should implement and train on the technology which shall be used during emergencies in trainings and exercises. Further, the different devices utilized by the different actors involved in an emergency, should be built on the same platform such that they may be compatible with each other. Lastly, the implementation of a continually updated log system, which gives all the actors involved in an emergency access to updated information, may increase the efficiency of information sharing and further a more efficient problem solving.

3) *Learn from external 2nd line emergency management organizations*
   The external 2nd line emergency management organizations utilize a great deal of collaboration technology during their emergency management. To witness how the external 2nd line emergency management organizations utilize this kind of technology, could be very helpful to the operator companies which handles their own emergency management such that they could see what possibilities exists within the technology. Learning from the external 2nd line emergency management organizations may make the emergency management at the operator companies which handles their own emergency management more resilient, since all the resilience pillars may be influenced by such a learning process.

Lastly, it is important to contemplate widening the term "emergency preparedness" to also include the "notification" phase. This could render it possible to implement measures when "early warnings" or incidents happens, and further avoid that they develop into accidents.

8 Further work

Since some of the actors did not reply on interview invitations, no interviews were carried out with contractor companies that perform drilling services for the operator companies. These interviews would give a greater degree of knowledge according to how the information sharing is handled between the operator and the contractor. This study shows that it is necessary with a greater degree of information sharing between the operator and the contractor before and during an emergency, in order to prepare oneself on how to handle such an emergency in collaboration with each other. It would also be interesting to closely study an operator company and see how the different actors within the company handles the emergency situation, e.g. how the information flow between the 1st, the 2nd and the 3rd line emergency management flows, and further analyze how the information flow is between e.g. the 1st and the 2nd line emergency management and the internal support groups. This should be analyzed for both operator companies which handles their own 2nd line emergency management, and also with operator companies which outsources this function. In this way, it would be possible to analyze the pros and cons within both ways of handling the 2nd line emergency management, and evaluate which one that functions best or if they both are equally good. Lastly, it would also be interesting to study more thoroughly the internal support groups' roles during emergencies.

References

Adams, B.D., Waldherr, S., Sartori, J. & Thomson, M. 2007. *Swift Trust in Distributed Ad Hoc Teams.* Humansystems Incorporated, Defence Research and Development Canada Toronto.

Aktivitetsforskriften § 79. 2011. FOR-2010-04-29-613. [Internet]. Available at: http://www.lovdata.no/cgi-wift/wiftldles?doc=/app/gratis/www/docroot/for/sf/ad/ad-20100429-0613.html&emne=aktivitetsforskrift*& [Accessed: 05 04 2011].

Albrechtsen, E. 2010. *Forelesningsfoiler: sikkerhet, teknologi og organisasjon. Del 2.* 2010. NTNU. Trondheim.

Albrechtsen, E., Wærø, I., Tveiten, C. K. & Wahl, A. M. 2009. *Referat fra workshop om IO og beredskap, 27 oktober 2009.* s.l. : SINTEF, 2009. 504143 IOSafe. Trondheim

Altschuller, S. & Benbunan, R. F. 2008. Potential Antecedents to Trust in Ad Hoc Emergency Response Virtual Teams. *Proceedings of the 5th international ISCRAM Conference- Washington DC,* USA, May 2008.

Boin, A. 2009. *The New World of Crisis and Crisis Management: Implications for Policymaking and Research*. Rewiew of policy Research, 26(4). pp. 367-377.

Bradner, E. & Mark, G. 2002. Why Distance Matters: Effects on Cooperation, Persuasion and Deception. *Proceedings of the 2002 ACM conference on computer supported cooperative work.* New York. USA.

Bryman, Alan. 2008. *Social Research Methods.* New York : Oxford university press, 2008. ISBN 978-0-19-920295-9.

Büscher, M., Kristensen, M. & Mogensen, P. H. 2008. When and how (not) to trust IT? Supporting virtual emergency teamwork. *Proceedings of the 5th international ISCRAM Conference- Washington DC, USA, May 2008.*

Chen, R., Sharman, R., Cook-Cottone, C., Rao, R. H. & Upadhyaya, S. J. 2010. Examination of emergency response from knowledge and psychology perspectives. *Proceedings of the 7th international ISCRAM Conference-Seattle, USA, May 2010.* This paper represents work in progress.

Dawes, R. M. 1994. *House of cards: Psychology and psychotherapy built on myth*. New York: Free Press. [Internett]. Available at: http://www.google.com/books?hl=no&lr=&id=J6iq_khf5HkC&oi=fnd&pg=PR7&dq=House+of+cards:+Psychology+and+psychotherapy+built+on+myth&ots=1anY7K3NF5&sig=fh8cLr9hvicm7cDIu3g97oGaRk4#v=onepage&q&f=false [Accessed: 18 01 2011].

Forurensningsloven § 46. 2009. LOV-1981-03-13-6. [Internet]. Available at: http://www.lovdata.no/all/hl-19810313-006.html [Accessed: 05 04 2011].

Foulquier, T. & Caron, C. 2010. Towards a formalization of interorganizatioal trust networks for crisis management. *Proceedings ot the 7th International ISCRAM Cinference- Seattle, USA, May 2010.*

Grøtan, T.O. & Albrechtsen, E. 2008. *Risikokartlegging og analyse av integrerte operasjoner (IO) med fokus på å synliggjøre kritiske MTO aspekter.* SINTEF, 2008. SINTEF A7085. Trondheim.

Haddow, G. D. & Bullock, J.A. 2003. *Introduction to emergency management*. Amsterdam. Butterworth-Heinemann.

Handy, C. 1995. *Trust and the virtual organisation.* Harvard Busiess Review, 73(3). pp. 40-50.

Hollnagel, E. 2011. To Learn or Not to Learn, that is the Question. In Hollnagel, E., Pariès, J., Woods, D. & Wreathall, J. (eds.). *Resilience Engineering in Practice. A Guidebook.*England. Ashgate Publishing Limited.

Hollnagel, E., Pariès, J., Woods, D. & Wreathall, J. (eds.). 2011. *Resilience Engineering in Practice. A Guidebook.*England. Ashgate Publishing Limited.

Hollnagel, E. 2010. *Resilience Engineering. Why, What and How*. Lecturefoil TIØ4200. Safety management HSE Masterstudy at IØT, 2010.

Nemeth, C.P., Hollnagel, E. & Dekker, S. (eds.). 2009. *Resilience Engineering Perspectives, Volume 2. Preparation and Restoration.* Surrey. England. Ashgate Publishing Limited.

Hollnagel, E., Nemeth, C. P. & Dekker, S. (eds.). 2008. *Resilience Engineering Perspectives, Volume 1. Remaining Sensitive to the possibility of Failure.* Hampshire. England. Ashgate Publishing Limited.

Hollnagel, E., Woods, D. D. & Leveson, N. (eds.). 2006. *Resilience Engineering. Concepts and Precepts.* Hampshire. England. Ashgate Publishing Limited.

Hollnagel, E. & Woods, D. D. 2006. Resilience Engineering. In Hovden, J. (2010). *TIØ 4200. Sikkerhetsledelse kompendium. HMS masterstudiet ved IØT. Trondheim: Institutt for industriell økonomi og teknologiledelse,* NTNU.Trondheim. Norway.

HRS. 2003. *Redningstjenesten. Hovedredningssentralene* [Internet]. Available at: http://www.hovedredningssentralen.no/ [Accessed 08 03 2011].

Landrigan, L. C., Milewski, A. & Baker, J. 2010. Determining cerdible sources during an emergency situation*: Proceedings ot the 7th International ISCRAM Cinference- Seattle, USA, May 2010.*This paper represents work in progress.

Johnsen, S. O. & Lundteigen, M. A. 2008. Sikrere fjerndrift med CRIOP. In Ranveig Kviseth Tinmannsvik (ed.). *Robust arbeidspraksis - Hvorfor skjer det ikke flere ulykker på sokkelen?* Trondheim : Tapir Akademisk forlag, 2008. pp. 57-73.

Julsrud, T. E. 2008. *Trust across Distance. A network approach to the development, distribution and maintenance of trust in distributed work groups.* Doctoral thesis for the degree of Philosophiae Doctor. Norwegian University of Science and Technology
Faculty of Social Sciences and Technology Management. Department of Sociology and Political Science. Trondheim.

Kasper-Fuehrer, E.C. & Ashkanasy, N. M. 2001. Communicating trustworthiness and building trust in interorganizational virtual organizations. *Journal of Management* 27. pp.235-254.

Kramer, R. 1999. Trust and distrust in organizations: Emerging perspectives, enduring questions. *Annual review of psychology,* 50. pp. 569-598.

Kvale, S. 1996. *Interviews. An introduction to qualitative research interviewing*. USA: Sage publications, Inc.

Kystverket. 2011. Kystverket. *Om Kystverket*. [Internet]. Available at: http://www.kystverket.no/?aid=9030586 [Accessed: 08 03 2011].

Maass, S. 1983. Why systems transparency? In Green, R.G., Payne, S.S. & Van der Veer, G.C. (eds.). *The Psychology of Computer Use*. Academic Press.

Manoj, B.S. & Baker, A. H. 2007. Communication challenges in emergency responce. *Communications of the ACM.* 2007, Vol. 50, 3.

Mayer, R., Davis, J. & Schoorman, F. 1995. An integrative model of organizational trust. *The Academy of Management Review,* 20(3). pp. 709-734.

Mendonca, D., Jefferson, T. & Harrald, J. 2007. Collaborative adhocracies and mix and match technologies in emergency management. Usinge the emergent interoperability approach to address unanticipated contingencies during emergency response. *Communications of the ACM.* 2007, Vol. 50, No.3.

Meyerson, D., Weick, K. E. & Kramer, R. M. 1996. Swift trust and temporary groups. In R. M. Kramer & T. R.Tyler (Eds.). *Trust in organizations.* London: Sage Publications

Milewsky, A. E. & Lewis, S. H. 1997. *Delegating to software agents*. [Internett]. Available at: http://heb.freeshell.org/ie662/Milewski_Agents.pdf [Accessed: 25 01 2011.]

Moray, N. & Iganaki, T. 1999. Laboratory studies between humans and machines in automated systems. *Transactions of the Institute of Measurement and Control*. 21:203.

Mostue, B. A. & Albrechtsen, E. 2010. Characteristics of decision-making processes within integrated operations, and implications on risk management. In Albrechtsen, E. et al. (eds.) *Essays on socio-technical vulnerabilities and strategies of control in integrated operations*. Sintef artikkel nr A14732. 2010, pp. 44-49.

NOFO. 2011. Norsk oljevernforening for operatørselskap. Om NOFO. Vår virksomhet [Internet]. Available at: http://www.nofo.no/modules/module_123/proxy.asp?D=2&C=165&I=3 [Accessed: 04 04 2011].

NTS. 2001. *Norsok standard Z-013. Risk and emergency preparedness analysis.* Norsk standard, 2001.

OLF. 2005. Oljeindustriens landsforening. *Integrated Work Processes: Future work processes on the Norwegian continental shelf.* [Internet]. Available at: http://www.olf.no/getfile.php/zKonvertert/www.olf.no/Rapporter/Dokumenter/051101%20Integrerte%20arbeidsprosesser,%20rapport.pdf, 2005. [Accessed 29-09-2010]

Olson, G. M., & Olson, J. S. 2000. Distance Matters. *Human-Computer Interaction*, 2000, 15. pp.139-178. Lawrence Erlbaum Associates, Inc.

Pariès, J. 2011. Resilience and the Ability to respond. In Hollnagel, E., Pariès, J., Woods, D. & Wreathall, J. (eds.). *Resilience Engineering in Practice. A Guidebook*.England. Ashgate Publishing Limited.

Perrow, Charles. 1984. Normal accidents.In Hovden, J. (2010) *TIØ 4200 Kompendium Sikkerhetsledelse, HMS masterstudiet ved IØT.*

Petroleumsloven § 9-2. 1996. LOV-1996-11-29-72. [Internett]. Available at: http://www.lovdata.no/all/tl-19961129-072-009.html. [Accessed: 19 08 2010].

Ptil. 2011. Petroleumstilsynet. *Om oss.* [Internet]. Available at: http://www.ptil.no/ [Accessed: 04 04 2011].

Ptil. 2010. Petroleumstilsynet. *Operatørens ansvar for beredskap*. [Internet]. Available at: http://www.ptil.no/beredskap/operatoerens-ansvar-for-beredskap-article6860-18.html [Accessed 05 04 2011].

Ptil. 2009. *Risikonivå i petroleumsvirksomheten, Hovedrapport Utviklingstrekk 2009, norsk sokkel.* Petroleumstilsynet, 2009.

Ptil. 2008. Petroleumstilsynet. *Om beredskap.* [Internet]. Available at: http://www.ptil.no/beredskap/om-beredskap-article3752-18.html. [Accessed: 18 08 2010].

Rammeforskriften § 21. 2010. FOR-2010-02-12-158. [Internet]. Available at: http://www.lovdata.no/cgi-wift/wiftldles?doc=/app/gratis/www/docroot/for/sf/ad/ad-20100212-0158.html&emne=rammeforskrift*& [Accessed 07 04 2011].

Rempel, J., Holmes, J. & Zanna, M. 1985. Trust in close relationships. *Journal of personality & Social Psychology*, 49(1).pp. 95-112.

Ringdal, K. 2001. *Enhet og mangfold - Samfunnsvitenskapelig forskning og kvantitativ metode.* Bergen : s.n., 2001. ISBN 82-7674-569-5.

Ringstad, A. J. & Andersen, K. 2007. Integrated operations and the need for a balanced development of people, technology and organisation. *Paper presented at the International Petroleum Technology Conference held in Dubai, U.A.E, 4-6 decemer 2007*.IPTC 1168, 2007.

Ringstad, A. J. & Andersen, K. 2006. Integrated operation and HSE- major issues and strategies.*Paper presented at the SPE International Conference on Health, Safety, and Environment in Oil and Gas Exploration and Production held in Abu Dhabi,U.A.E. 2-4 april 2006.* s.l. : SPE 98530, 2006.

Rosness, R., Forseth, U. & Wærø, I. 2010. *Rammebetingelsers betydning for HMS-arbeid.* SINTEF 2010. SINTEF rapport A16296. Trondheim

Schiefloe, P. M., Vikland, K., Ytredal, E. B., Torsteinsbø, A., Moldskred, I., Heggen, S., Sleire, D. H., Førsund, S. A. & Syversen, J. E. 2005. *Årsaksanalyse etter Snorre A hendelsen 28.11.2004.* Stavanger : Statoil ASA.

Sheridan, T. B. 1992. *Telerobotics, Automation and Human Supervisory Control*. Massachusetts. USA.The MIT Press.

Skjerve, A. B., Albrechtsen, E. & Tveiten, C. K. 2008. *Defined Situations of Hazard and Accident related to Integrated Operations on the Norwegian Continental Shelf.* NTNU/SINTEF/IFE, 2008. SINTEF A9123. Trondheim.

Statoil. 2008. Statoil. *Facts: Integrated operations*. [Internett]. Available at: http://www.statoil.com/en/NewsAndMedia/Multimedia/features/Pages/FactsAboutIO.aspx. [Accessed: 23 08 2010].

Strand, S. 2001. *Trust and Automation: The Influence of Automation Malfunctions and System Feedback on Operator Trust.* Thesis in Psychology (SVPSY 390). NTNU.

Styringsforskriften § 29. 2011. FOR-2010-04-29-611. [Internet]. Available at: http://www.lovdata.no/cgi-wift/wiftldles?doc=/app/gratis/www/docroot/for/sf/ad/ad-20100429-0611.html&emne=styringsforskrift*& [Accessed: 05 04 2011].

Sydow, J. 2006. How can Systems trust systems? A structurational perspective on trust building in inter-organizational relationships. In Bachmann, R. & Zaheer, A (eds.). *Handbook of trust research.* Cheltenham, UK. Edward Elgar.

Thagaard, T. 2003. *Systematikk og innlevelse. En innføring i kvalitativ metode*. Bergen. Fagbokforlaget.

Tveiten, C. K., Albrechtsen, E., Wærø, I. & Wahl, A. M. 2010a. *New Opportunities for Emergency Handling in the Intelligent Energy Organization. SPE 128651.*

Tveiten, C. K., Albrechtsen, E., Wærø, I. & Wahl, A. M. 2010b. *Building Resilience into emergency management.* 2010b. Presentation of paper on Working On safety 2010 Røros, Norway.

Tveiten, C. K., Andresen, G., Rosness, R. & Tinmannsvik, R. K. 2008. Underveis mot integrerte operasjoner- en borekontraktør tilegner seg nye løsninger. In Tinmannsvik, R.K. *Robust arbeidspraksis- Hvorfor skjer det ikke flere ulykker på sokkelen?* Trondheim. Tapir Akademisk Forlag, 2008. pp. 39-55.

Vinnem, J.E. 2009. *Sikkerhet og beredskap på norsk sokkel*. In Store Norske Leksikon. [Internet]. Available at: http://www.snl.no/Sikkerhet_og_beredskap_p%C3%A5_norsk_sokkel [Accessed: 18 05 2011].

Wilhelmsen, H. 2010. *The use of IO concepts in emergency management in light of resilience engineering.* Department of Industrial Economics and Technology Management. Faculty of Social Sciences and Technology Management. NTNU. Trondheim. Norway.

With, D. 2010. *Lecturefoil in "TIØ 4200 Sikkerhetsledelse 2010"- Beredskap Ormen Lange.* s.l. : NTNU, 2010.

Woods, D.D. 1996. Decomposing automation: Apparent simplicity, real complexity. In Parasuraman, R. & Mouloua, M (eds.). *Automation and Human Performance. Theory and Applications.* Lawrence Erlbaum Associates.

Yeh, M. & Wickens, C. D. 2000. Effects of cue reliability, realism and interactivity on biases of attention and trust in augmented reality. *The Journal of the Human Factors and Ergonomics Society.* 2001, 43: 355.

Zuboff, S. 1988. *In the Age of the Smart Machine: The Future of Work and Power*. Basic Books.

Appendix

Appendix A - Intervjuguide

Informasjon

Takk for at du vil stille opp.

Presentasjon av intervjuer:

Jeg er masterstudent innen HMS ved institutt for industriell økonomi og teknologiledelse, NTNU.

Bakgrunn og hensikten med intervjuene

Hovedmålet for masteroppgaven er å finne ut hvordan informasjonsflyten mellom de ulike aktørene under en beredskapssituasjon kan bli bedre, samt å gi generelle råd omkring hvordan planleggingen og samhandlingen kan forbedres i ulike faser av beredskapsstyringen. En del av oppgaven er å kartlegge aktørene som er innblandet i en beredskapssituasjon, har her tenkt å ta for meg to situasjoner/ DFU'er: 1) Utslipp av hydrokarboner eller akutt forurensning – tap av brønnkontroll og 2) eller fartøy på kollisjonskurs.

Resultat

- Informasjonen gitt i intervjuet skal brukes i masteroppgaven.

Anonymitet og konfidensialitet

- Den informasjon du gir meg vil ikke gjøres sporbar tilbake til deg.

Er det greit om jeg benytter båndopptaker?

Varighet av intervju: 1-1,5 time

Intervjuguide.

Bakgrunn.

1. Stilling/ Arbeidsoppgaver:
2. Erfaring innen beredskap (år, hvilke roller har du og hvilke har du hatt.):
   - Nåværende bedrift
   - Andre bedrifter

Beredskapsplanlegging

3. Hvordan foregår beredskapsplanleggingen hos dere?
4. Hyppighet av trening på DFU'er.
   - Trenes det internt/ eksternt
   - Hvilke planer foreligger

Aktører

5. Hvilke aktører kontaktes i en beredskapssituasjon?
   - Internt
   - Eksternt
6. Hvordan tas det hensyn til ulike aktører i analyse/planleggingsfasen? Hvordan identifiseres de?

Rolle i beredskapssituasjonen

7. Når i beredskapssituasjonen kontaktes disse aktørene? (Når i situasjonsutviklingen)
8. Hvordan kontaktes de?
9. Hvilken rolle spiller de i beredskapssituasjonen?
10. Hvorfor kontaktes de? (Finnes det her kriterier, avhenger det av hvilke typer scenarioer?)
11. Samhandlingsform/ samhandlingsteknologi.
12. Hvilke former for teknologi benyttes i kontakten med aktørene i beredskapssituasjonen? (telefon, samhandlingsrom, informasjonsdeling, crisis manager el.lignende.)
13. Hvor hyppig foregår kontakten med disse aktørene, frekvensen på samhandlingen/ kontakten.
14. Hva er den viktigste faktoren for å skape et godt samarbeid mellom de ulike aktørene under en beredskapssituasjon? (Tillit, myndighet, hyppige treninger, rolleavklarering.. osv.)
15. Hvordan oppfatter du informasjonsstrømmen under en beredskapssituasjon?
16. Hvordan sorteres informasjonen under en beredskapshendelse?
17. Hvilke problemer oppleves i dag ved kommunikasjon mellom ulike distribuerte aktører (i en normal situasjon)?
18. I hvilken grad ser du behov for å benytte samhandlingsteknologi i en beredskapssituasjon?
19. Hva ser du for deg kan bli aktuelle problemer i fremtiden ved bruk av samhandlingsteknologi i en beredskapssituasjon?
20. Har innføringen av ny teknologi medført at det er blitt en forskjell i aktørbildet i beredskapssituasjoner nå i forhold til hva det har vært tidligere?
21. Er det blitt dannet nye mønster i forhold til hvordan de ulike aktørene snakker sammen på bakgrunn av denne nye teknologien?
22. Hvorfor er ikke samhandlingsteknologi benyttet i beredskap?

Tillit

I forbindelse med beredskap er tillit en viktig faktor, personer som ikke kjenner hverandre skal samarbeide for å løse et problem. Dannelse av tillit uten noe kjennskap til personen på forhånd kalles swift trust, disse spm. Fokuserer på om hvordan en slik form for tillit dannes under en beredskapssituasjon.

23. Hva tenker du omkring tillit i en beredskapssituasjon?
24. Hvordan skapes tillit mellom ulike roller i en beredskapssituasjon (samlokaliserte/distribuerte)?
25. I hvor stor grad stoler du på tittelen/rollen til en person, uten å vite noe om personen fra før?
26. På hvilken måte vil du si at det er viktig å kjenne personene du skal samarbeide med under en beredskapssituasjon?
27. Hva skal til for at du mister tilliten til en aktør/ rolleinnehaver under en beredskapssituasjon?
28. Er det noen roller i en beredskapssituasjon som du har større tillit til enn andre? Hvem?
29. Har du tillit til teknologien som benyttes under en beredskapssituasjon?
30. Vil du på noen måte tvile på at informasjonen når frem under en beredskapssituasjon?

Fremtidige muligheter

I forbindelse med innføring av integrerte operasjoner, særlig det som har med opprettelsen av støttegrupper/speilorganisasjoner/ekspert-team på land, tenkes det på om man kan bli mer proaktiv (det vil si å være mer før var, tenke mulige fremtidige scenarier tidligere i utviklingen av avvik osv.) i beredskapshåndtering. Det kan f.eks. dreie seg om å etablere deler av beredskapsorganisasjonen tidligere eller å gi disse nye gruppene en plass i beredskapshåndteringen. Jeg har noen spørsmål til deg om dette:

31. På hvilken måte mener du at bruken av IO teknologi kan være med å virke proaktivt når det inntreffer et avvik på installasjonen?
32. Hvordan mener du at man kan man skape proaktivitet innen beredskap?
33. Er dagens beredskapssamarbeid godt nok til å forhindre en katastrofe lik Deepwater Horizon?
34. Hva er din mening om hva som bør gjøres for å forbedre dagens beredskapsarbeid?
35. Avslutning
36. Har du noe mer å tilføye, er det noe jeg har glemt å spørre om?
37. Kan jeg ta kontakt senere hvis det er noe jeg har glemt å spørre om?

Takk for intervjuet!

Appendix B – Transkripsjonstabell

Aktør A	
Informasjons område:	**Informant svar:**
Beredskapsplanlegging	Arbeidet mye for å finne sammenheng mellom kvantitativ risikoanalyse for den enkelte installasjon, beredskapsanalyser for den enkelte installasjon og barriereanalyse, beredskapsplanverk, trening og øvelser. Hensikten med dette var å lage en rød tråd gjennom hele denne prosessen. Fra risikoen som ble presentert i den kvantitative risikoanalysen til beredskapsanalysen hvor de blir benyttet i de situasjoner hvor du trenger strategier og ytelses krav for å håndtere disse, videre implementert i beredskapsregler og planverk og deretter gjennomgått i øvelser og trening. Dette er det etablert en egen intern prosess på egen intern styrende dokumentasjon. NORSOK Z-013- blitt revidert i den senere tid, der har de hatt en deltaker i gruppa, for å få denne metodikken inn i NORSOK standarden også.
Trening og DFU	Pga. omlegging av metoden analyser utføres på har medført at begrepet DFU er omdefinert. Tidligere DFU svært spesifikt definert (for eksempel lekkasje fra gitt ventil i et gitt system osv.) Nå er DFUene utvidet til å omfavne flere tema (for eksempel hydrokarbonlekkasje) Under en slik DFU kan det være flere hundre ulike scenarioer for et plattformkompleks. Mens DFUen mann over bord, alltid er den samme, nemlig mann over bord, her er det ikke så mange ulike scenarioer. Krav om til de som innehar beredskapsfunksjoner om å trene en gang pr. tur (pr. gang de er ute på plattform, båt osv.) på sin funksjon. Ingen spesifikk frekvens for hvor ofte den enkelte DFU trenes på. Trening knyttet til mange forskjellige DFUer på plattform samtidig, ikke alle med i hver enkelt DFU, kun de med en funksjon innen den spesifikke DFUen.
Oppdeling av beredskapsorganisasjonen	Beredskapssentralen (1. linje beredskap) ledes av plattformsjefen, han har det øverste ansvaret på plattformen, han bestemmer hva som skal gjøres. Beredskapssentralen snakker med HRS og 2. linje beredskap.
Aktører i en beredskapssituasjon	Beredskapssentralen varsler SAR m. crew, sentralbord, beredskapsfartøy og HRS tidlig. 2. linje beredskapssentral har en times mobiliseringstid, dvs. at det kan gå inntil en time før 2.linje beredskap er mobilisert. Når 2.linje beredskap er på plass varsler de også HRS, men dette blir gjort for å være sikker på at det er opprettet kontakt og for å avklare behov for en evt. liason. 3. linje beredskap varsles av 2.linje beredskap. 3. linje beredskap kan mobiliseres i crisis management team. Ptil varsles av 2.linje beredskap de skal videre varsle diverse andre myndigheter.
Hvordan tas det hensyn til ulike aktører i analyse/ planleggingsfase, hvordan identifiseres de?	De ulike aktørene identifiseres ut i fra hvilken rolle de innehar. Har de en sentral rolle i beredskapsarbeidet, blir de identifisert i form av sin funksjon, noen aktører blir identifisert på bakgrunn av at det står at de skal varsles i lovverket, det ligger her en plikt for operatør å varsle dem og holde de oppdatert om hva som skjer.
Teknologibruk mellom aktører i en beredskapssituasjon	Kommunikasjon internt, benyttes eget loggføringssystem. Alt det som beredskapssentralen i første linje, og andrelinje beredskapssentral loggfører vises til de ulike aktørene som er forhåndsdefinert for å få vite om denne typen informasjon. Alle de tre ulike loggene vises på veggen hos andrelinje beredskapssentral. All informasjon som blir loggført deles. I tillegg til loggføring er det kommunikasjonsformen telefon som benyttes. Andrelinje beredskapssentral består av: Beredskapsleder (foretar den interne varslingen), beredskapskoordinator (foretar den eksterne varslingen, myndigheter, HRS osv.), loggfører som loggfører alle aktivitetene i andrelinje beredskapssentralen, mediakontakt, pårørendekontakt, beredskapslege, telekommunikasjons tekniker. Dette

	betyr at når andrelinje beredskapssentral varsles, så blir alle disse funksjonene varslet. Internt i organisasjonen foregår kommunikasjonen hovedsaklig på logg og telefon, de benytter også e-mail, faks osv, men dette benyttes i mindre grad. Hvilke instanser som varsles kan variere fra hendelse til hendelse, f.eks. dersom det er mange skadde vil sykehus varsles, men dersom det ikke er noen skadde vil ikke sykehuset varsles. Det er et program som siler hvilken informasjon de ulike beredskapslinjene skal ha, hvilken tilgang de skal ha til de enkelte skjema. De interne fag- og støttegruppene som varsles av andrelinje beredskapssentral vil variere avhangig av hvilke scenarioer som utspiller seg. Ved en DFU som omhandler boring, vil onshore drilling centre varsles dette senteret har oversikt over tilstand til brønnene og borefremdrift fra land muliggjort ved hjelp av IO- teknologi. Den informasjonen som disse støttegruppene her vil bli gjort tilgjengelig for andrelinje beredskapssentral. Andrelinje beredskapssentral vil mobilisere de støttegrupper og de personer de har behov for under en gitt hendelse. Ptil får tidlig varsel av HRS om den oppståtte hendelsen. Ved en innleid flyttbar innretning som ligger på et felt og er koblet opp mot en permanent installasjon vil OIM på den flyttbare installasjonen bli varslet av generell alarm, og han har videre varslingsrutiner mot sin andre linje på land. Slik at andre linje hos entreprenører kan varsles denne veien, eller/og via operatørens andrelinje beredskapssentral. Dersom entreprenørene kun har personell ute på installasjonen, vil det være pårørendekontakten i andrelinje beredskapssentral som foretar varslingen til entreprenørselskapene. Dersom det er en situasjon som påvirker de andre installasjonene vil de bli varslet. I utslippsrelaterte DFUer er det dannet områdeberedskap. Da er det både områdeinterne ressurser og ressurser fra de samarbeidende områdene. Kystverkets oppgave i en DFU omkring utslipp av hydrokarboner er at de ivaretar statens sitt ansvar når det gjelder forurensning. Kystverket er ansvarlig for en oljevernaksjon hvis en tankbåt havarerer, men ikke ansvarlige hvis noe skjer på en installasjon. Kystverket har muligheten til å overta ledelse og koordinering av en oljevernaksjon hvis de synes at operatøren ikke gjør en bra nok jobb. Kystverket skal ha en plan over hvordan en beredskapshendelse skal håndteres innen en time etter mobilisering. HRS kan også overta ledelse og koordinering av ressursene i en redningsoperasjon. Ekstern informasjonsutveksling foregår hovedsaklig ved hjelp av telefon. Støttesenter og faggrupper benytter IO konsepter for å fremskaffe informasjon om de ulike hendelsene. F.eks. har onshore logistikk senter informasjon om hvor båter er, hvem eier er, hvilken last de har osv. De ulike fagmiljøene innen hver enkelt disiplin vil være involvert lenge før situasjonen blir en beredskapssituasjon, dette skjer ved hjelp av IO teknologi.
Informasjonsstrøm under en beredskapssituasjon	Loggen gir en informasjon overflow, det er for mye du skal forholde deg til. Vanskelig å ta stilling til alt som står i loggen, må lære seg å sortere ut det som trengs. Ingen form for sortering av Informasjonen som kommer inn til andre linje i beredskapsorganisasjonen. Under en beredskapssituasjon er det en utfordring av loggen ikke blir noe bedre enn det loggføreren er, graden av hvor god loggen er vil ha en svært stor sammenheng med loggføreren.
Mulighet for bruk av samhandlingsteknologi i beredskapssituasjon	Man kan ha en videokonferanse mellom de ulike linjene under en beredskapsorganisasjon. Men så langt er ikke en slik form for informasjonsdeling benyttet under en beredskapssituasjon. En større grad av bruk av samhandlingsteknologi for eksempel videokonferanse, bilder osv. kunne medført at det ble en raskere oppdatering av de ulike aktørene

	i en beredskapssituasjon, at de ulike aktørene satt med det samme situasjonsbildet over situasjonen, og innehadde den samme forståelsen over hvor langt i hendelsesforløpet man hadde kommet. Det finnes i dag muligheter for bruk av webkamera i andrelinje beredskapsrommet, men dette brukes ikke i utstrakt grad, dette er hovedsaklig benyttet i ettertid for å kartlegge omfanget av skadene. Så langt er det ikke blitt tatt i bruk IO teknologi i beredskapsorganisasjonen, men mulighetene skal kartlegges i dette året. Muligheter for at viktig informasjon ikke blir oppdaget raskt nok på grunn av lite oversiktlige logg tavler, lokal beredskapssentral har hovedansvar om å forhindre hendelsen, loggføring hos dem kommer i andre rekke. Det vil ikke forekomme at informasjon som skulle kommet fra lokal beredskapssentral forhindrer andrelinje beredskapssentral i å utføre sine oppgaver.
Tillit	Kjenner hverandre i vaktlaget og i beredskapssentralen, ikke tenkt på tillit som et problemområde innen beredskap, noe som kan implisere at det eksisterer tillit i en slik situasjon. Tilliten blir etablert under treninger og øvelser, da både med de interne samt også med de eksterne aktørene. Man stoler på den treningen og opplæringen en person har fått, uten å kjenne personen.
Tillit til teknologien	Har full tillit til at informasjonen som sendes kommer frem til riktig person. Men ved en stor eksplosjon på en installasjon vet man ikke hvordan kommunikasjonsutstyret vil klare seg, men det er her innebygd en redundans med kommunikasjonsverktøy i nummerert rekkefølge fra en til sju, over hva som skal benyttes i en situasjon. F. eks. linje via fiber, linje via andre installasjoner, linje via England osv. dette medfører at dersom en linje bryter sammen har man backup løsninger.
Hvordan kan IO teknologi være med å virke proaktivt v. avvik på installasjon?	Potensialet for bruk av IO teknologi proaktivt, gjør at det er mulig å trigge en beredskapssituasjon på et mye tidligere tidspunkt. Man kan ved hjelp av IO teknologi arrangere ressurser og løse situasjonen på et mye tidligere tidspunkt i forhold til tidligere. Men alt dette kommer av når i avviksprosessen man definerer beredskap, er det når du oppdager uregelmessigheter i prosessen og setter inn ressurser for å korrigere dette, eller er det når lekkasjen er oppstått. Men i det store og hele gjør IO teknologien det mulig å gripe inn i en hendelse på et mye tidligere tidspunkt. Kan kalle dette en omdefinering av beredskap, for å kunne bli proaktiv i en større grad.

Aktør G	
Informasjons område:	**Informant svar:**
Oppdeling av beredskapsorganisasjonen	Beredskapsorganisasjonen oppdelt i 1,2 og 3 linje. 1 linje- der hvor ting skjer, 2 linje- skal skaffe ressurser for 1 linje, organiserer beredskapsarbeidet. Denne linja innehar avtaler og kontrakter som den kan understøtte 1 linje med. 3-linje innehar den strategiske posisjonen, passer på at de riktige valgene blir tatt for selskapet. Samt at riktig informasjon blir sendt ut i media. Ansvar og utførelse av 2.linje er hos G blitt gitt til ekstern andre linje beredskapssentral.
Aktører i en beredskapssituasjon	Her varsler 1.linje, 2. linje som igjen varsler 3. linje.
Teknologibruk mellom aktører i en beredskapssituasjon	Informasjonen mellom 2. linje og 3. linje gjøres med loggeverktøyet CIM. Støttegrupper deltar på 2.linjes oppdateringsmøter ved hjelp av videokonferanse.

Aktør I	
Informasjons område:	**Informant svar:**
Beredskapsplanlegging	Det ligger en plan for første linje beredskap, denne planen er plattform spesifikk. Denne planen inneholder et sett med DFU'er som er behandlet i beredskapsanalysen. Den inneholder rundt 16-17 DFUer. Disse DFUene trenes det på, og det er derfor øvelser hver annen uke. Under disse øvelsene blir alle de ansatte på en oljeplattform involvert, både de som har en beredskapsfunksjon og de som skal evakueres. Ukentlig foregår det tabletop øvelser, dvs. papirøvelser hvor man har et scenario omkring hva som skjer, og man blir utfordret på hva man vil gjøre hvis spesifikke situasjoner kommer opp. Alle DFUer på alle skift skal ha vært trent på i løpet av to år. I tillegg til disse øvelsene, har de spesifikke beredskapslagene trening en gang per tur, dvs. en gang per fjortende dag. Alle som har en beredskapsfunksjon må inn på et beredskapssenter på et repetisjonskurs hvert andre år. Det blir foretatt område beredskapsøvelser hvert år. Her involveres flere installasjoner, helikopter, båter osv. Det er et viktig skille mellom øvelser og verifikasjonsøvelser. Rene øvelser er hvor du trener på en bestemt hendelse, mens verifikasjonsøvelse er øvelser hvor du foretar en øvelse for å undersøke om du når dine ytelseskrav. Verifikasjonsøvelser styres fra andre linje. Mens vanlige øvelser styres ute på installasjonen. Etter Scandinavian Star hendelsen ble proaktiv beredskapsledelse innført, dette gjelder i alle ledd av beredskapsledelsen. Proaktiv beredskapsledelse vil si at når man sitter ned med staben sin så vil man ha en fokustavle foran seg hvor man setter opp hva man skal fokusere på, hvilke emner man skal arbeide med. Disse møtene blir utført ca hver halvtime, hvor da beredskapsleder har muligheten til å sette opp nye fokuspunkt i hvert møte. Slik at man stadig fokuserer på de riktige tingene. Alle hendelser til lands og til vanns er et samspill mellom HRS og Politiet. Andre linje beredskap hos denne aktøren har radarbilde over norsk sokkel. Hvis andre linje beredskap ikke utfører sine arbeidsoppgaver godt nok, vil deres delegerings og koordineringsansvar kunne bli tatt over av HRS. Ved et oljesøl vil også kystverket sette ned sin egen stab, operatør må derfor sende over en aksjonsplan omkring oljesølet om hva man vil benytte for å rense området, som kystverket må godkjenne, være enige i. Det er operatørselskapene som er ansvarlig for utslippet i alle dets faser, også for opprydningen som foregår på land. På grunn av dette, må det også tas kontakt med de interkommunale aksjonsgruppene (IUA) , dette ble gjort gjennom NOFO. (IUA er aksjonsgrupper som nærliggende kommuner har satt sammen for å sikre at beredskapsarbeidet i kommunen er i overensstemmelse med det som kreves av forurensningsloven). NOFO har avtale med alle depotene kystverket har rundt omkring i landet slik at man kan gå inn og låne utstyr fra disse depotene. Norge er litt spesielt beredskapsmessig, i den sammenheng at her benyttes et prinsipp som kalles samvirkeprinsippet. Dette prinsippet går ut på at dersom man har en hendelse så vil det foregå et samvirke etatene imellom. Sagt på en annen måte, så vil man ikke konkurrere i beredskapssammenheng, men samarbeide om å nå de ønskede målene. For eksempel i en foregående øvelse, ble jagerfly fra forsvaret benyttet for å fly over et oljesøl for å kartlegge sølet, deretter ble bildene overført til NOFO og andrelinje beredskaps sentralen. I Norge finnes det to HRS sentraler, de er lokalisert i Stavanger og i Bodø. Under en beredskapssituasjon er det svært viktig å ha kontroll på personalet, dersom noen er sendt på sykehus, er det svært viktig å vite hvilket sykehus denne personen er sendt til osv. Det hjelper ikke hvor dyktig man enn er til å håndtere det tekniske dersom man ikke

	klarer å håndtere de menneskelige faktorene, nemlig hvor de ulike personene er, at det finnes personell på mottaksstedet for å ta imot dem, at de registreres osv. Dette kan eksemplifiseres ved at dersom en evakuert person kommer til land, men at det ikke er noen der til å ta imot han, han står der da uten noen ting, i denne settingen hjelper det ikke om man er aldeles så flink med resten av beredskapshåndteringen hvis man svikter på den menneskelige biten.
Oppdeling av beredskapsorganisasjonen	I en beredskapssentral er det ulike stillinger som skal fylles. Sjefen i en slik situasjon er beredskapslederen, videre har man en HSE representant, som er ansvarlig for driften når beredskapslederen er ute. HSE representanten er også ansvarlig for å utarbeide oljevernsplanen, siden han innehar spesialkompetanse på oljevern. Ved et oljesøl må du innen to timer levere en aksjonsplan til kystverket. Denne aksjonsplanen er lagd ferdig i prinsippet, og det må bare fylles inn den situasjonsspesifikke informasjonen for denne hendelsen før den kan sendes inn. Videre sitter det to logistikkansvarlige i beredskapssentralen en person for logistikk luft og en person for logistikk sjø. De mindre selskapene har kun en logistikkperson, men siden det i dette selskapet eksisterer så mange båter og helikopter er man nødt til å ha to personer i denne stillingen. Logistikk personene har som en av sine oppgaver i en beredskapssituasjon å skaffe raskt oversikt over ressurs tilgangen. F. eks. oversikt over hvilke fartøyer som er i området, samt at disse fartøyene må ha oljevernutstyr. Man må også ha informasjon om hvor mange barrierer som kan skaffes innen en viss tid. Noe av det viktigste innen en hendelse med oljesøl er å skaffe oversikt over sølet. En fin måte å gjøre dette på er å komme opp fra havoverflaten, v. f.eks. å sitte i et helikopter for å kartlegge sølet. F.eks. kan et SAR helikopter ha et infrarødt kamera som filmer/ tar bilde av sølet og sender dette over til beredskapsfartøyet. Da ser kaptein i dette fartøyet hvor oljen er tykkest, og vil starte å samle opp olje ved dette punktet. En annen rolle som befinner seg i andrelinje beredskap er "marine operations". Innehaveren av denne stillingen kjenner plattformen godt, og kan gi beredskapslederen gode råd og nyttig informasjon omkring hvilken form for utstyr som finnes der, rømningsveier osv. Teamene som arbeider i andrelinje beredskapsrommet går i et rotasjonssystem på seks skift. Andrelinje beredskapsrommet står tomt når det ikke er en beredskapssituasjon. Parallelt med dette rommet er det bygd opp et overvåkningssystem over kysten, dette er bygd opp på grunnlag av at det finnes tre radarkilder nedover langs kysten, disse tre radarkildene ble slått sammen, da fikk man et veldig godt bilde over all aktivitet. Dette bildet har marine operations og de har derfor oversikten over all aktivitet som foregår i sjøen på den norske kontinentalsokkelen. Men behovet for å slå sammen marine operations med et oversiktsbilde over luftrommet vil komme i løpet av noen år. Da vil man kunne se et samlet bilde over all aktivitet både til lands og til vans over den norske kontinentalsokkelen. I marine operations sitter det tre personer på vakt til enhver tid. marine operations følger med på alle skip, siden de har ansvarte for å oppdage skip på kollisjonskurs. De legger inn AIS og target på disse skipene, slik at dersom de har kurs mot en installasjon for lenge går det en alarm hos marine operations. Da må marine operations varsle installasjonen, slik at de kan starte nedstengning av installasjonen og evakuere. Et eksempel på dette er at det går store tankbåter fra Murmansk nedover langs kysten, disse svarer ikke på anrop hvis du ikke snakker russisk, dette har medført at marine operations har folk på vakt som snakker russisk. marine operations og andrelinje beredskap sitter nær hverandre, dette gjør at dersom en beredskapssituasjon skjer på nattestid,

	vil en person fra marine operations, gå over til andrelinje beredskapssentralen og starte alle systemer som finnes der inne, slik at alt er oppe og går når andrelinje beredskapslaget kommer på vakt. Videre i rommet for andrelinje beredskap sitter en pårørendekontakt, denne pårørendekontakten har en organisasjon rundt seg som kan mobiliseres. Hit ringer de pårørende,, det er her svært viktig å holde oversikt over hvem som har ringt, når de ringte osv. slik at den som ringer kommer i kontakt med den samme personen også neste gang han ringer for å få en update osv. Videre innehar en person (f.eks. journalist)en posisjon som innebærer å dele ut informasjon til media. Dette er en svært viktig funksjon siden beredskapshendelser også har et omdømme aspekt for bedriften. Derfor er det viktig at en fra selskapet skriver pressemeldinger (holding statements) for å holde media oppdatert. Disse pressemeldingene skal inn til beredskapslederen som skal godkjenne dem før de forsvinner fra rommet. Ved store beredskapssituasjoner er det reservert lokaler med mange telefonlinjer inn og muligheter for oppkobling til nettet, slik at man kan holde store pressebriefinger her. Men vanligvis vil journalistene komme opp til andrelinje beredskap og banke på denne døren for å få informasjon, da er det viktig at informasjonen som gis er korrekt, samtidig som man hverken gir for mye eller for lite informasjon. Den viktigste rollen i et andrelinje beredskapsrom ved siden av beredskapsleder og HSE representanten er loggføreren. Onshore føres denne loggen elektronisk, mens offshore føre den fortsatt manuelt. I tillegg til de standard tavlene som inneholder elektronisk oppdatert informasjon er det også andre tavler som skal føres. F.eks. fokustavlen, som forteller alle personene i beredskapssentralen hva som skal fokuseres på til enhver tid. Det føres ulike lister, f.eks. er været med oss eller mot oss. Dette viser hvor viktig loggføreren er i en beredskapssituasjon. Det er også en lege i andrelinje beredskap, hvor man har muligheten til å benytte telemedisin for å behandle skadd personell på installasjonen. Prøver å få etablert telemedisin ved sykehusene i trøndelagsregionen, men har så langt kommet lengst innen dette feltet i Bergen. Telemedisin fungerer ved at en lege / kirurg på land får en videoverføring av hva som skjer med pasienten ute på plattformen, og kan på denne måten være med å stille diagnose og bestemme hvilken behandlingsmetode som skal benyttes. Men selv om dette er et bra alternativ vil ikke dette erstatte tilstedeværelse av medisinskpersonell ute på plattformen. Andre linje beredskapsrommet er avstengt for uvedkommende ved hjelp av vakter som hindrer de å komme inn. Dette betyr at selv ikke selskapets direktør har tilgang til dette rommet, i andre linje beredskapsrommet er det beredskapslederen som er sjefen. I beredskapsrommet er det en egen tavle som benyttes for å opplyse om hvem som skal varsles. Dette er en svært viktig tavle, siden det tidlig i hendelsen må det gå ut varslinger til ulike aktører. Dette gjelder først og fremst politi, HRS og Ptil. Ptil har begynt å bli mye mere aggressive (ønsker informasjon raskere og hyppigere) enn det de tidligere var, dette kan være på grunn av at de selv har bygd en egen beredskapssentral, og vil vite hva som skjer tidlig i hendelsen. Helt avhengig av hendelsen (DFUen), må man gå inn på datasystemet og sjekke hvilke personer/ myndigheter som skal varsles. Ved bruk av Crisis Manager ligger det inne i systemet hvilke funksjoner som må varsles, og dersom en blir glemt blir du automatisk varslet om dette.
Aktører i en beredskapssituasjon	Dersom man får et oljesøl er det første plattformsjefen gjør å varsle områdeberedskapsfartøyet, SAR maskinen, HRS, Ptil og andrelinje beredskap. Hvem som varsles først av andre linje beredskap og

	områdeberedskapsfartøyet, SAR, HRS og Ptil er opp til den enkelte plattformsjef. Et oljesøl ses på som en situasjon hvor man har relativt god tid. Ennå har det ikke skjedd at et slikt søl har nådd land. HRS varsles også alltid av andrelinje beredskapsorganisasjonen, og det vil derfor være en dobbelt forsikring om at HRS er varslet på denne måten. Det vil alltid være en person (en Liaison) som møter på sentralen hos HRS ved behov, med vide fullmakter fra operatørselskapet, slik at denne personen har mulighet til å oppdatere HRS om situasjonen kontinuerlig. Denne personen kalles liaison. Det vil også kunne bli opprettet en liaison mot sokkelpolitidistriktet som er berørt av hendelsen ute på sokkelen. Andre linje er operative innen 30 minutter på nattestid. Når de da kommer på vakt tar de kontakt med kystverket. Dersom det er en stor operasjon vil kystverket mobilisere sin egen beredskapssituasjon for å følge med på om operatør gjør en god nok jobb. Når andrelinje beredskap varsler kystverket, skal aksjonsplanen for hvordan oljesølet skal håndteres leveres til dem innen to timer (I aktivitetsforskriften §79 står det innen en time). I denne planen skal det være informasjon om hvordan utslippet skal håndteres, om været er med oss eller mot oss, hvilke barrierer som er på plass, når lensene er på plass i sjøen, drivbaneberegninger(beregninger av hvordan utslippet vil bevege seg) osv. Dette dokumentet skal oppdateres under hendelsen, slik at dette blir et levende dokument gjennom hele hendelsen. Denne overleveringen av aksjonsplanen foregår elektronisk, ved at man først ringer kystverket og forteller at man er klar til å sende dokumentet og deretter sender det. Oljevern kan foregå i mange måneder, mens en beredskapssentral kun er samlet sammen i 2-3 dager, dette er grunnen til at under en større utslippshendelse vil man be NOFO om å komme til bedriften for å sitte i en stab for videre håndtering av oljeutslippet. I en beredskapssituasjon samarbeider de ulike operatørene på et felt for å skape en best mulig løsning på en beredskapshendelse. Andre linje beredskap vil kontakte NOFO, slik at de får oversikt over hvor NOFO fartøyer befinner seg. Andrelinje tar kontakt med marine operations for å få oversikt over hvor slepebåter og tankbåter befinner seg. For hvert diftsområdet blir en driftsvakt kontaktet av andrelinje beredskap, denne vakten er blant annet ansvarlig for å varsle eierne av plattformen. Hvis SAR maskin og beredskapsfartøyet som tilhører et område blir kaldt ut, sendes det ut varsel om dette til de andre installasjonene på området. Dette er på grunn av at da vil de andre installasjonene ha en svekket beredskap i tilfelle noe skulle skje hos dem.
Teknologibruk mellom aktører i en beredskapssituasjon	I loggen blir alt som skjer registrert dette gjør at man kan gå inn i loggen og se akkurat hva som skjedde ved et gitt tidspunkt. Loggen er ikke et optimalt verktøy for informasjonsdeling, siden man ikke alltid får med seg det viktigste først, men det er det beste man har per i dag, og man vil alltid forsøke å videreutvikle dette systemet. Hvis man ikke øver og trener på alle funksjoner i en beredskapsorganisasjon, vil alt falle sammen som et korthus hvis noe går galt et sted i organiseringen. Det er viktig at beredskapslederen har et proaktivt blikk på situasjonen, slik at han klarer å forutse hva som kan komme av utfordringer i neste fase av beredskapsarbeidet. Det er svært viktig at tredjelinje ikke blander seg inn i beredskapssituasjonen. De skal tenke på hvilke innvirkninger hendelsen får for selskapet, og ikke blande seg inn i detaljstyringen. Inne i andrelinje beredskapsrommet blir det også foretatt voice recording. I førstelinje foregår loggskrivingen ofte manuelt og ofte på tavler osv. Mye av informasjonsdelingen mellom andrelinje og førstelinje beredskap foregår over telefonen ved at en av aktørene ringer den andre for å oppdatere status. Disse

	oppdateringsmøtene blir ofte utført ved at hele andre linje stopper opp for å høre status for første linje. Disse oppdateringene skal skje hyppig, og det bør ikke være mere enn 30 minutter mellom hver oppdateringstelefon / time out. Grunnen til dette er at det er svært viktig at det er en vektlegging på å fokusere på de rette tingene til enhver tid. Dette på grunn av at risikobildet kan endre seg utover i situasjonen. Men det er også viktig at de som sitter i andre linje ikke hindrer førstelinje i å gjøre jobben sin, nemlig å stoppe utviklingen av situasjonen, ved å kontinuerlig mase om tilgang til ny informasjon. Hos personell ved første linje beredskap skal alltid målet være å bekjempe hendelsen, informasjonsoverføringen kommer i andre rekke. Støttepersonell som tilhører de ulike faggruppene blir kontaktet ved behov, enten kommer de til beredskapssentralen fysisk eller så har de kontakt via ulike media.
Viktigste faktor for godt samarbeid	Den viktigste faktoren for et godt samarbeid er klare beskjeder, i en beredskapssituasjon er det nesten litt militære forhold, det er ikke noe "dilldall". Det at man har trent så mye at man er trygg på hverandre er en viktig faktor i en beredskapssituasjon. Den dagen det smeller vet du i alle fall hvem du har rundt deg, du har trent med de, øvd med de og kjenner de. De ulike innehaverne av de ulike rollene i en beredskapssituasjon har møtt hverandre fra før som oftest, man kan ikke ha en fullstendig utskiftning av personell, det vil bli for farlig. Man må være svært selektiv i utvelgelsen av personale, man må velge folk som har en del erfaring. Det å sitte inne med en logg over når de enkelte personene trente sist og deres kompetanse innen beredskap er svært viktig. Dette for å sikre at de som er satt opp på vakt sammen har kompetansen som trengs for å løse en hendelse. Legger mye penger og ressurser i treninger og øvelser knyttet til beredskap. Øvelser blir foretatt både internt og eksternt, men i hyppigst grad internt. Når nye rigger kommer inn i et område blir det utført tabletop øvelser, dersom de ikke er fornøyde med disse øvelsene blir det foretatt en fullskala øvelse for å forsikre seg om at beredskapen blir ivaretatt. Det blir utført møter og seminarer med Ptil, HRS og andre offentlige aktører for å vise hvilke krav de setter til operatør og hvilke krav operatør setter til dem.
Tillit	Krav til kursing av personell i beredskapsstillinger gjør at man stoler på dem. Siden man forventer at de har gjennomført de øvelsene og treningene som det er obligatorisk at de skal gjennomføre. Samt at det blir utført verifikasjoner både internt og eksternt for å påse at beredskapsorganisasjonen er slik den skal være i følge lover og regler.
Tillit til teknologien	Viktig å få en verifikasjon på at ordren er forstått. At man får en tilbakemelding om at en beskjed er mottatt.

Aktør Ptil	
Informasjons område:	**Informant svar:**
Rolle I beredskapssituasjon	Offshore er Ptils rolle formellt å holde tilsyn med at operatørene og aktørene håndterer hendelsen på en forsvarlig måte.
Oppdeling av beredskapsorganisasjonen	Det som skjer i praksis, er at hvis det er en alvoring hendelse danner Ptil sin egen beredskapsorganisasjon. De har en egen beredskapssentral, et eget lokale for en minutt for minutt oppfølging. Denne dannelsen av en egen beredskapsorganisasjon gjøres av flere grunner, dels fordi det er en del av deres oppgaver å følge tilsyn, samt at ved å føre dette tilsynet setter man seg i en slik stilling at man kan føre videre informasjon til de som har behov for informasjon omkring hendelsen, det kan være politisk ledelse, departementet og de setter pressefolk i stand til å besvare spørsmål som kommer fra pressen. Ptils beredskapsorganisasjon vil

	reflektere Ptils oppgave når det kommer til organiseringen av denne organisasjonen. Deres beredskapssentral vil ikke inneha de samme rollene som en operatørs beredskapssentral. Ptil vil ikke ha noe operativt ansvar under en beredskapshendelse. Deres viktigste mål blir å skaffe seg et bilde over hva som skjer, samt hva operatøren gjør. Prøver videre å danne seg et bilde over ansvarligheten i måten operatøren håndterer situasjonen. Det de er opptatt av er hvilken langsiktig strategi selskapet har. F.eks. når man har mistet kontrollen over en brønn, tenker alltid på det verste utfallet som kan forekomme, og det kommer opp spørsmål om en avlastningsbrønn, sier operatør at de har startet sin planlegging av dette, da et det typisk Ptils oppgave å stille spørsmål ved, Plan A er ok, men hva hvis Plan A feiler, har dere en Plan B klar? Ptils oppgave blir å presse på operatør slik at de modner to alternativer parallelt, slik at man ikke kommer opp i en situasjon hvor man kun har satset på et bekjempningsalternativ, feiler der, og må deretter begynne på nytt igjen. Ptil vil forsikre seg om at en del planlegging osv. er utført omkring andre løsningsalternativ, slik at man ikke taper for mye tid dersom noe går galt under utførelsen av det første alternativet. Det å legge trykk på planlegging og mulig feiling, det å ha en horisont hvor man ikke bare ser hendelsen minutt for minutt er det som Ptil fokuserer på. Ptil vet at operatørselskapene er svært drillet på minutt for minutt håndtering av en hendelse. Det å redde menneskeliv osv. "ligger i blodet på operatørselskapet", Ptil vil følge med på denne delen av beredskapshåndteringen også, men det å ha flere bekjempningsstrategier som Ptil fokuserer på. Ptil legger trykk på aktøren ikke ved å komme med forslag om hvordan hendelsen skal opereres, men med spørsmål omkring hvilke faktorer de har tenkt på i en slik hendelse, f.eks. hvis noe feiler hva gjør de da?
Teknologibruk mellom aktører i en beredskapssituasjon	Varslingsbestemmelser, det har kommet en ny forskrift etter nyttår, styringsforskriften § 29- varsling og melding til tilsynsmyndighetene ved fare og ulykkes hendelser, alvorlig, akutt skade, død, livstruende sykdom, alvorlig svekking eller bortfall av sikkerhetsfunksjoner eller andre barrierer slik at innrettningens integritet er i fare, akutt forurensning. Hvis dette er på et veldig alvorlig nivå, så skal Ptil varsles umiddelbart per telefon av den ansvarlige. Om det er første eller andre linje som kontakter Ptil kommer an på hvordan organisasjonen har organisert seg. Men hovedsaklig er det andre linje som varsler Ptil. Ptil har ikke svarene på hvordan ting skal skje, men at de skal skje og når de skal skje. Det er slik de regulerer hele petroleumsvirksomheten, de er svært tilbakeholden med å gi svarene, men stiller en del krav som må tilfredsstilles, og hvilke funksjoner og ting som skal oppnås via kravene. Dersom en hendelse er skikkelig alvorlig vil man få et varsel innen en time. Det anbefales (står i styringsforskriften, §29 at Ptil skal informeres) at HRS nord eller sør skal bli varslet om hendelsen umiddelbart. Slik at de kan begynne å forberede seg, dvs. skaffe seg oversikt over ressursene. Denne ressursoversikten består i å kartlegge hva det finnes av helikopter i området, hvor har de sine redningshelikopter, hvor mange er operative. De kan derfor begynne å forberede disse helikoptrene på å rykke ut. Når noe skjer ute på en installasjon vil de ringe til sin andre linje og til HRS, HRS vil også varsle Ptil rett etter at de selv er blitt varslet. Dette medfører at Ptil allerede kan vite om hendelsen når operatøren ringer for å informere om den. Når Ptil varsles av operatører blir dette varslet gitt til Ptils sentralbord, der noteres navnet på varsleren og kort hva som er hendt. Deretter ringer sentralbordet til den personen som har beredskapsvakt i Ptil. Beredskapsvakten vil da ringe tilbake til kontaktpersonen hos operatøren

	for å bekrefte at informasjonen er mottatt og muligens også få mere informasjon. Alt etter hva som er skjedd kan man starte en dialog med selskapet for å forstå hva som har skjedd og hvor alvorlig dette er. Ved alle hendelser som inneholder akutt forurensning er det gjort en avtale med miljømyndighetene ved at alt skal varsles til Ptil som videre varsler Kystverket med en kopi til Klif. Dette gjøres på grunn av at Forskrift om styring og opplysningsplikt i petroleumsvirksomheten og på enkelte landanlegg er felles for Ptil, Klif og helsedirektoratet. Disse tre aktørene samarbeider derfor seg imellom, og har gjort det slik at Ptil er den myndigheten operatør skal varsle ved en hendelse. Hvis hendelsen er langvarig vil kystverket og Klif få jevnlige oppdateringer. Det er ulike former for varslinger til Ptil avhengig av alvorlighetsgraden av hendelsen. Dersom det er en alvorlig hendelse blir Ptil varslet pr. telefon, her får de ca. 350 varsler pr. år, mens de mindre alvorlige hendelsene som skal varsles på et skjema er det ca. 450-500 av pr. år. De fleste av disse 850-900 henvendelsene ringer Ptil tilbake og sier at de tar det som en del av den ordinære saksbehandlingen. Dette belyses tydelig av antallet ganger Ptil har organisert sin egen beredskapsorganisasjon de siste årene, som ligger på 6-8 ganger årlig. Ved Big Orange XVIII ulykken etablerte Ptil sin egen beredskapsorganisasjon. Dette og når fartøy mister kontrollen og driver mot installasjoner under vinterstormer er typiske situasjoner hvor Ptil bemanner sin egen beredskapssentral. Ellers etableres de under gasslekasjer, brønnhendelser, strømutfall- total blackout og den type hendelser. Ved slike hendelser vil Ptil ha kontakt med andrelinje beredskap og drifts- og faggrupper på en nesten kontinuerlig basis, dersom det er behov for dette. Kontakten med drifts og faggrupper er for å få en større forståelse av hva hendelsen egentlig går ut på. Ptil får oppdateringer på 30-60 minutts nivå omkring ressursnivå, værforhold, personellforhold, helikopter status osv. Denne informasjonsoverføringen foregår i svært stor grad over telefon. Videokonferanser osv. tar for mye tid på dette nivået. Ønsker rask og kjapp informasjon og statuser. Benytter e-post for å oversende informasjon. Benyttet tidligere faks, det er Ptil i ferd med å fase helt ut, de skal flytte til et nytt bygg med en ny beredskapssentral og vil da ikke ta telefaks med seg noe lengre, da vil det kun være e-post som er formidlingsmediet omkring skriftlig kommunikasjon.
Viktigste faktor for godt samarbeid	Det at Ptil og operatørselskapet har sine faste roller, at de er enige om hvem som har hvilken rolle er svært viktig. Det mener informanten at Ptil gjennom år med dialog, diskusjon og øvelser sammen med operatør har fått etablert en slik forståelse. Viktig at oljeselskapene vet hvilken rolle Ptil har, hvorfor de har behov for en gitt informasjon og hva de bruker denne informasjonen til. Trenger ikke å kjenne personen personlig, så lenge man vet hvilken rolle denne personen har. Det er viktig at systemene er oppbygd totalt personuavhengig, noe informanten også har inntrykk av at de er. Det blir ikke snakk om enkeltpersoner før man er på et høyt direktørnivå, på alle nivåer før dette er det snakk om selskapet i sin helhet.
Informasjonsstrøm under en beredskapssituasjon	I disse alvorlige hendelsene, ser man at ting tar litt for lang tid, informasjonen kommer ikke raskt nok. De får informasjonen, men de må be om den fremfor at den blir overbrakt uten at man ber om den, man må mase litt. Men det er viktig å huske på at det er operatøren som har det operative ansvaret, og det er i så måte viktigere å håndtere situasjonen ute på havet enn å informere myndighetene. Noen ganger kan det føles som om informasjonen kommer for seint, noen ganger er denne følelsen reell, mens andre ganger er den ikke det.

Mulighet for bruk av samhandlingsteknologi i beredskapssituasjon	Det er diskutert ulike muligheter for bruk av samhandlingsteknologi under en hendelse. En ting er hva Ptil selv skulle ønske, mens en annen ting er hva oljeselskapene ønsker. Det er ikke sikkert at oljeselskapene ønsker at Ptil sitter med et kamera inne i deres sentral, de har ofte et behov for å kvalitetssikre informasjonen som går til myndighetene. Teknologisk sett hadde det nok ikke vært noe problem for Ptil å koble seg opp i en slags videokonferanse situasjon direkte inn i operatørens andrelinje beredskapssentral og følge situasjonsutviklingen minutt for minutt. Da hadde de hatt all informasjon om hendelsen, men det Ptil ofte vil ha er operatørens, den ansvarliges vurdering av situasjonen. Grunnen til dette er at hvis Ptil sitter med all informasjon, kan operatør bare si; "vurder situasjonen selv", mens Ptil vil ha den ansvarliges, kanskje toppledelsens vurdering av forsvarligheten her og dette mister du hvis alt bare går automatisk til Ptil. Ptil vil ha informasjon, men de vil ha noe som er kvalitetssikret, noe som selskapet står for. Der er det en fare for at kan gå tapt hvis du benytter denne teknologien for langt, dette kan skje ved at man flytter utøvelse og ansvar over på myndighetene, et ansvar som skal ligge hos selskapet. Dette er noe informanten ofte føler faller ut av denne IO diskusjonen, man blir kanskje litt for teknologistyrt. Teknologi er vel og bra, men den må ikke benyttes til ansvarsfraskrivelse. Per i dag har Ptil svært lite av slik IO teknologi. De prøvde for en del år siden å utveksle logger med HRS, slik at man bare kunne logge seg opp, og deretter se den andres logg. Resultatet av dette ble at man koblet ned og fjernet hele greien på grunn av at det ble på dette tidspunktet mere styr rundt teknologien og hvordan man skulle få dette til å fungere, problemer med programmet, feil i oppdateringer osv. enn det ble fordeler ved å bruke utstyret. Resultatet ble at de koblet ned utstyret. Utstyret var ikke godt nok tilpasset, samt at når systemet var oppe og gikk fikk de så mye informasjon at man fikk følelsen av å drukne i informasjon. Man trengte ikke all denne informasjonen. Av og til er det ikke nødvendig å ha all informasjon selv. Av og til holder det med tre korte setninger for å vite hva som er viktig i en hendelse, dette er noe teknologien aldri kan erstatte mennesket i. Selv vil informanten hevde at han/hun sitter inne med en stor grad av konservativitet, med dette menes at alle teknologisystemer er gode verktøy, men de vil alltid være støttesystemer, siden Ptil alltid vil ønske å ha muligheten til å stille kritiske spørsmål omkring informasjonen de får fra operatør. Hos Ptil benyttes Telefon og e-post med bekreftelser.
Ny teknologi medført at det er blitt en forskjell i aktørbildet nå i fht. Tidligere	Det som nå skjer er at flere av de små aktørene og også de større kjøper andrelinje beredskapen hos en leverandør av dette. Det finnes i alle fall i dag 2-3 leverandører av denne typen tjenester. Det at de får dette til å fungere er teknologibasert.
Tillit	Tillit skapes på flere måter mellom ulike aktører, både i form av øvelser med selskapene og konkret ved måten hendelser blir behandlet på men også ved møter og samhandling med selskapene underveis i løsningen av en hendelse. På den ene siden har du selskapene som har vært på sokkelen i 20 år og som man kjenner til, mens på den andre siden har man disse nye selskapene som mangler mye historie og slikt, det Ptil ser er at når disse selskapene skal starte opp med sin første aktivitet, sin første letebrønn så inviterer de seg selv til Ptil hvor de får informasjon og en omvisning hos dem. Deretter etter at informasjonen fra Ptil er fordøyd blir det utført en øvelse i samarbeid med Ptil. Dette med informasjon, møter og samhandling er måten tillit skapes på.
Tillit til teknologien	Har arbeidet med beredskap lenge, erfaringen er at man ikke kan stole 100 % på teknologien. Hvis han sender en viktig e-post til noen i en

	beredskapssituasjon, så ringer han for å sjekke om e-posten er kommet frem. Dette har vist seg flere ganger å være nødvendig, og det trenger ikke være teknologien som feiler, men du skriver en feil bokstav eller et eller annet også kommer ikke beskjeden frem. Sender av og til noe til Ptils departement (arbeidsdepartementet), da ringer han og spør om det har kommet frem, eller ber de bekrefte at beskjeden er kommet frem. Det er ikke først og fremst teknologien han er redd for, den er så firkantet at der kommer ting frem, det er hovedsaklig menneskelige feil han er redd for.
Hvordan kan IO teknologi være med å virke proaktivt v. avvik på installasjon?	Ikke så veldig proaktiv på beredskapssiden, i første omgang vil nok teknologien være mer rettet mot driftssituasjonen, enn å hindre at en situasjon opptrer eller oppstår. Ser muligheten for at IO teknologi kan benyttes til overvåkning en kjappere informasjonsdeling, men du er hele tiden i tidsrekka før du har fått en beredskapssituasjon. For å hindre at man kommer inn i en beredskapssituasjon er det nok mye mere å hente, både på hurtighet og på overvåkning, kontroll, styring, oversikt. Proaktivitet i beredskapssammenheng kan være at HRS varsles tidlig i hendelses forløpet slik at de kan begynne å planlegge sin bistand i situasjonen. Når man tenker på den teknologiske utviklingen som har skjedd i beredskapssentralen hos Ptil på 20 år, så er det en ganske formidabel utvikling teknologisk sett. Får fortsatt informasjon inn per telefon, men det er ikke lenge siden de tegnet på tavler og skrev loggen på en tavle. Nå er alt datastyrt, og man får informasjon ved hjelp av skjermer på veggene osv. det er en helt ny verden. Det er kanskje informasjonsflyten for de personene som sitter i Ptils beredskapsrom og i forhold til ledelse og pressefolk hvor det har skjedd størst endring, og her vil det mest sannsynlig også skje mere. Men i informasjonsoverføringen mellom Ptil og operatørselskapet har det skjedd mindre. Redundansen man har bruk for på kommunikasjonssiden får man inn på en annen måte i dag enn i gamle dager. I dag har man telefonnettet, mobilnettet og PC nettet, mens tidligere hadde man reservelinjer til telefonsentralen til telenor osv. Noe informanten er redd for er at man stoler seg helt blind på mobilnettene, siden mobilnettet ikke er bygd opp med tanke på beredskapssituasjoner, i den forstand at en enkelt feil kan sette store deler av nettet ute av drift. Hvis det er et strømforsyningsbortfall i en region, så vil nettet falle ut. Mobilnettet har aldri vært bygd opp til å håndtere en beredskapssituasjon, man bør derfor ikke basere seg for mye på dette under en beredskapssituasjon.
Hva bør gjøres for å forbedre dagens beredskapsarbeid	Savner nye redningshelikopter, dette er noe som Norge skulle sett seg råd til. De Sea Kingene som fortsatt flyr er 40 år gamle.
Kan vi forhindre en katastrofe lik Deepwater Horizon.	En beredskapsorganisasjon er aldri bygd opp for å hindre en ulykke. Der er det helt andre tiltak som må settes i verk. Slik som han forstår beredskapsarbeid, så er dette arbeid som settes inn når en hendelse har skjedd. Ptil sin funksjon er å hindre at en slik hendelse skjer, og hvis den skjer er deres funksjon å få stoppet hendelsen så raskt som mulig.

Aktør B	
Informasjons område:	**Informant svar:**
Beredskapsplanlegging	B er en leverandørbedrift, når de jobber offshore jobber de på kundens installasjon. Da blir de underlagt kunden sitt beredskapssystem, varslingssystem på installasjonen. Som bedrift er de underlagt alt som kommer inn under kundens beredskaps- og varslingssystem som kommer inn under kundens førstelinje beredskap på installasjonen, og må derfor

	handle i henhold til dette. Som bedrift er de ansvarlige for andrelinje beredskapsarbeidet, det vil si alt som angår deres egen bedrift, varsling av aktuelle ledere, varsling av underleverandører og varsling av eventuelle pårørende dette gjør at de må ha systemer for å ivareta denne varslingen. Per prosjekt etableres det beredskapsplaner, som viser hvem som skal varsles i det enkelte prosjektet med kontaktpersoner. Dette er kontaktpersoner inn i deres egen bedrift og også kontaktpersoner inn mot kunden, prosjektorganisasjonen hos kunden. Når det er en hendelse offshore, som en av Bs ansatte er involvert i, vil operatørselskapet gi informasjon direkte til B, deretter blir, eller i alle fall skal B bli holdt løpende orientert om hendelsesforløpet fra operatøren. Deretter må B selv ta ansvar for videre varsling av ledere, underleverandører og pårørende. Prosjektplanene gir detaljene i forhold til hvem som skal varsles, men har også beredskapssystemet i konsernet som er hovedkontakten. Operatør sitter med telefonnummer til beredskapskontakten i konsernet, og de ringer dit ved en hendelse, deretter må henvendelsen behandles og man må se hvem som skal kontaktes i den gitte hendelsen. B er ikke involvert i planleggingen hos operatør, men de involveres i øvelser og treninger som operatør arrangerer. Når B ansatte er ute på installasjon vil det vanligvis være en evakueringsalarm for hvert skift, hvor de ansatte på installasjonen må ta på seg overlevelsesdrakten og gå ned i livbåten. Her er ikke Bs organisasjon på land involvert. Men så kan operatør kjøre større øvelser hvor de skal teste ut hele beredskapssystemet, da blir også Bs landavdeling involvert. Dette skjer i gjennomsnitt annen hvert år. F.eks for noen år siden ble de involvert i en svært omfattende beredskapsøvelse, hvor det var innleide media og pårørende som ringte og ba om informasjon hele dagen. Operatør vil ta seg av all informasjon til myndigheter, transport av skadde til land og håndteringen av selve hendelsen, mens B vil ha som ansvarsområde å varsle internt hos seg og til deres egne underleverandører, samt å holde ledere oppdatert om hva som skjer og kunne iverksette tiltak. Det er også viktig at B varsler pårørende om hva som har skjedd. Media kan også kontakte B direkte, men det er ikke Bs oppgave å informere media når det er operatør som sitter i førersetet, men de må ha et system for å kunne håndtere media, og evt. henvise de til operatørs informasjonssenter for media. Videre må B registrere hendelsen og komme med tiltak for å forhindre en liknende hendelse i fremtiden.
Rolle i beredskapssituasjonen	Under en beredskapssituasjon vil B danne sin egen andre linje beredskapsorganisasjon, dannelsen av en slik organisasjon er avhengig av hendelsens størrelse, siden beredskapsorganisasjonen blir mobilisert kun ved en større hendelse. Når Bs egne andrelinje beredskapsorganisasjon blir dannet, benyttes et eget rom for dette, dette rommet benyttes som ordinært møterom til vanlig, men her finnes det en del ekstra tavler og skap som kan låses opp hvis det har skjedd en hendelse. På dette rommet er det ikke noen særlig bruk av samhandlingsteknologi. Dette nevner informanten at er noe de kunne sett nærmere på for å anskaffe seg.
Oppdeling av beredskapsorganisasjonen	De gangene B oftest blir ringt opp av operatør er hvis det har vært en gasslekasje eller tilsvarende. Dette er et typisk eksempel på en beredskapssituasjon hvor B blir informert, men hvor operatør får situasjonen under kontroll etter hvert. I slike situasjoner er det som oftest bare den personen hos B som går beredskapsvakt som blir informert, og håndterer denne hendelsen. Den personen som går beredskapsvakt er den personen som er beredskapsleder til enhver tid og er ansvarlig for å lede en eventuell beredskapssituasjon. Ved en større hendelse varsles flere i beredskapsgruppa, dette er helt avhengig av hendelsen og er ikke definert

	på forhånd. Under slike hendelser har man forskjellige roller slik som; mediakontakt og pårørendeansvarlig, hvis man ser at det kan komme mange henvendelser til pårørendeansvarlig må man mobilisere flere personer i denne gruppa for å kunne håndtere telefoner fra de pårørende. Ved en større hendelse er det minst tre personer som må inn i denne rollen som pårørendekontakter. B har også en avtale med bedriftshelsetjenesten som ved behov kan mobiliseres inn i beredskapsgruppa, f.eks for å hjelpe personer som har fått traumer etter en hendelse. B er ansvarlig for eget personell etter at de har kommet i land, mens operatør er ansvarlig for alt personell på installasjon før de har kommet på land. B er også ansvarlig for at noen tar imot personell som kommer fra offshore på heliport og blir med personen på sykehus eller tilsvarende. Ved større beredskapshendelser, hvor mange blir sendt i land, vil operatør også ha hovedansvar for traumeoppfølging av personell, da blir B spurt om å inngå i operatørs team.
Teknologibruk mellom aktører i en beredskapssituasjon	All informasjonsoverføring mellom operatør og B foregår over telefon og e-mail. Dette gjelder også ved situasjonsoppdateringer som forgår utover i en hendelse. Det er så langt ikke tatt i bruk videomøter i beredskapssituasjoner, selv om dette er et kjent verktøy ved andre informasjonsdelings sammenhenger med operatør. I følge B er det heller ikke blitt tatt initiativ hverken fra B eller fra operatør om å benytte telefonkonferanse under en beredskapssituasjon. De blir ikke spurt så mye om hjelp under en beredskapssituasjon, men de kan bli spurt om å stille i operatørs beredskapsgruppe, hvis det for eksempel har vært en hendelse og det sendes i land en del folk til heliport, blir de gjerne spurt om å stille med ansatte fra B i denne beredskapsgruppa eller i mottaksgruppa på land, hvor man tar imot personell som er evakuerte fra offshore. Hyppighet av informasjonsutveksling har variert veldig i de ulike tilfellene. Også i øvelser har B ønsket at de kunne fått en hyppigere informasjonsoppdatering om hvordan hendelsen utvikler seg. Samhandlingsteknologi er viktig under en beredskapssituasjon, det er svært viktig å vite til enhver tid hvilken informasjon man kan gå ut med til omverden.
Mulighet for bruk av samhandlingsteknologi i beredskapssituasjon	Ved hjelp av samhandlingsteknologi kunne man i større grad fått en oppdatering om hva man kan gå ut med til omverdenen, hva innebærer de siste faktaopplysningene. Hvilke fakta kan offentliggjøres internt og hvilke momenter som er mere usikre som man kanskje ikke bør gå ut med offentlig ennå. Hvis man kunne fått en slik informasjon skriftlig ved delte data og delt skjem ville dette ha vært svært gunstig. Det er også selvfølgelig greit å se de personene man kommuniserer med, derfor hadde det vært bra om beredskapsgruppene kunne ha kommunisert via video. Dette ville vært med på å styrke følelsen av at man samarbeider. Informanten vektlegger spesielt viktigheten av å ha en klar oppdatering av siste fakta i hendelsen, det å sitte inne med rett informasjon til enhver tid. Pårørende til de ansatte hos B, vil i all hovedsak kontakte B når en hendelse er oppstått, dette øker nødvendigheten av at også Bs pårørendekontakter har en kontinuerlig oppdatering av hendelsen på lik linje med operatørs pårørendesenter.
Problemer ved bruk av samhandlingsteknologi i en beredskapssituasjon	En utfordring er å ha fasiliteter som gjør at informasjonsdelingen blir gjort på en enkel måte, og at det tekniske fungerer. Dette er ting som er vist å ikke fungere optimalt i en normal samhandlingssituasjon. Man har i slike situasjoner opplevd tilfeller hvor informasjonsdelingen ikke har gått smertefritt på grunn av problemer med oppkoblinger mot eksterne aktører osv. Dette kan være på grunn av at de som sitter og skal koble opp møter til enhver tid ikke innehar den nødvendige kompetansen på

	området. Ellers kan det være en utfordring hvis det er for mye folk som skal være med på disse møtene, informanten synes at videokonferanse er et ypperlig verktøy hvis antall deltagere på møtene er noe begrenset, dette på grunn av at hvis det blir svært mye folk kan det være en utfordring å få silt ut den riktige informasjonen, siden det kan være mange meninger og mye informasjon rundt et bord i en beredskapsgruppe. Det er derfor viktig at man også får informasjon "en til en" i en beredskapssituasjon, dette understreker viktigheten av å vite hvilke roller de enkelte har i en beredskapssituasjon slik at ikke alle får vite alt i en beredskapssituasjon. En utfordring på dette området kan være å vite hvem som skal være med på de ulike videomøtene, hvem skal ha hvilken informasjon osv. B ser en mulighet for at man kan snakke sammen på en bedre måte også internt i bedriften ved at man benytter videokonferanse, dette kan gjelde når man f.eks. skal lokalisere ansatte på et mottak ved en heliport.
Tillit	Tillit er en svært viktig faktor i en beredskapssituasjon, de har tatt det for gitt at når det ringes fra kundens beredskapssenter så gjelder dette en seriøs henvendelse. B er avhangige av at de har tillit til de som ringer til dem, ved at de opptrer ærlige og redelige, samt at de som ringer har tillit til sin leverandør om at de følger opp hendelsen, og setter i verk sin egen beredskapsorganisasjon og samtidig iverksetter et system for å følge opp hendelsen videre internt hos seg selv, og hos sine egne underleverandører. Tillit skapes i svært stor grad når de ulike aktørene har treninger sammen. Ser at i en beredskapsgruppe så er man avhengig av tillit, dvs. at man kan stole på hverandre og tørre å si ifra i selve gruppen internt også. Man befinner seg jo i en ekstremsituasjon hvis man kommer opp i en slik hendelse, og man må derfor tørre å si ifra i selve gruppen internt også, slik at man kan gi beskjed om hvordan enkeltpersoner eller gruppen kan forbedre seg i håndteringen av hendelsen, slik at hendelsen blir håndtert profesjonelt i størst mulig grad.
I hvor stor grad stoler du på tittelen/ rollen til en person, uten å vite noe om personen på forhånd?	Når man får henvendelser fra eksterne stoler man på rollen den personen som overfører informasjonen har. Når det ringer en person fra operatørs beredskapsgruppe, stoler B fullt og helt på denne personen. Internt i bedriften kvalitetssikres alle som har formelle roller i beredskapssystemet deres ved at de skal ha opplæring inne beredskap. De som er med i beredskapsgruppen skal ha en ledende stilling eller ha oversikt over hva som skjer i selskapet. Siden de ansatte som er involvert i en beredskapsgruppe skal ha denne formen for opplæring forventes det at de skal gjøre en god jobb, og resten av selskapet har tillit til at de gjør en god jobb i en beredskapssituasjon. B har også tillit til de ledere og andre som står i varslingslistene om at disse vil gjøre en god jobb. Informanten har aldri mistet tillit til noen av aktørene under en beredskapssituasjon, men bedyrer at det er ting som kunne vært gjort annerledes i enkelte situasjoner, f.eks. ved at noen flere kunne vært varslet eller at noen ekstra tiltak kunne vært utført av beredskapsgruppen.
Tillit til teknologien	Deres informasjonssystem i en beredskapssituasjon er telefonbasert.
Hvordan kan IO teknologi være med å virke proaktivt v. avvik på installasjon?	Ved bruk av IO løsninger er det lettere å dele informasjon, og få frem riktig informasjon til de personene som skal ha informasjonen. Hvis man ikke bare har ting muntlig, men også skriftlig og/ eller visuelt er det lettere å formidle riktig informasjon.
Hva bør gjøres for å forbedre dagens beredskapsarbeid	Hos B selv, mener de at bruk av ny teknologi kunne vært nyttig for å forbedre dagens beredskapsarbeid. De kan kjøre flere interne øvelser slik at de kan brife flere deltakere i beredskapsgruppa både gamle og nye om ulike scenarioer. B har allerede planlagt flere samlinger i beredskapsgruppen hvor de får inn eksterne personer for å fortelle om deres egne erfaringer i en beredskapshendelse. B har vært heldig og vært

	forskånet mot alvorlige hendelser hvor de har fått brynt seg, derfor for å få en påminnelse skal de ta inn noen andre firma som dessverre har fått prøvd ut sitt beredskapssystem i praksis, slik at de kan fortelle B litt mere om hvordan en aktuell beredskapshendelse foregår, hvilke problemer som oppstår osv. Dette har B satt inn som et tiltak mot at de ansatte i beredskapsgruppen skal bli sløve i sin håndtering av en beredskapssituasjon, og gi dem en påminnelse om at alvorlige ting faktisk kan skje. Det er også viktig å ha en kontinuerlig forbedring av prosedyrene, dokumentasjonen og systemet omkring en beredskapshendelse. Man kan også ta inn teedjeparter for å foreta en revisjon av systemet som man har lagt opp, slik at man er sikker på at systemet er kvalitetssikret. Informanten kunne videre tenkt seg en bedre samhandling mellom operatør og leverandør om hvordan beredskapen skal fungere. Per i dag får de kun papirer på hvordan denne informasjonen skal foregå, dette varierer fra prosjekt til prosjekt, men som bedrift får de ikke så mye informasjon som de skulle ønsket angående samhandlingen mellom operatør og leverandør under en beredskapsituasjon.

Aktør NOFO	
Informasjons område:	**Informant svar:**
Rolle I beredskapssituasjonen	NOFO skal være det operative utøvende organ under en beredskapssituasjon for operatørene når det gjelder oljevern, dvs. oljesøl på sjøen. De har ansvaret for å få samlet sammen og tatt opp den oljen som lekker ut, og slik hindre denne oljen i å nå land. Også når oljen har nådd land er det NOFO som fortsetter å samle opp oljen. Det er ingen krav om hvor tidlig NOFO skal varsles i en beredskapssituasjon. Selv om NOFO står for oppsamling og opprydningen av et oljesøl er det operatøren som har det rettslige ansvaret for at sølet blir ryddet opp.
Aktører i en beredskapssituasjon	Alle ressursene som deltar i en oljevernaksjon vil ha NOFO som kontaktpunkt. NOFO vil selv stå i kontakt med operasjonslederen som er operatøren. NOFO er det operative verktøyet, de skaffer ressurser, de styrer ressurser og de rapporterer situasjonen til operatøren. Det er da videre operatøren som varsler om situasjonen videre til tilsynsmyndighetene, som i dette tilfellet vil være kystverket. NOFO vil som regel ikke ha noen kontakt med HRS, siden HRS hovedsaklig skal koordinere det som går på livredning, og dette skal NOFO helst ikke forstyrre. Men i den grad det er snakk om å dele på felles ressurser vil NOFO også ta kontakt med HRS og koble seg opp mot dem. Det er viktig å merke seg at HRS ressurser og deres fokus på livredning alltid vil gå foran oljevern. Derfor vil NOFO vanligvis kun ha kontakt med operatør.
Teknologibruk mellom aktører i en beredskapssituasjon	NOFO har samhandlingsrom. Utfordringen innen bruken av samhandlingsrom er å ha en teknologi som er kompatibel mellom de ulike aktørene. Det er veldig ofte at de som utarbeider samhandlingssystemer lager de eksklusive på den måten at de ikke nødvendigvis er enkle å koble opp mot andre systemer. Dette er på grunn av den beskyttelsen de enkelte systemene har mot hverandre, f.eks. kan forsvaret ha krav til at deres system ikke skal være synlig for andre, politiet har de samme kravene for sitt system, helsevesenet har også beskyttelse på en del av systemene som de har, og dette medfører at systemene ofte ikke kan snakke sammen. En av utfordringene som NOFO nå arbeider med er å lage felles plattformer og standarder som gjør at de ulike systemene kan snakke med hverandre. F.eks. kan NOFO snakke enkelt og greit med HRS siden disse to selskapene har felles

	plattform. De har på samme måte et samarbeid med Kystverket, slik at når Kystverket nå skal bygge opp et slikt system vil de også bygge opp dette systemet på samme grunnlagsplattform som hos NOFO og HRS, NOFO har et mål om at de aktørene som deltar i et oljevern enten det er private eller offentlige skal bygge sin samhandlingsteknologi på den samme plattformen. Den formen for teknologi som benyttes under en beredskapssituasjon er både telefon, logg og e-mail. Når NOFO snakker med operatøren har de en automatisk overføring av situasjonsbildet og data ved at et fly flyr over et oljesøl og tar bilde av sølet ved hjelp av et vanlig kamera eller IR kamera, videre kan denne informasjonen sendes automatisk ned til de fartøyene som er med på denne operasjonen. Dermed sitter både fly og fartøyene med den samme informasjonen. Denne informasjonen kan også overføres til de som sitter på land. Denne informasjonen kan være i form av IR kamera, kartplott eller lignende informasjonskilder. NOFO har tilgang til loggen hos operatør, samt at også operatør har tilgang til loggen hos NOFO, slik at operatøren kan se hva de holder på med. Operatør kan også logge seg inn i NOFOs system og kan på denne måten skrive inn meldinger i deres logg også.
Viktigste faktor for godt samarbeid	Den viktigste faktoren for et godt samarbeid er at man har en god plan i bunnen som det er en felles forståelse for, her inngår rolleavklaringer mellom de ulike aktørene som en viktig faktor. Videre er det helt essensielt at for å kunne drive en bra beredskapsorganisasjon er man nødt til å trene på ulike beredskapssituasjoner. Denne øvingen er viktig både for å lære seg å kjenne sin egen rolle, for å teste om beredskapsplanen er god nok og tilstrekkelig for å løse oppgaven og for å se om folk kjenner planen godt nok
Informasjonsstrøm under beredskapssituasjon	Informasjonsstrømmen under en beredskapssituasjon oppfattes som voldsom. Sorteringen av loggen kan den enkelte variere selv i stor grad. De kan skille på hvilken type melding som skal vises, hastegrad av meldingen og området denne meldingen gjelder for slik at alle rollene i NOFOs operasjonsledelse kan velge om de vil ha alt opp på skjermen, eller om de vil ha kun det som er adressert til dem selv eller bare utestående oppgaver, eller oppgaver av en viss alvorlighetsgrad. Det som er viktig under en beredskapssituasjon er at beredskapsleder klarer å sette de riktige fokusområder slik at men vet hvilken informasjon man skal lete etter, dvs. "hva er fokusområdet nå, hva skal vi jobbe med nå?" og formidle dette videre til operasjonsledelsen, på dette nivået er det ledelsen i beredskapsarbeidet som har en svært viktig oppgave. Ledelsen må kjenne litt på situasjonen og peke på hvilke punkter det er viktig å fokusere på i beredskapssituasjonen. f.eks. i oppstartsfasen er det viktigste å forsterke grunnlagsdataene og mobilisere ressursene. Dette vil si at det er dette personalet skal arbeide med, da skal miljøavdelingen sette seg ned og beregne drivbaneberegninger, vurdere oljen, hvilken type olje det er og hvordan denne oljen vil oppføre seg på sjøen og i grove trekk kartlegge områder som kan være truet av dette oljesølet. Mens de som sitter på logistikk skal sørge for å få ut ressursene, få klargjort fartøyer, lenser, overvåkningssystemer, miljøeksperter, miljøteam som skal ut og undersøke området. Logistikks oppgave er å få dette til å fungere. I en slik situasjon er det viktig at alt personell fokuserer på de fokusområdene som er satt på forhånd. Det man ofte ser i en dårlig beredskapsorganisasjon er at det ikke er fokus, det er ikke en god nok styring av organisasjonen.
Mulighet for bruk av samhandlingsteknologi i beredskapssituasjon	Muligheten for bruk av samhandlingsteknologi i en beredskapssituasjon er svært avhengig av kompleksitetsgraden i aksjonen. Denne teknologien skal være med på å sortere informasjonen din, og man skal være sikker på

	at denne informasjonen gir et riktig bilde av situasjonen. Desto mere kompleks en situasjon er, desto mere avhengig vil man være av et system som sorterer informasjonen. Hvis man også tenker på beslutningsstøttesystemer, varierer graden av nyttighet av slike systemer, ved at noen systemer låser deg til en mal, slik at du blir ledet gjennom denne malen gjennom en sjekkliste, hvor du krysser deg gjennom operasjonen ved hjelp av denne sjekklisten. Mens andre systemer en mye mere åpne ved at du har mere oppgavestyring og tips, og ikke en slik sjekkliste. Hvilken form for beslutningsstøttesystem som benyttes er avhengig av hvilken organisasjon som man går inn i.
Problemer ved bruk av samhandlingsteknologi i beredskapssituasjon	Problemer ved bruk av samhandlingsteknologi kan bestå i det at systemet er svært låst i håndteringsformen, dvs. at man blir ført inn på feil spor av systemet. For eksempel kan systemet være bygd opp slik at for at man skal få tilgang til en funksjon, så må man utføre visse oppgaver. I et slikt tilfelle står man i en situasjon hvor det er systemet som forteller deg hvordan du skal jobbe, på denne måten kan verdifull tid bli kastet bort på grunn av systemets tungrodde funksjoner. Slike systemer eksisterer det mange av. Man har også et problem ved et system hvis personell ikke kjenner systemet, da blir kampen mot dataprogrammet og knottene viktigere enn fokuset på hovedproblemet ute i felt. Et annet problem er avhengighetsskapning, hvis man får et strømutfall så sitter man der, uten å kunne gjøre noe. En stor utfordring er hvis en operasjonsleder i femteledd gir en ordre/ policy/ focus hvordan sikre seg at den personen som står på stranden med spaden faktisk får med seg dette? Hvordan man kan sørge for at meldinger som går gjennom mange ledd ikke blir forringet i løpet av "transportetappen" er en svært stor utfordring. Denne formen for kommunikasjonsproblem / tap av informasjon er også gjeldende når beskjeder skal sendes fra personen på stranden til de øvrige kontorene.
Ny teknologi medført at det er blitt en forskjell i aktørbildet nå i fht. Tidligere	Nei, det har det ikke.
Nye mønster i fht. Hvordan de ulike aktørene snakker sammen	Når man snakker om samhandlingsteknologi, snakker man om beslutningsstøtte og tekniske systemer, i denne forstand vil man si at man snakker sammen på en tryggere måte. Når begge parter sitter med det samme situasjonsbildet foran seg, så er det dette bildet man diskuterer. Det som ofte var problemet tidligere var at dersom man satt på to ulike lokalisasjoner, så satt man i to ulike verdener og hadde ikke muligheten til å se på det samme bildet. En som sitter ute i felt vil ha et helt annet situasjonsbilde enn en person som sitter inne i stab. Hvis disse to personene da sitter og ser på den samme situasjonsoversikten så vil disse personene i utgangspunktet ha en mye større grad av mulighet for samhandling enn hvis de ikke hadde den samme situasjonsoversikten. Da ser den personen som sitter ute i felten om informasjonen som de på kontoret sitter med er riktig, f.eks. om et fartøy som er tegnet inn på kartet er tilstedet eller ikke. Man kan unngå mange feilvurderinger og man kan unngå mye feilkommunikasjon hvis man har det samme utgangspunktet.
Tillit	Tillit er svært viktig i en beredskapssituasjon. Hvis man ikke har tillit til at den personen som er ute på sjøen gjør det han skal, vil de som sitter på land bli fryktelig overstyrende. Det er heller ikke sikkert at den som sitter på land vet i like stor grad som den som er ute på sjøen hva som er den beste løsningen i enhver situasjon. Desto mere tillit du har til de personene som er ute på sjøen, desto mere ansvar kan du overlate til dem,

	og du kan heller bruke ditt eget hode til å tenke ut løsninger på andre problemer i stedet for å sitte å følge opp de vedkommende som er ute på sjøen. Den personen som mottar en ordre ute, må ha tillit til vedkommende som sitter inne, siden den som er ute i felt kan synes at ordren er helt feil, dette kan komme av to årsaker, enten er ordren helt feil eller så må de som er ute på sjøen ha en så stor grad av tillit til personene som sitter inne at de stoler på at de vet hva som er den beste løsningen, eller så har de en så god tillit og samhandling til de personene som sitter på land at de som er ute på sjøen kan ringe til dem og si at "sett i fra mitt ståsted er dette helt feil" og få en ny vurdering av hva som må gjøres. Tillit skapes i stor grad ved trening, samhandling og fellesskap i "fredstid". Når man trener sammen så ser de ulike partene at denne samhandlingen virker. Det vil si at de som sitter i de ulike stabene og koordinerer det hele de ser at fartøyene, flyene, personalet osv. de utfører sine oppgaver på en god måte. Dette virker også motsatt ved at de som befinner seg ute på sjøen ser at de er en del av en større plan og at denne planen virker i praksis. Dette medfører at problemet blir løst ved samhandling. Den sosiale biten er også viktig, ved at man møtes under evalueringer, ved festlige sammenkomster etter øvelsen, eller at man tar en kopp kaffe sammen på kontoret eller på brua etter at man har hatt en trening, og bygger på denne måten tillit mellom de ulike partene som deltar i en beredskapsituasjon.
I hvor stor grad stoler du på tittelen/ rollen til en person, uten å vite noe om personen på forhånd?	Dette kommer an på hvilket system man er i. Snakker man med kapteinen på en båt, så snakker man med sjefen og man vet at denne personen har et sett med verktøy for å kunne styre denne båten. Snakker du med personer fra tilfeldige organisasjoner som du ikke kjenner så godt, kan det komme en person fra et privat selskap som kaller seg for aksjonsleder eller skadestedsleder eller lignende. Du vet ikke helt hva dette innebærer, hva vil disse rollene bety. Nå er det akkurat blitt dannet et felles system for NOFO, kystverket og DSB for en helhetlig utdanning. Det vil si at hvis du skal inneha en tittel, så er det et enhetlig kravsetting om hva dette skal innebære. Da vet man hva den enkelte skal ha vært igjennom for å kunne påropе seg sin stillingstittel. Dette blir gjort for å kunne møte en situasjon hvor personene som innehar en tittel har den samme grunnopplæringen. Informanten har mange ganger opplevd å miste tilliten til en aktør under en beredskapssituasjon. Men dette tapet av tillit går i større grad på enkeltpersoner enn det går på organisasjoner. I NOFO har de faste øvelser og verifikasjoner med deres faste enheter (fartøy, fly osv.). Hvis man kjører en verifikasjonsøvelse med et fartøy og de ikke håndterer denne øvelsen på en tilstrekkelig god måte, dannes det øyeblikkelig en misstillit til organisasjonen, eller den skipperen som leder fartøyet. Dette er en form for formell mistillit. Gjennom sin erfaring med beredskap har informanten opplevd at man kan oppfatte en organisasjon eller person som solid, men at det ofte viser seg å ikke stemme, når ting settes under press. Når man er oppe i en beredskapssituasjon og trenger hjelp fra aktører, går man gjennom en database hvor man ser hva det står at disse aktørene skal kunne, man kan da ringe til disse aktørene og stille kontrollspørsmål for å sjekke om de virkelig kan det som det står at de skal kunne. Det er viktig å vektlegge den forskjellen man har i forventningsnivå hos de ulike organisasjonene. Hvis du ringer de offentlige apparatene, slik som politiet, HRS, forsvaret og kystverket, så har du en forventning om at disse skal håndtere henvendelsen på en skikkelig og redelig måte. Disse har som regel et veldig forutsigbart og enhetlig handlingsmønster. Dette gjelder også de frivillige organisasjonen, disse er også svært drillet og organiserte i en slik

	situasjon, men man kan her også oppleve svært store lokale variasjoner mellom de enkelte korpsene. Dette gjelder f.eks. Røde kors, folkehjelpen og redningsselskapet. Et supplyfartøy i Nordsjøen er underlagt helt andre regimer og regler når det gjelder HMS enn for eksempel et fiskefartøy eller fartøy ellers. Informanten vil også ha forskjellige forventninger til en gasstanker og til en som frakter sand. Dette på grunn av at en gasstanker vet du er vant til å jobbe innenfor sikkerhetsregimer og HMS regler osv, mens hos en som frakter sand er det ikke nødvendigvis like streng oppfølging av regimer, siden denne lasten ikke har en like stor risiko som gass.
Tillit til teknologien	Lite tillit til teknologien som benyttes i en beredskapssituasjon. Grunnlaget for dette er at denne teknologien svikter hele veien. Man kan rett og slett ikke ha tillit til teknologien, man er nødt til å legge opp til at teknologien ikke virker. Et eksempel er at hvis du har en ulykke, så vet du at mobilnettet sannsynligvis vil krasje. Fordi hvis du er i et litt grisgrendt strøk, så er ikke kapasiteten i telenettet tilstrekkelig til å håndtere situasjonen. Dette er noe man må gå ut i fra, og da må du forsterke opp denne teknologien. Men på den annen side har informanten tillit til teknologien hvis man bygger den opp og sørger for at den virker, så virker denne teknologien stort sett, men man er nødt til å vite at teknologien kan bryte sammen på grunn av at man er i en unormal situasjon. For å sikre at informasjonen kommer frem i en beredskapssituasjon legger man inn sjekkpunkter i en samtale for å sikre at den du snakker med virkelig skjønner hva det er snakk om. F.eks. "Gi beskjed når du er fremme, gi respons kl. 12, osv". Det å legge inn slike sikringer, går egentlig en del på din egen arbeidssituasjon også, siden du delegerer bort en del ansvar til andre personer. Men hvor hyppig en slik bruk av sikringer er, vil være avhengig av erfaringsnivå hos den enkelte.
Hvordan kan IO teknologi være med å virke proaktivt v. avvik på installasjon?	IO teknologi kan være med på å virke proaktivt i en slik situasjon, men da er det svært viktig at mennesket i relasjonen ""man-machine" vet hva de holder på med. Siden systemene i utgangspunktet ikke kan gi deg beskjed om at noe er galt. Derfor er det svært viktig at den menneskelige biten i dette skjønner hva det er som foregår i systemet, og er på høyden med hva som skjer, uten dette kan man aldri bli proaktiv. I enkle former per i dag kan du få en del "warnings", slik at du blir proaktiv. Du kan legge inn en del "heads up" funksjoner i systemene som gjør at man får beskjed om at man er på vei til å bryte barrierer som er lagt i systemet. Men disse "Heads up" funksjonene går på svært enkle forutsetninger. Mens de lange og viktige linjene vil ikke slike funksjoner kunne ta seg av. Noe som er viktig å få frem er at noen systemer ved IO konsepter er svært detaljerte, med sjekklister osv. Da blir du brakt gjennom en situasjons forskjellige faser på den måten systemet presenterer det for deg, og ved at du krysser ut sjekklista, dvs. at du sjekker ut hva som skal gjøres i den og den fasen. Dette er den ene siden, og denne siden med bruk av IO teknologi kan bli svært ekstrem. Mens den andre siden for bruk av IO teknologi er den siden som informanten pleier å kalle for "Clint Eastwood metoden". Denne metoden baserer seg på metodologien "adapt, improvise, overcome", det vil si at det ikke er noen løsningsplan, men man løser problemene når de dukker opp. Informantens problemløsningsstil vipper over i retningen av "Clint Eastwood metoden", fordi han kan sin profesjon svært godt. Men hvis man går inn i en organisasjon som ikke arbeider med beredskap, og man skal bygge opp en beredskapsorganisasjon, må dette systemet ha en større grad av tips og styring gjennom, enn systemet hos en person som arbeider med beredskap til daglig. Dette vil i praksis si at man må ha et helt annen form

	for styring av organisasjonen hos aktører som politi, HRS eller kystverket enn det det er hos en operatør som har et oljeutslipp "hvert 30 år". Derfor vil det som er riktig teknologi bruk for en person i en etat som arbeider hyppig med beredskap, være en annen enn for en person som sjelden driver med et slikt arbeid. For informanten er bruken av IO konsepter viktigst i den grad at teknologien kan benyttes til å gi et riktig situasjonsbilde over hendelsen, som opplyser de riktige faktorene omkring hendelsen. Informanten føler seg ikke trygg nok på teknologien til at den skal kunne ta beslutninger for en person under en hendelse, som han sier selv, "desto nærmere systemet er i å simulere og skulle ta avgjørelser for en, desto mere vondt i magen får jeg".
Andre måter for å skape proaktivitet innen beredskap	Treninger og øvelser vil være med å skape proaktivitet ved siden av bruk av IO konsepter. Siden gjennom trening og øvelse får du fokus på fagområdet, slik at man er i stand til å tenke gjennom situasjonen på forkant. Ved hjelp av dette er du "på" allerede før saken har hendt. Poenget er at hvis du trener og øver slik at du behersker området, så vil du isteden for å "komme på hælene" og rote rundt, beherske situasjonen, siden du står ovenfor en situasjon hvor du kjenner deg igjen i, og vet hva du skal gjøre. Når du derfor har løsningen på dette første problemet i en tidlig fase kan man i stedet begynne å tenke på det neste problemet og forsøke å finne en løsning på det. På denne måten har man vært proaktiv ved å ha foretatt øvelser og treninger, slik at man på forhånd har kartlagt ulike problemområder som oppstår i en slik situasjon.
Kan vi forhindre en katastrofe lik Deepwater Horizon.	Ved omdefinering av spørsmålet til å etterspørre om man er i stand til å håndtere det sølet som følger en utblåsning lik den ved Deepwater Horizon, vil han si ja, det er de i stand til. Men det er så mange variabler og avhangighetsfaktorer, at det vil ikke være noe problem å finne punkter og situasjoner som ville gjøre en slik operasjon svært svært vanskelig og som vil øke muligheten for at dette ikke går bra ganske kraftig. Men hvis man ser på en normal utblåsning, med normalt vær og en normal tilnærming så vil de takle en slik hendelse. En faktor som kan forringe en slik aksjon svært kraftig er for eksempel vedvarende sludd. Siden svært mange elektroniske systemer blir kraftig redusert ved slike værforhold. For eksempel vil kommunikasjonssystemer og radarer slite kraftig under slike forhold. Ved svært dårlig vær vil også selve oljevernoperasjonen bli problematisk, men på den andre side vil oljen ved svært dårlig vær bli vasket ned i vannmassene og løst opp, slik at de blir tilgjengelige for naturen. Derfor vil ikke dårlig vær nødvendigvis øke graden av forurensning, men vil redusere hvor stor grad av olje man får til å ta med seg inn til land.

Aktør C	
Informasjons område:	**Informant svar:**
Rolle I beredskapssituasjonen	C får tilsendt en del informasjon omkring den innretningen som de ser på av kunden. Kunden har gjerne med eksisterende analyser, eksisterende beredskapsplaner osv. Deretter ser C på hvilken form for beredskap de har i forhold til hvordan regelverkskravene er, samt hvordan beste praksis er i industrien. Deretter kommer C under et oppstartsmøte om hvilke endringer de ser for seg umiddelbart. C ser blant annet på hvilke DFUer de har, om kunden har for mange, for få, eller om det er noen som ikke er dekket. Ser også på ytelseskravene som kunden har til sin beredskap, dette er noe C tar for seg i en svært tidlig fase. Under en del av prosjektene utfører de også offshore befaringer, hvor de får snakket med de som arbeider offshore, og hørt om hvordan de praktiserer sitt

	beredskapsarbeid. Her menes hvor store beredskapslag de har, hvilke beredskapsfunksjoner de innehar på installasjonen. Det blir her også undersøkt dimensjonene av beredskapsfunksjonene, er det for mange personer som er involvert er det for få osv. Ser ofte på muligheten for å redusere antall personer i beredskapsorganisasjonen, det er jo ikke nødvendig at flere enn det som er nødvendig bli eksponert hvis man har en hendelse. Videre undersøker C om kunden har områdeberedskap og hvilke eksterne ressurser de har tilgang til. Det er gitt en del slike krav i NORSOK Z-013 og annet regelverk omkring hvilke DFUer og ytelseskrav de er forventet å kunne ivareta. Videre kommer C med anbefalinger omkring hva de ser at kunden kan bli bedre på. C kan også lage en kundes beredskapsplaner helt fra grunnen av, dette er noe som varierer mye fra kunde til kunde. Noen kunder ønsker å gjøre det selv, og får derfor C til å gjøre beredskapsanalysen, mens de ønsker å lage beredskapsplanene på egen hånd. C kan også være med i en arbeidsgruppe som kunden nedsetter for å lage beredskapsplanen, dette for å hjelpe dem med å lage en best mulig plan. Det har skjedd en del endringer spesielt layoutmessig, på beredskapsplanene, slik at de har blitt mye mere brukervennlig i de senere årene, det er en del innretninger som har en del gamle og ikke så brukervennlige beredskapsplaner, På dette området kan C hjelpe kunden med å få mere brukervennlige beredskapsplaner. C er kun med på å etablere en beredskapsorganisasjon. I det de sender fra seg planen så ser de ikke noe mer til beredskapsarbeidet i bedriften. Da får ikke C noe mere informasjon enn det som kommer frem gjennom media.
Hvordan tas det hensyn til ulike aktører i analyse/ planleggingsfase, hvordan identifiseres de?	Kartlegging av de ulike aktørene i en beredskapssituasjon foregår oftest gjennom kunden selv, slik at C foretar ikke i så stor grad en kartlegging av ulike aktører unntatt de som står nevnt i lovverket og de som kunden selv nevner. C lager ofte en varslingsmatrise for den enkelte kunde, dvs. et oppsett hvor det står beskrevet hvilke aktører man skal varsle for den enkelte DFUen. Da prøver man å få det til slik at førstelinje varsler færrest mulig, og at det heller er slik at det er andrelinje som sitter på land som varsler de ulike aktørene.
Teknologibruk mellom aktører i en beredskapssituasjon	Den største andelen av kommunikasjon mellom de ulike aktørene foregår via telefon. Internt på installasjonen benyttes radio. Det har vært arbeidet en del med å benytte færrest mulig kanaler, slik at det blir færrest mulig kanaler å holde styr på. Informasjonsflyten fra første linje til andre linje foregår hovedsaklig over telefon som benytter fiberforbindelse, med mobiltelefon som back-up løsning. Videre benyttes det også IP telefoner.
Hvordan kan IO teknologi være med å virke proaktivt v. avvik på installasjon?	Antar at kontrollrom funksjonen ligger på land. På de installasjonene som informanten har vært på har kontrollrommet og beredskapsledelsen befunnet seg like i nærheten av hverandre. Dette har vært svært godt likt av personalet siden kontrollrommet hele tiden får med seg hva som skjer på installasjonen, og da følte de som inneholdt beredskapsstillinger at det å være så nær kontrollrommet medvirket til at kommunikasjonslinjene ble korte og effektive. Et problem kan her være at hvis kontrollrommet plasseres på land, vil kommunikasjonslinjene mellom beredskapspersonalet offshore og kontrollrommet på land bli lengre, dette kan muligens bli et problem ved at du har distansert deg fra de som har kontroll over prosessen ved at disse personene sitter på land, da kan kommunikasjonen mellom disse bli en del tyngre. Informanten ser for seg at kontrollrommet og de beredskapsansvarlige vil fortsette med å ha den tette kommunikasjonen som de har i dag ved at de i stor grad benytter videokonferanse i sin samhandling.
Kan vi forhindre en	Tror ikke det er beredskapen i seg selv som kan forhindre at en hendelse

katastrofe lik Deepwater Horizon.	blir så stor, her er det heller alt som gjøres før en hendelse som er det viktige. Dette omfavner alt fra rutiner, kontroll og prosedyrer. På den norske kontinentalsokkelen har det vært en del hendelser i det siste som har omfattet arbeidsområder både innen brønnoperasjoner og i selve prosessen. Beredskapsarbeidet trer i kraft etter at hendelsen inntreffer, men det er en grunn til at denne hendelsen i det hele tatt inntreffer, man må heller se på de bakenforliggende faktorene som gjør at noe får lov til å inntreffe. Informanten tror at beredskapsarbeidet og beredskapsledelsen slik som den er i dag fungerer forholdsvis godt ute på innretningene. Informanten vektlegger at både de som sitter i kontrollrom og de som arbeider innen beredskapsledelsen er svært rutinerte og drillet, det er flinke personer som innehar disse stillingene. Når C diskuterer beredskapssituasjoner med beredskapsledelse og kontrollrom ansatte er de svært klare på hvilke handlingsmønster som må igangsettes. Derfor vil ikke C si at det er disse aktørene som må drilles innen beredskap i en større grad, det er viktigere å se på de bakenforliggende årsakene slik at disse hendelsene ikke vil kunne inntreffe på vår sokkel.

Aktør D	
Informasjons område:	**Informant svar:**
Beredskapsplanlegging	D er med på beredskapsplanleggingen, de har et samarbeidsforum for de ulike medlemsbedriftene. I dette samarbeidsforumet deler de planene seg i mellom og forsøker å lage planer som ser forholdsvis like ut mellom de ulike aktørene. D er med på å skrive brodokumentene for å knytte ressursene og organiseringen opp mot hver brønn og opp mot det selskapet som skal operere brønnen.
Rolle i beredskapssituasjon	D håndterer andre linje for operatørene. I staben hos D sitter det et fast beredskapslag som innehar roller som: Beredskapsleder, stabsleder, mediakoordinator, logistikkoordinator, personellkoordinator og myndighetskoordinator. Disse rollene innehar personell som skal være på plass i beredskapsrommet innen en time. D har også en støtteorganisasjon rundt seg utover disse rollene, de har et pårørende telefonsvarersenter, mottakssenter for de evakuerte og mottakssenter for pårørende. Slik at organisasjonen utvider seg etterhvert som en hendelse øker i omfang. Når det gjelder boretekniske problemstillinger stiller den enkelte operatør opp med sine egne well incident teams, og støtter D. Her benytter D en noe annen samhandlingsform enn andre aktører, men de har fått gode tilbakemeldinger på den måten dette gjøres på av de andre i bransjen. Man kan kjøre denne kommunikasjonen over videokonferanse, eller de enkelte well incident teams kan komme fysisk til D, for å sitte sammen i samme rom. Noen operatører sender også ut en liaison, for å sitte hos D under en hendelse, dette kan være til god hjelp under en hendelse. Hvordan denne koblingen mellom operatørene og D fungerer er opp til den enkelte operatør å bestemme seg for. Under en beredskapssituasjon er det alltid operatøren som har ansvaret, men de har gitt D en fullmakt til å handle på et fritt økonomisk grunnlag samt at D skal foreta all varsling av myndigheter og andre instanser som skal varsles. Normalt i en beredskapssituasjon vil riggen ringe til D, og informere om situasjonen. Når det blir slått alarm ombord, så får D beskjed samtidig. Dette gjør at D blir involvert i en hendelse på et svært tidlig tidspunkt. Etter D har blitt varslet om situasjonen fra riggen vil hele beredskapslaget bli varslet / kalt inn. Deretter vil HRS bli varslet for å sikre at de sitter med den samme situasjonsforståelsen som D, og for å varsle om at D igangsetter sine tiltak, slik at det ikke er noen tvil om

	hvem som styrer og gjør hva. Deretter varsles operatøren i tredje linje, slik at han er klar over at han har en hendelse og kan komme i gang med sin organisasjon. Videre vil det gå fortløpende varslinger til Ptil, riggeier osv. omkring hvordan situasjonen videreutvikler seg. Tredjelinje beredskap består av eiere og partnere, disse har fokus på den strategiske biten. Mens D gjør den praktiske biten opp mot støtte og myndigheter rundt hendelsen. Hvis f.eks. Ptil ønsker å snakke med toppledelsen i en bedrift, så gjør de bare det, det er ingen krav om at de må snakke med D. D gir ingen informasjon til media. De har en mediakoordinator som sitter i rommet, denne personen henter ut informasjon som er verifisert. Denne verifiserte informasjonen sendes hele tiden videre til tredje linje, slik at de har en kontinuerlig oppdatering av verifisert informasjon. Dette medfører at all informasjon som skal ut til media skjer gjennom tredjelinje beredskap. D har også informert media omkring hva de gjør under en beredskapssituasjon, slik at det ikke oppstår noen forvirring omkring dette under en eventuell hendelse.
Oppdeling av beredskapsorganisasjonen	De ulike medlemmene i D samarbeider relativt tett. Dersom det kommer en ny operatør som skal etablere seg på norsk sokkel, tar denne operatøren kontakt med en av de andre aktørene som har erfaring, og får på denne måten en erfaringsutveksling. D har også laget et eierforum hvor de samarbeider omkring planverk, slik at den planen som kjøres i andre linje er lik for alle. Medlemmene tar i tillegg erfaringer fra øvelser og diskuterer seg gjennom dette i forumet, for å kartlegge hva som gikk bra og hva som gikk dårlig. Man tar altså erfaringer fra øvelser og hendelser og deler denne informasjonen. De ulike støttegruppene i en organisasjon er det installasjonen som tar kontakt med. For eksempel er støttegruppen innen boring kontinuerlig på vakt, de er med på en hendelse fra det første tegn på at noe kan gå galt til det er blitt utviklet en beredskapssituasjon. De er inne i bildet svært tidlig som en ren arbeidsprosess, denne funksjonen har de hver dag. Hvis situasjonen utvikler seg, så slutter ikke disse støttegruppene å jobbe for å forflytte seg til Ds lokaler, men de arbeider fra hvor de er lokalisert. D har da kontakt med denne støttegruppen enten over telefon eller videokonferanse. Grunnen til at de gjør det slik er at hvis du sitter i et miljø hvor du har all mulig data, og nok oversikt slik at man får et best mulig situasjonsbilde er det bedre at man sitter å gjør jobben der enn at man skal på død og liv være fysisk tilstede på andrelinje beredskapssentral. Dette oppnår D ved at de har direkte kontakt med støttegrupper (f.eks. støttegruppen for brønn og boring). D har da en dialog direkte med støttegruppen og med installasjonen slik at man får en lik situasjonsforståelse i støtte teamet som den som eksisterer i brønn og boring ute på riggen. Informasjonsutvekslingen mellom andrelinje og institusjoner som Ptil og HRS foregår via telefon. Når det gjelder ressurser slik som beredskapsfartøy osv. er det operatør som må dokumentere at de har slike ressurser før de får lov til å operere. Det vil si at D kun bruker ressursene som operatøren stiller til rådighet.
Teknologibruk mellom aktører i en beredskapssituasjon	Mot første linje benyttes telefon, det er mulighet til å kjøre videokonferanse mot noen rigger, men i all hovedsak foregår denne kommunikasjonen ved hjelp av telefon. Det er lite bruk av IO konsepter mot de riggene som de er i kontakt med så langt. Når det gjelder kommunikasjonen mot tredjelinje går dette på telefon og video, samt at de har et informasjonssystem som utveksler informasjon, logger, ved at all data som legges inn i andrelinje også er synlig i tredjelinje. Andrelinje velger ut den informasjonen som er viktigst, slik at tredjelinje får et "vasket" bilde av hva det er som foregår, det vil si at andre linje sorterer

	ut den informasjonen de mener er relevant for tredjelinje. Andrelinje skjuler ingenting for tredjelinje, tredjelinje har muligheten til å lese hele loggen om de ønsker det. Når tredjelinje er flink til å få med seg det vaskede bildet av situasjonen, går telefonkontakten mye raskere, siden begge parter da sitter med den samme situasjonsforståelsen. Informasjonssystemet som benyttes under en hendelse er CIM. Når man får rapportert om en hendelse, hvor man er usikker på utfallet over tid, blir det etablert en hendelse i CIM. CIM benyttes kun mellom andre og tredjelinje. I førstelinje benyttes stort sett whiteboard tavler. For å bevare denne informasjonen blir det tatt bilder av disse tavlene, ellers kan det også hende at denne informasjonen går tapt ved at det foregår et gjenbruk av disse tavlene. Dette er med på å svekke graden av historikk som er mulig å oppnå ved hjelp av disse tavlene. Men det varierer i stor grad fra installasjon til installasjon med hvilke rutiner de har ombord for denne situasjonshåndteringen. Alle tredjelinjene som er medlem av D benytter CIM, de har alle en opplæring på dette slik at de er kompetente til å bruke CIM. D har to forskjellige typer medlemmer, de som er operatører og de som driver leting. Hvis du driver med leting, så kjøres det trening foran hver brønn som skal bores. Denne treningen inkluderer det å bli kjent med brønnen, hvilke utfordringer som er koblet til denne brønnen osv. Deretter blir beredskapssystemene gjennomgått av D sammen med operatøren og det blir foretatt en øvelse opp mot hver brønn. Mens operatørselskaper, for eksempel et som ble medlem i november kjører nå i disse dager runde to av sitt treningsopplegg, de utfører treninger kvartalsvis. Etter treninger med CIM vurderes innhold i meldinger, situasjonsforståelsen som oppnås med CIM, hva som kan forbedres og hva som er bra med dette verktøyet. Under en beredskapssituasjon er det ikke en fast bestemmelse om at det skal være en person med inngående kunnskap omkring installasjonen som skal sitte i andre linje, dette er noe som operatøren og D bestemmer underveis i situasjonen.
Viktigste faktor for godt samarbeid	Her er det mange viktige faktorer. Man må for eksempel ha tillit til at den personen som håndterer hendelsen hos D har den kunnskap, trening og myndighet som er nødvendig for å gjøre dette. Man oppnår jo tillit gjennom samtrening og ved at man viser at man kan gjøre jobben, slik at det er en nær sammenheng mellom faktorene.
Informasjonsstrøm under en beredskapssituasjon	Informasjonsstrømmen under en beredskapssituasjon fungerer veldig bra. Hvis man tenker på informasjonsstrømmen mellom første og andrelinje beredskap i de øvelsene man har hatt og de resultatene som er oppnådd, har man her en god kommunikasjonsstrøm. Videre er også kommunikasjonen mellom andrelinjeberedskap og operatørs støttegrupper svært god, ved at det her foregår en kontinuerlig oppdatering omkring status, ved hjelp av videokonferanse eller telefon. Dette medfører at de ulike partene oppnår å se det samme situasjonsbildet til enhver tid. Denne informasjonsoverføringen kan ses på som en integrert operasjon, ved at man ikke er nødt til å flytte støttegruppen, men man må flytte informasjonen for å kunne opprettholde et godt og samkjørt situasjonsbilde. Møtene mellom andrelinje og de andre involverte i en beredskapshendelse foregår ca. hvert 20 til 30 minutt, da vil de involverte enten være fysisk til stedet eller være tilstedet ved hjelp av videokonferanse/ telefon. Informasjonen som kommer inn til andrelinje under en beredskapssituasjon kommer opp på forskjellige tavler som omhandler ressurssituasjonen, personellsituasjon, hvilke oppgaver som er tildelt hvem. Det er altså ulike tavler som viser hva som skjer på de ulike områdene til enhver tid. Det finnes også egne tavler til media og pårørendesenter hvor man kan se hvilken informasjon som

	sendes ut til de ulike pårørende, samt hvilken informasjon som media får til enhver tid.
Mulighet for bruk av samhandlingsteknologi i beredskapssituasjon	Samhandlingsteknologi forenkler samhandlingen enormt hvis alle parter sitter med det samme situasjonsbildet når de skal løse en hendelse. Hvis tredjelinje ser hva andrelinje opererer med er det lettere for dem å forstå situasjonen på lik måte som andrelinje. Grunnen til at bruken av samhandlingsteknologi har kommet så mye kortere sett i en beredskapssammenheng enn det har ellers i andre deler av petroleumsbransjen er at man under en beredskapssituasjon ikke kan være hundre prosent sikker på at teknologien er oppe og går, derfor kan man ikke være sikker på at teknologien fungerer, det kan hende at man må forholde seg til en satellitt telefon og den informasjonen man har på tavler og på papir. Ut i fra dette vil D si at tryggheten omkring muligheten for at IKT og samhandlingsverktøyene er oppe og går under en beredskapssituasjon er svært usikker, og at dette kan være noe av grunnen til at man ikke i større grad har tatt i bruk denne formen for teknologi.
Problemer ved bruk av samhandlingsteknologi i beredskapssituasjon	Man har et kontinuerlig forbedringspotensiale innen bruken av samhandlingsteknologi. Det ene er å forbedre hvordan man presenterer informasjonen rundt seg og internt, det er en fortløpende prosess. D synes informasjonsstrømmen går bra, men det finnes alltid et forbedringspotensiale. Hovedfokus under hver øvelse er å sikre at informasjonsstrømmen mellom første- andre og andre-tredje linje fungerer som forutsatt, av og til gjør den det, mens av og til gjør den ikke det. Det er viktig å ikke bli så avhengig av samhandlingsteknologi at man ikke kan samarbeide når denne teknologien ikke virker. Det er viktig at man har god videokonferanse og samhandling med første linje, men når man har en situasjon der ute, kan systemet bryte sammen og da må du være trent på å håndtere situasjonen uten denne teknologien. Det samme gjelder for D, de har "back up på back up", men de må samtidig være forberedt på å kunne ta frem whiteboard tavler, og på denne måten kunne håndtere en situasjon uten bruk av teknologi også.
Tillit	D jobber svært mye med tillit. D har egne integreringsprosesser for både å bli kjent med rigg og OIMer og slik integrere disse på en god måte. D er en forholdsvis ny aktør, det å få en god kjennskap til OIM, det at OIM vet hvem D er, slik at OIM stoler på og responderer på det som de ber om er viktig, videre er de også avhengig av operatørs tillit siden de signerer fra seg en ubegrenset økonomisk fullmakt til D, hvis operatør ikke hadde hatt denne tilliten ville han ikke gjort dette, og da ville heller ikke D hatt mulighet til å operere. D bruker mye tid på en ny operatør med å samle nesten hele selskapet hos deg og presentere seg for hverandre, spise litt sammen og bli godt kjent før de i det hele tatt starter med opplæring og trening. Dette gjøres for at de ansatte hos operatøren skal forstå hvorfor de er der, samt hva de gjør. I oppstartsfasen hos D, møtte OIM med en ikke så alt for positiv holdning til å bruke tid i sin friperiode til å ha øvelser hos D. Men denne holdningen er nå helt borte, nå spør OIM om å få komme for å ha øvelser med sine egne beredskapslag som de skal ha med seg ut på riggen, de ser nytten av disse øvelsene og synes det er viktig å få lov til å være med å trene. Dette har å gjøre med tilliten som er oppnådd, og at OIM ser nytten av denne treningen som blir gjort.
I hvor stor grad stoler du på tittelen/ rollen til en person, uten å vite noe om personen på forhånd?	Beredskapsledere i første og andrelinje stoler informanten på siden D har vært med på å trene de opp, D vet hvilken kompetanse de har, hvis noen har dårlig kompetanse så er det noen som har fortalt det til D, og deretter har de trent på nytt. Siden D er bygd opp som en forening, så skal de ikke tjene penger, dvs. at dersom man ikke er fornøyd med kompetansen til

	noen, så trener man de bare på nytt. De som er i organisasjonen stoler D på, D kjenner både styrker og svakheter til disse og det blir derfor enkelt å forholde seg til dette. Når det gjelder Ptil har de også en svært god dialog med de, Ptil består av positive personer som er lette å samhandle med, det samme gjelder HRS. D har jevnlige øvelser sammen med HRS, og under disse øvelsene er det en god og positiv dialog. De rollene D samarbeider med er HRS, Ptil, NOFO alle disse organisasjonen kjenner de godt og har ingen form for misstillit til disse organisasjonene. D har også god kontakt med OIM ute på rigg og boreleder hvis OIM er opptatt med å lede en beredskapssituasjon. Man kan ikke si at man ikke har tillit til personer når man arbeider innen beredskap, hvis man ikke har tillit til noen aktører så må man etablere tillit til dem før man samarbeider med disse i en beredskapssituasjon.
Tillit til teknologien	D har ikke noen utstrakt grad av tillit til teknologien, D vil gjerne ha en "What if" tankegang. For eksempel hvis strømmen går, så har man en generator i back up, noe som vil si at man kan holde på en god stund på batteridrift, videre kan D miste telefonforbindelsen, men de har fortsatt en ekstra telefonforbindelse, D kan miste internettforbindelse, men de har allerede en ny internettforbindelse i bakhånd. Alt dette viser at D ikke har en så stor grad av tillit til teknologien, men at man alltid må ha "What if" løsninger tilgjengelige.
Hvordan kan IO teknologi være med å virke proaktivt v. avvik på installasjon?	I dag finnes det teknologi som gjør at man kan se hva som foregår på en installasjon til enhver tid, men problemet er at de som arbeider offshore ikke ønsker å ha denne formen for kontinuerlig overvåkning. Ved en slik kontinuerlig overvåkning vil man kunne få en hurtigere situasjonsforståelse på land uten å måtte gå gjennom rapporteringsfasen. Desto raskere man kan få denne situasjonsforståelsen på land, desto raskere får man i gang en proaktiv tankegang for å kunne støtte/hjelpe installasjonen.
Kan vi forhindre en katastrofe lik Deepwater Horizon.	Dette har Ognedal (Direktør i Ptil) svart på, han mener at en katastrofe lik Deepwater Horizon kommer til å skje, slik at D skal ikke si han imot på dette området. Det er derfor svært viktig at man forbereder seg på at dette kan skje.

Aktør HRS	
Informasjons område:	**Informant svar:**
Rolle I beredskapssituasjonen	Under en beredskapssituasjon vil bistand fra den offentlige redningstjenesten normalt tilbys i form av redningshelikopter og annet gjennom HRS. HRS vil normalt umiddelbart bli varslet av plattformen som er involvert i hendelsen offshore. Under hendelser som omhandler akutt forurensning er det kystverket som ivaretar det offentliges ansvar, mens HRS bistår ved behov. Vanligvis har det gjerne vært et redningstilfelle i forkant av et forurensningstilfelle(f.eks. Full City), slik at HRS har vært inne og koordinert innsats før kystverket kommer på banen med koordinering av innsatsen i form av bekjempelse av forurensningen. Dersom man har en DFU som omhandler fartøy drivende inn mot installasjon, vil HRS bli orientert og vil på eget initiativ foreta den nødvendige varslingen og/eller omdisponeringen av ressurser. Her har flere aktører forskjellig ansvar. 1) Skipets fører/eier/ befrakter har et eget ansvar for å forhindre kollisjon (Sørge for å få slepebåt osv.) De har et ansvar om å melde fra om situasjonen, vanligvis via kystradiostasjon til Kystverket etter HRS. 2) Offshoreinstallasjonen skal ha en egen beredskap i forhold til slike hendelser, det kan være standby fartøy, fartøy som inngår i områdeberedskap, helikopter for evakuering

	av personell osv. 3) Kystverket har et overvåkningsansvar for skipstrafikken og skal både bli varslet og varsle involverte, deriblant HRS om et slikt drivende fartøy. HRS er den overordnede koordinator i den offentlige redingstjenesten, og redningstjenesten har et hovedfokus på å redde menneskeliv. HRS vil være en koordinator for mange ulike ressurser/aktører både innen det offentlige, private og frivillige, alt etter hvilke behov som finnes i en hendelse. Men HRS har ikke noe "ansvar" i forhold til koordinering av innsats i form av forurensning og hendelser som er relatert til virksomhet som har et eget pålagt rednings- og beredskapsansvar som for eksempel operatører på norsk sokkel. Når dette er sagt så vil HRS være en sannsynlig aktør også i slike hendelser, enten i form av bistand, koordinering av deler av en hendelse (f.eks. innsats og koordinering av helikopter), der de blir anmodet om å overta koordineringen eller inngå som en del av det definerte beredskapsapparatet.
Oppdeling av beredskapsorganisasjonen	Redningstjenesten i Norge er et "samvirke" hvor de enkelte aktører (offentlige, kommunale, fylkeskommunale) plikter å delta. Aktørene skal i prinsippet ivareta det samme ansvaret i en hendelse som det de gjør i det daglige (Ansvarsprinsippet), slik at HRS ikke tar bort ansvaret fra noen under en krise, dvs. at det ikke lages en ny og ukjent kriseorganisasjon. I innsatsen i redningstjenesten inngår de ulike aktørene som deler av et hele, dermed blir utfordringen å få koordinert dette godt nok.
Aktører i en beredskapssituasjon	Når det gjelder DFU omkring hydrokarbonlekasje og/ eller tap av brønnkontroll har operatør et selvstendig beredskapsansvar (man skal ha en beredskap tilstrekkelig til å kunne ivareta de definerte fare og ulykkessituasjonene). På dette området har offshore industrien en betydelig egen beredskap i form av skip, helikopter og trent beredskapspersonell både i første og andre linje.
Teknologibruk mellom aktører i en beredskapssituasjon	Normalt foregår all varsling så direkte som mulig, normalt på telefon eller radio, telefonforbindelsen kan være på satellitt. Informasjonen foregår også gjennom telefon, e-post og gjennom organisasjonenes egne beslutningsstøttesystemer.
Hyppighet av informasjonsutveksling	HRS føler seg bra oppdatert omkring situasjonsbildet til enhver tid. Andrelinje beredskap vil være av stor viktighet her dersom de er etablerte, HRS har også et fokus omkring det faktum at førstelinje må få konsentrere seg om løsningen av hendelsen, og ikke ha en så stor grad av rapporteringsansvar. Ved reelle hendelser hvor det vil være et behov for en samordnet innsats vil operatør normalt sende en Liason til HRS, slik at kommunikasjonen med selskapet vil foregå gjennom denne.
Informasjonsstrøm under en beredskapssituasjon	I en beredskapssituasjon er det normalt kontrollrom som varsler HRS direkte, i noen tilfeller vil dette komme direkte fra andrelinje, dette er situasjonsbetinget. HRS har et eget planverk i forhold til ulike scenarier, og det vil være en operativ vurdering hvem som varsles, evt. Hvilke tiltak HRS gjør. Dersom varslingen kommer fra første linje, vil HRS normalt kontakte andre linje, HRS vil ta kontakt med Ptil og andre aktører. Men dette er svært situasjonsavhengig og basert på HRS egen vurdering, men selvsagt mest på operatørs/kontrollroms egen vurdering av potensial og evt. behov for bistand fra den offentlige redningstjenesten. Noen aktører er svært flinke til å informere HRS umiddelbart, men igjen så vet ikke HRS om de hendelsene hvor de ikke blir varslet, og de antar at det er ulik terskel for å "involvere" andre enn egen organisasjon. De selskaper hvor HRS deltar i øvelser og lignende er de som har lavest terskel for varsling.
Ny teknologi medført at det er blitt en forskjell i aktørbildet nå i fht.	Når man tenker på at det har blitt en del ekstra "Mygg-selskaper" (de små selskapene), så er det klart at man har fått en del selskaper som kanskje oppleves som "papirselskaper" uten en egen beredskapsorganisasjon, og

Tidligere	heller ikke noen særlig grad av kjennskap til beredskap. Disse selskapene vil kjøpe beredskapstjenesten av noen selskaper som "selger beredskap" slik at selskapets forpliktelser ivaretas gjennom disse. HRS har en relativt nær og god dialog med beredskapsleverandørene.

Aktør E	
Informasjons område:	**Informant svar:**
Beredskapsplanlegging	E driver med vanlig konsulentvirksomhet innen beredskapsplanlegging. DVS. risikovurderinger, beredskapsanalyser, beredskapsplaner osv. Es typiske kunder er selskaper som driver med leteboring, hvor hver brønn får sin egen beredskapsplan.
Rolle i beredskapssituasjon	E tilbyr sine kunder en andrelinje beredskapsorganisasjon. Es andrelinje beredskapsorganisasjon består av 5-6 vaktlag, og består totalt av 40-45 personer i selve den operasjonelle kjernestaben. De har miljørådgivere, kommunikasjonsrådgivere som bemanner et mediasenter, personell som kan bemanne en pårørendetelefon tjeneste. Mottaksgrupper i Kristiansund, Hammerfest, Stavanger, Bergen og Brønnøysund med ca. 10-15 personer til stedet på hvert sted, for å kunne håndtere evakuerte som komme lokalt inn. Avtaler med hoteller omkring evakueringer. Alt i alt er det ca. 180 personer involvert i dette berdskapsoppsettet. Dette er et stort apparat, noe som kan være vanskelig for små oljeselskap med 20-30 ansatte å håndtere på en tilfredsstillende måte. I de store operatørselskapene har beredskapspersonell andre jobber til daglig, mens i de selskapene som outsourcer slike tjenester blir beredskapspersonalet profesjonelle i sin stilling, siden deres profesjon er omkring beredskapshåndtering.
Oppdeling av beredskapsorganisasjonen	Ved introduksjon av konseptet omkring outsourcing av andrelinje beredskapsfunksjonen var Ptil svært skeptisk, de mente at beredskapsfunksjonen burde være noe som selskapene selv håndterte, og de var klart imot et slikt konsept. Men etter de fikk se hvordan dette systemet fungerte, endret de sitt synspunkt og de fikk en positiv holdning til denne formen for outsourcing av beredskapsarbeid, slik at de i dag mener at en slik outsourcingsmulighet er helt nødvendig for at man skal kunne ha et forsvarlig beredskapsarbeid hos disse nye små selskapene på norsk sokkel. Dette outsourcing konseptet har vært i drift i snart to år. Det første året utførte de ca. 100 større øvelser, hvor 50 av disse var rettet opp mot kunde. Siden andrelinje hos E trener opp mot mange ulike kunder, slik at hver person som er involvert i en beredskapssituasjon får hyppige treninger omkring sine ansvarsområder. Nå når E er i stabil drift har de ca. 2 øvelser per måned. Es oppdeling av beredskapsorganisasjonen består av en beredskapsleder som har kommandoen, denne personen sitter med fullmakt fra operatør om å gjøre det som trengs under en beredskapssituasjon, men det er fortsatt operatør som sitter med det "lovpålagte" ansvaret. Videre har denne beredskapslederen et team av mennesker under seg. Det finnes en myndighetskoordinator, denne stillingen er ofte kombinert med en HMS rolle. Videre vil det være en logistikkoordinator, en HR/ personal person denne personen har fokus på personal kontroll, identitet, persondata, pårørendeinformasjon osv. Denne funksjonen kobles også til politiet som en redningsressurs. Det sitter også en informasjonsrådgiver som orienterer seg om hva det er som foregår og leverer informasjon til de som sitter på utsiden av operasjonsrommet, de som skal håndtere media. Det er tredjelinje som bestemmer hvilke pressemeldinger og hvilken informasjon som skal gå ut til media, mens det er andrelinje som sitter inne med informasjonen omkring hvilke

	media som skal informeres . Den kanskje viktigste rollen inne hos andrelinje beredskap er den personen som sitter med kontakt offshore, denne rolles kalles riggkoordinator, hvor boreledere sitter i denne posisjonen hos E, siden de i stor grad arbeider med borerigger. I denne posisjonen er det viktig at det sitter personell som har kunnskap om offshore drift, boring og brønn, prosessystemer og slike ting. Det er viktig at den personen som innehar stillingen som riggkoordinator kan "stammespråket" offshore og samtidig forstår situasjonsbildet. Dersom det er en hendelse omkring en oljevernaksjon, vil det bli hentet inn miljørådgivere til andrelinje beredskap. En viktig faktor under en beredskapshendelse er at man ikke kan operere uten en tredjelinje involvering, tredjelinje er nødt til å involveres. Den største utfordringen innen beredskapsarbeidet nå er å få andre linje til å forstå sin rolle, siden andre linje har problemer med å legge seg på det strategiske nivået som de skal ligge på. Grovt fortalt skal første linje berge liv og verdier, andre linje skal hjelpe og støtte førstelinje med å berge liv og verdier, mens tredjelinje skal se i motsatt retning, de skal ha et fokus ut mot verden og de skal ha et hovedfokus på å berge selskapet. Tredjelinje fokus skal derfor være å tilfredsstille selskapets interessentgrupper. Problemet her er at de fleste lederne i disse selskapene har en operativ bakgrunn, slik at de blir "sugd" inn i den operative delen av beredskapsarbeidet. Og klarer derfor ikke å opprettholde sin strategiske rolle i organisasjonen. Her er det viktig at det blir et større fokus på at lederne skal berge selskapet og deres rykte, og ikke blande seg inn i første og andrelinjes håndtering av hendelsen.
Hvordan tas det hensyn til ulike aktører i analyse/ planleggingsfase, hvordan identifiseres de?	De ulike aktørene i en beredskapsorganisasjon kartlegges ved hjelp av to ulike typer for analyse. Det ene er en sikkerhetsrettet beredskapsanalyse, som i stor grad dreier seg om at du har tilstrekkelig med ressurser til medisinsk evakuering, ressurser tilgjengelig for en total evakuering, nok redningshelikopter nært nok til å kunne betjene riggen, se på avstander og flytider i forhold til avstander og posisjoner fra land, avstand til sykehus. I det hele tatt å kartlegge behovene og definere ressursene som trengs i en beredskapssituasjon. Noen steder er det en overflod av ressurser, mens andre steder er det en mangel på slike ressurser. F.eks nå driver E med en planlegging omkring en brønn som ligger langt fra land, her er det spesielle behov som må kartlegges, da spesielt i forhold til akuttmedisinske forhold, avstand til sykehus og slike faktorer, dette medfører at man må ha mere medisinsk kompetanse og utstyr ombord for å kunne håndtere en pasient i et lengre tidsrom enn det som fra før er vanligpraksis. I slike tilfeller må man foreta spesielle vurderinger. Når denne analysen er gjort, er det kun definert behovet for ressursene, deretter er det opp til beredskapsplanleggerne å få på plass disse ressursene. Det er en evig diskusjon omkring avtaler og kommersielle kontakter og slikt. Noen ganger blir dette en dyr affære, mens andre ganger trenger man ikke gjøre noen ting, siden det finnes så mange ressurser allerede. Akkurat det samme skjer på miljøsiden, ved en kartlegging av miljøsårbare ressurser, definere behov for oljeverntiltak, velge de rette oljeverntiltakene om det skal kun benyttes lenser, eller om man skal benytte dispergeringsmidler i tillegg til lenser, eller om man ikke trenger oljevern i det hele tatt siden feltet kun har gassforekomster. I praksis er en slik oljevernberedskap overlatt til NOFO. E utfører alt fra analyse og studier til en etablering av planverk, via trening på planverk gjennom kunder og bruken av planverket under en operasjon.
Teknologibruk mellom aktører i en	Riggkoordinatoren i andrelinje beredskap har kontakt med riggen, slik at han er kommunikasjonskanalen til og fra offshore, denne personen har

beredskapssituasjon	kontakt med boreentreprenørens organisasjon, i dette tilfellet riggselskapet. Riggkoordinatoren har også kontakt med boreavdelingen som er de som håndterer boretekniske, brønnkontroll problemer. Det er viktig å vektlegge at det er boreavdelingen som skal håndtere brønnsituasjonen, mens at det er beredskapsorganisasjonen som skal håndtere minutt for minutt situasjonen under en beredskapshendelse. All kontakt mellom første og andre linje foregår over telefon. E har tatt i bruk et webbasert informasjonsdelingssystem hvor hver enkelt fører logg selv, og den informasjonen som trengs blir gjort tilgjengelig for den som trenger den der hvor den trengs. De benytter CIM som har et rollebasert innloggingssystem i et webbasert grensesnitt. Dette gjør at man får den informasjonen man trenger. Et annet verktøy som også kan benyttes er Crisis Manager, både CIM og Crisis Manager er forholdsvis like å benytte. Utenriks Departementet har lagd sitt krisehåndteringsprogram rundt CIM. Det som disse systemene har gjort er at de i stor grad har eliminert telefonbruken siden informasjonen finnes på nett, og de som trenger denne informasjonen kan bare hente denne opp og se det på skjerm. Også etter at beredskapsleder har hatt statusmøter bli det lagd en logg som tredjelinje kan se på for å orientere seg. I dette loggsystemet kombineres lesing av planverk med utføring av de kommandoer som kreves i planverket. Grensesnittene er spesifikt utformet for de ulike rollene, dette gjør at de ulike rollene kun får opp den informasjonen de trenger. Det er beredskapslederen som ser "det store bildet", hvor man har all informasjon tilgjengelig. Så langt er det bare andre og tredjelinje som benytter dette loggsystemet, men det er også muligheter for at førstelinje kan benytte dette verktøyet. All informasjon til eksterne aktører foregår over telefon.
Viktigste faktor for godt samarbeid	Det viktigste er rolleavklareringen mellom andre og tredjelinje. Informanten mener at det kun er Statoil som klarer å håndtere tredjelinjerollen på en tilfredsstillende måte. Det er også viktig å trene på denne rolledelingen, hvor tredjelinje trener i samspill med andrelinje.
Informasjonsstrøm under en beredskapssituasjon	Informasjonsstrømmen er god. Etter at loggsystemet ble innført har det blitt mye mindre telefonbruk, tidligere satt personalet i andrelinje i svært stor grad i telefonen, nå sitter de ikke i nærheten av like mye som tidligere i telefonen. Dermed har fokuset forflyttet seg fra å formidle informasjon til problemløsning. Noen problemer har det imidlertid vært med denne loggdelingen, ved at enkelte har skrevet inn informasjonen på en gammel hendelse i loggsystemet, slik at informasjonen ikke formiddlet til de berørte partene i den pågående hendelsen.
Mulighet for bruk av samhandlingsteknologi i beredskapssituasjon	Per i dag har ikke førstelinje tilgang på den samme loggen som andre og tredjelinje har tilgang til, men det er her store potensialer for en effektivisering av informasjonsdelingen dersom man kunne innført dette også offshore. Et eksempel her er muligheten for førstelinje for å se ankomsttider og plassering av alle tilgjengelige helikopter og fartøy. Denne informasjonen går per i dag over telefon. Det er også muligheter for offentlige aktører å få se statustavlen under en slik hendelse, f. eks. kunne Ptil ha logget seg på systemet med tilgang til statustavlen, og slik kunne andrelinje og Ptil sluppet en telefondiktat omkring status. Men at de heller fikk en kontinuerlig statusoppdatering fra andrelinje ved hjelp av denne loggen. Teknologien er der, mulighetene er der, skjermene henger på veggen det som trengs er at noen griper muligheten og tar i bruk teknologien. Videre kan man benytte loggen til å ha en kontinuerlig oppdatert oversikt over hvor personell er til enhver tid. Dette ble gjort av E ved å koble bookingsystemet som benyttes offshore direkte opp mot loggsystemet.

Problemer ved bruk av samhandlingsteknologi i beredskapssituasjon	Hvis du baserer deg for mye på en form for teknologi, så blir man sårbar i forhold til linjebrudd og nettilgang. Dette er en utfordring, men den lar seg løse ved å organisere redundante nettilganger.
Ny teknologi medført at det er blitt en forskjell i aktørbildet nå i fht. Tidligere	Det er kommet flere aktører, for eksempel slike selskap som E, som påtar seg andrelinje beredskapsarbeidet for operatørselskaper. E forventer at også de større operatørselskapene vil innse at en slik form for outsourcing av andrelinje er den mest bærekraftige måten å utføre andrelinje beredskapsarbeidet på, både med tanke på profesjonalitet, utgifter og tidsforbruk.
Tillit	Tillit er noe som skal komme som et resultat av at organisasjonen er effektiv. Viktig at rolleinnehaverne demonstrerer at de behersker rollen sin, og at deres kompetanse sitter i ryggmargen. Viktig at ulike roller i en beredskapssituasjon virker solid og profesjonelt. Erfaringen fra deres andrelinje beredskap er at Ptil ved deltagelse i Es øvelser viser tillit til E ved at de ikke har merknader i sine rapporter i det hele tatt. Samt at også den økende grad av kunder som velger en slik løsning, viser at de har tillit til at E skal klare jobben som andrelinje beredskapslag. Uavhengig av om de ulike rolleinnehaverne er samlokaliserte eller ikke, vil tilliten dannes dersom de ulike rollene får tilstrekkelig med treningsvolum slik at de blir komfortable med sin egen rolle. Dette er noe E har erfart er et problem i industrien, ved at rolleinnehaverne ikke er komfortable med sin egen rolle under en beredskapssituasjon. De får en for sjelden eksponering av sin egen rolle, slik at de viser frykt når de skal utøve den i en beredskapssituasjon. Es erfaring er at andrelinje beredskapsorganisasjonene ikke er robuste nok, personene selv har ikke tillit nok til at de selv vil fungere i en beredskapssituasjon.
I hvor stor grad stoler du på tittelen/ rollen til en person, uten å vite noe om personen på forhånd?	I sin egen organisasjon er E sikker på at personalet har den riktige kompetansen. Men stoler ikke på rolleinnehavere i andre bedrifters andrelinje beredskap på grunn av mye observasjon av disse rollene hvor de ikke har vist seg å ikke ha kontroll over rollen sin i en beredskapssituasjon.
Tillit til teknologien	Hvis vi snakker om de nye informasjonssystemene som benyttes mener E at disse er så robuste som de kan være. Det er her også noen såre punkter, det kritiske er linjeforbindelser. Her har ikke E noen som helst tillit, siden det ikke virker som om linjeleverandørene står for sin oppetidsgaranti. Dette har E løst ved å ha to uavhengige leverandører i forhold til nettjenester, men de er litt skeptiske i forhold til hvor nettverkskablene er lagt i bakken, siden de kan være lagt i den samme grøften, og da forsvinner redundansen ved å ha to leverandører. Det mest kritiske er mobilleverandørene, disse nettene går ned fra tid til annen, slik at det er nødvendig å ha flere leverandører også her. Personell som har de mest kritiske stillingene innen varsling går nå med to telefoner på seg, slik at de har et backup nett hvis det ene nettet bryter sammen. Hvis begge disse systemene bryter sammen har de ikke noen backup løsning. Dette problemet gjelder både mellom første og andrelinje og for varsling innad i andrelinje. Et problem i følge E er at dersom man f.eks. er Telenorkunde og dette nettverket bryter sammen, vil man ikke automatisk kunne benytte Netcom sitt nett. En slik nettoverføring er noe som skjer automatisk hos kunder som kommer fra utlandet med utenlandske abonnement. Ifølge E burde det finnes en slik automatisk løsning hos de aktører som har spesielle sikkerhetskritiske funksjoner, slik at alle nettverk ble tilgjengelige for disse. Dette vil for eksempel innebære i praksis at man automatisk ville blitt rutet videre til Netcom hvis Telenor falt ut. Tidligere var det mulig å ha to ulike SIM-kort i en mobiltelefon, slik at når et nett falt ut kunne man koble over til det andre, dette er ikke

	mulig i dag. Alt i alt virker det ikke som mobilleverandørene er villige til å lage robuste systemer, samtidig som vi er utrolig avhengige av dem.
Føler du deg sikker på at info kommer frem under en beredskapssituasjon	Dette er en utfordring med disse websystemene. Man kan faktisk ikke være sikker på at de som trenger informasjonen faktisk leser den. I denne sammenheng er det dannet rutiner omkring at dersom det er viktig informasjon som sendes, så skal man ta kontakt med den som skal motta informasjonen for å sikre at de som trenger den har fått den med seg. Det er viktig å ha denne verifikasjonsbiten i forhold til det som er viktig informasjon.
Hvordan kan IO teknologi være med å virke proaktivt v. avvik på installasjon?	Det er ingen tvil om at bruken av IO teknologi har hatt en litt lang og treg fødsel. Men ser at denne teknologien har vært svært vellykket når den er blitt tatt i bruk
Andre måter for å skape proaktivitet innen beredskap	Problemet er at det nesten ikke er noen organisasjoner som er i stand til å kunne tenke proaktivt. Ofte har de som er involverte i en beredskapssituasjon mer enn nok med å skaffe seg kontroll over hva det er som skjer "se i bakspeilet" slik at de ikke greier å tenke fremover samtidig, "se ut av frontruta". All fokus blir på hva det er som har skjedd og hva det er som har blitt gjort, slik at man glemmer å tenke fremover på hva man skal gjøre. Eneste måten å få til en mere proaktiv tankegang hos personer er ved å "banke det inn" i folk ved hjelp av gjentatte øvelser og trening. En mulighet for å vise proaktivitet under en hendelse er ved at statustavlen under statusmøter deles i to, slik at en halvdel består av status og den andre halvdelen består av proaktive tiltak for hvordan man skal forhindre at ting går galt. Da vil denne proaktiviteten komme opp som et tema også til de som ikke er inne i rommet når statusoppdateringene foregår, slik at alle som leser statusoppdateringen også får med seg hva som er planene fremover i hendelsen. E mener at riggkoordinatorrollen er en svært viktig rolle i en andrelinjeberedskap. Uten denne rollen kan man miste mye av situasjonsforståelsen, og muligheten for å tenke worst case. Sagt på en annen måte er innsikt og operasjonell kompetanse en nøkkelbrikke for å kunne drive en god andrelinje beredskap.
Hva bør gjøres for å forbedre dagens beredskapsarbeid	Bruken av IO konsepter kan benyttes i en mye større grad innen beredskap. For eksempel burde første og andre linje blitt knyttet mye tettere opp mot hverandre. For eksempel burde logistikkoordinatoren som har oversikt over all logistikk jobbet tettere opp til radiooperatøren eller administrasjonspersonen ute på riggen, siden de trenger denne informasjonen. I en beredskapssammenheng er det ikke viktig å ha følelsen av å sitte i det samme møterommet, sånn som det som er meningen bak de virtuelle møterommene som mange benytter i den daglige drift. I en beredskapssituasjon er det viktig at ulike aktører har tilgang til den samme informasjonen og lage effektive samhandlingsrutiner knyttet til de konkrete behovene som eksisterer i en slik situasjon. Det er også viktig å ha en god kommunikasjon og en felles informasjonsplattform mellom andre og tredjelinje. En slik kommunikasjonsplattform kan også utnyttes og utvikles med eksterne aktører som Ptil. Men det er viktig å legge vekt på at det ikke er bruken av IO rom, med masse fancy utstyr som er det viktigste i en beredskapssammenheng, her er det informasjonsdelingen som er viktigst. Det er gjort forsøk på å benytte Crisis Manager for å håndtere en beredskapssituasjon hvor andrelinje ikke møttes fysisk, men hver enkelt satt på sin egen lokasjon og arbeidet fra dette stedet. Dette fungerte veldig bra, siden de hadde det de trengte av PC og telefonstøtte tilgjengelig. Det som i all hovedsak bør gjøres for å forbedre dagens beredskapsarbeid er å ha en større grad av trening og fokus på at de

	personene som betjener rollene i større grad må ha grunnkompetansen på plass innen det de holder på med, og på bakgrunn av dette benytte seg mindre av personell i en beredskapssituasjon som har andre roller i dagliglivet. Som en konsekvens av dette kommer denne outsourcingtjenesten av andrelinje inn i bildet ved at det ikke finnes nok personell i de enkelte selskap til å håndtere disse rollene, på daglig basis. Beredskap er et fagfelt som bør håndteres av fagfolk. I gamle dager hadde gårdbrukerne som malte mel selv møller som måtte plasseres i nærheten av en foss. Det var disse bøndene selv som bygde og drev denne møllen. Etter hvert kunne de flytte mølla bort fra fossen fordi de fikk levert elektrisitet til mølla fra et kraftverk. Men det var fortsatt bøndene som drev kraftverket, inntil noen av bøndene innså at de ikke kunne være spesialister på både gårdsdrift og på strømgenerering og dermed satte de bort strømgenerering til kraftselskapene, som var spesialister på å levere strøm. Denne analogien kan benyttes på oljeselskapene, siden de ikke lever av å levere beredskap, det bli en sekundær fokusform for dem, dette er kun noe de må ha i stand for å kunne drive sitt daglige virke. Disse selskapene kan aldri bli like proffe på det, som en ekstern leverandør av tjenesten vil bli. Ved å flytte tjenesten til en ekstern tjenesteleverandør vil tjenesten kunne bli både bedre og billigere.
Kan vi forhindre en katastrofe lik Deepwater Horizon.	Problemet med Deepwater Horizon var at ingen hadde et overordnet ansvar, slik som operatøren har i Norge. Her hadde BP, Transocean og Halliburton alle et sideordnet ansvar. Det var under Deepwater Horizon ikke utført noen beredskapsanalyser, det var ikke utført noen miljørisikoanalyser, det var ikke lagd noen overordnet plan, det var rett og slett organisert på en helt annen måte enn hva vi gjør i Norge. Det viktigste vi gjør i Norge er å ha en systematisk tilnærming til beredskap, dette skjer ved at man klassifiserer DFUene

Aktør B	
Informasjons område:	**Informant svar:**
Rolle i beredskapssituasjon	Når F er offshore blir de som sitter ved Fs andrelinje beredskap på land ikke involvert i en eventuell øvelse som utføres hos operatør. Fs ansvar under en beredskapssituasjon er å ta vare på sine egne ansatte. F ønsker å ha en mer aktiv rolle innen beredskap, og har nå planer om å ta opp kontakten med operatør for å får en mer inkluderende rolle. Informanten har stilt seg spørsmål omkring hvordan operatør involverer sine kontraktører i sine beredskapsplaner. F har et eget planverk omkring hvordan de skal opptre i en beredskapssituasjon, men det hjelper ikke hvor mange planer F har, dersom de ikke er inkludert i planverket til operatør. F mener at den ressursen de kan bidra med under en krisesituasjon burde vært implementert på en annen måte enn slik det gjøres i dag. Linjene for hva som skal gjøres under en beredskapssituasjon burde allerede vært dannet, f.eks. ved at F fikk tilgang på en logg for å holde seg oppdatert under en hendelse. Informanten mener videre at en person fra F burde vært tilstede i observasjonsrommet til operatør. Tidligere har informanten arbeidet med beredskap opp imot fly, og en av de viktigste faktorene her var tilstedeværelse og å skaffe kontakt opp mot de som satt med førstehåndsinformasjonen, men det er verdt å merke seg at han da innehadde en myndighetsrolle.
Oppdeling av beredskapsorganisasjonen	De har her en andrelinje beredskapsorganisasjon hvor det sitter en beredskapsleder, HR-personell, media-personell og HMS-personell. Det

	er ikke definert hvor rask mobiliseringstid dette personalet skal ha under en hendelse, men det vil være beskrevet i de nye planene.
Teknologibruk mellom aktører i en beredskapssituasjon	Mellom operatør og F foregår samhandlingen over telefon og e-mail.
Viktigste faktor for godt samarbeid	det å trene en organisasjon i forhold til gitte planer, samt at disse planene er godt forankret og bekjentgjort, slik at alle vet hva som skal gjøres er vel det aller viktigste. Det å ha planer liggende i en eller annen perm eller på en eller annen server vil ikke være godt nok for å kunne ha en robust beredskapsorganisasjon, siden beredskapsplaner og det å tenke "worst case" er noe folk ikke får "inn under huden" før de blir nødt til det. Derfor er en del av planen til informanten å trene de ansatte til å tenke "worst case scenario", slik at de er forberedt når en slik hendelse eventuelt kommer. Informanten tror ikke at de ansatte hos F vet hvilke samfunnskrefter som blir satt i gang under et "worst case scenario". For eksempel hvis man ikke har en god plan for å håndtere media under en slik situasjon, så har man i verste fall en situasjon som vil klare å forkludre hele organiseringen, slik at gode planer og gode organiseringer blir oppsmuldret på grunn av at man får en så stor grad av støy rundt seg.
Informasjonsstrøm under en beredskapssituasjon	Informasjonen som har tilfalt F har vært alt for liten.
Tillit	Informanten ønsker å synliggjøre at F har en beredskapsorganisasjon, og på denne måten skape en tillitsfunksjon opp mot de eksterne aktørene.
I hvor stor grad stoler du på tittelen/ rollen til en person, uten å vite noe om personen på forhånd?	Svært lite, dersom en ikke vet noe om personen fra før vil en ikke stole på denne personen under en beredskapssituasjon. Svært reservert i forhold til å stole på ukjente aktører.
Hva skal til for at du mister tilliten til en rolle, eksempel?	Ved at den enkelte ikke fyller den rollen han skal ved handling.
Tillit til teknologien	Ikke tillit til teknologien.
Føler du deg sikker på at info kommer frem under en beredskapssituasjon	Punkt nummer en under en beredskapssituasjon er å få folk på plass i observasjonsrommet, siden informanten er svært skeptisk på om informasjonen kommer frem til dem. Det er viktig å få en menneskelig ressurs fra F, tilstedet der hvor førstehåndsinformasjonen kommer inn. Det å tro at man skal nå visse personer på telefon eller at man skal få skapt en videokonferanse er noe man kan bare glemme i en hektisk beredskapssituasjon.
Andre måter for å skape proaktivitet innen beredskap	Tilhenger av trening som et middel for å skape proaktivitet. Informantens innrykk av beredskapshåndteringen er at dette er noe som befinner seg i den grå massen av prosedyrer og regelverk, det er ikke noe som ligger klart frem i dagen. Det er her informanten mener at man har et forbedrings potensial. Greit nok at folk drilles og trenes i forhold til hva de skal gjøre, men det er bevisstgjøringen av hver enkelt sin rolle i en beredskapssituasjon som er det største problemet i oljeindustrien, siden folk skifter roller svært ofte. Derfor skulle treningshyppigheten vært mye større. Det er nødt til å skje endringer innen dagens beredskapsarbeid, men F tror ikke dette kommer til å skje før det fatale skjer.
Hva bør gjøres for å forbedre dagens beredskapsarbeid	Ikke alle personer er lagd for å håndtere en beredskapssituasjon, man må ha ballast for å kunne håndtere slike ting. Selv om det nå dannes disse nye selskapene som tar på seg andrelinje beredskapsarbeidet for ulike operatørselskaper, tror ikke informanten at denne løsningen er god nok, på grunn av at beredskapsspørsmål bør bli løst innad i firmaet, siden man raskt kan miste den lokale kunnskapen ved å gi slike firma ansvaret for

	andrelinje beredskap. informanten tror heller ikke at det kun er spesielt for dette firmaet at ting ikke er "helt på stell" slik ting er nå, og det er dette disse organisasjonene som tilbyr andrelinje beredskap har innsett og tatt i bruk som et forretningskonsept.

Aktør Kystverket	
Informasjons område:	**Informant svar:**
Beredskapsplanlegging	Beredskapsplanleggingen er basert på en miljørisikoanalyse og en beredskapsanalyse. Hvor det blir definert behov for utstyr, kompetanse osv. Noe av beredskapsplanleggingen er politisk styrt, dette kan f. eks. eksemplifiseres ved at det etter Full City ulykken ble besluttet at man skulle ha en slepebåt på Sørlandet, dette var noe kystverket ved hjelp av analyser hadde kartlagt som et behov i 2006, men det ble da ikke avsett penger til dette av departementet. Selv om Full City hendelsen ikke hadde noe med en slepebåt å gjøre, så endte man opp med en anskaffelse av en slepebåt etter denne ulykken.
Rolle i beredskapssituasjon	Kystverket lager ikke regelverket, det er det helsedirektoratet, KLIF og PTIL som gjør. I dette regelverket står de ulike kravene som operatør er pålagt, f.eks. skal operatør lage en aksjonsplan som skal sendes kystverket innen en time etter at aksjonsledelsen er etablert. Etter at aksjonsplanen er mottatt og de har vært i dialog med operatøren, så vil kystverket stille spørsmål omkring de ulike tiltakene som er nevnt i denne planen, de vil også vurdere å sende representanter til operatørens beredskapssentral. Kystverket har en løpende dialog med operatøren omkring hvilke tiltak de har iverksatt og hvordan de planlegger å følge opp hendelsen. Det kystverket er spesielt opptatte av er hvilke påvirkninger utslippet har hatt på ytre miljø, de vil da iverksette et miljøovervåkningsprogram for å se hvilke skader det har blitt påført fugl, fisk osv. Kystverket driver havovervåkning via kystsentralen i Vardø, her kommer det en alarm hvis det her er et fartøy som er i drift, dvs. ikke har den hastigheten det burde ha. Da vil kystverket ta kontakt med båten, og videre dersom den er i nærheten av en installasjon vil de også ta kontakt med installasjonen. I slike hendelser vil det være et samspill mellom kystverket, Ptil og operatøren. Men når fartøyet kommer innen for en 500 meters radius av installasjonen vil operatør kunne ta i bruk sitt beredskapsfartøy for å avverge en mulig kollisjon. Kystverket har ikke myndighet til å foreta seg noe med et driftende fartøy hvis dette fartøyet er utenfor 12 nautiske mil fra land. Kystverket og Ptil har en samarbeidsavtale omkring hvordan de skal samarbeide under slike former for hendelser. Kystverket er både en tilsynsmyndighet og en deltager under en hendelse. De har også myndighet til å kunne overta den operasjonelle aksjonen under en hendelse med akutt forurensning. Alt som inkluderer brønndrift og bekjempelse, har kystverket ikke noe med. Det er kun driften av aksjonen mot akutt forurensning som de kan overta. Som følge av Deepwater Horizon hendelsen har Kystverket iverksatt et arbeid omkring hva man kan lære av denne hendelsen i USA, og en av de tingene de nå ser på er om det er aktuelt å etablere det som de i USA kaller "Unified Command", dette vil si et felles ledelsesapparat hvor operatør, statelige myndigheter (f.eks. Kystverket) og andre statlige aktører som er relevante inngår et felles ledelsesapparat, slik at man kan få utnyttet ressursene på en bedre måte. Under en hendelse er det Ptil som blir varslet av operatør, deretter varsler Ptil Kystverket. Denne varslingen foregår over telefon. Videre under et alvorlig oljeutslipp som har skjedd nært land vil kystverket varsle Fiskeri og Kystdepartementet, KLIF,

	Direktoratet for Naturforvaltning, Fiskeridirektoratet, Havforskningsinstituttet, IUA (interkommunale utvalgene) det er også flere som vil varsles her, det finnes en egen prosedyre for dette. Kystverket vil være i en tett dialog med Ptil under hele prosessen, siden Ptil har kontroll på tekniske ting under en hendelse.
Teknologibruk mellom aktører i en beredskapssituasjon	Under en hendelse benytter Kystverket en kystinfo kartløsning, dette er en viktig kilde for å vite hvor ulike ressurser er til enhver tid. Dette brukes både internt og eksternt i bedriften, for eksempel benytter IUA også dette. Under håndteringen av Godafoss benytter Kystverket nå Projectplace for f.eks. å legge ut aksjonsplanen, som omhandler hvordan ulykken skal håndteres. Ved hjelp av dette verktøyet kan ulike aktører se denne aksjonsplanen og legge inn endringer i dokumentet, slik at det blir forbedret ved neste gangs revisjon. I kystverket har de benyttet Projectplace i sitt daglige arbeide, slik at dette verktøyet er ikke nytt for dem nå under håndteringen av Godafoss. Kystverket benytter en logg for å holde oversikten over en hendelse. Dette loggføringssystemet har et stort forbedrings potensial, og de driver nå i dag å ser på hvilke andre loggsystemer som finnes som f.eks Crisis Manager og CIM. Teknologien som benyttes opp mot de ulike aktørene i dag er: telefon, e-post, kystinfokartløsning og projectplace.
Viktigste faktor for godt samarbeid	Involvering, dvs. at man har en tett dialog, at man involverer de ulike aktørene i de ulike fasene slik at de har kunnet gitt sin påvirkning til en ny aksjonsordre som skal ut. Også er det også det faktum at man følger opp ting man har blitt enige om. Videre er det også viktig at man har den nødvendige, treningen, opplæringen og forståelsen omkring hva sin egen rolle går ut på. Ser ofte personer som misforstår sin rolle, noe som bidrar til forvirring.
Informasjonsstrøm under en beredskapssituasjon	Utrolig mye informasjon under en beredskapssituasjon, for eksempel informasjon omkring hvor oljen er, hvor fuglene befinner seg i området, hvilke ressurser man har på plass, har IUA mobilisert seg, osv. Kystverket har en aksjonspostkasse som brukes under en beredskapssituasjon. Det er svært vanskelig å sitte med en total oversikt under en slik hendelse. Det som er svært viktig er at de enkelte som får informasjon, gjør denne informasjonen tilgjengelig for de andre, dette gjøres ved å loggføre viktige ting. Det er også viktig å ha oppdateringsmøter, i startfasen av en beredskapsaksjon blir slike oppdateringsmøter utført annenhver time. Informasjonen som skrives inn i loggen blir ikke på noen som helst måte gradert, den nyeste informasjonen kommer sist, uavhengig av alvorlighetsgrad. Det er definert en loggfører under en beredskapshendelse, men ansvaret for å loggføre viktige ting ligger allikevel på den enkelte.
Problemer ved bruk av samhandlingsteknologi i beredskapssituasjon	Ved å gjøre seg svært avhengig av en viss form for samhandlingsteknologi blir man sårbare, og det vil da bli svært kritisk at teknologien virker. Dette er noe som DSB påpeker i sin rapport, de nevner punkter som f.eks. tap av strøm, at teknologien virker når og slik den skal, at systemene er oppe og går osv. Derfor under en hendelse vil Kystverket har en IKT kyndig person som kan bistå med alt fra banale til kompliserte ting. Et problem hos kystverket er at noen lekker ting ut til media, når slike ting skjer kan ting bli tatt helt ut av sammenheng, og skape uro i befolkningen.
Ny teknologi medført at det er blitt en forskjell i aktørbildet nå i fht. Tidligere	Vil ikke si at det er flere som er innvolvert, men det er flere som sitter med informasjon som kan ha betydning, og denne informasjonen er blitt lettere tilgjengelig. Tidligere var det for eksempel vanskelig å ha oversikt over de sårbare områdene langs kysten, hvor var fuglefjellene, hvilke områder som skulle gis førsteprioritet hvis en hendelse hadde oppstått var

	informasjon som var svært vanskelig tilgjengelig tidligere. Nå er disse opplysningene tilgjengelige for "hvermansen" på kystverkets nettsider gjennom kystinfo kartløsningen. Dette gjør det mye lettere å skaffe seg informasjon, samt at man får tatt beslutninger på de riktige grunnlagene. Med den nye teknologien trenger man ikke alltid snakke med eksperten for å kunne ta de riktige beslutningene, siden man mye lettere kan skaffe seg informasjon selv klarer man å ta beslutninger på grunnlag av den informasjonen man har tilgjengelig.
Nye mønster i fht. Hvordan de ulike aktørene snakker sammen	Man benytter fortsatt telefon, men ikke i like stor grad som tidligere, nå benyttes også e-mail og projectplace i stor grad. Derfor kan man i stedet for å sitte i telefonen hele tiden, bruke tiden man har til overs og det man har igjen av hjernekapasitet til å tenke fremover. Hva er den forventede utviklingen, samt hvordan kan man redusere omfanget av denne negative utviklingen.
Tillit	Man er helt avhengig av tillit, at de du forholder deg til faktisk gjør det de skal og er etterrettelige. Særlig hvis du tar beslutninger som er viktige så må du ha tillit til at den informasjonen du får er riktig. For eksempel når Godafoss skulle trekkes av området der den gikk på grunn for noen dager siden, var det helt vesentlig at man hadde tillit til de fagpersonene som sa at det ikke ville komme olje ut hvis man dro båten av grunnen. Tillit skapes mellom ulike roller i stor grad ved at man tidligere har øvd på scenarioet. F.eks. ble det øvd på et scenario lik Godafoss, nå før jul, slik at man allerede hadde skapt et tillitsforhold med de ulike rollene som deltok i en slik hendelse. Men hvis man har en person som "skyter fra hofta", dvs. ikke helt kjenner og kan sin rolle i en beredskapssituasjon, vil man ikke få tillit til denne personen. Tillit til de innad i kystverket, dannes ved at de personene som innehar de ulike rollene under en beredskapssituasjon faktisk kan og vet hvilken rolle de har, og utfører denne korrekt under en beredskapssituasjon.
I hvor stor grad stoler du på tittelen/ rollen til en person, uten å vite noe om personen på forhånd?	Har en del erfaring på at tittelen ikke nødvendigvis har så stor betydning. Personer må vise til mer enn tittelen, de må vise at de faktisk kan gjøre noe. Det er med handling og ikke ved tittelen du viser om du er tilliten verdig. Men man kan heller ikke gå inn i et samarbeid hvor man har misstillit til de andre rolleinnehaverne. Man må anta at den enkelte har tilstrekkelig kunnskap og gjør det han skal.
Hva skal til for at du mister tilliten til en rolle, eksempel?	Når en person gjør noe *Jæ....* dumt, som han overhodet ikke skulle gjort.
Noen roller du har større tillit til enn andre	Har i utgangspunktet tillit til at operatør gjør det som er forventet av dem under en hendelse.
Tillit til teknologien	Har i utgangspunktet tillit til at den teknologien de benytter fungerer.
Føler du deg sikker på at info kommer frem under en beredskapssituasjon	Sjekker alltid om viktig informasjon er mottatt av mottager. Dersom informasjonen er svært viktig ringer informanten til de det gjelder for å forvisse seg om at informasjonen er kommet frem. Dersom informasjonen ikke er fullt så viktig så bes det om en bekreftelse om at informasjonen er mottatt.
Hvordan kan IO teknologi være med å virke proaktivt v. avvik på installasjon?	Det vil selvfølgelig være kjempe viktig at det sitter personer på land som kan følge med på hva det er som skjer på installasjonen, slik at tidlige avvik kan oppdages. For kystverket er dette noe perifert.
Andre måter for å skape proaktivitet innen beredskap	Det de ser ved å benytte Projectplace er at man ved å legge ut dokumenter her får et levende dokument, folk kan komme med innspill hele tiden, slik at man hele tiden er inne i en fase omkring kontinuerlig forbedring, og slik kan bli mer proaktiv.
Hva bør gjøres for å	Man må se på hele porteføljen av metoder, dvs. man må ha en større grad

forbedre dagens beredskapsarbeid	av forskning og utvikling i forhold til metodeutvikling, jamfør rapport fra risikogruppen: Ulykken i Mexicogolfen- Risikogruppens vurdering. I utarbeidelsen av denne rapporten deltok Ptil, KLIF, Kystverket samt også flere andre fagetater. Videre er det en uenighet mellom Kystverket og operatørselskapene, ved at operatørselskapene mener at oljevernutstyret de benytter har større kapasitet enn hva kystverket mener at dette utstyret har, dette har kystverket påpekt i rapporter. Ut i fra dette må det skaffes mere oljevern utstyr for å kunne bli mer proaktiv.
Kan vi forhindre en katastrofe lik Deepwater Horizon.	Det finnes ingen beredskap i verden som er dimensjonert i forhold til den type hendelser. Pågår et arbeid hos kystverket hvor de evaluerer Deepwater Horizon ulykken for å ta se på ting de kan forbedre. Men i Norge har ikke denne typen av hendelser vært dimensjonerende for beredskapen. F.eks. har det ikke vært en kollaps med en supertanker som har vært dimensjonerende for kystverkets beredskap, siden dette er så lite realistisk. Man dimensjonerer beredskap på en risikobasert måte, men ifølge informanten bør man også tenke worst case når man skal dimensjonere beredskapen. Denne problemstillingen er opp til KLIF å stille til operatøren, informanten vet at KLIF allerede har gjort dette opp mot ENI og Goliat feltet, hvor man er bedt om å se på mere langsiktige hendelser både i forhold til brønnproblematikk og oljevernutstyr i sin beredskapsplanlegging. Det er KLIF som stiller kravene til operatørene.