SURVIVABILITY OF SHIPS AT SEA: A PROPOSED MODEL TO ACCOUNT FOR HUMAN FACTORS IN A SAFETY-CRITICAL SYSTEM

V Rumawas, Norwegian University of Science and Technology, Norway
BE Asbjørnslett, Norwegian University of Science and Technology, Norway

SUMMARY

Most serious accidents at sea are caused by minor incidents that escalated into an uncontrolled situation. This study is aiming to develop a model to investigate the likelihood of fatal accidents, given that a critical incident has already occurred. The focus of the study is on the human factors by adopting a hardware reliability perspective. The vessel is considered as a safety-critical system to be protected by several barriers. The crew role is modelled as active barriers and distinguishing between different functions: perception, decision and action. A Markov approach is utilized to model different situations on the vessel. A mathematical model to estimate the probability of failure in an emergency situation is formulated. A new parameter is defined for the survivability of a vessel, given that a critical incident has taken place. The methods were applied to examine ship-platform collisions cases and the results show strong benefits for diagnosing and evaluating accidents from the human factors perspectives as well as for training purposes.

NOMENCLATURE

Symbols	**Definition**
α_a	Transition rate from the abnormal to the normal environment
α_e	Transition rate from the extreme or restricted to the normal condition
α_n	Transition rate from the normal to the abnormal environment
γ	Rate of the personnel adjustment
δ	Training effect
λ	Failure rate
λ_{ah}	Transfer rate to commit human error under abnormal environmental states
λ_h	Transfer rate to commit human error under normal environmental states
τ	Test interval
1oo1	one-out-of-one
1oo2	one-out-of-two
2oo2	two-out-of-two
a_{ij}	Markov transition rates from *i* to *j*
E	Extreme or restricted condition
N	Normal condition
$P_n(t)$	Probability of human error as a function of time
R(t)	Reliability as a function of time
S(t)	Survivability as a function of time
t	Time

Abbreviations

AIPA	Accident Investigation and Progression Analysis
DP	Dynamic positioning
ETA	Event Tree Analysis
ESD 2	Emergency shutdown class 2
FMECA	Failure Mode Effects and Critically Analysis
FSA	Formal Safety Assessment
FTA	Fault Tree Analysis
HAZOP	Hazard and operability study
HEP	Human error probabilities
HFO	Heavy fuel oil
HRA	Human reliability analysis
IMO	International Maritime Organization
MJ	Mega joule
MTTF	Mean time to failure
MTTHE	Mean time to human error
NB	Njord Bravo
NH	Navion Hispania
OAT	Operator Action Tree
PFD	Probability of failure on demand
PFE	Probability of failure on emergency
PRA	Probabilistic risk analysis
PSF	Performance shaping factors
SHARP	Systematic Human Action Reliability Procedure
SIS	Safety instrumented system
SMAS	Safety Management Assessment System
stbd	Starboard
SVC	Simrad Vessel Control
THERP	Technique for Human Error Rate Prediction

1. INTRODUCTION

Perrow [1] discuss safety in light of what he terms normal accidents in contrast to high reliability systems. He views marine system as an “error-inducing” system or a system where the configuration of its components induces errors and defeats attempts to correct error.

Spouge [2] and Lawson & Weisbrod [3] find that overcrowded and overloaded vessels are characterizing passenger ferry operations in developing countries. Rumawas & Asbjørnslett [4] have documented fatal ferry accidents at sea which occurred in developing countries due to extreme conditions. The accidents can be attributed to low operating standards, mixture of cargo and passengers, low safety awareness, inadequate regulations, substandard vessels and second-hand fleet.

According to Perrow [1], not a single failure is responsible to cause a fatal accident in an error-inducing system. Accidents are quite rare for any single ship. Marine system is moderately coupled. Even though failures occur continuously, recovery is possible because time constraints are not tight.

In the case of ferry accidents that were presented by Spouge [2] and Lawson & Weisbrod [3], recovery failed to take place when constraints become stricter due to the extreme situation.

Gardenier [5] states that vessels continue to have problems with system failure detection and diagnosis. In open and unrestricted waters, the ship navigation system is tolerant to errors and other failures. As ships approach narrow or restricted fairways and increasing traffic density, the system's failure tolerance decreases.

The purpose of this paper is to provide a model that can be used to examine and to evaluate the probability of the human operator to restore the situation given that an emergency has taken place. Human factors will be the focus of the analyses where a system reliability perspective will be adopted and human element will be treated as a barrier.

2. METHODS FOR RISK ANALYSIS AND MANAGEMENT

There are a number of methods and techniques that can be applied in risk analysis of marine systems in general, published in Ayyub et al [6], Kristiansen [7], Dhillon [8] and Vinnem [9]. Both qualitative and quantitative approaches are available: what-if analysis, hazard and operability study (HAZOP), probabilistic risk analysis (PRA), failure mode effects and critically analysis (FMECA), and the bow-tie model which includes fault tree analysis (FTA) and event tree analysis (ETA). The International Maritime Organization (IMO) has published the Formal Safety Assessment (FSA) guidelines for assessing the risks relating to maritime operations and the protection of the marine environment [10]. These methods do not focus specifically on human factors but the overall risks. The FSA adopts human reliability analysis (HRA) methods to assess the contribution the human element to system failure.

2.1 HUMAN RELIABILITY ANALYSIS (HRA)

A number of methods are available to conduct human reliability analysis. Gertman & Blackman [11] have documented 38 methods, Hollnagel [12] identified 35 - 40 HRA approaches, while Stanton et al. [13] reviewed over 200 methods and techniques, and documented more than 90 design and evaluation methods. Some methods which are considered relevant for ships operations are presented as below.

2.1 (a) Accident Investigation and Progression Analysis (AIPA)

AIPA is a method to assess the probability of an operator to carry out a certain response in a given a time frame. The method was developed in 1975 by Fleming et al. [12]. Expert judgements were utilized to estimate probabilities of actions. The operator was seen as a black box in this model.

2.1 (b) Operator Action Tree (OAT)

The OAT was developed for modelling cognitive errors by nuclear-power-plant operators during accident conditions [14]. It is based on the assumption that the response to an event can be separated into three stages: (1) observing or noting the event, (2) diagnosing or thinking about it, and (3) responding to it [12]. OAT focuses primarily on the probability of failure in the diagnosis stage.

2.1 (c) Technique for Human Error Rate Prediction (THERP)

Swain & Guttmann [15] have developed one of the most widely used HRA methods to predict human error probabilities (HEP). It was initially developed to evaluate the degradation of man-machine systems in nuclear power plants. The method relies heavily on task analysis which discriminates human performance into three different behavioural elements: (1) signal sensing and perception, (2) information processing and decision-making, and (3) the required responses. The basic HEP is acquired for a set of standard activities and then adjusted for the actual working conditions by considering, performance shaping factors (PSFs). The human performance, which is decomposed into tasks, is represented by means of an event tree. Each task can be performed successfully or unsuccessfully. Recovery mechanism for unsuccessful task is also incorporated in THERP.

2.1 (d) Systematic Human Action Reliability Procedure (SHARP)

SHARP is used to predict the probability that a nuclear control room operator will respond to a plant event within a given time. The approach is developed based on human cognitive reliability and the operator action model [16].

It can be seen that the goal of the HRA methods is mainly to evaluate if the operator can perform a certain response in a certain time for a certain condition. AIPA laid the basic foundation for the purpose. Seeing the operator as a black box is a simple approach but less meaningful for further analysis. OAT started to discriminate functions in a well-structured environment, which then were developed in THERP. This kind of approach is effective in activities which can be decomposed strictly into tasks.

2.2 MARKOV METHOD

Dhillon [17], [18] has proposed a Markov method for human reliability analysis (see Fig 1). It is assumed that an operator is conducting his tasks under changing conditions: either normal or abnormal. The transition rate from the normal to the abnormal environment is given by α_n, while for the opposite direction is αa. The transfer rate from state 0 where the task is correctly executed under normal condition, to state 2 where error is committed is defined by λ_h.

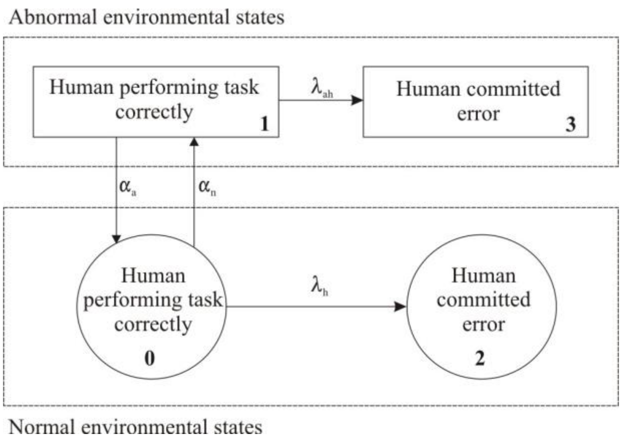


Figure 1: System state space diagram [18]

Under abnormal environmental condition the transfer rate from state 1 to state 3 is given by λ_{ah}. Other parameters of interest in this Markov model include the probability of human error as a function of time t, $P_2(t)$ and $P_3(t)$, and the mean time to reach the worst state, called mean time to human error (*MTTHE*). Detail solutions of those parameters can be found in Dhillon [18].

2.3 ACCIDENT MODEL AND ANALYSIS

There are alternative approaches to explain accidents at sea in terms of human and organization factors. Paté-Cornell [19] applied a probabilistic risk analysis (PRA) framework to analyse the Piper Alpha accident. Kristiansen et al. [20] proposed a methodology for marine casualty analysis based on elaborate taxonomy for human and organizational factors. Hee et al [21] developed Safety Management Assessment System (SMAS) to assess marine system from the human and organization factors perspective. There are seven key components evaluated in SMAS: operating teams, organizations, structure, equipment/hardware, procedures, environment and interfaces among them.

It is not the intention of this article to refute the existing methods mentioned above. However, based on published observations [2], [3] and [4] it seems that there is a gap between the existing frameworks and real accident cases occurred at sea. For instance, poor organizational factors are common in many shipping companies in developing countries. But, accident does not happen every day. Disaster does not always happen to the low-rated organization, with the poor quality equipment, and with bad management. The Deepwater Horizon case is a good example to contradict the existing models. The platform was one of the most outstanding facilities ever built, managed by the most respected companies in the business and operated by the most competent personnel in the field. Therefore, a more applicable approach is required.

2.4 SAFETY INSTRUMENTED SYSTEM (SIS)

In the field of system reliability engineering safety instrumented system (SIS) is defined as an independent protection layer that is installed to mitigate the risk associated with the operation of a hazardous system [22]. The SIS comprises sensors, logic solvers, and actuators (see Fig 2). Most of the time the system will be passive, but when a hazardous situation occurs, called a demand, the system becomes active.

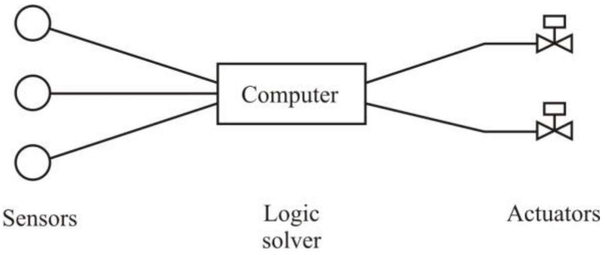


Figure 2: Safety instrumented system (SIS)

The SIS concept has been applied widely in various industries, such as for instance the airbag system in cars and blowout preventer in petroleum well completions. It is critical that the SIS is working when a hazardous event happens. The probability that an element fails to work when a demand occurs at $t = t_1$ is called the probability of failure on demand (PFD) (see Fig 3).

The average PFD of an element is determined by its failure rate (λ) and the test interval (τ, in hours). The average PFD for a single element is defined as follows [22]:

$$PFD_{1oo1} = \tfrac{1}{2} \lambda \tau \tag{1}$$

Where $\lambda\tau$ is assumed to be small.

The total PFD for the system is defined as [23]:

$$PFD_{SYS} = PFD_S + PFD_L + PFD_A \tag{2}$$

Where:
PFD_{SYS} is the average PFD of the SIS
PFD_S is the average PFD of the sensors subsystem
PFD_L is the average PFD of the logic subsystem
PFD_A is the average PFD of the actuators subsystem.

It is also assumed that all PFD's are small.

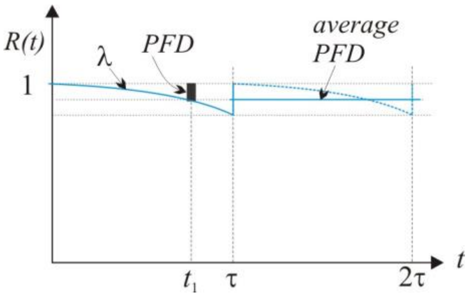


Figure 3: Probability of failure on demand (PFD)

3. SYSTEM DESCRIPTION: SHIP OPERATIONS

Most vessels operate all year around. Some ships have a fixed route and schedule, while others have ever changing transportation tasks and routes. Some ships may have a transit duration within hours, while others may sail for days or weeks. Some ships can be operated by one or two persons, while others have a crew of more than fifty persons. Environmental conditions and the vessels' technical conditions may vary from time to time. During normal conditions, most vessels can operate without any significant problem. It is however assumed that a ship might experience an unfavourable condition, such as a storm, blackout, critical system failure, or fire. These abnormal situations can trigger a severe incident and subsequently an accident, unless the crew onboard detect the problem in time and handle the situation adequately.

3.1 SURVIVABILITY OF SHIPS

Survivability of ships from the human factors perspective is defined as the probability that the crew can manage emergency situations, given that a hazardous event has occurred. The crew must be able to perform the following functions: (1) sense the hazard, (2) analyse the situation and take the proper decision, and (3) execute the right action. All these functions can be performed by one person or may be distributed among several crew members.

The main ship accidents are collision, contact, grounding, foundering, capsize, fire and explosion. Each accident category has its own scenario and typical hazardous elements which the crew must be able to handle.

3.2 SIS MODEL OF THE HUMAN ELEMENT

The SIS framework is applied to model the situations on a ship. The human element is regarded as the SIS and the vessel as the system to be protected. A hazardous event is taken as the demand.

An example of a SIS model which involves the human element in a bridge operation is shown in Figure 4. The officer in centre (logic solver) is dependent on input from the crew and another officer. These personnel act as sensors. They must observe the situation around the vessel, such as seaway, sea state, navigational markers and available displays. Should there be any deviations, the crew will directly take necessary actions, e.g., by adjusting a lever, push a button or turn a knob. In more serious cases, the situation will be reported to a higher rank officer before a decision is taken and executed. A hazardous event may be present without being detected and is called a latent failure.

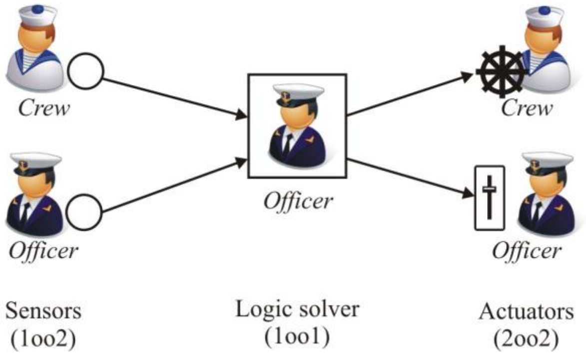


Figure 4: Crew modelled as SIS in bridge operations

Similar situations occur in other departments on board. The crew in the engine room must monitor equipment and engine processes through visual and auditory indicators. The crew on the deck will monitor the conditions and handling of the cargo, the passengers and mooring equipment.

Sensors work as a parallel system or one-out-of-two system (1oo2) where only one is required to function. Actuators work as a serial system or two-out-of-two system (2oo2) where both units must work properly to maintain the integrity of system. The logic solver works as a single element or a one-out-of-one system (1oo1).

The probability of failure of an emergency (PFE) is defined in the similar way as the PFD in the hardware reliability perspective.

Unlike a hardware element which is considered to work well when it is new, the human element is the less reliable on the outset. When a seafarer is recruited and manned on a vessel, he or she is not completely ready for the job. The crew is assumed to hold a certain level of competence and skill based education, training and experience. Since every vessel is unique, some briefing, orientation and adaptation will be required. The crew's capability to handle the vessel given a hazardous situation is called the survivability, while the probability of failure on emergency (PFE) reflects the opposing index. The more competent the crew, the higher the survivability index will be.

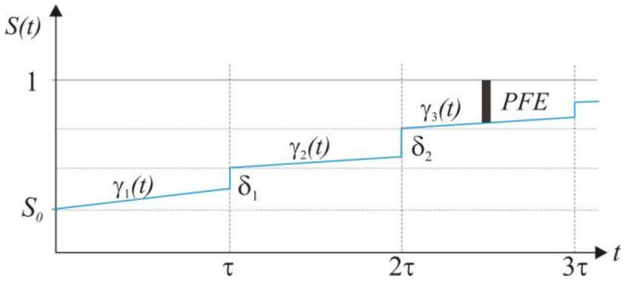


Figure 5: Probability of failure on emergency (PFE) and survivability

Survivability, S(t) is determined as the function of previous knowledge (S_0), briefing, adaptation and on-the-job learning processes (γ) and formal training or assessment (δ).

$$S(t) = S_0 + \sum \gamma_i \tau + \sum \delta_i \tag{3}$$

Consequently, PFE can be defined as:

$$PFE = 1 - S(t) \tag{4}$$

In this case, test interval (τ) refers to the time between training, or between assessment programs. The rate of the adjustment (γ) and training (δ) can be different from time to time and person to person.

3.3 MARKOV METHOD FOR SHIP OPERATIONS

In this part, a Markov method is employed to model ship operations. Two conditions are defined normal condition and extreme or restricted condition. Taking the model in Figure 1 as a starting point, the human function is broken down in three different functions: (1) monitoring the situation, (2) analysing the situation and making the correct decision, and (3) conducting the proper action. The complete model is shown in Figure 6. The defined system states and transfer rates are given in Table 1 and Table 2. Following notation is applied: N or n stands for the normal condition and E or e for the extreme condition. The transfer rate from the normal to extreme condition is α_n and α_e for the reverse direction. A vessel can switch from being in a normal condition to an extreme condition, for instance when the weather deteriorates. Transition from normal to restricted condition is experienced when the vessel is sailing from open sea to confined water.

A vessel is assumed to be safe in state 4 when the crew perform all the tasks correctly: monitor, decide and act. The crew may fail in performing any of these tasks and bring the vessel into a less safe state (3, 2 or 1). The most likely path is that the crew fail to monitor the situation (a_{43}), which then leads to a wrong decision (a_{32}), and consequently an improper or wrong action (a_{21}) (see bold lines in Fig 6).

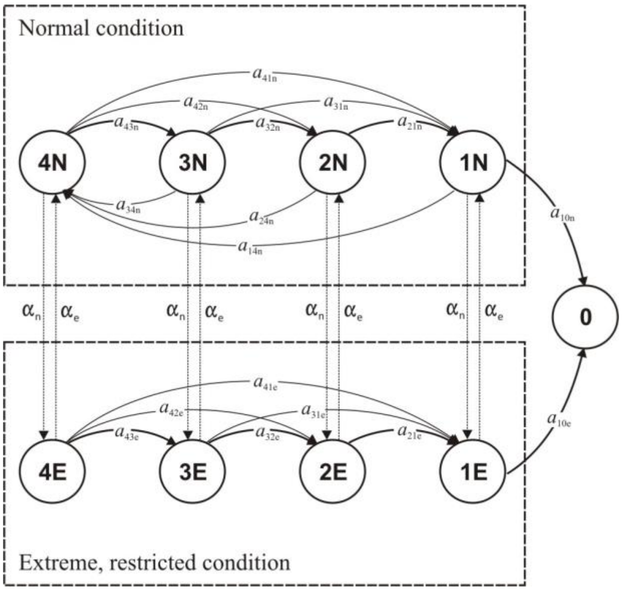


Figure 6: Markov model for ship operations

Table 1 System states for ship operations

System State	Description
4	The crew perform the tasks correctly
3	The crew fail to monitor the situation
2	The crew fail to make the correct decision
1	The crew fail to conduct the proper action
0	The vessel fails to maintain integrity

Table 2 Markov transition rates for ship operations

Transfer rate	Description
a_{43}	failure in monitoring the situation
a_{42}	making a wrong decision
a_{41}	conducting an improper action given
a_{32}	making a wrong decision
a_{31}	crew failure rate in conducting the proper
a_{21}	conducting an improper action given
a_{10}	loss of vessel integrity given wrong action
a_{34}	restoring adequate monitoring
a_{24}	restoring adequate decision making
a_{14}	restoring adequate action

In the normal condition a crew member may realize a mistake and restore the situation back to the previous and correct state (4N). The likelihood of bringing the situation back to the initial state is called the restoring rate. Under the extreme condition the likelihood of restoring the situation is extremely low. This is expressed in the model by the lack of any restoring transitions.

4. CASE STUDIES

The methods proposed above were tried out on six collision cases between facilities and visiting vessels in the Norwegian shelf [24]. One example is presented as follows.

4.1 AN EXAMPLE INCIDENT [24, 25]

12 Nov 2006. HFO filters on Navion Hispania were clogged leading to both main engines stop working and the vessel suffered a blackout. The crew cleaned and reinstalled the filters. The cause for the blackout was fuel starvation as a result of dirty oil. The voyage continued. It seems that there was a practice onboard to drain HFO filters to the overflow tank and to pump the content of the overflow tank back into the fuel system via HFO storage tanks. Prior to arrival at the Njord field both separators stopped working due to heavily contaminated fuel oil. The engine officers decided to continue the voyage without separators.

13 November 2006. Upon arrival at the Njord field the level in both settling tanks were abnormally low. The reason for this was there was no more fuel in the storage tanks to fill the settling tanks except from the HFO received in Falmouth on Nov 9th. Engine officers decided not to use from bunker received in Falmouth before the fuel analyses were available. This is according to company procedures. The vessel passed the 500 m zone and connected to the Njord B's mooring line and closed the chain stopper on the chafing chain.

The master and the chief mate junior were on duty at the bridge. The chief mate junior was operating the DP under supervision of the master. An indication of malfunctioning appeared on the DP screen: "Stbd Propeller prediction error" which then was followed by drive off alarm. The Master and the chief mate junior observed red alarms on the SVC control panel. The master rushed over to the centre control console and registered that the vessel had lost all thrusters on stbd side. The same information was registered on the DP's screen. The port bow and stern thruster stopped, leaving the vessel with only the port main propeller and rudder in operation. The master gave order to disconnect the hose handling wire. The deck crew did as ordered and clear the bow area. Then, the master ordered the chief mate junior to execute ESD 2 to release the chain stopper and mooring line. The DP was taken over in manual (joystick control) and the master set out full astern command. But it was too late. About half a minute later the bow of NH hit the NB's stern. The collision energy exceeded 60 MJ.

4.2 A SIS MODEL OF THE EXAMPLE INCIDENT

Two separate incidents were identified in the engine room that can be described as SIS mechanism (Figure 7). The deviations were straightforward and easy to detect: the system stopped working. Anybody on the vessel could identify the symptoms. The person-in-charge in the engine room made the decisions to cope with the deviations and the crew on watch performed the actions. However, unfortunately in this case the decisions did not really solve the actual problems. The actual hazardous event in the operation was that the engine stopped working. The real cause of the event was contaminated or low quality fuel oil. But, the decisions made by the engine officer did not settle this problem.

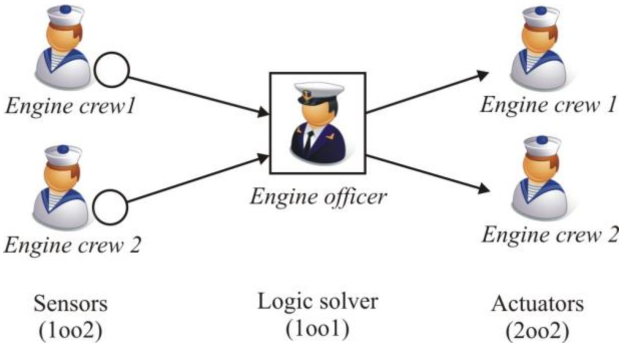


Figure 7: Engine crews modelled as SIS in the NH case

Two SIS occurrences were identified on the bridge as a logical consequence of the deviations in the engine room. The first SIS occurred between the bridge and the crew on the deck (Figure 8).

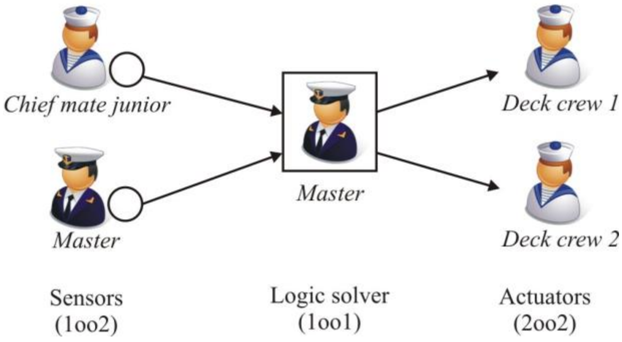


Figure 8: Bridge to deck SIS: prepare for emergency release

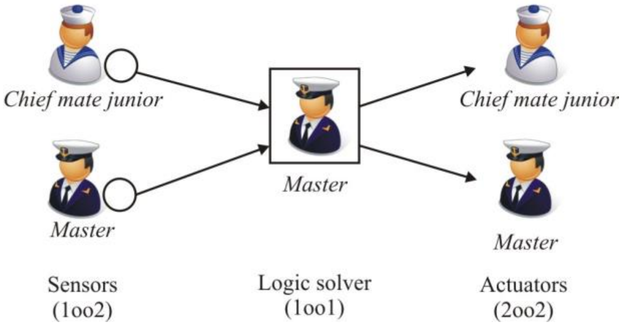


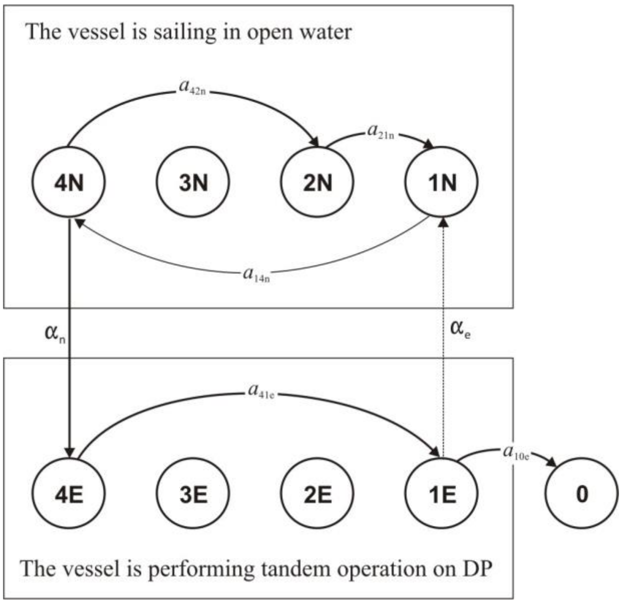
Figure 9: Bridge operation described as SIS

The hazardous event identified was DP problem. The crew on the bridge acknowledged the problem. The master has analysed the situation and decided to conduct some actions. He asked the deck crews to prepare for emergency release. After it was completed, the master and the chief mate junior tried to conduct the second SIS mechanism (Figure 9) i.e., set the control to manual and bring the vessel away from the installation. But, they failed to avoid the collision.

Since the study was conducted solely based on published incident reports without access to first hand data, the purpose to provide actual numbers is restrained.

4.3 MARKOV MODEL FOR THE EXAMPLE INCIDENT

The Markov model for the Navion Hispania case is presented in Figure 10. The information presented in Table 1 and Table 2 is also applicable in this case. It is assumed that initially the crew performed their tasks correctly (state 4). Then, a hazard emerged – the demand to the SIS. The crew did acknowledge that something was wrong; therefore state 3 is not visited. But, the crew did not make a correct decision and did not perform the correct actions. Hence, state 2 and 1 are visited. During normal condition, when the vessel is sailing in open water towards the installation, the crews had the opportunity to bring the vessel back to operation (a_{14n}).



However, when the same situation occurred in restricted condition (running on DP in tandem operation) the crew did not have the same opportunity to recover from the situation. The master was trying to alter the situation by changing from DP to manual and to leave the restricted condition to normal (α_e). The master was trying to alter the situation by changing from DP to manual (α_e); meaning to leave the restricted condition (1E) to normal (1N). But, his effort was ineffective.

4.4 SUMMARY OF THE OTHER CASES

The rest of five collision cases are summarized in Table 3 below.

Table 3 Summary of collision cases and analyses [24]

Case A. 18.01.2010. Supply vessel Far Grimshader was working on the lee side of the drilling facility Songa Dee. The vessel was asked to move to the windward side of the installation. During the move the vessel's propeller was caught in a wire attached to the facility's anchoring. **Analysis:** Far Grimshader was a substitute vessel for the operation and it was the first time for the crews to conduct such an operation. The crews did not have a proper knowledge to perform the whole operations, they failed to see the hazards, and they made wrong decisions in operating the vessel and thus failed to operate the vessel properly.
Case B. 06.06.2009. Well stimulation vessel Big Orange XVIII was approaching installation Ekofisk 2/4 X. The captain engaged the autopilot and forgot to switch it off. He could not control the vessel manually as he intended to do. Instead of slowing down, the vessel struck the installation at a speed of 9.5 knots. **Analysis:** The captain failed to see that the autopilot was engaged and made a wrong decision in operating the vessel.
Case C. 18.07.2007. Supply vessel Bourbon Surf was assigned to installation Grane. After entering the safety zone, both the captain and the first officer left the bridge. When the crew returned, it was too late to stop the vessel. **Analysis:** The captain failed to estimate the speed, heading and position of the vessel and made a wrong decision to leave the bridge and to come back late.
Case D. 02.05.2005. The first officer navigated the vessel Ocean Carrier towards the installation Ekofisk 2/4 in dense fog. The sea was calm but visibility was poor. The captain entered the bridge and there were misunderstandings as to who was responsible for the navigation. The vessel was cruising towards the installation. When the captain saw the facility, he reduced the speed, but it was too late. **Analysis:** The crews failed to identify the problem that nobody was really in charge of the control, failed to make the right decision on time and therefore failed to control the vessel.
Case E. 07.03 2004. Far Symphony had a course towards the facility West Venture. Entering the safety zone, the autopilot was engaged. The officer on the bridge did not realize that the autopilot was engaged and could not navigate the vessel. This ended in a collision. **Analysis:** The crew failed to see that the autopilot was engaged and made a wrong decision in operating the vessel.

The detail human factors analyses based on the model proposed in this paper are presented in the Appendix.

4.5 DISCUSSIONS

The benefits of the proposed methods were recognized as they were applied to analyse the incident cases in the Norwegian continental shelf. Both, the SIS model and the Markov method are effective to analyse the incident cases from the human factors perspective. The methods can provide an accurate diagnosis of the incident; what hazard is coming, what should be monitored, who should do the tasks, what decisions could be made, and what actions should or should not be performed. The approach does not treat the operator as a black box, yet it does not involve abundant details which might obscure the analysis. Since the methods are quite generic, it offers the flexibility in their application. They can be developed for various accident scenarios at sea and they can be implemented for planning purposes as well as for ex-post-facto evaluation.

Markov model offers an opportunity to accommodate the dynamic nature of most of the problems faced at sea. While most of the existing HRA methods focus on the probability of failure or the human error probability [14], [15], the adopted SIS model in this paper focuses on the probability of the human operator to survive the hazard. Furthermore, unlike the other existing methods which consider human factors as influencing factors to SIS [26], [27] and [28], the present approach treats human elements as the SIS themselves. The operator is not positioned as a threat, but as a barrier.

The case studies show that nonconformities exist most of the time, such as polluted fuel, engine problems, unqualified vessel, incapable crew, and violation of procedures, e.g., leaving the unattended and negligence in operations. As Gardenier [5] and Spouge [2] mention, these deviances do not escalate nor become critical in normal conditions. However, when the vessel entered a riskier situation, such as approaching offshore installations then the story changed dramatically. Although this study cannot present quantitative results at this point, but the findings are worthy of note.

This study implies that the first important factor to be recognized is the crew's awareness of the potential hazards. In the case of Navion Hispania the crew did not realize that polluted fuel may disturb the DP system. The second factor that is important for the survivability of the vessel is the crew's knowledge of their vessels and the overview regarding the operations. The crew's 'unawareness' of the autopilot that was being engaged is an example of lack of knowledge of the vessel, while the case of Far Grimshader is an example of lack of the overview of the operations. Finally, the capacity of the crew to make an appropriate decision is also considered crucial for survivability. Should the crew recognize the hazard and be aware of the situation, the next important factor will be the decision that they make in order to avoid fatal accident. In the case of Navion Hispania the safe alternative decisions were the unfavorable options, i.e., to postpone the tandem operation until the fuel problem solved. This can be done by changing the fuel intake from the bunker received in Falmouth which had not been analyzed. In the case of Far Grimshader one of the safe alternatives would be to decline the operation in the first place due to insufficient knowledge of the crew regarding the operation. The PFE in such a situation is close to one.

In the hardware reliability perspective it is important to estimate the state probabilities and especially states 1 and 0 ($P_1(t)$, $P_0(t)$). Those parameters represent the likelihood of critical incidents or accidents to take place in a given time frame. It is also essential to know the mean time to system failure ($MTTF_S$). In the human factors perspective, providing these numbers can be challenging, but not impossible. The motivation at this stage is more analytical. In a system design stage, requirements are set and standards are to be followed. It is implemented in a safety integrity level (SIL) requirements for components. Similar mechanism can be employed in the proposed approach. To come up with more realistic numbers, the model needs access to the existing incident databases, simulator facilities and expert judgments.

The proposed methods might be used to examine the types of hazards that should be avoided in a certain operation, such as engine problems in DP operation. These methods are also applicable to analyze the deficiencies in the system that hamper the human operators and difficult to deal with, e.g., the autopilot system which status was not obvious to detect and not easy to override. However, the methods become less effective when the hazards were originated from the human operators themselves, i.e., when the crew commit error or violation (e.g., the case of Big Orange XVIII and Bourbon Surf). It is obvious because the methods were developed based on the assumption that the operator acts as the barrier, not the threat.

4. CONCLUSIONS

Two models are adapted from the hardware reliability perspective to account for human factors in a safety-critical system. The Markov model and the SIS model are borrowed to emulate the human role as a barrier in ships operations. Both models have a potential to be used as a retroactive as well as a predictive tool. They provide a holistic approach in analysing the problems which may involve different scenarios. The methods are simple, practical and manageable to be implemented.

Some important steps in this approach to be implemented are summarized as follows:

- Examine the previous accidents and incidents scenarios
- Identify various hazards comprised in each scenarios

- Identify the corresponding human functions that are required to overcome the hazards:
    - What kind information to identify
    - What decision(s) to made
    - What action(s) to perform

The results look promising; it is useful for diagnosing purposes as well as for evaluation. However, the methods are not suitable for those cases where the operator initiates hazards in the first place or when the human element performs more as a threat rather than a barrier.

Further validation with direct access to first hand data is required to improve the models. Combining these methods with a simulator-based training center will bring strong practical benefits for the industry. It has the potential to ensure safety and to reduce risk by increasing awareness and competences of the crew.

8. REFERENCES

1. PERROW, C. 1999. *Normal Accidents Living with High-Risk Technologies.* Princeton University Press, Princeton, NJ.
2. SPOUGE, J. 1991. Passenger ferry safety in the Philippines. *Trans RINA Vol 133, 179-197.*
3. LAWSON, C.T. & WEISBROD, R.E. 2005. Ferry transport: the realm of responsibility for ferry disasters in developing nations. *Journal of public transportation, Vol. 8, No. 4: 17-31.*
4. RUMAWAS, V. and ASBJØRNSLETT, B.E. 2010. A proposed model to account human factors in safety-critical systems. *ESREL Conference. 5-9 Sept 2010.* Rhodes, Greece.
5. GARDENIER, J.S. 1981. Ship navigational failure detection and diagnosis. In *Human detection and diagnosis of system failures*. J. Rasmussen & W.B. Rouse (eds): 49-74. Plenum Press, New York and London.
6. AYYUB, BM, BEACH J.E., SARKANI, S., and ASSAKAF, IA. 2002. Risk analysis and management for marine systems. *Naval Engineers Journal Vol 114, 181-207.*
7. KRISTIANSEN, S. 2005. *Maritime transportation safety management and risk analysis.* Elsevier Butterworth-Heinermann.
8. DHILLON, B.S. 2007. *Human Reliability and Error in Transportation Systems.* Springer-Verlag, London.
9. VINNEM, J.E. 2007. *Offshore Risk Assessment Principles, Modelling and Applications of QRA Studies.* 2nd Ed. Springer-Verlag, London.
10. INTERNATIONAL MARITIME ORGANIZATION (IMO). 2002. *Guidelines for Formal Safety Assessment (FSA) for Use in the IMO Rule-making Process.* MSC/Circ.1023. MEPC/Circ.392.
11. GERTMAN, D.I. & BLACKMAN, H.S. 1994. *Human reliability & safety analysis data handbook*. John Wiley & Sons, Inc. New York, NY.
12. HOLLNAGEL, E. 1998. *Cognitive Reliability and Error Analysis Method (CREAM).* Oxford New York: Elsevier.
13. STANTON, N.A, et.al. 2005. *Human factors methods: a practical guide for engineering and design.* Ashgate Publishing Ltd.
14. WREATHALL, J. 1984. Operator-action Trees, A method for modeling cognitive errors in risk analysis. Anticipated and abnormal plant transients in light water reactors. *Proceedings of an American Nuclear Society Topical Meeting.* Jackson Hole, WY, USA. pp 1029-1040.
15. SWAIN, A.D. and GUTTMANN, H.E. 1983. *Handbook of human reliability analysis with emphasis on nuclear power plant applications.* Final Report. US Nuclear Regulatory Commission, Washington DC, USA. Report No. NUREG/CR-1278.
16. SPURGIN, A.J., LYDELL, B.O.Y., HANNAMAN, G.W. & LUKIC, Y. Human reliability assessment – Systematic approach. *Proceeding Reliability '87 Conference.*
17. DHILLON, B.S. 1982. Stochastic models for predicting human reliability. *Microelectron reliab. Vol 22 No. 3: 491-496.*
18. DHILLON, B.S. 2003. Human and medical device reliability. In *Handbook of reliability engineering.* Hoang Pham (ed). Springer-Verlag, London.
19. PATÉ-CORNELL, M.E. 1993. Risk Analysis and Risk Management for Offshore Platforms: Lessons from the Piper Alpha Accident. *Journal of Offshore Mechanics and Arctic Engineering Vol 115, 179-190.*
20. KRISTIANSEN, S., KOSTER, E., SCHMIDT, W.F., OLOFSSON, M., GUEDES SOARES, C. and CARIDIS, P. 1999. A new methodology for marine casualty analysis accounting for human and organisational factors. *Learning from Marine Incidents Conference.* 20-21 Oct. London SW1.
21. HEE, D.D., PICKRELL, B.D., BEA, R.G., ROBERTS, K.H., WILLIAMSON, R.B. 1999. Safety Management Assessment System (SMAS): a process for identifying and evaluating human and organization factors in marine system operations with field test results. *Reliability Engineering and System Safety 65: 125-140.*
22. RAUSAND, M & HØYLAND, A. 2004. *System reliability theory, models, statistical methods, and applications.* 2nd Ed. John Wiley & Sons, Inc.
23. BS EN 61508-6:2002 *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3.*
24. PETROLEUM SAFETY AUTHORITY (PSA) Norway. 2011. *Risk of Collisions with Visiting Vessels.* [Online: http://www.ptil.no/news/risk-of-collisions-with-visiting-vessels-article7524-79.html?lang=en_US]. Accessed 03.11.2011.
25. TEEKAY SHIPPING LTD, 2006. *Significant Incident Investigation Navion Hispania DP Incident on Njord Bravo 13th November 2006*. Canada.
26. REDMILL, F. & RAJAN, J. 1997. Human factors in safety-critical systems. Butterworth-Heinemann. Oxford.

27. CAREY, M. 2001. Proposed framework for addressing human factors in IEC 61508. Contract Research Report 373/2001, Health & Safety Executive (HSE).

28. CACCIABUE, P.C. 2004. Guide to applying human factors method human error and accident management in safety critical systems. Springer-Verlag London.

APPENDIX

Table A Human factors analysis on collisions of vessels and offshore installations

Case	Abnormal states	Hazardous event	Sensory failure (state ③)	Decision failure (state ②)	Action failure (state ①)
A	• Substitute vessel for the operation • No dynamic-positioning (DP) system on the vessel • First time for the crew to perform such an operation • Adverse weather • Typical configuration of the installation, using spread mooring system	The vessel was asked to move to the weather side	Fail to see the risk of operating the vessel on the weather side in such a situation	Wrong decision to move to the weather side of the installation	Fail to operate the vessel properly: applied 100% of the engine capacity and wrong maneuvering path
		Overloaded engines	Fail to identify the engine overloaded alarms, but recognized that the deck lights went off	Fail to interpret the situation properly and fail to make the right decision (should cancel the operation and move away from the installation)	Fail to operate the vessel properly: reduced the pitch to zero which then led the vessel to be drifted towards the installation
B	• New officer on board, not yet receive proper training • Vessel entering 500 m safety zone • Telephone call for the captain			The captain decided to use the autopilot during the time he took the call	Activating autopilot inside 500 m safety zone
		The vessel was running on autopilot inside the safety zone heading towards the installation	Fail to see that autopilot was engaged	Fail to interpret the behavior of the vessel	Fail to override the autopilot, therefore could not reduce the speed and collision occurred
C	• Entering 500 m safety zone	Violation of procedures regarding watch keeping	Fail to identify the risk or the criticality of operation within 500 safety zone	Fail to decide what to prioritized; captain ordered 2nd officer to prepare for loading	Fail to operate the vessel properly: 2nd officer left the control station
		Bridge was left unattended	The captain fail to estimate the speed, heading and position of the vessel	The captain made a wrong decision leaving the bridge unattended	Fail to control the vessel, resulting in collision

Case	Abnormal states	Hazardous event	Sensory failure (state ③)	Decision failure (state ②)	Action failure (state ①)
D	• Dense fog • Poor visibility • Shift changes when vessel approaching installation	Ambiguous situation, unclear who is steering the vessel	Fail to identify the problem that nobody is really in charge of the control	Fail to make the right decision, to take over the control in time	Fail to control the vessel in time
E	• Entering 500 m safety zone	The vessel was running on autopilot inside the safety zone heading towards the installation	Fail to see that autopilot was engaged	Fail to interpret the behavior of the vessel	Fail to override the autopilot, therefore could not reduce the speed and collision occurred