Improving Safety of DP Operations: Learning from accidents and incidents during offshore loading operations

Yining Dong & Jan Erik Vinnem & Ingrid Bower Utne

Department of Marine Technology

Norwegian University of Science and Technology (NTNU), Trondheim, Norway.

Abstract

The risk caused by DP vessels in offshore marine operations is not negligible, due to wide applications of DP vessels in complex marine operations, and the sharp increase of DP vessel population. The DP accidents/incidents on the Norwegian Continental Shelf (NCS) that have occurred after 2000 indicate a need for improving safety of DP operations, which calls for new risk reduction measures. The focus of this paper is particularly on the offshore loading operations with DP shuttle tanker in offloading from Floating Production Storage and Offloading (FPSO) vessels on the NCS, but the results may be relevant also for other types of DP vessels in offshore oil and gas operations. In the paper, Man, Technology and Organization (MTO) analysis is applied to investigate the causes and barrier failures of nine reported accidents/incidents occurring over a 16-year period (2000-2015). MTO is based on three methods, including structured analysis by use of an event- and cause-diagram, change analysis by describing how events have deviated from earlier events or common practice, and barrier analysis by identifying technological and administrative barriers which have failed or are missing. The results are categorized into technical failures, human failures, organizational failures, as well as a combination of failures. The main finding is that the majority of the accidents are caused by the combination of technical, human and organizational failures. Critical root causes, results of change analysis and barrier analysis, and combination of failures are focused on in the discussion. Recommendations of potential safety improvements are made on the aspects of the assessment of the actual system function, barrier management for marine systems, risk information to support different decision-makings, and the development of an on-line risk monitoring and decision supporting system.

Keywords: Dynamic positioning, complex marine operations, risk reduction measures, MTO analysis

1 Introduction

Offshore exploration and exploitation of hydrocarbons have opened up an era of dynamically positioned (DP) vessels. A DP vessel is by the International Maritime Organization (IMO) defined as a vessel that maintains its position and heading (fixed location or pre-determined track) exclusively by means of active thrusters [1]. A DP system generally consists of three main subsystems, i.e., power system, thruster system and DP control system.

The number of DP vessels worldwide has increased sharply in the past three decades. According to Bierman [2], the number of DP vessels was 65 in 1980 and 150 in 1985. In 2011, the number of DP vessels was estimated to reach 2000 worldwide. The number of DP vessels worldwide in 2015 may reach 3000, according to Chen [3]. There is a wide range of applications of DP vessels in the offshore oil and gas industry, e.g., diving support vessels, pipe-layers, heavy lifting vessels, drilling rigs, subsea construction vessels, platform support vessels, shuttle tankers, etc. The marine operations performed by these DP vessels are different in terms of position excursion tolerance and consequence potential. Large vessels with high thrust and power capacity may pose significant collision risk to adjacent offshore installation in case of position loss. A typical example is DP shuttle tankers during offshore loading operations. Diving support vessels and pipe-layers may pose risk towards personnel (drivers) and assets (pipes being laid) respectively, in case of a position loss. A DP drilling unit must ensure safe disconnection of the Lower Marine Riser Package (LMRP) on top of the Blowout Preventer (BOP) in case of a position loss. The risk caused by DP vessels in offshore marine operations is therefore not negligible, due to the wide number applications of DP vessels in complex marine operations, and the sharp increase of the DP vessel population.

Risk analysis, assurances and management activities of DP vessel in marine operations have traditionally been performed in a qualitative manner. Typical methods include, for example, the failure mode and effect analysis (FMEA) and criticality ranking (FMECA) of the entire DP system, hazard identification (HAZID) and hazard and operability analysis (HAZOP) of operational procedures, well and/or site specific operating guidelines (WSOG/LSOG), independent surveys of the DP system, various testing and FMEA proving trails, hardware-in-loop (HIL) testing of control software, training and certification of key DP personnel, and so on. These are considered as effective activities to mitigate failures of technical systems and increase the reliability of human and operational barriers against DP incident.

However, it is argued by many DP experts and researchers that there is a need for new risk reduction measures [3, 4, 5, 6]. The main reason is that collision still occurs frequently in the offshore oil and gas industry, on not only DP1 vessels, but also DP2 and DP3 vessel. To classify the designed equipment, the IMO MSC Cir. 645 [1] defines three classes, i.e. DP1, DP2 and DP3. For DP class1 position loss may occur given a single failure event. For DP class2, position loss should not occur given a single failure, and for DP class3 position loss should not occur given a single failure including fire and flooding of watertight compartment or fire sub division.

In the period 2000-2010, there were 26 collisions between offshore installation and visiting vessels on the Norwegian Continental Shelf (NCS) [7]. Many of these vessels were DP vessels, and out of the 26, there were 6 incidents which had a major accident potential. The Petroleum Safety Authority (PSA) of Norway has also rang the alarm bell to the industry [7]. In terms of offshore loading operation with shuttle tankers on the NCS, there have been two collisions between shuttle tankers and facilities since 2000. In addition, there have been four near misses (collision events) and seven incidents related to loss of position, with varying degree of severity.

It is actually not the first time that risk reduction measures for FPSO (Floating Production Storage and Offloading) and Shuttle Tanker (ST) collision has been focused on and addressed. Up to 2000, there were several position loss incidents and collisions during offloading operations, especially during tandem offloading between FPSO/FSU (Floating Storage Unit) and shuttle tankers on the NCS, as well as the United Kingdom Continental Shelf (UKCS). Major research activities were performed in a Joint Industry Project (JIP) with participation from Norway, UK and US, giving recommendations to prevent further accidents. Vinnem et al. [8] proposed a risk influencing diagram for collision between FFPSO-ST, with three levels of risk influencing factors (RIFs) in the analysis of FPSO-ST collision accidents, involving operational, organizational and regulatory RIFs. Chen [9] introduced a frequency modelling of collision between FPSO and shuttle tanker in offloading operation. The model is structured in two stages, i.e., the initiating stage and the recovery stage, where the former involves an uncontrolled forward movement of tanker, and the latter involves the recovery actions initiated from the tanker and FPSO to avoid the collision. In terms of recovery action initiated by the tanker DP operator, Chen [9] concluded that tanker DP operators in general need more time to initiate a recovery action than the allowable time windows, i.e., recovery failure is likely due to lack of available reaction time (within typically 45 seconds). Two principle recommendations were proposed to reduce the recovery failure probability, i.e., to provide a longer time window for the operator to initiate recovery action, and/or to provide various kinds of assistance to the operator to reduce the recovery action initiation time. After implementing some of the risk reduction measures, the number of position loss incidents and collision fell sharply in the following five years (2001-2005). During the period, only one position loss incident was reported to PSA.

However, a new DP accident occurred in 2006 and several near misses have occurred in the following years. Due to this, it has been questioned if the improvements made in the early 2000's have disappeared [7] or have not been followed up systematically. DP operation generally involves a complex human-machine system, including a DP control system, reference system, power system, thruster system, and DP key personnel. To improve the safety of DP operation thus requires that all major elements in the human-machine system should be taken into account. Verhoven et. al. [10], Chen [9] and Vinnem et.al. [8] highlighted that risk modelling and analyses of DP operations should include not only technical failures, but also human operational failures, and interactions between these two types of failures. The potential improvements were considered from a broad perspective with emphasis on human and organizational contributions. When searching for new risk reduction measures, the reason why the improvement vanished after implementing for 5 years should be also concerned, i.e., the problems of the safety management systems to maintain the performance of existing safety barriers (i.e., physical/technical barriers, human barriers and organizational barriers), and the emerging of new risk.

There are also challenges to DP accident prevention, which are attributed to the weaknesses of the risk assessment approach and the complexity of the DP system. The DP system is obviously a complex system, as it consists of hardware, software and power systems. It is challenging to assess the risk for a complex system. For example, conceptually, software reliability is almost impossible to compute, since many of the aspects of the software which influence the reliability are of qualitative nature and not directly measurable. Nevertheless, it has to be estimated, e.g., by expert judgement. In addition, FMEA inherits some important limitations [11]. First, it considers hazards arising from single-point failures and will normally fail to identify hazards caused by combinations of failures. Second, the actual system function could be overlooked, since the interactions between subsystems are not assessed in FMEA, when failure modes are reviewed separately in each subsystem. Therefore, some uncertainties are unavoidable in the system due to the complexity of the DP system and limitations of this risk assessment approach. Due to the uncertainties, it seems to be very important that DP operator should maintain or increase awareness of barrier status or be provided with more effective guidance to be taken if barriers or critical functions are degraded. Indeed, the DP operator plays a critical role in terms of the safety of DP operation. The challenge is that the decision about risk mitigating actions currently have to be made rapidly to avoid collision in the case of position loss. With regard to new risk reduction measures, the recommendations should be targeted at how to provide improved decision-making support to DP operators.

The objective of the paper is to provide an up-to-date analysis of DP accidents and incidents, using the Man, Technology and Organization (MTO) analysis method. Nine incidents on the NCS are investigated occurring over a 16-year period (2000-2015). The emphasis is on root causes and barrier failures, as an input to making decisions about risk reducing measures. The focus is particularly on the offshore loading operations with a DP shuttle tanker in offloading from FPSO vessels on the NCS, but the results may be relevant also for other uses of DP vessels in the offshore oil and gas industry.

The results of the analyses are categorized into technical failures, human failures, organizational failures, as well as a combination of failures. The main finding is that the majority of the accidents are caused by the combination of technical, human and organizational failures. Critical root causes, change analysis, barrier analysis, and combination of failures are focused on in the discussion. Recommendations of potential safety improvements are made on the on the aspects of the assessment of the actual system function, barrier management for marine systems, risk information to support different decision-makings, and the development of an on-line risk monitoring and decision supporting system.

The paper is structured as following way: Section 2 provides the explanation of the important concepts using in the analysis of DP accidents/incidents. The purpose and scope of the accident analysis, together with a description of the MTO analysis, are stated in Section 3. Section 4 offers an overview of DP position loss and collision on NCS (2000-2015). Section 5 presents the results of MTO analysis, following by a discussion based on the results in Section 6. Recommendations of potential safety improvements can also be found in Section 6. Finally, conclusions are summarized in Section 7.

2 Important Concepts

2.1 Accidents and Incidents

In the paper, both *accident* and *incident* are chosen for use. Rausand [11] defines an *accident* and a sudden, unwanted, and unplanned event or event sequence that lead to harm to people, the environment, or other assets, while *incident* is defined as an unplanned and unforeseen event that may or may not result in harm to one or more assets. According to the definitions, an accident is a special case of incident: that is, an incident that results in harm to assets (including people and/or environment). In addition, the term *near miss* is defined as: unplanned and unforeseen event that could reasonably have been expected to result in harm to one or more assets, but actually not. A near miss is also called *a near accident*.

2.2 What are Root Causes?

Effective prevention of accidents requires a proper understanding of their causes. Several approaches to accident causation have been used throughout history. In earlier times, many accidents were considered acts of God, meaning that nobody could be held responsible for the accident and that there was no possibility of preventing the accident. This view has few supporters today. In the 1920s, studies of accidents suggested that accidents were caused by individuals, who were more disposed than others to being injured [12]. It was claimed that these individuals had inherent characteristics that predisposed them to a higher probability of being involved in accidents. This theory, called the *accident proneness* theory [13], is very controversial, but it is still influencing in, for example, accident investigations by the police. In addition, there are other popular accident theories, such as scientific safety management in 1930s, system theory in 1940s, quality management in 1960s, and safety culture in 1990s. On a general level, the causes and contributing factors are often classified as follows [11]:

- *Direct causes* are the causes that lead immediately to accident effects. Direct causes are also called immediate causes or proximate causes, as they usually result from other, lower –level causes.
- *Root causes* are the most basic cause of an accident/incident, i.e., a lack of adequate management control resulting in deviations and contributing factors. Root causes are also called *underlying causes*.
- *Risk influencing factor* (RIF) is an aspect (event/condition) of a system or activity that affects the risk level of this system/activity.

Rausand & Høyland [11] pointed out that a root cause is the cause that, if corrected, would prevent recurrence of this and similar problems. Hence, every event can be unique and the direct causes often differed, but the underlying causes should be identified as recurring problems.

2.3 Barrier Management

Barriers should prevent undesired events or reduce consequences should such events occur. The main purpose of barrier management is to establish and maintain the necessary safety barriers. It includes the processes, systems, solutions and measures needed [14]. The PSA has emphasized the need to develop barrier strategies during the last few years. An updated barrier memo was recently issued in March 2017, where the following definitions are stated [15]:

- *Barrier function*: the task or role of a barrier.
- *Barrier elements*: technical, operational or organizational measures or solutions, which play a part in realising a barrier function.
- *Performance requirements*: verifiable requirements related to barrier element properties to ensure that the barrier is effective.
- *Performance influence factors*: conditions which are significant for the ability of barrier functions and elements to perform as intended.

In the updated version of barrier memo, the barrier elements have been distinguished into technical barrier elements, organizational barrier elements and operational barrier elements.

- *Technical barrier elements:* equipment and systems, which constitute a part of realising a barrier function. (What equipment shall be used?)
- *Organizational barrier elements:* personnel with defined roles or functions, and specific competences, which constitute a part of realising a barrier function. (What shall be done?)
- *Operational barrier element:* the actions and activities that personnel have to perform to constitute a part of realising a barrier function. (Who is doing it?)

Based on the barrier element definitions, it is imperative to have good answers to the question "who does what with what equipment in failures, hazard and accident situations?" In addition, the definitions of *robust barrier*, *risk*, *risk picture* and *risk management* are also provided [15].

Compared to topside systems, the emphasis on barrier management for marine system has so far been much more limited. A part of the goal in this study is to review the accident scenarios to address the effectives of barriers and critical functions by identifying [16]:

- Barriers that are in place to prevent occurrence or escalation of an accident.
- Performance of the barriers during accident scenarios including equipment effectiveness, human decision making and actions taken to restore the barrier or critical functions.

- Opportunities to strengthen existing barriers or create additional barriers to reduce the likelihood of potential accident scenarios or reduce their consequences.
- Opportunities to improve human performance aspects of barrier management by increasing awareness of barrier status or providing more effective guidance to be taken if barriers or critical functions are degraded.

3 Method – Accident Analysis

3.1 Purpose and Scope

Accident and incident analysis can be performed with different purposes. Sklet [17] stated a couple of them: (i) to identify and describe the true course of events (what, where, when), (ii) to identify the direct and root causes/contributing factors of the accident (why), and (iii) to identify the risk reducing measures to prevent future, comparable accident (learning). (iv) to investigate and evaluate the basis for potential criminal prosecution (blame), and (v) to evaluate the question of guilt in order to assess the liability for compensation (pay). The analysis in this paper is mainly aimed at the first three purposes.

According to Rasmussen [18], accidents are caused by loss of control of physical processes that are able to injure people, and/or damage the environment or property. The propagation of an accident course of event is shaped by the activity of people, which can either trigger an accidental flow of events or divert a normal flow. Many levels of politicians, managers, safety officers, and work planners are involved in the control of safety by means of laws, rules, and instructions that are established to control some hazardous, physical process. The socio-technical system actually involved in the control of safety is shown in Figure 1.

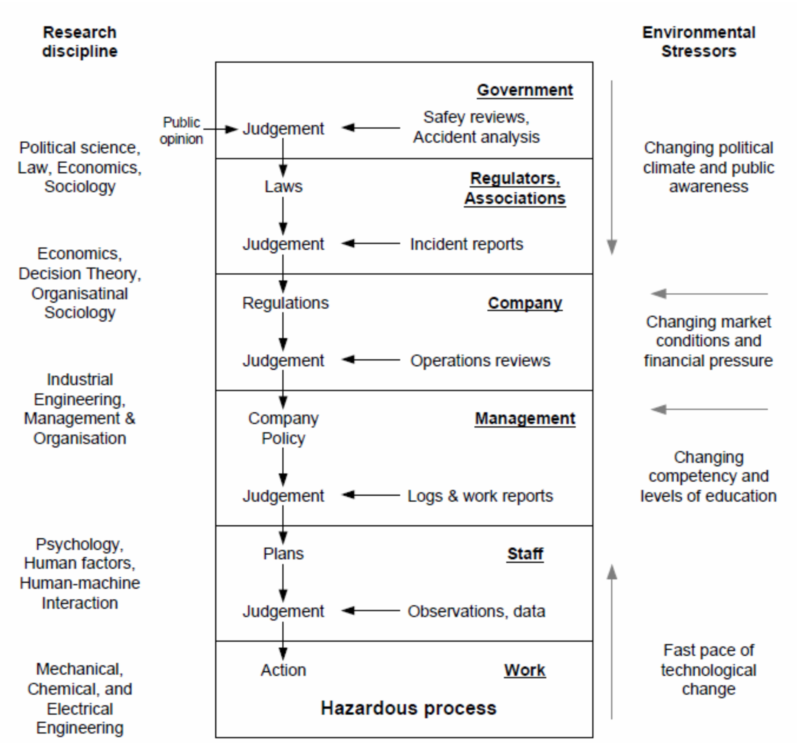

Figure 1 The socio-technical system involved in risk management. (Adopted from [18])

As illustrated in Figure 1, different levels of the socio-technical system involved in risk management generally include (1) the work and technological system, (2) the staff level, (3) the management level, (4) the company level, (5) the regulators and associated level, and (6) government level. Ideally, the accident analysis should cover all these levels. However, the scope of most of the state-of-the-art accident analysis methods is limited to level (1) – (4). Even though some methods may be used to analyze events influenced by the regulators and the government, the results of the analysis is to a large extent determined by the experience and practical judgement of the analyst, rather than the outcomes from formal analysis methods. In addition to the limitations of the methods, the scope of the analysis should also be defined considering the available information in the incident reports. This paper focuses on investigation reports from PSA. Most of the investigations were stopped at the company level. Therefore, the scope of the analysis in this paper is on level (1) – (4) of the socio-technical system.

3.2 The MTO Method

There are a number of accident models to support accident analysis. Each accident model has its own characteristics based on what types of casual factors it highlights [19]. Rausand [11] summarized the development of accident models into three phases. The first accident models were very simple and attributed accidents primary to single technical failures. A bit later, human factors and human errors were included in the models. Current accident researchers realize that systems also consist of societal, organizational and environmental elements in addition to technology and individuals, which should all be integrated into the accident model [20]. Based on the purpose and scope of analysis, the MTO method is used to perform the accident analysis. The MTO analysis is a well-established approach that considers human, technical and organizational factors either alone or in combination.

MTO analysis was originally developed as a technique for the investigation of accidents and incidents in the nuclear industry. In the past a few decades, the usage of the MTO analysis has made contributions to other sectors, as well. It is the main investigation technique used by PSA for investigation of accidents on the NCS. Meanwhile, it has also been recommended for analytical purposes to acquire a brief summary of the accidents and incidents [21].

There are different perspectives in terms of the description of MTO analysis. Vinnem [21] and Sklet [17] describe that MTO is based on three methods, including structured analysis by use of an event- and cause-diagram, change analysis by describing how events have deviated from earlier events or common practice, and barrier analysis by identifying technological and administrative barriers which have failed or are missing. Rollenhagen [22] states that MTO mainly consists of three levels. On the basic level, it is a chain of events, where the breached and/or missing barriers (administrative and physical/technical) are identified. The second level describes causes and conditions allowing the events at the first level to occur. The third level focuses on influences from what is called the safety management system level. A MTO diagram (See in Figure 2) has been developed to illustrate how the MTO method is applied for the incident analysis in this study, and the viewpoint is basically the same as the description given by Vinnem [21] and Sklet [17]. As shown in Figure 2, the MTO analysis is based on three elements:

1. A structured analysis by use of an event and causal diagram to describe the event sequence of the accident and incident. Immediate and root causes are identified and positioned vertically in relation to the events in the diagram. While the immediate causes are in general related to technical and human failures, the root causes mostly represent the organizational failures.

2. A change analysis describing how events have deviated from earlier events or common practice. Normal situations and deviations are illustrated in the diagram, shown in Figure 2.

3. A barrier analysis identifying technical, human and administrative barriers that have failed or are missing. Missing or failed barriers are represented below the events in the diagram.

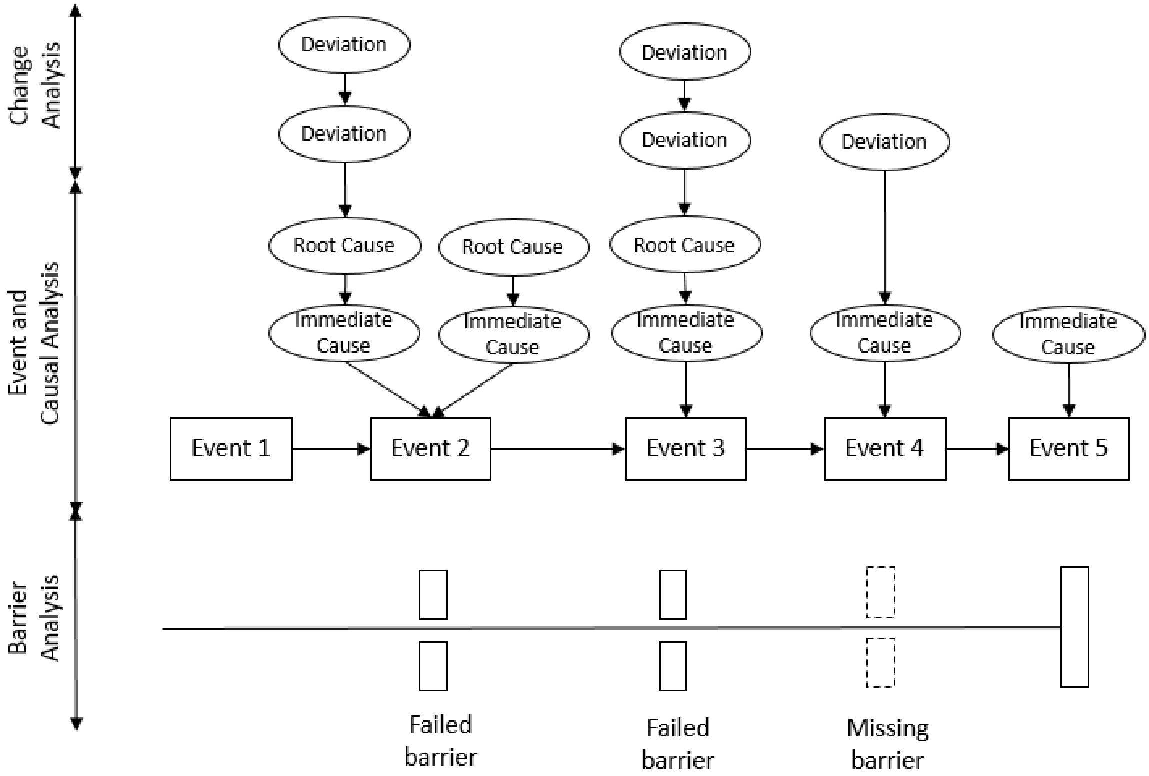

Figure 2 A MTO diagram that is used in the incident analysis

The basic questions in the analysis are [11]

- What could have prevented continuation of the accident sequence?
- What could the organization have done in the past to prevent the accident?

4 An Overview of DP Position Loss and Collisions on NCS

On the NCS, regulations for petroleum activity demand that incidents related to permanently installed installations are reported to the PSA. The PSA (before 2004, part of Norwegian Petroleum Directorate, NPD) has been collecting data on incidents and reports on condition deviations for installations on the NCS since the mid-1970s, with the aim to be used for statistical and analytical purposes. Vessel owners, DP equipment vendors, and oil companies may also have position loss data for DP vessels. However, such data are normally not open to the public, and can be scattered among various sources, e.g., WSOG (Well specific Operational Guidelines) logging, DP watch checklist, or in various SYNERGI databases which is a widely used incident reporting system on the NCS.

In this study, we have collected nine available incident reports from PSA, covering from the early of 2000 to the end of 2015. An overview is presented in Table 1. As shown in Table 1, the last incident took place in 2011. PSA has confirmed that after the incident in 2011 until the end of 2015 no DP accidents and incidents were reported to PSA. The information in the investigation reports is confidential. Therefore, the installations and shuttle tankers are anonymous in the following analysis.

Table 1 Overview of FPSO/Shuttle tanker collision and drive-off accidents/incidents (2000-2015)

					Type of incident/accident			
Case	**Year**	**Sector**	**Offloading**	**Phase**	**Drive-off**	**Collision**	**Other**	**DP class**
1	2000	Norway	Tandem offloading	Disconnection		X		DP2
2	2004	Norway	Tandem offloading	Loading	X			DP2
3	2006	Norway	Tandem offloading	Connection		X		DP2
4	2007	Norway	Tandem offloading	Loading	X			DP2
5	2008	Norway	Loading buoy	Loading			X	DP2
6	2009	Norway	Loading buoy	Loading			X	DP2
7	2010	Norway	Loading buoy	Loading	X			DP1
8	2010	Norway	Loading buoy	Approach			X	DP2
9	2011	Norway	Tandem offloading	Loading			X	DP2

4.1 Loss of Position

Relative motions between FPSO and shuttle tanker, which are termed as excessive surging and yawing events, are identified as the “failure prone situation” in tandem offloading [9]. Surging is synchronous relative surge motions between shuttle tanker and FPSO, while yawing is signification mean heading differences and asynchronous relative yaw motions between shuttle tanker and FPSO.

Overall, there are two basic failure modes of loss of position during offloading operation, namely drive-off and drift-off [10].

- *Drive-off* Failures onboard of shuttle resulting in active thruster forces driving the shuttle tanker away from its target position. The drive-off may involve, false position information, DP control failures, thruster failures and operator errors as primary or secondary causes. Principally, a drive-off can be in any direction.
- *Drift-off* Failures onboard of shuttle tanker resulting in deficiency of thruster forces in relation to the environmental forces, e.g. partly or total blackout. The shuttle tanker is drifting off its position due to insufficient thruster forces.

The nine accidents and incidents collected from PSA are all focused on the drive-off scenario, because this is the primary concern. It does not imply that drift-off scenarios have not occurred during this period. Note in principle, drive-off can be forward, astern, or side way and it is the drive-off forward that may lead to collision. When it comes to the causes for drive-off, both tandem-offloading and loading buoy are taken into account. However, the potential consequences of drive-off given the recovery actions fail are different.

With regard to the consequence (refer to the sixth column in Table 1), the drive-off accidents/incidents collected from PSA are divided into three different groups: collision, drive-off and other events. The division of the incidents and accidents into these three groups is its concern about the performance of the barrier functions, i.e. to prevent loss of position, to arrest vessel movement, and to prevent collision. Other events are the events that could have resulted in a drive-off but the drive-off is avoided due to early detections by operators or functions by the DP system. Drive-off are the events that the shuttle tanker has had an excursion beyond the operating limits, but collision was avoided because of successful human interventions. When human interventions were failed in the scenario, the shuttle tanker finally collided on the FPSO or offloading station, which it ended up with potential human loss, asset loss or even environment damage. Even if the ‘other events’ and ‘drive-off’ could also be associated with asset loss or environment damage, the severity of the consequence is negligible compared to collision.

4.2 Offloading Systems

In the fourth column in Table 1, accidents and incidents are linked to the type of offloading systems. There are different types of offshore loading systems that are used or have been used in Norway, mainly including (1) tandem loading from FPSOs to shuttle tankers, (2) loading from buoys as ALP (Articulated Loading Platform) or SPM (Single Point Mooring), (3) Draugen FLP (Floating Loading Platform), UKOLS (Ugland-Kongsberg Offloading System) and (4) STL (Submerged Turret Loading) or STP (Submerged Turret Production). As illustrated in Table 1, there are two collisions, which both occurred during tandem offloading between FPSO and DP shuttle tanker. Regarding the remainder of position loss incidents, three of them occurred during tandem offloading and four of them occurred during loading from buoys. The incidents for loading buoys are included because the DP incidents for these systems may also be relevant for tandem offloading from FPSO.

4.3 Operational Phases and Context

Offloading operation with shuttle tanker from FPSO can in principle be summarized into five operational phases (related to the fifth column in Table 1), from the point of view of the DP tanker [9]:

- Approach: tanker approaches i.e., FPSO stern and stops at a wanted distance.
- Connection: massager line, hawser and loading hose are connected.
- Loading: oil is transferred i.e., from FPSO to tanker.
- Disconnection: manifold is flushed, and loading hose and hawser are disconnected.
- Departure: tanker reverses away from i.e. FPSO stern while sending back hawser messenger line, and finally sails away from field.

The operational phases for offloading from loading buoys are in principle the same as for the tandem offloading.

The loading phase occupies more than 90% of the total duration of a loading cycle, and it is therefore not surprising that six out of the nine incidents in Table 1 occurred during the loading operations.

In addition, it should be noted that with respect to the actual operation of the DP tanker in off-loading (Level (1) in the socio technical system illustrated in Figure 1), there is a distinction between normal operation, where the DP operator is passively monitoring, and response to abnormal occurrences, where the DP operator is required to perform rapid detection, decision-making and implementation of mitigating actions, as discussed by Chen [9] and Hogenboom et al. [23].

4.4 DP Class

In Norwegian petroleum industry, activities regulations were officially issued in 2002 [24]. Since then, Class 2 has been the minimum requirement for tanker vessels when loading from facilities handling hydrocarbons, subsea loading and offloading installations. In some cases, when the tanker is moored or anchored to these installations, Class 1 might be also accepted if the distance between the facility/facilities in question is 2.5 km or more, if not class 2 should apply. In addition, Class 1 is acceptable for loading operations from buoys. Even so, risk of position loss is intrinsic to all DP vessels [3]. A position loss may happen on DP1 vessels, as well as on DP2 and DP3 vessels.

5 Results from the MTO Analysis

The details of the results of the MTO analysis are summarized in Table 3, which contains event sequences, immediate causes, root causes, deviations and failed or missing barriers. Based upon the information given in Table 3, the results are summarized into four categories that are technical failures, human failures, organizational failures and combination of failures.

The basis of MTO analysis is mainly the available incident investigation reports, which were prepared by field operators/or regulators. It should be noted that an incident investigation report might be inaccurate or incomplete, even when prepared by experienced investigators. In order to compensate for the inaccurate and incompleteness of the collected data, discussions about the accidents and incidents were arranged by involving a group of marine engineers, who has background in DP FMEA, marine cybernetics, offshore marine operations, and offshore risk assessment including DP marine operations. Many valuable comments on what have been missing in the investigation reports were collected during the meetings, which have also been used as the information to ensure the validity of the conclusions that will be drawn from this study. Ideally, it would have been possible to contact investigators and clarify outstanding issues; however, this is not feasible in practice in the offshore industry with rapid job changes, shift rotations, etc.

When analysing the accidents, the basis for the MTO method is that human, technology, and the organization are equally important when analysing accidents [17]. In this study, the category of technology (T) includes the hardware, software and design of the DP systems. The identification of technical failures are aimed at the subsystem level (i.e., positioning control system, sensors, electrical power systems and thrusters and propulsion), and the results are presented in Section 5.1. The category of Man (M) comprises the DP operators at the sharp end, design teams and maintenance teams. The results can be found in Section 5.2. When identifying human failures, the attention is essentially given to the human actions and their interaction with technical failure events. Furthermore, the category of the organization comprises management, vessel owners, verification organization, vendors, supervisory authorities and class providers. The number of accidents and incidents analyzed, where organizational failures were present is illustrated in Section 5.3.

5.1 Technical Failures

The results of MTO analysis show that technical failures appeared in the 9 accident and incidents, including software failure of DP control system, failure of single main diesel generator, failure of position reference system, failure of auxiliary engine, failure of main switch board, failure of CPP (controllable pitch propeller) and so on. The number of accidents and incidents, where technical failures were present, is shown in Figure 3. The DP system is divided into several sub-systems (such as positioning control systems, sensors, thruster and propulsion, as well as electrical power system) in accordance with [25]. It is worth noting that some accidents and incidents were caused by a combination of technical failures in different sub-systems, i.e., the combination of wrong DP logic (software failure in DP control system) and non-optimal setting of main propeller (failure in thruster and propulsion), the combination of error in gyro sensors (failure in gyro-compass) and the missing barrier and failure in the DP control system.

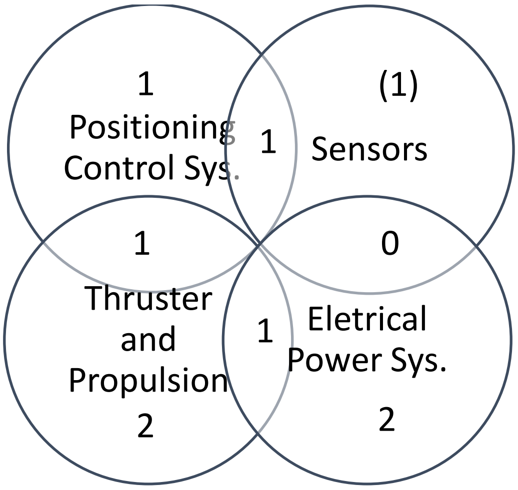

Figure 3 Number of accidents and incidents analyzed where technical failures were present in different subsystems.

5.2 Human Failures

The human actions and their interaction with technical failure events can be categorized into the following three categories:

- Initiating action – an action initiates a failure event in the system.
- Response action – an action responds to meet system demands, typically under technical failure vents or special external situations. It may save or worsen the situation or cause a transition to another event.
- Latent action – an action influences (but does not directly initiate) the technical failure. E.g. maintenance action, and/or the above two types of human actions.

In addition to different human actions, different roles are also taken into account in terms of human failures. DP operators, designers and maintenance workers have been particularly considered. Figure 4 illustrates the number of accidents and incidents where fault actions of different persons were present. The failure of designers is based on the assumption that designers take the main responsibility for safety design. Both failure of designers and failures of maintenance workers were involved in the accident with a relatively high portion.

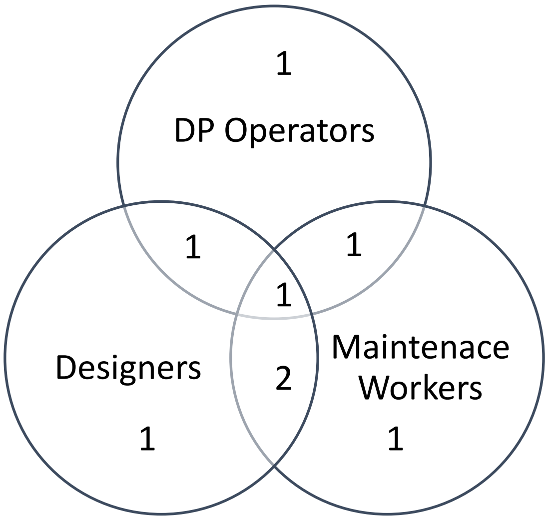

Figure 4 Number of accidents and incidents analyzed where human failures were present.

5.3 Organizational Failures

There are different organizations (see Figure 5) involved in the DP system accidents and incidents, such as the ST (operating) organization, the verification organizations, vendors and authorities. It seems like ST organization is a dominant contributor, when 7 out of 9 accidents and incidents were contributed by lacking of training, lacking of operational procedure, lacking of inspection regime, etc. The verification organization is also involved in the accident and incidents, if any design failure was not identified during verifications. In 2 out of 9 accidents and incidents, vendors were also taken account, when there were improper settings of equipment and insufficient support after new installations. Even if it is not highlighted in Figure 5, supervisory authorities and class providers also have obvious responsibilities for safety management of marine operations involving DP systems.

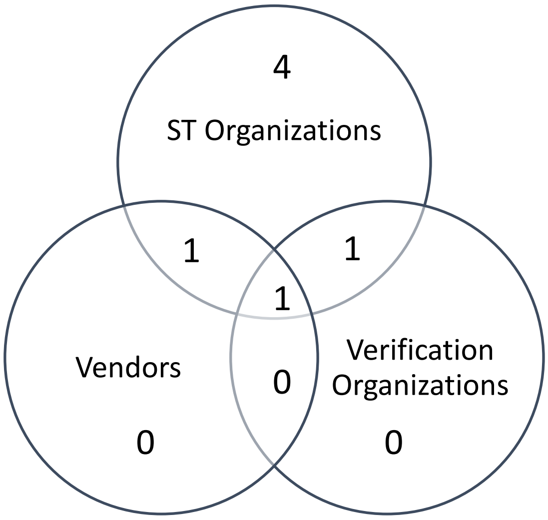

Figure 5 Number of accidents and incidents analyzed where organizational failures were present.

5.4 Combination of Failures

From the results, we see different types of failures, i.e., technical failures, human failures and organizational failures. Each type of failures can be subdivided into different groups, depending on which subsystem the technical failure emerged, who performed the task, and which organization was involved. However, few accidents and incidents were contributed to a single type of failure. It means the accidents and incidents are normally resulted from a combination of technical, human and organizational failures. This accounts for 7 out of 9 accidents and incidents analysed in this study.

In each subdivision group, there are also combinations of failures. In terms of technical failures, 3 out of 9 accidents and incidents were due to the combination of technical failures triggering from different subsystems. If we define failures made by designers and maintenance personnel as latent failures, 3 out of 9 accidents and incidents were caused by the combination of operator failures and latent failures. In addition, the combination of different organizational failure were present in 3 out of 9 accidents and incidents. The combination of failures in the risk and barrier management of DP operations is what should be highlighted.

6 Discussions of the Results

6.1 Validity of Analysis

The MTO analysis was performed based on nine DP incidents investigation reports. The sample size is relatively limited, since there were luckily few incidents. Still, the findings are valid because the focus is on the root causes, which represent the weaknesses in the general and safety, health and environment (SHE) management systems of the company. To enhance safety in DP operations, attention should be given to the root causes, so that the recommendations will not only affect the probability of a recurrence of the particular (drive-off) event in question, but the general safety level of the company.

A larger data set could be available if incidents from other DP operations were included. If so, the advantage with the present data set would be lost, in that the present data set all incidents apply to shuttle tankers in off-loading mode from either FPSO of loading buoy.

6.2 Incident Analysis based on the MTO Method

The MTO diagram is illustrated in Figure 2. Based upon the investigation reports, the first task was to establish event sequences for each accidents and incidents. The focus of the analysis is on the events leading to a drive-off. In some investigation reports, the event- and cause diagram can be found; however, it is missing in a number of them. MTO analysis is only enclosed in two investigation reports, although it has been used as the main investigation technique by PSA for investigation of accidents on the NCS. To identify the events, information was searched from the incident descriptions stated in the incident reports, the BLOM Positioning Monitoring System (PMS)[1] data and DP print-out. In addition, group discussions have been used to compensate for the missing information. A detailed description of each event can be found in the second column in Table 3. The events are numbered to display the sequence of the events. While each event sequence is composed by a series of different events, they are labelled with capital letters, A-I.

Once the event sequences were established, immediate causes and root causes were identified in relation to the events. With regard to the immediate causes (third column in Table 3), about 90 percent of the information is found from the cause analysis enclosed to the investigation reports or other

[1] BLOM PMS system is a position monitoring system, which is installed on shuttle tankers. It has a position data log, e.g. tanker position and speed.

contents in the investigation reports. The remaining is based on the information collected from the group discussions. While, the root causes (fourth column in Table 3) are about 60 percent from the investigation reports and 40 percent from the group discussions, respectively.

In terms of the change analysis, it has been the challenging part in the MTO analysis due to lack of information in the investigation reports. The change analysis can only be found in the reports when MTO analysis was applied in the original investigation. Otherwise, terms such as “change”, “deviations”, and “facts” are seldom utilised in the writing of the investigation reports. As a change analysis is used to identify how events have deviated from earlier events or common practice, the involvement of the analysis in an investigation can be beneficial for an organization’s ability to learn from accidents and incidents. For instance, to determine the effects of each of these deviations, to identify the main system vulnerabilities caused by the deviations, to determine the risk influence of each deviations, and to identify which new safeguards and/or other precautions are necessary to control the risk impacts. Deviations are summarized in the fifth column in Table 3. Last, but not least, a barrier analysis is applied to identify technical, human and administrative barriers that failed or are missing. Missing or failed barriers are represented in the last column in Table 3. It was recognized that there is insufficient attention to the barrier concept during accident investigation. Barrier analysis was not included in 4 out of 9 incident investigation reports. For the incidents lacking of information, barrier analyses were performed based on group discussions and expert judgement. Based on the findings from the MTO analysis, further discussions are given in the following sections. To analyse the results, the root causes, deviations and barrier failures identified in the MTO analysis are extracted from Table 3 and summarized in Table 2.

6.3 Critical Root Causes

It shows that the root causes cover a broad perspective, including the weaknesses in hardware and software design, ergonomics, maintenance activities, management of work, training, procedures, communications and risk management. All the root causes seem critical to prevent drive-off accidents and incidents. Many of these have been mentioned by previous studies [9] [26]. However, we have found that some root causes are related to the management perspectives, such as management of work, communication and risk management. For instance, in one collision accident, poor communication among Engine Officers, heavy workload and a large amount of administrative work, and deficiency in design (mainly due to unintended cross connections between switchboards were not discovered by any of the FMEA tests during verifications) were identified. This points to the prevention of DP accidents which should be addressed with not only technical improvements and human factors, but also with a management perspective. This has been not really focused on as a need in the offshore industry; however, some research work has been performed in health care for instance, focusing on system weaknesses as contributing causes of accidents. It has been concluded that system weakness plays an important role in accident evolution [27]. A system weakness here is broadly defined as a deficiency in system management that has given or may give rise to an incident/accident.

6.4 Change Analysis

Regarding the change analysis, the results indicate the need to provide adequate information to the design team and other personnel, when a new installation or a new change in the offloading configuration are demanding. Moreover, it shows that the activity consequence risk is not thoroughly assessed to support operational decisions for DP operations, for instance, abnormal settings of main propeller during installation; Artemis Mk V was configured with a wrong frequency update mode after two verification tests. According to [28], the *activity consequence risk* is in principle an update of the site-specific average risk information related to the activity that is going to be performed and what effects this activity will have on the long-term risk level for the facility. The results also show that the information of time-dependent action risk is lacking to support execution decisions, for example, in one of the cases, Engine Officer decided to continue the voyage without running any separators in the fuel system. *Time-dependent action risk* is to express what the risk right now to assist in assessing an ongoing activity or operation. Yang and Haugen [28] described that it is a measure of risk subject to safety critical operating parameters against operating limits while doing one activity or activities.

6.5 Barrier Analysis

There are a number of missing barriers, such as missing test regarding system integrity after new installation, missing barrier in Gyro for rejecting of incorrect latitude and speed compensation and missing barrier to protect UPS from transient spike, etc. While many of the missing barriers are technical barriers, it shows that the design of barriers is limited by not only the knowledge and experience, but also the design standard or guidance. This indicates a need for a good reporting system to continuously improve the safety design. Chen and Nygård [3] pointed out that the incident reporting scheme in the industry at present has some disadvantages, such as it does provide position loss frequency. Regarding the problem, they have recommended an alternative DP incident data reporting scheme which combines both incidents and corresponding DP operational time.

Based upon the results, it also shows that some necessary performance requirements are not well defined for the concrete operational and organizational barrier elements, as well as for the technical elements in DP operations. For instance, clear requirements for the tasks of hired Captain were lacking (see Acc. & Inc. B in Table 3), in which case the tasks are the operational barrier elements and hired Captain is the organizational barrier element. Furthermore, lack of a well-planned maintenance inspection regime, considering maintenance intervals and inspection routines, are identified in several accidents and incidents. This shows that factors that can significantly influence the performance of the technical, or maybe organizational and operational as well, barrier elements need to be identified and handled adequately.

Finally yet importantly, training is still essential in order to strengthen DP operators' competence. According to [15], the personnel must know and understand their role in the barrier functions in order to ensure that a barrier function is carried out effectively.

6.6 Combination of Failures

From the results, it was found that no accidents/incidents were a result from single technical failure or human action, while 7 out of 9 accidents and incidents were due to a combination of technical, human and organizational failures. Accidents and deviations have been considered as symptoms of the underlying SHE problems in the organization and the technical systems [19]. The idea is that the identification and amelioration of these basic causes will have lasting effects on the SHE level. Latent failures and root causes are very often used in the research literatures to label the underlying problems. Reason [29] found that the latent failures will overcome the system's defences and produce accidents, combined with local triggering factors in the work system. Moreover, Rasmussen [30] defined a so-called *fallacy of the defences-in-depth philosophy*, which he explained that many barriers must fail before the system shows obvious signs of reduced safety. An accumulation of such latent errors can in combination with a sudden disturbance result a catastrophic event. Perrow [31] draws the attention to the contradictions in applying a multiple-barrier safety philosophy. He argues that the high-technology systems involving in major accident risks have become more complex and opaque and thus more difficult to operate and maintain. Indeed, there is an inherent difficulty in identifying and quantifying every important causal link [32].

For each type of failure, there are also combination of different subgroups of failures. Among the accidents/incidents, 8 out of 9 were contributed by latent failures (made by designer/maintenance personnel), while three of them were due to the combination of operator (initiating or response) action and latent failures. To propose safety barriers, we may need to subdivide the latent failures for the combination of subgroups of failures. For instance, Ternov and Akselsson [27] distinguished between two types of latent failures: process control latent failures and interactional latent failures. However, the proposal was made particularly for the safety issue of health care. How to subdivide the latent failures in DP operations and the benefits of it can be a topic for our future research work.

6.7 Improvement Potential

Focus on actual system function based on design objectives

Nowadays, risk assessment and verification of DP systems are focused on technical reliability, and the main effort is centred on design and demonstration of redundancy in order to protect against component failures. In this study, we observed that all the accidents and incidents, except one case, involved a shuttle tanker, which is designed with DP 2 station keeping capabilities. (In one exceptional case, the incident involved a vessel with DP 1 station keeping capability and was mainly caused by a failure in position reference system.) According to IMO, loss of position may occur in the event of a single failures are on DP 1 vessel. Nevertheless, all of the other eight losses of position due to single failure or combination of failures are under DP 2 station keeping capacities, which means that they violated the regulations or DP classifications.

It should be noted that a reliability perspective cannot be treated as total coverage of safety. Actual system function should be assessed according to the design objectives, even though regulations and DP classifications focus on component failures, single failures and so forth. A recent study [33] has also demonstrated that the reliability-centred approaches, such as the FMEA analysis, sea trail and hardware-in-the-loop testing, are insufficient and that their view on safety is too narrow. While safety constraints can be violated in a number of manners other than component failures for DP systems, a new approach needs to be considered to complement the currently applied methods. For instance, Rokseth et.al [33] present how a system theoretic process analysis (STPA) can be performed for the risk analysis of maritime operations based on a case study of a generic DP system. There may also be other alternatives in addition to STPA, but STPA has been proposed for this purpose by several authors, such as Rokseth et.al [33] and Abrecht and Leveson [34]. The main advantage of the STPA approach is that a conceptual link between local scenarios and potential system losses is provided, where potential consequences of scenarios can be evaluated at a local level rather than on the system level during further test and verification activities. This reduces the context space, such that the confidence gained from verification activities is enhanced. Furthermore, STPA is a hazard analysis technique based on control theoretic principles, which provide an integrated system view.

Barrier management for marine systems

This study indicates the need for more attention on barrier management for marine operations, particularly DP operations. The core of barrier management is to establish barrier performance requirements. First priority is to select technical, operational and organizational solutions that reduce the likelihood for failure, hazard and accident situation to occur. In addition effective barriers shall be established to identify failures, hazard and accident situations and limit the development of these into accidents. The barrier functions are often handled by technical barrier elements only, but in a significant numbers of barrier functions the technical barrier elements have to be activated or handled by personnel. The personnel and the actions they have to perform to ensure that a barrier function effectively are carried out must be identified. In other words, the organizational and operational barrier elements must be identified. According to Barrier Memo (2017) [15], it is imperative to have good answers to the questions “What do DP operators do with which part of the DP system in failure, hazard and accident situations?”

Necessary performance requirements have to be defined for the concrete operational and organizational barrier elements as well as for the technical elements, like the example of the hired Captain (see Section 6.5 Barrier Analysis). Factors that can significantly influence the performance of the technical, operational or organizational barrier elements shall be identified and handled adequately. The personnel must know and understand their own role in the barrier functions, while training and practices are essential.

At the same time, it is also admitted that safety cannot be guaranteed only by reacting. It is equally important to look ahead, to identify potential new risks, and then to devise barriers against them [35]. As shown by the accidents, vulnerabilities can be introduced into DP systems during installation, commissioning, operation or maintenance, due to errors or inadequacies. For instance, failures associated with maintenance is one of the major causes underlying drive-off accidents and incidents. Therefore, safety barriers should be developed and integrated in improved technological solutions, work procedures and organizations, as well as workplace designs. It is also necessary to establish a close cooperation between safety experts and designers/engineers.

Risk information to support different decision-makings

The results show the need for improvements related to decision making in different levels of organizational hierarchy, not only the work-system level, but also decisions made by designers, planner, etc. and top management decisions at the strategic level. Meanwhile, complexity in operations, software systems, sub-systems and components is increasing and current decision support systems are insufficient [36]. To achieve a better decision-making, Yang and Haugen [28] distinguish decision scenarios into strategic decisions, operational decisions, instantaneous decisions, and emergency decisions. This forms a basis for discussing the different role risk and risk assessment plays in these decisions. In terms of risk information, a proposal is created with five categories of risk information, consisting of average risk, site-specific average risk, activity risk (activity performance risk and activity consequence risk), period risk, and time dependent action risk. Therefore, different risk information is required for each type of decision. The framework by Yang and Haugen [28] is general, but tailored to the needs of manual maintenance work in an oil and gas process plant offshore or onshore. Still, it is considered generally to be applicable in the present context, since the classification provides a structure that helps in understanding how we need different aspects of risk and different ways of expressing risk in different situations. Moreover, it improves communication among decision-makers by clarifying what aspects we are addressing when we use the term “risk”. Some types of the risk information were mentioned in 6.4 Change Analysis, regarding how events have deviated from earlier events or common practice due to inadequate or insufficient risk information to support the specific type of decision-making.

Development of an on-line risk monitoring and decision supporting system

From the results, we have learned that the ability of DP operators to perform rapid detection of unwanted behavior and make rapid decisions about compensating actions should be improved. Up to now, a large focus has been on the alarms. While, they are not proactive and often leave short time for operators to react. To improve the safety of DP operations, DP operators need to have a full picture of the status ahead of any alarms. Vinnem et al. [36] have proposed an overall concept for on-line risk monitoring and decision support system, which can be installed in parallel with existing systems, such as automatic on-board control systems, to supply systems with independent, early warning of possible accidents or incidents. With advisory functions, it enables operator to make better timely decisions, but probably also with independent automatic avoidance maneuvering as a last resort. One significant characteristic of on-line risk modelling is that it aims at providing proactive barriers to prevent the occurrence of possible accident while alarms in DP system functions as reactive barriers after hazardous event.

Moreover, it has been further stated that the focus of the on-line risk model and decision support tool should be on supporting execution decisions: instantaneous and emergency decisions [23]. According to Yang and Haugen [28], these two types of decisions are related to time-dependent risk using indicators derived from operating parameters against operating limits. Safety barrier performance has been recognized as one of the operating parameters for the estimation and control of time-dependent action risk [28]. With regard to DP operations, it is such as minimum requirements for availability of DP system itself (i.e., level of redundancy) or degradation condition of the DP system. However, these types of information have not been the focus in the human machine interface (HMI) design of DP systems. The emphasis of most of the state-of-the-art DP control panel is insofar on the information about vessel speed, heading, power consumption, thruster force vector, wind trend and so on. Therefore, the development of the on-line risk monitoring and decision-supporting system will compensate for the missing information to provide a better support for DP operator's decision-making.

In essence, an on-line risk monitoring system should not become 'just another box' on the bridge, but should act as an advisory system during routine loading operations in order to give the DP operator on-line updated information about the DP system and impact of any deviations or limitations in the system, as well as early indications of barrier failures. To ensure that a decision support tool for DP operators is tailored to the needs and context of the operators, four design principles have been recognized for the on-line risk model, including complementarity, integration, early detection, early warnings and transparency [23]. Even if these design principles need to be supplemented by further research, it has proved that user-centered design [37] is one way to safeguard end users' needs and to respect their capabilities.

The overall concept for on-line risk modelling has been established. Nevertheless, the validity and feasibility of the framework cannot be proved until it is applied to the real cases such as DP systems for FPSO-shuttle tanker operation. The main objective of the PhD work is to further develop the on-line risk modelling of DP systems. Firstly, a risk modelling tool will be developed to properly reflect the causality of the system in all possible operational configurations and states, including those outside the design intentions. Secondly, mathematical relations need to be established between a set of risk indicators and a set of controllable risk influencing factors. Based on the mathematical relations, the risk will be controlled in a predictable manner by manipulating the configuration variables and the system states. Furthermore, the risk model need to be implemented in a way that is applicable to update on-line based on state measurements or estimates. In addition, it is also inevitable to focus on the emerging risk, for instance due to HMI design failures in on-line risk management system.

7 Conclusions

The detailed overview of event sequences, immediate causes, root causes, deviations and barrier failures in the paper has documented that the majority of accidents and incidents is caused by a combination of technical, human and organizational failures. In order to reduce the problem related to the combination of failures, this study suggests that new risk reduction can be targeted at root causes and latent failures, which are underlying SHE problems in the organization and the technical systems.

The results show that there is a need for improvements in the decision making at different levels of the organizational hierarchy; not only in the work-system level, but also decisions made by designers, planner, etc. and top management decisions at the strategic level. When a new installation or a new change in the offloading configuration are demanding, adequate information should be provided to the design team and other personnel on the work-system level. Resources, i.e., user manual of new software function, training for new installations should be sufficiently allocated to the sharp-end operators.

It is recognized that there is insufficient attention to the barrier concept during accident investigation. A good reporting system to continuously improve the safety design is discussed in the paper. More importantly, necessary performance requirements should be well defined for the concrete operational and organizational barrier elements, as well as for the technical elements in DP operations.

In addition, to improve safety barriers, we may need to subdivide the latent failures for the combination of subgroups of failures, for instance, combination of operator failures and latent failures were present in 7 out of 9 DP incidents analyzed in this data set. Latent failures in these cases were mainly related to mistakes made by either the designers or maintenance personnel.

Lastly, recommendations of potential improvements are made on the aspects of risk analysis method, barrier management for DP systems, classification of risk information to support decision making and development of an on-line risk monitoring and decision supporting system, .

Acknowledgement

The authors appreciate the permission from PSA to utilize information in the nine incident investigation reports in an anonymous manner, these nine reports is the basis of the analysis. Ingrid Bower Utne acknowledges the support from the research project, Design to Verification of Control Systems for Safety and Energy Efficient Vessel with Hybrid Power Plant (D2V), with the Research Council of Norway as the main sponsor. NFR:210670/070, 223254/F50. Moreover, two anonymous reviewers are acknowledged for their valuable comments to an earlier version of the paper.

References

[1] IMO MSC Circ.645, “Guideline for vessels with dynamic positioning systems,” 1994.

[2] R. Bierman, “DP marine operations growing operability but at what risk.,” [Online]. Available: Online barrier performance prediction model .

[3] H. Chen and B. Nygård, “Quantified Risk Analysis of DP Operations - Principles and Challenges,” in *SPE International Conference*, Stavanger, Norway, 2016.

[4] J. E. Vinnem and I. B. Utne, “Risk reduction for floating offshore installations through barrier management,” in *Proceedings of the ASME 2015 34th International Conference on Ocean, Offshore and Arctic Engineering*, Newfoundland, Canada, 2015.

[5] M. E. K. Lundborg, “Human Technical Factors in FPSO-ST interactions and their influence on the collision risk during operations in the North Sea,” NTNU, Trondheim, 2014.

[6] Y. Dong, B. Rokseth, J. E. Vinnem and I. B. Utne, “Analysis of Dynamic Positioning System Accidents and Incidents with Emphasis on Root Causes and Barrier Failures,” in *Risk, Reliability and Safety: Innovating Theory and Proceedings of ESREL 2016*, Glasgow, Scotland, 2017.

[7] A. Kvitrud, “Collisions between platform and ships in Norway in the period 2001-2011,” in *The 30th International Conference on Ocean, Offshore and Arctic Engineering*, 2011.

[8] J. E. Vinnem, P. Hokstad, T. Dammen, H. Saele, H. Chen, S. Haver, O. Kieran and H. Kleppestoe, “Operational safety analysis of fpso-shuttle tanker collision risk reveals areas of imporvement,” in *Proceedings of the OTC conference*, Houston, USA, 2003.

[9] H. Chen, Probabilistic evaluation of FPSO-tanker collision in tandem offloading operation, Trondheim: NTNU, 2003.

[10] H. Verhoeven, H. Chen and T. Moan, “Safety of Dynamic Positioning Operation on Mobile Offshore Drilling Units,” in *Dynamic Positioning Conference*, 2004.

[11] M. Rausand, Risk Assessment-Theory, Methods, and Applications, New Jersey: John Wiley & Sons, 2011.

[12] M. Green and W. Woods, “The incidentce of industrial accidents upon individuals with special reference to multiple accidents,” Industrial Fatigue Resaerch Board, London, 1919.

[13] A. J. Rawson, “Accident Proneness,” *Psychosomatic Medicine*, vol. 6, no. 1, pp. 88-94, 1944.

[14] PSA, “Principles for barrier management in the petroleum industry,” 2013.

[15] A. Eltervåg, T. B. Hansen, E. Lootz, E. Rasmussen, E. Sørensen, B. Johnsen, J. E. Heggland, Ø. Lauridsen and G. Ersdal, “Barrierenotat 2017: Prinsipper for barriererestyring i petroleumsvirksomheten,” PSA, Oslo, 2017.

[16] N. Paltrinieri and S. Haugen, “Towards a dynamic risk and barrier assessment in an IO context,” in *Safety, Reliability and Risk Analysis: Beyond the Horizon*, London, 2014.

[17] S. Sklet, “Methods for Accident Investigation,” SINTEF, Trondheim, 2002.

[18] J. Rasmussen, “Risk Management in a Dynamic Society: A modelling Problem,” *Safety Science*, pp. 183-213, 1997.

[19] K. Urban, Prevention of Accidents through Experience Feedback, CRC Press, 2000.

[20] Z. Qureshi, “A review of accident modelling apporaches for complex critical sociatechnical systems,” Defence Science and Technology Organizations, Edinburgh, 2008.

[21] J. E. Vinnem, Offshore Risk Assessment, London: Spinger, 2013.

[22] C. Rollenhagen, “Event investigations at nuclear plants in Sweden: Reflections about a method and some associated practices,” *Safety Science,* pp. 21-26, 2011.

[23] S. Hogenboom, J. E. Vinnem and I. B. Utne, “Towards an online risk model for DP operations: decision-making and risk information,” in *Submitted to ESREL 2017,* 2017.

[24] “Guidelines to regulations relating to conduct of activities in the petroleum activities,” Petroleum Safety Authority Norway, Norwegian Pollution Control Authority, Norwegian Social and Health Directorate, 2002.

[25] “Navigation, manoeuring and position keeping,” DNV GL, Olso, 2015.

[26] N. Patrinier, S. Massaiu and A. Matteini, “Human Reliability Analysis in the Petroleum Industry: Tutorial and Examples,” in *Dynamic Risk Anslysis in the Chemical and Petroleum Industry,* Elsevier Inc., 2016, pp. 181-192.

[27] S. Ternov and R. Akselsson, “System weaknesses as contributing causes of accidents in health care,” *International Journal of Quality in Health Care,* vol. 17, pp. 5-13, 2005.

[28] X. Yang and S. Haugen, “Classification of risk to support decision-making in hazardous process,” *Safety Science,* pp. 115-126, 2015.

[29] J. Reason, “Too little and too late: A commentary on accident and incident reporting systems,” in *Near-miss reporting as a safety tool,* Oxford, Butterworth-Heinemann, 1991.

[30] J. Rasmussen, “Learning from experience? How? Some resaerch issues in industrial risk management,” in *Reliability and Safety in Hazardous Work Systems,* Hove, Eas Sussex, Lawrence Erlbaum Associates, 1993.

[31] C. Perrow, Normal Accidents: Living with High-Risk Technologies, Princeton: Princeton University Press, 1999.

[32] A. Klinke and O. Renn, “A new approach to risk evaluation and management: risk-based, precaution-based and discourse-based strategies,” *Risk Analysis,* vol. 6, pp. 1071-1094, 2002.

[33] B. Rokseth, I. B. Utne and J. E. Vinnem , “A systems appraoch to risk analysis of maritime operations,” *Journal of RIsk and Reliability,* pp. 53-68, 2017.

[34] B. Abrecht and N. Leveson, “System Theoretic Process Analysis (STPA) of an Offshore Supply Vessel Dynamic Positioning System,” Massachusetts Institutte of Technology Lincoln Laboratory, 2016.

[35] E. Hollnagel, “Risk+barriers=safety?,” *Safety Science,* pp. 221-229, 2008.

[36] J. E. Vinnem, I. B. Utne and I. Schjølberg, “On the need for online decision support in FPSO-shuttle tanker collision risk reduction,” *Ocean Engineering,* pp. 109-117, 2015.

[37] A. Hale and D. Borys, “Working to rule or working to safely? Part 1: A state of the art review,” *Safety Science,* pp. 207-221, 2013.

[38] A. Hale and D. Borys, “Working to rule or working to safely? Part 2: The management of riles and procedures,” *Safety Science,* pp. 222-231, 2013.

[39] D. Besnard and E. Hollnagel, “I want to believe: some myths about the management of industrial safety,” *Cogn Tech Work*, pp. 13-23, 2014.

[40] J. C. Coze, “Relecting on Jens Rasmussen's legacy. A strong program for a hard problem,” *Safety Science*, pp. 123-141, 2015.

[41] R. Rosness, “Safety culture: Yet another buzzword to hide our confusion?,” SINTEF, Trondheim.

[42] J. Reason, Managing the Risks of Organizational Accidents, Nurlington: Ashgate Publishing Limited, 1997.

[43] G. Boothby, “Ship/platform collision risk in the UKCS-the regulator's perspective, health and safety executive presentation to oil & gas UK seminar”.

[44] A. J. Snørensen, “A survey of dynamic positioning control systems,” *Annual Reviews in Control*, pp. 123-136, 2011.

[45] D. Wickens, J. Lee, Y. Liu and S. G. Becker, “Chapter 15 Automation,” in *An Introduction to Human Factors Engineering 2 Edition*, Peason Education Limited, 2014, pp. 398-415.

[46] A. Kvitrud, H. Kleppestø and O. R. Skilbrei, “Position Incidents during Offshore Loading with ST on the NCS 2000-2011,” in *Proc. of the Twenty-second (2012) International Offshore and Polar Engineering Conference*, Rhodes, Greece, 2012.

[47] A. Hopkins, “Issues in safety science,” *Safety Science*, pp. 6-14, 2014.

[48] T. Aven, “What is safety science?,” *Safety Science*, pp. 15-20, 2014.

[49] E. Hollnagel, “Is safety,” *Safety Science*, pp. 21-24, 2014.

[50] N. N. Taleb, The Black Swan: The Impact of teh Higly Improbable, Radom House, 2007.

[51] F. Khan and S. Abbasi, “Major accidents in process industries and an analysis of causes and consequences,” *Journal of Loss Prevention in teh Process Industries*, vol. 12, pp. 361-378, 1999.

[52] N. R. Crutchfield, “Overview of basic safety management system,” in *Safety Culture*, Elseview Science, 2013, pp. 93-108.

[53] C. Taylor , S. Øie and N. Patrinieri, “Human reliability in the petroleum industry: a case study,” in *Risk, Reliability and Safety: Innovation Theory and Practice*, London, 2017.

[54] Y. Pan , S. K. Renganayagalu and S. Komarndur, “Tacticle cues for ship bridge operations,” in *Proceedings 27th European Conference on Modelling and Simulation* .

[55] K. I. Øvergård, L. J. Sorensen, S. Nazir and T. J. Martinsen, “Critical incidents during dynamic positioning: operators' situation awareness and decsion-making in maritime operations,” *Theoretical Issues in Ergonomis Science*, pp. 366-387, 2015.

[56] L. J. Sorensen, K. I. Øvergåard and T. J. Maritinsen, “Understanding huamn decision making during criticl incidents in dynamic positioning”.

[57] H. Chen, T. Moan and H. Verhoeven, “Safety of dynamic positioning operations on mobile offshore drilling units,” *Reliability Engineering & System Safety,* pp. 1072-1080, 2008.

[58] T. Aven, S. Sklet and J. E. Vinnem, “Barrier and operational risk analysis of hydrocarbon releases,” *Journal of Hazardous Materials,* pp. 681-691, 2006.

[59] T. W. Van der Schaaf, D. A. Lucas and A. Hale, Near-miss Reporting as a Safety Tool, Butterworth-Heinemann: Oxford, 1991.

[60] R. Leonhardsen, G. Ersdal and A. Kvitrud, “Experience and risk assessment of FPSOs in use on the NCS description of events,” in *The 11th International Offshore and Polar Engineering Conference*, Stavanger, 2001.

[61] M. Endsley, “Towards a theory of situation awareness in dynamic systems.,” *Human Factors,* pp. 32-64, 1995b.

[62] J. Sudano, “Minimizing human-machine interface failures in high risk systems,” in *Aerospace and Electronics Conference,* Dayton, 1994.

Table 2 Summary of the root causes, deviations and barrier failures.

Root causes	Deviations	Barrier failures
- The requirements about how to operate DP system, when aligning ST with FPSO are missing in the procedures. - Lack of training, education and experience from offshore loading, particularly about DP operations. - Deficiency in DP software design. - Poor ergonomic/deficiency in design - Lack of training after new installations. - Poor communication among engine officer. - Heavy workload and a large amount of administrative work. - Insufficient maintenances. - Deficiency in design. - Lack of training on similar incidents. - Lack of DP emergency procedures. - Inadequate maintenance regime (for fuel oil filters and pumps). - Lack of testing for emergency supply by emergency generator. - Insufficient maintenance activity. - Lack of a controlled follow-up and closing of findings related to photography reports. A detailed description of the findings in thermos photography reports are not entered into the vessel's PMS system. - Lack of procedure with regard to closing or follow up the observations in the thermos photography reports. - Lack maintenance inspection regime, considering maintenance intervals and inspection routines. - Lack of procedure on the use of the emergency stops.	-Inadequate information to software design team, when new offloading configuration is introduced. -Inadequate information to the operational team after new installation. -Abnormal settings of main propeller during installation. -Engine officers decided to continue the voyage without running any separators in the fuel system. -Engine Chief Officer did not inform the decision. -Engine officer decided not to use from the bunker received from Falmouth, before fuel analysis is available. -Non-compliance with company's requirement about when to carry out a position drop-out. -After two verification tests, Artemis Mk V was configured with «continuous» mode for telegram updates. -DPO decided not to report the incident immediately.	-There should be clear requirements regarding how DPO should operate the DP system when aligning ST with FPSO. -There should be sufficient training before DPOs are permitted to start working offshore. -There should some basic requirements of education and experience, when DPOs are recruited. -There should be clear guidelines for the tasks of hired Captain. -Sea test should be properly and thoroughly performed according to FMEA. -There should be a standard procedure regarding how shuttle tanker should be tested according to FMEA. -Training should be provided to DPO after new installations. -Missing test regarding system integrity after new installations. -Supporting manual should be provided onboard after new installations. -Unintended cross connections between the switchboards was not discovered by any of the FMEA tests during verifications. -Missing barrier in Gyro for rejecting of incorrect latitude and speed compensation, -Missing requirement in the design standard/guidelines. -DP barrier for calculating deviation between calculated and measured heading is too wide. -Missing barrier to protect UPS from transient spike. -There should be follow-up and closing of findings related to photography reports. -There should be a check of the frequency update mode of Artemis Mk V after verifications. -There should be a well-designed maintenance inspection regime, considering maintenance intervals and inspection routines.

Table 3 Results of the MTO analysis

Acc. & Inc.	Event Sequences	Immediate causes	Root causes	Deviations	Failed or missing barriers
A	E1. ST was operated in tandem loading mode using FSU heading function with bow-base distance of 72m. Due to swell and current, DPO wanted to change heading and requested FSU to change heading for 10 degrees in two steps.	- DPO gave improper command to the DP control system.	- Lack of training after new installations. - Manual of tandem software was not onboard	-Inadequate information to the operational team after new installation.	-Training should be provided to DPO after new installations. -Supporting manual should be provided onboard after new installations.
	E2. When ST changed heading, it started increasing speed ahead.	- Incorrect estimation of the maximum thrust values resulted in the tuning of the main propeller.	- Deficiency in DP software design	-Abnormal settings of main propeller.	-Missing test regarding system integrity after new installations.
B	E1. It was 24 degrees heading difference between ST and FPSO, Captain wanted to align the ST hose reel onboard FPSO and to send hose back. Captain changed DP from “weather vane” mode to “auto position” mode in order to move the ST 50m port side in one movement and 0.2 knots max.	- The 50 meters are given as a single movement, which should have been given in several transfers, i.e., 50 meters in 5 transfers, while 10 meters for each transfer. - DPO was uncertain with respect to how PRS is handled by DP system between the transition of different modes. With uncertainty, “position drop-out” was performed to calibrate the PRS, which led to an unpredictable situation.	- The requirements about how to operate DP system when aligning ST with FPSO are missing in the procedures. - Lack of training, education and experience from offshore loading, particularly about DP operations.		-There should be clear requirements regarding how DPO should operate the DP system when aligning ST with FPSO. -There should be sufficient training before DPOs are permitted to start working offshore. -There should some basic requirements of education and experience, when DPOs are recruited. -There should be clear guidelines for the tasks of hired personnel.
	E2. DP started to have increased current input and commanded thrust ahead for balance.	- The DP logic initiated a full ahead movement based on the PRS in the change from “weather vane” mode to “auto position” mode. - The increased current might be caused by adding the pressure from hawser during the transition of mode.	- Deficiency in DP software design.	-Inadequate information to software design team	-Sea test should be properly and thoroughly performed according to FMEA. - There should be standard procedure about how shuttle tanker should be tested according to FMEA.

Acc. & Inc.	Event Sequences	Immediate causes	Root causes	Deviations	Failed or missing barriers
	E3. Captain and Advising Captain discovered the increased current on DP monitor and went to discussed it. None of them discovered the ahead thrust, which was shown in another DP monitor.	- Poor man-machine interface. Important information was given on different monitors.	- Poor ergonomic/deficiency in design		
	E4. After 55 seconds from switching the DP mode, captains noticed that the thrust on both main engines showed "red forward" and ST had been driven ahead.	- Insufficient alarms, i.e., no alarm when speed exceeded 0.5knots.	- Poor ergonomic/deficiency in design		
C	E1. The ST was operating in DP2 "autopos" mode, while mooring hawser was just received and secured. A blackout of the starboard MSWB occurred, when bow crew was in the progress of preparing the loading hose.	- Fuel starvation. - Ignorance of company procedures for fuel treatment	- Poor communication among engine officer. - Heavy workload and a large amount of administrative work.	-Engine officers decided to continue the voyage without running any separators in the fuel system. -Engine Chief Officer did not inform the decision. -Engine officer decided not to use from the bunker received from Falmouth, before fuel analysis is available.	
	E2. The starboard main propulsion and two of the side thrusters were lost. Blackout on the MSWB also triggered blackout on the ESWB. Loss of power to fix mounted UHF oil movement radios on bridge.	- The starboard main propulsion and two of the side thrusters were powered by the starboard MSWB.			
	E3. Loss of the remaining two side thrusters. DP remained in DP autopos-mode. Only the main propeller and rudder available on the DP, the vessel remained in DP autopos-mode. The DP is not able to maintain/control the position with only one rudder and one propeller.	- Backup batteries were out of power. - UPS for soft starter to the other porn stern thruster failed due to wrong cabling and faulty settings for change over. ESWB was fed from stbd MSWB, instead of port MSWB.	- Insufficient maintenances. - Deficiency in design.		-Unintended cross connections between the switchboards was not discovered by any of the FMEA tests during verifications.

Acc. & Inc.	Event Sequences	Immediate causes	Root causes	Deviations	Failed or missing barriers
	E4. Three min after max hawser tension was registered, the Master changed from DP autopos-mode to manual mode and gave full astern on port main engine.	- Manual control of maneuvering system was taken too late to prevent the collision.	- Poor ergonomic/deficiency in design. (Massive visual and audible alarms on a large number of monitors and panels, which are located on a relatively large area on the bridge.) - Lack of training on similar incidents. - Lack of DP emergency procedures.	-Concern for the safety of the crew working in the BLS area.	
D	E1. Loss of power on the Stbd MSWBD.	- Fuel starvation in Starboard common system. Low fuel system pressure resulted in auxiliary engines load variations and unstable power supply. - Restrictions in flow meters and fuel filters detected through different readings of pressure.	- Inadequate maintenance regime (for fuel oil filters and pumps). - Poor ergonomic/deficiency in design		
	E2. Loss of power on the emergency switchboard.	- Emergency generator failed to connect to the emergency SWBD due to a faulty time relay.	- Lack of testing for emergency supply by emergency generator.		
	E3. Loss of updates from PRSs and instantaneous failure of all gyros. The main mathematical DP model was still intact.	-UPS failure was caused by unstable power supply (transient spiker), which resulted in loss of DP position reference systems and instantaneous failure of all gyros. - One of the PRSs (hydro acoustic positioning reference system) was powered by emergency SWBD without UPS.			-Missing barrier to protect UPS from transient spike.
	E4. DPO initiated ESD2 for disconnection. However, the last part of the ESD2 sequence failed. (Disengage button was pressed by	- A stuck BLS dog clutch.	- Insufficient maintenance activity.		

Acc. & Inc.	Event Sequences	Immediate causes	Root causes	Deviations	Failed or missing barriers
	the operator but dog clutch did not operated as expected.)				
E	E1. Heading prediction error. **<u>Note:</u>** <u>No alarm was given at heading difference of 10 degrees between measured and calculated heading in DP model.</u>	- Common cause failure of GPSs was due to receiver interference. - Incorrect Gyro heading due to error on Gyro latitude and speed compensation.	- Deficiency in design		- Missing barrier in Gyro for rejecting of incorrect latitude and speed compensation, - Missing requirement in the design standard/guidelines.
	E2. DP accepted incorrect Gyro heading input. Subsequently, DP model was corrupted.		- Deficiency in design		- DP barrier for calculating deviation between calculated and measured heading is too wide.
	E3. All PRS (Artemis, HPR and DARPS) were lost. Without PRS and correct gyro input, the DP system was not able to keep vessel in position based on corrupted DP model. A high rate of turn of the vessel was estimated by the DP system.	- Errors in PRSs were due to corrupted DP model and incorrect Gyro heading, while gyro heading was used as offset compensation for all PRSs.			
F	E1. At the final stage of loading and de-ballasting, a short circuit of the port 440V SWBD occurred. The shot circuit led to the secondary transformer breaker being overloaded and tripped.	- The design of spring loaded terminal block in combination with cable size. - Insufficient repair of the hot-spot detection during IR work. - Breaker to ballast vacuum pump starter did not trip to fulfill selectivity.	- Lack of a controlled follow-up and closing of findings related to photography reports. A detailed description of the findings in thermos photography reports are not entered into the vessel's PMS system. - Lack of procedure with regard to closing or follow up the observations in the thermos photography reports.		There should be follow-up and closing of findings related to photography reports. -There should be procedures with regard to closing or follow up the observations in the thermos photography reports.
	E2. The electrician witnessed a flame tongue of 20 to 30 cm from the upper part of the 440V SWBD followed by a fume emission in ECR.				
	E3. Evacuation followed by the initiation of ESDI and ESDII.				

Acc. & Inc.	Event Sequences	Immediate causes	Root causes	Deviations	Failed or missing barriers
	E4. The DP screens were frozen and 3 (both stern thrusters and one fwd bow thruster) out of 4 thrusters were lost. The PRS systems were operational. The CCTV screen and the BLOM data logger screen were out of order.	- On the bridge, a fuse supplying the CCTV and the BLOM monitor was tripped because of the short circuit. - The fuse being blown in the HV SWBD might be caused by overloads due to faulty settings on thruster control systems.			
	E5. Both main engines were running. The DP was switched off and the vessel maneuvered manually by lever controls to safe are off the loading facilities.				
G	E1. Alarm CPP control failure triggered for port main engine. Port main engine is subsequently rejected by DP.	- It was a prediction error between command and response. - Split pin for coupling on EI motor shaft was worn out.	- Lack maintenance inspection regime, considering maintenance intervals and inspection routines. There was no specific mention of the split pin in overhaul jobs related to stepper motor or pitch control. - Lack of procedure on the use of the emergency stops.		There should be a well-designed maintenance inspection regime, considering maintenance intervals and inspection routines.
	E2: Controls were transferred to emergency control room and were switched over to emergency pitch control. However, no response on port main engine.				
	E3: Immediately local maneuver on hand wheel for stepper motor was attempted. Still, no response on port main engine.	- During attempt to control the pitch locally and putting local control astern, the hydraulic pressure of the pitch controller allows the action, however, with the split pin broken, attempts to control and adjust pitch will fail, and pitch will remain full astern.			
	E4: During the attempt to maneuver manually, pitch goes full astern, without possibility to reestablish zero pitch.				

Acc. & Inc.	Event Sequences	Immediate causes	Root causes	Deviations	Failed or missing barriers
	E5: Port main engine was stopped by emergency stop on bridge.				
H	E1. Malfunction on stepper motor for port CPP causing the propeller to freeze in 10% pitch forward while position controlled by DP.	- Faulty stepper motor/servo motor.	- Inadequate design - Inadequate inspection intervals and inspection routines.		
	E2. CPP could not be operated.				
	E3. CPP was deselected from DP and operated in emergency mode from the center console on the bridge.				
	E4. Malfunction degraded vessels DP class during tandem loading operation (from Class2 to Class1). The situation was not reported.			-DPO decided not to report the incident immediately.	
	E5. Captain conducted informal risk assessment of loading with degraded position keeping capability (port adjustable pitch propeller disengaged from DP) and deemed prevailing weather conditions and forecast acceptable to continue loading.				
I	E1. DPO observed a bow-base deviation of 5 meters between DP and BLOM PMS, and 2 to 5 tons tensions in hawser. The DP bow-base set point was moved from 37m to 35m to reduce hawser tension.	- 5 meter deviation might be caused by inaccurate DP system offset(s) for PRS(s) and /or gyros deviating from the true north.			
	E2. When the bow-base deviation was still observed unchanged, the DPO performed a DP position drop-out with the object to recalibrate the position reference systems to align the DP distance readings (35m) with the BLOM PMS (40m).	- Inadequate risk identification with regards to performing a position drop-out.	- Lack of training. Some advanced training courses are no longer available.	-Non-compliance with company's requirement about when to carry out a position drop-out.	

Acc. & Inc.	Event Sequences	Immediate causes	Root causes	Deviations	Failed or missing barriers
	E3. Following the confirmation of DP position drop-out, DPO reselected Artemis as DP reference origin. An erroneous Artemis Mk V signal was activated as the initial DP position reference system. The displayed DP bow-base distance rapidly increased from 35m via 56m to 70m within a few seconds. The main propeller responded with full ahead thrust causing a drive-off.	- Position drop-out left DP system without position references, then only one reference active when Artemis MkV was calibrated. (When Artemis was calibrated the main propeller immediately gave full ahead, interrupting the normal procedure of activating the secondary position reference.) - Misconfigured MkV and DP processor overloaded.		-After two verification tests, Artemis Mk V was configured with «continuous» mode for telegram updates.	-The frequency update mode should be checked after verifications.
	E4. Suspecting and erroneous set point, the DPO deselected the main propeller from DP, entered set point radius corresponding to DP bow-base distance and reselect main propeller into DP.	- DPO attempted to verify the correct DP set point was active.			
	E5. Following the reselection into DP, the main propeller again set toward full ahead thrust. Alarm «Position exceeds fore limit" triggered.				