A systems approach to risk analysis of maritime operations

Børge Rokseth[1*], Ingrid Bouwer Utne[1], Jan Erik Vinnem[1]

[1]Norwegian University of Science and Technology (NTNU), Department of Marine Technology
[*]To whom correspondence should be addressed; E-mail:borge.rokseth@ntnu.no

Abstract

Technological innovations and new areas of application introduce new challenges related to safety and control of risk in the maritime industry. Dynamic-positioning systems (DP systems) are increasingly used, contributing to a higher level of autonomy and complexity aboard maritime vessels. Currently, risk assessment and verification of DP systems are focused on technical reliability, and the main effort is centered on design and demonstration of redundancy in order to protect against component failures. In this article, we argue that factors, such as software requirement errors, human errors, including unsafe or too late decision-making, and inadequate coordination between decision makers, also should be considered in the risk assessments. Hence, we investigate the feasibility of using a systems approach to analyzing risk in DP- systems and present an adapted version of the system-theoretic process analysis (STPA). A case study where the STPA is applied to a DP system is conducted to assess whether this method significantly expands the current view on safety of DP systems. The results indicate that the reliability-centered approaches, such as the failure mode and effect analysis (FMEA), sea-trials and hardware-in-the-loop (HIL) testing, are insufficient and that their view on safety is too narrow. The article shows that safety constraints can be violated in a number of manners other than component failures for DP systems, and hence, STPA complements the currently applied methods.

Keywords: Maritime system safety, Safety analysis, Hazard analysis, Maritime risk, Safety engineering, Software reliability, Risk analysis, Maritime system reliability

1. Introduction

Maritime vessels have been subject to rapid technological advances during recent decades, enabling a number of new applications, such as deep-water hydrocarbon explorations. The introduction of automatic navigation and positioning systems has resulted in not only a top layer of automation handling these functionalities, but also advanced power systems and thruster systems capable of an increased level of autonomy. The high level of automation and autonomy, as well as system interactions on both the component level and the information level, are challenging with respect to risk and risk management. Software errors and software-requirement errors are important hazards to consider in these systems. Even if each individual software system is working as intended, unintended consequences might arise in the interaction between several software systems, due to insufficient software-design requirements and constraints.

A dynamically positioned (DP) vessel is, according to the International Maritime Organization's (IMO) international standard for dynamically positioned vessels,[1] a vessel that is able to maintain its position and heading and to maneuver slowly along a predefined track exclusively by means of active thrusters. In simple terms, the thruster system positions the vessel by realizing thrust commands from the DP control system, using electrical power produced by the power system. This technology has, since its birth in the 1960s, become essential for a number of offshore and maritime industries. Today, applications of DP include station keeping of mobile offshore drilling units (MODUs), platform-support vessels during loading/offloading to platforms, diving vessels, loading operations of shuttle tankers from floating production, storing and offloading units (FPSOs) and maneuvering of pipe-layer vessels. Possible consequences of loss of position during these operations can be severe. For example, the sudden loss of position for a MODU can, in the worst case, escalate into a blowout.[2]

The prevailing method for risk analysis and verification of these systems is, first, to perform a failure mode and effect analysis (FMEA) in order to provide evidence that the DP-system is redundant[3] and, second, to perform verification tests referred to as sea trials (i.e., tests on the finished system) on a selection of subsystems analyzed in the FMEA.[4] Both these required activities are aimed at verifying redundancy, something that gives an inadequate view on risk for the complex and heavily automated DP systems. FMEA considers the system as an assembly of components and does not emphasize the operational context (for details on FMEA, see, for example, Rausand[5]). Risk management of DP systems should not only focus on component failures. Also, software errors, i.e., errors resulting from software that is not operating according to requirements; software-requirement errors, i.e., errors caused by software which occur even though the software fulfills the formal requirements; unsafe or too late decision-making; and inadequate coordination between decision makers, are important factors to consider. Hence, more systems-focused risk-analysis methods may be beneficial.

Although regulatory agencies and the industry have long since recognized the need for improving the safety of DP-operations due to a relatively high frequency of incidents,[6] there has been limited research on the topic. This conclusion is supported by the Petroleum Safety Authority[7] (PSA) in a literature survey mapping our present understanding of causal links between underlying causes and DP incidents (among other types of marine incidents). The PSA study[7] states that the literature is only useful to a limited extent in this endeavor. Some former studies on risk analysis related to DP systems are nevertheless discussed.

DNV-GL has developed a recommended practice for FMEA of redundant systems[3] where the FMEA method has been customized for DP-redundancy verification. The FMEAs produced in accordance to this recommended practice will, throughout this article, be referred to as DP FMEAs. The objective of the DP FMEA is to systematically go through the detailed design plans of DP vessels and verify that the vessels are designed in such a way that no single component failure can result in loss of position. In addition, the DP FMEA often produces input to verification tests by framing assumptions and questionable conclusions as test cases. As such, the DP FMEA can be viewed as a systematic procedure for going through and verifying more or less completed design plans, rather than a hazard identification and analysis technique. Spouge[8] discusses issues, such as whether redundancy is a sufficient approach for risk management in DP systems and whether DP FMEA is better suited than other traditional methods, such as fault three analysis, (FTA) for demonstrating redundancy on DP vessels. The conclusion to these questions is that redundancy is necessary, but may not be sufficient, and that DP FMEA, in principle, is a suitable tool for demonstrating redundancy, if careful guidance is provided and an appropriate objective for the analysis is formulated. The results from the study presented in this article support the view that DP FMEA is suitable for verifying redundancy in terms of failure propagation through physical components. Nevertheless, failures may also propagate through different layers of abstraction, such as through physical processes, which a DP FMEA may not be able to take into consideration. Furthermore, it is found that even though redundancy is important for safe DP operations, it is not a sufficient means for ensuring safety in these systems.

Vinnem et al.[9] characterize the safety of FPSO and DP shuttle-tanker offloading operations in terms of resistance to loss of position and robustness of recovery. Verhoeven et al.[10] use these parameters to model loss of position in a human-machine interaction perspective for DP-drilling operations. Some risk analyses of specific operations also exist. Phillips and Deegan,[11] for example, consider an operation where a vessel is positioned in the proximity of fixed installations. A worst-case failure is defined, and previous experience is used to estimate the frequency of occurrence. The consequence is quantified in terms of the potential impact energy in the event of the worst-case failure. This approach is similar to that proposed in International Maritime Contractors Association[12] (IMCA), where credible failures are selected, historical data are used to estimate the frequency, and consequences are quantified by considering impact energy. Recent studies[13-15] on risk related to DP systems have focused on classifying basic causes, risk-influencing factors, (defined in Øien,[16] as an aspect, event or condition of a system or an activity that affects the risk level), and barrier failures involved in incidents, and on estimating frequencies of occurrence of the various causes or classes of causes. Chen and Nygård[17] present a new technique for quantifying the risk related to DP operations near offshore installations, where the frequency estimate is based on previous accident rates, while the consequence part is based on impact speed and impact energy, along with installation structural capacity, etc. This approach also takes into account human-intervention actions, which may have an effect on the impact speed.

None of the above-mentioned studies addresses the potential for using systemic approaches for analyzing risk or focuses on identifying and mitigating potential hazards in new systems, but instead classifies and quantifies the already-known causes. Abrecht and Leveson[18] present a case study where Systems-Theoretic Process Analysis (STPA) is used to analyze an offshore supply vessel in a target-vessel escort operation with focus on operational aspects. Functions, such as power generation are, however, not considered. Still, they did identify several hazards that were not found in an independent FMEA.

Recent developments with respect to system testing and verification are hardware-in-the-loop (HIL) testing and software-in-the-loop (SIL) testing. A challenge with the DP-related software is that almost every vessel is unique. A large number of software vendors deliver control systems that must be integrated into the DP system.[19] The result is that, although most software is tested isolated by the individual vendors, the integrated system is not tested. HIL verification offers the opportunity to test the integrated software system in a simulation of the environment in which it is embedded. Some challenges with HIL testing are to select test cases and to set up a suitable context for the simulations.

The objective of this article is to assess the feasibility of using STPA for hazard identification and assessment of complex and automated systems, like the DP system. The article develops an adapted version of STPA, and addresses whether STPA can be used to (i) expand the current view on safety of DP systems to include factors, such as software errors, software-requirement errors, human errors and unsafe decision making (i.e., decision making of any decision maker that directly or indirectly can result in an accident) and (ii) provide an operational context for verification. The analysis is based on a case study of a generic DP system and demonstrates how a STPA can be performed for such a system. Since a DP system is complex and comprehensive, a broad approach is used initially, and then selected parts of the system are focused on in more detail. In particular, emphasis is put on the operation of the power system. The results of the case study show that it is beneficial to use STPA, because, first, it does not seem to require detailed knowledge about the various subsystems within the DP system but, rather, focuses on a purpose-oriented system view. Second, it allows for an extended view of the safety of DP systems, because we decompose the system according to functional abstraction, rather than a structural decomposition.

The remainder of the article is structured as follows: Section 2 gives a short overview of incidents with DP systems and typical causes; Section 3 presents the STPA methodology; Section 4 presents the case study, and Section 5 presents and discusses the results. The conclusions are stated in Section 6.

2. Incidents with DP systems

IMO[1] categorizes the DP system into the DP-control system, thruster system and power system. The main concern is loss of position-keeping capability. Chen and Moan[20] define loss of position as: *the vessel loses, either temporarily or for an extended time, the capability to maintain its position by means of thruster force, and consequently has a position excursion which is beyond the normal distance range.* There are three main DP classes[1]:
DP-equipment class 1: Loss of position may occur in the event of a single fault.
DP-equipment class 2: Loss of position should not occur from single fault of an active component or system, such as generators, thrusters, switchboards, remote-controlled valves, etc., but may occur after failure of a static component, such as cables, pipes, manual valves, etc.
DP-equipment class 3: Loss of position should not occur from any single failure, including a completely burnt fire sub division or flooded watertight compartment. A single fault includes a single inadvertent act by any person on board the DP vessel.

In addition to these class definitions, IMO provides a few requirements for each of the subsystems of the DP system. Classification societies, such as DNV-GL[21] and American Bureau of Shipping[22] (ABS), provide more comprehensive sets of requirements for DP, aimed mainly at ensuring that the requirements in the international standard for DP systems[1] are satisfied. In addition, these classification societies also offer class certificates based on IMO-class definitions. To obtain a class certificate, a vessel's design and construction must be verified according to the respective class society's rules. The verification strategy of DNV-GL consists of two activities; first, a FMEA shall be performed in order to demonstrate redundancy,[21] and second, sea-trials shall be performed in order to verify certain issues in the FMEA.[4]

According to Chen,[23] the frequency of shuttle tanker-FPSO collisions during the first decade of tandem DP-offloading operations was as high as $2 \cdot 10^{-2}$ collisions per loading. Lundborg[24] estimated the frequency, based on more recent data, to about 10^{-3} collisions per installation year. Chen[23] revealed that the performance of the technical system and the human operators were key factors in the incidents. Erroneous operator actions related to nine drive-off events were grouped into three types. The first type involved wrong expectations of the technical system functions, the second type involved improper use of the technical equipment, such as erroneous configuration of the DP system, and the third type involved wrong assessment of the internal or external situation. Furthermore, Vinnem et al.[9] studied 19 FPSO and shuttle-tanker collisions and near misses and identified the combination of technical factors and human/operational factors as the most significant contributors to the collision frequency. It was found that 40% of the collisions are caused by this combination of factors.

Chen and Moan[20] analyzed DP incidents on the Norwegian Continental Shelf (NCS) and collected DP drilling experience from six MODUs. The data was collected from the SYNERGI$^{\mathrm{TM}}$ database[25] along with DP-event logging files and DP-watch checklists. The drive-off incidents were studied more in depth than drift-off incidents, and it was found that the DP control system was involved as a cause in all incidents, key DP personnel in 50% of the incidents, and the environment in 25% of the incidents. Three problem areas were identified (i.e., areas that most frequently are involved in drive-off incidents as a cause): the position reference system (considered a subsystem of the DP control system), DP software and its robustness in handling erroneous position reference, and key DP personnel and their competence and management.

PSA[7] reported sixteen DP-related collisions on the NCS between 2000 and 2013. Furthermore, PSA[6] claimed that there was a large frequency of incidents related to DP systems for mobile offshore units in the Norwegian petroleum industry and recommended the offshore industry to improve safety in DP operations and DP drilling operations, in particular.

Yuhan[14] used the annual reports from IMCA on station-keeping incidents from 2000 to 2011 to estimate the frequencies of drift-off and drive-off worldwide for DP equipment class 2 and class 3 vessels. Out of the 267 incidents between 2000 and 2010 that were considered (any incident involving either drift-off or drive-off for DP class 2 and class 3 vessels that have been reported to the IMCA organization), 110 drive-off incidents and 136 drift-off incidents were reported.

3. Methodology

Rasmussen[26] argues that emergent properties, such as safety, must be studied using a systems-theoretic approach, based on functional abstraction rather than structural decomposition. A complex dynamic system cannot successfully be decomposed into structural elements, and activities cannot be decomposed into a sequence of tasks. This is because the operation of complex dynamic systems leaves too many degrees of freedom in terms of choice of means and time.[26] Instead, Rasmussen suggests that risk management should be considered a control function with the objective of maintaining processes within the boundaries of safe operation, and that a systems approach should be applied to describe the overall system functions.

Leveson[27] proposes an accident-causation model, the *Systems-Theoretic Accident Model and Processes* (STAMP), based on these ideas. In this framework, safety is controlled by enforcing constraints on the system behavior, and accidents occur because of inadequate control or inadequate enforcement of safety constraints. The following three important concepts are defined within this framework: (i) safety constraints, (ii) hierarchical safety control structures, and (iii) process models.

Safety constraints are constraints that must be enforced on the behavior of the system in order to ensure safety. Hierarchical safety-control structure refers to the manner in which systems are viewed as a hierarchy of controllers enforcing safety constraints between each level. A controller might be, for example, an organization, an operator or a piece of software controlling an actuator. In this context, a classification company exercising control over the design of a ship by providing class rules can be viewed as a controller.

The term *process model* in the STAMP framework is derived from the discussion on cybernetic models for human operators presented in Rasmussen.[28] These models are necessary for the human to act as a goal-oriented operator. In STAMP, this concept is extended from a human operator to any entity exercising control in a system. The key point is that a controller needs to have a perception of the state of the system it is controlling and an idea about the effect of different control outputs on the system. This is true for automated controllers as well as for human controllers.[27] If, for example, the controller in question is a designer of ships, a perception about which effects different design choices have for, e.g., building cost and operation of the ship, is necessary. Without a consistent process model, the designer will likely not be able to design serviceable and practicable ships at the agreed cost.

The systems-theoretic process analysis (STPA) is a hazard identification and analysis method based on the STAMP framework.[27] The method enables a practical implementation of the fundamental ideas behind STAMP, namely those of viewing risk management as a control function. In STPA, the system under consideration is viewed as a control system (or a hierarchy of control systems), and hazardous states are caused by unsafe control actions (UCAs), i.e., control actions (or the lack thereof) that might result in inadequate enforcement of safety constraints. The generic STPA process can be divided into two main steps, i.e., (i) identifying UCAs and (ii) determining how the UCAs may occur, i.e., identifying scenarios and causal factors.[27] When the scenarios and causal factors are identified, safety constraints, which, if enforced, will keep the system away from hazardous states or will mitigate the consequences, can be identified. In this article, we have adjusted these two main steps into six steps applicable for risk analysis of maritime operations. The steps are explained in detail and applied to the DP system in the next section:

Step 1. Describe the system and conceptualize it as a control system.
Step 2. Identify system-level accidents, system-level hazards and system-level safety constraints.
Step 3. Identify controller responsibilities and process models.
Step 4. Identify UCAs.
Step 5. Identify causal factors and scenarios, (i.e., the causes for unsafe control).
Step 6. Identify safety constraints.

Steps 1 through 3 mainly represent what is referred to in Leveson[27] as *laying the engineering foundation*. The purpose of formalizing this into three distinct steps is that the engineering foundation is of vital importance to the analysis, and that the results of the analysis is, to a significant degree, dependent on how this part is performed. In Step 1, the system is conceptualized as a control system. The manner in which this is done sets the boundaries for the scope of the analysis. The scope depends significantly on, for example, whether or not classification companies, international standard-setting organizations and flag-states are included into the control loop. Step 2 is where the system-level accidents and the corresponding system-level hazards and safety constraints are defined. The choices made in this step are significant with respect to the focus of the analysis. If we are interested in avoiding that sailors get hurt by falling objects aboard the vessel, this must be defined as a system-level accident. If we, on the other hand, are most interested in loss of position, falling objects may not be relevant to include. Step 3 specifies the responsibilities and process models of each controller. This further defines the focus of the analysis, because this will directly influence the next step in terms of which control actions are analysed.

In Step 4, i.e., identifying UCAs, the idea is to identify possible manners in which inadequate control can occur. Leveson[27] defines four possible manners in which this may occur as:

1. A necessary control action is not provided (or is not followed/executed).
2. An unsafe control action is provided.
3. A potentially safe control action is provided too late or too early.
4. A control action required for safety is applied too long or stopped too soon.

Considering each responsibility of each controller together with each item in the above list can identify the potential UCAs for a system.

Step 5 is to determine how each of the UCAs could occur by identifying causal factors and scenarios. This is achieved by investigating each part of the control loop or control hierarchy and assessing whether any of the parts could cause the UCA in question. As an aid in this step, Leveson[29] provides a list of generic causal factors, while Leveson[27] maps these causal factors into a generic control loop, (see Leveson[27] p. 223). Examples of such causal factors are inadequate sensor operation and process-model inconsistency. Bladine[30] argues that this representation is impractical, because many of the causal factors are not disjoint explanations of a UCA. For example, the explanation for process-model inconsistency is, in many cases, inadequate sensor performance. As an alternative, the tree structure shown in Bladine[30] (page 172) is suggested.

Figure 1 illustrates the workflow and the input/output-relations between the various steps when performing STPA. The system understanding developed in Step 1 is used in order to identify system accidents, corresponding hazards (i.e., hazards that may lead to the accidents) and safety constraints. The control structure is used to define responsibilities and to identify process models for the controllers. The controller responsibilities and process models are used to identify UCAs that may result in the hazardous states related to the system-level accidents. In Step 5, manners in which UCAs may occur, and how, are identified. At this stage, considering the process models of the responsible controller is highly relevant, because the process model is often involved in the scenarios. Finally, in Step 6, safety constraints at the UCA level, scenario level, as well as safety constraints related to each causal factor can be developed. An advantage of this is that once a safety constraint is developed at a low level, e.g., connected to a certain scenario or a causal factor, this safety constraint can be traced up to a certain UCA or the corresponding safety constraint and further up to the system-level accident.

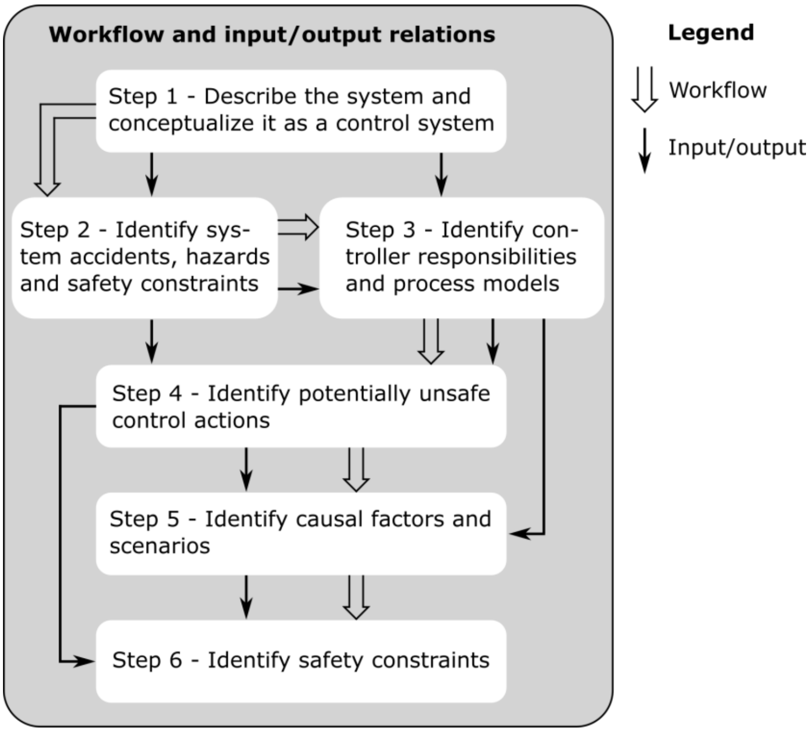
Workflow and input/output relations
Step 1 - Describe the system and conceptualize it as a control system
Step 2 - Identify system accidents, hazards and safety constraints
Step 3 - Identify controller responsibilities and process models
Step 4 - Identify potentially unsafe control actions
Step 5 - Identify causal factors and scenarios
Step 6 - Identify safety constraints
Legend
Workflow
Input/output

Figure 1: Workflow and input/output relations when performing the STPA analysis.

4. Analysis

In this section, each of the steps described above is applied to a DP system. The intention is to demonstrate how a DP system can be modelled as a control system and analyzed accordingly. As such, we seek to keep the system as generic as possible, such that the case study can be used as a foundation for conducting detailed STPA analysis for any specific vessel or operation. Therefore, special emphasis is put on the three first steps, as these lay the engineering foundation for the STPA.

Figure 2 gives a brief description of how data has been gathered and processed, the output of each step in terms of figures and tables, and how this relates to other steps in the process. The Figure also serves as an overview of the analysis.

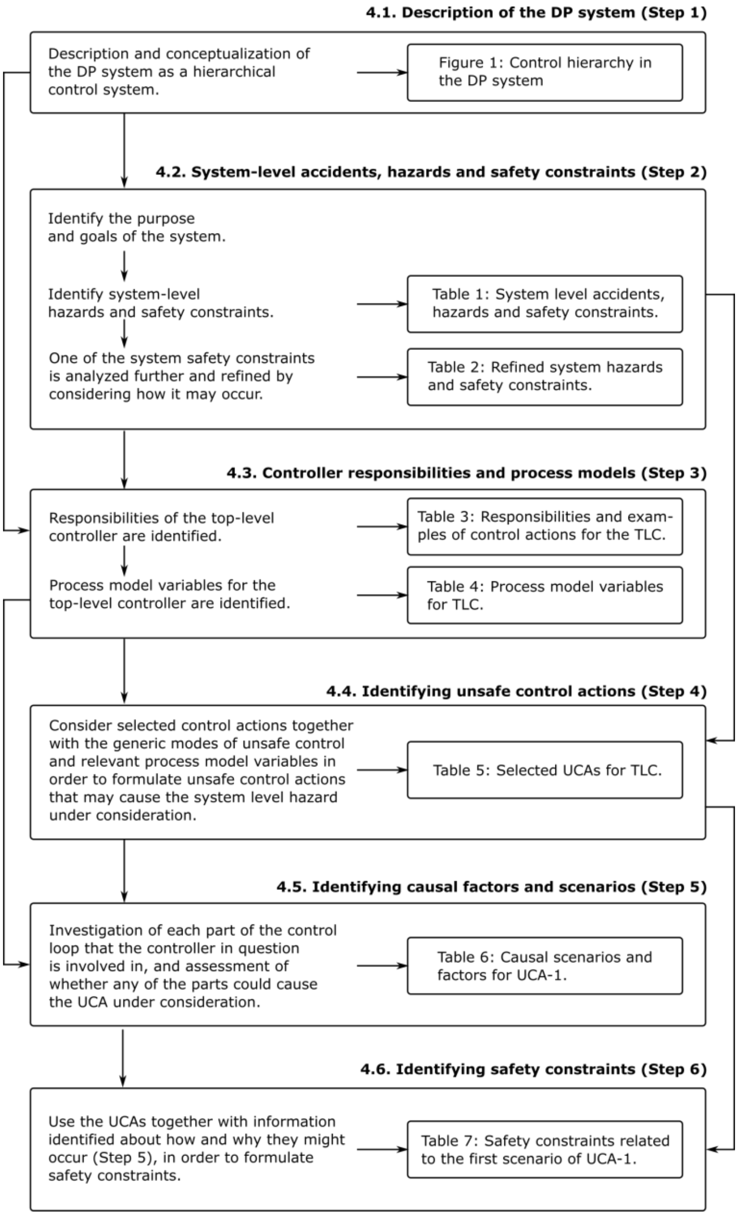
4.1. Description of the DP system (Step 1)
Description and conceptualization of the DP system as a hierarchical control system.
Figure 1: Control hierarchy in the DP system
4.2. System-level accidents, hazards and safety constraints (Step 2)
Identify the purpose and goals of the system.
Identify system-level hazards and safety constraints.
Table 1: System level accidents, hazards and safety constraints.
One of the system safety constraints is analyzed further and refined by considering how it may occur.
Table 2: Refined system hazards and safety constraints.
4.3. Controller responsibilities and process models (Step 3)
Responsibilities of the top-level controller are identified.
Table 3: Responsibilities and examples of control actions for the TLC.
Process model variables for the top-level controller are identified.
Table 4: Process model variables for TLC.
4.4. Identifying unsafe control actions (Step 4)
Consider selected control actions together with the generic modes of unsafe control and relevant process model variables in order to formulate unsafe control actions that may cause the system level hazard under consideration.
Table 5: Selected UCAs for TLC.
4.5. Identifying causal factors and scenarios (Step 5)
Investigation of each part of the control loop that the controller in question is involved in, and assessment of whether any of the parts could cause the UCA under consideration.
Table 6: Causal scenarios and factors for UCA-1.
4.6. Identifying safety constraints (Step 6)
Use the UCAs together with information identified about how and why they might occur (Step 5), in order to formulate safety constraints.
Table 7: Safety constraints related to the first scenario of UCA-1.

Figure 2: Process overview map.

4.1. DP system description (Step 1)

In the first step, the DP-system is described and conceptualized as a control system. This is necessary, because one of the fundamental ideas behind STPA is to view safety as a control problem.

The intention of the DP system is to enable position and heading keeping along with slow and precise navigation of the DP vessel by means of thruster force. For the thrusters to create the necessary forces, suitable control signals for the thrusters must be developed, and adequate amounts of power for the thrusters to satisfy the commands must be available. Figure 3 shows the functional control structure of the DP system. The system consists of a controller controlling an actuator system, and a disturbance-processes (wind, waves and current). The actuators and disturbances induce a response on the motion of the vessel. The objectives of the controller are to cancel the response of the disturbing process and to induce the desired motion on the vessel by providing suitable commands to the actuator system.

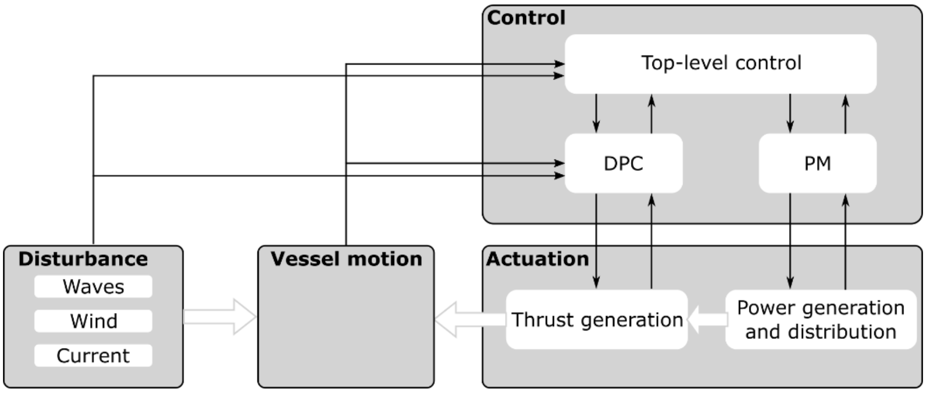

Figure 3: Control hierarchy in the DP system.

The controller can be decomposed into top-level control (TLC), DP-control (DPC) and power management (PM), while the actuator system can be decomposed into thrust generation, and generation and distribution of power. The TLC represents the overall mission control, i.e., control over system configurations, along with strategic decision making, such as whether or not to continue the mission under given circumstances. Furthermore, the TLC must decide on and communicate to the DPC the desired motion of the vessel. The DPC is responsible for implementing relevant configurations commanded from the TLC and for providing each thruster with command signals so that the desired motion of the vessel is realized. The function of the PM is to affect the desired power generation and distribution configurations provided by the TLC. Note, these three controllers (TLC, DPC and PM) are not to be taken as subsystems in the DP system, but rather as groups of functions.

The actuator system can be decomposed into a power system and a thruster system. The thruster system receives command signals from the DP control and draws power generated in the power system in order to actuate the commands.

To find individual commands for each thruster under DP-control, it is necessary to calculate a thrust-vector command in surge, sway and yaw, i.e., forces in the forward and sideways direction and a torque about the vertical axis.[31] This is the thrust vector, which, if applied to the vessel, will induce the desired vessel motion. The thrust-vector command can be calculated from a comparison between the current position, velocity, yaw angle and turn rate and the corresponding desired states, i.e., the states representing the desired motion or control objectives.[31] The current motion states are found by using measurements of the position and heading. The position can be measured by means of Differential Global Positioning Systems[2] (DGPS), and heading measurements can be obtained from a gyro.[31] The remaining motion states are estimated and the position and heading measurements filtered by means of a vessel observer, often implemented as a Kalman-filter. Thrust allocation refers to the problem of finding thrust and direction command for each of the thrusters under DP control,[31] i.e., finding a thrust-force command (and a direction command for thrusters with variable direction, such as azimuth thrusters), which, if followed, will result in the thrust-vector command being satisfied. Thrust allocation is usually calculated by using some kind of optimization criterion, such as minimization of the power consumption.[32]

For the thrusters to satisfy the commands, adequate amounts of power must be available. Today, most DP vessels are equipped with diesel-electric power systems.[33] This means that the thrusters are driven by electric motors, drawing electrical power from an electric bus supplied by diesel generators. In order to provide redundancy for DP Class 2 and 3 vessels, the electrical bus is commonly split into two or more separations so that only a part of the power system can be directly affected by a single fault, such as a short circuit[21]. Recent years have seen a fast pace of development in the diesel-electric power systems. Examples are inclusion of energy storage units (e.g., batteries), alternative power sources (e.g., nuclear steam generators, liquid natural gas (LNG) engines and fuel cells) and a conversion from AC distribution to DC distribution.[33, 34] In this analysis, we do not specify any particular power-system solution but, instead, try to keep the analysis at a “generic” level.

4.2. System accidents, hazards and safety constraints (Step 2)

Unsafe control actions, causal scenarios and safety constraints should always be possible to trace back or relate to system-level accidents, hazards and safety constraints. By defining the system-level accidents, we define what we want to avoid. By defining the system-level hazards and safety constraints, we define which states

might result in the accidents and how we can avoid those states. In this section, a discussion on the system-level accidents, hazards and safety constraints, is provided. The objective of the discussion is to reveal data and reasoning for the data presented in Table 1 and
Table 2. The starting point of this discussion is to ask what the control objectives and purposes of the system are.

The control objectives depend on the function of the vessel in the operational context. If, for example, the operation is offshore drilling and the role of the DP vessel is to serve as the drilling platform, the motion-control objective of the DP systems would be to keep the position and heading fixed. Instead of taking loss of position as the system-level accident, we define the accidents in terms of losses that may occur if the motion of the vessel is unsuitable with respect to the operational function of the vessel, (i.e., the role of the vessel in the operational context). Such accidents might occur, either if the motion-control objectives are not followed or if the motion-control objectives are not suitable with respect to the operational function of the vessel. System-level safety constraints can be derived directly from these hazards. First, we require that adequate control over the motion of the vessel must be maintained and, second, that the motion-control objectives must be in line with the operational function of the vessel. The system-level accidents, hazards and safety constraints are summarized in Table 1, where the abbreviations SLA, SLH and SLSC denote system-level accident, system-level hazard and system-level safety constraint, respectively.

Table 1: System-level accident, hazards and safety constraints.

System Accident	System Hazards	System Safety Constraints
SLA-1: Loss of life, damage to property or the environment, or loss of mission, due to unsuitable motion of the vessel.	**SLH-1:** Vessel motion is not controlled according to the motion-control objectives.	**SLSC-1:** Adequate control over the motion of the vessel must be maintained.
	SLH-2: The motion-control objectives are not in line with the operational function of the vessel.	**SLSC-2:** Motion-control objectives must be in line with the operational function of the vessel.

To proceed, it is necessary to refine the system-level safety constraints to a general-function level (see the discussion on levels of abstractions in Rasmussen).[35] They are found to be too abstract to enable a discussion of specific control actions. In other words, it is necessary to ask *how* adequate motion of the vessel can be maintained and *how* motion-control objectives can be ensured to be in line with the operational function of the vessel. The answer to the former of these questions is given by the only means by which the DP system can control the motion of the vessel, namely that of producing the resultant thrust force and yawing torque, which induces the desired motion. This force and yawing torque will be produced, given that the two general functions listed in

Table 2 are satisfied.

The latter question is more difficult to answer, because there are several means to the end, and they are dependent upon the operation and upon the specific context in which the operation is taking place. For example, if the vessel in question is a MODU and drilling is being performed, the control objectives are obviously to keep position over the well. If the vessel is an icebreaking vessel charged with breaking up drift ice before the ice collides with a MODU or some other critical object, the motion-control objective will become more obscure. Questions – such as: How should the vessel path be planned to minimize the ice loads on the MODU? – must be answered. These questions, in turn, depend on variables, such as the velocity and direction of the drift ice (e.g., which ice formations could possibly collide with the MODU, and when) and the ice-thickness distribution (i.e., which parts of the drifting ice would disturb the critical object the most). In general, however, in order to keep control objectives in line with the operational function of the vessel, it is necessary to establish a definition of the operational function of the vessel and to derive constraints on the motion of the vessel, based on the function.

In order to limit the length of the presentation in this article, the focus in the following is on maintaining adequate control over the motion of the vessel, i.e., studying how SLSC-1 can be enforced. More specifically, the focus will be on SLSC-1.2, ensuring that adequate amounts of power are available for producing the required thrust force.

Table 2: Refined system hazards and safety constraints.

System Safety Constraint	Refined System Hazard	Refined System Safety Constraints
SLSC-1: Adequate control over the motion of the vessel must be maintained.	**SLH-1.1:** Thrusters are not controlled in a manner that satisfies the control objectives.	**SLSC-1.1:** Thrusters must be controlled so that the resultant thruster forces induce vessel motion according to objectives.

	SLH-1.2: Adequate amounts of power are not available for thrusters.	**SLSC-1.2:** Adequate amounts of power must be made available for producing the required thrust force.

4.3. Controller responsibilities and process models (Step 3)

To identify UCAs, it is necessary to define what the different responsibilities of each controller in the control hierarchy are. This is because, in STPA, each responsibility or, alternatively, each specific control action derived from the responsibilities, is considered with respect to whether it can cause inadequate enforcement of safety constraints according to the four generic manners in which inadequate control can occur. Based on the above description, responsibilities for each of the controllers can be defined. Relevant process-model variables can be identified based on the control responsibilities. To limit the scope of this presentation, responsibilities and process-model variables are formulated only for the TLC.

At the system level, the TLC has only two responsibilities. These are closely related to the refined system-level safety constraints listed in Table 1. First, it is responsible for formulating (and communicating) the motion-control objectives and, second, for configuring the DP system so that is able to satisfy the provided control objectives, or simply making sure that the motion-control objectives are met. The former of these responsibilities can be refined into specifying DP reference and selecting DP mode. DP reference can be position and heading set points if the motion-control objective is station keeping. Alternatively, it can be a moving reference based on the motion of a target vehicle along with a minimum and maximum separation, if the objective is to track a target vessel. The second responsibility can be refined into configuring system functions, such as the position reference and state-estimation functions, thrust generation and generation and distribution of power. This is summarized in Table 3, where also examples of specific control actions are provided.

In addition to considering the responsibilities of the controllers, it is necessary to consider the process models of the controllers. Thomas[36] argues that a description of a UCA must contain a context, along with the control responsibility or control action. As an example, a control action for the TLC is to put power sources online. Not putting an additional power source online might be an unsafe control action. This is, however, not the case in most situations, and as such, a more specific context is necessary for the UCA. A more appropriate UCA would be, for example, that TLC does not put an additional power source online when the available power for the thrust generation is insufficient. In this case, the power availability is a variable, and when this variable takes the value *insufficient*, it is unsafe not to put an additional power source online. Furthermore, process models are also important when identifying scenarios and causal factors. The reason why an additional power source is not put online when available power is insufficient might be that the TLC process-model variable *available power* had not been updated from the value *sufficient* to the value *insufficient*, even though the available power had actually made that transition.

Table 3: Responsibilities and examples of control actions for the top-level control (TLC).

Responsibilities	**Description**	**Examples of control actions**
Specify DP reference	Specify, e.g., desired position and heading, target to track, path to follow or velocity.	Provide position set-point. Change position set-point. Provide virtual center of yaw rotation.
DP mode selection	Define in which mode to operate the DP system.	Go to station-keeping mode. Go to target-tracking mode.
Configure position reference and state estimation	Select, enable and calibrate position-reference devices and position-signal treatment parameters.	Select a position-reference system for DP. Set signal-variance alarm limits.
Configure thruster generation	Set up and reconfigure thruster system and individual thrusters.	Enable thruster for DP control. Disable thruster for DP control. Fix azimuth direction. Release azimuth direction. Restrict azimuth angle within range.
Configure power generation and distribution	Set up and reconfigure power sources and power distribution.	Put power source online (engage a particular power source).

	Put power source offline (disengage a particular power source). Open circuit breakers (change the manner in which power is distributed). Close circuit breakers.

Process model variables relevant for the different responsibilities and control actions for the TLC are defined and described in

Table 4. The first column contains the identifier for each process variable, where PV is an abbreviation for process variable. The second column provides the process variable, and the third column provides description or possible values of the variables.

Table 4: Process model variables for the TLC.

ID	Process variables	Description/possible values
PV-1	Suitable modes of operation	Relates to the function of the vessel in the operation. For example, if a fixed position is to be maintained, automatic position-keeping mode may be suitable.
PV-2	Actual mode of operation	What the current mode and mode configurations are.
PV-3	Suitable reference states	Where should the vessel be stationed, which path to follow, or which target should be tracked, and how close?
PV-4	Actual motion states of the vessel	What is, e.g., the position, and does it coincide sufficiently with the desired one?
PV-5	Level of vessel actuation	Whether or not the level of actuation is sufficient.
PV-6	Thrusters under DP control	Which thrusters are currently under DP control?

PV-7	Thruster saturation	Whether any of the thrusters under DP control are saturated.
PV-8	Working order of each thruster	Whether or not the thrusters are taking and following commands adequately.
PV-9	Allocation setting for each azimuth	If azimuth thrusters are fixed to a specific angle, restricted to a range or free to rotate.
PV-10	Level of available power	Quantitative measure of the difference in consumed power and maximal capacity in the current configuration.
PV-11	Available power adequacy	Whether or not the quantitative measure on available power is sufficient.
PV-12	A belief regarding available power in the near future	An opinion about whether the available power will increase or decrease in the future along with worst-case scenarios.
PV-13	Behavioral state of the power units	Working/not working, behaving erratically (unstable).
PV-14	Online power sources	Which power sources are currently online?
PV-15	State of each circuit breaker	Open/closed. This defines how the power is distributed.

4.4. Identifying unsafe control actions (Step 4)

In the previous step, responsibilities, some examples of possible control actions as well as process-model variables for the TLC were defined. In this step, we use the control actions and process-model variables in order to identify UCAs.Table 5 presents the UCAs identified for two of the control actions (*put power source online* and *put power source offline*) defined for the TLC. The UCAs are identified by considering each of the two control actions together with each of the generic modes of unsafe control and relevant process model variables.

Table 5: Selected UCAs for TLC.

Control Action	**Mode**	**Unsafe control action**
Put power source online	Not provided causes hazard	**UCA-1:** Additional power source is not put online when available power is TBD close to insufficient. *Rationale: If power consumption increase or capacity is reduced rapidly, there may not be enough time available to engage an additional power source.*
	Provided causes hazard	**UCA-2:** A power source that is not in proper working order is put online. *Rationale: The power source may disturb the power generation and distribution by sudden dropout or erratic behavior.* **UCA-3:** An already-online power source is commanded online. *Rationale: Possible repeat-errors.*
	Provided too early/too late causes hazard	**UCA-4:** Additional power source is put online too late when available power is decreasing. *Rationale: Available power will become insufficient if there is not enough time to increase the capacity.*
Put power source offline	Not provided causes hazard	**UCA-5:** An online power source that is not working properly is not put offline. *Rationale: The power source that is not working properly is likely to disturb the power generation and distribution.*
	Provided causes hazard	**UCA-6:** A power source is put offline when this will result in insufficient amounts of available power. **UCA-7:** A power source that is already offline is commanded offline. *Rationale: Possible repeat errors.*

4.5. Identifying causal factors and scenarios (Step 5)

In the previous step, a number of potentially unsafe control actions were identified. To design strategies for avoiding these (i.e., safety constraints), it might be useful to enhance our insight as to how and why they can occur. This is achieved by identifying scenarios (i.e., manners in which the UCAs may occur) and causal factors (i.e., reasons why the scenarios may take place). In Table 6, we present scenarios and causal factors for UCA-1.

Table 6: Causal scenarios and factors for UCA-1.

UCA-1: Additional power source is not put online when available power is TBD close to insufficient

ID	Scenario	Possible reasons (causal factors)
S-1	TLC does not realize that power available is too low.	**a)** Information about power consumption is missing, delayed or wrong. **b)** TLC thinks power-production capacity is different from what it actually is, because a power source is not able to deliver according the rated power. **c)** TLC thinks power-production capacity is different from what it actually is, because TLC has wrong information about rated power. **d)** Production capacity is less than TLC believes, because a power source that TLC believes to be online is actually offline. **e)** TLC does not pay attention to available power.
S-2	Load increases so rapidly that there is not sufficient time to engage an additional power source.	**a)** Sudden non-DP event, such as start-up of hydraulic pump or drilling equipment. **b)** Fault in thruster system (e.g., a thruster failing to full power).
S-3	Sudden or rapid reduction in power production/supply so that there is not enough time to engage additional power source.	**a)** Loss or suddenly reduced performance of power source. **b)** Power suddenly fails to be distributed or distribution changes (e.g., a circuit breaker changes state).
S-4	TLC is aware that available power may become insufficient, but there are no additional power sources to put online.	**a)** All power sources are currently utilized. **b)** The remaining power sources are not working properly. **c)** There are additional power sources, but they are not compatible with the current configuration of the power system or the current power source.
S-5	TLC believes that there are no additional power sources to put online, even though there are.	**a)** Power sources that are offline are believed to be online, because their status was not updated or TLC did not register the update the last time they were put offline.

	b) Power sources that are working properly are believed to be not working. (They may, for example, have been not working previously and repaired, but the repair has not been reported to TLC).
S-6 Additional power sources are commanded online by TLC, but command is not followed.	**a)** Power management does not receive the command, because the command is interrupted. **b)** Power management misinterprets the command, (e.g., believing that the command is regarding another power source). **c)** Command regarding the wrong power source is issued. **d)** Power management is not able to actuate the command (i.e., put power source online). **e)** Power source is put online, but not able to take load.

4.6. Identifying safety constraints (Step 6)

In this step, safety constraints related to UCA-1 and the corresponding scenarios found in the previous step are identified. Safety constraints can be seen as controls implemented to ensure that inadequate safety control does not occur, or to reduce the likelihood or mitigate the consequences of inadequate control. In this analysis, a safety constraint is formulated on the UCA level, i.e., a constraint aimed at avoiding UCA-1 from occurring. This safety constraint is refined into more detail by considering each of the scenarios identified in the previous step. Because UCA-1 relates to the system-level hazard SLH-1.2, the safety constraint at the UCA-level can be viewed as a part of a refinement of the system-level safety constraint SLSC-1.2. This safety constraint can be refined further by considering the scenarios identified for UCA-1, and each of the causal factors related to each of the scenarios can be used to produce safety constraints that are yet more specific. Table 7 presents the identified safety constraints for scenario S-1. The first column, denoted *relations*, illustrates from which level the corresponding safety constraints are derived.

Table 7: Safety constraints related to the first scenario of UCA-1.

Relation	Safety constraint
UCA-1	Additional power source must be put online when available power is TBD close to insufficient. (TBD depends on the nature of available power sources).
S-1	TLC must detect that available power is too low when this is the case.

a) Correct information about power consumption (i.e., instant production) must always be available for TLC.
Provisions must be made for the case when information about consumed power goes missing, such as procedures stating that a vessel shall disengage from an operation as fast as safely possible.

b) Periodic tests of maximum performance should be carried out to confirm that the performance of the power sources are according to rated values.

c) Correct information about the rated power of each installed power source must be available for TLC.

d) Updated information about which power sources are online must always be available for TLC.

e) Suitable notification must be provided for TLC whenever available power makes a transition from adequate to inadequate in order to increase the likelihood that the TLC process-model variable (available power) is updated.

5. Results and discussion

The objective of this article is to assess the feasibility of using the STPA for hazard identification and assessment of complex and automated systems like the DP system and, in particular, to assess whether STPA can be used to expand the current view on safety of DP systems, and to provide an operational context for verification of these systems. An adapted version of STPA has been presented, and a case study of a generic DP system has been conducted, where a broad approach is taken initially before selected parts relating to the operation of the power system are investigated more in detail.

STPA may be considered feasible for risk analysis of DP systems in two possible manners:

1. STPA may replace the current DP FMEA. For this conclusion to be reached, it has to cover all the functions of the DP FMEA and offer significant advantages.
2. STPA may be considered as complementary to the DP FMEA, providing a better risk picture of the DP system if performed, additionally. In this case, it

must be demonstrated that there are important issues not covered properly by the DP FMEA, which would be covered by STPA.

To assess whether STPA satisfies one of the two situations above, both DP FMEA and STPA have been assessed, according to the following six criteria of feasibility:

1. **Requires detailed design documents:** This is an important consideration because DP systems are typically composed of a large number of subsystems provided by different vendors, some of which may be reluctant to share information about how their systems work. This criterion also indicates how early in the system design process the analyses can be performed. We assume that starting safety considerations early in the design phase is beneficial both in terms of resulting system safety level and in terms of cost.
2. **Areas of focus:** Can be used to assess whether the areas of focus are complementary, redundant or overlapping.
3. **Objective of analysis:** Compares the objectives of the DP FMEA to those of STPA.
4. **Treatment of software:** DP systems are composed of a great number of computer control systems with the associated software. As such, an adequate treatment of software is necessary.
5. **Treatment of human in the loop:** Currently, the human operators are situated at the top of the DP system control hierarchy at the operational level (e.g., in the TCL). As such, adequate treatment of this element is of great importance.
6. **Generates input to verification tests:** The DP FMEA is often used for verification of redundancy in DP systems, and it is, as such, necessary to evaluate whether STPA also can serve this function and to which extent.

Table 8 presents the authors’ evaluation of the feasibility of STPA and DP FMEA, according to the criteria listed above. Arguments and observations supporting these assessments are provided in the following.

Table 8: Criteria used for assessing the feasibility of DP FMEA and STPA

	Criteria	**Requires detailed design plans**	**Areas of focus**	**Objective of analysis**	**Treatment of software**	**Treatment of human in the loop**	**Generates input to verification test**
Method	**DP FMEA**	Yes	Robustness against loss of position,	Verify that no single failure can result in	Failed/not failed – considers software as	Whether an inadvertent act can	Yes

		single point failures.	loss of position.	a component.	cause loss of position.	
STPA/case -study	No	Safety, unsafe control.	Identify how unsafe control may occur and corresponding safety constraints.	How software can operate unsafely.	How humans can operate unsafely.	Yes

5.1. Requires detailed design documents

By taking a purpose-oriented view of the system, STPA turns out to be able to provide useful output without having access to detailed knowledge about the system in question. Consider, for example, a vessel where the power management system (PMS) is responsible for putting power sources online and offline according to power demand. All the safety constraints presented in Table 7 would be relevant for the design and operation of the PMS in this case. As such, the analysis in the case study has produced safety constraints for the design and operation of a PMS without having knowledge about the particular implementation in question, and without having specified whether the PMS or a human operator is responsible for accomplishing the task in question. In contrast, a DP FMEA would assume that the PMS was built and operated according to regulations, due to lack of information about the software and the system design.

5.2. Areas of focus

Currently, DP-system safety is focused on robustness against loss of position in the event of a single-component failure.[8] By viewing system safety as a control problem, it becomes apparent that *loss of position* is too narrow as an accident definition for the risk analysis. Instead, by considering the control objectives and system purpose, we define the system accident in Table 1 in terms of losses that may occur if the motion of the vessel is unsuitable with respect to the operational function. This, unlike the term *loss of position,* does, for example, not exclude cases where the unsafe control objectives cause accidents, such as, if the vessel is positioned at an unsafe position because it was commanded to be there.

The DP FMEA has a relatively clear area of focus; robustness against loss of position in the event of single-point failures. The focus of the STPA, on the other hand, is not so specific. The focus of the analysis is on whatever or whoever may be seen as controllers in the system, and on how the control may be unsafe. This does not exclude single-point component failures, as these in many cases may be possible causes for unsafe control.

5.3. Objective of the analysis

A DP FMEA does not necessarily consider how the system should be operated besides stating that the analysis is only valid as long as there are no active alarms, the system is set up according to class regulations, etc. As such, a safe state of operation is briefly defined before the analyst proceeds to verifying that the defined safe state actually is safe, where safety is considered in terms of whether a single point failure can cause loss of position. STPA, on the other hand, defines unsafe states in terms of system-level hazards and proceeds by identifying how these unsafe states may be inadvertently entered and how we can avoid entering the unsafe states. The key difference is that the DP FMEA assumes that the only manner in which the system will leave the safe state is through a single failure (rendering the system no longer redundant), while in the STPA, the main objective is to identify safety constraints that will ensure that the system avoids reaching hazardous states. This is important because there are manners in which an unsafe state may be entered which does not involve single-point failures and which could occur on a perfectly redundant vessel. For example, every scenario presented in Table 6 may occur without component failures (see, for example, the causal factors in the same Table) and may still result in loss of position, due to insufficient amounts of available power. Consider, for example, causal factor (c), scenario S-1 in Table 6. In this case, an additional power source is not put online when necessary, because the TLC believes the rated power of one or some of the active power sources to be different than what it actually is. No amount of redundancy verification can protect against this scenario occurring, as it does not involve any failures.

Obviously, it is important to verify that a vessel is actually built according to requirements (e.g., that the system is redundant). To ensure this, it is necessary to go through the technical system and verify that it is designed in such a manner. In scenario S-3, causal factor (a), loss or suddenly reduced performance of a power source can lead to a sudden reduction in power production such that the available power becomes insufficient before an additional power source can be engaged. If safety constraints for this scenario were to be developed, it would be natural to implement a constraint limiting the consequence of a short circuit on the electrical network. Such a constraint could be that the technical design must be redundant (for example, ensuring that a short circuit can travel through a limited part of the system, only). One could, perhaps, further identify requirements necessary to ensure redundancy. At some point, however, it must be verified that these requirements are actually embedded in the design (for example, by verifying that unintended paths in which a short circuit may propagate, are not designed into the system). While the STPA method is designed to produce requirements (or constraints) for the design and operation intended to ensure that the system does not enter an unsafe state, the FMEA might be better suited to verify the actual design, if sufficient information about the design is available. It is, however, important to realize that verification of redundancy should only be a subset of the risk analysis of the DP-system..

The main objective of the DP FMEA is to verify that no single failure can result in loss of position, while the main objective of STPA is to identify how inadequate safety control may occur, and to identify safety constraints to mitigate it. Both these aspects are important. While the DP FMEA is suited for verifying a detailed design against requirements, the STPA is better suited to ensure that those requirements actually are safe and sufficient. This indicates that the methods are complementary.

5.4. Treatment of software

The manner in which software is treated is inadequate in the DP FMEA. It considers software in terms of consequences if the software or hardware on which it is embedded stops working. Further, it verifies that, if sensors or other software providing input fails, redundant sources for the input are available. There are two aspects to this: First, the DP FMEA considers which hardware (and embedded software) might be lost in the event of single failures, typically through loss of electrical power or signals through failures of sensors or signal busses. Second, what happens if software is lost and, in particular, whether or not there is redundant software, is considered. In short, FMEA seems to consider software only in terms of component failures. The STPA does not explicitly focus on software but, rather, on control and control actions. Considering control actions provides a broader perspective on software failures, because it also includes software-requirement errors. If the management of power sources is seen as a software responsibility, rather than an operator responsibility, all the scenarios identified in Table 6 can be seen as inadequate software performance. The underlying reasons for the inadequate software performance can be anything from insufficient vessel management (e.g., lacking routines for testing maximum performance of power sources, see causal factor (b), scenario S-1), to wrong calibration of software parameters (e.g., wrong information about rated power, see causal factor (c), scenario S-1). Another example is if TLC for some reason deactivates a generator when this will result in insufficient available power (UCA-6). Hence, we may conclude that STPA treats software thoroughly, while the DP FMEA does not.

5.5. Treatment of human in the loop

The DP FMEA does not mention or treat human operator concerns. STPA treats human operators in the same manner as software. Potentials for unsafe control are identified, regardless of whether the control is performed by human operators or software. As such the same arguments and examples as was provided above, is valid for human operators, as well as for software. If the management of power sources is seen as a human operator responsibility, rather than a software responsibility, all the scenarios identified in Table 6 can be seen as inadequate operator performance. We may conclude that a DP FMEA does not consider human operators at all, while the STPA treats the issue adequately.

5.6. Generates input for verification tests

Most DP-related class rules and recommended practices (e.g., DNV-GL[21]) require that various systems and components are verified through, e.g., sea trials. In many cases, however, such requirements fail to specify the context of the test. For example, the recommended FMEA practice[3] requires software to be tested to demonstrate how it responds to what is termed *relevant failures*. One challenge then is to determine what the meaning of *relevant failures* is, or which failures are relevant, and another one is to determine in which context the tests should be performed. The results from the analysis presented in this article (for example, the causal scenarios) may be suitable for specifying particularly interesting scenarios for testing. One example, identified in the analysis conducted in this article, is to test what happens if information about power consumption fails to reach the software responsible for activating power sources, or is wrong, in a situation where it is necessary to activate power source (causal factor (a), scenario 1, Table 6). Furthermore, the STPA safety constraints may, in some cases, point to straightforward, but important design issues that may be verified through simple inspection. For example, *correct information about the power consumption* is an identified safety constraint that is relevant when interfacing power sources to a PMS handling start and stop of diesel generators or an operator interface. This is something that can be verified upon system completion by inspection. That is, it can be verified that the correct information from the power plants are being issued to the correct input port of the relevant software, and that the signal represents the actual power consumption and is interpreted as such by the software in question. Thus, it may be feasible and beneficial to use STPA in order to provide an operational context for verification.

The DP FMEA also generates input for verification. This is mainly achieved by utilizing conclusions from the analysis, as test cases, e.g., as input to HIL testing. Mostly, such tests aim to verify that the vessel position can be maintained after single component failures, such as sensors, to ensure that the system is redundant. Sometimes, however, the analysts must make additional assumptions, for example, that some bus-tie breakers do not close upon partial blackout. Such assumptions are commonly reformulated into verification tests, as well.

5.7. Evaluating the feasibility of using STPA for risk analysis of DP systems

Table 8 presents the six feasibility criteria for assessing STPA and DP FMEA, qualitatively. The following observations are made from the discussions and Table 8:

- STPA can be applied without detailed design plans, whereas DP FMEA cannot. This means that STPA can be started at an earlier stage in the design process and will be more suitable for analyzing subsystems where only the interfaces and functionality is known.
- The DP FMEA is better suited than STPA for systematically going through design documentation and verifying that the system is designed according to requirements (e.g., verifying that the redundancy design intent is complied with).
- Contrary to SPTA, DP FMEA is not suited for verification of safety if the term safety is interpreted in a broader sense (systems perspective) than *robustness against loss of position.* The DP FMEA, unlike STPA, cannot analyze whether requirements are safe.
- Both methods can identify single point failures that may result in accidents. The DP FMEA may not necessarily be able to identify hazards emerging from the interaction between single point failures and software or human operators. Nor does it focus on human operators, or software, as such.
- Both methods can provide input to verification tests (e.g., HIL testing), but due to different scopes and areas of focus, some differences in test cases are likely.

6. Conclusion

This article has developed an adapted version of STPA specifically aimed at risk analysis of complex and automated maritime systems, such as the DP system. Further, the article has assessed the feasibility of using the STPA for hazard identification and assessment of a DP system, based on a case study and comparison with the currently used method; the DP FMEA. The DP FMEA is focused on verifying redundancy by ensuring that no single component failure can result in loss of position. One observation from the case study, which strongly supports the use of STPA, is that a number of manners, not involving component failures, in which safety constraints can be violated, have been identified. Consider, for example, when TLC does not realize that available power is too low because power-production capacity is different from what TLC believes, due to wrong information about rated power, (causal factor c), scenario S-1). Another example is that TLC believes that there are no additional power sources to put online, even though there are. This can occur when power sources that are offline are believed to be online because their status was not updated or TLC did not register the update the last time they were put offline. It can also occur or when power sources that are working properly are believed not to be working, (causal factor a) and b), scenario S-5). From this observation, it is clear that DP FMEA is not sufficient for risk analysis of DP systems.

For STPA to be considered as feasible for risk analysis of DP systems, it is not sufficient to show that the DP FMEA is insufficient. The STPA can serve either as a (i) complete replacement of DP FMEA, or (ii) as an additional risk analysis. In the former, STPA should provide the same output as DP FMEA and offer considerable advantages. In the latter, STPA should cover important issues not currently addressed by the DP FMEA. Based on six criteria for feasibility assessment, it was found that the only weakness of the STPA when compared to the DP FMEA is that it is not well suited for a systematic walk through of design documentation, such as electric diagrams, and verifying that the system is designed according to requirements. This is the main purpose and one of the strengths of the DP FMEA, assuming that the requirements in question are those prescribing that single failures not shall result in loss of position. On the other hand, the STPA is beneficial when the input to analysis is not detailed (e.g., in the early design phase), to verify safety in design plans and requirements, and to analyze software and human operators, adequately. Both methods were found to be able to generate input to verification tests and identify single point failures that may result in accidents. Hence, STPA as a complementary activity to the DP FMEA seems as the most feasible option and beneficial because the STPA covers important hazards not covered by the DP FMEA, and opposite.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Acknowledgments

The authors greatly appreciate discussions and input to the paper from Dr. HyungJu Kim, NTNU and Odd Ivar Haugen, Marine Cybernetics/DNVGL.

Founding

Rokseth and Utne acknowledge the funding through the project Design to verification of control systems for safe and energy-efficient vessels with hybrid power plants (D2V), where the Research Council of Norway is the main sponsor. NFR: 210670/070,223254/F50. This work was also partly supported by the Research Council of Norway through the Centres of Excellence funding scheme, project number 223254 - AMOS.

References

1. IMO. Guidelines for vessels with dynamic positioning systems (IMO MSC Circular 645). 1994.
2. Chen H, Moan T, Verhoeven H. Effect of DGPS failures on dynamic positioning of mobile drilling units in the North Sea. *Accident Analysis & Prevention. 2009*;41(6):1164-71.
3. DNV. Recomended practices DNV-RP-D102: Failure mode and effect analysis (FMEA) of redundant systems. 2012.
4. DNV-GL. Rules for classification of ships, part 6, chapter 3: Navigation, manoeuvring and position keeping. 2016.
5. Rausand M. Risk assessment, theory, methods, and applications: John Wiley & Sons, Ltd; 2011.
6. PSA. Utvikling i risikonivå - Norsk sokkel - Fase 3 rapport for 2002. 2003.
7. PSA. Risikonivå i petroleumsvirksomheten - Norsk sokkel 2013. 2013.
8. Spouge J. Review of methods for demonstrating redundancy in dynamic positioning systems for the offshore industry. 2004.
9. Vinnem JE, Hokstad P, Dammen T, Saele H, Chen H, Haver S, et al. Operational safety analysis of FPSO-shuttle tanker collision risk reveals areas of improvement. Offshore technology conference. 2003.
10. Verhoeven H, Chen H, Moan T. Safety of dynamic positioning operation on mobile offshore drilling unit. Dynamic Positioning Conference. 2004.

11. Phillips D, Deegan J. Risk analysis of a DP diving vessel up weather of platform and jack up. Dynamic positioning conference. 2005.
12. IMCA. Risk analysis of collision of dynamically positioned support vessel with offshore installations (115 DPVOA). 1994.
13. IMCA. Dynamic positioning: Station keeping incidents - Incidents reported for 2013 (DPSI 24). 2015.
14. Yuhan J. Offshore QRA: Assessing safety during DP operations [Master thesis]: Norwegian University of Science and Technology and Technical University of Denmark; 2014.
15. Dong Y, Rokseth B, Vinnem JE, Utne IB. Analysis of dynamic positioning system accidents and incidents with emphasis on root causes and barrier failures. Accepted for publication in: ESREL 2016 Proceedings. 2016.
16. Øien K. Risk indicators as a tool for risk control. *Reliability Engineering & System Safety*. 2001;74(2):129-45.
17. Chen H, Nygård B. Quantified risk analysis of DP operations - Principles and challenges. SPE International Conference and Exhibition on Health, Safety, Security, Environment, and Social Responsibility: Society of Petroleum Engineers. 2016.
18. Abrecht B, Leveson NG. Systems theoretic process analysis (STPA) of an offshore supply vessel dynamic positioning system. Massachusetts Institute of Technology. 2016.
19. Skogdalen J, Espen, Smogeli Ø. Looking forward - Reliability of safety-critical control systems on offshore drilling vessels. 2011.
20. Chen H, Moan T. DP incidents on mobile offshore drilling units on the Norwegian continental shelf. *Advances in safety and reliability*. 2005;1:337-44.
21. DNV-GL. Rules for classification of ships, part 6, chapter 26: Dynamic positioning systems with enhanced reliability. 2014.
22. ABS. Guide for dynamic positioning systems. 2013.
23. Chen H. Probabilistic evaluation of FPSO-tanker collision in tandem offloading operation [PhD thesis]: Norwegian University of Science and Technology; 2003.
24. Lundborg ME. Human technical factors in FPSO-shuttle tanker interactions and their influence on the collision risk during operations in the North Sea [Master thesis]: Norwegian University of Science and Technology; 2014.
25. Pride AS. Synergi database. 2005.
26. Rasmussen J. Risk management in a dynamic society: a modelling problem. *Safety Science*. 1997;27(2-3):183-213.
27. Leveson NG. Engineering a safer world: Systems thinking applied to safety: The MIT Press; 2011.
28. Rasmussen J. On the structure of knowledge-a morphology of metal models in a man-machine system context. DTIC Document, 1979.

29. Leveson NG. A new accident model for engineering safer systems. *Safety science.* 2004;42(4):237-70.
30. Bladine A. Systems theoretic hazard analysis (STPA) applied to the risk review of complex systems: An example from the medical device industry [PhD thesis]: Massachusetts Institute of Technology; 2013.
31. Sørensen AJ. A survey of dynamic positioning control systems. *Annual reviews in control*. 2011;35:123-36.
32. Radan D. Integrated control of marine electrical power systems [PhD thesis]: Norwegian University of Science and Technology; 2008.
33. Bø I, Torstein. Scenario- and optimization-based control of marine electric power systems [PhD thesis]: Norwegian Univeristy of Science and Technology; 2016.
34. Skjong E, Rødskar E, Molinas M, Johansen TA, Cunningham J. The marine vessel's electrical power system: from its birth to present day. *IEEE proceedings.* 2015.
35. Rasmussen J, Pejtersen AM, Goodstein LP. Cognitive systems engineering: John Wiley & Sons Inc; 1994.
36. Thomas J. Extending and automating a systems-theoretic hazard analysis for requirements generation and analysis [PhD thesis]: Massachusetts Institute of Technology; 2013.