Deriving Verification Objectives and Scenarios for Maritime Systems Using the Systems-Theoretic Process Analysis

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

The process applied for verification of maritime systems lacks the ability to properly examine complex networks of interconnections. Verification is mainly focused on single failures of components, not properly accounting for the complexity emerging through interactions between human operators, computer systems and electro-mechanical components. The problem apparently resides in the supporting studies, or the lack thereof, for the development of test cases. A new methodology that can be introduced to the current verification process for these systems is proposed in this article. It employs Systems-theoretic process analysis (STPA) to generate verification objectives and related hazardous scenarios. These specify or extend the scope and provide acceptance criteria for verification activities, and may further serve as input to test case generation. The method is used in a case study to identify verification objectives for an automated module in the power management system of a maritime vessel. The results show that the method is able to reduce the number of context variables that verification results depend upon, and to highlight remaining context dependency, to allow for an integrated system view. It will help capture accidental scenarios with more complex causal relations than what is currently considered during verification of these systems.

Keywords: Risk; Verification; STPA; Maritime Systems; Maritime Safety

1. Introduction

During recent decades, maritime vessels have evolved from assemblies of electro-mechanical components into complex systems featuring advanced automation such as dynamic positioning (DP) systems. Today, integrated software control systems are essential parts of all maritime vessels [1]. This evolution has enabled new types of operations, such as deep-water hydrocarbon exploration, which are both more complex in execution and associated with more severe consequences in the event of accidents. Loss of position for a dynamically positioned mobile offshore drilling unit (MODU) may, for example, result in a subsea blowout [2]. Therefore, risk management and system verification have become not only more challenging, but also more important. Skjetne and Sørensen [3] point out some characteristics and trends that contribute to the increased challenges of verification and testing of maritime vessels. Some of these are the increased use and dependence on computer-based systems, extended use of off-the-shelf technology, a drive towards low-cost solutions and the increased level of integration and system complexity.

A DP vessel is able to maintain its position and heading and to maneuver along a predefined track exclusively by means of automated thruster force [4]. Examples of typical applications of DP systems are positioning of MODUs, and positioning and maneuvering of crane vessels, shuttle tankers, cable and pipe layers, platform support vessels and diver support vessels. The consequences associated with loss of motion control for DP vessels can be, for example, blowouts, collisions and drowning of divers. Currently, the design requirements for DP systems address robustness against loss of position in the event of single failures by enforcing redundancy. Consequently, the main effort in verification is currently to verify technical redundancy.

The need for new methods for testing, verification and validation of advanced maritime systems was stated in a joint industry project documented in Skjetne and Sørensen [3] in 2004. The main reason for this need is the increased system complexity introduced by computer control systems, such as DP. The same year, Spouge [5] published a comprehensive review of the current methods for verifying redundancy in DP systems. Spouge concludes that failure mode and effect analysis (FMEA) may be a suitable tool, provided that sufficient guidance is given and that appropriate objectives for the analysis are formulated [5]. Some of the weaknesses identified in the report are that the current verification methods only consider technical failures, not human operators and onshore management, and that the methods may be unsuitable for some systems that are typically brought in by external vendors such as the DP control system and the power management system (PMS). The report does not discuss computer control systems or software in particular. A relatively recent method being employed in the maritime industry, and that addresses computer control systems and software, is HIL testing [6-8].

Guidelines and standards for software development and verification processes have during recent years appeared in the maritime industry [9]. In particular, the classification societies DNV-GL and ABS have developed class notations for software verification processes (see DNV-GL [10] and ABS [11]). Both these class notations focus on hardware in the loop (HIL) testing in order to provide a higher degree of certainty that systems meet applicable requirements and function as intended. DNV-GL addresses the verification challenges by publishing a recommended practice [12], introducing a specialized version of FMEA, aimed specifically at verifying redundancy in the DP system. In addition to the classification societies, organizations such as the International Maritime Contractors Association (IMCA) provide guidance on vessel design, on conducting FMEA for verification purposes, and on conducting sea-trials [13-15].

The current verification activities (i.e., FMEAs to demonstrate technical redundancy and verification tests such as practical sea-trials and HIL tests) focus on specific system dimensions, such as hardware redundancy and computer control. Emergent properties such as safety, however, are not properties associated only with the individual components or system dimensions. They emerge through attuned interactions between these components and dimensions. As a consequence, the safety of, for example, a piece of software, cannot be evaluated and verified outside the context of the system in which it is operating [16]. And indeed, Skjetne and Sørensen [3] find that one of the main types of software-related problems is interaction problems between hardware, software and the human operator. This conclusion is also supported in Dong et al. [17], where a number of DP accidents and incidents are analyzed, and it is found that the majority are influenced by both technical and human/operational factors.

Even if the specialized version of FMEA proposed by DNV-GL [12] is an improvement for DP vessel applications, the weaknesses of the FMEA method is well known. The system perspective necessary to cope with the current level of system complexity is lacking. Furthermore, it is focused solely on verifying technical redundancy, which is inadequate from a safety perspective for complex software-intensive systems [18, 19]. The FMEA process described in [12], is used as a tool to systematically going through the technical design of the system to ensure that it is designed according to certain requirements related to system redundancy, rather than as a traditional FMEA. An additional shortcoming with this is that it does not include any steps to ensure that the requirements themselves are safe for each particular system. The Systems-theoretic process analysis (STPA) is a relatively new hazard analysis technique based on the Systems-theoretic Accident Model and Processes (STAMP) [20-22]. The main idea in this accident causation model is that safety is a control problem, in accordance with the ideas presented in Rasmussen [23], and that accidents occur because of inadequate control and enforcement of safety constraints. The system is modeled as a hierarchical control structure, where each layer of control enforces control on the next layer. The objective when performing an STPA is to identify potentials for inadequate control, how inadequate control may occur in a system and to impose constraints on the control.

STPA has been successfully applied to a number of systems during recent years. Examples are safety analysis of defense systems such as a missile defense system [24], medical devices such as a radiation therapy system [25], air traffic control systems [26], security analyses where STPA is used in order to identify vulnerable system states [27], and hazard analyses for space craft [28]. Two applications for DP systems can also be found in the literature. Abrecht and Leveson [29] apply STPA to analyze a DP platform support vessel, and compare the results to independently conducted FMEA and fault tree analysis (FTA). Several safety concerns were identified in the STPA that were not identified in the other analyses. Rokseth et al. [19] present a case study for selected parts of the system of a generic DP vessel, and evaluate whether it is beneficial to replace the currently conducted FMEA with STPA or to combine the two methods. The conclusion is that a combination is most beneficial, but that FMEA alone is not sufficient to ensure safety. Rokseth et al. [19] also conclude that robustness against single point failures is not adequate in order to ensure the safety of DP systems, and that it would be beneficial to employ STPA to develop safer DP systems.

A safety engineering process that employs STPA for software development has been developed [30]. This process includes verification of software by building a safe behavior model based on results from an STPA. Software is verified against the safe behavior model by using formal software verification approaches. Although this method takes an integrated system view by applying STPA, only software is subject to verification.

The objective of this article is to present a methodology for systematically deriving verification objectives and determining the necessary scope of verification activities for complex maritime systems. The methodology can be used as input to improve the current verification activities, such as the FMEAs required by the classification societies to demonstrate redundancy, sea-trials and HIL tests, to better handle the complexity in the systems. A case study is performed to demonstrate the methodology, focusing on important functions in a marine diesel-electric power system.

When the proposed methodology is used as input to the specialized FMEAs required for DP vessels, the verification objectives will help ensure that sufficient guidance is given and that appropriate objectives for the analysis are formulated. Additionally, the verification objectives may help define more specific acceptance criteria than “No single failure shall result in loss of position”, and similar high-level criteria. When used as input for test activities such as practical sea-trials and HIL tests, the verification objectives will serve as input to the test case generation process. In this case, the verification objectives may define a suitable scope and specific acceptance criteria, and highlight relevant context.

The methodology, which is rooted in STPA, considers all system dimensions (such as human factors, software and physical components) as an integrated whole to capture potential safety concerns related to interactions between these dimensions, and to handle complexity. This means that the focus of the proposed methodology in this article is much wider than the current verification activities aiming to ensure that “No single component failure shall result in loss of position”. This is important not only because accidents can happen without the occurrence of component failures [19], but also because it is difficult to evaluate the consequences of events (such as a component failure) at a global system level during current verification activities. When observing outcomes of low-level tests at the system level, the outcome becomes too dependent on the circumstances in which the test is conducted, (i.e., too context-dependent), meaning that small variations in the context variables describing the circumstances (or test conditions) can potentially have a significant impact on the outcome of the tests. Thus, when testing a sequence of component failures in a random context, and observing the results at system level, it is not necessarily clear whether a successful outcome can be ascribed to system safety or to a favorable set of context variables. The proposed methodology both reduces the dependency of test results on context variables, and highlights and provides insight into the remaining ones. This is achieved by deriving verification objectives that can be observed and evaluated at a local level, while also examining how observations may be affected by the context. In other words, if we think of a scenario taking place during a test as a complex causal path that may result in some defined system loss, our objective is to enable observation of test results near the initiating event, rather than at the end of the causal path, while substituting the remaining causal development with the STPA.

The following section gives a brief overview of the currently employed verification process for DP systems along with a discussion of the requirements that this process aims to verify. In section 3, the proposed methodology is described in detail, including a description of STPA. The case study is presented in section 4. In section 5, the methodology is discussed in light of the results from the case study before a conclusion is provided in section 6.

2. DP system requirements and verification

The DP system life cycle is modeled in this article as consisting of four phases. These are illustrated in Figure 1 together with the current verification activities. The life cycle phases are (i) concept development, (ii) physical design and software development, (iii) installation, integration and commissioning, and (iv) operation. In the first phase (concept development), the vessel designers consider factors such as the industrial mission of the vessel and the geographic areas of operations. Based on this, general characteristics and vessel design philosophy can be produced (such as identifying which class certificates are needed).

The general characteristics and the vessel design philosophy can be used as input to the second phase (i.e., the physical design and software development). In this phase, specific requirements from classification societies must be considered in order to ensure that the desired class certificates can be obtained. The output from this process is all the necessary drawings, diagrams and specifications to vendors, etc. Currently, these documents, together with class rules, are used as input to the FMEA. Conclusions drawn and assumptions made in the FMEA can be verified in the verification tests (such as sea-trials and HIL tests). In the installation, integration and commissioning phase, the DP system is installed on the vessel, the various building blocks are integrated, the vessel is commissioned, and findings from the FMEA can be addressed. Before the final phase (the operations), sea-trials and possibly HIL tests are conducted.

During the design process, vendors and shipyards must comply with rules and regulations and consider standards such as the international standard for DP systems [4] provided by the International Maritime Organization (IMO), and class rules provided by classification societies such as DNV-GL when developing DP vessels. The international standard [4] specifies three DP equipment classes that, in effect, specify the level of redundancy for a vessel. For equipment class 1, loss of position may occur in the event of a single failure. For equipment class 2 and 3 vessels, single failure of an active component shall not result in loss of position. The requirement stating that single failures of any active component shall not result in loss of position will henceforth be referred to as “the single failure requirement”.

The verification and testing process consists of an FMEA to verify system design, and in particular, to demonstrate that the single failure requirement is satisfied, sea-trials to verify that the vessel is functioning according to the design intent and that the single failure requirement is satisfied (for class 2 and 3), and periodic trials with similar scopes. This process is focused on the redundancy and compliance with the single failure requirement. Most classification societies that offer additional class notations for DP, require that such an FMEA is conducted (see e.g., [31, 32]). HIL testing, on the other hand, has a strong focus on the software and computer control systems. According to Smogeli and Vik et al. [33], this activity can take place during the same phase as the sea-trials, and during the operational phase, for example, after software updates. In this case, we refer to the activity as HIL for vessels in operation (HIL VIO). Software in the loop (SIL) is a similar activity where software is executed on emulated hardware.

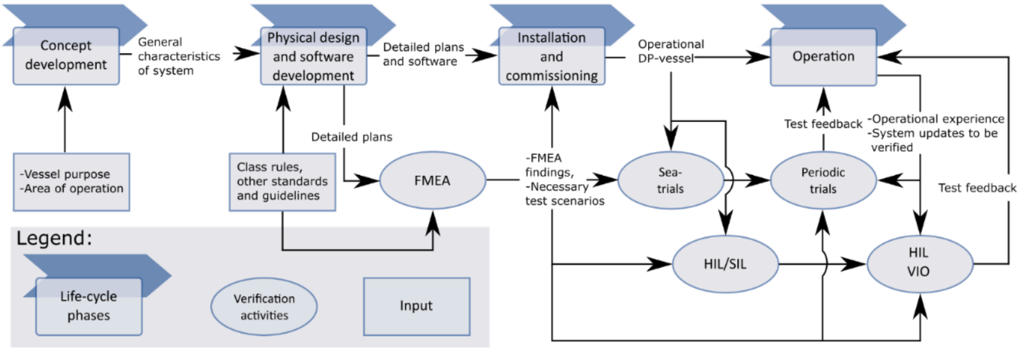

Figure 1: Verification activities and system life cycles

3. Methodology

The methodology proposed in this article is proposed as an addition to the verification process already established in the maritime industry. The methodology introduces STPA as part of the verification process to achieve an integrated system view and make a conceptual link between losses at system level, and localized verification test results. In the proposed methodology, STPA is used to identify safety constraints on system interactions, along with scenarios of violation. The safety constraints are translated into verification objectives. The verification objectives can then be processed further by using the methods that are currently employed in the verification process, such as FMEA, sea-trials, and HIL tests. Detailed test case generation is not within the scope of this article because the most suitable verification method will depend on the nature of each verification objective. Furthermore, we assume that detailed knowledge about the internal workings of different subsystems is unavailable because system vendors may be reluctant to share detailed information with third party verification organizations and system integrators. As such, verification organizations and system integrators may only have knowledge about input and output ports, and the functions of a system. In this approach, we therefore utilize functional knowledge of the system, and avoid relying on details about implementation (i.e., we take a black-box view).

The proposed verification method can be outlined in nine steps as follows:

1. Define the system accidents and system hazards.
2. Model the system as a hierarchical control structure.
3. Identify control action that may lead to a defined hazard, i.e. an unsafe control action (UCA).
4. Derive high-level safety constraints, aimed at ensuring that the UCAs cannot occur.
5. Identify how the high-level safety constraints may be violated (i.e., identify causal scenarios of violation), if they can be violated. It is important to specify the context in which the scenarios may cause violation of safety constraints. This may be achieved by describing the scenarios in a precise manner. It may also help to explicitly list relevant process variables and assign values or describe their states.
6. Identify potential conflicts between high-level safety constraints and resolve or store them for future reference. (Conflicts may have been revealed when developing scenarios of violation).
7. Scenarios of violation for the high-level safety constraints were identified in Step 5. It is necessary to develop safety constraints aimed at ensuring that these cannot occur. Examine whether scenarios of violation for these safety constraints can be found, and if so, identify safety constraints at this level as well. This process should be continued until either reasonable scenarios of violation cannot be identified, or the safety constraints can be considered as readily verifiable. It is important to be precise in terms of context when describing the scenarios.
8. Develop verification objectives based on the safety constraints in a hierarchical manner, meaning that high-level verification objectives should be derived from the high-level safety constraints, and lower-level verification objectives from the lower-level safety constraints. This is to ensure traceability, so that, if we are performing verification activities based on the lower-level safety constraints, we can always explain what higher-level objective we are trying to satisfy.
9. Decide how each verification objective should be processed further. The alternatives are:
    a. Specify or extend the scope and acceptance criteria of the DP FMEA.
    b. Can be verified on inspection of physical system.
    c. To be verified during sea-trials. (Note that refined processing, such as formal test case development, may be necessary).
    d. To be verified during HIL or SIL testing. (Note that refined processing, such as formal test case development, may be necessary).
    e. To be verified through a review of operational procedures and guidelines, or maintenance plans.
    f. Other activities, such as specialized STPA of a particular sub-system where the verification objective can be used in order to define the scope.

Figure 2 illustrates how the proposed method relates to the current verification process. In Step 1, system accidents and hazards are defined. In this step, general characteristics or desired characteristics should be taken into account, because the system accidents and hazards set the scope of the analysis. If for example, it is desired that the vessel should be as environmentally friendly as possible, the analyst should ensure that this becomes part of the verification scope during Step 1. In Step 2, input should be taken from the physical design and software development phase because functional descriptions and functional layout are necessary in order to develop the hierarchical control structure. In Steps 4 and 7, safety constraints are identified. At these stages, the class rules as well as other rules, standards and guidelines, should be considered as solutions for safety constraints (where applicable). Step 9, together with

Figure 2, illustrates how the verification objectives formulated in Step 8 may be distributed to other verification activities in the verification process.

The proposed methodology for identifying verification objectives (referred to as STPA VO in

Figure 2) can be conducted in parallel with the physical design and software development process. The main objective of steps 1-7 is to identify how unsafe control can occur, and how to avoid it. Identifying UCAs is achieved by considering whether each control action of each controller in the system can be unsafe in one of the following four ways [20]:

1. A necessary control action is not provided.
2. An unsafe control action is provided.
3. A potentially safe control action is provided too early or too late.
4. A potentially safe control action is provided for too long or stopped too early.

The proposed methodology will produce a hierarchy of verification objectives that can be distributed to other parts of the process for further processing. In particular, some of them can help define or extend the scope, objectives and acceptance criteria of verification activities, and some may be used in order to develop test cases for sea-trials, HIL/SIL tests, periodic trials, or HIL-VIO. One verification objective can be used as input for several parts of the process. It may, for example, be beneficial to analyze a verification objective further through the DP FMEA in order to generate test cases out of it. Note also that, in the case of software testing, a number of formal software verification methods [34, 35] can be used to refine the verification objectives into test cases. This part of the process is not considered as part of the methodology presented here, but rather as integral parts of the various verification activities such as HIL testing.

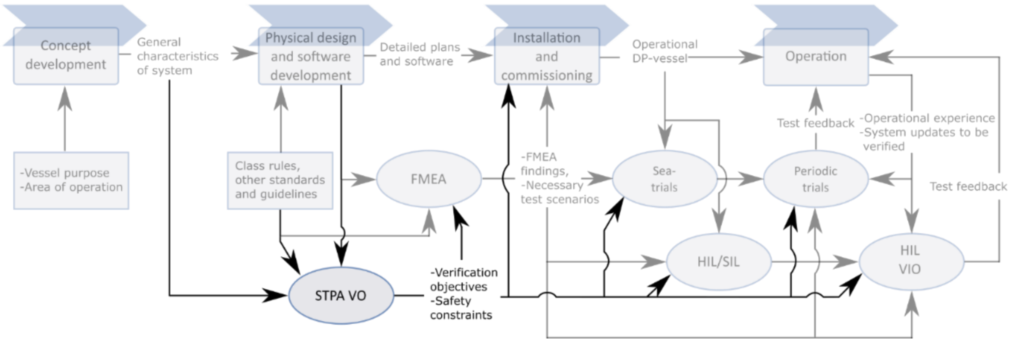

Figure 2: New proposed verification process. The STPA for identifying verification objectives, and its inputs and outputs, are highlighted.

4. Case Study

Diesel-electric power systems have become widely used in the maritime industry, mainly in cruise vessels, ferries, DP drilling vessels, thruster-assisted moored floating production facilities, shuttle tankers, cable layers, pipe layers, icebreakers and other ice-going vessels, platform supply vessels and warships [36]. One of the advantages of these power systems is that they provide flexibility in terms of the placement of components such as thrusters and power sources, because the power sources and consumers are not connected by a shaft, but by electrical wires.

A traditional maritime diesel-electric power system consists of several diesel generators (DGs), supplying power to an electrical bus. The electrical bus, in turn, distributes the power to various consumers. The main consumers of electrical power are thrusters and other propulsion units. In addition, consumers such as auxiliary equipment for DGs and thrusters, ship functions such as lighting, air conditioning, hot water and empowering of computer control systems, must be served from the power system. To increase the level of redundancy, the electrical bus can be separated into two or more segments by bus tie breakers, where each segment of the bus should be supplied by enough DGs to allow for continued operation if one of the other segments is lost. The power system is controlled by a power management system (PMS) and a human operator. To limit the extent of the case study, we consider a particular function in the PMS, responsible for automatically activating and deactivating DGs when necessary. This control module is referred to as Load Dependent Start and Stop (LDSS) of DGs.

4.1. Step 1: Defining system accidents and system hazards

The system hazards and accidents set the scope for verification of the system, and all resulting verification activities can be traced back to these. Table 1 and Table 2 describe the system accidents and hazards selected for this case study. These tables are not exhaustive, but they will serve to demonstrate the approach.

Table 1: System accidents.

Identifier	System accident description
A-1	Power system not able to serve loads. (Loss of motion control)
A-2	Full power system blackout. (Loss of motion control)
A-3	Partial power system blackout. (Loss of availability)
A-4	Unacceptable amounts of fuel consumption or greenhouse gas emissions

The first system accident reflects a situation where the vessel is not able to perform actions that it should have performed in order to satisfy control objectives because there is not enough power. Such situations arise, for example, when automatic load limiters restrict the power consumption of thrusters so that they are not able to fulfil their control objectives. The consequence of this is loss of control over the motion of the vessel. The second and third accidents reflect power system blackouts. The difference between a full and a partial blackout (A-2 and A-3) is that partial blackout means blackout of one or some, but not all, bus segments, whereas full blackout means blackout of the entire system. No motion control will be possible after a full blackout. A partial blackout is in many cases equivalent to loss of availability, as the technical power redundancy is lost. The fourth accident (unacceptable amounts of fuel consumption and emission of greenhouse gases) is included to demonstrate that the rather wide definition of the term system accident within the STAMP framework allows us to consider not only safety issues, but also other issues that may be relevant to stakeholders. Unacceptable amounts of fuel consumption or emissions may, for example, refer to compliance with requirements related to prevention of pollution of the marine environment stated in, e.g., The International Convention for the Prevention of Pollution from Ships (MARPOL) [37].

Table 2: System hazards.

Identifier	System hazard description	Can result in accidents
H-1	Available power becomes too low	A-1, A-2, A-3
H-2	Disturbance to power production or electrical distribution is introduced	A-1, A-2, A-3
H-3	Available power becomes too high	A-4

Table 2 presents some hazards that may result in the defined accidents. The first hazard reflects a situation where the load demand becomes significantly greater than the instantaneous production capacity. This system state can result in either a case where certain loads have to be left unserved (e.g., load limitation of thrusters), or a case where the loads are not reduced, something that may result in blackout. The second hazard reflects system states where significant disturbances are introduced to the power production or electrical distribution. This can be, for example, issues that alter the electrical frequency on the bus, resulting in an emergency disconnect of power consumers (A-1) or power producers (A-2 and A-3). The third hazard reflects situations where the available power is unnecessarily high, resulting in increased consumption and emission.

4.2. Step 2: Modeling the system as a hierarchical control structure

4.2.1. System overview

We define available power as the power production capacity if all the active DGs were to be loaded at 100% of maximum continuous rating (MCR), minus the instantaneous load demand. The available power is given for the entire power system if all bus tie breakers are closed (power system not separated into segments), or for each segment if the bus is separated into two or more segments. The load demand during operations can vary with a number of variables such as the weather state, the operational phase, and system modes. It is desirable to maintain an appropriate load condition on the active DGs because if the available power is too high (i.e., the load on each DG is too low), the fuel consumption and emission of greenhouse gases will be increased [38]. Furthermore, according to Bø [38], low load conditions introduce problems such as sooting, increased maintenance costs and inefficiency of NOx reduction systems. On the other hand, if the available power is too low, the power system may become overloaded, something that can result in under-frequency, and in the worst case, a blackout [39]. Hence, to maintain an appropriate level of available power, the number of active DGs must be controlled. In the power system under consideration, a human operator can perform the control through a power management operator station (PMOS), or the automation system, referred to as the LDSS, can perform the task. The operator can also activate and deactivate the LDSS, and configure DG standby sequences for the LDSS. The standby sequence is a list that informs the LDSS in which order to start and stop DGs. Figure 3 shows the hierarchical control structure model of the system. Available control actions for the controllers are represented by the arrows pointing downwards, while feedback signals are represented by the arrows pointing upwards. The operator may, for example, issue a command to the PMOS to turn the LDSS functionality on. The PMOS can in turn issue an activation command to the LDSS. PMOS can observe the state (on or off) of the LDSS by monitoring the feedback signal “LDSS state”, and this feedback is also made available to the operator, for example through a display.

The case study focuses on the LDSS. The available control actions and the input ports of this module can be seen in Figure 3. In order to make decisions, the module needs a “process model” [20]. This is a concept that can be seen as an extension of the concept of cybernetics models, necessary for humans to act as goal-oriented operators [40]. In the STAMP framework, this concept is extended to any controller. If effective control is to be exerted, the controller needs a perception of the state of the controlled process as well as an idea regarding the effect of implementing the available control actions.

Table 3 presents the process variables found for the LDSS. These are identified by asking: What does the LDSS need to know to control the system effectively? Regarding the last process variable, we assume that a healthy DG is defined as a DG that will be able to produce power according to rated values, to control speed and frequency properly, and/or to start, synchronize or connect to the bus within a reasonable amount of time. Process model variables for the human operator and the PMOS are not presented in order to limit the extent of this case study.

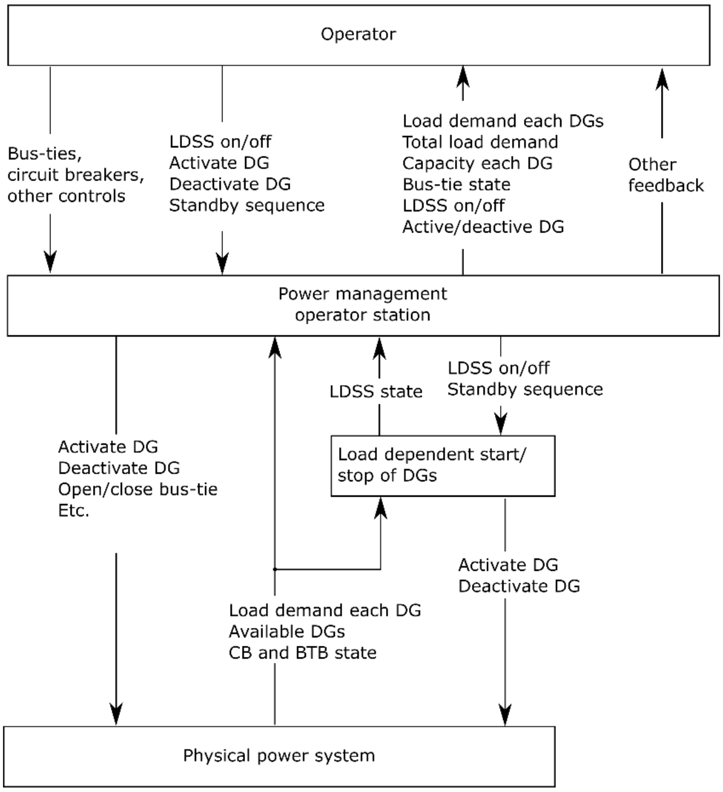

Figure 3: Control structure diagram for marine power system.

Table 3: Process variables for LDSS

Process variable	Description
PV-1	Whether LDSS is on or off
PV-2	The sequence in which to activate DGs
PV-3	The sequence in which to deactivate DGs
PV-4	Which DGs are on standby
PV-5	The bus configuration (how is the bus configured into segments)
PV-6	Which of the standby DGs are available for which bus segment
PV-7	The capacity of active DGs
PV-8	The capacity of standby DGs
PV-9	The total capacity of active DGs on the bus segments
PV-10	The total standby capacity on the bus segments
PV-11	The load demand on DGs
PV-12	The load demand on the bus segments
PV-13	The available power on DGs
PV-14	The available power on the bus segments
PV-15	Threshold on available power for activation of DG for each bus segment
PV-16	Threshold on available power for deactivation of DG for each bus segment
PV-17	Whether a DG is in service or taken out of service
PV-18	The health state of DGs

4.3. Step 3: Identifying UCAs

To identify UCAs, each of the control actions can be considered in light of the four ways in which UCAs may occur, as discussed in Section 3. Table 4 presents some selected UCAs found by considering all the control actions from Figure 3 that are directly related to the LDSS module and interactions between the human operator and LDSS through the PMOS. No UCAs were identified for applying a control action for too long or for stopping too early.

Table 4: Selection of UCAs found by analyzing the control actions relevant for LDSS. The abbreviation "TBD" means "to be decided"

Control action	Control action not provided causes hazard	Control action provided causes hazard	Control action stopped too early or applied for too long causes hazard
LDSS ON/OFF (Operator to PMOS)	**UCA-1:** Operator believes he/she has activated LDSS when this is not the case. *Rationale: Operator may not pay attention to available power and performance of DGs, thinking that LDSS is in control (H-1, H-3).*	**UCA-2:** Operator accidentally activates LDSS without realizing it. *Rationale: LDSS may deactivate generator that operator has activated in preparation for expected load increase due to e.g. planned engagement of heavy deck equipment, or otherwise hinder preparation (H-1).*	**UCA-3:** Operator does not deactivate LDSS when LDSS behaves erratically. *Rationale: May result in stopping too many generators, resulting in insufficient available power (H-1), or starting too many, resulting in too much available power (H-3).*
LDSS ON/OFF (PMOS to LDSS)	**UCA-4:** PMOS does not issue "LDSS on" command when operator selects to turn it on. *Rationale: Operator may believe that LDSS is "on" when it is not, leaving no-one in control (H-1, H-3).* **UCA-5:** LDSS-off not issued by PMOS when selected by operator. *Rationale: Same as UCA-2 and operator may be unable to deactivate LDSS if it is behaving unsafely (H-1, H-3).*	**UCA-6:** PMOS provides 'LDSS on' when operator did not issue command to do so. *Rationale: Same as UCA-2, (H-1).* **UCA-7:** LDSS-off is issued when operator did not command it. *Rationale: Operator may be unaware that LDSS is not in control, leaving no-one in control (H-1, H-3).*	**UCA-8:** LDSS activated too late after operator selected it. *Rationale: Same as UCA-4 (H-1, H-3).*
Activate DG (LDSS to power system	**UCA-9:** Additional DG not selected for activation by LDSS when LDSS is active and available power is TBD close to insufficient. *Rationale: Available power may become too low (H-1).*	**UCA-10:** Unhealthy DG is selected for activation by LDSS. *Rationale: Power system may be disrupted or DG may not be connected successfully (H-1, H-2)*	
Deactivate DG (LDSS to power system)	**UCA-11:** Unhealthy DG not deactivated by LDSS when LDSS is on. *Rationale: DG may be allowed to disturb system (H-2).*	**UCA-12:** Deactivate DG command issued by LDSS when this will result in insufficient available power. *Rationale: Available power may become low (H-1).*	
Standby sequence for LDSS (Operator to PMOS)	**UCA-13:** No standby sequence is provided for LDSS when LDSS is active. *Rationale: LDSS may not know which generators to start or stop when necessary (H-1, H-2, H-3).* **UCA-14:** Standby sequence not updated if it is found that one of the DGs in the sequence is not working properly. *Rationale: A generator that is not working properly may be started (H-1, H-2).*	**UCA-15:** A DG that is not working properly is included in the standby sequence. *Rationale: A generator that is not working properly may be started (H-1, H-2).* **UCA-16:** An incomplete standby sequence in the sense that it does not include that sufficient power capacity is provided. *Rationale: LDSS may not be able to activate additional DGs (H-1).* **UCA-17:** The standby sequence is changed during operation and a sequence is selected that is not consistent with the current DG configuration. *Rationale: LDSS may stop all generators not in the list, resulting in H-1, or disregard all generators not in the list resulting in H-3.* **UCA-18:** Standby sequence including non-existent DGs is provided. *Rationale: System may crash, DGs may fail to be started or stopped when necessary (H-1, H-3).*	
Standby sequence for LDSS (PMOS to LDSS)	**UCA-19:** PMOS does not update standby sequence in LDSS after operator has provided updated sequence. *Rationale: LDSS will continue operating in accordance with outdated version of the standby sequence. If, for example, the standby sequence was updated because a DG was taken out of service, LDSS may later try to start it (H-1, H-2)*		**UCA-20:** Standby sequence is updated/generated too early during operator input while the list is incomplete. *Rationale: LDSS may stop the generators that are no longer in the list without having replacements available (H-1).*

4.4. Step 4 and step 5: High-level safety constraints and scenarios of violation

The next step in the methodology is to derive high-level safety constraints for all the UCAs. In order to limit the extent of this case study, three UCAs are selected for further treatment. The safety constraints should ideally be constraints on the system behavior such that if they are successfully enforced, the UCAs cannot occur. In some cases, it will be necessary to define more than one safety constraint for each UCA. The first column in Table 5 shows the safety constraints identified for UCA-9, UCA-10 and UCA-18. Once the safety constraints have been identified, scenarios of violation can be identified for each safety constraint. These are scenarios describing how the safety constraints can be violated, or manners in which the UCAs may occur despite the safety constraints. The second column in Table 5 presents the scenarios of violation for the safety constraints in the first column. In this step, we have chosen to specify the context explicitly in terms of process variables (see the third column in Table 5). This may be a convenient way to highlight the context for test engineers when they are to develop specific test cases. It is, however, not strictly necessary, because the same information is provided in the textual specification of each scenario together with the associated higher-level safety constraint. For example, scenario S-9.1.1 has revealed that the LDSS obtaining a wrong perception regarding load demand can potentially result in violation of safety constraint SC-9.1. Clearly, in this scenario, the process variable PV-12: "The load demand on the bus segments", is relevant. Furthermore, the relevant state of this variable is that PV-12 is perceived as lower than the actual value. That is, the LDSS assigns a value to the process model variable that is lower than the actual value of the corresponding variable in the real world.

Table 5: High-level safety constraints and scenarios of violation for selected UCAs.

Safety constraint	Scenarios of violation	Process model variables relevant for describing context in scenarios of violation
SC-9.1: LDSS must activate additional DG when available power is [TBD] close to insufficient and LDSS is active	**S-9.1.1:** LDSS is not aware that available power is too low because LDSS perceives the load demand as lower than it actually is	**PV-1:** LDSS is on **PV-12:** Load demand is perceived by LDSS as lower than actual value **PV-14:** Available power is low
	S-9.1.2: LDSS is not aware that available power is too low because LDSS perceives the generating capacity as higher than it actually is	**PV-1:** LDSS is on **PV-7 and PV-9:** Power capacity is perceived as higher than actual value **PV-14:** Available power is low
	S-9.1.3: LDSS is not aware that available power is too low because the calibration of the lower threshold for the available power is set too low	**PV-1:** LDSS is on **PV-14:** Available power is low **PV-15:** Threshold is set too low
	S-9.1.4: LDSS does not activate additional DGs because there are no standby DGs to activate on the bus segment in question	**PV-1:** LDSS is on **PV-6:** There are no standby DGs on the bus segment in question **PV-14:** Available power is low
	S-9.1.5: LDSS does not activate additional DGs because it incorrectly believes that there are no standby DGs	**PV-1:** LDSS is on **PV-6:** LDSS incorrectly *believes* that there are no standby DGs on the bus segment in question **PV-14:** Available power is low
	S-9.1.6: LDSS tries to engage additional DG but the target DG is not responding	**PV-1:** LDSS is on **PV-18:** DG does not respond to activation command **PV-14:** Available power is low
	S-9.1.7: LDSS did not activate additional DG when available power became low because load demand increased too rapidly	**PV-1:** LDSS is on **PV-12:** Load demand increases rapidly **PV-14:** Available power is/becomes low
	S-9.1.8: LDSS did not activate additional DG when available power became low because a sudden reduction in production resulted in a sudden reduction in available power, too rapid to allow time for starting standby DG	**PV-1:** LDSS is on **PV-7:** Capacity of active DGs on a bus segment is suddenly reduced **PV-14:** Available power is/becomes low
	S-9.1.9: LDSS starts DG connected to the wrong bus when bus tie breakers are open, such that the available power is not increased on the bus where it was low, but on another one.	**PV-1:** LDSS is on **PV-6:** Relevant, but further scenario development is required to specify state **PV-14:** Available power is low
	S-9.1.10: LDSS does not start additional DG because the next DG in the standby sequence is not responding to the activation command, and LDSS does not proceed to the next in line	**PV-1:** LDSS is on **PV-14:** Available power is low **PV-18:** DG is not responding to activation command
SC-10.1: Unhealthy DG must never be activated	**S-10.1.1:** Unhealthy DG has not been removed from standby sequence and is therefore considered as standby by LDSS	**PV-1:** LDSS is on **PV-2:** Unhealthy DG is included in the standby sequence **PV-18:** DG is unhealthy
	S-10.1.2: Unhealthy DG has been included in the standby sequence and is therefore considered as standby by LDSS	**PV-1:** LDSS is on **PV-2:** Unhealthy DG is included in the standby sequence **PV-18:** DG is unhealthy
	S-10.1.3: There are no standby DGs available in the standby sequence, but the available power is getting low. LDSS selects a DG that is not in the standby sequence. (DG may have been omitted from the sequence because it is unhealthy).	**PV-1:** LDSS is on **PV-2 and PV-6**: There are no available standby DGs for the bus in question in the standby sequence **PV-14:** Available power is low
SC-18.1: Standby sequence that includes non-existent DG must not be provided	**S-18.1.1:** Standby sequence has not been updated after DG has been taken out of service	LDSS process model variables are not considered as relevant
	S-18.1.2: Operator inadvertently typed in wrong name for DG identification	
	S-18.1.3: Operator included DG, not being aware that the DG was out of service	
SC-18.2: LDSS must not accept standby sequence that includes non-existent DGs	**S-18.2.1:** LDSS does not go through the standby sequence verifying that all standby DGs are feasible upon receiving the list	**PV-2 and PV3:** Standby sequence includes non-existent DG
	S-18.2.2: LDSS goes through the standby sequence when receiving it, but crashes when encountering illegal data.	**PV-2 and PV3:** Standby sequence includes non-existent DG
	S-18-2.3: LDSS accepts the non-existent DG because LDSS incorrectly believes that it exists.	**PV-2 and PV3:** Standby sequence includes non-existent DG **PV-4:** LDSS incorrectly believes that a DG that does not exist is on standby

4.5. Step 6: Identifying and resolving conflicting safety constraints

Sometimes, the safety constraints will be in conflict with each other. As an example, we have identified that an additional DG must be activated when the available power is low (SC-9.1). We have also identified that an unhealthy DG must never be activated (SC-10.1). If a situation arises where the available power is low and the only remaining available DG for activation is an unhealthy one, the LDSS would necessarily have to violate one of these safety constraints. This conflict is highlighted in scenario S-10.1.3, where we identified the activation of an unhealthy DG because there are no other DGs available, as a potential violation.

At some point, it is necessary to describe how the LDSS should act if the described situation should arise. For the scenario of violation S-10.1.3, this depends on the degree to which the DG is unhealthy, and the severity of the power shortage, and there may be no universally correct resolution to the conflict between the two safety constraints. One possible option is to demand that the LDSS should alert the human operator to take control over the situation. Then the human operator needs sufficient information and response time to be able to take proper action.

4.7. Step 7: Deriving lower-level safety constraints and scenarios of violation

In step 5, we identified scenarios of violation for the high-level safety constraints, and trade-offs were considered in step 6. In step 7, we develop lower-level safety constraints to ensure that the scenarios identified in step 5 cannot occur. The “refined” safety constraints should be examined in turn by trying to identify new scenarios of violation for these. It may be that the analyst finds it unnecessary to continue along a “sequence of constraints” when a safety constraint that is considered straightforward to verify is identified.

To illustrate this step, we take a closer look at scenario S-9.1.1 LDSS is not aware that available power is too low because LDSS perceives load demand as lower than it actually is. This is one way in which safety constraint SC-9.1 can be violated (LDSS must activate additional power source when available power is TBD close to insufficient). A safety constraint that can be enforced to avoid this scenario is “LDSS must never underestimate the load demand on any bus segment”. This safety constraint is not particularly easy to verify, and it is therefore necessary to consider how this new constraint can be violated. One possibility is that the signal from one of the sensors responsible for gathering data about the available power is wrong. Based on this scenario, a possible safety constraint could be defined as: Wrong feedback from a single sensor should not lead the LDSS to perceiving the load demand as lower than it actually is. This safety constraint can be tested and verified, and it is therefore not seen as necessary to analyze further. Refined scenarios of violation and corresponding safety constraints are identified for four of the scenarios of violation identified under safety constraint SC-9.1. These are presented in Table 6.

Table 6: Refined safety constraints and scenarios of violation for the four first scenarios of violation of safety constraint 9.1.

High-level safety constraint	Scenario of violation for high-level safety constraint	Safety constraints	Scenarios of violation	Safety constraints
SC-9.1: LDSS must activate additional DG when available power is [TBD] close to insufficient and LDSS is active	**S-9.1.1:** LDSS is not aware that available power is too low because LDSS perceives the load demand as less than it actually is	**SC-9.1.1.1:** LDSS must never underestimate the load demand on any bus segment	**S-9.1.1.1.1:** Wrong feedback (e.g., sensor drift, bias, excessive noise, or frozen signal) makes LDSS perceive the load demand as less than it actually is	**SC-9.1.1.1.1.1:** Wrong feedback from a single sensor should not make LDSS perceive the load demand as less than the actual value
			S-9.1.1.1.2: LDSS thinks that the load demand denotes the load demand on the entire bus, while it actually denotes the load demand for a single bus segment	**SC-9.1.1.1.2.1:** Bus tie states must be correctly accounted for when LDSS evaluates the available power **SC-9.1.1.1.2.2:** Inconsistency between LDSS perception on bus tie states and feedback from bus tie breakers must be detected by LDSS
	S-9.1.2: LDSS is not aware that available power is too low because LDSS perceives the generating capacity as higher than it actually is	**SC-9.1.2.1:** LDSS must never overestimate the generating capacity for each bus segment	**S-9.1.2.1.1:** LDSS incorrectly perceives DGs that are offline (e.g. standby DGs or DGs that are out of service) as active.	**SC-9.1.2.1.1.1:** LDSS must be designed such that offline DGs can never be perceived as active DGs.
			S-9.1.2.1.2: LDSS may have a wrong belief regarding which DGs are supplying which bus segments, and as such perceive a bus segment to be better supplied than is actually the case	**SC-9.1.2.1.2.1:** LDSS must always be aware which DGs are supplying which bus segments
			S-9.1.2.1.3: LDSS may believe that the capacity of DGs is higher than it actually is because calibration of the maximum continuous rating is set too high.	**SC-9.1.2.1.3.1:** Calibration of DG generating capacity must be correct in LDSS software
			S-9.1.2.1.4: LDSS may believe that the capacity of DGs is higher than it actually is because DGs capacity has degraded and the degradation has not been accounted for.	**SC-9.1.2.1.4.1:** Calibration of DG generating capacity must be reassessed at regular intervals based on practical trials on capacity of DG.
	S-9.1.3: LDSS is not aware that available power is too low because calibration of the lower threshold for the available power is set too low.	**SC-9.1.3.1**: The lower threshold for the available power must be calibrated to a safe level	**S-9.1.3.1.1:** Operator alters the parameter to an unsafe level	**SC.9.1.3.1.1.1:** Operator must not have access to change the parameter value
			S-9.1.3.1.2: Service engineer provides the wrong value	**SC.9.1.3.1.2.1:** Procedures for review of parameter settings must be in place after service engineer has accessed a menu on the interface where alteration of the parameter is possible
			S-9.1.3.1.3: Software update resets the parameter to some default value that, in the context of a particular vessel, is unsafe	**SC.9.1.3.1.3.1:** Procedures for reviewing parameter values after system update must be in place
	S-9.1.4: The LDSS does not activate additional DG because there are no standby DGs to activate on the bus segment in question	**SC-9.1.4.1:** The number of standby DGs in the standby sequence must be sufficient to ensure that adequate amounts of available power can be maintained	Further scenario development is not seen as necessary	
		SC-9.1.4.2: Expected power demand should be estimated and evaluated against power capacity (accounting for possible DGs that are out of service) before operations are started.	Further scenario development is not seen as necessary	

4.8. Step 8: Developing verification objectives

All the identified safety constraints can now be translated into verification objectives. The verification objectives should be developed in a hierarchical manner so that each verification objective can be traced back to higher-level verification objectives. Figure 4 shows a selection of verification objectives organized in a tree-structure together with scenarios of violation. This representation highlights the traceability gained by using STPA. The intention of each verification objective is to establish confidence that the corresponding safety constraint cannot be violated. The scenarios of violation represent the ways in which the safety constraints can be violated. As such, the verification objectives contain information about acceptance criteria for verification activities (i.e., the corresponding safety constraint should not be violated) and the scenarios contain information about the context which is identified as critical for the above verification objectives.

4.9. Step 9: Assigning verification objectives to further processing

The verification objectives can now be assigned to further processing by considering the nature of each. Note that there may not be a unique solution but several possible options for each objective. Some examples of options for further processing are provided in the following.

We start by considering verification objective VO-9.1. The corresponding safety constraint (SC-9.1), can potentially be violated if either of the scenarios from S-9.1.1 to S-9.1.10 occurs. If verification objective VO-9.1 is to be satisfied, it must be verified that none of these scenarios will result in violation of the safety constraint SC-9.1. Alternatively, if this is not the case, or if it is impractical to show this, lower-level safety constraints can be verified to ensure that the scenarios S-9.1.1 to S-9.1.10 cannot occur. Scenario S-9.1.1 describes a situation where the LDSS perceives the load demand as less than the load demand actually is. The verification objective VO-9.1 stipulates the acceptance criterion – that additional DGs should be activated when available power is [TBD] low. Relevant verification activities in this case could be to go through the LDSS documentation to see if the LDSS module on the installation to be verified includes functions aimed at handling the occurrence of scenario S-9.1.1 (such as a conservative lower threshold for the available power). Such functions will strengthen the confidence in the safety constraint SC-9.

If it is found that verification objective VO-9.1 cannot be satisfied with sufficient confidence, the confidence can potentially be increased by considering lower-level verification objectives. The intention with these is to ensure that the scenarios of violation for safety constraint SC-9.1 will not take place.

The acceptance criterion stipulated by verification objective VO-9.1.1.1.1.1 is that wrong sensor feedback from a single sensor should not make the LDSS perceive the load demand as less than it actually is. Test cases for HIL, aimed at violating this acceptance criterion, can be developed. It is specified that only cases where the load demand can be perceived as less than the actual value are relevant. As such, relevant sensor failures and errors that should be tested include negative bias on a single sensor, a signal fixed at the lower boundary of the physical range for a single sensor, a signal that goes to zero and loss of signal for a single sensor, signal freeze on a single sensor during increasing load demand, and time delay on a signal during increasing load demand.

An alternative approach for verification objective VO-9.1.1.1.1.1 is to use it as a specific objective for the FMEA. The current objective of the DP FMEA is to verify the requirement that no single failure should result in loss of position [12]. As such, VO-9.1.1.1.1.1 can be seen as part of a refinement of this objective. If the FMEA were to be conducted without this specification, it is possible that the analyst would not consider the fact that wrong perception of the load demand for the LDSS can result in e.g. blackout. Relevant findings and assumptions in the FMEA can further be used as input to test case generation for sea-trial or HIL tests. This approach may be relevant if the system is complex, and it is necessary to gain an understanding of how the sensor system is working, how different sensor units are connected, and how different failures may propagate.

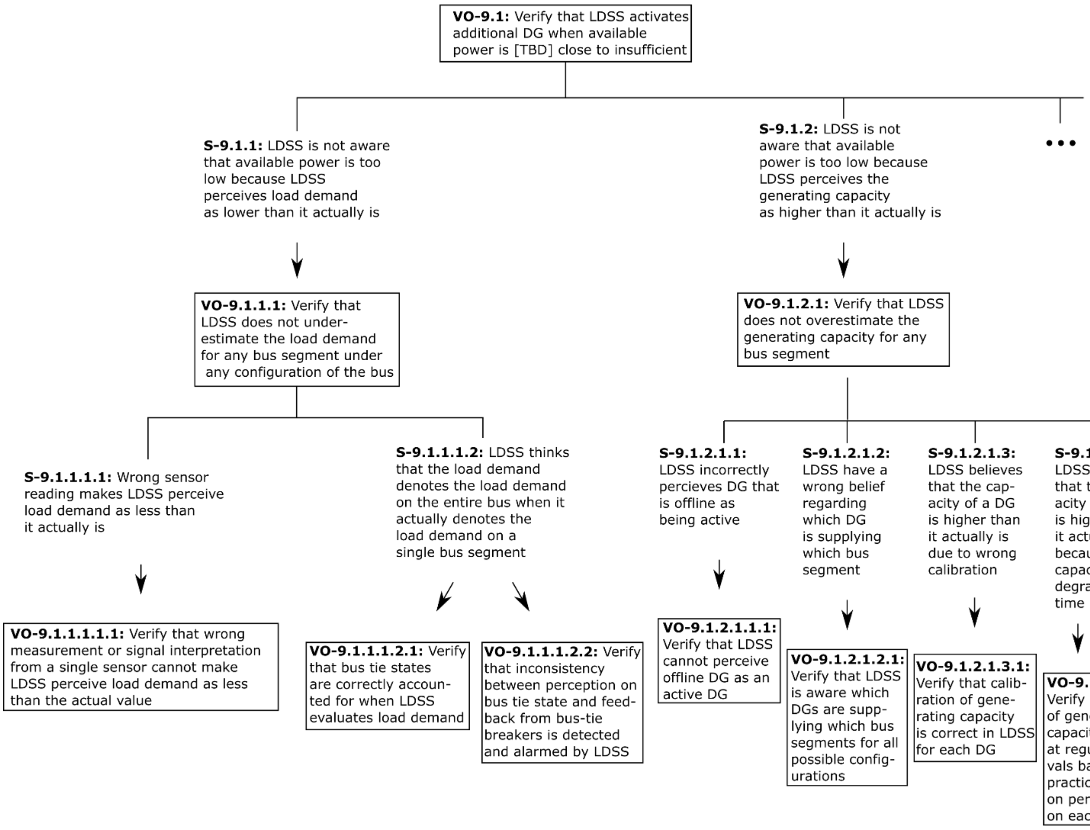
VO-9.1: Verify that LDSS activates additional DG when available power is [TBD] close to insufficient
S-9.1.1: LDSS is not aware that available power is too low because LDSS perceives load demand as lower than it actually is
S-9.1.2: LDSS is not aware that available power is too low because LDSS perceives the generating capacity as higher than it actually is
•••
VO-9.1.1.1: Verify that LDSS does not under-estimate the load demand for any bus segment under any configuration of the bus
VO-9.1.2.1: Verify that LDSS does not overestimate the generating capacity for any bus segment
S-9.1.1.1.1: Wrong sensor reading makes LDSS perceive load demand as less than it actually is
S-9.1.1.1.2: LDSS thinks that the load demand denotes the load demand on the entire bus when it actually denotes the load demand on a single bus segment
S-9.1.2.1.1: LDSS incorrectly percieves DG that is offline as being active
S-9.1.2.1.2: LDSS have a wrong belief regarding which DG is supplying which bus segment
S-9.1.2.1.3: LDSS believes that the cap-acity of a DG is higher than it actually is due to wrong calibration
S-9.1.2.1.4: LDSS believes that the cap-acity of a DG is higher than it actually is because DG's capacity has degraded over time
VO-9.1.1.1.1.1: Verify that wrong measurement or signal interpretation from a single sensor cannot make LDSS perceive load demand as less than the actual value
VO-9.1.1.1.2.1: Verify that bus tie states are correctly accoun-ted for when LDSS evaluates load demand
VO-9.1.1.1.2.2: Verify that inconsistency between perception on bus tie state and feed-back from bus-tie breakers is detected and alarmed by LDSS
VO-9.1.2.1.1.1: Verify that LDSS cannot perceive offline DG as an active DG
VO-9.1.2.1.2.1: Verify that LDSS is aware which DGs are supp-lying which bus segments for all possible config-urations
VO-9.1.2.1.3.1: Verify that calib-ration of gene-rating capacity is correct in LDSS for each DG
VO-9.1.2.1.4.1: Verify calibration of generating capacity for DGs at regular inter-vals based on practical trials on performance on each DG

Figure 4: Selection of verification objectives and associated scenarios of violation organized as a tree structure.

Although test case generation is outside the scope of the proposed methodology, we provide an example of how verification objectives can be used in order to generate a test case for HIL with corresponding acceptance criteria. Verification objective VO-9.1.1.1.2.1 states that it shall be verified that bus tie states are correctly accounted for when the LDSS evaluates the load demand. A test case can be formulated as follows:

- Test: Start simulation with all bus tie breakers open, and apply a known load to each bus segment. Open and close bus tie breakers until all possible bus configurations have been visited. Monitor the load demand as perceived by the LDSS for each of the bus configurations (if available).
- **Acceptance criteria:** The load demand as observed from the LDSS must correspond to the applied loads for each segment in all configurations.

This test case is developed under the assumption that the load demand can be observed as perceived by the LDSS. If this is not the case, the test case and acceptance criteria must be reformulated. One option then is to gradually increase the load on a segment while maintaining low load on all other segments. This must be done for each segment in each possible bus configuration while observing that DGs are activated at appropriate times when the available power becomes low on a bus segment. The test can in this case be accepted if the available power never decreases below the lower threshold. At this stage, questions such as how fast loads should be applied arise. As the verification objective makes no mention of this issue, loads can be applied at a slow rate. The answer to such questions is that it does not matter. The objective in this test is to verify that bus tie states are correctly accounted for when the LDSS evaluates the load demand. The problem has been isolated from circumstances such as the rate at which loads are applied, and the system can only falsely fail the test, not falsely pass. Whether the system is able to respond to loads fast enough, or whether the system can be loaded too fast, should be covered by verification objectives derived from scenario S-9.1.7.

5. Results and Discussion

This article outlines a methodology aimed at improving the current verification and testing approach for maritime systems such as DP systems by introducing a specialized STPA for identifying verification objectives. This has been done to address two challenges: (i) the need for better defined and specified system verification scopes, objectives and acceptance criteria; and (ii) the need for better tools for handling the complexity (in terms of obtaining adequate test coverage).

5.1. Defining and specifying scope, objectives and acceptance criteria

We argue that the scope, objectives and acceptance criteria are not well defined for the verification activities currently taking place. As pointed out in Spouge [5], the FMEA, for example, can be a suitable method for analyzing redundancy given that appropriate guidance is provided and that the objectives of the analysis are well defined. Currently, acceptance criteria are mostly defined at the system level, and test outcomes and FMEA results must be observed and evaluated at this level. The consequence is that results become too context-dependent and, as such, that the value of the verification and test activities in terms of increased confidence in the system diminishes. Note that FMEA in this context, does not refer to traditional FMEA analysis, but the specialized technique for systematically going through a technical design to ensure that it satisfies certain requirements. This process does not take into consideration whether those requirements are sufficient and safe. This, however, is ensured when verification objectives are provided from the STPA analysis. Note also that currently, this process is mainly used to identify potential redundancy flaws. This is not the only available approach to designing for safety, and with increased dependency on software, the approach is becoming less applicable. By replacing static redundancy requirements as input to the FMEA, with dynamic and appropriate verification objectives obtained through an STPA analysis, we allow for modern approaches to safety design to replace the redundancy approach where it is appropriate.

This challenge is addressed in our approach as the verification objectives provide a conceptual link between local test outcomes and system-level accidents. The interface between the verification objectives and the rest of the verification process is that the verification objectives, together with the causal scenarios of violation, define, refine or extend the scope and the acceptance criteria for FMEA, HIL tests and sea-trials as required in order to ensure safety. Introduction of the STPA allows us to determine unacceptable scenarios that may result in unacceptable states at the system level. Consider for example scenario S-9.1.1.1.1: “Wrong sensor reading makes LDSS perceive load demand as less than it actually is”. Assume that this scenario occurs during an operation. For the scenario to result in one of the associated system accidents (A-1, A-2 or A-3), the LDSS needs to be misled by the corrupted signal, and in such a manner that it thinks that the load demand is less than it is. Furthermore, the available power must become too low during the time where the LDSS is misled, and the LDSS must be active and in control of the DG configuration. If all these circumstances are such that an additional DG is not activated when required, the scenario may result in a load limitation on thrusters or other equipment, or alternatively, a blackout or partial blackout will result. In short, there are a number of context variables or circumstances affecting observations made at the system level. It is then more predictable to observe whether or not various failures in these sensors can result in the LDSS underestimating the load demand. This is achieved by using the analysis to isolate scenarios from the wider context of the system, while simultaneously specifying the remaining context and, as such, letting the analysis conceptually outline the relationship between undesired system states and specific scenarios. Notice also that this scenario results in a safety constraint that is in line with the single failure requirement: a wrong sensor reading from a single sensor should not make the LDSS perceive the load demand as less than it actually is. The difference is that the consequence part (or acceptance criterion) of the statement is defined at a local level (LDSS belief regarding load demand is wrong), rather than at a system level (e.g. power system blackout).

Currently, test cases in the maritime industry are often based on a set of failure modes (see for example Johansen and Sørensen [6]) An example of such a failure mode is “unavailable diesel engine”. To highlight our point, we can list some context variables that may be relevant in terms of whether this failure mode will result in a blackout. Such context variables can be whether other diesel engines are available; whether other available diesel engines are included in the standby sequence; whether the available power is low; how the electrical bus is configured; whether there are other bus segments that could take the load; whether the DP control system will allocate load to other bus segments; and whether alternative diesel engines are healthy or not. Without somehow reducing the context space through the application of an analysis, as is done in the work presented in this article, a test result stating that an unavailable diesel engine does not result in accidents is of limited value. In fact, it may be nearly impossible to determine whether a favorable test outcome should be ascribed to system safety or whether it should be ascribed to a favorable set of context variables. Our approach, using STPA in order to identify scenarios with reduced context space, will reduce this problem considerably, ensuring that each verification activity will have a significant impact on system confidence.

5.2. Addressing complexity of systems and an integrated systems view

The causality of modern maritime systems with advanced integrated control systems is too complex to be modeled thinking in terms only of failure modes.

In Johansen and Sørensen [6], experiences with HIL testing of power management systems for DP vessels is reported and discussed. They present scenarios in terms of failure modes, including shutdown of diesel engines, short-circuit on one bus, unavailable diesel engine, locked governor, full throttle of diesel engine, reduced max power from engine, etc. This approach will be able to capture scenarios with a relatively direct causality. For example, a short-circuit on a bus will result in either partial blackout or full blackout if the system is operating with a single bus configuration, regardless of other circumstances. However, scenarios where a more complex causality is involved in the potential accident may not be identified. The list of scenarios in Johansen and Sørensen [6] does not account for any of the scenarios in Table 6. Examples are situations where sensor failures make the LDSS perceive load demand as less than it actually is (S-9.1.1.1.1); the LDSS thinks that the load demand denotes the load demand on the entire bus, while it actually denotes the load demand for a single bus segment, e.g., because of a wrong perception regarding bus tie breakers (S-9.1.1.1.2); the LDSS is unaware that available power is too low because it has a wrong perception regarding which or how many DGs are currently running (S-9.1.2.1.1), or the LDSS does not activate additional DGs because it is not aware that available power is too low due to wrong calibration of the lower threshold for the available power (S-9.1.3). Our approach enables verification organizations to identify causal scenarios that involve more complex causality than single failures that directly lead to system accidents.

Emergent properties such as safety are not properties associated with individual building blocks or individual engineering disciplines such as software, electromechanical component assemblies or human operators, but emerge through attuned interactions between building blocks from different disciplines. It is therefore not sufficient to consider, for example, a piece of software, or even the entire software system, in isolation when verifying and testing safety-critical systems. The same is true for hardware components and component assemblies. This is, however, often the case today. The traditional testing and verification activities are mainly focused on verifying component assemblies through FMEA and practical sea-trials, and the computer control system through HIL and SIL tests.

Instead of focusing on one or the other system dimension, such as component assemblies or computer control systems, our approach identifies verification objectives based on how interactions in the system may be unsafe or inadequate. Human factors, for example, are not considered in the current verification scope. Using STPA as a foundation, cases relevant to this topic can be considered because we have an idea about which requirements must be enforced on the system in order for the human to do a good job of controlling the vessel. Although UCA-1 to UCA-3 were not pursued further in the case study, it is reasonable to expect that these would result in verification activities aimed at reducing the probability of unsafe interactions between LSDD and the human operator.

Furthermore, human factor issues, such as ensuring that unhealthy DGs are removed from the standby sequence (S-10.1.1, Table 5), ensuring that unhealthy DGs are not included in the standby sequence (S-10.1.2, Table 5), or ensuring that non-existent DGs are not included in the standby sequence (SC-18.1, Table 5), have been considered. In fact, these potential issues may emerge from interactions between onshore management, the human operator and computer control systems because the problem needs to be considered both from an organizational point of view and from the operator's point of view, as well as from the point of view of the LDSS software development and integration into the power system. Further analyses of these could have resulted in safety constraints and verification objectives at the onshore management level, for example by considering procedures to ensure that detection of unhealthy DGs is registered and processed as necessary. At the software development level, we identified that the LDSS must not accept standby sequences that include non-existent DGs (SC-18.2, Table 5). Using the current process, each verification activity is seen only from the perspective either of hardware redundancy or of software controllers. By introducing STPA as a means by which to identify verification objectives, these are tied together into an integrated system view.

5.3. Other features of the approach

Another important aspect of verification is traceability. Using a top-down analysis as a basis for verification will enable effective communication regarding what has been tested and why. This is because each of the verification objectives will be linked to high-level safety constraints, system hazards and accidents. An added benefit of this is that system experts can review the tests and suggest improvements because they can readily understand the intentions of the verification objectives. This will also reduce the uncertainty on how much confidence to place in the system among different stakeholders.

A potential disadvantage with the proposed methodology is that it may result in increased verification expenses. This reduces the feasibility of the methodology in the maritime industry where even HIL testing or other software verification techniques are not widely used due to the costs, despite the fact that safe operations to a large extent depends on software performance. One observation, however, is that it may not be necessary to conduct the proposed methodology in full for every vessel that is to be verified. Although entirely similar vessels are rare, if hardly existent, many are quite similar at a functional level. Therefore, it is reasonable to assume that parts of an analysis for one vessel can be reused for another vessel, especially as the proposed methodology relies on functional descriptions rather than a particular implementation. If we assume that the verification is performed by third party test organizations, it may be possible for these organizations to develop generic analyses to identify verification objectives that are applicable for several vessels, thus distributing the cost of conducting the analysis over several vessels.

Potentially, the proposed methodology may also result in additional cost because it identifies a more comprehensive verification scope. This is because STPA may uncover safety issues that are currently not being considered (as demonstrated in Rokseth et al. [19]). A more comprehensive verification scope (e.g., more test cases) need not necessarily result in increased costs in the future. For example, one may imagine a situation where HIL simulators are integrated into each vessel working on a test scope while performing other activities or waiting for weather or laying at dock. Such an approach would require a well-defined and organized test program, which can be obtained by employing the proposed methodology. Furthermore, if an intelligent strategy for prioritizing verification objectives is employed, a more complete set of verification objectives offers the potential for better verification using the same resources. One possible strategy for prioritization may be to focus on key parameters such as safety, availability and environmental friendliness. These parameters can be linked to the system-level accidents. For example, A-1 (power system not able to serve loads) and A-2 (full power system blackout) are safety concerns, while A-3 (partial blackout) is an availability concern. Further prioritization can be based on the hazards in terms of severity.

The application of the proposed methodology in the verification process can also contribute to reduced cost because STPA will provide more insight into the context variables relevant for each verification objective, and subsequent verification activities will become more precise or “on target”. That is, the improved insight provided by using the proposed approach may serve to focus verification efforts and avoid using resources on unnecessary verification activities. Consider again verification objective VO-9.1.1.1.1.1 “Verify that wrong sensor reading from a single sensor does not make LDSS perceive the load demand as less than it actually is”. This verification objective specifies that only cases where the load demand may be perceived as lower than is actually the case are of interest. Thus, efforts will not be wasted on conducting tests with, for example, positive sensor bias or drift. The consequence of conducting verification without such insight is that a number of scenarios that may not potentially result in hazards are also being considered. Filtering those out may result in considerable savings.

Even though it is outside the scope of this article to quantify the potential gain in reduced risk vs. potentially increased expenses, it is clear that a more comprehensive verification program will serve to reduce the risk associated with major accidents, such as blowouts, drowning of divers, and collisions. The costs of such accidents may potentially be enormous. Furthermore, downtime and abrupted operations may also result in considerable economic losses (consider, for example, the cost of loss of availability of a mobile offshore drilling unit for a few days).

6. Conclusion

This article proposes the introduction of STPA into the verification and testing process of maritime automation systems such as DP systems. The STPA produces verification objectives that define the scopes, objectives and acceptance criteria for further verification and testing activities such as FMEA, HIL tests and sea-trials. The main advantage of the proposed methodology is that it provides a conceptual link between local scenarios and potential system losses, where potential consequences of scenarios can be evaluated at a local level rather than on the system level during further test and verification activities, thus reducing the context space, such that the confidence gained from verification activities is enhanced. Furthermore, using STPA, a hazard analysis technique based on control theoretic principles provides an integrated system view. This better enables us to consider interaction problems across the boundaries of various engineering disciplines, such as interaction problems between operators, software and component assemblies. Finally, the introduction of STPA into the verification process increases the coverage of the verification and testing activities because scenarios that are not possible to identify by thinking in terms of failure modes, can be identified.

The methodology has been demonstrated through a case study of an automation module that is responsible for activating and deactivating diesel generators in a marine power system as the load demand changes. The case study demonstrates that the method is able to produce verification objectives that can be utilized further to define the scope and acceptance criteria for the FMEA, and to generate test cases for practical sea-trials, HIL tests and SIL tests. Although application of the proposed methodology may result in additional cost, both in terms of development of the analysis and more comprehensive verification scopes, reasonable benefits may be expected due to reduced major accidents risks and operational downtime.

Future work includes a broader case study where a wider representation of shipboard automation systems is analyzed. A larger case study would enable a quantitative estimate of the costs associated with the method. A broader case study can also provide a foundation for research on formal methods for building more functional modularity into the STPA model. This is in order to readily enable reuse of models, and as such reduce the cost associated with including the approach in the verification process. Furthermore, a strategy for prioritizing among verification objectives should be established. If limited resources for testing and verification are available, strategies for intelligent prioritization are of importance. One possible strategy is to prioritize based on the relevance of the verification objective to various key parameters, such as redundancy, availability, environmental friendliness, etc. Another approach would be to base the prioritization on particular losses. This can be readily achieved by prioritizing between system accidents, and then selecting only those verification objectives that can be related directly to those system accidents.

Declaration of Conflicting Interests

The author(s) declare 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 Odd Ivar Haugen, Marine Cybernetics/DNVGL.

Funding

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] Skogdalen J, Espen, Smogeli Ø. Looking forward - Reliability of safety-critical control systems on offshore drilling vessels. 2011.
[2] 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.
[3] Skjetne R, Sørensen A, J. Computer-based systems on ships and offshore vessels: The software problem ++. Trondheim, Norway: Marine Cybernetics AS; 2004.
[4] IMO. Guidelines for vessels with dynamic positioning systems (IMO MSC Circular 645). 1994.
[5] Spouge J. Review of methods for demonstrating redundancy in dynamic positioning systems for the offshore industry. 2004.
[6] Johansen T, A., Sørensen A, J. Experiences with HIL Simulator testing of Power Management Systems. Dynamic Positioning Conference: Marine Technology Society; 2009.
[7] Johansen TAF, Tor, I.; Vik, Bjørnar Hardware-in-the-loop testing of DP systems. Dynamic positioning conference. Houston, TX2005.
[8] Skjetne R, Egeland O. Hardware-in-the-loop testing of marine control systems. Modeling, identification and control. 2006;27:239-58.
[9] Marine Cybernetics. Relevant rules and regulations for HIL testing (white paper). 2013.
[10] DNV-GL. Rules for classification of ships, part 6, chapter 6, section 12: Enhanced system verification - ESV. DNV-GL; 2016.
[11] ABS. Guide for systems verification. ABS; 2014.
[12] DNV. Reccomended practices DNV-RP-D102: Failure mode and effect analysis (FMEA) of redundant systems. 2012.
[13] IMCA. Guidance for developing and conducting annual DP trials programmes for DP vessels. IMCA; 2011.
[14] IMCA. Guidance on failure mode and effect analyses (FMEAs) (M 166). IMCA; 2016.
[15] IMCA. Guideline for the design and operation of dynamically positioned vessels (M 103). www.imca-int.com/marine: IMCA; 2016.
[16] Leveson NG. Safeware: system safety and computers: ACM; 1995.
[17] Dong Y, Rokseth B, Vinnem JE, Utne IB. Analysis of dynamic positioning system accidents and incidents with emphasis on root causes and barrier failures. Risk, Reliability and Safety: Innovating Theory and Practice: Proceedings of ESREL 2016. Glasgow, Scotland2016.
[18] Haugen OI. Independence in testing safety critical applications. Test Magazine: 31 Media Limited; 2016. p. 16-21.
[19] Rokseth B, Bouwer Utne I, Vinnem JE. A systems approach to risk analysis of maritime operations. Journal of risk and reliability. 2017;231:53-68.
[20] Leveson NG. Engineering a safer world: Systems thinking applied to safety: The MIT Press; 2011.
[21] Leveson NG. A new accident model for engineering safer systems. Safety science. 2004;42:237-70.
[22] Leveson NG. A New Approach to Hazard Analysis for Complex Systems. Conference of the System Safety Society. Ottawa2003.
[23] Rasmussen J. Risk management in a dynamic society: a modelling problem. Safety Science. 1997;27:183-213.
[24] Periera SJ, Grady L, Jeffrey H. A system-theoretic hazard analysis methodology for a non-advocate safety assessment of the ballistic missile defense system. Missile defence agency Washington DC; 2006.
[25] 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.
[26] Fleming CH, Spencer M, Thomas J, Leveson N, Wilkinson C. Safety assurance in NextGen and complex transportation systems. Safety Science. 2013;55:173 - 87.
[27] Young W, Nancy L. Systems thinking for safety and security. Annual Computer Security Applications Conference: ACM; 2013. p. 1-8.
[28] Ishimatsu TL, Nancy G.; Thomas, John P.; Fleming, Cody H.; Katahira, Masafumi; Miyamoto, Yuko; Ujiie, Ryo; Nakao, Haruka; Hoshino, Nobuyuki. Hazard analysis of complex spacecraft using systems-theoretic process analysis. Journal of spacecraft and rockets. 2014;51:509-22.

[29] Abrecht B, Leveson NG. Systems theoretic process analysis (STPA) of an offshore supply vessel dynamic positioning system. Massachusetts Institute of Technology; 2016.
[30] Abdulkhaleq; A, Wagner; S, Leveson N. A comprehensive safety engineering approach for softwareintensive systems based on STPA. Procedia Engineering. 2015;128:2-11.
[31] ABS. Guide for dynamic positioning systems. 2016.
[32] DNV-GL. Rules for classification of ships, part 6, chapter 3: Navigation, manoeuvring and position keeping. DNV-GL; 2016.
[33] Smogeli Ø, Vik B, Haugen OI, Pivano L. Risk management for control system software for the maritime and offshore oil and gas industries. IMCA Annual Seminar 20142014.
[34] Chow TS. Testing software design modeled by finite-state machines. IEEE transactions on software engineering. 1978;4:178.
[35] Kuhn DR, Kacker RN, Lei Y. Introduction to combinatorial testing: CRC press; 2013.
[36] Ådnanes A, Kåre. Maritime Electrical Installations And Diesel Electric Propulsion. Oslo, Norway: ABB Marine AS; 2003.
[37] MARPOL. MARPOL Annex VI Prevention of air pollution from ships. IMO; 1997.
[38] Bø I, Torstein; Johansen, Tor, A.; Sørensen, Asgeir, J.; Mathiesen, Eirik. Dynamic consequence analysis of marine electrice power plant in dynamic positioning. Applied Ocean Research. 2016;57:30-9.
[39] Damir RJ, Tor, A.; Sørensen, Asgeir, J.; Ådnanes, Alf, Kåre. Optimization fo load dependent start tables in marine power management systems with blackout prevention. WSEAS transactions on circuits and systems. 2005;4:1861-6.
[40] Rasmussen J. On the structure of knowledge-a morphology of metal models in a man-machine system context. 1979.