DERIVING SAFETY REQUIREMENT HIERARCHIES FOR FAMILIES OF MARITIME SYSTEMS

(DOI No: 10.3940/rina.ijme.2019.a3.526)

B Rokseth and **I B Utne** Department of Marine Technology, Norwegian University of Science and Technology (NTNU), Norway

SUMMARY

Ensuring the safety of advanced maritime vessels is a challenging task. While technological developments provide new options for their design and operation, the criteria for certification, such as class rules intended to ensure safety, may not be flexible enough to accommodate rapid changes. Innovation may enable more efficient, greener, and smarter systems but it may also introduce new hazards that are not addressed by current safety requirements. This paper proposes a method aimed at developing requirement hierarchies that are generic for a family of systems (such as a class of ships) and that can be adapted and specialised for a subset of the family or a particular system. Systems-theoretic process analysis (STPA) is used to develop safety requirements that are structured in a way that ensures that they can easily be kept up to date to accommodate new technological solutions and new alternatives for the design and operation of maritime vessels.

NOMENCLATURE

DP	Dynamic Positioning
FMEA	Failure Mode and Effect Analysis
GBS	Goal Based Standards
HIL	Hardware in the Loop
IMCA	International Maritime Contractors Association
IMO	International Maritime Organisation
MCR	Maximal Continuous Rating
SOLAS	Safety of Life At Sea
STAMP	Systems-Theoretic Accident Model and Processes
STPA	Systems-Theoretic Process Analysis
TLVC	Top Level Vessel Controller
UCA	Unsafe control action

1. INTRODUCTION

Technological progress provides a growing range of advanced and potentially greener solutions in the maritime industry, such as hybrid power systems (Miyazaki et al., 2016, Bø and Johansen, 2016, Sørensen et al., 2017) and autonomous marine activities and ships (Reilly and Jorgensen, 2016, Levander, 2016, Sørensen and Ludvigsen, 2015, Utne and Schjølberg, 2014, Sørensen et al., 2017, Valdez-Banda et al., 2018, Montewka et al., 2018). During recent decades, the maritime industry has experienced rapid technological development. With new market demands and new enabling technologies, vessels with new purposes and new physical implementations have emerged to achieve these purposes. In the 1960s, the desire to enable offshore drilling at deeper waters resulted in the need to position vessels over wells without anchor lines. This resulted in the development of the first dynamic positioning (DP) vessel (Brevik et al., 2015) i.e., a vessel that was able to maintain its position and heading (i.e. perform station keeping) solely by means of thrusters (IMO, 1994). This, in turn, called for several new technical solutions in terms of power generation, thrust generation and position reference systems. Today, DP vessels have evolved into highly advanced systems.

Although a rapid pace of innovation may be of vital importance for obtaining sustainable solutions for the future (DNV-GL, 2014), the challenge of timely safety verification before deployment of the new technology is a challenge. International conventions and guidelines, such as SOLAS (IMO, 1974) and "Guidelines for Vessels and Units with Dynamic Positioning (DP) Systems" (IMO, 1994, IMO, 2017), play an important role in maritime safety. Classification societies have traditionally supplied an independent opinion on the quality and safety of maritime vessels (Boisson, 1994). They now develop class rules, such as DNV-GL's rules for classification of ships (see DNV-GL, 2018). The class rules consist of detailed requirements for ensuring compliance with relevant international conventions, standards and guidelines and are used by the classification societies as criteria for the certification of systems. For example, for DP systems, verification of their compliance to the relevant chapters in the class rules traditionally involves practical sea trials (IMCA, 2011, Spouge, 2004), inspections, documentation review (such as a Failure Mode and Effect Analysis (FMEA) intended to document technical equipment redundancy (IMCA, 2016, DNV, 2012, Spouge, 2004)) and, in some cases, hardware-in-the-loop (HIL) testing (Section 2 in DNV-GL, 2018, Johansen and Sørensen, 2009, Marine Cybernetics, 2013, Skjetne and Egeland, 2006, Skogdalen et al., 2011, Smogeli and Augustson, 2012). When novel systems are not covered by the current, prescriptive regulation, new technology qualification processes can be applied to evaluate the parts of a system that are not covered by existing requirements (Hother and Hebert, 2005, Sabetzadeh et al., 2011, Rahimi, 2013, McGregor et al., 2012, Rahimi and Rausand, 2015). Industry standards and guidelines also exist for such processes (DNV, 2011, ABS, 2017a, ABS, 2017b). The challenge for this approach is that it tends to lack a holistic view on safety. Safety is not a property that is associated with individual components, subsystems or system disciplines and properties and reliability at a sub-system level, need not imply safety at system level (Leveson, 1995). In addition to investigating the reliability of the

new technology, the focus should be on how the new technology integrates with the system and how this may affect system-level behaviour.

In other industries, such as the Norwegian and UK offshore oil and gas industry, a shift towards goal-based regulation has taken place (McAndrews, 2011). Such an approach, in contrast to prescriptive certification criteria which, at best, only encodes the best practice at the time the requirement is written (Bloomfield and Bishop, 2010), can represent a dynamic and flexible approach to safety verification. With such an approach, novel systems can be analysed individually to derive criteria for certification intended to ensure compliance with high-level goals, such as safety. There are several methods and approaches for doing this, such as safety cases and goal refinement methods. Challenges, such as confirmation bias and the "out of sight, out of mind" phenomenon may make analysts less likely to detect safety hazards than would be the case if they actually set out to uncover short-comings with the system, rather than to collect evidence that it meets performance goals (Leveson, 2011a). In systems engineering, requirements are commonly derived by means of goal refinement or goal-oriented requirements engineering (Lamsweerde, 2001). Safety requirements, however, cannot be derived successfully by means of refining goals alone. Typically, properties, such as safety and security are, in the requirements engineering literature, vaguely referred to as a non-functional addendum to the requirements (e.g. Lamsweerde, 2001). Zave (1997) explicitly classifies the problem of converting such vague goals into specific system properties and behaviours as one of the research problems in the field of requirements engineering.

In IMO's Goal Based Standard (GBS) approach, (IMO 2011), goals are defined as high level objectives to be met and functional requirements provide criteria for meetings those goals. GBS requires that rules and regulations containing detailed requirements for meeting the functional requirements are derived. A specific process or method for doing this is not prescribed. Nunez Sanchez (2016) argued that there may be no need to develop rules and regulations to ensure compliance with functional requirements and goals but that risk analysis can be used to show compliance with the functional requirements. The approach proposed in Rokseth et al. (2018) develops detailed verification objectives and scenarios as a qualitative link between high level goals and acceptance criteria at the level of physical implementation. The method introduces flexibility and helps to uncover new hazards related to new technology. To become economically feasible in the maritime industry however, methods to ensure safety may have to be developed that are applicable to a larger number of systems (i.e. a family of systems).

The objective of this paper is to present a robust way of deriving, structuring and updating detailed safety requirements. Instead of analysing individual systems to derive criteria for compliance with high-level goals, detailed requirements are developed for families of systems (such as classes of ships). Potentially hazardous scenarios and safety requirements to avoid these are derived by means of Systems-Theoretic Process Analysis (STPA). The safety requirements and the scenarios are structured in a requirement hierarchy where the scenarios represent the rationale behind the safety requirements branching out from them. The proposed method, as such, can potentially be used as a tool in GBS to ensure and show that goals and functional requirements are met by those who need to meet the goals. More generally, the proposed method can be used to ensure compliance with any high-level safety goals.

The safety requirement hierarchies proposed in this paper can evolve during technological evolution of systems. Relevant previous experiences and new implications for safety are captured when new technologies, such as autonomous ships and hybrid power systems, emerge. This is achieved by modelling and analysing systems initially at a generic level and, then, by gradually refining the models and analyses until they describe a specific physical implementation. As noted in Leveson (2000), models described at high levels of abstraction are related to a specific purpose that can be realised by several physical implementations. Describing models at lower levels requires specifying and choosing between possible physical implementations. When new technology and alternative solutions appear, relevant models are developed that describe the new physical implementation. The method ensures traceability in terms of intentions and highlights which assumptions each safety requirement is based on.

The following section provides the necessary theoretical background and describes the proposed method. Section 3 presents a case study where the proposed method is applied, initially on station-keeping systems for marine surface vessels. The case study illustrates the method and describes each step in more detail. In Section 4, the proposed method is evaluated in the light of results and experience from the case study and, finally, the work is concluded in Section 5.

2. METHOD

The method presented in this section consists of two phases: the first phase deals with how to develop a generic safety requirement hierarchy for a family of systems (such as station-keeping systems for marine vessels) and the second phase deals with how to utilise and adapt the generic requirement hierarchy to specific systems or subsets of the family of systems (such as DP systems). The method proposed in this paper is based on the following theory.

2.1 THEORETICAL FOUNDATION

STPA is a method for hazard identification and hazard control based on the Systems-Theoretic Accident Model and

Processes (STAMP)-framework. Successful application of the method has been reported in several industry domains (Periera et al., 2006, Blandine, 2013, Young and Nancy, 2013, Ishimatsu et al., 2014, Rosewater and Williams, 2015, Adesina et al., 2017, Mahajan et al., 2017). In STAMP, safety is considered as a control problem (Leveson, 2011b). Previous work has demonstrated that STPA is a method that is well suited to identifying hazards and for deriving safety requirements for advanced maritime vessels, such as DP vessels (Abrecht and Leveson, 2016, Rokseth et al., 2017, Rokseth et al., 2018). It is also well suited to developing a traceable hierarchy of requirements because it focuses on identifying hazardous scenarios. The safety requirement intention can be linked back to potential system accidents through the hazardous scenario they are intended to prevent.

The system under consideration is modelled as a hierarchical control structure, where controllers, control responsibilities, control actions and feedback signals are identified, along with the control topology of the system and process model variables. A process model is a controller's "mental model" of the system or controlled process. It represents a controller's understanding, belief, or perception regarding relevant states in the system and its environment and how to affect them, if possible.

Next, the system accidents (events that involve losses (Leveson, 2011b)) and system hazards (system states that will result in accidents under worst case environmental conditions (Leveson, 2011b)) are identified. The wide definition of accidents in STPA may include problems that are traditionally not considered as being safety problems, such as security (Young and Nancy, 2013, Williams, 2015).

The next step is to identify potentially Unsafe Control Actions (UCAs) that may result in hazardous system states. Leveson (2011b) defines four generic ways that a control action may result in a hazard: a necessary control action is not provided; an unsafe control action is provided; a control action is provided too early or too late or in the wrong sequence; and a control action is applied for too long or not long enough.

When UCAs have been identified, STPA proceeds to identify scenarios that may cause the UCAs by examining each relevant control loop to see whether any parts of it can cause the UCA.

2.2 DERIVING AND ORGANISING SAFETY REQUIREMENTS

The two phases of developing a generic requirement hierarchy and utilising and specialising it, are presented in the following section. The structure of a requirement hierarchy is presented in Figure 1. As illustrated, the ultimate purpose of the safety requirements is to make sure that unsafe control does not occur. Scenarios of violation are scenarios in which a safety requirement can be violated. In the safety requirement hierarchy, scenarios of violation branch out from the safety requirements. Safety requirements aimed at avoiding the scenarios from occurring are defined for each scenario of violation.

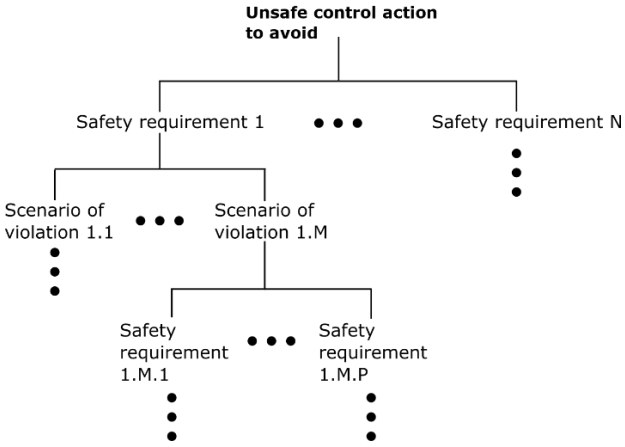

Figure 1: The structure of a requirement hierarchy.

2.2 (a) Phase 1 – Developing a Generic Safety Requirement Hierarchy

The method for developing a generic safety requirement hierarchy can be outlined in five steps, as illustrated in Figure 2. A generic requirement hierarchy includes safety requirements for a family of systems. A "family of systems" means a group of systems with similar capabilities achieved through different means. It may refer, for example, to types of maritime vessels with similar performance characteristics (e.g. offshore supply vessels) or maritime vessels with station keeping capabilities. A "generic" requirement hierarchy means that all requirements and scenarios in the hierarchy are applicable to all members of a given family of systems.

In Step 1, a basic model is developed. Description of the physical implementation level should be avoided to keep the model generic for the intended family of systems. Hence, the model must be described at a high level of abstraction. The modelling process involves determining a control topology, identifying basic control actions and identifying process model variables. Step 1 determines which specific systems the requirement hierarchy can be adapted and utilised for later. The basic system model should be documented by means of figures, tables, and natural language or by whatever means appropriate.

Step 2 is to determine system-level accidents and hazards. A collision is an example of a system-level accident for a ship. Violation of some minimum distance of separation to an obstacle is an example of a system-level hazard that may cause a collision. The third step deals with identifying unsafe control actions. These can be developed by combining the basic control actions identified in Step 1 with the generic modes of unsafe control presented in the previous section and combinations of states of process model variables. In Step 4, safety requirements are identified to control or avoid unsafe control actions or

scenarios. Step 5 identifies scenarios in which the safety requirements can be violated. Steps 4 and 5 represent an iterative process where new safety requirements are identified for scenarios of violation. This iterative process is continued until reasonable scenarios of violation cannot be formulated without making additional assumptions regarding system implementation.

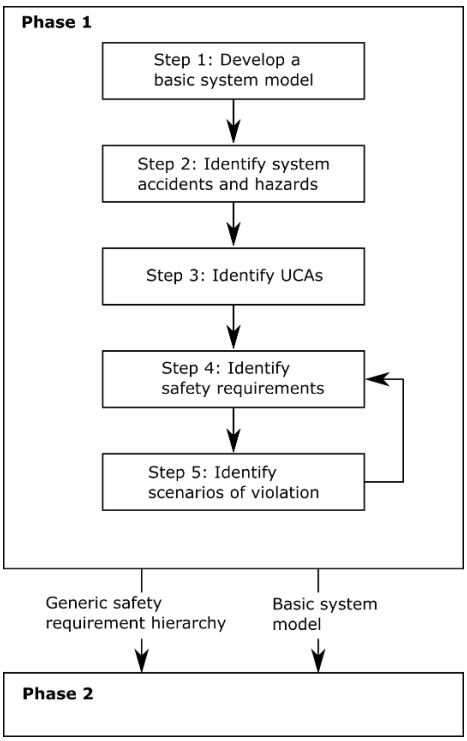

Figure 2: Steps to develop a generic safety requirement hierarchy.

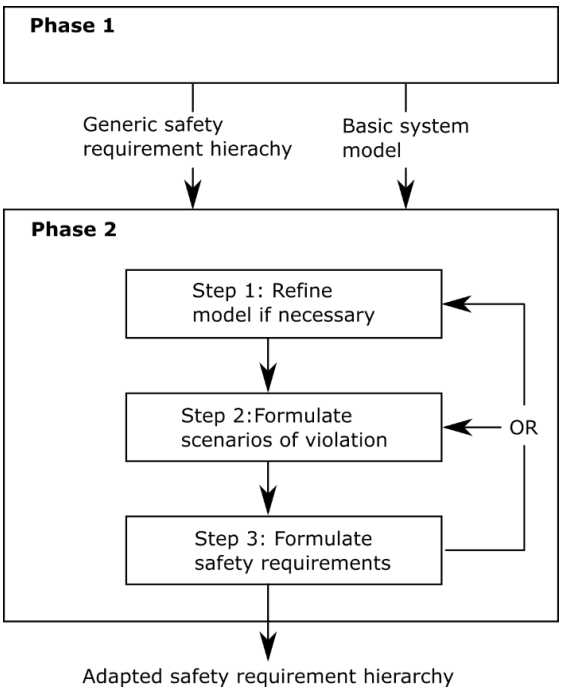

Figure 3: Steps to utilise and adapt a generic safety requirement hierarchy.

2.2 (b) Phase 2 – Utilising and Adapting the Generic Safety Requirement Hierarchy

The generic safety requirement hierarchy, which results from Phase 1, is applicable for a family of systems. The objective of Phase 2 is to utilise and adapt the generic requirement hierarchy to derive more detailed specifications for a system. Figure 3 presents the steps for this second phase.

The generic requirement hierarchy, along with a basic system model from Phase 1, is input to this phase. Phase 1 is finished when it is not possible to formulate new scenarios of violation without making assumptions about the physical implementation of the system. Making refinements to the basic system model by specifying physical implementation, typically enables scenarios of violation to be formulated. In the second phase, such refinements to the basic system model are made as necessary to formulate scenarios of violation. This corresponds to the first step in Figure 3.

The iterative process of formulating safety requirements and scenarios of violation is continued in Steps 2 and 3, and the generic safety requirement hierarchy is extended with refined requirements. When a scenario of violation cannot be formulated without further specifying physical implementation, the basic model can be refined. As new scenarios and safety requirements are identified, different requirements and scenarios will be associated with different sets of assumptions, regarding the physical implementation of the system.

3. CASE STUDY: STATION KEEPING

The method explained in the previous section has been applied to an example system for illustration and evaluation. The case study is designed to highlight i) how a basic system model can be used to develop a generic safety requirement hierarchy, ii) how this hierarchy can be specialised, and iii) how new technology may affect system safety by making safety requirements inapplicable or inadequate and how this can be addressed.

The case study starts by considering maritime surface vessels capable of station keeping. Station keeping refers to the function of restricting horizontal excursions and providing directional control of the surface vessel, in line with the definition in Moan (2009). Examples of how station keeping may be conducted include DP systems, mooring systems and tug-assisted station keeping. A maritime surface vessel refers to any ship or floating construction, such as a mobile offshore drilling unit. A generic requirement hierarchy is made for “maritime surface vessels capable of station keeping”, using the steps from Phase 1. Next, the generic requirement hierarchy is adapted and specialised by assuming that station keeping is performed by means of DP. First, it is assumed that the DP system is powered by a traditional diesel-electric

power system. The current technological trend is to equip new vessels with other, more versatile types of power systems (Miyazaki et al., 2016). The case study illustrates how a requirement hierarchy that was specialised for DP vessels with traditional diesel-electric power systems, can be adapted to DP vessels with battery-enhanced diesel electric power systems.

3.1 PHASE 1 – DEVELOPING A GENERIC HIERARCHY OF SAFETY REQUIREMENTS

3.1 (a) Step 1. Developing the Basic System Model

The common way of modelling control structures in STPA is to base the control hierarchy topology on the physical layout of the system under consideration. This is convenient if the analysis is conducted at a level of abstraction where specific control entities are defined. When developing a basic system model however, this may not be the case, because the basic system model should be representative of all possible implementations of a family of systems. If a typical DP system topology is used to represent a station-keeping system, it will not apply, for example, to vessels where station keeping is performed by means of a mooring system. In a basic system model, basic control functions can be collected into control entities based on features such as the level of authority and whether they are distributed or local control functions, making an abstract representation of the control structure. For example, a control function aimed at engaging or disengaging a vessel from an operation being conducted, must be issued from a controller with relatively high authority and it must be distributed throughout the vessel. At even higher levels, control actions are aimed at coordinating the efforts of several vessels.

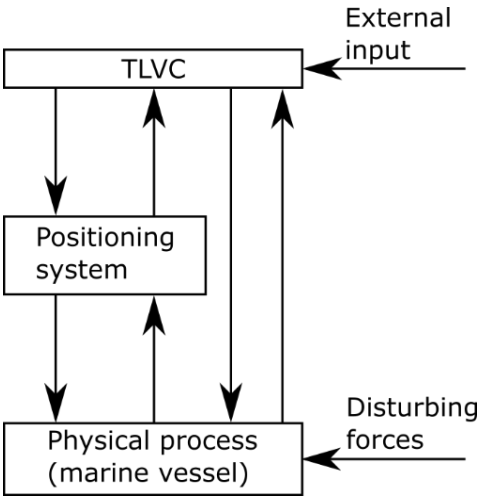

Figure 4: Control structure diagram for station keeping of marine surface vessel.

The basic control hierarchy (presented in Figure 4) includes the following entities:

- The Top Level Vessel Control (TLVC) is an entity responsible for strategic and distributed control tasks on a marine vessel. It does not represent a physical entity, such as a computer control system or a vessel officer, but rather it represents a collection of high-level control functions.
- The positioning system is a generalised, physical implementation that enables station keeping; it constitutes the “station-keeping actuator”.
- The physical process represents the controlled process, i.e. the motion of the vessel.

An example of a basic control action for TLVC is "terminate work in progress". How work is terminated depends on the operation that is conducted. A mobile offshore drilling unit may cut or retrieve the drill string and disconnect the riser from the well. For a diving support vessel with divers in the water, terminating work may refer to retrieving divers from the water.

Examples of relevant process model variables for the TLVC are presented and described in Table 1. “Disturbing forces” refers to the forces imposed by wind, waves, current and, in some cases, from the work being conducted (such as forces acting on a winch). “External input to TLVC” may refer to weather forecasts, procedures and instructions from shore or other vessels or installations.

Table 1: Process model variables for the station-keeping model

ID	Process variable	Description
PV-1	Station keeping capability/precision	TLVC's belief regarding the relationship between external forces and the ability of the system to maintain the vessel at station at given levels of precision
PV-2	Future weather conditions	Expected weather conditions during the rest of the operation and their effect on the station-keeping capability
PV-3	Necessary station keeping precision	The level of precision necessary for the work currently taking place
PV-4	Safety-critical work	Whether safety-critical work is being conducted
PV-5	Operational mode and configuration of the positioning systems	How is the positioning system configured and in which operating modes is it operating?

3.1 (b) Step 2. Identifying System-Level Accidents and Hazards

The next step is to define system accidents and hazards that should be avoided. Guidelines for this step can be found in Leveson (2011b). Relevant accidents are, for example, damage to equipment used to conduct the work in progress, collision of the vessel with fixed structures or terrain, and collision of the vessel with other vessels. A hazard that may result in any of these is:

- H-1: Loss of station-keeping capability or the required precision while work is conducted.

3.1 (c) Steps 3 to 4. Identifying UCAs and Safety Requirements

UCAs that can result in the specified hazard can be found by considering each possible control action together with the generic modes of unsafe control, described in Leveson (2011b) and summarised in Section 2.1. The process model variables can be used to specify the context in which the control actions may be unsafe. In this case study, we consider the control action "terminate work in progress" together with the generic mode of unsafe control "a necessary control action is not provided". A context in which this is unsafe is identified by considering the process model variables PV-1, PV-3, and PV-4 from Table 1 (station-keeping precision is not sufficient while safety critical work is taking place). Combining this, a UCA becomes:

- UCA-1: Work in progress is not safely terminated before the station-keeping capability or the required station-keeping precision is lost.

A safety requirement for this is found by re-phrasing UCA-1 as:

- R-1: Work in progress must be safely terminated before the station-keeping capability or the required station-keeping precision is lost.

3.1 (d) Steps 4 to 5. Refining Safety Requirements through Scenario Identification

Scenarios of violation are identified by examining all relevant control-loops for the controller under consideration, to see if any part of the control loops can lead to unsafe control. Safety requirements are identified to prevent hazardous scenarios. Examples of scenarios of violation for safety requirement R-1 are:

- SoV-1: Weather forecast did not provide warning of deteriorating weather conditions in time for work in progress to be terminated safely.
- SoV-2: TLVC incorrectly concludes that performance of the positioning system is adequate by evaluating position feedback, when in fact position feedback has frozen and station keeping is performed less precisely than required.
- SoV-3: TLVC does not choose to terminate work in progress due to economic or other pressures, even though the station keeping performance is approaching an inadequate level of precision.
- SoV-4: TLVC overestimates the system capability and therefore does not initiate termination of work in progress in time when external forces are increasing and approaching system maximum capacity.
- SoV-5: TLVC reconfigures the positioning system to a state in which it is not capable of performing adequate station keeping because TLVC is unaware that the reconfigured state will not be able to perform as required.
- SoV-6: TLVC is not aware of how much time is needed to terminate work in progress and therefore issues the command to terminate work in progress too late, when the system is approaching maximum capability.
- SoV-7: Component failure or other sudden change in the positioning system renders the positioning system unable to perform station keeping with the required performance, leaving insufficient time to safely terminate work in progress.
- SoV-8: An abnormal wave, a gust of wind, or drift ice suddenly forces the vessel out of position.
- SoV-9: External force from work in progress suddenly forces vessel out of station.
- SoV-10: The control action to initiate termination of work in progress has not been relayed or is not followed by the responsible party.

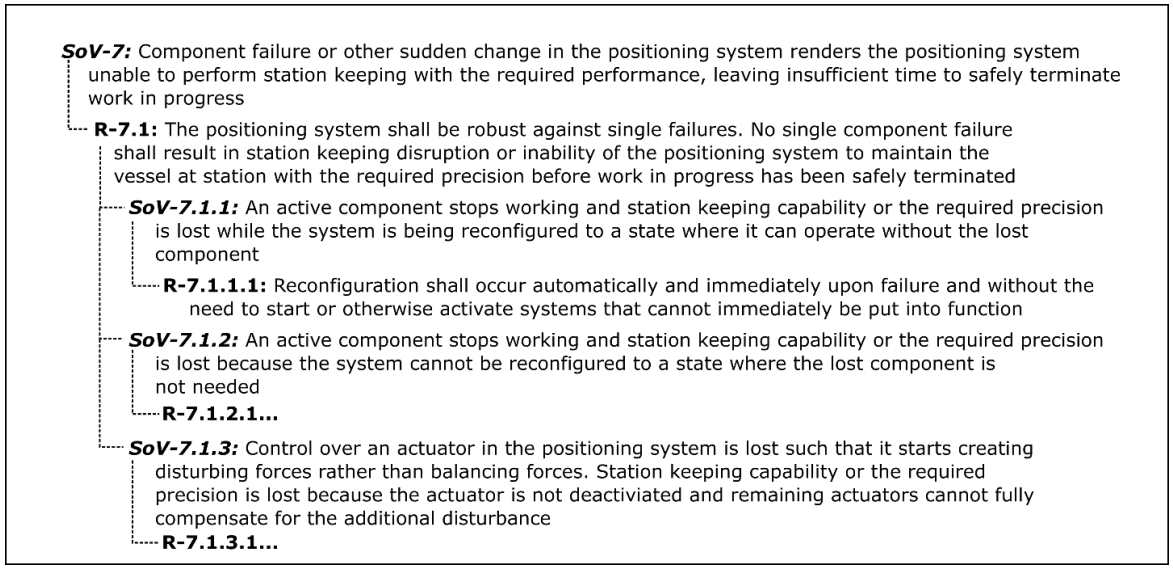

Figure 5: Excerpt from a generic requirement hierarchy for station keeping

Figure 5 shows a few iterations of the scenario of violation SoV-7. No assumptions about the physical implementation of the system have been made, except for those defined in the basic system model. It is difficult to formulate further scenarios of violation for the safety requirement R-7.1.1.1 without making new assumptions regarding system implementation. We therefore proceed to Phase 2.

3.2 PHASE 2 – UTILISE AND ADAPT THE GENERIC SAFETY REQUIREMENT HIERARCHY

3.2 (a) Model Refinement Step

The basic system model can be refined according to specific assumptions regarding the physical implementation to enable the formulation of new scenarios of violation. Model refinements can be performed by refining the control hierarchy, defining more precise control actions, or defining additional process model variables for controllers. This means that the basic system model, describing maritime vessels capable of station keeping, is refined into a more specific model, which describes a maritime vessel capable of performing station keeping by means of a DP system. This model (maritime vessel capable of station keeping by means of DP) is, in turn, refined into two alternative physical implementations to satisfy the function electrical power generation, i.e. a traditional diesel-electric power system and a battery-enhanced diesel-electric power system.

Station keeping by means of DP: A refined control hierarchy is illustrated in Figure 6. The actuator system, in the basic system model referred to as the positioning system, has been refined into a thruster system and a power system. Additionally, the physical process has been refined into work in progress and vessel motion, where "work in progress" refers to the work process that is being conducted (i.e. the reason why the vessel is performing station keeping) such as diving, crane operation or drilling. The vessel motion is affected by forces from the thruster system, environmental forces, and forces induced by the work in progress. Sufficient amounts of power must be available for the thruster system to produce the required forces. The maximal amount of power that can be immediately provided under a given configuration is referred to as the available power.

Some relevant process model variables for TLVC in this model are "available power" and "load demand". An example of refined control responsibility is that TLVC is responsible for configuring the thruster system and the power system.

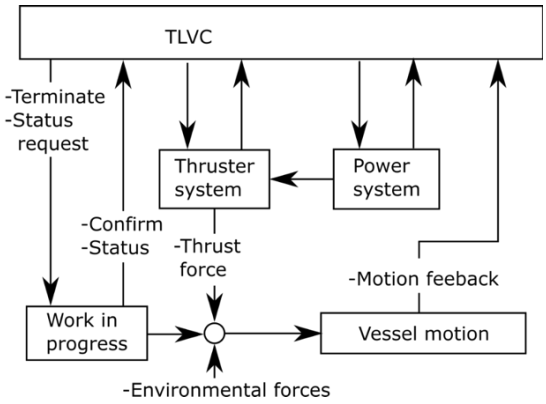

Figure 6: Control structure diagram for station keeping by means of DP.

The traditional diesel-electric power system: A common type of power system for DP vessels is a diesel-electric power system (Ådnanes, 2003). Diesel generators transform mechanical energy from a diesel engine into electrical energy that is distributed over an electrical bus. The electrical distribution supplies power for thrusters and other consumers. The configuration of the power distribution is controlled by means of various power switches.

Figure 7 shows a control structure for a traditional diesel–electric power system, as described above. Some process model variables that are relevant for TLVC in this model are listed in Table 2.

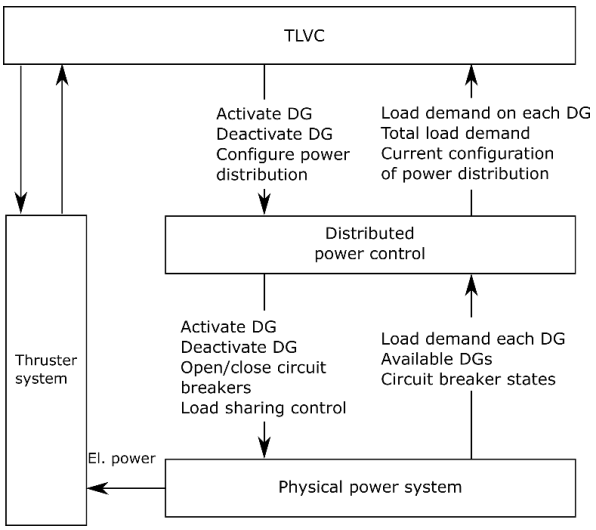

Figure 7: Possible control structure for a diesel-electric power system for a DP vessel.

Table 2: Additional process model variables for TLVC for DP-vessels powered by diesel-electric power systems.

Process model variable	Description
Worst case failure	The failure that most severely affects the power system's ability to produce power
Load condition for each diesel generator	How much power is produced by each active diesel generator
Maximal Continuous Rating (MCR) for each diesel generator	The maximum power output that can be produced continuously by each diesel generator
Potential load step	The largest potential loads step that may reasonably be expected to occur for each active generator (e.g. in the event of the failure of another generator)
Tolerable load step	The largest sudden load step each diesel generator may handle without sustaining a severe drop in frequency

The battery-enhanced diesel-electric power system: In recent years, batteries have become feasible power supplies for marine propulsion. One example is the employment of batteries to let diesel engines operate at optimal loading conditions (in terms of minimising their specific fuel consumption), by charging or discharging batteries and starting and stopping a diesel generator accordingly. Another function of batteries is to serve as "spinning reserves" as an alternative to running additional diesel generators to satisfy safety requirement R-7.1.1.1. We will refer to diesel–electric power systems where batteries can serve one or more of these functions, as "battery-enhanced diesel–electric power systems".

The control hierarchy presented in Figure 7 is also suitable for representing battery-enhanced diesel–electric power systems, if we include the physical batteries in the "Physical power system" and assume that the controller "Distributed power control" also controls the batteries. It is necessary however, to add the following process model variables to the TLVC: "state of charge for each battery"; "power output for each battery"; "estimated time left to full discharge"; and "safe operating area" (i.e. limitations on rates of charge and discharge to limit battery temperature). New control actions must also be defined. First, TLVC must choose operating strategies and decide how to employ batteries and diesel generators. Second, the control entity named "distributed power control" must connect and disconnect batteries and control the charge and discharge rates, such that the batteries behave in a manner that is suitable for the desired operating modes.

3.2. (b) Refining Safety Requirements Through Scenario Identification

Using the assumptions developed for station keeping by means of DP, scenarios of violation are identified for safety requirement R-7.1.1.1 in Figure 5. One of these is presented in Figure 8, with two associated safety requirements. Two scenarios of violation are identified for the first of these, one of which assumes a traditional diesel electric power system, and the other applies to all DP vessels. One scenario of violation is identified for the latter safety requirement. This one is also based on the assumption of a traditional diesel-electric power system. The safety requirements, scenarios of violation and underlying assumptions are presented in the figure. Thus, Figure 8 shows examples of the safety requirements applicable to all vessels that can perform station keeping, for vessels that can perform station keeping by means of DP, and the safety requirements specific to vessels that use traditional diesel-electric power systems to perform station-keeping by means of DP.

Now let us consider a case where a DP vessel outfitted with a battery-enhanced, diesel-electric power system is to be designed. In this case, the assumption of a traditional diesel-electric power system is not valid and, therefore, the safety requirements in the dark grey areas in Figure 8 (i.e. those based on the assumption of a traditional diesel-electric power system) may not be applicable and do not ensure safety. The simplest way to update the safety requirements hierarchy in Figure 8, so that they are applicable to and ensure the safety of the new system, is to replace these requirements with requirements derived from the model assumptions formulated for battery- enhanced diesel-electric power systems. Using the model assumptions derived for battery-enhanced diesel-electric power systems, new appropriate scenarios of violation and safety constraints are identified and presented in Figure 9.

4. RESULTS AND DISCUSSION

4.1 RESULTS COMPARED TO CURRENT REQUIREMENTS AND STANDARDS

To evaluate the results from the case study, we consider the similarities and differences between the safety requirements found in the case study and the requirements navigation, manoeuvring and position keeping (DNV-GL, 2018). The results from the case study are compared to requirements for DP equipment classes 2 and 3 (in IMO, 1994), and the corresponding class notations because "DYNPOS(AUTR)" or "DPS(2)" and vessels that satisfy "DYNPOS(AUTRO)" or "DPS(3)" in (DNV-GL, 2018), found in the IMO's guidelines for vessels with DP systems these requirements are usually required for safety critical operations. Table 2 shows the extent to which the safety requirements for station keeping by means of DP for vessels equipped with traditional diesel–electric power systems (presented in Figure 8), are represented in DNV-GL (2018) and IMO (1994). Table 3 shows that some of the safety requirements are present in all three sources, but the method proposed in this paper also reveals and specifies additional requirements.

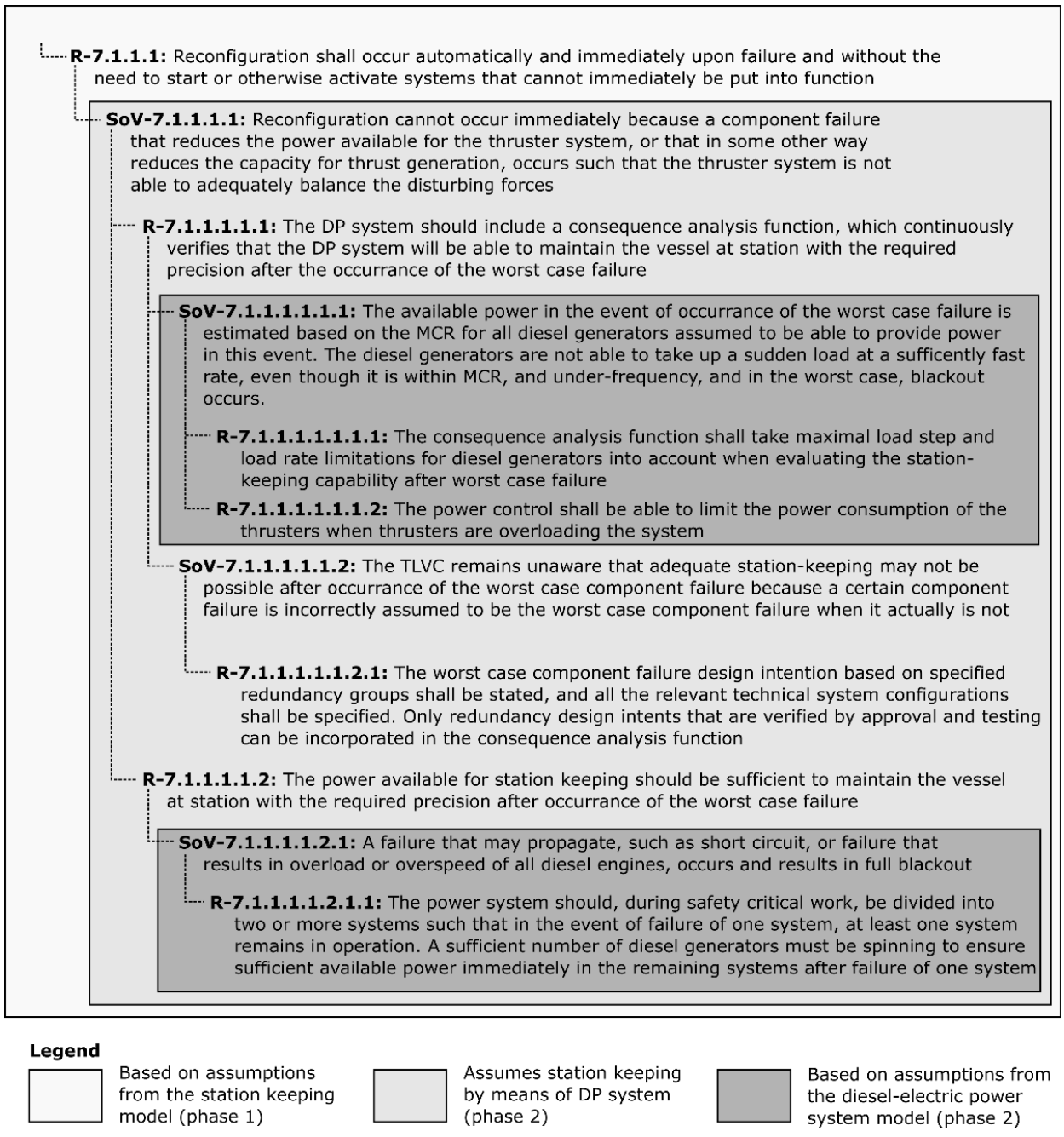

Figure 8: Excerpt of a safety requirement hierarchy for descendants of safety requirement R-7.1.1 for DP vessels with traditional diesel-electric power systems.

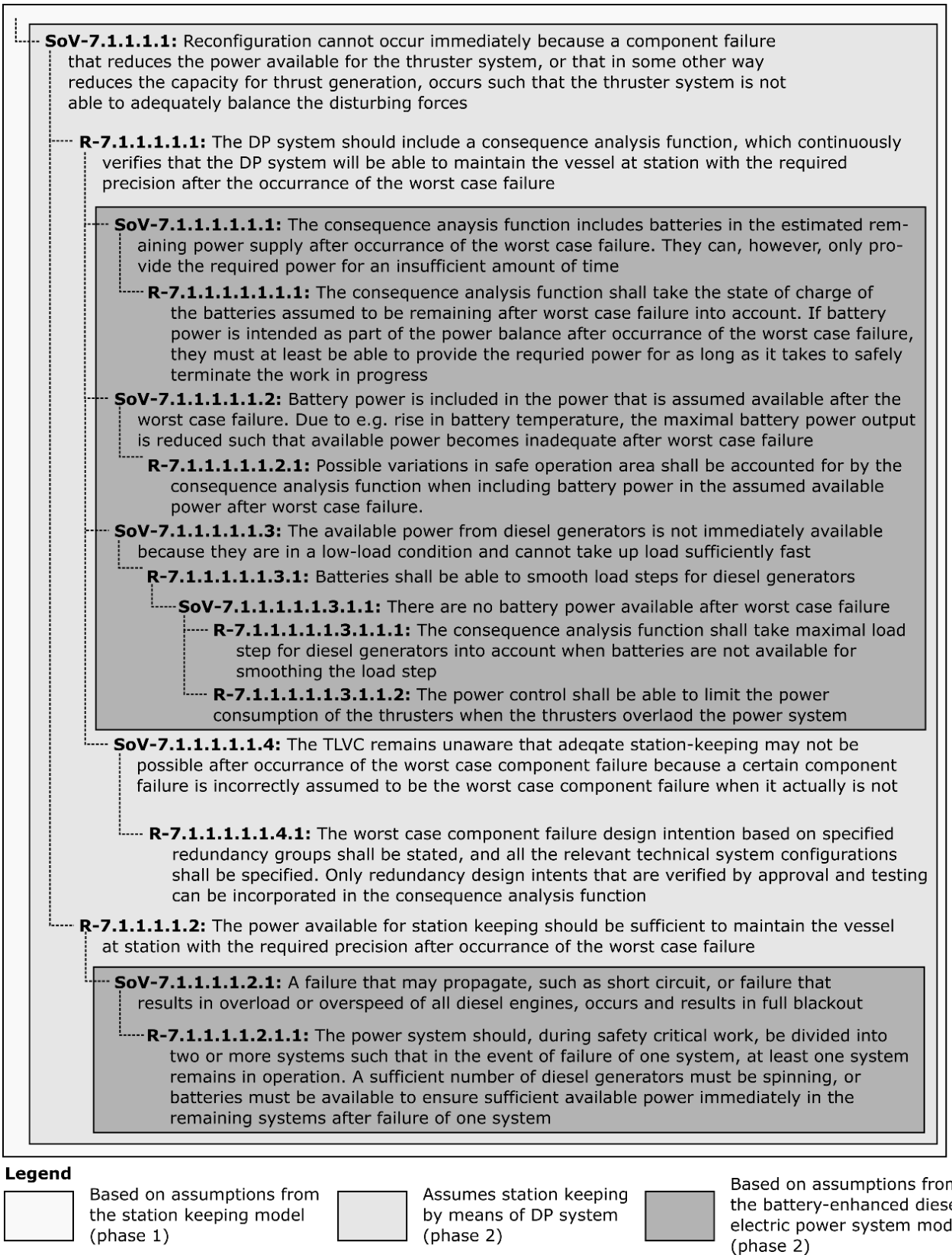

Figure 9: Excerpt of a requirement hierarchy for descendants of safety requirement R-7.1.1 for DP vessels with battery-enhanced diesel-electric power system

Safety requirement R-7.1.1.1 states that reconfiguration of the positioning system should occur automatically and immediately upon failure without the need to start or otherwise activate systems that cannot immediately be put into function. Similar requirements are found in IMO (1994) and DNV-GL (2018). The difference is that where we specify that it should not be necessary to start or activate "systems", IMO specifies that there should be no need to start or activate "redundant equipment" and DNV-GL uses the term "machinery" in the same context. The difference here is that R-7.1.1.1 is more general, including, for example, software and not just physical equipment and machinery.

Safety requirement R-7.1.1.1.1.1.1.1, which states that the maximal load step for diesel engines should be taken into account by the consequence analysis function, is covered by neither DNV-GL (2018) nor IMO (1994). The reason for this may be that it is too impractical. Instead, DNV-GL (2018) requires that the power control shall be able to limit the power consumption of the thrusters when thrusters are overloading the system (i.e. equivalent to R-7.1.1.1.1.1.1.2). Note, however, that this is not a perfect solution because full motion control will be lost while the thruster system is limited. If safety requirement R-7.1.1.1.1.1.1.1 is not implemented in the class rules because it is too impractical, this is clearly a point in favour of the battery-enhanced system, for which this does not appear as a problem in the analysis.

Unlike the class rules and the IMO's requirements, the requirement hierarchy developed in this paper provides full traceability of the intention of each safety requirement through the scenarios of violation.

Table 3: Safety requirements derived in the case study for DP vessels with traditional diesel-electric power systems and comparison with existing requirements from IMO and DNV-GL.

Safety requirements	**Covered by IMO circ. 645 (IMO, 1994)**	**Covered by DNV-GL (DNV-GL, 2018)**
R-7.1: The positioning system shall be robust against single failures. No single component failure shall result in station keeping disruption or inability of the positioning system to maintain the vessel at station with the required precision before work in progress has been safely terminated.	2.2.2 (Equipment classes) 2.2.3 (Equipment classes) 4.3 (Operational requirements)	4.1.2 (General arrangements – General requirements) 4.3.1 (General arrangements - Redundancy)
R-7.1.1.1: Reconfiguration shall occur automatically and immediately upon failure and without the need to activate systems that cannot immediately be put into function.	3.1.4 (General)	4.3.3 (General arrangements – Redundancy)
R-7.1.1.1.1.1: The DP should include a consequence analysis function, which continuously verifies that the DP system will be able to maintain the vessel at position with the required precision after the occurrence of the worst-case failure.	3.4.2.4 (DP-control system – Computers)	6.13.1.1 (Control systems – Consequence analysis)
R-7.1.1.1.1.1.1.1: The consequence analysis function shall take maximal load step and load rate limitations for diesel generators into account when evaluating the station-keeping capability after worst case failure.	No	No
R-7.1.1.1.1.1.1.2: The power control shall be able to limit the power consumption of the thrusters when thrusters are overloading the system.	No	8.1.2 (Power systems - General) 8.8.4 (Power systems – Power management)
R-7.1.1.1.1.1.2.1: The worst-case component failure design intention based on specific redundancy groups shall be stated, and all the relevant technical system configurations shall be specified. Only redundancy design intents that are verified by approval and testing can be incorporated in the consequence analysis function.	No	4.2.2 (General arrangement – Redundancy and failure modes)
R-7.1.1.1.1.2: The power available for station keeping should be sufficient to maintain the vessel at station with the required precision after occurrence of the worst-case failure.	3.2.5 (Power system)	No
R-7.1.1.1.1.2.1.1: The power system should, during safety critical work, be divided into two of more systems such that in the event of failure of one system, at least one system remains in operation. A sufficient number of diesel generators must be spinning to ensure sufficient available power immediately in the remaining system after failure of one system.	3.2.3 (Power system)	Refers to 3.2.3 IMO (IMO, 1994) (Power system – General)

4.2 FEATURES OF THE HIERARCHICAL STRUCTURE

The main challenge when introducing flexibility, with respect to new physical implementations by updating sets of safety requirements, is that safety is a system property (Leveson, 2011b). Safety is an emergent property that is affected by the interactions between components and functions in a system. It is therefore not simply a matter of identifying a set of additional safety requirements associated with the new physical implementation and removing those associated with any replaced physical implementations. Unlike most ways of organising requirements, this paper does not organise requirements according to a system–subsystem-component or function–sub-function (i.e. structural or functional) arrangement. A requirement that is enforced, for example, on the thruster system is not, as in (DNV-GL, 2018) or (IMO, 1994), found under a subdivision referred to as a "thruster system", or under "requirements to generate thrust".

Instead, the hierarchies are organised according to safety concerns, in terms of how scenarios may violate safety requirements. This is important because whenever new technology is introduced, the implications to safety may propagate across functional or structural sub-divisions. Replacing a certain physical implementation to achieve some purpose in a different way, may put new restrictions on how a different function can be realised. By tracing which assumptions the safety requirements are based on in a specialised requirement hierarchy, it is possible to identify which safety requirements must be adapted to accommodate a change by observing which assumptions are not compatible with the change.

A reasonable question to ask is whether the method of updating safety requirements actually covers all new hazards that are introduced by a new technology, when changing a physical implementation. The approach is based on top-down reasoning and produces a set of safety requirements, branching out from each hazardous scenario. These safety requirements will ensure that the scenario cannot occur as long as the safety requirements are not violated. Any safety requirement at a lower level addresses a part of the problem of satisfying a safety requirement at a higher level, but at an increased resolution. This means that as long as the safety requirements at the top level are all satisfied, the system is considered to be safe (in terms of the defined system accident). To ensure compliance with the top-level safety requirements, it is necessary to ensure that all of the lower-level requirements are satisfied. Any changes in the physical implementation of the real system may cause the real system to become incompatible with some of the safety requirements in the specialised hierarchy. Due to the top-down approach, safety concerns emerging as a consequence of a new physical implementation should manifest as an incompatibility between system assumptions and the actual system. This is only true as long as new potential system level accidents or hazards are not introduced.

Safety concerns relating to a new type of technology may not be addressed in a requirement hierarchy (generic or specialised) if they are not related to any of the already existing system accidents. In this case, an entirely new safety concern is introduced to the system, for example, a radiation hazard for a system where this has not been a concern previously. As such, it may be relevant to consider if any new potential system accidents have been introduced when updating or adapting a requirement hierarchy.

The internal structure of a set of safety requirements is not necessarily the best way of presenting them to users, such as system designers and test engineers. The structure presented in this paper is aimed at making adaptations and implementing changes as effectively as possible. Structures, such as those in DNV-GL (2018) and IMO (1994), on the other hand, while not supporting adaptation and implementation of change, are suitable, for instance, for a test engineer who is responsible for verifying a power system or for an engineer designing a power system.

4.3 CERTIFICATION AND VERIFICATION OF NEW TECHNOLOGICAL SOLUTIONS

The method proposed in this paper can be a feasible way of developing and maintaining class rules. Class rules address classes of systems (denoted "family of systems" in this paper), such as ships of a certain type. The method provides safety requirements with a documented intention and a systematic way of updating and altering the hierarchies when new technology appears.

The approach proposed in this paper can be integrated into other proposed approaches, such as IMO's GBS-approach (IMO, 2011). Failure to satisfy the functional requirements defined in the GBS-approach can be defined as system accidents. Both generic and detailed safety requirements can be derived, as demonstrated in this paper. Nunez Sanchez (2016) proposed to perform a risk analysis on each vessel to show compliance with the functional requirements of the GBS approach. While the motivation in Nunez Sanchez (2016) is to introduce flexibility in satisfying the functional requirements, the downside is the significant costs associated with analysing each vessel. By using the approach proposed in this paper, the flexibility is retained, but without the cost of conducting a full-scale analysis for each system development project. Instead, only the relevant parts of a requirement hierarchy could be updated, as illustrated in Figure 8 and Figure 9. Furthermore, the safety requirements may constitute a basis for certification and verification of new technological systems, as it provides and documents a detailed and visible process justifying each safety requirement.

5. CONCLUSION

Ensuring the safety of advanced maritime vessels, such as DP vessels, is becoming an increasingly challenging task. Although improved verification techniques, such as hardware in the loop (HIL)-testing, have become available for DP vessels, new techniques for developing requirements that ensure safe design and operation, yet allowing for flexibility, are needed. One challenge, in particular, is that identical DP vessels are rarely built, if ever. Still, certification of vessels is based on verification of relatively prescriptive requirements that are common to a class (or family) of vessels. While this simplifies some of the challenges related to verification, it also makes the application of new enabling technology, new solutions, and general innovation more difficult, because these innovations may not be compatible with the prescriptive requirements.

This paper presents a method that can be used to elicit safety requirements and verification objectives based on an adapted version of STPA. The paper proposes a method where a generic safety requirement hierarchy for a family of systems can be developed. The requirement hierarchies can be adapted for specific technological systems. The motivation for starting the analysis process at a generic level, instead of analysing specific systems from the beginning, is that it allows organisations to re-use the generic hierarchy and only make adaptions for each specific system, saving work effort. Adaptations can be made for a subset of a family of systems. As such, further adaptations that are made for each member of that subset will require less work than adaptions from the generic hierarchy.

The adaptations that can be developed for specific systems can be used to specify more detailed safety requirements that are easier to relate to actual design choices. The method proposed in this paper can be employed by organisations that commonly verify systems within defined families of systems, where specific hierarchies can be developed for standard systems, and adaptations can easily be made afterwards, when a novel system is encountered.

Further work includes conducting a more comprehensive case study. One interesting research objective of further study would be to evaluate, in detail, the adaptations made in the class rules of various classification societies to accommodate the use of batteries in combination with diesel generators for propulsion of advanced offshore vessels. This can be achieved by comparing the adaptations made by the classification societies with those identified in a comprehensive case study.

6. ACKNOWLEDGEMENTS

The authors greatly appreciate the constructive feedback from two anonymous reviewers on a previous version of this paper. The authors are also grateful for the discussions with and input to the paper from Odd Ivar Haugen at DNV-GL. 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)”, of which 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).

7. REFERENCES

1. ABRECHT, B. & LEVESON, N. G. 2016. *Systems theoretic process analysis (STPA) of an offshore supply vessel dynamic positioning system.* Massachusetts Institute of Technology.
2. ABS 2013. *Guide for dynamic positioning systems*. American Bureau of Shipping.
3. ABS 2017a. *Guidance notes on qualifying new technologies*. American Bureau of Shipping.
4. ABS 2017b. *Review and approval of novel concepts*. American Bureau of Shipping.
5. ADESINA, A. A., HUSSAIN, Q., PANDIT, S., REJZEK, M. & HOCHBERG, A. M. 2017. *Assessing the Value of System Theoretic Process Analysis in a Pharmacovigilance Process: An Example Using Signal Management*. Pharmaceutical Medicine, 31**,** 267-278.
6. ÅDNANES, A. K. 2003. *Maritime Electrical Installations And Diesel Electric Propulsion*. Oslo, Norway: ABB Marine AS.
7. BLANDINE, A. 2013. *Systems Theoretic Hazard Analysis (STPA) applied to the risk review of complex systems: an example from the medical device industry.* PhD, Massachusetts Institute of Technology.
8. BLOOMFIELD, R. & BISHOP, P. 2010. *Safety and Assurance Cases: Past, Present and Possible Future – an Adelard Perspective*. In: DALE, C. & ANDERSON, T. (eds.) *Making Systems Safer: Proceedings of the Eighteenth Safety-Critical Systems Symposium, Bristol, UK, 9-11th February 2010.* London: Springer London.
9. BØ, T. I. & JOHANSEN, T. A. 2016. *Battery Power Smoothing Control in a Marine Electric Power Plant Using Nonlinear Model Predictive Control*. IEEE Transactions on Control Systems Technology, 25**,** 1449-1456.
10. BOISSON, P. 1994. *Classification societies and safety at sea: Back to basics to prepare for the future*. Marine Policy, Elsevier, 18**,** 363-377.
11. BREVIK, M., KVAAL, S. & ØSTBY, P. 2015. *From Eureka to K-pos: Dynamic positioning as a highly successful and important marine control technology*. IFAC-PapersOnline, 48**,** 313-323.
12. DNV 2011. *Recommended practice DNV-RP-A203: Qualification of new technology*. DNV.
13. DNV 2012. *Recommended practice DNV-RP-D102: Failure mode and effect analysis (FMEA) of redundant systems*. DNV
14. DNV-GL 2014. *From technology to transformation*. Høvik: DNV-GL.

15. DNV-GL 2018. *Rules for classification of ships, part 6, chapter 3: Navigation, manoeuvring and position keeping*. DNV-GL.
16. HOTHER, J. A. & HEBERT, B. J. 2005. Risk *Minimization by the use of Failure Mode Analysis in the Qualification of New Technology - Recent Project Experience*. SPE annual technical conference adn exhibition. Dallas, Texas: Society of petroleum engineers.
17. IMCA 2011. *Guidance for developing and conducting annual DP trials programmes for DP vessels*. IMCA.
18. IMCA 2016. *Guidance on failure mode and effect analyses (FMEAs) (M 166)*. IMCA.
19. IMO. 1974. *International Convention for the Safety of Life at Sea (SOLAS), 1974* [Online]. http://www.imo.org/en/About/Conventions/ListOfConventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-(SOLAS),-1974.aspx: IMO. [Accessed 20.10.2017 2017].
20. IMO 1994. *Guidelines for vessels with dynamic positioning systems (IMO MSC Circular 645).* International Maritime Organization.
21. IMO 2011. *Generic Guidelines for Developing IMO Goal-Based Standards (MSC.1/Circ. 1394)*. 4 Albert Embankment London SE1 /SR.
22. IMO 2017. *Guidelines for vessels and units with dynamic positioning systems (IMO MSC.1/Circ. 1580)*. International Maritime Organization.
23. ISHIMATSU, T., Leveson N. G., THOMAS, J. P., FLEMING, C. H., KATAHIRA, M., MIYAMOTO, Y., UJIIE, R., NAKAO, H. & HOSHINO, N. 2014. *Hazard analysis of complex spacecraft using systems-theoretic process analysis*. Journal of spacecraft and rockets, 51**,** 509-522.
24. JOHANSEN, T. A. & SØRENSEN, A. J. 2009. *Experiences with HIL Simulator testing of Power Management Systems*. Dynamic Positioning Conference. Marine Technology Society.
25. LAMSWEERDE, A. V. 2001. *Goal-oriented requirements engineering: a guided tour*. Proceedings Fifth IEEE International Symposium on Requirements Engineering**,** 249-262.
26. LEVANDER, O. 2016. *Ship intelligence - A new era in shipping*. Proceedings of the International Smart Ships Technology Conference, 2016 London. 25-32.
27. LEVESON, N. G. 1995. *Safeware: system safety and computers*, ACM.
28. LEVESON, N. G. 2000. *Intent specifications: an approach to building human-centered specifications*. IEEE transactions on software engineering, 26.
29. LEVESON, N. G. 2011a. *The use of safety cases in certification and regulation*. Journal of system safety, 47.
30. LEVESON, N. G. 2011b. *Engineering a safer world: Systems thinking applied to safety*, The MIT Press.
31. MAHAJAN, H. S., BRADLEY, T. & PASRICHA, S. 2017. *Application of Systems Theoretic Process Analysis to a Lane Keeping Assist System*. Reliability Engineering & System Safety. 167, 177-183.
32. MARINE CYBERNETICS 2013. *Relevant rules and regulations for HIL testing*. White paper.
33. MCANDREWS, K. L. 2011. *Consequences of Macondo: A summary of recently proposed and enacted changes to US offshore drilling safety and environmental regulation*. SPE Americas E&P Health, safety, security and environmental conference. Houston, Texas: SPE.
34. MCGREGOR, D., BORG, J. & AHEIM, V. 2012. *New methods for qualification assisted innovation applied to a practical example*. International conference on ocean, offshore and arctic engineering. Rio de Janeiro, Brazil: ASME.
35. MIYAZAKI, M. R., SØRENSEN, A. J. & VARTDAL, B. J. 2016. *Hybrid marine power plants model validation with strategic loading*. IFAC-PapersOnLine, 49**,** 400-407.
36. MOAN, T. 2009. *Safety management of deep water station-keeping systems*. Journal of Marine Science and Application, 8**,** 83-92.
37. MONTEWKA, J., WRÓBEL, K., HEIKKILA, E., VALDEZ-BANDA, O. A., GOERLANDT, F. & HAUGEN, S. 2018. *Challenges, solution proposals and research directions in safety and risk assessment of autonomous shipping*. PSAM 14-Probabilistic Safety Assessment and Management. Los Angeles, CA.
38. NUNEZ SANCHEZ, M. 2016. *Towards a new SOLAS convention: A transformation of the ship safety regulatory framework*. International journal of maritime engineering, 158**,** A139-A146.
39. PERIERA, S. J., GRADY, L. & JEFFREY, H. 2006. *A system-theoretic hazard analysis methodology for a non-advocate safety assessment of the ballistic missile defense system*. Missile defence agency, Washington DC.
40. RAHIMI, M. 2013. *A contribution to reliability qualification of new technical equipment.* PhD, Norwegian University of Science and Technology.
41. RAHIMI, M. & RAUSAND, M. 2015. *Technology qualification program integrated with product development process*. International journal of performability enginerring, 11**,** 3-14.
42. REILLY, G. & JORGENSEN, J. 2016. *Classification Considerations for Cyber Safety and Security in the Smart Ship Era.* Proceedings of the International Smart Ships Technology Conference, 2016 London. 26-27.

43. ROKSETH, B., BOUWER UTNE, I. & VINNEM, J. E. 2017. *A systems approach to risk analysis of maritime operations*. Journal of risk and reliability, 231**,** 53-68.
44. ROKSETH, B., BOUWER UTNE, I. & VINNEM, J. E. 2018. *Deriving Verification Objectives and Scenarios for Maritime Systems Using the Systems-Theoretic Process Analysis*. Reliability Engineering & System Safety. 169, 18-31.
45. ROSEWATER, D. & WILLIAMS, A. D. 2015. *Analysing system safety in lithium-ion grid energy storage*. Journal of Power Sources, 460 - 471.
46. SABETZADEH, M., FALESSI, D., BRIAND, L., DI ALESIO, S., MCGEORGE, D., ÅHJEM, V. & BORG, J. 2011. *Combining goal models, expert elicitation, and probabilistic simulation for qualification of new technology*. High-Assurance Systems Engineering (HASE), 63-72.
47. SKJETNE, R. & EGELAND, O. 2006. *Hardware-in-the-loop testing of marine control systems.* Modeling, identification and control, 27**,** 239-258.
48. SKOGDALEN, J., ESPEN & SMOGELI, Ø. 2011. *Looking forward - Reliability of safety-critical control systems on offshore drilling vessels.* Deepwater Horizon Study Group.
49. SMOGELI, Ø. & AUGUSTSON, T. 2012. *Third party HIL testing of safety critical control system software on ships and rigs*. OMAE.
50. SØRENSEN, A. J. & LUDVIGSEN, M. 2015. *Towards Integrated Autonomous Underwater Operations*. IFAC-PapersOnLine*,* 48**,** 107-118.
51. SØRENSEN, A. J., SKJETNE, R., BØ, T. I., MIYAZAKI, M. R., JOHANSEN, T. A., UTNE, I. B. & PEDERSEN, E. 2017. *Toward Safer, Smarter, and Greener Ships: Using Hybrid Marine Power Plants*. IEEE Electrification Magazine, 5**,** 68-73.
52. SPOUGE, J. 2004. *Review of methods for demonstrating redundancy in dynamic positioning systems for the offshore industry*. Health & Safety Executive.
53. UTNE, I. B. & SCHJØLBERG, I. 2014. *A Systematic Approach to Risk Assessment: Focusing on Autonomous Underwater Vehicles and Operations in Arctic Areas*. In ASME 2014 33rd International Conference on Ocean, Offshore and Arctic Engineering (pp. V010T07A026-V010T07A026). American Society of Mechanical Engineers.
54. VALDEZ-BANDA, O. A., KUJALA, P., GOERLANDT, F., BERGSTRÖM, M., AHOLA, M., VAN GELDER, P. H. A. J. M., & SONNINEN, S. 2018. *The need for systematic and systemic safety management for autonomous vessels*. Marine Design XIII, (June).
55. WILLIAMS, A. D. 2015. *Beyond a series of security nets: applying STAMP & STPA to port security*. Journal of Transportation Security*,* 8**,** 139-157.
56. YOUNG, W. & NANCY, L. 2013. *Systems thinking for safety and security*. Annual Computer Security Applications Conference. ACM.
57. ZAVE, P. 1997. *Classification of Research Efforts in Requirements Engineering*. ACM Comput. Surv.*,* 29**,** 315-321.

