A?
Aalto University

Development of functional safety requirements for DP-driven servicing of wind turbines

Romanas Puisa[1,*], Victor Bolbot[1] and Ivar Ihle[2]
[1] Maritime Safety Research Centre, University of Strathclyde, UK
[2] Kongsberg Maritime, Norway

ABSTRACT

The adage "prevention is better than cure" is at the heart of safety principles. However, effective accident prevention is challenging in complex, highly automated systems such as modern DP-driven vessels, which are supposed to safely transfer technicians in often unfavourable environmental conditions. FMEA analysis, which is required for DP-driven vessels, is helpful to build-in a necessary level of redundancy and thereby mitigate consequences of failures, but not particularly helpful to inform preventive measures, not least against functional glitches in controlling software. In this paper we develop a set of functional safety requirements which are aimed at prevention of causal factors behind drift-off, drive-off and other hazardous scenarios. For this purpose, we use a systemic hazard analysis by STPA, which delivers both failure and interaction-based (reliable-but-unsafe) scenarios. The functional requirements cover both design and operational (human element related) requirements, which are then ranked based on our proposed heuristic. The ranking is not predicated on statistics or expert option but instead it is proportional to the number of hazardous scenarios a requirement protects against, hence indicating the relative importance of the requirement. The paper also summarises the suggested areas of safety improvement for DP-driven vessels.

Keywords: windfarm; wind turbine; dynamic positioning; service offshore vessel; technician transfer

1. INTRODUCTION

1.1 SERVICE OFFSHORE VESSELS

Offshore wind-framing is becoming a major source of renewable energy in many countries. As wind farms are moving further offshore, significant innovations in the infrastructure and services are required to maintain the judicious trend. One of such innovations is the specialised service vessels, or service offshore vessels (SOVs), which are offering new logistical concepts for servicing windfarms further offshore. They enable an extended stay of technicians (typically for two weeks) in the vicinity of a windfarm, thereby replacing the logistical concept of technician transfer from shore. The latter becomes unreasonable due to prolonged sailing times and increased risk of seasickness. SOVs, which are typically around 90 meters in length, can also endure more severe environmental conditions and offer a wide array of services. They are smart ships (highly automated), hosting dozens of technicians, heavy equipment and means of its handling. SOVs are also complex systems with many components (some subsystems are partly autonomous) and layers of communication between them.

---

[*] Corresponding author: +44 141 548 32 45 and r.puisa@strath.ac.uk

There are various ways of how the SOV can be utilised, and depends on specific circumstances (current and future) of a windfarm. In some cases, the SOV can be the only vessel at a windfarm to transfer technicians and equipment. In others, it can be part of a bigger fleet of vessels of various sizes and functions; a SOV would normally interact with all players in the fleet. Such a fleet, for instance, can comprise a SOV, daughter crafts, and a floatel (floating hotel). The latter is well suited for technicians and crew to be resting on undisturbed, when the other vessels are serving turbines 24/7. Daughter crafts (DCs) are medium size boats (under 20 meters) which are carried by the SOV and used to transport lighter equipment to turbines in moderate environmental conditions (< 1.8m significant wave height). DCs are loaded with technicians and launched from a SOV deck by some davit system (typically 3-5 times per day) and then recover (lift up) DCs from the water. SOVs would also have a sophisticated system for transferring technicians and equipment to and from a turbine. It is normally a motion-compensated (3 or 6 DoF) gangway which allows for the safest (based on experience so far) and time-efficient (within 5 minutes) transfer.

Regardless a logistical concept selected for a given windfarm, there are a number of functional requirements that a SOV has to fulfil. One of them is station keeping, i.e. the ability to maintain position and heading within their tolerable ranges and for an extended period of time under all operational conditions. Another is the ability to strictly follow a predefined trajectory along waypoints. These two functions are needed for both productivity (the number of turbines serviced per unit of time) and safety (prevention of injury and death among crew and technicians). The key system that provides these functions is the *dynamic positioning system* (DP system). The DP system is the object of this paper.

Figure 1: Operation modes when DP system is used (courtesy of Kongsberg Maritime / fmr Rolls-Royce Marine)

The DP system is, hence, involved in multiple operational modes of a SOV (cf. Figure 1). That is, when the vessel is transiting from shore to a windfarm, resting (night time) with people onboard, manoeuvring between turbines, and interfacing with turbines or daughter crafts. These modes of operation are safety critical and there are different safety hazards to watch for. For instance, during a transit or manoeuvring, the vessel might collide with turbines or other vessels, e.g. when the vessel deviates from a correct trajectory or inadequately performs collision avoidance. This can happen even in the area of a windfarm where fishing and other vessels are allowed to enter, as the case in the UK and other nation states. The loss of position or heading due to drift-off or drive-off scenarios are primary hazards during the resting and interfacing modes. Drift-off is a situation of the vessel drifting away after a loss of thruster power, whereas drive-off happens when the vessel is being pushed away by excessive thruster force.

1.2 SAFETY ASSURANCE AND ITS DEFICIENCIES

These safety hazards are normally pre-empted by ensuring a necessary level of reliability of station (position and heading) and trajectory keeping functions. Reliability of critical sub-systems and components is achieved through their redundancy. The vessel can operate at a different level of reliability (aka DP-equipment class (IMO, 1994)), depending on the safety criticality of a current mode of operation. For instance, DP-equipment class 1 (DP1) does not require redundancy and would normally be used when the vessel is resting, transiting and manoeuvring within so-called safe zones. In turn, DP2 and DP3 would be used in other operational modes where station keeping is key, e.g. technician transfer to or from a turbine. Therefore, DP2 and DP3 require redundancy against single failures of active and statics components such as generators, thrusters, valves, cables etc. Such single failures also include inadvertent acts by the people onboard the vessel. Currently, the main design and verification method of sufficient redundancy is the failure mode and effect analysis (FMEA) (DNVGL, 2015; IMCA, 2015). Other operational hazards, including those occurring when the vessel is in DP mode, are essentially left to be "managed by vessel operators as part of their safety management system." (IMCA, 2015).

However, although this approach to achieving safety is necessary, it is insufficient in several aspects. Firstly, ensuring reliability of both technology and people does not guarantee safety in complex systems, and can even be iatrogenic (Besnard & Hollnagel, 2014; N. G. Leveson, 2011). Complex systems feature *complex* interactions between system components, i.e. "the interactions in an unexpected sequence" (Perrow, 1984, p. 78), and accident can occur because of uncontrolled interactions of otherwise healthy components (Tiusanen, 2017, p. 464). Example interactions occur when one component is using another component when it should not or how it should not, i.e. typical cases of mode confusion. As these interactions within the entire system, safety is a system but not a component property. A related issue is that FMEA is used in a bottom-up manner, i.e. it attempts to identify the effect of a component failure on system safety. This is contrary to the notion that safety is a system property. Consequently, FMEA becomes also insufficient, for it is fundamentally biased towards accident scenarios caused by component failures and discounts those caused by dysfunctional interactions, i.e. system design errors. Secondly, one cannot foresee all interactions (and effects thereof) in complex systems, and hence a safety analyst should focus on improving control of component interactions at the functional level, as opposed to physical level where FMEA would normally operate at. Thirdly, FMEA would also misinterpret the contribution of people and software to accident scenarios (Victor Bolbot et al., 2018), for neither people nor software can credibly be said to fail rather than merely following wrong instructions (Dekker, 2014; N. G. Leveson, 1995).

1.3 CONTRIBUTION

Given these deficiencies of the current approach to safety of DP-driven vessels, we applied an alternative one. It is based on the method of systems theoretic process analysis (STPA) (N. Leveson, 2011; N. Leveson & Thomas, 2018). The method allowed addressing the highlighted deficiencies of failure-based analysis by FMEA and end up with functional safety requirements, which can be used by both system designers (e.g., software developers and integrators) and operators as part of their safety management systems. STPA is a hazard analysis method and it, hence, targets the initial phase of risk assessment, namely the hazard identification and analysis (ISO 31000, IEC/ISO 31010). The paper explains how we performed the STPA analysis of the DP system within various modes of SOV operation (cf. Figure 1), specifically focusing on hazards, analysis process, development of functional requirements, and result communication.

The latter conventionally requires to quantitatively rank individual scenarios identified through hazard analysis, essentially following the bottom-up approach. This was found especially challenging, given that the information about individual scenarios is scant (unreliable) or absent. We, hence, developed a heuristic to bypass this difficulty: instead of scenarios (pathways to system hazards), functional requirements against these scenarios were ranked. The used approach is congruent with the systems thinking that underpins STPA.

STPA has been applied to DP-driven vessels before, e.g. (Abrecht & Leveson, 2016; Rokseth et al., 2017). However, the analysis presented in this paper addresses different operational context and modes of operation (e.g., SOV interfacing with a turbine), and covers scenarios excusive to SOV servicing of windfarms. The paper does not explain the STPA method and expects the reader to be conversant with it. The unfamiliar reader is referred to the STPA handbook (N. Leveson & Thomas, 2018).

The paper is organised in two parts. The first part explains the assumptions behind the hazard analysis by STPA. Essentially, it explains what has been done, how and why. The second part summaries the analysis results in terms of high-level requirements, and concludes the paper.

2 ANALYSIS ASSUMPTIONS

This section covers essential assumptions behind the hazard analysis process by STPA. These assumptions concern about the system analysed, its objectives and hazards, generation of hazardous scenarios and corresponding functional requirements for their prevention and mitigation. The adopted approached for ranking and validation of the requirements is also discussed in this section.

2.1 SYSTEM AND ITS HAZARDS

As explained in the introduction an SOV is a highly-automated and multifunctional vessel. The DP-system is used in various, fairly mutually exclusive, modes of SOV operation and interaction with other objects in a windfarm (cf. Figure 1). The overall system of such interactions is shown in Figure 2. The analysis covered the five interactions whose safety is affected by the DP system. These interactions are of physical contact (e.g., SOV and turbine), communication via radio (e.g., SOV and shore, turbine and shore), and sensory (distance, visual, and audio) by installed sensors and people. Other interactions at the system level (i.e. the links between the DC and turbine or other ships) were not analysed.
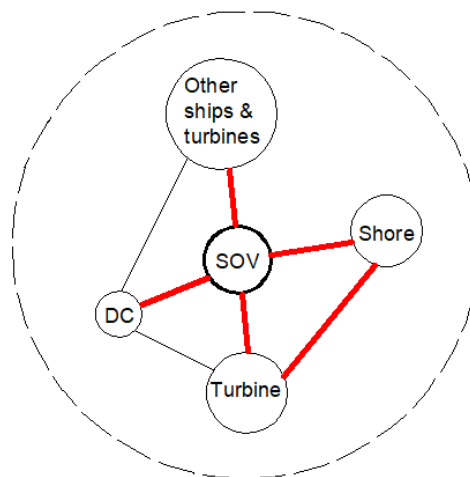

Figure 2: System components and system boundary

Figure 3 shows a simplified version of hierarchical control diagram with the DP control system involved. The human operator (HO) acts as the top controller and there are essentially four modes of interaction with the DP system:
1. DP system is in auto mode. DP autonomously achieves position, heading, or trajectory setpoints, whereas the role of HO is only supervisory with the ability to intervene when required. DP can also automatically switch thrusters to manual control by levers if failure or other anomalies are detected.

2. DP system in joystick mode. HO can control certain vessel axes (sway, surge or yaw) with DP controlling others. DP can also switch thrusters to manual control as described above, in turn HO can ask DP to take over control of manually controlled axes.
3. DP system controls some axes only. HO uses manual levers to control specific thrusters.
4. DP system is not controlling thrusters and it is either in standby or disabled mode. HO controls thrusters by manual levers.
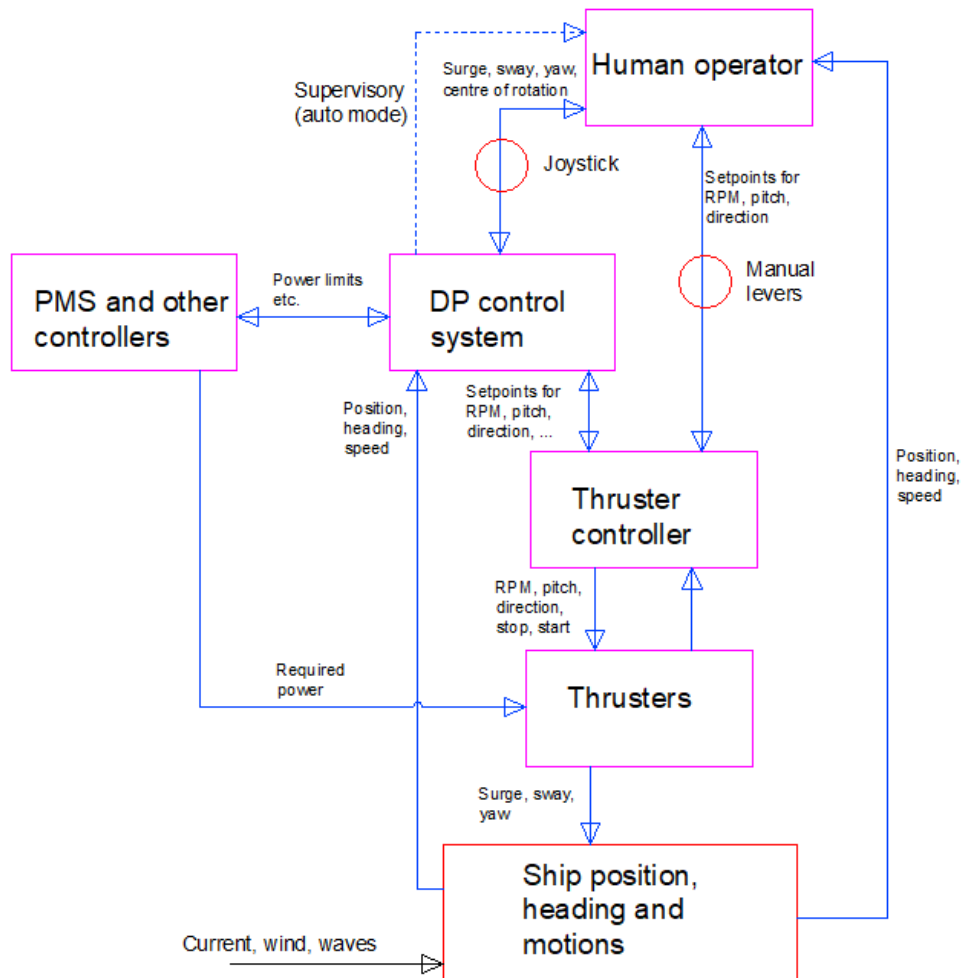

Figure 3: High-level representation of DP control and other systems (only a part of control and feedback information is displayed; some control and feedback channels are joined for simplicity)

During the transit mode, the SOV can either be in auto pilot (i.e., DP controls thrusters by following waypoints) or manual (joystick or levers). During manoeuvring between turbines (incl. turbine approach and departure), all axes of the SOV would normally be controlled by joystick. However, an autonomous manoeuvring would also be possible on novel vessels, when the SOV would autonomously approach a turbine, unload/load technicians and equipment via a gangway, and depart. In this case, the DP system will need to have this function. During interfacing with a turbine or DC, the SOV is supposed to keep station (position and heading) and this is usually done by the DP system being in auto mode (i.e., controlling all axes).

The control diagram in Figure 3 also shows other controllers such as the power management system (PMS). The interactions between these systems were included in the presented analysis, however PMS hierarchy and other systems were analysed in a separate study also presented in this conference (V. Bolbot et al., 2019).

Once the system has been defined, the next step is to formulate accidents (undesirable losses) and system-level hazards (how these losses can occur). The used rule of thumb, when formulating accidents and system hazards, was that accidents would correspond to undesirable deviations from or disturbances to the prime system objective (this formulation agrees with the definition of risk in ISO 31000), whereas hazards would essentially correspond to violated constraints which are necessary to achieve the objective. For instance, the prime system objective is to safely transfer technicians and equipment in minimal time (or minimal fuel consumption rate) and across a range of prescribed environmental conditions. Requirements and constraints to achieve this objective correspond to availability of adequate capacity of engineering systems (e.g., DP, davit) and adequate interactions between technology and people. Specific violations (or disregard) of such requirements and constraints, would allow formulating the hazards such as drifting off or driven off the position or hearing. Thus, in our case the accidents in question are: (A1) Injuries or loss of life, (A2) damage or loss of ship or other assets (daughter craft, gangway, davit system, or turbine). Table 1 list system hazards considered in various modes of operation. Note, only hazards related to the DP system and the interaction between DP and HO are shown, whereas other hazards (e.g., the gangway is retracted while in use by technicians) were also considered but are outside the scope of this paper. Some of the listed hazards were informed by current safe rules and recommendations such as IMO COLREGS (safe navigation), IMCA MSF (safe operation of DP, (IMCA, 2015)), etc.

Table 1 System hazards

Mode of operation	System hazards
Transit	H1: Sailing and stopping (crash stop) within a distance appropriate (minimal safe distance) to the prevailing circumstances and conditions (other ship, turbine etc.) is not achieved. H2: Ship course does not change promptly to avoid collision (astern, forward, sway, yaw). H3: Large and observable alteration of course are not achieved (as opposed to small alterations).
Manoeuvring between turbines (incl. turbine approach and departure)	H1 H4: Required course cannot be maintained for predefined time (on autopilot / DP / manual).
Rest	H5: Position and/or heading is not maintained (drive-off, drift-off) within the predefined ranges before an operation is completed. H6: Station keeping capability does not match the operational requirements of the vessel.
Interface with turbine	H5, H6
Interface with daughter craft	H5, H6

The control diagram in Figure 3 was analysed by considering four separate loops: HO-joystick-DP, HO-levers-Thruster Controller, DP-Thruster Controller, Thruster Controller-Thrusters. The system hazards were decomposed into loop-related sub-hazards to facilitate the local analysis. For instance, the loop Thruster Controller-Thrusters had the following sub-hazards:

- H5.1: Setpoints are not achieved in required time.
- H5.2: Setpoints are not maintained within alarm limit.
- H5.3: Communication between thruster and remote controller is not maintained at required frequency.
- H5.3: Loading of el. motors and/or diesel engines exceeds the limits.

Table 2 summarises control actions per control loop. The list of analysed control actions is helpful to grasp the scope and detail of the analysis.

Table 2 Summary of control actions per control loop

Control loop	Control actions
HO-joystick-DP	• Update setpoint (sway, surge, yaw, or all) • Change joystick device gain for manual heading/position/rotation and thrust bias (low, medium, high) • Change axis control mode (auto, joystick, no control/levers) • Change centre of rotation • Change DP control mode (relaxed, normal) • Change vessel control mode (manual/auto position, auto/manual sway, auto/manual surge, manual/auto heading, trajectory) • Change vessel draught in operation monitor panel (for auto heading) • Change alarm/warning limits (4/5m for default warning/alarm) • Wait until DP settles (20 min) • Release to Manual • Change operational objective/task • Change IMO DP class
HO-levers-Thruster Controller	• Start thruster (make thruster ready to use; lever in command) • Update setpoint (RPM, pitch, direction) • Enable/disable thruster • Stop/shutdown thruster • Control transfer (transfer command between bridge and engine control room) • Command transfer (take command from other controllers of thruster. Make the lever in command)
DP-Thruster Controller	• Update setpoint for individual thrusters or thruster group (RPM, pitch, direction, moment, timing/acceleration) • Enable thrusters • Disable thrusters • Take control of axis • Release control of axis
Thruster Controller-Thrusters	• Acknowledge communication signals from remote control system • Achieve setpoint (RPM, pitch, direction) • Maintain load control (azimuth thrust controllers)

2.2 HAZARDOUS SCENARIOS

We used the STPA process described in (N. Leveson & Thomas, 2018) to come up with hazardous scenarios, i.e. combinations of unsafe control actions (UCAs) and their causal factors (CFs). The identification of UCAs and CFs was done manually, and with the guidance of the conventional modes and guidewords for UCAs (e.g., control action is not provided, wrong provided, provided too late, etc.) and CFs (e.g., inconsistent process model, out-of-range disturbances etc.); see (N. Leveson & Thomas, 2018).

Formulation of potential CFs is generally more challenging than of UCAs. It is particularly strenuous when it comes to human controllers, as opposed to automated counterparts. CFs for the latter were addressed by answering the following guiding questions:

- What process model (PM) would cause a given UCA?
- How such a PM would be created?
- How PM should be interpreted to cause the UCA?
- How the control action should be executed to cause UCA?

For human controllers (e.g., human operator controlling the vessel position by manual levers), similar questions could be asked (although replacing PM by the mental model). Additionally, we used a list of further guidewords grouped into four phases of decision/action making on the part of human: observing/receiving information, interpreting and updating the mental model, deciding on specific action, and executing action. Some of the generic causal scenarios of how each group can be undermined are shown in Table 3; comments on these scenarios are found in (Bainbridge, 1983; Hollnagel, 2017; Lee, 2008; N. Leveson, 2011; N. G. Leveson, 1995; Sarter et al., 1997). These generic scenarios can be regarded as templates for specific causal factors which reflect the context at hand.

Table 3 Sample guidewords for formulating causal factors for human controllers

Function	How this function can be undermined
1. Observing / receiving	- Clarity of information (display design, visual destructions etc.): information is unnoticed, noticed too late or misunderstood - Low alertness, monotonicity of process: information is unnoticed or noticed too late - Graceful failure of automation: information is unnoticed or noticed too late - Supra commands (missing, wrong, untimely): no relevant and timely information from top controllers - Operator is unskilled and over loaded: automation requires more skilful and less loaded operator for effective reaction in emergencies - Controlled software/process does not provide adequate feedback on operator errors, who hence does not notice them or notice too later (in life such feedback often instant and clear) - Tunnel vision (extreme fear or distress, most often in the context of a panic attack, sleep deprivation): information is incomplete or wrong - Control panel displays change unexpectedly and to a different, less familiar one / operator is used to some display, but it changes to different one in emergency: information is unnoticed, ignored or misinterpreted - Uncertain default settings which do not change with operational modes (difficult to know when the settings are hazardous): crucial information is ignored, misinterpreted
2. Interpreting and updating mental model	- Mode confusion when modes change automatically/autonomously, seamlessly, without warning: crucial information is unnoticed, misinterpreted - Operator does not know what task the computer is dealing with and how (unclear allocation of responsibilities): information is misinterpreted, ignored - Nondeterministic automation, irregular, unpredictable behaviour: information is misinterpreted or ignored (e.g. assuming a fault or outlier) - Complacency, overreliance on automation (when automation makes no sense): information is misinterpreted or ignored - Training, experience: information is unnoticed, misinterpreted or ignored (e.g. unfamiliar factors are ignored)

Function	How this function can be undermined
	• Working storage, i.e. limited (only local) information is available just after take-over (i.e. after taking over the operator has limited info about the system state): information is misinterpreted
3. Deciding on action	• Cost-benefit trade-off (e.g., wrongly thinks it is not beneficial to do, or beneficial to do): necessary action may not be taken or delayed • Safety criticality (e.g., operator thinks it is not safety critical): necessary action is not taken or delayed • Confused accountability, responsibility with other controllers: necessary action is not taken or delayed, wrong action is taken • Unrepaired/partly repaired fault (by some other controller) is unexpectedly returned to operator (e.g., for manual control): relevant action is not found in time, action is delayed
4. Executing action	• Procrastination: execution is postponed (e.g., waiting on favourable weather) • Due to irresponsiveness etc., operator assumes a failure in automation: action is delayed, action is inadequate

2.3 FUNCTIONAL REQUIREMENTS

A function is a useful capability provided by one or more components of a system. Functional requirements describe what the system *must do* (or, formally, 'shall do'), rather than how it must do it (Young, 2004). The latter is addressed by non-functional requirements. Functional safety requirements (incl. safety constraints at the functional level) define functions for safety barriers (or defences) to be put in place against specific hazardous scenarios. Each requirement should have a rationale, type, priority and other information to facilitate decision making by designers or operators (see for instance ISO/IEC/IEEE 29148:2018). In our work, the rationale corresponded to hazardous scenarios—combinations of UCAs, CFs and hazards—and other contextual information such as corresponding control actions, controlled processes etc.

Causal factors

The env. conditions conditions have significantly changed (e.g., wind changes to the opposite direction) which makes the previously used the joystick device gain/thruster bias too aggressive/sluggish.

Unsafe control action

Operator orders too high/low thrust, leading to large and sudden overshoot/undershoot

Hazardous states

Vessel control does not reflect environmental conditions and other pertinent factors

CF1
CF2
CF...
UCA
H1
H2
H...

Prevention requirements
Control panel shall inform operator of how significant changes in env. conditions might affect the vessel inertia when axis is controlled by joystick
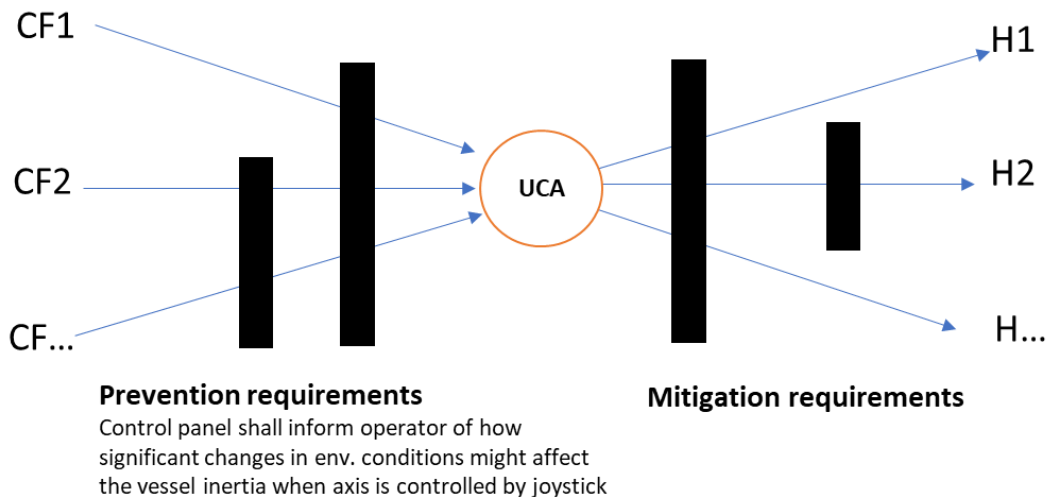
Mitigation requirements

Figure 4: Prevention and mitigation functional requirements (examples are provided in small print)

The derived requirements were classified into UCA prevention and mitigation requirements as illustrated in Figure 4. Prevention requirements would directly aim at causal factors, thus preventing UCAs in the first place. Mitigation requirements would react to the realisation of the UCAs, so they do not lead to hazards. Clearly, the adopted classification is subjective and relative to what we put in the middle of the bowtie. For instance, if a hazard (some hazardous system state) is in the centre, then both requirements become preventive. Both set of requirements were further classified into design and operational.

As the hazard analysis covered four control loops (cf. Section 4), requirements were primarily aimed at design and operation of controllers. Some controllers (e.g., human operator) were involved in several loops and hence contexts. That allowed to derive additional requirements for such controllers. As the number of requirements was significant, were ranked according to a heuristic described in the next section.

2.4 REQUIREMENT RANKING

A hazard analysis by STPA would normally end up with many hazardous scenarios—in our case hundreds of them—with similar number of requirements (typically smaller, for some requirements cover multiple scenarios). The myriad of requirements is obviously unconducive to the communication of hazard analysis results. Therefore, some quantitative ranking of requirements is usually adopted to alleviate this problem. Ranks would normally reflect risk-related information attached to corresponding scenarios, e.g., scenario likelihood, consequences or both.

However, the likelihood information was missing in our case. The uncertainty with scenario likelihood (or probability) is common, especially for non-standard and new technology. We were also reluctant about eliciting subjective estimates from domain experts, given how biased and unreliable outcomes could have been, e.g. (Skjong & Wentworth, 2001). The situation with scenario consequences was much simpler, for the identified scenarios led to predefined hazards and corresponding accidents.

There are, however, a number of conceptual issues with quantification of hazardous scenarios. Firstly, there is no evidence that quantification per sei improves safety (e.g., by directing resources to high risk scenarios) (Rae et al., 2012). Inaccurate estimates of associated likelihoods can be precarious, equally as navigating by a map of a wrong city. It is hence better to have no guidance at all, than the wrong one. Secondly, safety is an emergent system property, i.e. the system is not the sum of its components (Rasmussen, 1997). Hence, the assumption is that—given the emergent property of safety—there is no need to quantify individual scenarios leading to system hazards, in fact it would be incongruent with systems thinking. Quantification should only be done to system hazards—based on experience (typically supported by statistics) or expert opinion—but not to component-level scenarios.
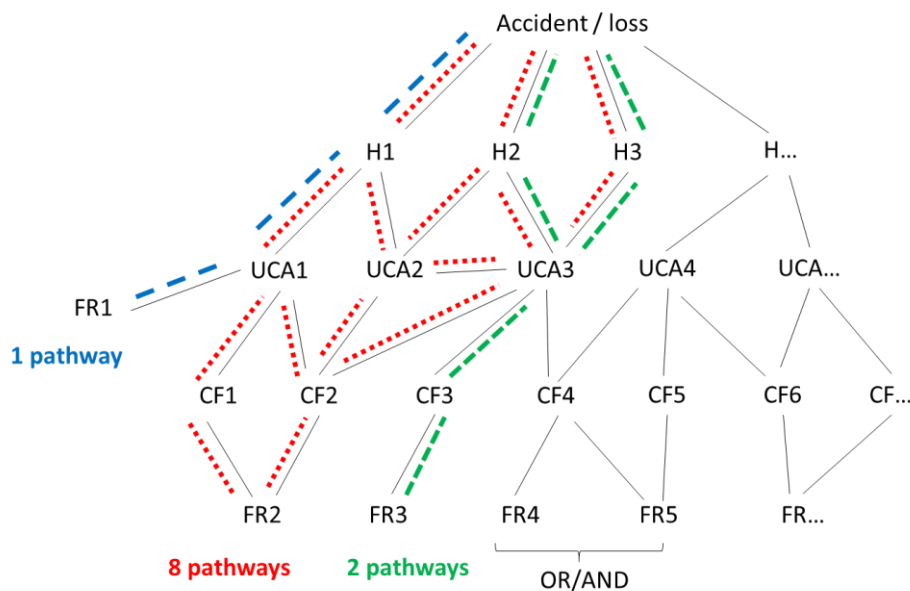
Figure 5: Accident pathways addressed by safety requirements

With the above in mind, we adopted a heuristic to rank the requirements, as opposed to hazardous scenarios directly. We took advantage of the available traceability between requirements and accidents, additionally factoring in the information on the type of requirements. Figure 5 shows a resultant tree of the hazard analysis by STPA. Functional requirements (FRs) address specific causal factors (CFs) or directly unsafe control actions (UCAs). In the latter case, the requirements would be of mitigation type (e.g., FR1). If a requirement is implemented, it blocks specific pathways to accidents in question. As shown in Figure 5, FR1 would blocks just one pathway, whereas FR2 and FR3 block 8 and 2 pathways respectively. Clearly, the importance of a requirement is proportional to the number of pathways it blocks. Note, there could be also a path from one UCA to another (e.g., UCA2 to UCA3) in the scenario tree. This path reflects the control hierarchy, i.e. UCA2 belong to a high lever controller which controls (or affects in some other way) a controller that issues UCA3. This result scenario tree is comprehensive.

In addition to the number of pathways to accident, which reflects the impact level of a requirement, the requirement type was factored in into the requirement rank. In this case, the requirement type corresponded to whether a requirement aims to prevent or mitigate a UCA. We followed the general principles compactly reflected in the adages: "prevention is better than cure" and "an ounce of prevention is worth a pound of cure". In other words, prevention of some unfavourable events such as UCAs is more effective than their mitigation; recall the hierarchy of control by HSE (Books, 1997) and risk control by NASA (Bahr, 2014, p 29). Other figures such as the difficulty to implement a requirement (as proxy for cost) can also be added, but they are not discussed in this paper.

The requirement rank was then calculated as follows:

$$\text{Rank} = \text{Impact} \times \text{Effectivness} \qquad\qquad (1)$$

Where the impact equals to the number of pathways counted on the result tree (cf. Figure 5), whereas the effectiveness equals 1 for mitigation and 2 for prevention requirements. There is, however, one caveat to the ranking of this kind. Requirements that receive low ranks can, in principle, be equally safety critical as those of high rank. Hence, a low rank should not be the basis for discarding the requirement, but rather as an indicator that the requirement is lower in the review priority list.

Note that some requirements can be complementary (AND) or redundant (OR), as indicated in Figure 5. This information was not factored in the ranking, and is meant to be used during the later stages when requirements are fulfilled by specific safety barriers, i.e. design, operational or organisational measures.
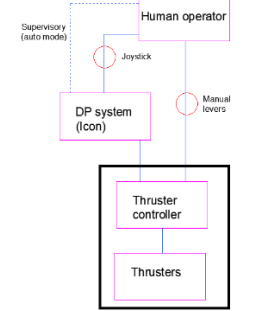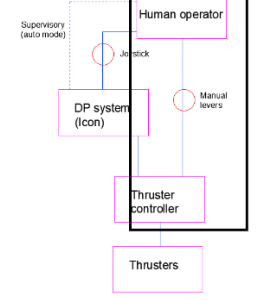
2.5 REQUIREMENT VALIDATION

Requirements validation was performed by designers (of DP and other control systems) and experts working in design approvals. The experts were asked to review the requirements (starting with high rank ones) and corresponding scenarios, and comment on their validity, i.e. if scenarios were possible (can happen) and requirements were realistic and sound. Consequently, only valid scenarios and requirements were retained. An analogous conservative approach for scenarios filtering is advocated by Leveson (N. Leveson, 2015).
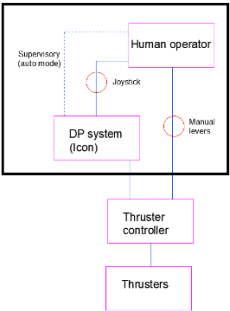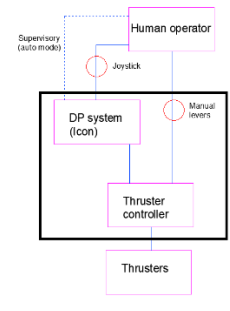
3 SUMMARY OF RESULTS

Table 4 contains sample requirements which scored highest ranks. Each requirement blocks dozens of hazardous scenarios behind vessel drift-off, drive-off and other situations. The requirements are predominantly preventive (i.e., target causal factors of UCAs) in the analysed control loops. Same requirements were derived in two control loops: FR3-5 are same as FR7-9, also FR6 is same to FR13. Consequently, these requirements have higher ranks than the others.

In summary, the functional requirements target inadequate feedback to the operator about system malfunction (and early precursors thereof) and healthy states, both of which are hazardous, as well as emergency states. In the latter case, the requirements imply the need for decision support in emergency. Some requirements such as FR19 echo the current requirements for the DP system.

Table 4 Sample requirements of high priority

Control loop (simplified versions of Figure 3)	Design requirements	Operational requirements
	1. Thrust control system shall be able to deal with external obstructions of thrusters (e.g., fishing nets, plastic waste)	2. Precautions shall be in place against manual setting of wrong load limits for el. motor and engines
	3. Indication shall be provided of malfunction criticality of thrusters (not just failed/not failed) 4. Warning of emergency situation shall be provided to operator 5. Assessment with and indication of env. effects on vessel's manoeuvrability shall be provided to operator	6. Operator shall have adequate conversancy with emergency procedures and recovery actions

Control loop (simplified versions of Figure 3)	Design requirements	Operational requirements
	7. Indication shall be provided of malfunction criticality of thrusters (not just failed/not failed) 8. Warning of emergency situation shall be provided to operator 9. Assessment with and indication of env. effects on vessel's manoeuvrability shall be provided to operator 10. Operator shall be advised with recover actions in emergency 11. Accurate visuals (using cameras etc.) of the relative vessel position/heading with respect to turbine, DC etc. shall be provided to operator	12. Timely and unambiguous communication of operational objectives to operator shall be provided 13. Operator shall have adequate conversancy with emergency procedures and recovery actions
	14. DP system shall get immediate awareness of all failure modes of thrusters/thruster controller 15. DP system shall check the entered (by operator) position/ heading/trajectory alarm limits against safety etc. criteria (i.e., sanity check) 16. DP system shall warn operator about inadequate alarm limits 17. DP system shall consider delays and irregularities in thruster signals 18. DP system shall notify operator about communication delays with thruster 19. DP system shall perform continuous assessment of the effect of environmental conditions on DP operability	20. Operator shall check the entered position /heading/trajectory alarm limits against safety etc. criteria (i.e., sanity check)

4 CONCLUSIONS

The paper has summarised a hazard analysis of a DP-driven vessel servicing windfarms which are located far offshore. The objective of the analysis was to come up with functional design and operational requirements to be used as input to a vessel design process, as well as to the development of a safety management system (SMS). The requirements were meant to be at the functional level (non-prescriptive), so designers could use them at early design stages and decide on specific safety measures that fulfil them. To this end, the hazard analysis was performed by the method of systems theoretic process analysis (STPA), which we found pertinent to achieve this objective.

The hazard analysis has focused on the DP system as it operates in various operational modes when vessel drift-off, drive-off and other hazards can happen. Hundreds of scenarios that can lead to such system hazards have been identified and used to derive functional safety requirements. The requirements were ranked by the proposed heuristic which takes advantage of the scenario tree and other aspects. The scenario tree allows to count the number of hazardous scenarios (component-level pathways to system hazards) a requirement protects against, hence indicating the relative importance of the requirement. In other words, the ranking is not predicated on scenario risk contribution, likelihood or other scenario-level information. And it is not because creditable likelihood information on hazardous scenarios in is absent in complex systems, but that quantifying individual

scenarios is incongruent with the systems thinking. Hence, the proposed ranking approach matches the systemic spirit of STPA.

The paper has then summarised and discussed design and operational requirements which received high ranks. Thus, adequate feedback (timely, accurate and complete) to the bridge operator was found to be indispensable to maintain safety during technician and equipment transfers by the SOV. And improvements should be firstly directed to providing adequate:

- Feedback to the bridge operator about system malfunctions and early precursors thereof.
- Feedback on DP settings that can become hazardous in certain modes.
- Feedback when the vessel enters emergency states.
- Feedback on current and unfolding environmental conditions, and their effect on the DP and vessel performance.
- Decision support in emergency.

There are a few caveats to the study. The paper has not discussed how the requirements can be implemented or achieved, given these are only functional requirements that define functions for safety barriers but not barriers themselves. Consequently, cost effectiveness analysis of corresponding safety barriers could not be considered. The paper has not provided a detailed comparison of the derived requirements against the current requirements for the DP systems, although some high priority requirements (cf. FR19 in Table 4) echo the existing safety rules; a detailed gap analysis will be the object of a follow-up study.

ACKNOWLEDGEMENTS

REFERENCES

Abrecht, B., & Leveson, N. (2016). Systems theoretic process analysis (STPA) of an offshore supply vessel dynamic positioning system. *Massachusetts Institute of Technology, Cambridge, MA*.

Bahr, N. J. (2014). *System safety engineering and risk assessment: a practical approach*: CRC Press.

Bainbridge, L. (1983). Ironies of automation. In *Analysis, design and evaluation of man–machine systems* (pp. 129-135): Elsevier.

Besnard, D., & Hollnagel, E. (2014). I want to believe: some myths about the management of industrial safety. *Cognition, Technology & Work, 16*(1), 13-23. doi:10.1007/s10111-012-0237-4

Bolbot, V., Puisa, R., Theotokatos, G., Boulougouris, E., & Vassalos, D. (2019). *A comparative safety assessment for Alternate Current, Direct Current and Direct Current with hybrid supply power systems in windfarm Service Operation Vessel using System-Theoretic Process Analysis*. Paper presented at the The 7th edition of the European STAMP Workshop and Conference (ESWC), Helsinki.

Bolbot, V., Theotokatos, G., Bujorianu, M. L., Boulougouris, E., & Vassalos, D. (2018). Vulnerabilities and safety assurance methods in Cyber-Physical Systems: A comprehensive review. *Reliability Engineering & System Safety*.

Books, H. (1997). Successful health and safety management. *HS (G)*.

Dekker, S. (2014). *The field guide to understanding'human error'*: Ashgate Publishing, Ltd.

---

† www.nexus-project.eu

DNVGL. (2015). Dynamic positioning vessel design philosophy guidelines. Recommended practice (DNVGL-RP-E306). In.

Hollnagel, E. (2017). *The ETTO principle: efficiency-thoroughness trade-off: why things that go right sometimes go wrong*: CRC Press.

IMCA. (2015). International Guidelines for The Safe Operation of Dynamically Positioned Offshore Supply Vessels (182 MSF Rev. 2). In.

IMO. (1994). Guidelines for vessels with dynamic positioning systems (IMO MSC Circular 645). In. London.

Lee, J. D. (2008). Review of a pivotal Human Factors article:"Humans and automation: use, misuse, disuse, abuse". *Human Factors, 50*(3), 404-410.

Leveson, N. (2011). *Engineering a safer world: Systems thinking applied to safety*: MIT press.

Leveson, N. (2015). A systems approach to risk management through leading safety indicators. *Reliability Engineering & System Safety, 136*, 17-34.

Leveson, N., & Thomas, J. (2018). *STPA Handbook*. Retrieved from http://psas.scripts.mit.edu/home/materials/

Leveson, N. G. (1995). Safeware. *System Safety and Computers. Addison Wesley*.

Leveson, N. G. (2011). Applying systems thinking to analyze and learn from events. *Safety Science, 49*(1), 55-64.

Perrow, C. (1984). Normal accidents: Living with high risk systems. In: New York: Basic Books.

Rae, A., McDermid, J., & Alexander, R. (2012). The science and superstition of quantitative risk assessment. *Journal of Systems Safety, 48*(4), 28.

Rasmussen, J. (1997). Risk management in a dynamic society: a modelling problem. *Safety Science, 27*(2), 183-213.

Rokseth, B., Utne, I. B., & Vinnem, J. E. (2017). A systems approach to risk analysis of maritime operations. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, 231*(1), 53-68.

Sarter, N. B., Woods, D. D., & Billings, C. E. (1997). Automation surprises. *Handbook of human factors and ergonomics, 2*, 1926-1943.

Skjong, R., & Wentworth, B. H. (2001). *Expert judgment and risk perception.* Paper presented at the The Eleventh International Offshore and Polar Engineering Conference.

Tiusanen, R. (2017). Qualitative Risk Analysis. *Handbook of Safety Principles*, 463-492.

Young, R. R. (2004). *The requirements engineering handbook*: Artech House.