A Systems Approach to Modelling Safe Behaviour of Maritime Control Systems Using the Composition, Environment, Structure, and Mechanisms (CESM) Metamodel

Odd Ivar Haugen
Group Research and Development department, DNV AS
Trondheim, NORWAY
e-mail: odd.ivar.haugen@dnv.com

***Abstract*—Society increasingly relies on complex systems whose behaviour is determined, not by the properties of each part, but by the interaction between them. The behaviour of such systems is emergent. Modelling emergent system behaviour requires a systems approach that incorporates the necessary concepts that are capable of determining such behaviour. The CESM metamodel (Composition, Environment, Structure, Mechanisms) is a model of system models. A set of system models needs to address the elements of CESM at different levels of abstraction to be able to model the behaviour of a complex system. Modern ships contain numerous sophisticated equipment, often accompanied by a local safety system to protect their integrity. These control systems are then connected into a larger integrated system in order to achieve the ship's objective or mission. The integrated system becomes, what is commonly known as, a system of systems which can be termed a complex system. Examples of such complex systems are the ship's dynamic positioning system and the power management system. Three ship accidents are provided as examples of how system complexity may contribute to accidents. Then, the three accidents are discussed in terms of how the Multi-Level/Multi-Model Safety Analysis might catch scenarios such as those leading to the accidents described.**

Keywords-emergent properties; cesm metamodel; multi-level/multi-model safety analysis; safety; system complexity; systems approach.

I. Introduction

The number of ship control systems has increased tremendously in the last 25 years. There are dedicated control systems related to power generation, such as controlling switchboard circuit breakers, stopping and starting generators, and reducing load to avoid blackouts. Moreover, fire and gas systems may start deluge systems, leading to the automatic stop of power generation equipment. Dynamic Position Systems (DPS) rely upon the fact that there is adequate thrust available to maintain position. Local dedicated thruster control systems control pitch (Angle of the thruster blade) and the RPM (Revolutions Per Minute of the thruster blade) of the thruster, which is part of the DPS. There are automatic shut-down systems whose sole purpose is to protect the equipment.

A more and more prevailing challenge is to gain oversight over how the control systems interact and how an action taken by one local control/safety system affects other control systems. The control system can be seen as located in a hierarchy of control at different levels of authority and responsibility. An action taken by one local safety system may inadvertently shut down equipment necessary for another control system to work as intended.

Lately, there have been accidents outside the Norwegian coast where, at least one of them, in a worst-case scenario, could develop into the worst maritime catastrophe in modern history, on par with the sinking of Titanic.

Today, methods for safety analysis and assurance of maritime systems have not kept up to the task of dealing with increased system complexity due to increased tight integration between the control systems.

This paper suggests a framework for system analysis to adequately deal with increased system complexity, using maritime control systems and maritime accidents as a background and examples.

The remainder of this paper is structured as follows. Section (II) "A few recent maritime accidents on the Norwegian Coast" briefly describe three recent maritime accidents on the Norwegian coast, which serve to motivate our discussion on increased system complexity. In Section (III) "Commonalities between the accidents", we examine the common factors among these accidents, highlighting the role of complex interactions among control and safety systems. Section (IV) "Reductionism versus systems thinking" discusses reductionism and explains why it is insufficient for ensuring safety in modern maritime systems. Section (V) "The Systems Approach to handle system complexity and emergence" introduces the CESM metamodel and explains how its four elements—Composition, Environment, Structure, and Mechanisms—offer a systemic view of system-level behaviour. Section (VI) "System analysis" outlines a systematic analysis approach based on Multi-Level, Multi-Model Safety Analysis (ML/MM-SA). In Section (VII) "Application of the method", we demonstrate how this method might have captured the accident scenarios described earlier. Finally, Section (VIII) "Conclusion" concludes and provides avenues for future work.

II. A few recent maritime accidents on the Norwegian Coast

To set the stage, this section will go through three recent accidents on the Norwegian Coast. The actual loss in each accident differs, and the amount of information from the accident investigation also varies. The motivation is not to question the official stated direct cause of the accident. Indeed, the cause of one of the accidents is not known. Instead, we use these accidents to argue that system complexity could have been a contributing factor, even if this is not explicitly mentioned in the accident reports.

A. Vessel: Sjoborg

Sjoborg is a supply vessel that, at the time of the accident, operated as a Platform Supply Vessel (PSV) for the Norwegian energy company Equinor. Equinor is the operator of the Statfjord oil field, where one of the production platforms is Statfjord A [1]. Statfjord A is the world's largest Condeep (CONcrete DEEP water structure) production platform [2], with a weight of 290.000 tonnes and a storage capacity of 1.3 million barrels of oil. It is a fixed platform with a total height of 270 metres, standing on three concrete legs.

Sjoborg's power system is a hybrid [3], that is, a combination of diesel generators and battery power. This design introduces additional control systems related to the battery system compared to a more traditional system that is based exclusively on diesel generators.

A PSV carries goods and equipment to and from the platforms. In general, when such vessels load or discharge goods, they need to be stationary at a particular position in relation to the platform due to, for instance, the sea and weather conditions or the location of the cranes onboard the platform.

For a floating vessel to maintain its position, it uses Dynamic Positioning (DP). Simplified, a DP system maintains a fixed vessel position by providing thrust to counteract the environmental forces.

A vessel such as Sjoborg that operates on DP close to an offshore oil installation will typically be classified in accordance with the DP guideline published by the International Maritime Organization (IMO) - Maritime Safety Committee (MSC): IMO MSC.1/Circ.645 - Equipment class 2 [4]. For such vessels, loss of position shall not occur in the event of a single failure in any active component or system.

On 7 June 2019, while loading/discharging alongside Statfjord A, the control systems onboard Sjoborg initiated a power reduction in response to an event. This automatic power reduction resulted in a series of events that eventually resulted in the Sjoborg colliding with the platform [5].

The initial event led to a communication network failure in the blackout safety system; this led to the main switchboard frequency measurement being lost (the frequency was at this point not affected), which again led to the activation of the load reduction mode, which led to that all the power from all thrusters where reduced to 10%-15% of their maximum output, this led to a discrepancy between the DP systems's thruster RPM command signal and the feedback from the thrusters, which eventually led to that two thrusters where automatically shut down.

In the end, Sjoborg did not have enough power to counteract the environmental forces, drifted towards the platform, and eventually collided.

One of the Sjoborg crew was hit in the face by a diesel hose; fortunately, it did not result in a fatality, but under slightly different circumstances, it could have. Moreover, Sjoborg suffered material damage, and the lifeboats onboard Statfjord A were damaged. This led to the helicopter evacuation of 218 people from Statfjord A.

We see here that the analysis of the behaviour of the system did not capture how the different control systems interacted as a response to the initial event.

B. Vessel: MS Richard With

MS Richard With is one of the "Hurtigruten" vessels trafficking the Norwegian coastline, and it has a capacity of 590 people [6]. In 2022, the power system onboard MS Richard With was converted to a hybrid power system, that is, diesel generators and battery package [7].

On the sea trial, before going into ordinary operation, the ship grounded caused by a blackout in the power system [8]. As there was no public accident investigation, it is difficult to get information about the direct cause. The only known cause was "technical system failure" [9].

Luckily, the accident happened before the ship went into regular traffic along the Norwegian coast. The grounding only caused damage to the ship.

Although "technical system failure" does not provide much insight into what actually caused the blackout, it is worth noticing that this ship was also rebuilt to hybrid power, resulting in a number of additional control systems, just as on Sjoborg. We stress that we do not know the cause of this accident, so we do not conclude that the accident was related to increased complexity as a result of hybrid power. However, a hybrid power system will, in general, increase the complexity of the power system.

C. Vessel: Viking Sky

Viking Sky is a cruise ship equipped for 930 passengers [10]. The cruise ship is classified in accordance with IMO MSC.216, which includes the "Regulation 21 Casualty threshold, safe return to port and safe areas" [11]. Safe Return to Port (SRtP) requires that a vessel be able to return to port under its own propulsion after a casualty that does not exceed a certain threshold.

On the afternoon of 23 March 2019, with a total of 1374 people onboard, the ship experienced a total blackout and lost all propulsion while crossing Hustadvika at the coast of Norway during a heavy storm. The ship was pushed or drifted towards the reefs in Hustadvika. Hustadvika is a well-known area with difficult sailing conditions [12].

The direct cause of the blackout was a combination of low oil levels in all engine lubrication oil tanks and heavy rolling and pitching, causing the hose that is supposed to suck lubrication oil from the tanks to the engine to instead suck air, which again caused the lubrication oil pressure to drop, resulting that the engine safety system kicked in and stopped all engines [13]. The purpose of the engine safety system is to protect the engine against damage.

It was estimated by the accident report that the ship was about one ship length from the reefs when the crew managed to restart two of the engines after 39 minutes so that power was restored and they could get clear of the reefs. If the crew did not get to restart the engines in time, this could have developed into the worst maritime catastrophe in modern times [13]. In

the Titanic catastrophe, about 1500 people died [14], and in the fire and sinking of MS Estonia, 852 people died [15]. The Viking Sky accident could have caused as many people's lives as those two catastrophes.

IMO MSC.216 is not as strict as IMO MSC.1/Circ.645 for DP Equipment class 2, so there is no requirement that a blackout cannot occur. However, it requires that the power be restored in due time to avoid situations like this one, and it is based on the same fundamental principles such as redundancy and component reliability.

There is no discussion about the direct cause of the accident; that is indisputable. However, in the context of the discussion about the increased system complexity, and the many control systems, one could start to ask why the crew could not start the engines quicker than after more than 30 minutes when the situation was so critical. Indeed, in an interview with the Norwegian National Broadcaster, NRK, the pilot stated (translated to English from Norwegian): "I really missed a button that said override on it" [16].

This opens a number of (rhetorical) questions like: "Why can an engine safety controller be allowed to stop all engines at the same time and no one can prevent it"?, and "Who has the best oversight over the situation? The engine safety system, or the pilot on the bridge"?, and "What is more valuable? A couple of diesel engines, or 1374 human lives"?

These questions point to some interesting discussions, not only about the oil level in the tank, but also about what controller should have the highest authority, the human controller on the bridge, or a safety system whose sole purpose is to protect equipment. There might, of course, be good reasons for the design, and we are not going to provide design advice, but the question remains: who should control the "override button"?, and, should there even be an "override button"?

III. Commonalities between the accidents

All ships had redundant equipment and were certified in accordance with relevant IMO safety guidelines. In all cases, neither the equipment redundancy, nor the equipment reliability prevented the accidents from occurring. Both Sjoborg and MS Richard With, utilise a hybrid power system, which is known to create increased system complexity due to extra control and safety systems. These control systems need to interact in such a way that safety is maintained. In the case of Sjoborg and Viking Sky, a safety system completely defeated the redundancy philosophy.

The commonality between all accidents may be said to be a lack of understanding of the behaviour of the integrated control system, including the actions taken by different control systems and their associated authority. A reservation needs to be made for MS Richard With because of a lack of information.

IV. Reductionism versus systems thinking

The IMO system safety standards are based on redundancy and equipment reliability, that is, reductionism. Reductionism interprets the world as a pile of things [17] so the world can be understood by investigating these parts. This leads to system safety becoming a question about avoiding component and equipment failures by highly reliable components and/or the concept of component redundancy. However, as we saw in the previous examples, redundancy is not the "silver bullet" to safety in complex systems.

This view on safety is typically represented by using the method Failure Mode and Effect Analysis (FMEA) for safety analysis [4][11][18]. FMEA was invented as a reliability analysis, not a safety analysis [19][20]. Charles O. Miller, one of the founders of system safety, put this clearly: "distinguishing hazards from failures is implicit in understanding the difference between safety and reliability" [21].

While reductionism may have served some industries well in the past, where the safety principle is founded upon a dedicated safety function where there is one single action that brings the system into a predetermined single safe system state. This safety function is achieved by a controller that has the highest authority. Such systems are characterised as KISS (Keep It Simple, Stupid). These safety systems are found in the process industry, such as oil production. If a process gets too hot, or too high pressure, or some flow is too high or too low, the actions would often be to open or close a valve, or, by some means, shut down the process or flow. Typically, these actions can be summarised as removing energy from the system, which would bring the system into its single predefined safe state. The reliability of the components in the safety system may determine safety in such simple systems.

Recall what happened in the case of Sjoborg when the available power was removed from all thrusters, followed by a shutdown of thrusters 1 and 3. This action of removing energy may have brought the switchboard into its "safe" state, but it definitely did not bring the ship into a safe state. The same explanation can be applied to Viking Sky; the engine safety system brought the engine into its "safe" state; however, the lack of power to the ship propulsion system resulted in one ship length from potentially the worst maritime catastrophe in modern times.

The complexity of many of today's industrial safety-critical systems, including ship systems, requires a shift in how we understand safety. Safety is an emergent property [21] that cannot be fully understood through reductionism because the property of interest is not a property of the components but of the system.

This complexity applies not only to the system of interest but also to the environment in which it is operating. As with the system, neither can its environment be seen as a "pile of things", but as a set of complex systems. This definitely applies to an autonomous ship sailing in a shipping lane where the object detection system of the autonomous navigation and collision avoidance system cannot only detect other ships as objects or "things" in its environment, but must also understand their intended route, their manoeuvring capabilities, in general, the system state of this "thing" called a ship which must be expanded to more than of its physical appearance.

V. The Systems Approach to handle system complexity and emergence

Complex socio-technical systems consist of components and agents (human and artificial) that interact and perform a series of interdependent actions to achieve goals in different environments that, themselves, are systems with non-trivial interacting components. The system properties and behaviour cannot be understood by investigating single components inside the system. Due to the interaction of interdependencies between components and agents, and between the system and its environment, the system properties and behaviour are emergent.

Such properties do not exist in each component, but emerge due to their interactions. By reducing the system into its components, the properties are lost, and therefore become unobservable. Such properties can be said to be computationally irreducible [22].

The growth/decline of macroeconomics and the stock market, the social life of army ants, the wetness of a raindrop, human culture, the global climate, a city's resilience against a catastrophe, and system safety are all examples of emergent behaviour or properties [21][23][24].

A. Complexity - emergence and the CESM metamodel

Complexity and emergent behaviour, or emergent properties, are closely related; hence, the science of emergence is really about complexity [23][25]. There is no single and all-encompassing definition of either complexity or emergence. In the same way, a universal understanding of how to measure them does not exist among either scientists or philosophers [24]. One reason for the lack of a definition is that complexity can come in many forms, such as [21][24][26]:

- Size,
- level of entropy,
- logical and functional depth,
- level and amount of interaction and interdependencies among system entities,
- non-linear causes and effects,
- feedback loops,
- number of system states,
- intricate transition rules between states.

The forms of complexity indicate intractability, non-trivial ways of understanding, explaining and predicting the behaviour of a complex system.

However, it is important to notice that complexity and emergence are properties of the system, not of epistemology [27]. Explained emergence (and complexity) is still emergence [28]; that is, a system does not cease to be complex just because we understand (to a certain degree) its behaviour.

A way to understand and analyse complex systems and emergence is to model the system behaviour in terms of its composition, structure, mechanisms and the environment in which it operates. These system aspects are termed the CESM metamodel [28]:

- **Composition** (C): Collection of all the parts or objects in the system.
- **Environment** (E): Systems outside (excluded from) the target system, but act upon, or are acted upon by, the target system.
- **Structure** (S): The relationships and bonds among the system agents and between the system agents and the environment.
- **Mechanisms** (M): The processes that make the system behave in the way that it does.

The emergent behaviour becomes a function of the above elements; that is, any system s may be modelled, at any given instance, as the quadruple: $\mu(s) = <C(s), E(s), S(s), M(s)>$.

Complexity can be understood in the context [29]:

- **Composition**: Number of system objects, parts and elements. Size of composition hierarchies.
- **Environment**: Size of state space, number of agents and their autonomy, (lack of) rules of interaction with the system.
- **Structure**: The stability of the relationship, responsibility and authority between the system agents, and between the system agents and the environment. The degree of cooperation needed to achieve a goal.
- **Mechanisms**: Number of functions, what agent can/must perform them, needed resources, number of preconditions, possible postconditions, and the control of their execution.

In short, emergent properties result from the conceptual interaction between the elements in the CESM metamodel [30], and complexity can be thought of by how intricate these interactions are.

To investigate the nature of such interactions, the bonds, roles, and responsibilities of agents (the Structure), how they interact (the Mechanisms), and the properties of the system components (the Composition) must be analysed and synthesised.

The above pseudo-definition of emergence and complexity does not entirely describe what these concepts entail; however, it is helpful when developing a framework for understanding and analysing complex systems.

B. Levelism

What constitutes a system depends on the observer's point of view [31]. For two different observers, the same entity may be seen as a system with interacting components, and for another, it can be seen as a (single) component within a larger system.

System behaviour can be analysed (explained) at different Levels of Abstractions (LoAs), depending on the observer's viewpoint; that is, depending on the knowledge we seek [32]. Hence, interactions and dependencies must also be explained at different LoAs. This means that (abstract) system constituents (items, agents and actions) must be identified at different LoAs [30].

An analysis at one LoA is not "better" than at another; they are just different because they provide different kinds of knowledge about the system. The search for knowledge in the current context, driven by the objective of the analysis, guides our choice for LoAs, that is, epistemic levelism.

We may divide levelism (LoA) into epistemic and ontological. Epistemic levelism addresses the kind of knowledge that we seek; ontological levelism is how (we choose to) divide the system into levels of detail. The two kinds of levelism are

often closely related; that is, how the system is divided into levels is often related to what kind of knowledge we seek.

C. System models

Models representing the system are abstractions of constituents and their relationships and bonds. The entities within the system models are also abstractions. The entities included in a system model at certain LoAs may not exist in the actual system or even be planned to exist. The names of the system model entities may indicate their function, role, type, or other features.

More than a single system model is needed to address μ(s). As the conceptual interaction between the elements of the CESM metamodel is both necessary and sufficient to describe any system behaviour, the collection of system models must address every element of the CESM metamodel at the LoAs (epistemic and ontological) needed to gain adequate knowledge [29]. Moreover, they must also be connected so that the emergent system behaviour, μ(s), becomes observable.

For each element in the CESM metamodel, we can assign different model categories. Moreover, the model categories must be connected to elicit μ(s). The following model categories represent the CESM metamodel:

- Composition: **Object model** representing the system elements and components and their ontological relationship to each other.
- Environment: Also modelled as a system containing all aspects of the CESM metamodel, which means that the environment must be represented by models representing the composition, structure and mechanisms (our target system is part of the environment of its environment).
- Structure: **Agent model** includes entities such as controllers, actuators, sensors, humans, and AI subsystems. The agent concept includes authority, responsibility, goals, concerns, motivation, and wishes (humans).
- Mechanisms: **Function model** represents the operations that must be performed (by the agents) to achieve goals.

A specific system model is an instantiation of the above categories. A control structure including a controller, control actions, feedback, and a controlled process known from Systems-Theoretic Process Analysis (STPA) [21] is one instance of an agent model. Another agent model may focus more on the agent's goals, motivation, concerns and wishes, like a model used in a stakeholder analysis where social and business aspects are emphasised.

A function model may focus on the preconditions, resources, and timing for achieving it, like the model used in the Functional Resonance Analysis Method (FRAM) [26]. Or, it may focus on functional dependencies to other functions, like in the Functional Analysis System Technique (FAST) [33].

The different models give different views of the same system, which means that the models should be consistent. Every model has qualities the others lack; however, they need points of contact to ensure their consistency; they need to "borrow" some aspects from each other [29]. The models should be distinguished, not detached or isolated. On top of these borrowed aspects, consistency rules regulate their relationship.

These relationships and rules increase rigour (formalism) in revealing the system behaviour. This is important for the objectivity, the transparency, and thereby the trustworthiness in any context in which these models are used.

Such consistency rules and relationships among multiple system models naturally lend themselves to a Model-Based Safety Analysis (MBSA) toolchain, which is itself an application of Model-Based Systems Engineering (MBSE) as advocated by the International Council on Systems Engineering (INCOSE) community. In this sense, frameworks like SysML can capture and integrate the four CESM elements (Composition, Environment, Structure, and Mechanisms) into a single authoritative system model (Figure 1). Only the model categories for the system are included, not for the environment; however, these model categories should also be incorporated into the environment's system model.

By grounding the safety analysis in an MBSE environment, one follows established INCOSE guidelines for improving system complexity management via formal modelling and consistent architectures. In an MBSA setting, the different views introduced here (object, agent, function, and environment models) are instantiated in SysML, enabling partially or fully automated generation of safety analysis artefacts. Consequently, emergent properties, dynamic behaviours, and critical interdependencies become explicit model elements. This helps ensure rigour (formalism), transparency, and trustworthiness in how complex maritime control systems are designed, analysed, and assured.

From the above discussion, we can conclude that the method for analysing complex systems must be conducted using multiple models at multiple levels of abstraction. The method is called Multi-Level, Multi-Model Safety Analysis (ML/MM-SA) [34].

VI. System analysis

A system may fail to meet expectations due to defects in the elements, or in a combination of the elements, in the CESM-model [35], [30]:

- **Composition**: E.g., missing components, inappropriate component types, component redundancy, etc.
- **Environment**: The system works outside the operational environment for which it was designed.
- **Structure**: E.g., inappropriate or lack of connections, bonds, relationships, or associations between the components.
- **Mechanisms**: E.g., inappropriate or missing rules of interaction between the components

For any analytical method or simulation model, it is important to know the extent to which it explores these defect causes, or combinations thereof, including their potential evolution over time. It indicates causes rooted in the system design, and that should, therefore, be mitigated in the system design phase. The list below, on the other hand, indicates the context in which the system may fail to meet expectations:

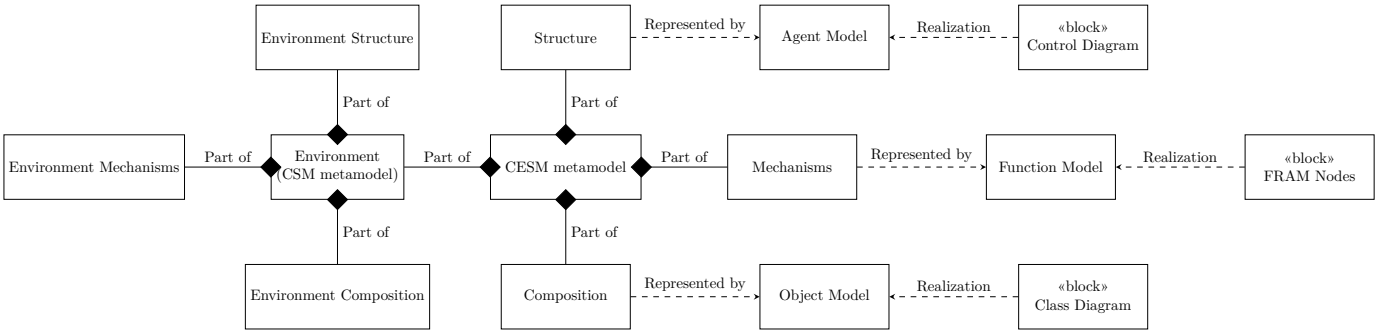

Figure 1. SysML Block Definition Diagram (BDD) of the CESM metamodel.

- **Composition**: The current state of the components, like fully operational /overloaded /degraded /stopped /failure mode, etc.
- **Environment**: State space of the environment, such as temperature /daylight /humidity of a physical environment, or, for an environment consisting of other agents, their speed /course /location, or their (presumed) intention /operational mode etc.
- **Structure**: The state of the relationship between the system components or the environment. This may depend on the current role of a component in relation to other components, or towards the environment, or the current operational mode of the system.
- **Mechanisms**: The current rule-set of interaction; this may depend upon the state of the structure (e.g., roles and relationships), but also on the current state of the composition (e.g., a component, like a sensor, may be out of service and thereby other rule-sets are active).

By combining the items in the above two lists, it becomes clear that there is a substantial number of ways leading to what is known as the combinatorial explosion, in which a system may fail to meet expectations. Therefore, building confidence that a system will meet expectations in all possible situations can be highly challenging. Nevertheless, a system safety analysis must encompass both the above lists in a systematic way.

VII. Potential Application of the Method

In this section, we illustrate how the proposed method could have helped identify or predict the scenarios leading to the accidents described in Section II. Rather than presenting a complete, real-world application or post-accident analysis, we provide a hypothetical demonstration of how the method's core concepts—examining Composition, Environment, Structure, and Mechanisms—might uncover unsafe control actions and emergent behaviours. This illustrative approach highlights the potential of the method to capture the behaviour of complex systems. Still, it does not constitute a full validation of the method against actual case-study data.

The method has also been used as the basis for making DNV-specific guidelines for the DP industry and for guidelines for the assurance of Artificial Intelligence (AI). Moreover, the method has also been used to analyse a subsea Christmas tree.

In the case of Sjoborg, the different local control systems, including the safety systems, such as the blackout prevention system, did not properly interact in such a way that an adequate amount of power was maintained for station keeping using the DP system.

An agent model, such as the control structure found in STPA, represents the system structure ("S" in CESM) that investigates the connections, and relationships between the controllers in the different subsystems and of the safety systems. Such an investigation would focus on the authority, responsibility, and goals (purpose) of each controller associated with the DP system. Moreover, the control structure in STPA also includes the concept of control actions, which is a function achieved by a controller. STPA also specify a set of guidewords to identify unsafe control actions. In particular, STPA identifies how control actions could become unsafe if they are provided too early, too late, or not at all when needed. By examining these possible deviations, STPA makes the system's pathways to hazard more transparent. This is the way by which a controller, through its control action, may or may not set the controlled process into a hazardous state. Although the STPA guidewords are a good help in identifying unsafe control actions, a more explicit approach is to develop a function model ("M" in CESM), such as the one used in FRAM, to systematically investigate the timing, resources, and other conditions that might either hinder a safe action from being achieved, or promote an unsafe action to be achieved by the controller. Such scenarios may be caused by an abnormal state of a system component ("C" in CESM). It is important to notice that the state of the elements in the composition need not be in a failure state to affect how a controller achieves a function. From the investigation report of the accident with Sjoborg, it was indicated that it was a component failure that initiated the scenario, however, still, a vessel like Sjoborg should be able to maintain its position despite such a failure.

In the case of Viking Sky, the method would address the fact that the engine safety system possesses maximum authority over the shutdown of the diesel engines. Whether this design would be maintained after identifying this fact, or the crew would get access to an override button, would, of course, be up to the design team and the class society responsible for approving the design. It is worth noting that the human operators are treated

as controllers in the same manner as the automatic controllers, therefore, the authority and responsibility of the pilot onboard Viking Sky would be taken into account in the analysis.

In the case of MS Richard With, it is difficult to say in detail whether this method would identify the scenario leading to the blackout during the sea trial because of lack of information; however, given the power system was hybrid, it may not be surprising that this method also would shed light in this case.

DNV, Equinor and Shell initiated a Joint Development Project (JDP) together with the DP industry to address the underlying cause of the Sjoborg accident. This project resulted in a Recommended Practice (RP): DNV-RP-0684 "Dynamic Positioning Systems – systems integration" [36], which is a guideline to be used by the industry to be able to analyse and predict such scenarios causing the Sjoborg accident. This is a bespoke guideline for the DP industry, but the theoretical foundation is the method described in this paper.

Safety-related control systems based on AI are being deployed. In the maritime domain, autonomous navigation has already been deployed in several places in Europe. DNV has made a Recommended Practice: DNV-RP-0671 "Assurance of AI-enabled Systems" [37] that requires that the AI system is modelled in accordance with the CESM-metamodel at all relevant abstraction levels as per described in this paper.

DNV, together with the subsea oil and gas industry operating on the Norwegian continental shelf, created a Joint Industry Project (JIP) to address increased system complexity in safety-critical subsea systems. In this project, an analysis of a subsea Christmas tree was performed using this method [38].

VIII. Conclusion

Ship accidents occur can be related to increased ship system complexity. Methods for analysing the behaviour of such systems are based on a reductionist view of the world, which sees it as a "pile of things". Therefore, such methodologies are conceptually inadequate to achieve the objective of such analysis, and the practitioners end up looking for the needle in the haystack.

This paper has described an alternative methodology based on systems thinking. This method acknowledges that the behaviour of complex systems is emergent. Such properties emerge as a result of the interaction and interdependencies within the system constituents, and between the system and the environment in which it operates. One such property is system safety.

These principles have already led to practical outcomes. For instance, the method directly informed the development of DNV's recommended practices for dynamic positioning systems and AI assurance, and it was used in the analysis of a subsea Christmas tree.

By explicitly addressing composition, environment, structure, and mechanisms at multiple levels of abstraction, this approach advances the literature on maritime safety analysis and provides a concrete, systems-based framework for tackling emerging technological challenges.

References

[1] Equinor, 'The Statfjord area', Accessed: 26th Mar. 2025. [Online]. Available: https://www.equinor.com/energy/statfjord.

[2] *Facts about Statfjord "A":The World's Largest Condeep Production Platform*. Aker Group, 1979, ISBN: nb.bibsys.no (991000918904702202).

[3] 'Fact Sheet – Sjoborg', Skansi Offshore, 2012, Accessed: 18th Mar. 2025. [Online]. Available: https://skansi.fo/fleet/sjoborg/.

[4] *Guidelines for vessels with dynamic positioning systems (MSC Circular 645)*, Guideline, Obsolete, replaced by MSC.1/Circ.1580 on 9~June 2017}.

[5] A. Oplenskedal, L. G. Bjørheim and R. L. Leonhardsen, 'Investigation of collision between Sjoborg supply ship and Statfjord A on 7 June 2019', Statens havarikommisjon, Investigation report 001037045, Jun. 2019.

[6] 'MS Richard With Itinerary, Current Position, Ship Review', CruiseMapper, Accessed: 26th Mar. 2025. [Online]. Available: https://www.cruisemapper.com/ships/MS-Richard-With-772.

[7] 'Hurtigrutens første grønne hybridskip klar for seilas langs norskekysten (The first green hybrid ship from Hurtigruten ready to set sail along the cost of Norway)', *Maritimt Magasin*, 23rd Sep. 2022.

[8] C. Salas-Gulliksen, 'Hurtigruten har grunnstøtt nord for Sognefjorden (Hurtigruten has grounded north of Sognefjorden)', NRK, 5th Aug. 2022, Accessed: 26th Mar. 2025. [Online]. Available: https://www.nrk.no/vestland/hurtigruten-har-grunnstott-nord-for-sognefjorden-1.16058532.

[9] T. Stensvold, 'Hurtigruten: Teknisk feil var årsak til grunnstøtingen (Hurtigruten: The cause was a technical failure)', *Tu.no*, 5th Aug. 2022.

[10] 'Viking Sky', Accessed: 26th Mar. 2025. [Online]. Available: https://www.vikingcruises.co.uk/oceans/ships/viking-sky.html.

[11] *Resolution MSC.216(82) - Adoption of Amendments to the International Convention for the Safety of Life at Sea, 1974 as Amended - (Adopted on 8 December 2006)*, Guideline, Dec. 2006.

[12] M. K. Korsnes, 'Difor er det så dramatisk å få motorstopp over Hustadvika (This is why an engine stop gets so dramatic across Hustadvika)', *NRK, dk*, 26th Aug. 2021.

[13] NSIA, 'Loss of propulsion and near grounding of Viking Sky, Hustadvika, Norway, 23 March 2019', Norwegian Safety Investigation Authority, Accident investigation MARINE 2024/05, Mar. 2025.

[14] P. K. Sebak, *Titanic*, in *Store norske leksikon*, 18th Jun. 2024.

[15] P. Sebak, *M/S Estonia*, in *Store norske leksikon*, 20th Jun. 2024.

[16] O. Bjørneset, 'Losen på «Viking Sky» meiner automatikken må kunne overstyrast (The pilot onboard the "Viking Sky" suggests that it should be possible to override the automatic control)', *NRK, dk*, 24th Sep. 2019.

[17] M. Bunge, *Emergence and Convergence: Qualitative Novelty and the Unity of Knowledge*, Reprint edition. Toronto: University of Toronto Press, Scholarly Publishing Division, 9th Jul. 2014, 344 pp., ISBN: 978-1-4426-2821-2.

[18] *MSC.1/Circular.1580 – Guidelines for Vessels and Units with Dynamic Positioning (DP) Systems – (16 June 2017)*, Guideline, Jun. 2017, Current.

[19] N. Leveson, *SafeWare: System Safety and Computers*. Reading, Mass: Addison-Wesley, 1995, 680 pp., ISBN: 978-0-201-11972-5.

[20] C. A. Ericson, 'Failure Mode and Effects Analysis', in *Hazard Analysis Techniques for System Safety*, John Wiley & Sons, Ltd, 2005, pp. 235–259, ISBN: 978-0-471-73942-5. DOI: 10.1002/0471739421.ch13.

[21] N. G. Leveson, *Engineering a Safer World: Systems Thinking Applied to Safety*. Cambridge, Massachusetts: MIT Press, 13th Jan. 2012. DOI: 10.7551/mitpress/8179.001.0001.

[22] S. Wolfram, 'Undecidability and intractability in Theoretical Physics', in *Emergence*, Cambridge, Massachusetts: The MIT Press, 2008, pp. 387–393, ISBN: 987-0-262-02621-5.

[23] J. H. Holland, *Complexity: A Very Short Introduction* (Very Short Introductions 392), First edition. Oxford, United Kingdom: Oxford University Press, 2014, 95 pp., ISBN: 978-0-19-966254-8.

[24] M. Mitchell, *Complexity: A Guided Tour*. New York, NY: Oxford University Press, 2011, 349 pp., ISBN: 978-0-19-979810-0.

[25] M. M. Waldrop, *Complexity: The Emerging Science at the Edge of Order and Chaos* (A Touchstone Book), 1. Touchstone ed. New York, NY: Touchstone, 1993, 380 pp., ISBN: 1-5040-5914-X 978-1-5040-5914-5.

[26] E. Hollnagel, *FRAM: The Functional Resonance Analysis Method, Modelling Complex Socio-Technical Systems*. Ashgate Publishing Limited, 2012.

[27] M. A. Bedau, 'Is Weak Emergence Just in the Mind?', *Minds and Machines*, vol. 18, no. 4, pp. 443–459, 1st Dec. 2008, ISSN: 1572-8641. DOI: 10.1007/s11023-008-9122-6.

[28] M. Bunge, *Emergence and Convergence: Qualitative Novelty and the Unity of Knowledge* (Toronto Studies in Philosophy). Toronto ; Buffalo: University of Toronto Press, 2003, 330 pp., ISBN: 978-0-8020-8860-4.

[29] O. I. Haugen, 'The Systems Approach', in *Demonstrating Safety of Software-Dependent Systems; With Examples from Subsea Electric Technology*, T. Myhrvold and M. van der Meulen, Eds., DNV AS, 2022, pp. 145–163, ISBN: 978-82-515-0324-2.

[30] O. I. Haugen, 'Safety assurance of complex systems Part 2: Assurance and analysis', DNV AS, Høvik, Norway, Whitepaper, 2019.

[31] G. M. Weinberg, *An Introduction to General Systems Thinking*. Dorset House, 2001, 308 pp., ISBN: 978-0-932633-49-1. Google Books: eU9gDxt9X0wC.

[32] L. Floridi, 'The Method of Levels of Abstraction', *Minds and Machines*, vol. 18, no. 3, pp. 303–329, 1st Sep. 2008, ISSN: 1572-8641. DOI: 10.1007/s11023-008-9113-7.

[33] C. W. Bytheway, *FAST Creativity & Innovation: Rapidly Improving Processes, Product Development and Solving Complex Problems*. Fort Lauderdale, Fla: J. Ross Pub, 2007, 254 pp., ISBN: 978-1-932159-66-0.

[34] O. Haugen, 'Developing a safety argument', in *Demonstrating Safety of Software-Dependent Systems : With Examples from Subsea Electric Technology*, Høvik, Norway: DNV AS, Mar. 2022, pp. 55–82, ISBN: 978-82-515-0324-2.

[35] O. Haugen, 'Safety assurance of complex systems Part 1: Complexity', DNV AS, Høvik, Norway, Whitepaper, 2019.

[36] DNV, *DNV-RP-0684 Dynamic Positioning Systems – systems integration*, Recommended Practice, version March 2025, Mar. 2025.

[37] DNV, *DNV-RP-0671 Assurance of AI-enabled systems*, Recommended Practice, version September 2023, Sep. 2023.

[38] O. I. Haugen, 'Application of ML/MM-SA on a subsea Christmas tree', in *Demonstrating Safety of Software-Dependent Systems; With Examples from Subsea Electric Technology*, T. Myhrvold and M. van der Meulen, Eds., DNV AS, 2022, pp. 321–370, ISBN: 978-82-515-0324-2.