# Assessing complex failure scenarios of on-board distributed systems using a Markov chain

Habben Jansen, Agnieta; Duchateau, E. A.E.; Kana, A. A.; Hopman, J. J.

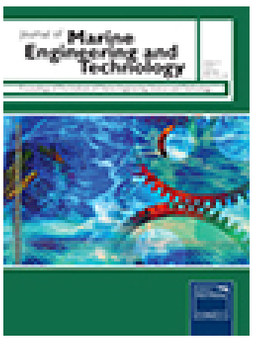
**DOI**
10.1080/20464177.2019.1673032

**Publication date**
2020

**Document Version**
Final published version

**Published in**
Journal of Marine Engineering and Technology

**Citation (APA)**
Habben Jansen, A., Duchateau, E. A. E., Kana, A. A., & Hopman, J. J. (2020). Assessing complex failure scenarios of on-board distributed systems using a Markov chain. *Journal of Marine Engineering and Technology*, *19*(Sup1), 45-61. https://doi.org/10.1080/20464177.2019.1673032



Taylor & Francis
Taylor & Francis Group

Journal of Marine Engineering & Technology

ISSN: 2046-4177 (Print) 2056-8487 (Online) Journal homepage: https://www.tandfonline.com/loi/tmar20

# Assessing complex failure scenarios of on-board distributed systems using a Markov chain

A. C. Habben Jansen, E. A. E. Duchateau, A. A. Kana & J. J. Hopman

**To cite this article:** A. C. Habben Jansen, E. A. E. Duchateau, A. A. Kana & J. J. Hopman (2019): Assessing complex failure scenarios of on-board distributed systems using a Markov chain, Journal of Marine Engineering & Technology, DOI: 10.1080/20464177.2019.1673032

**To link to this article:** https://doi.org/10.1080/20464177.2019.1673032



Published online: 30 Sep 2019.

JOURNAL OF MARINE ENGINEERING & TECHNOLOGY
https://doi.org/10.1080/20464177.2019.1673032

Taylor & Francis
Taylor & Francis Group



# Assessing complex failure scenarios of on-board distributed systems using a Markov chain

A. C. Habben Jansen[a], E. A. E. Duchateau[b], A. A. Kana [a] and J. J. Hopman [a]

[a]Department of Maritime & Transport Technology, Delft University of Technology, Delft, Netherlands; [b]Maritime Systems Division, Defence Materiel Organisation, Utrecht, Netherlands

**ABSTRACT**

Vulnerability reduction is an important topic during the design of naval ships because they are designed to operate in hostile environments and because their on-board distributed systems are becoming increasingly complex. The vulnerability needs to be addressed in the early design stages already, in order to prevent expensive or time-consuming modifications in later, more detailed design stages. However, most existing methods for assessing the vulnerability are better suited for more detailed design stages. Furthermore, existing methods often rely on pre-defined damage scenarios, while damage – or system failure in general – may also occur in ways that were not expected beforehand. This paper proposes a method that addresses these gaps. This is done by incorporating several additions to an existing vulnerability method that has been developed by the authors, using a Markov chain. With this method, there is no longer a need for modelling individual hits or failure scenarios. The additions are illustrated by two test cases. In the first one, a notional Ocean-going Patrol Vessel is considered, and damage is related to physical locations in the ship. The second test case considers a chilled water distribution system in more detail, with failures modelled independent from the physical architecture. The quantitative nature of the results provide an indication of the generic, overall vulnerability of the distributed systems, which is meant to be used in the early design stages for identifying trade-offs and prioritising capabilities.

**ARTICLE HISTORY**
Received 1 May 2019
Accepted 6 September 2019

**KEYWORDS**
Naval ship design; vulnerability; distributed systems; early stage design; Markov chain

## 1. Introduction

Naval ships are designed to operate, survive, and win in hostile environments. As such, vulnerability reduction is one of the key aspects that needs to be considered during the design of a naval ship. The United States Department of Defense definition of vulnerability is: 'The characteristics of a system that cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (man-made) hostile environment' (Gortney 2010). Several other definitions of vulnerability exist, which have a similar scope, with 'incapability to perform mission' and 'man-made hostile environment' as key aspects.

The vulnerability of a naval ship is largely determined by the ship layout. As such, obtaining an intelligent layout is in general regarded as the most effective protective measure (Brown 1991). Traditionally this has mainly been realised by ensuring sufficient damage stability with watertight compartments (e.g. Boulougouris and Papanikolaou 2013) and by incorporating blast resistant bulkheads (e.g. Erkel et al. 2002). Though these topics continue to remain highly relevant for vulnerability reduction of modern naval ships, technological changes have introduced a new topic of interest with regard to vulnerability, namely, the availability of distributed systems. These are systems that supply and distribute vital resources such as electricity, chilled water, data, and fuels through the ship. The increasing degree of on-board electrification, automation, and digital transformation has resulted in distributed systems that are more complex, more interdependent, and more difficult to understand than before (Brefort et al. 2018). The availability of these systems after damage has therefore become as critical for vulnerability reduction as the more traditional measures that involve damage stability and structural integrity. This holds in particular for ships with an integrated power system, where propulsion, hotel and combat power are all electric. This powering concept is known as IPS (integrated power system) or IFEP (integrated full electric powering/propulsion). This paper uses the term IFEP.

**CONTACT** A. C. Habben Jansen a.c.habbenjansen@tudelft.nl Department of Maritime & Transport Technology, Delft University of Technology, Mekelweg 2, 2628CD Delft, Netherlands

In addition to this perspective of external threats, the distributed systems themselves can also become more vulnerable. This is because their complexity may result in an increased opportunity for cascading failures, such as those that have occurred on the USS Yorktown, or, more recently, on UK Type 45 destroyers (Goodrum et al. 2018). Though internal ship failures, that are not related to hostile environments, are usually referred to as reliability rather than vulnerability, the distinction between the two has become less sharp. Yet, the resulting impact remains unchanged. Altogether, vulnerability reduction concerns what the consequences of failures are, and how they can be mitigated – not how they occurred in the first place. Because of the high complexity of distributed systems, this may also encompass failures that have not occurred previously, or failures that are still unknown.

Many existing methods for vulnerability reduction, which are reviewed in more detail in Section 2, consider a relative high complexity of the distributed systems and the ship, and a lower complexity of the damage, i.e. a small number of hits with a known extent of the subsequent damage. This aligns with historical experience with hostile incidents but does not necessarily account for more complex or even unknown failures that may occur due to the increased complexity of distributed systems. In addition to that, the relative high level of detail of the ship and its distributed systems that is required for some vulnerability methods makes them less suited for early stage design, where such level of detail usually is not available yet. At the same time, this is the design stage where the most important decisions for distributed systems are made, such as which components to include, and whether they should be redundant. As such, vulnerability reduction can benefit from extending the focus of vulnerability methods to earlier design stages. To address these topics, this paper introduces a method for vulnerability reduction at a low level of detail, while accounting for complex failure scenarios. This is an extension of the authors' earlier work, that has previously been presented at the International Naval Engineering Conference (INEC) in Glasgow, 2018 (Habben Jansen et al. 2018a).

The remainder of this paper is organised as follows. Section 2 provides an overview of existing methods for vulnerability assessments and ends with a set of requirements for the new method. Section 3 introduces the new method and explains how it incorporates the requirements. Subsequently, Sections 4 and 5 provide two test cases, with an OPV and a chilled water distribution system, respectively. Conclusions are drawn in Section 6, and recommendations are provided in Section 7.

## 2. Review of vulnerability assessment methods

Various methods exist for assessing the vulnerability of distributed systems. Examples include dedicated software applications such as RESIST (TNO 2018), SURVIVE (Schofield 2009), or SURMA (Surma Ltd. 2018). These tools provide a high-fidelity overview of the consequences, such as floodings or fire spreads, of various damage scenarios. Their analyses are not limited to distributed systems but also take into account damage stability and structural integrity. Many of these tools are mostly suited for more detailed design stages, as they typically require a detailed definition of the hull structure, and a design and layout of the distributed systems, which are usually not available in early stage design. However, dedicated vulnerability tools for earlier design stages exist as well, such as the commercially developed tool PREVENT (Heywood and Lear 2006), which uses a significantly reduced level of detail. For example, the routings between systems are not considered. Similar to the tools that have been mentioned before, PREVENT assesses vulnerability in the context of a man-made hostile environment. For example, weapon characteristics such as warhead weight and blast pressure are assumed to be known beforehand.

Apart from these commercially developed tools, several other vulnerability methods exist as well, which have mainly been developed within an academic context. For example, Goodfriend and Brown (2017) use genetic optimisation to define an overall measure of vulnerability, which can be combined with other measures of performance, in order to define a more complete overall measure of effectiveness for the ship. The method is intended for the early design stages. Yet, their vulnerability calculations are similar to the program MOTISS, which is comparable to the earlier mentioned tools like SURVIVE and RESIST. As such, considerable detail is still required. Further reduction in detail is applied by van Oers et al. (2012), who have developed a 2D routing method for the connections between distributed systems, allowing for variations on shortest paths between system components. Based on that work, Duchateau et al. (2018) have developed a similar routing method, but in 3D and allowing for detours of the shortest path, which may be longer, but potentially less vulnerable. Both methods include a computation of the vulnerability, which is done by assessing the connectivity of the distributed systems after the loss of one or more compartments. As the number of lost compartments increases, the computational effort increases as well. As such, these methods are mostly suited for limited complexity of the damage scenarios, but a relatively high complexity of the distributed systems topology is allowed.

Another vulnerability method of a more conceptual nature is developed by Goodrum et al. (2018). This network-based method calculates an operability score for the ship by systematically removing the network nodes that represent the different compartments of the ship. The quick and robust nature of the network-based method fits well in the early design stage, but also with the limitation of the number of damage scenarios that are assessed. Furthermore, the operability score does not further specify the residual capability after damage, while this may be an important design requirement that needs to be met. A method with a slightly different perspective has been developed by Shields et al. (2017). Rather than developing actual routings, their method mainly focusses on gaining insight between the arrangement of the compartments (physical architecture), the distributed systems topology (logical architecture), and the overlap between the two (physical solution). The results of their method can be used for a vulnerability assessment, but such an assessment is not included in the method itself.

The methods mentioned above consider both the topology of distributed systems and the way in which the topology is routed through the ship, i.e. the physical and logical architecture, and their overlap: the physical solution. This terminology has been introduced by Brefort et al. (2018), and will be used throughout this paper. In addition to these methods, several vulnerability methods with a specific focus on the logical architecture exist, i.e. methods that assess the vulnerability of a topology itself, regardless of how that topology is routed through the ship. A recent example is the work of de Vos and Stapersma (2018), who have developed a tool that can automatically generate a vast number of topologies in order to explore the design space. A genetic algorithm is used to obtain topologies with low vulnerability as well as low 'system claim', which is defined as the degree to which a topology 'claims' space, weight, and cost in the ship. They define reconfigurability of a topology as a critical aspect of vulnerability reduction, which can be realised by connecting hubs in the topology. As such, their vulnerability metric is a network-based metric that quantifies the connectedness between hubs, which they introduce as 'max-flow-between-hubs'. They do not include an actual flow analysis, i.e. it only matters whether the topology is connected. This does not necessarily imply that sufficient flow and capacity is available. The latter has been investigated by e.g. Trapp (2015), who has developed a method for survivable design of flow networks. The flow computations require several additional characteristics, such as flow volume and flow rate capacity, inherently requiring more detailed input data. In his test case, a survivable network is defined as one that can still operate – with sufficient flow – after the loss of one edge, regardless of which one.

As mentioned in Section 1, vulnerability reduction of distributed systems is particularly important for ships with an IFEP concept, which is confirmed by several literature contributions. For example, Cramer et al. (2011) have developed a method that particularly focusses on the vulnerability of an IFEP concept. They mention no specific intended design stage, but as some of the input data is rather specific, such as voltages, currents, temperatures and flow rates for given operational conditions, a more detailed design stage seems most suitable for this method. The method also introduces a way to compute an overall dependability metric (where dependability is defined as operability over a range of damage scenarios), but it is noticed that this computation is limited by the number of damage scenarios. A method to identify the worst-case scenario is presented as well. Interestingly enough, a genetic algorithm is used for this. This is exactly opposite from other methods that use a genetic algorithm, as they usually intend to find the best solutions. IFEP ships are also main topic of the work of Schuddebeurs (2014), who specifically considers advanced modelling and simulation techniques for de-risking IFEP ships, aiming at high-fidelity results that are particular useful for detailed design or modifications to in-service ships. A more early stage context is discussed by Chalfant (2015), who confirms the need for early stage vulnerability assessments for IFEP ships, while at the same time noting that the number of available suitable methods is limited. Doerry (2007) states that vulnerability in IFEP ships can be reduced by zonal design, where damage can be confined to a single zone, without interrupting operations in adjacent zones. He discusses this concept in more detail in Doerry (2006). In addition to damage by external threats, Doerry (2007) also notes that distributed systems on board IFEP ships need to operate adequately in normal operating conditions, which addresses the more internal aspect of vulnerability. To quantify this, he introduces a Quality-of-Service metric that is based on, amongst others, the mean time between failure rates for the different components and a fault effects analysis. Such types of analyses in the context of IFEP ships are discussed in more detail by e.g. Logan (2007) and Menis et al. (2012).

Based on this review, a need for further development in assessing the vulnerability of distributed systems can be identified. More specifically, the need arises for a method that assesses vulnerability,

- in the early design stage, i.e. with a limited level of detail and in a rapid fashion;

- with the focus on the consequences of the hits, rather than how the hit occurred in the first place;
- for complex failure scenarios, i.e. without a limitation to pre-defined, known failure scenarios;
- with a focus on residual capabilities after failure, i.e. from a capabilities perspective in addition to a systems perspective.

In order to address these points of attention, the authors have previously developed a method in which the damage scenario has been generalised (Habben Jansen et al. 2018b). This method reduces the need for simulating individual damage scenarios. The method assesses the vulnerability of distributed systems in naval ships using a discrete Markov chain. Subsequently, further developments have been made in order to apply the method in a more practical environment (Habben Jansen et al. 2018a). The present paper is an extension of that work, and addresses two test cases for the method. The first test case considers a notional Ocean-going Patrol Vessel (OPV) with two powering concepts: a conventional concept with separate mechanical propulsion, and an IFEP concept. For this test case, the vulnerability is assessed in the physical and logical architecture. In other words, it takes into account at which location in the ship a failure occurs, and in which residual capability this results. This test case was already included in Habben Jansen et al. (2018a) and is now extended with an improved comparison of the two powering concepts. The second test case, which is new work, considers the comparison of two logical architectures (i.e. topologies) of a chilled water system, where the level of detail is increased relative to the first test case. This test case shows how the method can be used to assess any failure, regardless of where in the ship it occurs.

As will be described in Section 3.1, the new method uses a discrete Markov chain, as it is particularly suited for describing various conditions of a system, and the transitions between them, over discrete time steps (Lay 2006). Various applications of Markov chains for the design of physical systems exist, often with a focus on vulnerability. For example, Jung et al. (2002) apply a discrete Markov chain for designing electrical power systems under vulnerable conditions. A Markov chain is used to describe load shedding of a power system. In combination with adaptive control systems, the load shedding can be used to prevent catastrophic failures. Markov chains are also applied in combat aircraft design for assessing vulnerability (Pei et al. 2006). In a naval ship design context, Kim and Lee (2012) use a Markov chain to assess the vulnerability of a notional warship. They calculate the probability of kill for several vital ship components. Information on the relationship between the components (e.g. whether they are redundant or not) is included upfront in the Markov chain. However, this method is less applicable for shifting the perspective from systems to capabilities, as one capability may require multiple systems, or one system may support multiple capabilities. The set-up of the Markov chain in this paper therefore differs from the set-up used by Kim and Lee (2012). An advantage of the Markov chain is that the vulnerability assessment is not limited by the number, location, or size of hits, or failures in general. As such, the complexity of the failures can be increased. As will be discussed in Section 4.1, this comes at the cost of a reduction in the complexity of the distributed systems. The relation between existing methods, the new Markov method, and the desired scope of the vulnerability assessment is visualised in Figure 1.


**Figure 1.** Relation between existing vulnerability methods and the new Markov method, in terms of complexity of failures and the distributed systems.

## 3. Method

This section elaborates on the technical details of the vulnerability method. The previous set-up of the method is first discussed in Paragraph 3.1. The improvements and modifications to the method are discussed in Paragraphs 3.2 to 3.4.

### 3.1. Previous set-up of the method

The key elements of a Markov chain are the state vector **s** and the transition matrix *T*. The state vector describes the probabilities for the system to be in a certain state. In the case of the vulnerability method presented in this paper, the system is the ship itself and the states are the availabilities of different components of the distributed systems, described with the state vector. The components

are located in different compartments. When a compartment gets hit, the components and routings located in that compartment become unavailable. This is modelled with the transition matrix. The probability for each state at any point in time can be calculated according to Equation (1).

$$\mathbf{s}(k) = \mathbf{s}(0) \cdot T^k \tag{1}$$

The following assumptions apply to this assessment:

(1) All systems can be either on or off. As a result, the number of states is $2^n$, where $n$ is the number of systems. Hence, the size of the $\mathbf{s}$ is $2^n$ and the size of $T$ is $2^n \times 2^n$.
(2) All states are initially on, meaning fully operational
(3) At each time step, one hit occurs, disabling one compartment.
(4) All compartments have equal hit probability at each time step. This assumption is investigated in more detail in the test case of Section 4.
(5) Once a system is off, it cannot be repaired.

An example of a physical solution that was used for the proof-of-concept for this method is shown in Figure 2. Two systems, A and B, are present in this physical solution. Because of Assumption 1, this leads to four states for the Markov chain: both A and B on, only A on, only B on, and both A and B off. The transition matrix then becomes Equation (2).

$$T = \begin{bmatrix} 3/9 & 3/9 & 2/9 & 1/9 \\ 0 & 6/9 & 0 & 3/9 \\ 0 & 0 & 5/9 & 4/9 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{2}$$

Because of Assumption 2, the initial state becomes Equation (3).

$$\mathbf{s}(\mathbf{0}) = \begin{bmatrix} 1 & 0 & 0 & 0 \end{bmatrix} \tag{3}$$

The state probabilities for all four states after an increasing number of hits is presented in Figure 3. It can be seen that the probability for State 4, where both systems are off, increases and approaches 1. This makes sense, as a large number of hits will eventually highly likely disable both systems. Similarly, the the probability for State 1, where both systems are on, rapidly decreases. The probabilities for State 2 and State 3 hold an intermediate position. As discussed in more detail in Habben Jansen et al. (2018b), the results of the method affirm the necessity for an integrated approach, in which the vulnerability of all distributed systems is assessed simultaneously. In other words, the vulnerability of system A and system B needs to be assessed in an integrated fashion, rather than decomposed. Furthermore, it has previously been shown that the fact that distributed systems are placed together in a ship already connects them from a vulnerability point of view. This also holds when the systems do not have any physical, logical, or operational overlap. However, several improvements are needed to apply the method in a more practical environment. To that end, three adjustments are made: scaling up in complexity, adjusted hit probabilities, and systems to capabilities. These are discussed below in more detail.

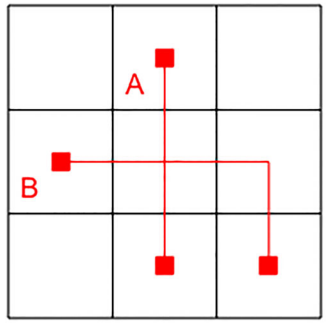



**Figure 2.** Physical solution used for the proof of concept, as defined in Habben Jansen et al. (2018b).

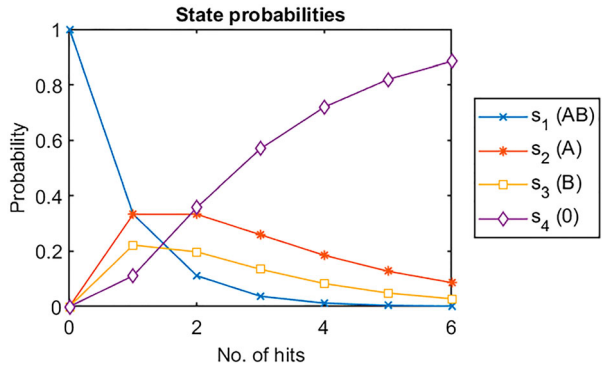



**Figure 3.** State probabilities for the proof of concept, retrieved from Habben Jansen et al. (2018b).

### 3.2. Scaling up in complexity

The physical solution of the proof-of-concept only considers two systems, both consisting of a supplier, a consumer, and a routing between them. Assessing the availability of such systems is straightforward; if either the supplier, the consumer, or the connection is off, the entire system is off. Otherwise, the system is on. This is not representative for a distributed systems network on an actual ship, where more components and connections, possibly redundant, are included, and where one or multiple hubs, e.g. electrical switchboards, valve chests or data switches may be located between the supplier and the consumer (de Vos and Stapersma 2018). Furthermore, some components may be part of multiple types of

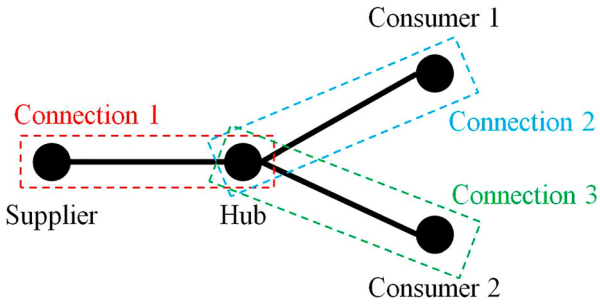



**Figure 4.** Definition of connections as used for the extended vulnerability method.

distributed systems, such as a chilled water unit, which is a consumer for the electrical network, but a supplier for the chilled water network. A different definition of systems is therefore needed.

Consider the example network in Figure 4. The system components are the nodes, and the connections between them are the edges. Because this network contains a single supplier and hub, and two different consumers, there is no clear, isolated system that can be on or off, like in the previous situation. The availability of the consumers depends on where a hit occurs. Furthermore, it may not be clear whether a node is at the beginning or at the end of an edge, which is the case for the hub. In order to account for that, the states are no longer described by the number of systems, but the number of connections. These connections include the start node and the end node. The fact that the hub is counted three times does not impose complications. If the hub is hit, it disables all three connections at once, instead of only one connection. The same applies to other nodes that are part of multiple connections. Another option is to consider all nodes and edges separately as individual items that can be on or off. However, this quickly increases the size of the computation. For this example, it results in assessing seven items (four nodes and three edges) instead of three connections.

Compared to the proof-of-concept, which evaluated a small layout with nine compartments, the number of compartments increases as well for practical applications. The number of compartments does however not limit the computational effort; it merely changes the values of individual entries in the transition matrix.

### 3.3. Hit probability

When a compartment gets hit, a transition to another state may occur, depending on what is located inside that compartment. Though the method does not model individual hits, the hit probabilities of each compartment are still required for the assessment. It is assumed that a hit occurs at each time step in the Markov chain, disabling one of the compartments. Previously, each compartment was assumed to have an equal hit probability, regardless of its size or location in the ship. To perform a more representative assessment, it may be necessary to adjust this. For example, larger compartments are generally expected to have higher hit probabilities than smaller compartments, or compartments in the centre of the ship may have higher hit probabilities than compartments at the fore or aft end. To account for that, the possibility to use weight factors for individual compartments has been introduced.

In order to apply a Markov chain for the vulnerability method, the weight factors must be scaled in such way that the sum of all elements of each row in the transition matrix equals 1 (Lay 2006). Let $n_c$ be the number of compartments of the ship. A weight factor $w$ is assigned to the hit probability of each compartment, as expressed in Equation (4):

$$w_1 \cdot \frac{1}{n_c} + w_2 \cdot \frac{1}{n_c} + \cdots + w_{n_c} \cdot \frac{1}{n_c} = 1 \tag{4}$$

From this, Equation (5) can be derived:

$$\sum w_1 \ldots w_{n_c} = n_c \tag{5}$$

Any combination of values that complies with the scaling method of Equation (5) can be used within the vulnerability method. For example, if the hit probability of Compartment 2 is twice as high as the hit probability of Compartment 1, the associated weight factor is twice as high, as long as the sum of all weight factors equals the total number of compartments. The two examples mentioned earlier, with higher weight factors for larger compartments or compartments located in the centre of the ship, are discussed in more detail in the test case presented in Section 4.

### 3.4. Systems to capabilities

Paragraph 3.2 explains why systems need to be broken down in individual connections to apply the vulnerability method on a larger scale. However, the eventual question is whether critical capabilities are still available after hits, rather than which systems or connections are still on. For example, from an operational point of view it is not directly important that a component fails, such as a diesel generator set. However, it does matter that the self-defence capability is lost, if this particular diesel generator set provides the radar of a close-in weapon system (CIWS) with electricity. This subtle, but important different perspective requires a transition from thinking in systems or connections to thinking in capabilities.

These main capabilities may for example be fight, move, and float, which can be further broken down in sub-capabilities, such as offensive and defensive fighting, if necessary. The capabilities that are required after a hit may depend on the impact level of a hit. For example, if a hit with a minor impact level has occurred, the focus may remain with the primary mission capability, which is fight, while after a hit with a major impact level the focus may be with float. This also relates to the architectural framework of Brefort et al. (2018). While the physical and logical architecture have been discussed previously, the framework also includes a third component: the operational architecture. This architecture describes how on-board distributed systems are used. The transition from systems to capabilities, which may shift in priority because of operational circumstances, is an example of operational architecture. Yet, operational architecture also considers other aspects, which are not discussed in the present paper, such as man-machine interaction or varying load balances over time.

It may sound contradictory that there is a need for thinking in high-level capabilities, while Paragraph 3.2 advocated for a method where distributed systems are broken down into individual connections. However, these connections are still needed because of the supplier-hub-consumer structure of the distributed systems network. Consider for example the network of Figure 4 again. Let us assume that Consumer 1 and Consumer 2 both are self-defence systems, for example CIWS's. If a hit occurs that disables Connection 2, while Connections 1 and 3 remain available, the self-defence capability is still available. However, if Connection 2 becomes disabled while Connection 3 already was disabled, the self-defence capability is lost. Hence, in order to properly assess the availability of capabilities, individual connections are still needed.

To make the transition from connections to capabilities, states of the Markov chain that contribute to a capability need to be clustered and added together. Logical relations should be taken into account while doing this. For example, the capability fight may need electricity AND chilled water for a weapon system, while the electricity for this weapon system may be supplied by switchboard 1 OR switchboard 2.

## 4. OPV test case

In order to demonstrate the improvements to the method, and their benefits, a test case with a notional Ocean-going Patrol Vessel (OPV) is introduced. The model of this notional OPV has previously been introduced in other early stage vulnerability research (Duchateau et al. 2018; de Vos et al. 2018). The physical architecture of the model is presented in Figure 5.

### 4.1. Distributed systems layout

The main capabilities fight and move are considered in this test case. The capability fight has two sub-capabilities: offensive and defensive. These sub-capabilities are provided by an offensive high-energy weapon (HEW) and a defensive close-in weapon system (CIWS). The capability move is provided by two propellers (PS and SB). A distributed systems network provides power to the weapons and propellers, and chilled water to the weapons. Two fundamentally different powering concepts are tested:

(1) *Conventional concept*: A concept with separate propulsion, provided by mechanical energy with diesel engines (DEs) and shafts. The electrical power is provided by diesel generators (DGs). Power is transferred to the weapons via switchboards (SBs). In addition to that, chilled water units (CWs) provide chilled water to the weapons.
(2) *Integrated Full Electric Propulsion* (*IFEP*) *concept*: For this concept, both the weapons and the propellers are powered by electric energy. The chilled water for the weapon systems is provided with two local CWs.

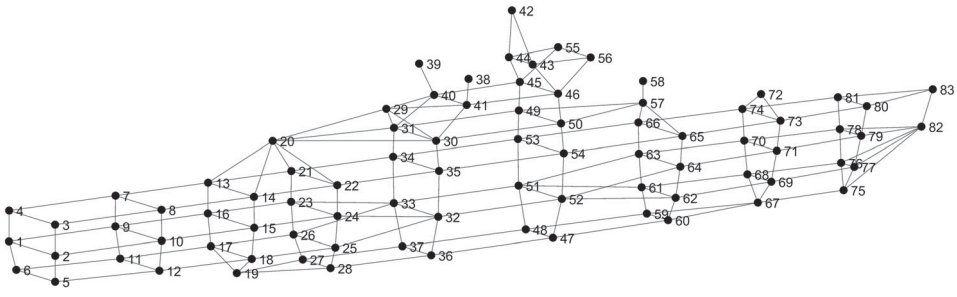



**Figure 5.** Physical architecture of the notional OPV used for the test case. Each node represents the geometric centre a compartment. Each edge denotes a physical adjacency between compartments, i.e. the compartments are located on both sides of the same deck or bulkhead.

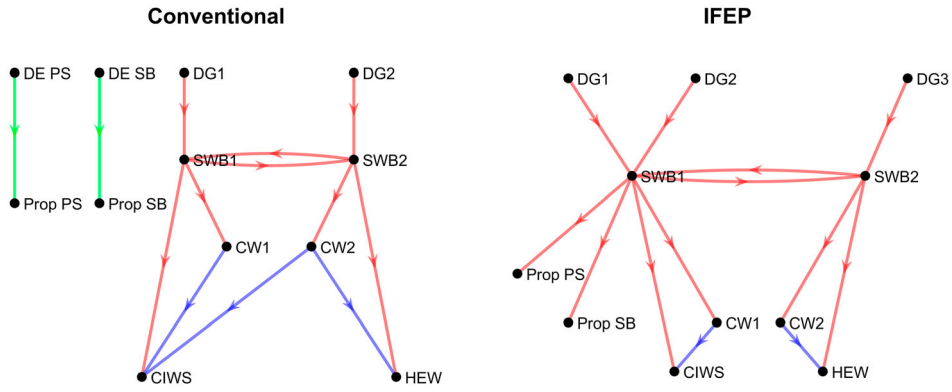



**Figure 6.** Logical architectures for the two powering concepts, with mechanical energy (green), electrical energy (red) and chilled water (blue). For interpretation of the references to colour in this figure, the reader is referred to the web version of this article.

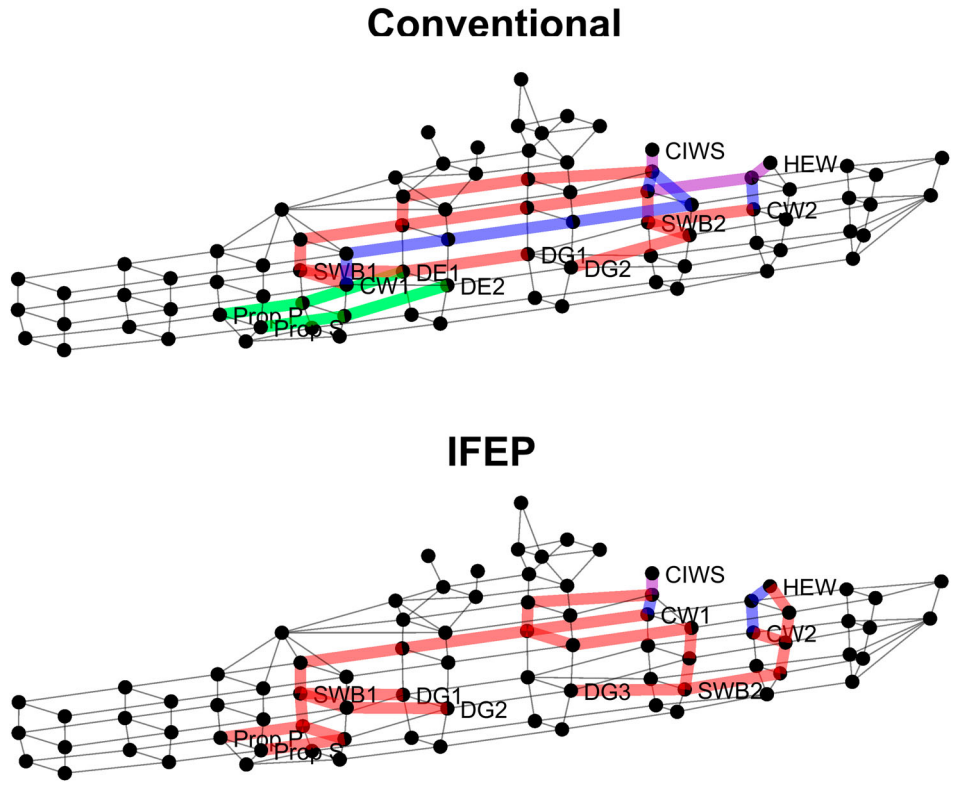



**Figure 7.** Physical solutions for the notional OPV. Purple lines represent routings of both chilled water and electricity through the same compartments.

The attempt was made to make the physical architectures as similar as possible to 'isolate' the differences in the logical architecture. However, due to the difference in logical architecture, this is not entirely possible, causing some of the results to be dependent on the physical architecture. The logical architectures of these powering concepts are visually presented in Figure 6. Figure 7 shows the associated physical solutions.

The logical architectures consist of 11 or 12 nodes and 12 connections. A typical logical architecture that is assessed during early stage design consists of about 10–100 nodes (de Vos and Stapersma 2018). Hence, the logical architectures in this test case do not do full justice to the complexity of the design of on-board distributed systems. Yet, the logical architectures for this test case have deliberately been developed this way. As discussed in Section 3.1, the length of the state vector becomes $2^n$, and the size of the transition matrix becomes $2^n \times 2^n$, where $n$ is the number of edges in the logical architecture. As a result, the amount of data generated increases exponentially. More specifically, this limits the number of edges to 13 for a normal, modern PC using standard settings of MATLAB. This means that only small logical architectures can be assessed. At the same time,

the allowed complexity of the damage scenarios is very high, which is deemed a useful contribution based on the review of Sections 1 and 2. The computations of this test case go up to 8 hits, which accounts for any damage scenario of 8 hits, for example including one major damage that stretches over 8 compartments, four minor damages that stretch out over 2 compartments, or even 8 minor hits that all damage the same compartment. Though it is acknowledged that some of these scenarios may be likelier than others to occur, the goal of this method is to assess the vulnerability in a probabilistic way, which gives an indication of the general vulnerability, rather than the specific vulnerability for certain damage scenarios.

### 4.2. Test case set-up

With the improvements to the method and layout of the ship and its networks available, the improved vulnerability method can be tested. Both powering concepts are tested in three ways:

(1) Uniform hit distribution over all compartments, such as it previously has been done.
(2) Hit probabilities adjusted to the projected lateral area of the compartments.
(3) Hit probabilities adjusted to the longitudinal positions of compartments.

For Options 2 and 3, the scaling method of Equations (4) and (5) is used. The projected lateral areas of the compartments, which are required for Option 2, are presented in Figure 8. The variety in projected lateral areas can clearly be observed. Several compartments stand out for their exceptional large projected area, i.e. their significant higher hit probability: the hangar, the radar mast, and the engine rooms. This solely relates to the projected area, and does not account for any other signature, which may not be available in the early design stages. The distributed systems networks that are considered in this test case use the engine rooms for several vital components and routings, which is likely to influence the results. The weight factors for the hit probabilities for the longitudinal positions of the compartments as used in Option 3 are given in Figure 9. It is assumed that the aft end of the ship has a unit weight factor. The centre of the ship has weight factor 3, meaning that a compartment in this zone has a three times higher hit probability than a compartment in the aft zone. Similarly, the forward zone has weight factor 2.

### 4.3. Results

This section presents the results of the vulnerability assessment that is described in Sections 4.1 and 4.2. A distinction is made between a comparison of the different hit types in Paragraph 4.3.1 and the different powering concepts in Paragraph 4.3.2. A discussion and further interpretations are provided in Section 6. As explained, the method calculates the probability for each state after any given number of hits. Both concepts have 12 connections, resulting in $2^{12} = 4096$ states. These states have been clustered according to the required residual capacity after various impact levels. For low impacts, practically no loss of capability is accepted, while for high impacts some capabilities do not have priority any longer. In other words: the higher the impact level, the fewer residual capabilities are required. The different impact levels and their associated required residual capabilities are presented in Table 1. To ease the discussion of the results, a short qualitative term is provided for each level of required residual capability.

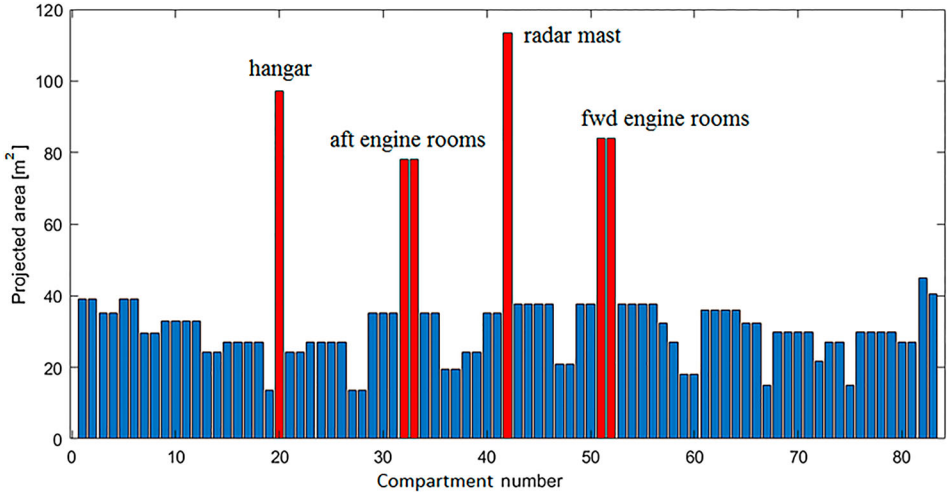



**Figure 8.** Projected lateral areas for all compartments.

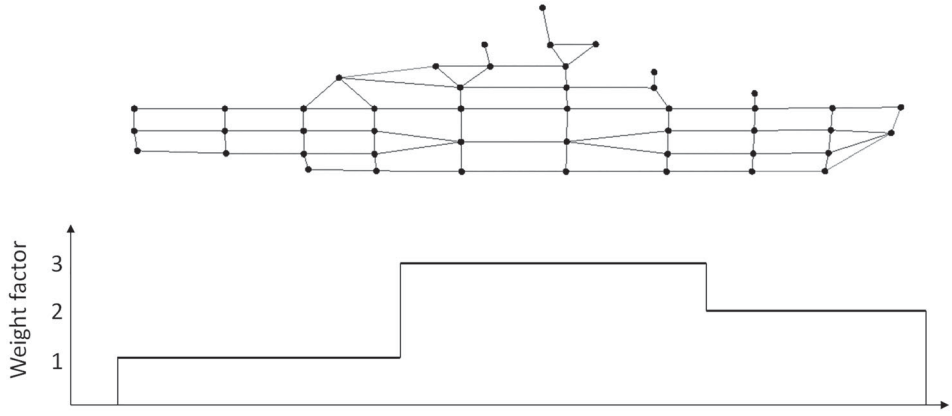



**Figure 9.** Weight factors for different longitudinal positions.

**Table 1.** Required residual capability for various impact levels.

| Impact level | Required residual capability | Qualitative term |
|---|---|---|
| Negligible | Offensive and defensive weapons, two-shaft propulsion | Full |
| Minor | Defensive weapon, two-shaft propulsion | Considerable |
| Medium | Defensive weapon, one-shaft propulsion | Moderate |
| Major | One-shaft propulsion | Minimal |

### *4.3.1. Comparision of hit types*

Figure 10 shows the results for the conventional concept. The increasing impact level is represented on the horizontal axis. This is done with an increasing number of hits, up to 8 hits. This hit scale should be seen as a way to represent different impact levels in an increasing order and is not related to the likelihood of actually encountering such numbers of hits. The general trend in the presented data indicates that higher residual capabilities have a lower probability of being available, which is in line with the expectations. The case with minimal residual capability clearly stands apart from the cases with higher residual capabilities. Furthermore, it can be seen that the step from moderate to considerable capability is slightly larger than from considerable to full capability. The differences between the different hit types (uniform, area, or zones) are not remarkably large. For the minimal residual capability, the zonal hit type shows the most optimistic results, though the difference with the uniform hit type is small. For the higher residual capabilities, the uniform hit type is more optimistic. The area hit type shows the most pessimistic results, except for the moderate residual capability.

Figure 11 shows a similar graph for the IFEP concept. The gap between minimal residual capability and the higher residual capabilities is still present, but it is smaller. Furthermore, the difference between moderate

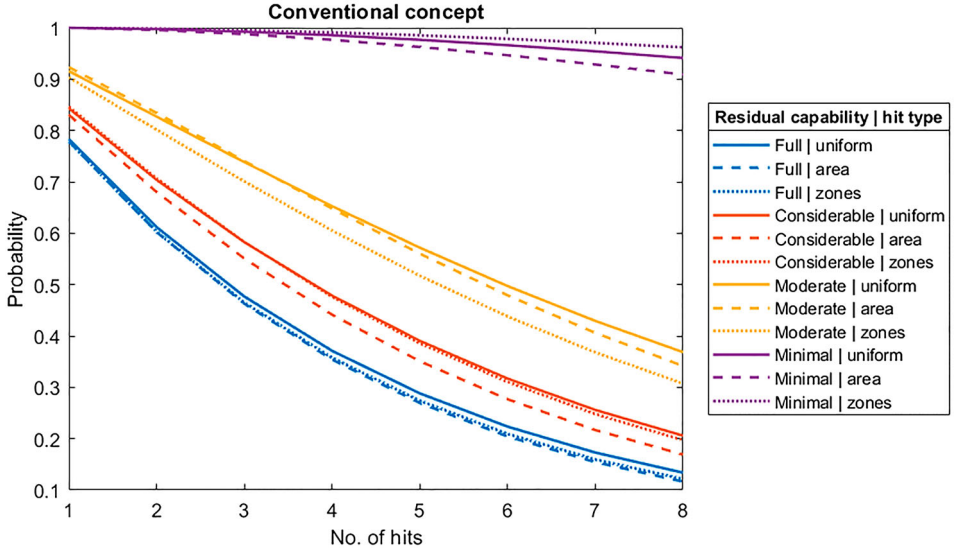



**Figure 10.** Probability of availability of main capabilities for the conventional layout.

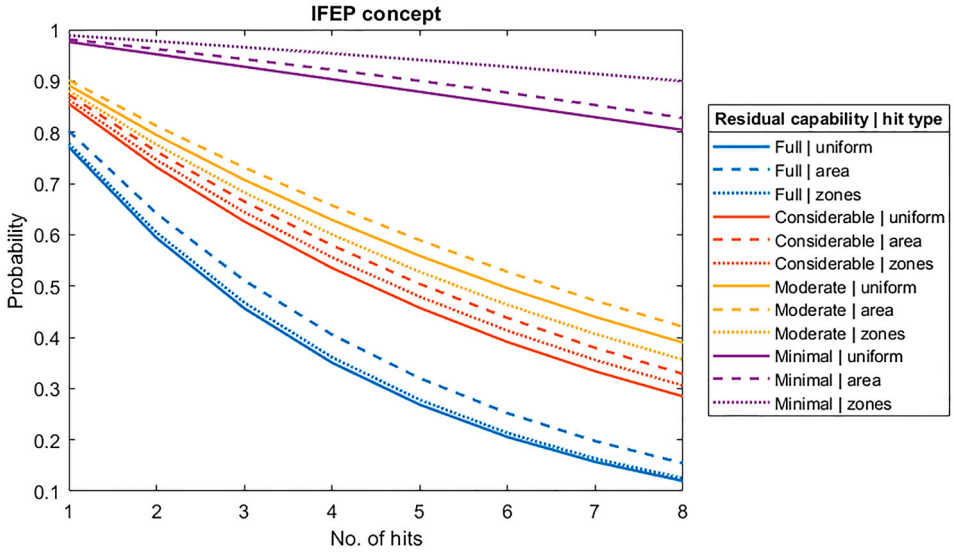



**Figure 11.** Probability of availability of main capabilities for the IFEP layout.

and considerable residual capability is remarkably small. Other than for the conventional layout, the area hit type yields more optimistic results than the uniform hit type. This holds for all residual capabilities. The zonal hit type leads to significant more optimistic results for the case with minimal residual capability. For other residual capabilities, the differences between the zonal hit type and other hit types are smaller.

These results can be linked to the actual areas and weight factors for both concepts. For the conventional concept, there are relatively many connections in compartments with an area that is above average. This results in higher hit probabilities for these connections, yielding more pessimistic results than the uniform approach. For the IFEP concept it is the other way around: many connections are located in relatively small compartments, yielding more optimistic results than the uniform hit type. The results of the zonal hit type are quite similar to the uniform hit type, apart from the minimal residual capability case. This case only requires propulsion at one side. Since the connections required for propulsion are mostly located at the aft, where the hit probability is smaller, the zonal hit type yields more optimistic results. The comparison between these or other hit types considers the interplay between vulnerability and susceptibility. The uniform hit type can be thought of as a general indication of the distributed system vulnerability of a concept, whereas comparing any other hit type with the uniform hit type gives an indication of the vulnerability given a susceptibility context.

### *4.3.2. Comparison of powering concepts*

In addition to comparing the results of different hit types for a given concept, such as in Figures 10 and 11, it also possible to compare the results of the two concepts for a given hit type. Figure 12 presents these results. The curves represent the absolute difference between the two concepts. A positive difference indicates that the IFEP concept performs better, while a negative difference denotes a better performance of the conventional concept. The scale on the vertical axis denotes the absolute difference of the probability of having a capability available. For example, a value of +0.10 for a certain capability means that the IFEP concept has a 10% higher probability of having that capability available.

A fully comprehensive comparison between the two concepts requires an explicit mathematical formulation of these curves. This is not considered in this paper, but is recommended for future research, as described in more detail in Section 7. Nevertheless, an interpretation of the results can be made by relating the shape of the curves to the distributed systems networks and the layouts of the concepts. This provides an estimation of the reasons behind the differences in performance between the two concepts. These estimations are given below for the four levels of residual capability.

- *Minimal*: For this case, propulsion at one side is required. The conventional concept is better, because it requires significantly fewer compartments for propulsion than the IFEP concept. However, the area and zonal hit types enlarge the hit probability for the diesel engines and generators. Since the IFEP concept has an additional generator to account for this, it performs slightly better for these hit types, compared to the uniform hit type. Nevertheless, it does not outweigh the disadvantage of the larger number

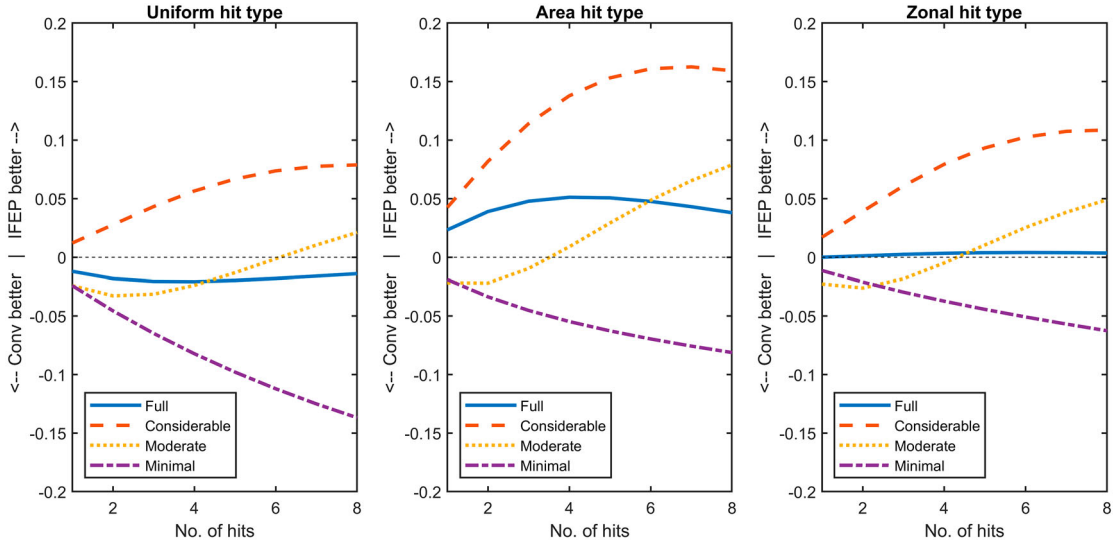



**Figure 12.** Difference in probability of availability of main capabilities for the both layouts, calculated with the area hit type.

of compartments that are needed, and thus the conventional concept is still preferred.

- *Moderate*: For this case, the CIWS is needed, in addition to propulsion at one side. The conventional concept has redundant chilled water supply for the CIWS. This gives the preference to this concept for low numbers of hits. However, the redundant chilled water routings run through a considerable number of compartments. For higher numbers of hits, these are likely to be hit, eliminating the advantage of the conventional concept. Instead, the IFEP concept is preferred for such numbers of hits.
- *Considerable*: For this case, all end users except for the high energy weapon are required. In the IFEP concept this weapon is strictly isolated from the remaining systems. The routings for the remaining systems systems run through 20 compartments in this concept. In the conventional concept, the high energy weapon is not isolated, and the routings for the remaining systems run through 26 compartments. Hence, the compartments for the remaining systems are significantly less likely to get hit for the IFEP concept, which gives the preference to this concept.
- *Full*: For this case, all end users are required. For the uniform hit type, the conventional concept performs better. This could be because of the low number of compartments taken up by the propulsion system and the redundancy in chilled water for the CIWS. For the area hit type the compartments with diesel engines or generators are significantly more likely to get hit. For the IFEP concept the supplier-part of the logical architecture is more flexible (2 out of 3 generators may be lost without losing full capability), giving the preference to the IFEP concept for this hit type. The same applies for the zonal hit type, but in this case the differences between the weight factors are not as strong as for the area hit type.

With this comparison, it can be seen that the IFEP concept mostly performs better when high residual capabilities are required, which is associated with low impact levels. For minimal residual capability, usually required after more severe impact, the conventional concept performs better. In other words, the IFEP concept could be described as 'performs well for most damage situations, but is has less residual capability in severe situations'. The conventional concept could be described as 'is likely to have minimal capability with severe damage, but is less able in withstanding small damage'. These results are not meant to provide a decisive answer to the question whether the conventional concept or the IFEP concept is better; that is up to the naval staff and the designers. However, these results help in making this decision, by quantifying the consequences of choosing one concept over the other.

## 5. Chilled water distribution test case

It has been noted in Section 4.1 that the logical architectures that can be used for the method are limited to 13 edges. At the same time, it can be desired to perform a vulnerability assessment on a higher detail level as the OPV test case discussed in Section 4. This can be achieved by considering a smaller part of the logical architecture, but in more detail. To illustrate this, this section provides a test case where the vulnerability of the chilled water distribution system of the conventional concept of the OPV is assessed in more detail. Compared to the OPV test case, more system components and routings are included. This comes at the cost of removing

other parts of the logical architecture, such as electrical power and mechanical propulsion power. As such, information on the performance of the logical architecture as a whole is lost. In other words, a balance needs to be made between the overall completeness and the level of detail.

In addition to the different logical architectures, the test case of this section also differs from the OPV test case in the way in which damage is modelled. Previously, damage was associated with physical locations in the ship, representing damage as a result of enemy weapon deployment, i.e. a man-made hostile environment. However, Sections 1 and 2 have identified that vulnerability can also exist due to increased complexity of distributed systems, potentially resulting in unexpected or unknown failures. Such types of failures are not necessarily associated with physical locations in the ship. As such, this test case uses a logical architecture (without any information on physical locations our routings) instead of a physical solution.

### 5.1. Distributed systems layout

This test case considers the chilled water supply and distribution to the same two weapon systems as the OPV test case: the defensive close-in weapon system (CIWS) and the offensive high energy weapon (HEW). The CIWS is assumed to be more critical than the HEW. Chilled water to both weapon systems is supplied by two chilled water plants ( CWPs) and distributed via two chilled water hubs (CW hubs). Yet, the supply of chilled water to both weapon systems is not sufficient to operate them. The weapon systems also need other resources, such as data. Though data is not within the scope of this test case, the components associated with data supply need to receive chilled water as well. This means that the logical architecture of the chilled water distribution system also contains a sensor mast (SM), two PC rooms (PC) and a command and information centre (CIC). Hence, the logical architecture consists of 10 nodes.

Two versions of connecting the 10 nodes are compared. These are adapted from de Vos (2018), and presented in Figure 13. In the first one, the connectivity of the nodes is low. Every node is supplied by only one other node, except for the CIWS, which has a redundant connection because it is considered critical. In the second version the connectivity is high. The SM, CIC and CIWS are all supplied by two connections. In addition to that, forward and back connections between the CW hubs have been established. In the case of a chilled water distribution system, a hub can be considered as a main pipeline (de Vos 2018). As such, the version with high connectivity is an initial step towards modelling a zonal distribution with the main pipeline as hub–hub connection, while the version with low connectivity resembles a radial distribution. It is acknowledged that the version that resembles the zonal distribution does not fully compare to other examples of zonal distributions, for example provided by Doerry (2006). However, if multiple logical architectures of the high connectivity type are linked together, a more complete representation of the full ship can be realised. This allows for more detail in the distributed systems, while maintaining the benefit of smaller individual logical architectures of the separate zones. This is not considered in the present paper, but the high connectivity version of the logical architecture for the chilled water distribution system is considered a useful contribution to this test case.

### 5.2. Test case set-up

Similar to the OPV test case, the logical architecture in this test case is subject to events that cause loss of capability. However, the term 'hit' is not used for this test case, as the capability loss is no longer associated with physical damage resulting from hits. Instead, the more generic term 'failure' is used. It is assumed that one failure occurs at every time step in the Markov chain. In addition to

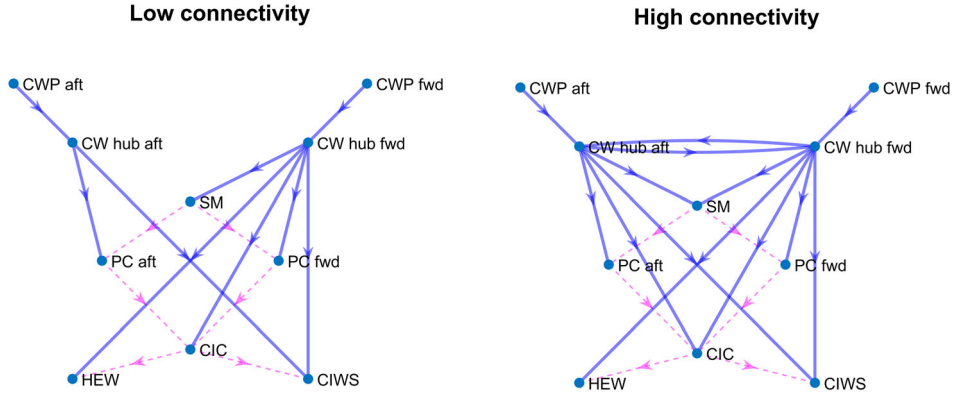



**Figure 13.** Two logical architectures for the chilled water distribution system, adapted from de Vos (2018). The dotted lines in magenta represent the data network, which is not considered in this test case, but which should be supplied with chilled water.

that, a failure is assumed to encompass one connection in the logical architecture at the time. Also, connections that have failed previously are not subject to further failure. For example: three failures represents the loss of three distinct connections in the logical architecture. Contrary to the OPV test case, no weight factors are used. For the low connectivity version, the number of edges is 9. Hence, there are 512 states, so **s** has a length of 512, and $T$ has a size of $512 \times 512$. The high connectivity version has 13 edges, resulting in 8192 states, and the associated size for the state vector and transition matrix.

### 5.3. Results

The results of the test case can be visualised in a similar way as the OPV test case. The residual capabilities are different. A distinction has been made for both offensive and defensive residual capability, only defensive residual capability, and only offensive residual capability. The results are presented in Figure 14. It can be seen that for both connectivity versions, the probability for both defensive and offensive capability is the lowest. This is in line with the expectations, as this is the most demanding residual capability. The probability for defensive residual capability is higher than for offensive residual capability. This illustrates that adding the redundant routing to the CIWS has indeed the intended effect.

When the low and high connectivity versions are compared, it can be seen that the high connectivity version performs better, which is also in line with the expectations. An interesting difference between the two is the shape of the curves. The curves for low connectivity have a concave shape right from the first failure, while the curves for high connectivity first have a convex shape. As a result, the advantage of the high connectivity version over the low connectivity version is most distinct for two to four failures. This is further illustrated by Figure 15. These results can be linked to the logical architectures. In the low connectivity version, every connection except for the supply to the CIWS is non-redundant, causing rapid loss of capability when one of them is lost. The high connectivity version can first rely on redundant routings, which results in delay of this effect.

The previous results consider capability that is still left after failure. Another interesting perspective is to consider what is not left. This is the same as the inverse of the previous curves but provides another perspective on the availability of the residual capabilities. For example, the probability for defensive and offensive residual capability for the low connectivity version becomes zero at the fourth failure. This means that the combination of offensive and defensive residual capability is definitely not available for four or more failures. However, this says nothing about the minimum number of failures that is needed to loose the combination of these capability. In other words: in order to identify the worst-case scenario (in this case: both defensive and offensive capability lost), the perspective on capabilities needs to be mirrored. This is done in Figure 16. It can be seen that for the low connectivity version the probability for the worst-case scenario is indeed 1 for four hits or more. However, also for fewer hits a considerable probability for the worst-case scenario exists, starting at over 40% for only one hit. For the high connectivity version the probability for the worst-case scenario starts lower, increases less steep, and becomes 1 at a higher number of hits compared to the low connectivity version. The values for these curves are the sum of a subset of individual state probabilities. A more detailed investigation of this subset can identify which

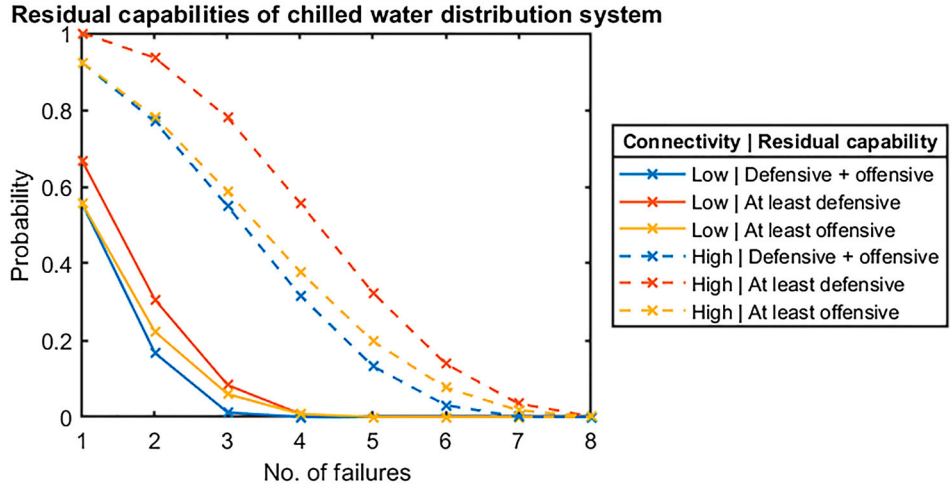



**Figure 14.** Probability of availability of the main capabilities for the chilled water distribution plant.

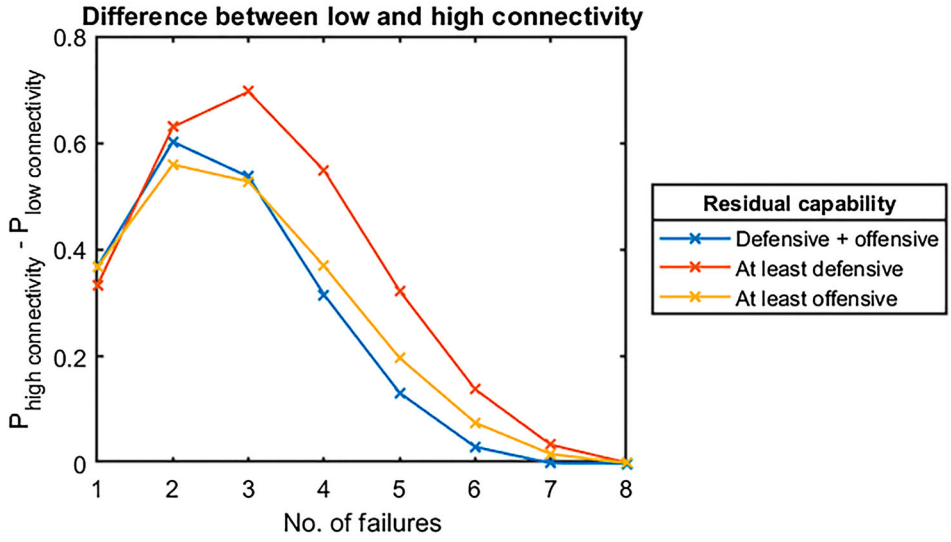



**Figure 15.** Difference in the probability of availability between the high and low connectivity architectures, in favour of the high connectivity version.

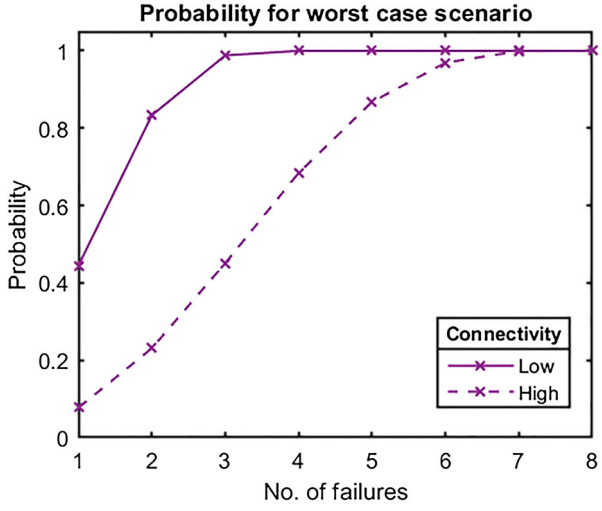



**Figure 16.** Probability for the worst-case scenario for the high and low connectivity architectures.

actual states contribute to the worst-case scenario, and how they can be avoided.

## 6. Conclusion

This paper has presented ongoing developments of a new method for assessing vulnerability of on-board distributed systems in the early design stage. The method has been illustrated with two test cases. A key feature of this method is its ability to evaluate residual capability for complex failure scenarios. This aligns with the observation that modern naval ships are not only vulnerable because of the hostile environment they operate in, but also because of the increasing complexity and opacity of their distributed systems. The ability to assess complex failure scenarios is an addition to the current body of work in vulnerability research, as most existing methods consider failure or damage scenarios that are defined or known upfront. However, the increased complexity of the failure scenarios comes at the cost of a reduction in the complexity of the logical architecture and/or physical solution. This currently limits the new method to a very rough description of the distributed systems layout, or a more detailed description of a subset of the distributed systems. Hence, the new method has explored a new scope for vulnerability assessments, but the desired scope has not yet been achieved. As such, further research in this field is recommended.

A second key feature of the new method is the quantitative nature of the results. In addition to rules of thumb or design guidelines, that for example state that systems for a given capability need to be duplicated, concentrated, isolated, and/or separated, the new method also gives information on how much the vulnerability reduces by doing so, without relying on more detailed computations that are usually applied in later design stages. Furthermore, it can be derived from the shape of the curves how the availability of a main capability behaves when failure increases. Capabilities with convex curves are likely to become unavailable for higher failure levels, whereas capabilities with concave curves are more likely to be come unavailable for lower failure levels. This can for example be used for identifying trade-offs and prioritising capabilities.

## 7. Recommendations

The method presented in this paper is part of an ongoing research effort. Further development of the method is therefore proposed. As described in Sections 3 to 5, the physical architecture, logical architecture, and physical solution are assumed to be available for this method. Other methods exist that can provide this. For example, the logical architecture can be developed with automatic topology generation (de Vos and Stapersma 2018), and the physical solution can be made with an optimisation algorithm (Duchateau et al. 2018). These methods, along with the method explained in this paper, are developed to be self-contained methods. However, integration of these methods may facilitate a more integrated approach on early stage design of on-board distributed systems. Further research in this area is recommended, both from a rather fundamental design theory perspective, as well as from a more practical, mathematical perspective. An initial discussion on this topic has recently been provided by Habben Jansen et al. (2019), but opportunities are left for further maturation of this topic.

Another topic for further research is the definition of availability of capabilities. In its current form, the method assumes that a capability is available if there is a connection in between a supplier and a user in the logical architecture. In practise, there also needs to be sufficient flow and effort at the right time. Similarly, the availability of a redundant routing in itself is not sufficient to ensure that a capability remains available, as reconfigurability efforts (either by the crew or by smart systems) are needed as well. Further research in how to incorporate this may increase the meaningfulness of the method. Yet, the method in its current form already provides valuable information, as connectivity, though not sufficient, is a necessary condition. In the very earliest design stages, this may be important to investigate first because if no connectivity can be ensured, there is no need to perform flow capacity or reconfigurability assessments.

Finally, it is envisioned that this method can be used for developing concepts, rather than only for assessing concepts. This way, the search for less vulnerable concepts can become more targeted, and is no longer limited by the concepts that were developed by the designer upfront. This may be achieved with the mathematical representation of the ship with the transition matrix of the Markov chain. Currently, the transition matrix is derived from an existing ship model. However, it may also be possible to apply this the other way around: use the transition matrix to obtain a promising concept. This requires a more in-depth study of the transition matrix, using linear algebra theory such as eigenvalue properties. With this mathematical evaluation, the vulnerability curves may be expressed as explicit equations, giving the designer a better understanding of which systems or connections contribute to the vulnerability. This enables the designers to generate new concepts in a more targeted fashion, ultimately leading to concepts that are less vulnerable and better understood.

## Disclosure statement

No potential conflict of interest was reported by the authors.

## Funding

Funding for this research is provided by Ms. Kelly Cooper from the United States Office of Naval Research (ONR) [grant number N00014-15-1-2752].

## ORCID

*A. A. Kana* http://orcid.org/0000-0002-9600-8669
*J. J. Hopman* http://orcid.org/0000-0002-5404-5699

## References

Boulougouris E, Papanikolaou A. 2013. Risk-based design of naval combatants. Ocean Eng. 65:49–61.
Brefort D, Shields C, Habben Jansen A, Duchateau E, Pawling R, Droste K, Jaspers T, Sypniewski M, Goodrum C, Parsons M, et al. 2018. An architectural framework for distributed naval ship systems. Ocean Eng. 147:375–385.
Brown D. 1991. The future British surface fleet. London: Conway Maritime Press.
Chalfant J. 2015. Early stage design for electric ship. Proc IEEE. 103(12):2252–2266.
Cramer A, Sudhoff S, Zivi E. 2011. Performance metrics for electric warship integrated engineering plant battle damage response. IEEE Trans Aerosp Electron Syst. 47(1):634–646.
de Vos P. 2018. On early-stage design of vital distribution systems on board ships [PhD thesis]. Delft University of Technology, Delft.
de Vos P, Stapersma D. 2018. Automatic topology generation for early design of on-board energy distribution systems. Ocean Eng. 170:55–73.
de Vos P, Stapersma D, Duchateau E, van Oers B. 2018. Design space exploration for on-board energy distribution systems: a new case study. Proceedings of the 17th International Conference on Computer and IT Applications in the Maritime Industries (COMPIT '18); Pavone. p. 463–481.
Doerry N. 2006. Zonal ship design. Naval Eng J. 118(1):39–53.
Doerry N. 2007. Designing electrical power systems for survivability and quality of service. Naval Eng J. 119:25–34.
Duchateau E, de Vos P, van Leeuwen S. 2018. Early stage routing of distributed ship service systems for vulnerability reduction. 13th International Marine Design Conference; Helsinki.
Erkel A, Luyten J, Galle L. 2002. TNO-PML developments of blast resistant doors and walls. Proceedings of the RTO Applied Vehicle Technology Panel (AVT) Symposium; Aalborg.

Goodfriend D, Brown A. 2017. Exploration of system vulnerability in naval ship concept design. J Ship Prod Des. 33(3):1–17.

Goodrum C, Shields C, Singer D. 2018. Understanding cascading failures through a vulnerability analysis of interdependent ship-centric distributed systems using networks. Ocean Eng. 150:36–47.

Gortney W. 2010. Dictionary of military and associated terms, as amended through February 2016. United States Department of Defense. Technical report.

Habben Jansen A, de Vos P, Duchateau E, Stapersma D, Hopman J, van Oers B, Kana A. 2019. A framework for vulnerability reduction in early stage design of naval ship systems. Proceedings of the Intelligent Ships Symposium; Philadelphia, PA.

Habben Jansen A, Duchateau E, Kana A. 2018a. Towards a novel design perspective for system vulnerability using a Markov chain. Proceedings of the 14th International Naval Engineering Conference; Glasgow.

Habben Jansen A, Kana A, Hopman J. 2018b. An approach for an operational vulnerability assessment for naval ships using a Markov model. Proceedings of the 13th International Marine Design Conference; Helsinki.

Heywood M, Lear T. 2006. PREVENT – a tool to reduce vulnerability early in the design. Proceedings of Warship 2006; London.

Jung J, Liu C, Tanimoto S, Vittal V. 2002. Adaptation in load shedding under vulnerable operating conditions. IEEE Trans Power Syst. 17(4):1199–1205.

Kim K, Lee JH. 2012. Simplified vulnerability assessment procedure for a warship based on the vulnerable area approach. J Mech Sci Technol. 26(7):2171–2181.

Lay D. 2006. Linear algebra and its applications. 3rd ed. Boston, MA: Pearson Education.

Logan K. 2007. Intelligent diagnostic requirements of future all-electric ship integrated power system. IEEE Trans Ind Appl. 43(1):139–149.

Menis R, da Rin A, Vicenzutti A, Sulligoi G. 2012. Dependable design of all electric ships integrated power system: guidelines for system decomposition and analysis. Electrical Systems for Aircraft, Railway and Ship Propulsion; Bologna: IEEE.

Pei Y, Song B, Han Q. 2006. A generic calculation model for aircraft single-hit vulnerability assessment based on equivalent target. Chinese J Aeronaut. 19(3):183–189.

Schofield J. 2009. SURVIVE and SURVIVE lite – survivability assessment from concept to operational support. Proceedings of the American Society of Naval Engineers Day; Baltimore, MD.

Schuddebeurs J. 2014. De-risking integrated full electric propulsion (IFEP) vessels using advanced modelling and simulation techniques [PhD thesis]. University of Strathclyde, Glasgow.

Shields C, Rigetrink D, Singer D. 2017. Investigating physical solutions in the architectural design of distributed ship service systems. Ocean Eng. 135:236–245.

Surma Ltd. 2018. SURMA survivability analysis [online]. http://survivability.fi/surma/demo/. Accessed June 2019.

TNO. 2018. RESIST Lite [online]. https://www.tno.nl/media/1644/resist_lite.pdf. Accessed June 2019.

Trapp T. 2015. Shipboard integrated engineering plant survivable network optimization [PhD thesis]. Massachusetts Institute of Technology, Cambridge, Massachusetts.

van Oers B, van Ingen G, Stapersma D. 2012. An integrated approach for the design of survivable ship services systems. Proceedings of the International Naval Engineering Conference (INEC); Edinburgh.