Towards a novel design perspective for system vulnerability using a Markov chain

Habben Jansen, Agnieta; Duchateau, Etienne; Kana, Austin

DOI
10.24868/issn.2515-818X.2018.028

Publication date
2018

Document Version
Final published version

Published in
Proceedings of the 14th International Naval Engineering Conference & Exhibition (INEC)

Towards a novel design perspective for system vulnerability using a Markov chain

Ir. A C Habben Jansen[a*], Dr. Ir. E A E Duchateau[b], Dr. A A Kana[a]

[a]*Delft University of Technology, The Netherlands;* [b]*Defence Materiel Organisation, The Netherlands*

*Corresponding author. Email: A.C.HabbenJansen@tudelft.nl

Synopsis

In order to investigate to which extent naval ships can execute their operational scenario after damage, an early stage assessment of the vulnerability of distributed systems needs to be carried out. Such assessments are currently mostly done by evaluating the performance of predefined concepts. However, such an approach does not necessarily lead to the most desirable solution, since solutions outside the scope of the designer's preconceived ideas or experience are inherently hard to investigate. This paper therefore proposes several steps towards an approach that enables a vulnerability assessment that is independent of predefined concepts. This is done by incorporating several additions to an existing system vulnerability approach developed by the authors, using a Markov chain. With this approach there is no longer a need for modelling individual hits or damage scenarios. Whereas the approach has previously been shown in concept, this paper introduces three improvements that contribute to the applicability of the approach: 1) it is scaled up in order to model a larger number of compartments and distributed systems, 2) the hit probabilities for different compartments can be adjusted, and 3) it is shown how the availability of main ship functions can be derived from the availability of individual connections. A test case that compares two powering concepts (conventional and full electric powering) of a notional Oceangoing Patrol Vessel (OPV) is provided to illustrate the principles behind the improvements. From the results the two main contributions of this paper can be obtained: 1) the possibility to assess the system vulnerability for different levels of required residual capacity at different impact levels, and 2) and the quantitative nature of the results, aiding ship designers and naval staff with understanding the consequences of various concepts on the system vulnerability.

Keywords: Vulnerability; Distributed systems; Early stage design; Markov chain

1 Introduction

Due to the hostile environment in which naval ships operate, survivability is one of the key aspects that needs to be considered during the design. Survivability is known as 'the capability of a ship and its shipboard systems to avoid and withstand a weapons effects environment without sustaining impairment of their ability to accomplish designated missions' [12]. Survivability for naval ships is usually expressed as the combination of three sub-categories: susceptibility, vulnerability and recoverability. Susceptibility is the inability of a ship to avoid being damaged. Vulnerability refers to the inability of a ship to withstand damage mechanisms from one or more hits. Recoverability addresses the ability of a ship and its crew to prevent loss and restore essential functions, given one or more hits [ibid.]. Susceptibility and vulnerability are mainly informed by characteristics of the ship itself, e.g. signatures, self-defensive measures, and redundancy of equipment, and can be addressed during the design of the ship. Recoverability is mostly determined by active response on board, such as firefighting and reconfiguration of systems, though some design choices may affect recoverability as well [11]. This paper addresses the assessment of the vulnerability of two main functions of the ship, 'fight' and 'move', from a distributed systems perspective.

1.1 Vulnerability reduction of distributed systems

Various measures for vulnerability reduction exist, such as damage containment by zoning, redundancy and separation of systems, and protection with blast-resistant materials. The purpose of most of these measures is to obtain an intelligent layout, which is in general deemed the most effective protective measure [4]. With the increasing focus towards automation and electrification of naval ships, the extent to which a layout is intelligent is largely determined by the layout and routing of the ship's distributed systems, i.e. systems that manage and distribute electrical power, flow of liquids, and data among critical weapons, communication systems, sensors,

Authors' Biographies

Ir. Agnieta Habben Jansen is a PhD candidate in the field of early stage naval ship design at the Maritime & Transport Technology department of the Delft University of Technology. Prior to her PhD project she carried out both her BSc and MSc education in Maritime Technology at the same university.

Dr. Ir. Etienne Duchateau holds the position of Naval Architect at the Maritime Systems Division of the DMO. He is involved in design tool development and concept exploration studies for future replacement and newbuilding projects of the Royal Netherlands Navy. In 2011 Etienne graduated as Naval Architect at Delft University of Technology. In 2016 he obtained his PhD also at Delft University of Technology for his research on an interactive steerable concept exploration tool for early stage ship design.

Dr. Austin Kana is an Assistant Professor in the Maritime & Transport Technology Department at Delft University of Technology. His research is on developing techniques to aid early stage ship design activities. His received his PhD from the University of Michigan in 2016 in Naval Architecture and Marine Engineering.

 http://doi.org/10.24868/issn.2515-818X.2018.028

and platform systems. The extent to which these systems can meet their requirements needs to be assessed and maximised during the design of the ship, also for damaged situations [3], [6].

There are various existing methods and tools that address the vulnerability of distributed systems, such as the ones discussed in [7]. 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 detailed systems design and layout. However, early stage assessments of the vulnerability of distributed systems are necessary as well, for keeping up with varying requirements and concepts in this stage, and for preventing costly and time-consuming design modifications in later design stages. Though several early stage tools exist as well, the common procedure remains with first generating one or more concepts, and then analysing the performance of these concepts [6]. Hence, the vulnerability assessment tools, including those meant for early design stages, are more analysis methods rather than design aids, precluding the designer from realising potentially better solutions that he or she had not thought of earlier. Furthermore, vulnerability has an interrelated nature, i.e. layout, systems design, and routing all affect each other. This makes it difficult for the designer to take the possible effect of often changing concept designs on vulnerability into account during the early design stages. Approaches that enable vulnerability assessments without predefined concepts are therefore worth further investigation.

1.2 Vulnerability in early stage design

An important goal of the early design stage is to find out what is wanted, and whether this is technically and economically feasible. Since this currently can only be addressed through physically realisable design solutions, generating and analysing concepts is required in this design stage [1]. However, current vulnerability tools provide results for predefined concepts or requirements. Concepts that are not defined can inherently not be analysed. Hence, the concept with the most appropriate vulnerability characteristics may be outside the part of the design space that has been investigated by the designer.

To obtain a better understanding of the design space, in this case the design space of vulnerability of distributed systems in particular, a different, more general approach may be beneficial. Such an approach should be based on identifying universal responses to damage rather than analysing the damage response of previously generated concepts. It could help designers to understand vulnerability characteristics of concepts a priori, rather than after analysis of predefined concepts that have been developed using existing preferences. An example of such an approach in structural dynamics is considering the response of a mass-spring system in the frequency domain instead of the time domain, where knowledge about the response of the system can be obtained without having actual values for the mass or the spring. Though ship design is fundamentally different from the design of a mechanical system based on laws of physics [2], an approach analogous to this mass-spring example can be beneficial to ship designers as well: in order to find out what is preferred, there is no longer a need for analysing concepts that already included the designer's preconceptions.

With an approach that has previously been developed by the authors [9], the damage scenario has been generalised, effacing the need for modelling individual hits. This approach assesses the vulnerability of distributed systems in naval ships using a Markov model. Since the damage scenario has been generalised, it is no longer necessary to simulate (a series of) individual hits. However, the approach has only been shown in concept, and needs further development. For that reason, this paper presents the following three improvements of the approach:

1. Scaling up in size: The method is scaled up to a larger concept, using a ship model and a larger number of distributed systems.
2. Hit probability: The possibility to enable a user-defined distribution of the hit probability is included.
3. Systems to functions: It is shown how the availability of main ship functions can be derived from the availability of individual systems.

The remainder of this paper is organised as follows. Section 2 gives a brief description of the approach, and an elaboration on the improvements of the approach. In Section 3 a test case with a notional Ocean-going Patrol Vessel (OPV) is presented. Section 4 provides the results of the test case. Conclusions are drawn in Section 5. Section 6 gives several recommendations for further research.

2 Approach

This section elaborates on how the vulnerability assessment approach has been set up previously, and which additions and modifications are now implemented. A proof-of-concept of the approach has been provided in [9], consisting of a conceptual example. This paper assumes the proof-of-concept as basis and builds further upon it. However, for the sake of completeness, a description of the proof-of-concept has been adapted from [9] and is included in the Appendix.

 http://doi.org/10.24868/issn.2515-818X.2018.028

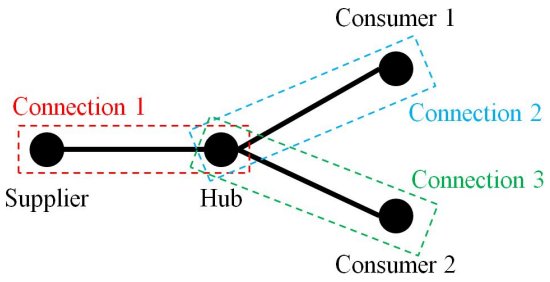

Figure 1: Definition of connections for the purpose of the vulnerability approach

2.1 Previous set-up of the approach

In the approach, the ship layout and the locations and routings of distributed systems, which are still assumed to be available from the concept, are modelled with a Markov chain. A Markov chain is suited for describing various conditions of a system, and the transitions between them, over time. The key elements of a Markov chain are the state vector and the transition matrix. The state vector gives the probabilities for the system to be in a certain state. In the case of the vulnerability assessment, 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, of which the contents become unavailable when they get hit. This is modelled with the transition matrix. The following assumptions apply to the vulnerability assessment:

- All systems can be either on or off.
- At each time step, one hit occurs, disabling one compartment.
- All compartments have equal hit probability at each time step.
- Once a system is off, it cannot be repaired.

The results of the approach affirm the necessity for an integrated approach, in which the vulnerability of all distributed systems is assessed simultaneously. Furthermore, it has 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 or operational overlap. However, several improvements are needed to increase the applicability of the approach for a more practical environment. To that end, three adjustments are made, which have already briefly been mentioned in Section 1. These are discussed now in more detail.

2.2 Scaling up in size

Previously, the approach has been demonstrated with two systems, both consisting of a supplier, a consumer, and a connection 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. The total number of states then becomes 2^{n_s}, where n_s is the number of systems. The size of the transition matrix inherently becomes $2^{n_s} \times 2^{n_s}$. This is however not representative for a distributed systems network on an actual ship, where components and/or connections may be redundant, and where one or multiple hubs, e.g. electrical switchboards, valve chests or data switches may be located between the supplier and the consumer [5]. Furthermore, some components may be part of multiple distributed systems, such as a chilled water plant, 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 1. 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 is not clear whether a node is at the beginning or at the end of a connection, such as 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 just one connection. The same applies to other nodes that are part of multiple connections. Another option is to consider all nodes and connections separately as individual components that can be on or off. However, this quickly increases the size of the computation. For this example, it results in assessing 7 components instead of 3 connections.

Compared to the proof-of-concept, which evaluated a small layout with nine compartments, the number of compartments is expected to increase 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.

 http://doi.org/10.24868/issn.2515-818X.2018.028

2.3 Hit probability

When a compartment gets hit, a transition to another state may occur, depending on what is located inside that compartment. Though the approach 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 approach, the weight factors must be scaled in such way that the sum of all elements of each row in the transition matrix equals 1 [10]. 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 1:

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

From this, Equation 2 can be derived:

$$\sum w_1 \ldots w_{n_c} = n_c \tag{2}$$

Any combination of values that complies with the scaling approach of Equation 2 can be used within the vulnerability approach. 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 3.

2.4 Systems to functions

In Paragraph 2.2 it is explained why systems need to be broken down in individual connections to apply the vulnerability approach on a larger scale. However, the eventual question is whether critical functions can still be executed after hits, rather than which systems or connections are still available. 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 electric energy. This subtle, but important different perspective requires a transition from thinking in systems or connections to thinking in functions. These main functions may for example be fight, move, and float, which can be further broken down in sub-functions, such as offensive and defensive fighting, if necessary.

It may sound contradictory that there is a need for thinking in high-level functions, while Paragraph 2.2 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 1 again. Let us assume that Consumer 1 and Consumer 2 both are self-defence systems, for example CIWSs. If a hit occurs that disables Connection 2, while Connections 1 and 3 remain available, the capability ‘self-defence’ is still available. However, if Connection 2 becomes disabled while Connection 3 already was disabled, the capability ‘self-defence’ is lost. Hence, in order to properly assess the availability of functions, individual connections are still needed.

To make the transition from connections to functions, states of the Markov chain that contribute to a function need to be clustered and added together. Logical relations should be taken into account while doing this. For example, the function ‘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.

3 OPV test case

In order to demonstrate the improvements to the approach, 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 [7]. A network visualisation of the model is presented in Figure 2.

3.1 Distributed systems layout

The main functions ‘fight’ and ‘move’ are considered in this test case. ‘Fight’ has two sub-functions: offensive and defensive. These sub-functions are provided by an offensive high-energy weapon (HEW) and a defensive

 http://doi.org/10.24868/issn.2515-818X.2018.028

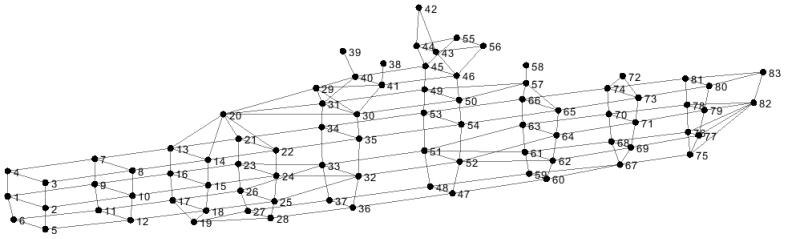

Figure 2: Layout of the notional OPV used for the test case. Each node represents the geometric centre a compartment. Each edge denotes a physical adjacency between compartments, i.e. the compartments are located on both sides of the same deck or bulkhead.

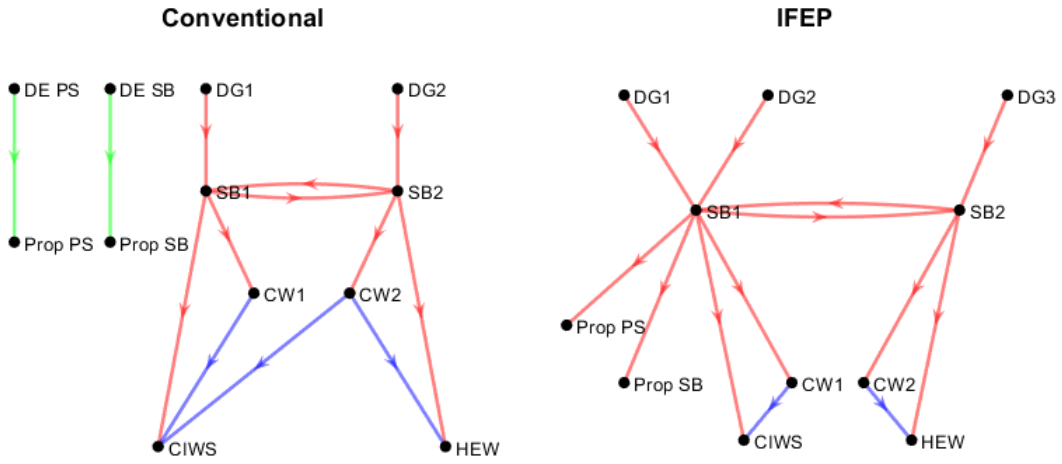

Figure 3: Distributed systems networks for the two powering concepts, with mechanical energy (green), electrical energy (red) and chilled water (blue).

close-in weapon system (CIWS). The function '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.

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 networks of these powering concepts are visually presented in Figure 3. Figure 4 shows these networks located inside the ship.

3.2 Test set-up

With the improvements to the method and layout of the ship and its networks available, the improved vulnerability approach 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 1 and 2 is used. The projected lateral areas of the compartments, which are required for Option 2, are presented in Figure 5. The variety in projected lateral areas can clearly

 http://doi.org/10.24868/issn.2515-818X.2018.028

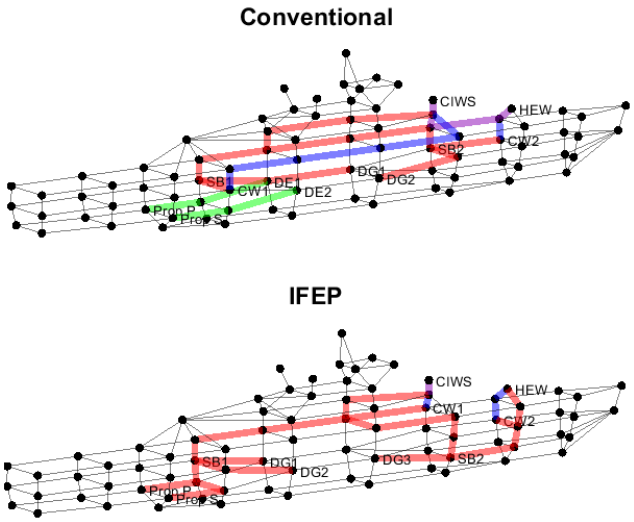

Figure 4: The layout of the two distributed systems networks in the notional OPV. Purple lines represent routings of *both* chilled water and electricity through the same compartments.

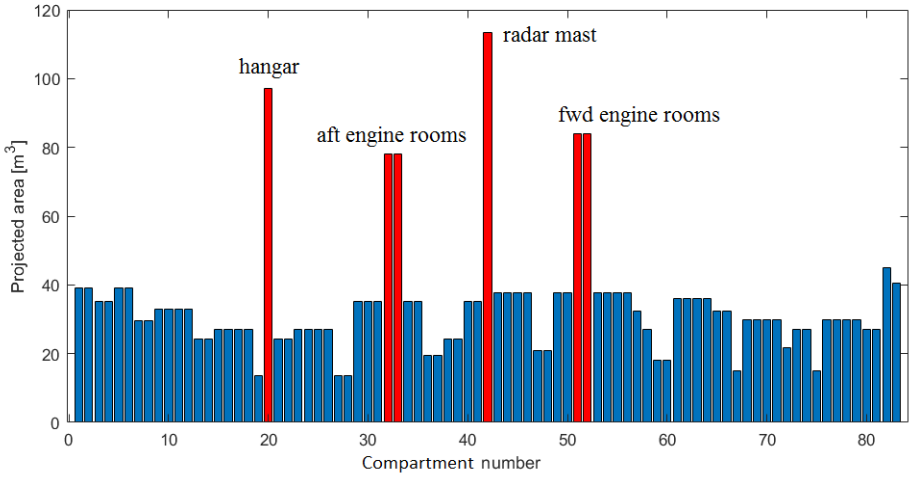

Figure 5: Projected lateral areas for all compartments

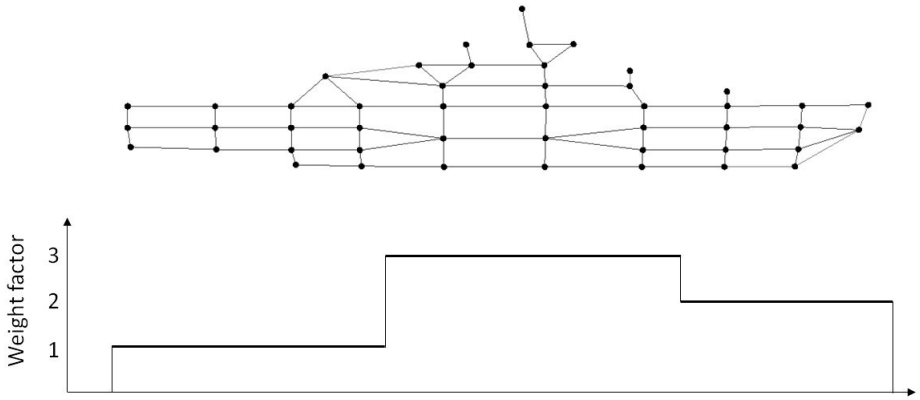

Figure 6: Weight factors for different longitudinal positions

 http://doi.org/10.24868/issn.2515-818X.2018.028

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 6. 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 Results

This section presents the results of the vulnerability assessment that is described in Sections 2 and 3. A discussion and further interpretations are provided in 5. As explained, the approach calculates the probability for each state after any given number of hits. Both powering 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 given for each level of required residual capability.

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

Figure 7 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 what could be expected. It is remarkable to see that the case with minimal residual capability stands apart from the cases with higher residual capability. 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 that large. For the minimal residual capability, the zonal hit type shows the most optimistic results, though the difference with the uniform type is small. For the higher residual capabilities, the uniform hit type is more optimistic. The area-based hit type shows the most pessimistic results, except for the moderate residual capability.

Figure 8 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 and considerable residual capability is remarkably small. Other than for the conventional layout, the area-based 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.

In addition to comparing the results of different hit types for a given concept, such as in Figures 7 and 8, it also possible to compare the results of the two concepts for a given hit type. Figure 9 does this for the area hit type. The results show that the IFEP concept performs better - that is, has a higher probability of availability - for considerable and full residual capability. The probability to have considerable residual capability is particularly high for the IFEP concept. Moderate residual capability is more likely to be available for the conventional concept at low impact levels. For high impact levels, the IFEP concept is more likely to have moderate residual capability available. For minimal residual capability, the conventional layout performs better at any impact level.

5 Conclusion and discussion

From the results of Section 4 several conclusions can be drawn, with regard to both the specific test case as well as the development of the approach in general. In the test case the distributed system vulnerability of two powering concepts, a conventional concept and an IFEP concept, was tested. When the results of the two concepts are compared, it can be seen that the IFEP concept performs better when high residual capabilities are required. This

 http://doi.org/10.24868/issn.2515-818X.2018.028

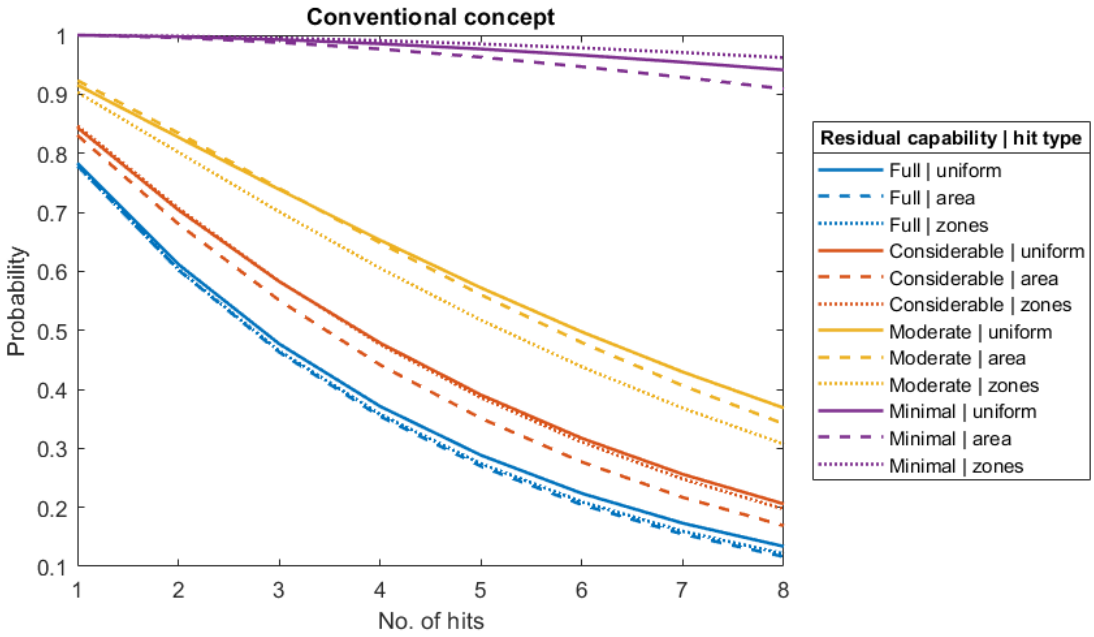

Figure 7: Probability of availability of main functions for the conventional layout

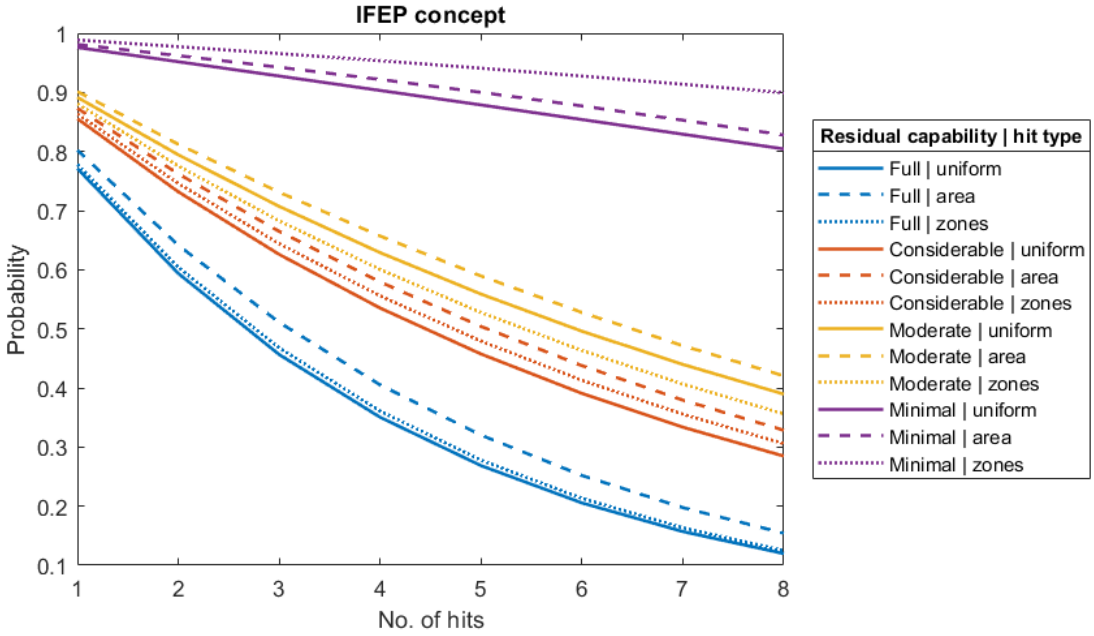

Figure 8: Probability of availability of main functions for the IFEP layout

 http://doi.org/10.24868/issn.2515-818X.2018.028

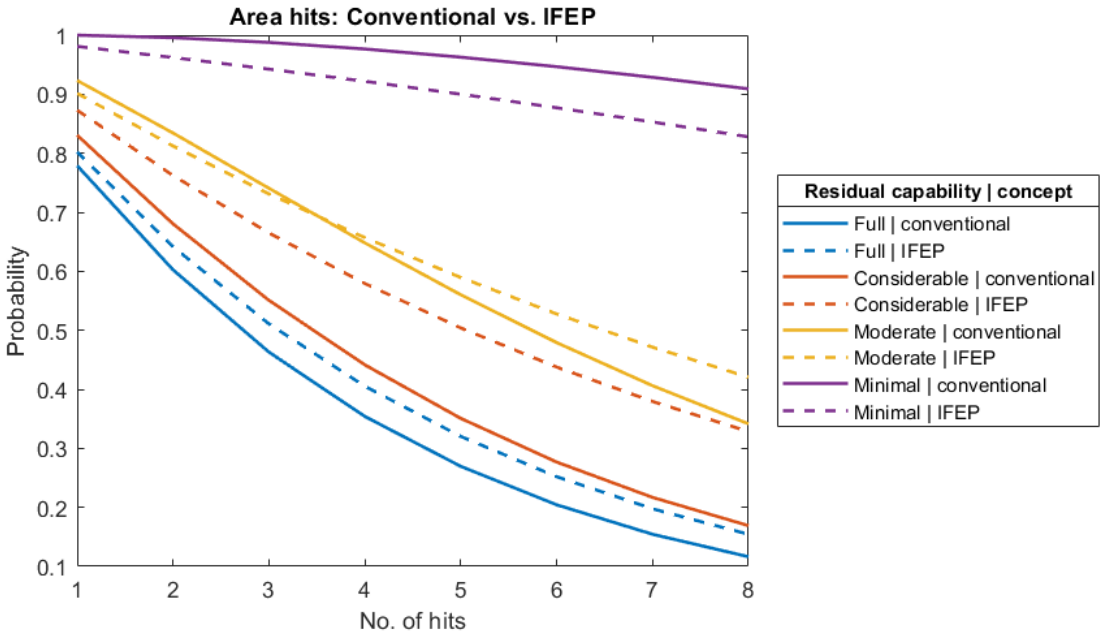

Figure 9: Probability of availability of main functions for the both layouts, calculated with the area hit type

is usually the case at 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 *the* 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 do help in making this choice, by quantifying the consequences of choosing one concept over the other.

The effect of different hit types (uniform, area, or zonal) has been investigated as well. Some effect is noticed, though the differences between the hit types are not major. For the conventional concept, there are relatively many connections in compartments with an area 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 system vulnerability of a concept, whereas comparing any other hit type with the uniform hit type quantifies the influence gives an indication of the vulnerability *given* a susceptibility context.

The previous conclusions apply to the test case specifically. Yet, some general lessons can be leaned as well. The approach shows to be suited to provide quantitative figures on the vulnerability of main ship functions for different impact levels. These different impact levels are considered to be a valuable contribution. Some present approaches, e.g. [7] and [8], apply network percolation, where damage is simulated by systematically disabling all compartments, and their associated equipment and connections. This quickly increases the computational effort for multiple hits (the effort increases exponentially with the number of simulated hits), limiting the applicability of such methods to one- or two-hit scenarios. The approach presented in this paper considers any number of hits in any location and does not face this problem. It needs to be pointed out, however, that the present approach quickly increases in computational effort for large numbers of connections. It is therefore well suited for many impact levels and few connections, but less suited for few impact levels and many connections.

The quantitative nature of the results is considered as another benefit of the present approach. In addition to rules of thumb or design guidelines, that for example state *that* systems for a given main function need to be duplicated, concentrated, isolated, and/or separated, the present approach also gives information on *how much* the vulnerability of the main function reduces by doing so. Furthermore, it can be derived from the shape of the curves how the availability of a main function behaves when damage increases. Functions with convex curves are likely

 http://doi.org/10.24868/issn.2515-818X.2018.028

to become unavailable for higher impact levels, whereas functions with concave curves are more likely to be come unavailable for lower impact levels. This can for example be used to prioritise sub-functions of the main functions 'fight' and 'move'.

6 Recommendations

The approach presented in this paper is part of an ongoing research effort. Further development of the approach is therefore proposed. As mentioned in Section 1, an early stage design approach that is detached from preconceived concepts is envisioned. Though the present paper describes how the damage scenario can be generalised, the approach still uses an existing ship layout and distributed systems network. Describing the ship model in a more generic fashion is therefore regarded as the indispensable next step. 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 potentially also be possible to apply this the other way around: use the transition matrix to obtain a layout of the ship. This requires a more in-depth study of the transition matrix, using general linear algebra theory such as eigenvalue properties. If such an approach turns out to be fruitful, the need for generating concepts in the early design stage may be reduced. This may help designers in getting a better understanding of what is wanted, and a better, non-confined view of the design space.

Disclaimer

The opinions presented in this paper are the personal opinions of the authors and the authors alone. Specifically, they do not represent any official policy of The Netherlands Ministry of Defence, the Defence Materiel Organisation, or the Royal Netherlands Navy. Furthermore, the results presented in this paper are for the sole purpose of illustration and may not have an actual relation with any past, current, or future warship procurement project at the Defence Materiel Organisation.

Acknowledgements

Funding for this research is provided by Ms. Kelly Cooper from the United States Office of Naval Research (ONR) under grant no. N00014-15-1-2752, and is gratefully acknowledged. Furthermore, the authors would like to thank the Defence Materiel Organisation of the Dutch Ministry of Defence for their in-kind contribution to this research.

References

[1] D.J. Andrews. Marine requirements elucidation and the nature of preliminary ship design. *International Journal of Maritime Engineering*, 153(23), 2011.

[2] D.J. Andrews. Art and science in the design of physically large and complex systems. *Proceedings of the Royal Society A*, 468:891–912, 2012.

[3] D.C. Brefort, C.P.F. Shields, A.C. Habben Jansen, E.A.E. Duchateau, R.J. Pawling, K. Droste, T. Jaspers, M. Sypniewski, C. Goodrum, M. Parsons, M. Yasin Kara, M. Roth, D.J. Singer, D.J. Andrews, J.J. Hopman, A. Brown, and A.A. Kana. An Architectural Framework for Distributed Naval Ship Systems. *Ocean Engineering*, 147:375–385, 2018.

[4] D.K. Brown. *The future British surface fleet*. Conway Maritime Press, London, 1991.

[5] P. de Vos. On the application of network theory in naval engineering - Generating network topologies. In *International Naval Engineering Conference*, Amsterdam, 2014.

[6] R. Dougal and D. Langland. Catching it early - Modeling and simulating distributed systems in early stage design. *SNAME Marine Technology*, pages 63–69, 2016.

[7] E.A.E. Duchateau, P. de Vos, and S. van Leeuwen. Early stage routing of distributed ship service systems for vulnerability reduction. In *13th International Marine Design Conference*, Helsinki, 2018.

[8] C.J. Goodrum, C.P.F. Shields, and D.J. Singer. Understanding cascading failures through a vulnerability analysis of interdependent ship-centric distributed systems using networks. *Ocean Engineering*, 150:36–47, 2018.

[9] A.C. Habben Jansen, A.A. Kana, and J.J. Hopman. An approach for an operational vulnerability assessment for naval ships using a Markov model. In *Proceedings of the 13th International Marine Design Conference*, Helsinki, 2018.

[10] D.C. Lay. *Linear Algebra and Its Applications*. Pearson Education, Boston, 3rd edition, 2006.

[11] A. Piperakis and D.J. Andrews. A comprehensive approach to survivability assessment in naval ship design. *International Journal of Maritime Engineering*, 154, 2012.

[12] M. Said. Theory and Practice of Total Ship Survivability for Ship Design. *Naval Engineers Journal*, 107(3):191–203, 1995.

 http://doi.org/10.24868/issn.2515-818X.2018.028

Appendix

This appendix contains a brief description of the proof-of-concept of the vulnerability assessment approach presented in this paper. The appendix aims to demonstrate the mathematical set-up of the approach. Additional information and more elaborate interpretations are given in [9].

Consider a square grid with 3 x 3 compartments. The grid contains two different systems, system A and system B. The routings of systems A and B occupy three and four compartments, respectively. The routings cross each other in one compartment. A visualisation of this conceptual layout is shown in Figure 10.

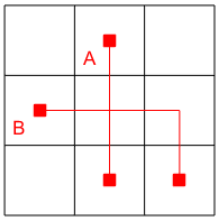

Figure 10: Visualisation of conceptual layout

Both systems can either be on or off. This results in four possible states for the availability of systems:

- State s_1: A and B are both on
- State s_2: only A is on
- State s_3: only B is on
- State s_4: both systems are off

Hence, state vector s has length 4, and transition matrix T has size 4×4. In the initial state all systems are on, so:

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

The transition matrix is dependent on the layout. The nine compartments are referred to with the abbreviations of the compass card (N, E, S, W, their intermediate directions, and center compartment C). From the initial state, the NW, NE and SW compartments can be hit without affecting system A and/or B. Hence, the probability for staying in s_1 is $3/9$. If the W, E or SE compartment is hit, only system A stays on, so the probability for transferring to s_2 is $3/9$. Similarly, if the N or S compartment is hit, only system B stays on, so the probability of transferring to s_3 is $2/9$. If the C compartment is hit, both systems go off, so the probability of transferring to s_4 is $1/9$. These numbers fill the first row of T.

The subsequent rows of T can be filled in a similar fashion. The starting state is now assumed to be s_2. In that situation only system A is on. This state implies that either compartment W, E, SE or multiple of them are already off. Returning to s_1 is not possible, because no repair of systems is assumed. Going to s_3 is also not possible, since system B is off. It is possible to stay in s_2. This happens if compartment NW, NE or SW is hit (no systems in those compartments) or if compartment W, E or SE is hit (any of those compartments has already been hit anyway). In other words, the probability for staying in s_2 is $6/9$. There is also a probability to transfer to s_4, if compartment N, C or S gets hit, i.e. a probability of $3/9$. The third row of T can be filled likewise. The fourth row represents the state where all systems are down. If that state is reached, it cannot be left, because under the current assumptions no repair of systems is considered. T therefore becomes as follows:

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

The probabilities for each state at each given time step can now easily be determined with:

$$s^k = s(0) \cdot T^k$$

In this equation, k is the number of time steps, i.e. the number of hits. The results of this assessment are visualised in Figure 11.

 http://doi.org/10.24868/issn.2515-818X.2018.028

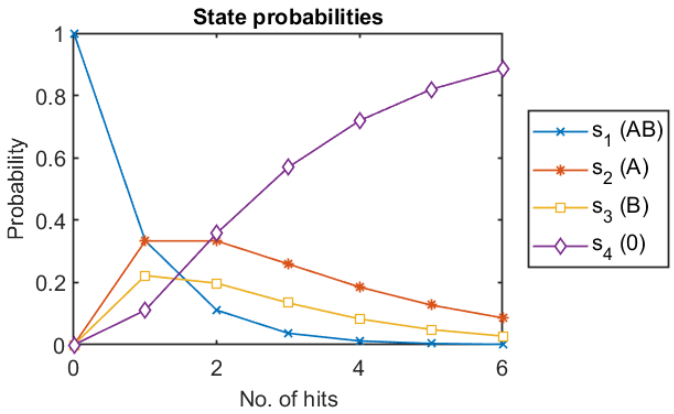

Figure 11: Results of the vulnerability assessment of the conceptual layout

 http://doi.org/10.24868/issn.2515-818X.2018.028