# A Markov-based vulnerability assessment of distributed ship systems in the early design stage

Habben Jansen, Agnieta

**DOI**
10.4233/uuid:f636539f-64a5-4985-b77f-4a0b8c3990f4

**Publication date**
2020

**Document Version**
Final published version

**Citation (APA)**
Habben Jansen, A. (2020). *A Markov-based vulnerability assessment of distributed ship systems in the early design stage*. [Dissertation (TU Delft), Delft University of Technology]. https://doi.org/10.4233/uuid:f636539f-64a5-4985-b77f-4a0b8c3990f4

# Propositions

accompanying the thesis

## A Markov-based vulnerability assessment of distributed ship systems in the early design stage

of
A.C. Habben Jansen
September 1$^{st}$, 2020
Delft University of Technology

1. The fact *that* systems are placed together on one ship already relates them from the viewpoint of vulnerability. This even holds if the systems are not physically or logically related. (This dissertation)
2. During concept exploration it is more useful to obtain guidance towards *less* vulnerable concepts, than to find *the least* vulnerable concept. (This dissertation)
3. When balancing scholarliness and usefulness in ship design research, the decisive factor should always be usefulness. (This dissertation)
4. In order to design a ship, one first needs to design a ship.
5. The way in which scientific research is set up, focussing on a unique contribution, inherently hinders collaboration with other researchers.
6. Naval ship design is no different than the popular TV shows 'Say yes to the dress' or 'Droomhuis gezocht' (Dutch for 'Wanted: dream home'): all are about the acquisition of an affordable, feasible, and relevant product.
7. The cause of traffic jams in The Netherlands is stubbornness, not cars.
8. Mankind needs to save itself, rather than the planet.
9. The true value of an orchestra lies behind the music.
10. The best metric for the effectiveness of a naval ship (and other defence materiel) is the number of shots *not* fired.

These propositions are considered opposable and defendable and have been approved as such by the promotors prof. ir. J.J. Hopman and dr. A.A. Kana.

# Stellingen

behorende bij het proefschrift

## A Markov-based vulnerability assessment of distributed ship systems in the early design stage

van
A.C. Habben Jansen
1 september 2020
Technische Universiteit Delft

1. Het feit *dat* systemen samen op één schip zijn geplaatst, relateert ze al aan elkaar vanuit het oogpunt van kwetsbaarheid, zelfs als ze geen fysieke of logische relatie met elkaar hebben. (Dit proefschrift)
2. Tijdens conceptexploratie is het nuttiger om richting te vinden naar *minder* kwetsbare concepten, dan om *het minst* kwetsbare concept te vinden. (Dit proefschrift)
3. Bij het afwegen van wetenschappelijke vooruitgang en praktisch nut tijdens onderzoek op het gebied van scheepsontwerp moet praktisch nut altijd de doorslaggevende factor zijn. (Dit proefschrift)
4. Om een schip te ontwerpen, moet je eerst een schip ontwerpen.
5. De aard van wetenschappelijk onderzoek, waarbij wordt gefocust op een unieke bijdrage, hindert inherent samenwerking met andere onderzoekers.
6. Het ontwerpen van marineschepen is niet anders dan de populaire tv-programma's 'Say yes to the dress' of 'Droomhuis gezocht': allen gaan over het verwerven van een betaalbaar, haalbaar, en relevant product.
7. De oorzaak van files in Nederland is niet auto's, maar koppigheid.
8. De mensheid moet zichzelf redden, niet de planeet.
9. De echte waarde van een orkest bevindt zich achter de muziek.
10. De beste maatstaf voor de effectiviteit van een marineschip (en ander defensiematerieel) is het aantal schoten dat *niet* wordt gelost.

Deze stellingen worden opponeerbaar en verdedigbaar geacht en zijn als zodanig goedgekeurd door de promotoren prof. ir. J.J. Hopman en dr. A.A. Kana.

# A Markov-based vulnerability assessment of distributed ship systems in the early design stage

# A Markov-based vulnerability assessment of distributed ship systems in the early design stage

## Proefschrift

ter verkrijging van de graad van doctor
aan de Technische Universiteit Delft,
op gezag van de Rector Magnificus prof. dr. ir. T.H.J.J. van der Hagen;
voorzitter van het College voor Promoties,
in het openbaar te verdedigen op
dinsdag 1 september 2020 om 12:30 uur

door

**Agatha Christiana HABBEN JANSEN**

scheepsbouwkundig ingenieur, Technische Universiteit Delft, Nederland,
geboren te Alphen aan den Rijn, Nederland

Dit proefschrift is goedgekeurd door de promotoren.

Samenstelling promotiecommissie:

| | |
|---|---|
| Rector Magnificus | voorzitter |
| Prof. ir. J.J. Hopman | Technische Universiteit Delft, promotor |
| Dr. A.A. Kana | Technische Universiteit Delft, copromotor |

Onafhankelijke leden:

| | |
|---|---|
| Prof. dr. ir. P.H.A.J.M. van Gelder | Technische Universiteit Delft |
| Prof. dr. F.M. Brazier | Technische Universiteit Delft |
| Prof. dr. S.O. Erikstad | Norwegian University of Science and Technology |
| Prof. dr. A.J. Brown | Virginia Polytechnic Institute and State University, USA |

Overige leden:

| | |
|---|---|
| Dr. ir. E.A.E. Duchateau | Defensie Materieel Organisatie |

This research was funded by the United States Navy Office of Naval Research under grant no. N00014-15-1-2752. The views expressed in this dissertation are those of the author and do not reflect the social policy or position of the United States Navy or the United States Government.

*Keywords:* early stage ship design, vulnerability reduction, Markov chain, eigenvalues

Cover design by: Vera van Beek | ProefschriftMaken

Published by: ProefschriftMaken, The Netherlands

ISBN: 978-94-6384-145-0



An electronic version of this dissertation is available at:
`https://repository.tudelft.nl/`

*"He that will not sail till all dangers are over, must never put to sea."*

Thomas Fuller (1608-1661)
English clergyman and writer

# Contents

**Summary** **iii**

**Samenvatting** **vii**

**1 Introduction** **1**

1.1 Nature of early stage ship naval design . . . . . . . . . . . . . . . . . . . . 2
1.2 Vulnerability reduction of naval ships . . . . . . . . . . . . . . . . . . . . 7
1.2.1 Definitions of survivability . . . . . . . . . . . . . . . . . . . . . . 9
1.2.2 Vulnerability reduction of distributed systems . . . . . . . . . . . 10
1.3 Research objective and scope . . . . . . . . . . . . . . . . . . . . . . . . 13
1.4 Outline of the dissertation . . . . . . . . . . . . . . . . . . . . . . . . . 14

**2 A review of ship design and vulnerability methods** **15**

2.1 *What* to design versus *how* to design . . . . . . . . . . . . . . . . . . . 15
2.2 Review of methods for overall ship design . . . . . . . . . . . . . . . . . 19
2.3 Review of vulnerability reduction . . . . . . . . . . . . . . . . . . . . . . 25
2.3.1 General considerations for ship vulnerability reduction . . . . . 25
2.3.2 Methods for ship vulnerability reduction . . . . . . . . . . . . . 28
2.3.3 Methods for assessing vulnerability in other fields . . . . . . . . 33
2.4 Gap analysis . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 34
2.5 Selecting a mathematical approach . . . . . . . . . . . . . . . . . . . . . 37

**3 Early stage vulnerability assessment method** **41**

3.1 Mathematical principles of Markov theory . . . . . . . . . . . . . . . . . 41
3.2 Set-up of the method . . . . . . . . . . . . . . . . . . . . . . . . . . . . 43
3.3 Method computations . . . . . . . . . . . . . . . . . . . . . . . . . . . . 44
3.4 Method results . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 47
3.5 Extended features of the method . . . . . . . . . . . . . . . . . . . . . . 50
3.5.1 Scaling up in complexity . . . . . . . . . . . . . . . . . . . . . . . 51
3.5.2 Hit probabilities . . . . . . . . . . . . . . . . . . . . . . . . . . . 52
3.5.3 Systems to capabilities . . . . . . . . . . . . . . . . . . . . . . . . 52
3.5.4 Automatic generation of the transition matrix . . . . . . . . . . 54
3.6 Eigenvalue analysis . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 55
3.7 Method summary . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 57

**4 Test case: Oceangoing Patrol Vessel** **59**
4.1 Test case set-up . . . 59
4.2 Hit type assessment . . . 63
4.2.1 Comparison of hit types . . . 65
4.2.2 Comparison of concepts . . . 67
4.2.3 Conclusion . . . 69
4.3 Capability trade-off assessment . . . 69
4.3.1 Conventional concept . . . 70
4.3.2 IPS concept . . . 74
4.3.3 Conclusion . . . 75
4.4 Verification and validation . . . 77

**5 Integration of the method into early stage design** **83**
5.1 Management of design knowledge . . . 83
5.2 Relation of method to other early stage vulnerability methods . . . 87
5.2.1 Method integration framework . . . 87
5.2.2 Work flow for early stage design of distributed systems . . . 91
5.2.3 Computational integration . . . 92
5.3 Final considerations for design knowledge . . . 95

**6 Extended opportunities of the method** **99**
6.1 Separate residual capability levels . . . 99
6.2 Hits vs. failures . . . 104
6.3 Level of detail in logical architectures . . . 106
6.4 Closing remarks . . . 110

**7 Conclusions** **111**
7.1 Conclusions . . . 111
7.2 Contributions . . . 113
7.3 Societal context and impact . . . 114
7.4 Recommendations . . . 115

**References** **119**

**Acknowledgements** **129**

**Curriculum Vitae** **131**

**Publications** **133**

# Summary

Naval ships are designed to operate, survive, and win in hostile environments. In such environments, there is a probability that a ship gets damaged, either due to warfare activities or due to other risks, such as collisions or fires. Though this probability may not always be large, it is definitely present. In some cases, damage is unavoidable. As such, vulnerability reduction is a major point of attention that needs to be considered during the design of a naval ship. Various measures can be taken to reduce the vulnerability. Traditionally, the focus has been on damage stability and structural integrity. These topics continue to be highly relevant today, but ongoing developments in electrification, automation, and digital transformation in (naval) ship design have expanded the scope of vulnerability reduction to the perspective of on-board distributed systems. These are the systems that supply and distribute vital resources, such as electricity, chilled water, and data, to critical systems, such as radars, weapon systems, and propulsion systems. The availability of distributed systems has become equally important as the traditional naval architecture disciplines in vulnerability reduction of naval ships.

The most important design decisions for distributed systems, such as which system components to include, where to locate them, and how to connect them, are made during the early design stage. At this stage, there is limited design information available for making these decisions. At the same time, these decisions have a major influence on the vulnerability, as well as on other performance characteristics, such as cost. In order to overcome these challenges, an adequate design process is needed, including suitable methods and tools.

Early stage ship design can be subdivided in concept exploration and concept definition. During concept exploration, the focus lies on identifying overall performance, trends, and trade-offs by exploring a vast set of solutions (i.e. ship concepts). Using the results from concept exploration, the design process converges to a limited number of alternative concepts, which are worked out in more detail during concept definition. At this stage, the focus lies on de-risking the concepts and identifying local performance and potential bottlenecks. Concept definition eventually results in a single concept that is used for defining a contract, and subsequently for detailed design and engineering. Where concept exploration focusses on obtaining knowledge, i.e. generalised understanding on *why* certain trends and trade-offs exist, concept definition focuses on information, i.e. quantifying actual parameters for specific concepts. This results in a challenge: generalised design knowledge is needed for generating feasible

specific concepts, while obtaining that knowledge also needs information from those specific concepts.

Various design methods, both for overall ship design and vulnerability reduction specifically, exist to support the design of survivable naval ships. However, they are in general less suited for obtaining the generalised design knowledge that is needed during concept exploration, as they are either high-fidelity and aimed at the detailed design stage, or provide a quantification of the vulnerability without identifying the underlying factors that lead to that level of vulnerability. As such, there is a need for an early stage design method that is meant for concept exploration, which elucidates the driving factors for vulnerability in a fast and generic fashion, and at a low level of detail. The knowledge that results from this method is intended to be used for obtaining design recommendations and directionality on how a concept can be improved, which serves as input for concept definition.

Following a further, in-depth gap analysis, a discrete-time Markov chain has been selected as the mathematical basis for the new method. This mathematical technique is based on linear algebra. It describes various conditions of a system (in this case: the ship) in a state vector and the probability that this condition changes after events (in this case: hits that result in damage) in a transition matrix. For the new vulnerability method, a compartment layout and a topology with the main system components (which is named *logical architecture* in this dissertation) are assumed to be available. A logical architecture is represented as a network with nodes and edges, where the nodes describe the system components, and the edges describe the connections between them. It is assumed that one hit occurs at each time step in the Markov chain. This hit disables one compartment, including any system components and/or routings that are located inside that compartment. Due to the probabilistic nature of the Markov chain, all hit scenarios are inherently considered at once. The associated computation provides the probability that individual connections are on or off after one or more probabilistically defined hits. The availability of individual connections is subsequently translated to the availability of higher-level capabilities.

The probability for the availability of the capabilities is presented in curves. These curves quantify the vulnerability of the ship. It has been found that, due to the mathematical set-up of the Markov chain, the shape of the curves is only dependent on the eigenvalues of the transition matrix. This also holds if the routing of the topology through the ship is changed. The same eigenvalues continue to be decisive for the vulnerability, only the actual numeric value changes. In other words: the eigenvalue formulation is generalised for all possible routings given a fixed logical architecture. Furthermore, the eigenvalues relate to specific connections in the logical architecture. Using this knowledge, direction towards other, better routings of the same logical architecture can be found through design recommendations.

The new method has been demonstrated with a test case of a notional Oceangoing Patrol Vessel (OPV). Two fundamentally different powering concepts have been tested: a conventional concept, with separate, mechanical propulsion, and an Integrated Power System (IPS), where both the propulsion power and the power for other users is electrical. The method has shown to be able to quantify the vulnerability by means of various curves of residual capability, highlighting the advantages and disadvantages of both concepts. Furthermore, guidance towards improvement for both concepts has been found by means of the eigenvalue assessment, that has provided design recommendations on which routings to concentrate and which components to relocate. The method also quantifies the interaction between different levels of residual capability, as improving one level may affect (either positively or negatively) other levels. Additionally, extended features of the new method have been explored, such as the opportunity to apply user-defined hit probabilities and the ability to consider other levels of detail of a topology.

The knowledge that the new method provides, has been compared to results that various other vulnerability methods provide. Combining various methods, an existing work flow for early stage design of distributed systems has been updated. The quality of this work flow is discussed in terms of design knowledge. Since design knowledge is highly subjective and unspecific, it is unlikely that early stage ship design and vulnerability reduction will ever have *definite* procedures and methods. Yet, that does not mean that these cannot be *useful*, which should be the driving factor for ship design research and practice.

# Samenvatting

Marineschepen worden ontworpen om te kunnen opereren, overleven, en winnen in vijandige omgevingen. In zulke omgevingen is er kans op schade aan het schip door oorlogsvoering of door andere risico's, zoals aanvaringen of brand. Deze kans is niet altijd groot, maar wel reëel, en soms is schade onvermijdelijk. Kwetsbaarheisreductie is daarom een belangrijk aandachtspunt tijdens het ontwerp van marineschepen. Verschillende maatregelen kunnen worden getroffen om de kwetsbaarheid te verminderen. Van oudsher heeft de focus vooral gelegen op lekstabiliteit en integriteit van de constructie. Deze onderwerpen blijven zeer relevant, maar recente ontwikkelingen in elektrische energievoorziening, automatisering en digitalisering hebben de focus van kwetsbaarheidsreductie uitgebreid naar distributiesystemen. Deze systemen voorzien vitale gebruikers, zoals radars, wapens, en voortstuwingssytemen van onder andere elektriciteit, koelwater, en data. De beschikbaarheid van distributiesystemen en de middelen waarin zij voorzien, is net zo belangrijk geworden voor kwetsbaarheidsreductie als de traditionele scheepsbouwdisciplines.

De belangrijkste ontwerpkeuzes voor distributiesystemen worden gemaakt tijdens het conceptontwerp. Dit betreft onder andere welke componenten geselecteerd worden, waar deze geplaatst worden in het schip, en hoe ze aan elkaar verbonden worden. Tijdens het conceptontwerp is er slechts beperkte ontwerpinformatie beschikbaar om deze keuzes te maken. Tegelijkertijd hebben deze keuzes een zeer grote invloed op de uiteindelijke kwetsbaarheid van het schip, net als op andere factoren, zoals kosten. Deze uitdaging vraagt om een adequaat ontwerpproces met passende ontwerpmethodes en (software)programma's.

Het conceptontwerpproces kan worden onderverdeeld in conceptexploratie en conceptdefinitie. Tijdens conceptexploratie ligt de focus op het bepalen van trends, ontwerpcompromissen, en algehele prestaties van het schip. Hiervoor wordt een uitgebreide set aan scheepsconcepten onderzocht. Met de resultaten van conceptexploratie convergeert het ontwerpproces naar een beperkt aantal alternatieve concepten, die tijdens conceptdefinitie in meer detail worden onderzocht. In deze fase ligt de focus op het verkleinen van de ontwerprisico's van de overgebleven concepten, en het identificeren van lokale (systeem)prestaties en potentiële knelpunten in het ontwerp. Conceptexploratie focust zich op het verkrijgen van kennis, dat wil zeggen: generiek begrip over *waarom* bepaalde trends en ontwerpcompromissen bestaan. Conceptdefinitie focust zich op informatie, dat wil zeggen: het daadwerkelijk kwantificeren van parameters voor specifieke concepten. Dit resulteert in een probleem: algemene

ontwerpkennis nodig is om geschikte specifieke concepten te genereren, terwijl deze concepten op hun beurt ook weer nodig zijn om die algemene kennis te vergaren.

Er bestaan verschillende ontwerpmethodes, zowel voor algeheel scheepsontwerp als voor kwetsbaarheidsreductie specifiek, die kunnen helpen bij het ontwerpen van robuuste schepen. Over het algemeen zijn deze methodes echter minder geschikt om de generieke ontwerpkennis te verkrijgen die tijdens conceptexploratie nodig is. Dit komt veelal doordat deze methodes te veel detail bevatten en bedoeld zijn voor het een later ontwerpstadium, of doordat de kwetsbaarheid gekwantificeerd wordt zonder dat de onderliggende factoren worden geïdentificeerd. Er is daarom behoefte aan een ontwerpmethode voor conceptexploratie die de belangrijskte factoren voor kwetsbaarheid bepaalt op een snelle en generieke manier, op een laag detailniveau. Met de kennis die zo'n methode oplevert, kunnen ontwerpaanbevelingen en sturing richting verbeterde concepten worden gevonden. Deze kunnen dienen als invoer voor conceptdefinitie.

Na een verdere analyse van deze kennisleemte is een discrete Markovketen geselecteerd als wiskundige basis voor de nieuwe methode. Deze wiskundige techniek is gebaseerd op lineaire algebra. Verschillende condities van een systeem (in dit geval: het schip) worden beschreven met een conditievector, en de kans dat deze condities veranderen na een bepaalde gebeurtenis (in dit geval: een wapeninslag die resulteert in schade) wordt beschreven met een transitiematrix. Om de methode te gebruiken, wordt aangenomen dat een basisplan van compartimenten en een topologie van de belangrijkste systeemcomponenten beschikbaar zijn (in dit proefschrift wordt zo'n topologie dit een *logical architecture* genoemd). Een topologie wordt weergegeven als een netwerk met knooppunten en bogen, waarbij de knooppunten staan voor de systeemcomponenten en de bogen voor de connecties tussen de componenten. Er wordt aangenomen dat er één wapeninslag plaatsvindt bij elke tijdstap in de Markovketen. Deze wapeninslag beschadigt één compartiment, inclusief de systeemcomponenten en routeringen die zich daarin bevinden. Omdat de Markovketen probabilistisch is, worden alle schadescenario's per definitie allemaal tegelijk beschouwd. De berekening geeft de kans dat individuele connecties wel of niet werken na één of meerdere probabilistisch gedefinieerde wapeninslagen. De beschikbaarheid van individuele connecties wordt vervolgens vertaald naar de beschikbaarheid van meer generieke capaciteiten van het schip als geheel.

De kans dat de capaciteiten beschikbaar zijn, wordt weergegeven in krommes. Deze krommes kwantificeren de kwetsbaarheid van het schip. Het blijkt dat de vorm van deze krommes alleen afhankelijk is van de eigenwaarden van de transitiematrix. Dit komt door de wiskundige eigenschappen van de Markovketen, en geldt ook als de routering van de topologie in het schip wordt veranderd. In dat geval blijven dezelfde eigenwaarden bepalend voor de kwetsbaarheid, slechts de daadwerkelijke numerieke waarden van de eigenwaarden veranderen. Met andere woorden: de formulering van de kwetsbaarheid als functie van de eigenwaarden is hetzelfde voor alle mogelijke routeringen voor een gegeven topologie. Daarnaast relateren de eigenwaarden aan specifieke connecties in de topologie. Met deze kennis kunnen ontwerpaanbevelingen worden opgesteld die leiden tot andere, betere routeringen van dezelfde topologie.

De nieuwe methode is getest met een testcase van een fictieve Oceangoing Patrol Vessel (OPV). Twee fundamenteel verschillende energieconcepten zijn getest: een coventioneel concept, met gescheiden mechanische voortstuwing, en een Integrated Power System (IPS), waar zowel het voorstuwingsvermogen als het vermogen voor andere gebruikers elektrisch is. Er is aangetoond dat de methode de kwetsbaarheid kan kwantificeren door middel van verschillende krommes van restcapaciteit. Hierbij worden de voordelen en nadelen van beide concepten uitgelicht. Daarnaast kan worden geïdentificeerd welke aanpassingen aan het concept kunnen worden gedaan om de kwetsbaarheid te verminderen. Dit wordt gedaan door middel van ontwerpaanbevelingen die beschrijven welke routeringen geconcentreerd moeten worden, en welke systeemcomponenten verplaatst moeten worden. De methode kwantificeert ook de interacties tussen de verschillende niveaus van restcapaciteit. Als één niveau verbeterd wordt, kunnen andere niveaus immers ook veranderen, dan wel op een positieve of negatieve manier. Daarnaast zijn enkele mogelijkheden voor verdere uitbreiding van de methode onderzocht. Dit omvat onder andere de mogelijkheid om van te voren te specificeren waar wapeninslagen waarschijnlijk zullen plaatsvinden, en de mogelijkheid om andere detailniveaus van de topologie te onderzoeken.

De kennis die de nieuwe methode oplevert, is vergeleken met resultaten die andere kwetsbaarheidsmethodes opleveren. Door enkele verschillende methodes te combineren met de nieuwe methode, is een bestaande procedure voor het conceptontwerp van distributiesystemen bijgewerkt. De kwaliteit van deze procedure is beschouwd in termen van ontwerpkennis. Aangezien ontwerpkennis een zeer subjectief en niet specifiek gedefinieerd begrip is, is het onwaarschijnlijk dat er ooit *sluitende* procedures en methodes voor conceptontwerp worden gedefinieerd. Dit neemt echter niet weg dat deze procedures en methodes niet *nuttig* kunnen zijn. Dit laatste is waar het uiteindelijk om draait bij het ontwerpen van schepen, zowel op onderzoeks- als praktijkgebied.

# Chapter 1

# Introduction

The sea has been of vital importance for mankind since ancient times. It allows us to trade, to discover the world, and to harvest natural resources, such as fossil fuels or, more recently, future-proof alternatives such as solar and wind power. However, equally common and old as maritime transport is the activity of naval warfare. In 1210 BC the Hittites, a people that lived in the area where Turkey is located nowadays, conquered the Cypriots with their naval fleet, which is said to be the first naval battle in recorded history (Mark, 2018). As time progressed, warships became larger and more sophisticated. By the $17^{th}$ century the Dutch Republic had a considerable navy, whose ships were mainly deployed for the Anglo-Dutch Wars. It happens to be that the *Slag bij Ter Heijde* (see Figure 1.1), the famous naval battle where Admiral Maarten Tromp lost his life, took place a mere kilometre away from the place of residence of the author of this dissertation. Though the times of these enthralling but grievous naval battles are long gone, the possibility that modern naval ships find themselves in hostile situations remains.

**Figure 1.1:** The *Slag bij Ter Heijde*, painted between 1653-1666 by Jan Abrahamsz. van Beerstraten, displayed in the Rijksmuseum in Amsterdam

Parts of this chapter are based on Habben Jansen et al. (2019, 2020b).

In order to ensure that naval ships can operate and survive in hostile environments, vulnerability reduction is a major point of attention that needs to be considered during the design. However, many other key factors are involved as well, such as seaworthiness, operational effectiveness, and cost. More often than not, some of these key factors impose conflicting design requirements. It is simply impossible to acquire the ship with the most advanced weapon systems, sailing at the highest speed, having the best self-defence measures, for the lowest cost. In other words: naval ship design is strongly characterised by making trade-offs (e.g. Andrews, 2011; van Oers et al., 2018). Especially during the early design stages of a naval ship, this can result in major challenges for the ship designer. In this stage he or she needs to make important design decisions, such as which powering concept to select, or which weapon systems to include. The consequences of these decisions have a strong influence on the final performance and cost of the ship. Yet, they need to be made with limited information, as barely any plans or arrangements are available in the early design stage, and if any, they are of very limited detail (Duchateau, 2016, p. 5). In order to overcome these challenges, the naval ship designer needs an adequate and thoughtfully developed design process, including suitable methods and tools.

Many existing tools and methods for ship design focus on *what* a particular performance of the ship is, but do not directly reveal *why* the performance is as it is. This makes it difficult for the designer to identify important trade-offs and underlying driving factors, and to obtain guidance for improvement of the design, which is needed to develop a satisfactory solution during concept design. For that reason, this dissertation aims to develop an early stage design method that both assesses the performance of a ship and identifies the reasons behind that performance. In other words, it addresses both the *what* and the *why* in early stage ship design. This method has specifically been developed within the context of vulnerability reduction, as this is a key factor that applies to naval ships in particular.

This chapter first discusses the nature of early stage naval ship design in Section 1.1, which needs to be understood before the new method can be developed. The same holds for the field of vulnerability reduction of naval ships, which is discussed in Section 1.2. The research objective and scope are outlined in Section 1.3. The outline of the remainder of this dissertation is given in Section 1.4.

## 1.1 Nature of early stage ship naval design

The early stage design challenge of making high-impact decisions with limited information and resources does not limit itself to naval ship design, but is a known issue to engineering design in general, such as discussed by e.g. Ostergard et al. (2016) for design of buildings and Renzi et al. (2017) for the automotive industry. The challenge has previously been captured by Mavris and DeLaurentis (2000) in a well known and often used generic design timeline, of which an adapted version is presented in Figure 1.2. It clearly shows that the design freedom is large in the early stage, while the problem knowledge is limited. At the same time, the committed cost increases quickly. In other words, decisions made in the early design stage lock in a large share of the cost, as well as many other performance metrics. These decisions are difficult

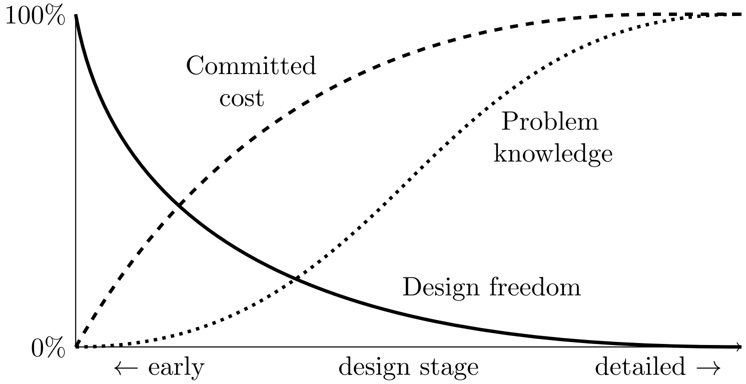



**Figure 1.2:** Simplified generic design timeline, adapted from Mavris and DeLaurentis (2000)

to modify in later, more detailed design stages, as the design freedom has reduced significantly then. Hence, for obtaining an adequate design while avoiding overruns in cost and time, there is a vital need for an adequate early stage design process, including suitable methods and tools. These methods and tools have a strong influence on the actual shape of the curves in Figure 1.2. Though presented in a simplified way as continuous curves, the tools and methods that are selected may cause the curves to be more discrete and step-wise. Hence, design methods and tools are a critical aspect of the (early stage) design process, and will be discussed in more detail later in this dissertation.

Apart from this observed mismatch between problem knowledge, design freedom, and locked-in performance, several other challenges are involved as well in the early design stage of naval ships (or ship design in general, as discussed by e.g. Gaspar (2013)). These include, but are not limited to the enormous number of potential solutions, the interactions between various systems and components within the ship, and the probability that design requirements change over time, either due to progressive insights or due to external factors such as political considerations. These challenges are discussed and dealt with by e.g. Brown and Thomas (1998), van Oers (2011), Duchateau (2016), and Shields (2017), and have led Andrews (2011) to defining naval ship design as a “wicked problem”, i.e. a design problem in which defining the requirements is more complex than finding the actual solution. This results from the strong link between the requirements and the solution. Before generating a solution to a design problem, feasible design requirements need to be developed. However, in order to evaluate whether the requirements are indeed feasible, they have to be checked with one or more physically realisable concepts, which are in fact solutions themselves. In other words: generating a solution needs requirements, while defining requirements needs solutions: a self-loop that makes the design problem “wicked”.

In order to structure the complex early stage naval ship design process, it is usually subdivided into separate sub-stages. These stages are defined as concept exploration and concept definition by van Oers et al. (2018). According to their definitions, these stages have the following characteristics:

- Concept exploration: This stage aims to establish a set of operationally relevant, technically feasible, and affordable requirements. This is done through a divergent, exploratory investigation where numerous (up to tens of thousands) potentially interesting concepts are investigated at a low level of detail, followed by a more targeted convergence towards a smaller number of most promising concepts.

- Concept definition: This stage aims to de-risk one or several concepts by developing them into sufficient detail, ensuring that the requirements that have been established during concept exploration can actually be met.

It must be noted that this terminology is not prevailing universally. Andrews (2018), for example, refers to early stage design as the *concept phase*. He uses *concept design* for concept definition, and adds an additional stage in between: *concept studies*, which is equivalent to the converging part of concept exploration. Outside of the naval ship design scope, comparable terms are used as well. In the field of systems engineering, which deals with the very topic of *how* to design, the concept development stage is subdivided in needs analysis, concept exploration, and concept definition, for example discussed by Kossiakoff et al. (2011). According to their definitions, the needs analysis focusses on the validation of an operational need and the development of a set of operational requirements. The concept exploration phase aims at exploring engineering-oriented solutions to the operationally oriented requirements. Subsequently, a preferred solution that meets the requirements is selected in the concept definition stage. As discussed above, defining requirements and exploring solutions could influence each other - at least in the case of naval ship design. As such, needs analysis and concept exploration as defined by Kossiakoff et al. (2011) become intertwined. For that reason this dissertation uses the terminology of van Oers et al. (2018).

There is a difference between the considerations in concept exploration and concept definition, and the types of questions asked at these stages (van Oers et al., 2018; Habben Jansen et al., 2020b; Brouwer, 2008). During concept exploration, the overall performance and trends are assessed. The focus is on *why* certain trade-offs exist, or *why* certain parameters drive the design. At this stage, obtaining directionality on how these parameters make the design better or worse is more important than what actual values for the parameters should be selected. In other words: the focus is on the general performance of the ship as a whole. When proceeding towards concept definition, more specific issues become of increasing importance. Performance assessments are then carried out on a more specific level, for example for individual systems or components rather than for the entire ship, such that bottlenecks or worst-case scenarios can be identified. The assessments that are carried out at this stage, are more specific and have a more quantitative nature. However, the overall performance of the ship as a whole is still considered as well, but now in more detail. Going from concept exploration to concept definition is therefore mainly an expansion of scope, not so much a shift of scope. The same holds for the process after early stage design, where plans and arrangements are developed in detail to check and confirm the performance

**Table 1.1:** Overview of main activity and area of focus for different design stages, adapted from Habben Jansen et al. (2020b)

| **Design stage** | **Early stage design** | | **Detailed design & engineering** |
|---|---|---|---|
| | **Concept exploration** | **Concept definition** | |
| **Main activity** | Exploring | De-risking | Detailing, checking, confirming |
| **Area of focus** | Overall performance and trends | Local performance and bottlenecks | Detailed plans and performance analyses |

of the ship and its systems, eventually for the purpose of construction. A summary of the activities and focus areas for these design stages is provided in Table 1.1.

The different considerations of concept exploration and concept definition can further be understood by using the DIKW pyramid, a commonly used hierarchical structure in the field of information and knowledge management (Rowley, 2007). DIKW is an abbreviation for the four elements in the pyramid: data, information, knowledge, and wisdom, in ascending order of meaning and value (see Figure 1.3). Various definitions for these four items exist, but according to the review of Rowley (2007), there exists consensus on what the items mean. The bottom of the pyramid contains data. Data has a specific nature, can often be computed or programmed, but has little meaning in itself. Information is structured, organised, or formatted data, that is meaningful to the recipient. Subsequently, knowledge includes information combined with personal aspects such as experience, common sense and intuition. Rowley (2007) finds that there are no common, clear definitions for wisdom, but concludes that is associated with understanding, interpretation, decision-making and 'right judgement'.

An important elaboration on these definitions is made in the definition of knowledge. In a further discussion on the definition of knowledge, Rowley (2007) refers to the distinction between explicit knowledge and tacit knowledge. Explicit knowledge is knowledge that is recorded or documented, and that is easily communicated. Tacit knowledge, on the other hand, is personal and resides in individuals though experience. Frické (2019) elaborates further on this distinction, stating that explicit knowledge mostly has a "know-that" nature, while tacit knowledge refers more to "know-how". In the original definition of the DIKW-pyramid, the knowledge refers to the latter. Frické (2019) also performs a critical review of the DIKW-pyramid, specifically focussing on the layout of the pyramid. The pyramid structure implies that the bottom parts are needed to acquire the top parts. Hence, knowledge can be obtained from information, and information can be obtained from data. In other words: higher parts of the pyramid inherently include lower parts. According to Frické (2019), this is irreconcilable with the tacit, "know-how" nature of knowledge, as its elusiveness and subjectiveness can not simply be obtained by induction and empiric reasoning. To support this argument, he refers to Weinberger (2010), who states that:

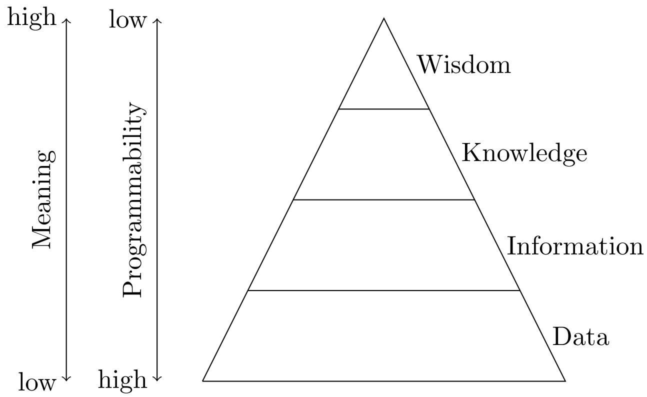



**Figure 1.3:** DIKW pyramid, showing the hierarchy between data, information, knowledge, and wisdom, adapted from Rowley (2007)

*"The image that knowledge (much less wisdom) results from applying finer-grained filters at each level, paints the wrong picture... Knowledge is more creative, messier, harder won, and far more discontinuous.*

Despite the discussion on the correctness of the DIKW-pyramid in its existing shape, the pyramid can be used to better understand considerations in early stage ship design. Since concept exploration mainly considers *why* certain trends and trade-offs exist, focussing on the level of overall performance, this dissertation places concept exploration at the higher end of the pyramid. More specifically, the considerations of concept exploration are categorised as knowledge, as they are rather generalised and represent a higher degree of understanding. This can include both explicit, "know-that" knowledge on the performance of the ship, but also tacit, "know-how" knowledge that resides within the ship designer. Section 5.1 elaborates further on this. In terms of generality and understanding, the category 'wisdom' even transcends the level of knowledge, but as stated above, wisdom is commonly associated with decision-making or 'right judgement'. In the case of naval ship design, this suggests being able to define or select 'the right design'. Though concept exploration supports this, it does not necessarily include this inherently. Hence, concept exploration is allocated to knowledge in the DIKW pyramid. Similarly, the more specific and quantitative nature of concept definition is allocated to the lower part of the pyramid, at the level of information. This is because selecting the right parameter values for a concept is quite specific, but at a higher level than simply a collection of numbers and characters, i.e. data.

This hierarchy further illustrates the challenge in early stage design. Concept exploration is intended to be carried out before concept definition. Yet, as it is located higher in the pyramid, it can only be based on more specific and quantitative assessments, at the level of the entire ship (Andrews, 2011). However, these more specific and quantitative assessments are the focus of concept definition, which is carried out *after* concept exploration. Hence, an incompatibility between concept exploration (focused on knowledge) and concept definition (focused in information) occurs. For that reason, practical naval ship design therefore does not contain a strict distinction between concept exploration and concept definition - it goes back and forth (van Oers et al., 2018). There remains a need to obtain generalised design knowledge during concept exploration, in order to acquire one or several feasible concepts in concept definition. The availability of generalised design knowledge has two advantages:

1. The likelihood that concept definition will lead to feasible concepts is increased.
2. If concept definition nonetheless leads to infeasible concepts, guidance and directionality for overcoming these problems is available.

Summarising this early stage design challenge, it can be stated that *generalised design knowledge is needed to generate feasible specific concepts, while it also needs information from those specific concepts.*

## 1.2 Vulnerability reduction of naval ships

Section 1.1 explained why it is challenging to make early stage design decisions that have a large influence on the final performance of the ship. This holds for any performance metric, but for a naval ship, an undisputed key design factor is survivability. This is because naval ships are designed to operate and win in a hostile environment. The hostility of naval operations - as well as operations of other military forces - is usually described in terms of the violence spectrum. The low end of this spectrum embodies environments and missions of relative safety, where threats and required weapon capacity are low. Analogously, the high end of the violence spectrum describes high-violent warfare or combat, usually associated with deployment of offensive weapons. Figure 1.4 shows an overview - which is not meant to be fully exhaustive - of missions that are carried out by a typical navy, sorted in increasing level of violence.

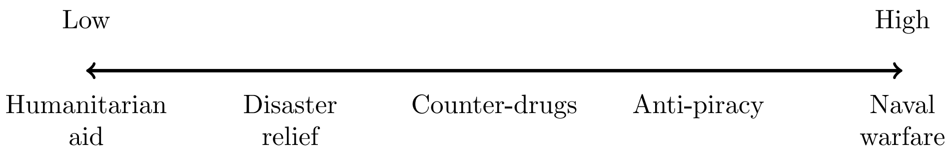



**Figure 1.4:** Violence spectrum for typical naval missions. Note that this figure is generic and not to scale, and that individual mission circumstances may deviate from this example.

Examples of missions carried out by the Royal Netherlands Navy (RNLN) at the lower end of the violence spectrum include the deployments of the Zr. Ms. Karel Doorman for ebola relief in 2014 (Ministerie van Defensie, 2019) and the Zr. Ms. Van Amstel for European border security management in 2016 (Nederlandse Omroep Stichting, 2016). These missions were carried out in relatively safe conditions with low threats, though Zr. Ms. Karel Doorman faced a rather serious security issue when three stowaways were found to have boarded the ship (Nederlandse Omroep

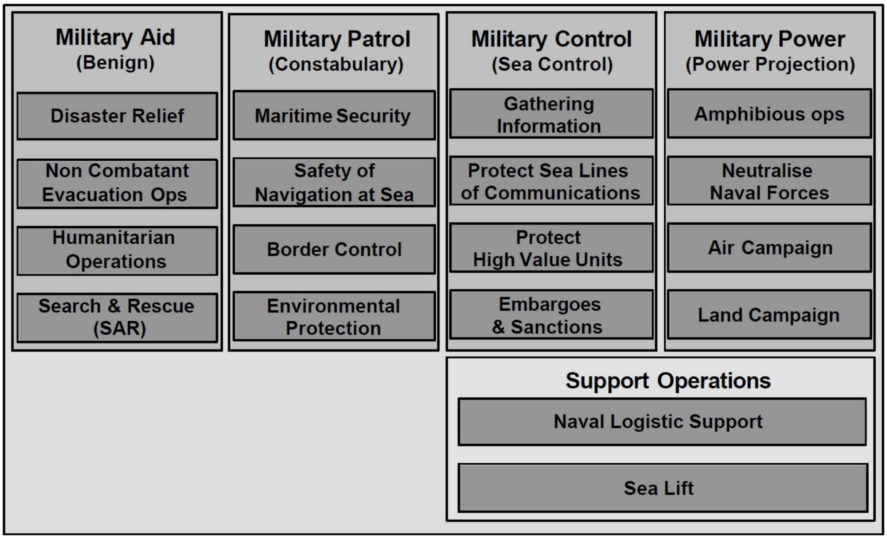



**Figure 1.5:** Template for military sea presence and typical associated operations. Figure retrieved from NATO Naval Group 6 on Ship Design (2004).

Stichting, 2015). An example of a mission higher in the violence spectrum is the anti-piracy mission of the - back then named - Hr. Ms. Rotterdam in 2012, when one of its RHIBs suffered minor damage during a gunfight with pirates (Marineschepen.nl, 2012). Though incidents in the highest end of the violence spectrum involving Dutch naval ships have not taken place in recent years, training in this part of the spectrum continues to be a major focus of the RNLN (Ministerie van Defensie, 2018). A relatively recent example of an incident in the high end of the violence spectrum is the sinking of the ROKS Cheonan in 2010, which sank due to an underwater explosion. 46 crew members died as a result of the incident. Its cause remains disputed, though evidence has suggested that the sinking resulted from a torpedo fired by North-Korea (United Nations Security Council, 2010).

The violence spectrum has been formalised in further detail by the NATO Naval Group 6 on Ship Design (2004), that defines a template with four categories of military sea presence, including examples of operations. This template is shown in Figure 1.5. It shows that the examples of the RNLN missions typically relate to categories lower in the spectrum, more specifically: humanitarian operations and maritime security. The ROKS Cheonan incident is an example of military power projection, where naval forces were neutralised. These examples illustrate the hostile environment in which naval ships are designed to operate. Though the probability of getting hit and suffering damage from weapon deployment of an enemy may not always be large, it is definitely present, and it may have severe consequences. Due to this, survivability is a major design driver for naval ships. A survivable ship can operate, survive, and win in a hostile environment, without compromising its ability to perform its designated missions.

### 1.2.1 Definitions of survivability

Survivability is a frequently used keyword in a military context, also beyond the scope of naval ships. In its broadest sense, it is defined by the United States Department of Defense as "All aspects of protecting personnel, weapons, and supplies while simultaneously deceiving the enemy" (Gortney, 2010). Alternatively, NATO defines survivability as "The capability of a weapon system to continue to carry out its designated mission(s) in a combat environment" (as cited by Piperakis (2013), who refers to an original NATO document). In order to make survivability more tangible for ships, a definition that has historically often been used, is "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" (Said, 1995). To transfer this into actual engineering solutions, survivability is usually expressed as the product of three key aspects: susceptibility, vulnerability, and recoverability (Said, 1995), (Ball and Calvano, 1994), (Piperakis, 2013), (Kim and Lee, 2012). In some cases, survivability is defined as the combination of only susceptibility and vulnerability, and recoverability is considered as a separate aspect (e.g. by Boulougouris et al. (2017)). Nevertheless, regardless of the actual subdivision, the three key aspects have the same definitions, which are now discussed in more detail.

Susceptibility is the inability of a ship to avoid damage. This strongly relates to its inability to get hit. For a positive contribution to the survivability of a ship, its susceptibility needs to be reduced. The most obvious measure that can be taken to achieve this, is avoiding hostile situations. However, this is often a rather trivial solution. Though there are examples of naval ships designed to stay away from hostile situations, such as a mine countermeasures vessel that remains in a safe area, while it deploys UUV's to handle the mines, naval ships are usually purposely designed to operate in hostile environments. Hence, a more meaningful effort is reducing the signatures of the ship itself. Signatures are all emitted signals of the ship that allow others to see or identify it. Various types of signatures exist, such as visual, acoustic, infra-red, and electromagnetic signatures. Reducing these signatures means reducing the susceptibility of the ship. Typical measures for this include adequate propeller design (with low vibrations and cavitation), deperming and degaussing the hull, cooling the exhaust gasses, or applying grey paint to the hull. Most of these measures are dealt with during the design of the ship, and to a lesser extent during operations.

Vulnerability is the inability of a ship to withstand damage of one or more hits. The fact that a hit has already occurred is considered as starting point. Vulnerability contributes negatively to survivability. In other words: to increase the survivability, the vulnerability needs to be reduced. Various measures for vulnerability reduction exist, such as damage containment by zoning, redundancy and separation of systems, and protection with ballistic-proof materials. The purpose of most of these measures is to obtain an intelligent layout, which is in general deemed the most effective protective measure (Brown, 1991). Similar to susceptibility, most vulnerability reduction measures can be implemented during the design of the ship.

Recoverability is the ability of a ship and its crew to repair and recover from damage. It contributes positively to the survivability. Contrary to susceptibility and vulnerability, recoverability is mainly dealt with by active operational response on board. Examples include fire-fighting, flood containment, re-routing vital resources, and treating injuries. The degree to which successful recoverability can be achieved strongly depends on crew abilities and training. However, several measures to increase the recoverability can be taken during the design already. For example, Piperakis and Andrews (2012) argue that recoverability is highly dependent on the ship layout and configuration, and propose a method to assess this in more detail during the design. Autonomous reconfiguration of vital routings can also be addressed during the design, as discussed by Janssen et al. (2016). Still, recoverability is mainly considered as an operational aspect.

The relation between susceptibility, vulnerability, and recoverability is visually shown in Figure 1.6. During the design, measures can be taken to remain at full capability by reducing the susceptibility (represented by the blue line) or to minimise the loss of capability after a hit by reducing the vulnerability (represented by the red line). It can be argued that extensive susceptibility reduction measures reduce the need for vulnerability reduction measures. However, a historic overview of incidents where Western naval ships were attacked by anti-ship cruise missiles shows that some hits are unavoidable, even if the ship is defendable (Schulte, 1994). The same holds for situations where it is not possible to ascertain the hostile nature of an enemy until it is too late (Reese et al., 1998). Hence, vulnerability reduction remains to be of critical importance during the design of a naval ship, and is therefore the focus of this dissertation.

Vulnerability in a military context refers to a man-made, hostile environment. However, that does not imply that vulnerability reduction measures only apply to damage caused by weapon hits. Other circumstances can also imply a need for reducing the vulnerability, such as accidental fires, collisions, or cascading failures that result from increasingly complex system design. Examples of non-hostile environments that have resulted in damage include the collision of the KNM Helge Ingstad with a tanker (BBC, 2018) and repeated power failures on board Type 45 frigates (Elgot, 2016). What matters for vulnerability is how the damage and its consequences can be reduced, not necessarily how the damage occurred in the first place.

### 1.2.2 Vulnerability reduction of distributed systems

Vulnerability reduction of naval ships comprises several topics of interest. Traditionally, the watertight subdivision and damage stability have received much attention. This highly important topic continues to be important today, and is for example addressed by Boulougouris and Papanikolaou (2004), and more recently in Boulougouris et al. (2017). In addition to that, structural integrity and blast-resistant bulkhead design are primary topics of interest (Erkel et al., 2002). However, recent developments in the field of naval ship design cause a need to expand the focus for vulnerability reduction. With the increasing interest in electrification, automation, and digital transformation, the design of the ship's on-board systems has become equally important as the more traditional naval architecture disciplines such as hydrodynamics and structures (Brefort et al., 2018). As a result, reducing the vulnerability of a modern

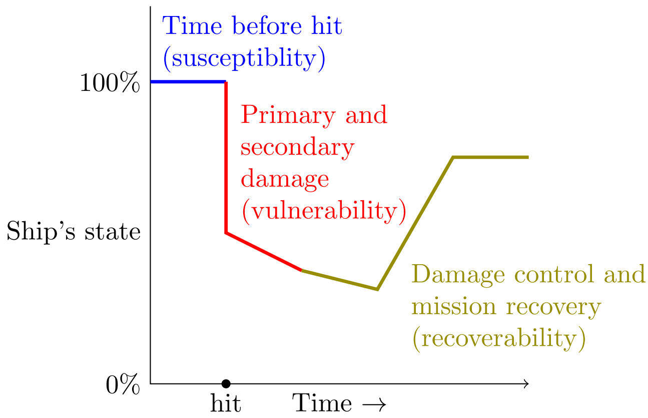



**Figure 1.6:** Stages of survivability, expressed as the ship's state over time

warship no longer only comprises the hull and stability - resilience of the ship's on-board systems has become at least equally important.

The trend towards electrification commenced in the 1980's and has since become more distinct as a result of growing electrical demands for existing and future weapon systems, such as rail guns, and their associated sensors (Clayton et al., 2000). Doerry (2015) identifies several advantages of an Integrated Power System (IPS), where the ship's propulsion and the electrical system are combined in one power system. These advantages include - amongst others - an improved support of high-power mission systems, higher efficiencies of prime movers and propulsors, and a reduced acoustic signature. The trend towards electrification also poses challenges, such as insufficient power supply of existing ship powering concepts, which require rethinking the ship's power system (see Jung (2019) for a practical example). Due to its advantages, the IPS concept is particularly interesting for naval ships, more so than for commercial cargo ships. Examples of naval ships with an IPS concept include the Zumwalt class destroyers of the US Navy, the Type 45 destroyers of the Royal Navy, and the Daegu class frigate of the Republic of Korea Navy. Other trends in (naval) ship design are automation and digital transformation. Selected intended advantages of digital transformation are reduced overall safety risks and reduced support costs (Bolton et al., 2018). Automation and digital transformation have applications on board, such as for manoeuvring and power control (see e.g. Gonsoulin (2018), Geertsma (2019)), as well as for ship support, such as smart maintenance (see e.g. Raptodimos and Lazakis (2019)).

In order to enable an these developments, complex networks for distributing vital commodities such as electricity, fluids, air, and data are indispensable. The systems that provide those commodities are known as either *distributed systems*, a term used by e.g. Doerry (2006) or *distribution systems*, a term used by e.g. De Vos and Stapersma (2018). There is a slight and subtle difference between these terms. *Distributed* systems are systems that are distributed throughout the ship, where *distribution* systems are systems that distribute vital commodities throughout the ship.

In practice, these systems usually cover both characteristics, and the terms can be regarded interchangeable. This dissertation uses the term *distributed* systems. A simplified example of a distributed systems network, usually known as a topology or a logical architecture, is provided in Figure 1.7.

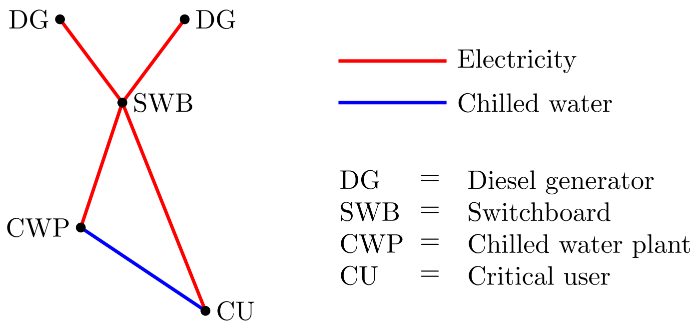



**Figure 1.7:** Example of a simplified logical architecture, including supply and distribution of electricity and chilled water

With the increasing interest in IPSs, the distributed systems networks become more complex and interdependent. This makes them more opaque and difficult to understand during the design (Brefort et al., 2018). For example, the amount of connections in the distributed systems networks may become so large that two seemingly unrelated components may both go off if one of them is disabled, even if they are not in the vicinity of each other. In addition, the way in which the ship is used, becomes more determinative for the design of distributed systems (Dougal and Langland, 2016). With an IPS, energy can easily be shared between users. For example, a high energy weapon can temporarily use power that is normally used for propulsion. This is not possible with a conventional powering concept, where propulsion power is mechanical. This increased flexibility only works if all components of the distributed systems are able to handle this power division. If not, cascading failures may occur, which increase the vulnerability.

The larger and more complex the distributed systems networks become, the more likely it becomes that such failures may not have been expected or simulated in advance. Hence, a ship with an IPS concept may be more prone to vulnerability in the non-hostile way that has been described in Section 1.2.1, even if it is not a naval ship. To identify and prevent such cascading failures, the vulnerability of distributed systems needs to be addressed in the early design stage (Goodrum et al., 2018a). However, this is a non-trivial effort. Following the same argumentation as in Section 1.1, it can be stated that the vulnerability characteristics need to be understood before a concept with low vulnerability - be it in terms of hits or in terms of cascading failures - can be designed. At the same time, concepts are needed for understanding the vulnerability characteristics. Hence, a method to overcome this self-loop is desired.

## 1.3 Research objective and scope

Section 1.1 has identified that there exists an incompatibility between generalised design knowledge and specific design information in early stage naval ship design. As a result, obtaining early knowledge on how design parameters influence the design is non-straightforward, which makes it difficult to establish directionality and design recommendations in the early design stage. Subsequently, Section 1.2 has specified this challenge in the context of vulnerability reduction of distributed systems. Up to now, existing ship design methods and vulnerability reduction methods are not yet able to account for this challenge when vulnerability is addressed in the early design stage. In order to overcome this challenge, the following research objective is defined:

*Develop a knowledge-providing early stage ship design method that assesses the performance of a concept, identifies the driving factors for that performance, and provides design recommendations towards better solutions, in the context of vulnerability reduction of naval ships.*

This research objective considers two perspectives: a generalised perspective regarding the design knowledge and information incompatibility, and a more specific perspective regarding vulnerability reduction. The specific problem can be seen as the manifestation of the generalised problem in a specific naval architecture discipline, i.e. vulnerability reduction. This dissertation aims to contribute to solving the generalised problem *via* addressing the specific problem. In other words, this dissertation considers a ship design problem that manifests itself in vulnerability reduction, rather than a vulnerability problem that occurs during ship design.

In order to address the research objective in a structured fashion, several limitations have been defined to mark out the scope of this research. This comprises the following issues:

1. This research, including the test case, applies to naval ships. As explained in Sections 1.1 and 1.2, early stage design of naval ships enfolds several specific challenges, and the topic vulnerability reduction particularly applies to naval ships. As such, naval ships are the focus of this dissertation. Nevertheless, this does not imply that this research is not applicable for other ship types. The topic of vulnerability reduction, for example, is also relevant for other ships that highly rely on distributed systems, such as DP-vessels, cruise ships, and autonomous vessels.

2. The term 'vulnerability reduction' specifically relates to vulnerability reduction of distributed systems. Section 1.2.2 has highlighted the topics of interest for vulnerability reduction of naval ships. Though damage stability and structural integrity have been identified as highly relevant aspects as well, they are not included in the vulnerability assessment that is developed in this dissertation. For the sake of simplicity, the remainder of this dissertation uses the term 'vulnerability' for vulnerability of distributed systems.

3. The method for assessing vulnerability that is developed in this thesis assumes that the compartments of the ship and the logical architecture of the main

components of the distribution system are known. As explained in Section 1.1, physically realisable solutions are needed for early stage design. What doesn't exist, can simply not be assessed. However, the level of detail of the logical architecture is limited to a selection of the most important components. The logical architecture itself remains fixed during the assessment, while the way in which the logical architecture is routed through the ship is a major subject of the method.

## 1.4 Outline of the dissertation

Several steps are taken to achieve the research objective, which correspond to the chapters of this dissertation. First, the field of research has briefly been introduced in this chapter, as well as the research objective and scope. A generalised problem in the field of early stage ship design and a specific problem in the field of vulnerability reduction have been identified. Subsequently, Chapter 2 provides a review of previous research and existing methods that have contributed to this field of research. More specifically, Sections 2.1 and 2.2 focus on the generalised ship design problem, and Section 2.3 addresses the specific vulnerability problem. Subsequently, Chapter 3 introduces the vulnerability method, which is based on Markov theory. The relevant mathematical background is provided, and the principle of the method is explained. Chapter 4 provides a test case, where the method is applied and the associated results and contributions are shown. Subsequently, Chapter 5 reflects on how the method, that applies to the specific vulnerability problem, relates to the generalised ship design problem. Chapter 6 provides an overview of other opportunities of the method. The outline of these chapters, which together form the core of this dissertation, is summarised in Table 1.2. Conclusions and recommendations for future research are provided in Chapter 7.

**Table 1.2:** Overview of the outline of Chapters 2-6 of this dissertation

| | **Problem** | **Solution** |
|---|---|---|
| **Generalised (early stage ship design)** | Chapter 2, Sections 1 - 2 | Chapters 5 - 6 |
| **Specific (vulnerability)** | Chapter 2, Section 3 | Chapters 3 - 4 |

# Chapter 2

# A review of ship design and vulnerability methods

This chapter provides background related to the research objective that has been outlined in Chapter 1. The goal of this chapter is to identify which research efforts have already been carried out, and which methods have already been developed for assessing and understanding the performance of a ship concept in early stage design. First, Section 2.1 gives an overview of design methodology in engineering. Section 2.2 addresses design methods and tools for of early stage ship design. Subsequently, Section 2.3 discusses vulnerability reduction methods specifically. The purposes and contributions of both types of methods and research efforts are investigated. Based on this analysis, the research gap and requirements for the new method are identified in Section 2.4. Section 2.5 selects the mathematical basis for the new method.

## 2.1 *What* to design versus *how* to design

Since a ship is a physical product, it is natural to express a ship design in terms of physical characteristics, which could range from highly specific (e.g. length, displacement) to more abstract (e.g. profitability, operability). However, as the design of complex ships can be categorised as a "wicked problem" (see Section 1.1) it is not out of place to discuss the design process that eventually leads to the physical design in more detail. In other words: not only *what* to design matters, but also *how* to design it. To that end, this section gives an overview of design methodology. It is recognised that the literature contributions in this field are inexhaustive. Without suggesting that the overview of this section is complete, it covers a selection of contributions to (ship) design methodology that are considered most relevant for this dissertation.

The wicked problem is investigated in more detail by e.g. Roberts (2000), who proposes three types of coping strategies:

- Authoritative strategies: Reduce the level of conflict by appointing a limited number of stakeholders who have the authority to come to a solution. This

Parts of this chapter are based on Habben Jansen et al. (2018, 2019, 2020a).

approach can make the decision-making quicker, but has the drawback that the authorities may be biased, or not fully informed. In terms of ship design, the authority in this strategy shows similarities to the 'overall ship designer', whose task it is to combine all sub-disciplines into a single design effort. Overall ship design is discussed in more detail in Section 2.2.

- Competitive strategies: Select a 'winner' who gets the right to define the problem and establish the solution. Notwithstanding negative associations, this strategy has distinct advantages, one of them being that competition can accelerate the development of new ideas. However, in terms of ship design this strategy is unlikely to succeed. For example, if the design of a ship is defined from a structural perspective, it is unlikely that it will have good weight, stability, and speed characteristics, thus leading to an infeasible or irrelevant solution.

- Collaborative strategies: Engage all stakeholders in the problem in order to come to a commonly defined and appreciated solution. These strategies tend to be preferred and have proven benefits in e.g. government and business. However, substantial stakeholder interactions are required for these strategies, which could be time-consuming and costly.

Various design approaches exist for coping with complex (engineering) projects, which all aim to exploit the benefits of one or more of these strategies. Three approaches that are common to the design of complex ships are discussed now in more detail.

An approach that is relatively new to the ship design community is concurrent engineering. The approach originates from the aeronautic industry, and is for example in use at the European Space Agency, as discussed by Bandecchi et al. (2000). They use the following definition for concurrent engineering:

*"Concurrent Engineering is a systematic approach to integrated product development that emphasises the response to customer expectations. It embodies team values of co-operation, trust and sharing in such a manner that decision making is by consensus, involving all perspectives in parallel, from the beginning of the product life-cycle."*

Relating this to the coping strategies for wicked problems, concurrent engineering can be defined as a collaborative strategy. As discussed by e.g. Koufteros et al. (2001) and Koskela (2007), it embodies a set of key elements, of which a multidisciplinary team is a major one. All team members, from all involved disciplines, congregate in meetings held at a dedicated facility with a fixed layout. During these meetings, design decisions are discussed and eventually made, using real-time input from the various design disciplines. An integrated design model (in software) is used to investigate implications of design decisions. Another key element of these sessions is that the customer is present and actively involved as well. The meetings are led by an independent chair, who facilitates the process, but is not technically involved in decision-making. Concurrent Engineering could lead to reductions in cost and product development time, but it also has drawbacks. For example, it may be difficult to develop the integrated design model. Different design disciplines may need different types of assessments for different design stages. This could make it complex to assemble all design information in one overarching model that includes all interdependencies between the design disciplines.

Another approach that focusses on the design process is systems engineering. This approach aims to decompose higher level needs, such as business needs or missions, into more specific functions and eventually actual systems and components. This is accompanied by clearly defined design stages, and formal documents that need to be delivered at the end of each stage (see e.g. Kossiakoff et al. (2011) for a general overview, and Calvano et al. (2000) for systems engineering in the context of naval ship design). Systems engineering is at the intersection between how to design and what to design. Systems engineering is not easily categorised in one of the coping strategies for wicked problems, but rather describes a set of steps in the design process. This is usually visualised by means of the V-diagram. This diagram exists in many forms. The one that is considered most relevant for this dissertation is provided in Figure 2.1. It shows how high-level missions (in this case of the ship) are made more specific in terms of operations and functions, which in turn result in actual systems and sub-systems, which form the actual solution (i.e. the ship). The solution is checked by means of verification, simulation, and validation to ensure that it is appropriate for fulfilling the mission. A feature of this diagram that is highly relevant for this dissertation is the role of requirements in this process. It can be seen that missions and functions, for example, lead to requirements, and that requirements lead to a certain performance and effectiveness. However, the relation between systems and requirements is bi-directional. Hence, requirements lead to systems, but systems also affect the requirements. This illustrates the nature of the wicked problem, and also exposes the main challenge in applying the V-diagram in the design of complex ships (or other products or structures), namely: requirements that are needed to define a solution can only be defined *through* the solution. This has led Andrews (2011) to question the appropriateness of systems engineering approach for defining requirements.

Another design approach that can be used for defining requirements and solutions is set-based design. In a naval ship design context it has been discussed by Singer and Doerry (2009). Set-based design addresses the issue that early in the design process, the committed cost increases quickly, while design knowledge is limited (see Figure 1.2). In set-based design, feasible sets of parameters are investigated by individual design disciplines. For example, from a structural perspective, feasible length-beam combinations may be different than from a hydrodynamic perspective. These sets are kept open longer than typically done in order to fully identify trade-offs. Once these have been understood, the sets are narrowed down, and the level of detail increases, resulting in an optimum solution. Hence, this approach aims to bring design knowledge forward, and to delay committed cost. The approach is visually shown in Figure 2.2. In terms of the coping strategies for wicked problems, set-based design deliberately has a competitive nature in the initial stages, where specialists from the different design disciplines are allowed to consider the design from their own perspective. Subsequently, a collaborative approach is applied to come to overlap in the sets, and to eventually define a solution. A major challenge in set-based design is an appropriate definition of the individual sets, especially since different design disciplines

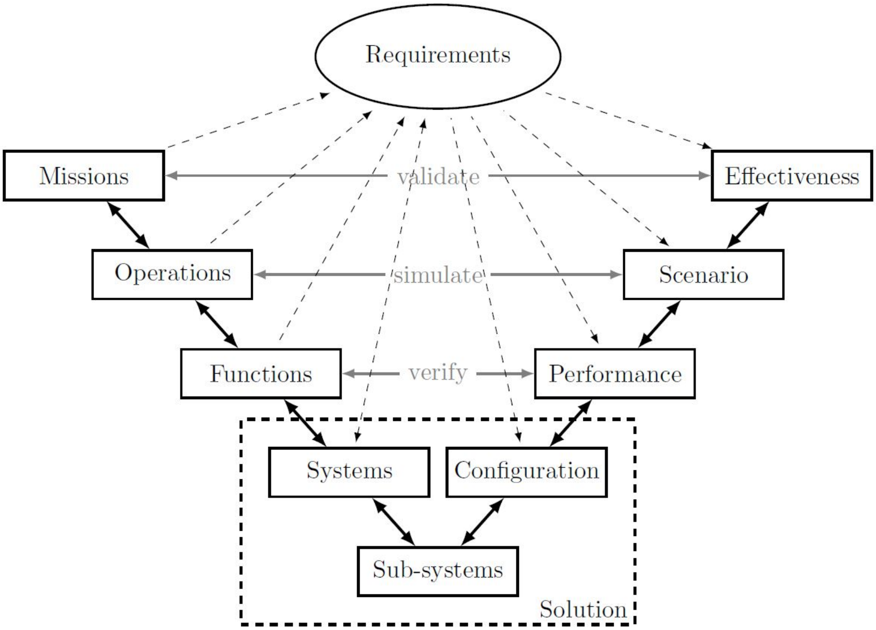



**Figure 2.1:** The systems engineering approach visualised through the V-diagram. Figure retrieved from Duchateau (2016).

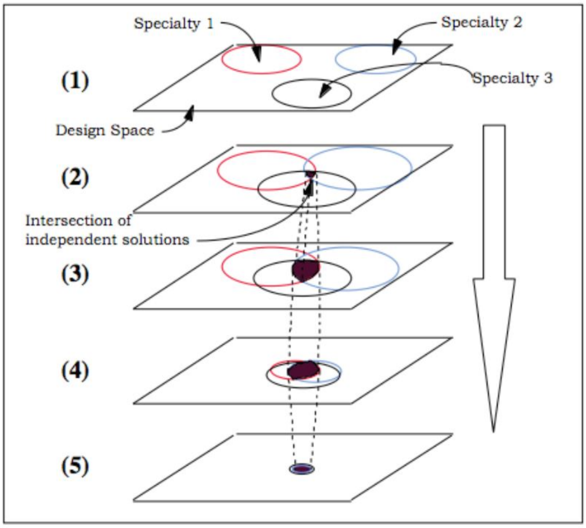



**Figure 2.2:** Visualisation of the set-based design approach. Figure retrieved from Singer and Doerry (2009). The term ‘specialty’ is referred to as ‘design discipline’ in this dissertation.

use different assessment tools, while variables used in these tools may link to multiple design disciplines. This is discussed in more detail by Goodrum et al. (2018b), who in response to that issue have developed a network representation for describing the coherence of design variables within and between different design disciplines. Based on that framework, they conclude that the naval architect, as in the overall ship designer, not only generates design information, but also acts as an integration manager.

It must be noted that the (ship) design approaches discussed in this section are not mutually exclusive. They all have their own key features. Concurrent engineering has a rather facility-minded nature, systems engineering has a stronger focus on describing a process with a set of steps, and set-based design deals with how many design alternatives should be considered over time. Yet, the methods have several common characteristics as well. First, they all agree on the need to integrate different design disciplines early on. Secondly, they agree that there needs to be a central authority to facilitate and/or guide the design process. This has a very strong relation to the role of the overall ship designer. To that end, the next section elaborates on methods and tools that can be used to investigate *what* to design, within the context of *how* to design as discussed in this section.

## 2.2 Review of methods for overall ship design

Historically, methods for early stage overall ship design have had a strong focus on parametric design, i.e. selecting appropriate values for key parameters of the ship. Typical examples of such methods include the design spiral (Evans, 1959) and the parametric ship design method described by Parsons (2004). The parameters considered in such methods typically include hull form parameters, such as length, beam, draft, and block coefficient, and mission-related parameters. In case of cargo vessels, these mission-related parameters can be specified adequately by physical characteristics, such as deck area or hold volume. However, for complex ships, such as naval ships or commercial vessels like multi-functional offshore heavy lift ships, it is less straightforward to capture the mission in physical characteristics. Moreover, the relation between key ship parameters and performance may be discontinuous. An example is provided by Duchateau (2016), who shows that the longitudinal position of a working deck, which is a continuous parameter, may cause strong discontinuities in displacement of the ship, as the position of the working deck forces the superstructure to be placed either forward, aft, or to be split. Such discontinuities are difficult - if not impossible - to capture by parametric models. This makes them less suitable for early stage design of complex ships. This argument is discussed in more detail by Pawling et al. (2017).

As a result, parametric design methods are ill-suited for the early stage design challenge of complex ships, where requirements and concepts (i.e. technical solutions, being models of actual ships), as well as knowledge and information are highly interdependent. Over the past years, this issue has been discussed in considerable detail by Andrews, who already advocated the need for an adequate design philosophy during the early rise of computer-aided design (CAD) tools (Andrews, 1981). He identifies the fact that “everyone’s problem is the designer’s problem” as an important characteristic of the tasks of the ship designer (Andrews et al., 2018). This illustrates the fact that the designer is responsible for integrating all sub-disciplines (e.g. marine engineering, safety, hydromechanics, structures), which can only be done through a physically realisable concept. In other words, the relation between requirements, concepts, knowledge, and information is first and foremost relevant for the designer, that is, the 'overall ship designer'. As such, this section focusses on a selection of existing methods and tools that are available for the overall ship design perspective.

In response to this early stage design challenge, Andrews has developed the Design Building Block (DBB) approach, of which an overview is provided in (Andrews et al., 2012). This approach addresses the required characteristics from a layout point of view, using an existing computer aided ship design system. An example of the graphical screen of the DBB is provided in Figure 2.3. With the approach, a ship concept can be generated based on individual blocks, which vary in size and detail throughout the design process. A key feature of the approach is the subdivision of the building blocks according to their function (i.e. float, move, fight/operations, and infrastructure) in contrast to the more traditional weight groups. The purpose of this feature is to allow more innovative configurations and to elucidate the impact of adding or removing blocks. The approach has an architectural nature, where the focus lies on layout. The approach purposely relies strongly on the input of a capable human ship designer. Throughout the design process, the designer receives visual feedback on the design, while it is being tracked whether the solution is technically feasible. The number of solutions that can be developed and assessed with the DBB approach is few, over the course of days. This makes the approach less suited for (automated) design space exploration with an extensive amount of potential concepts, which could be carried out during concept exploration. The approach, however, was never designed to facilitate this. The level of detail is variable and increases over the course of the design process.

Another method that has been developed to facilitate identifying trends, trade-offs, and underlying reasons, is the Packing approach. It was originally developed by van Oers (2011), and has later been adapted by Duchateau (2016). Similar to the DBB approach, the Packing approach uses building blocks to define concepts. However, this is done at a considerably lower level of detail, and for a higher amount of concepts ($\sim$ 10.000's), specifically aiming at concept exploration. With the Packing approach, concepts are automatically generated, using a genetic algorithm. These concepts are deemed feasible if they meet certain basic measures of technical feasibility, such as sufficient stability and acceptable trim. The generated set of designs is part of a larger work flow, where concept exploration and steering can be applied. This work flow is presented in Figure 2.4. The Packing approach particularly aims to elucidate trade-offs and design drivers with regard to overall sizing - the internal layouts that consists of the separate blocks do not necessarily represent feasible layouts. The limited number of constraints aims to facilitate finding a broad set of potential solutions. Visual feedback can be provided upon request of the designer by means of a 3D visualisation. However, this is not deemed a key feature of the method, since there are too many concepts for visually inspecting them all. Instead, the Packing approach helps in linking design requirements to solutions and identifying trade-offs by representing

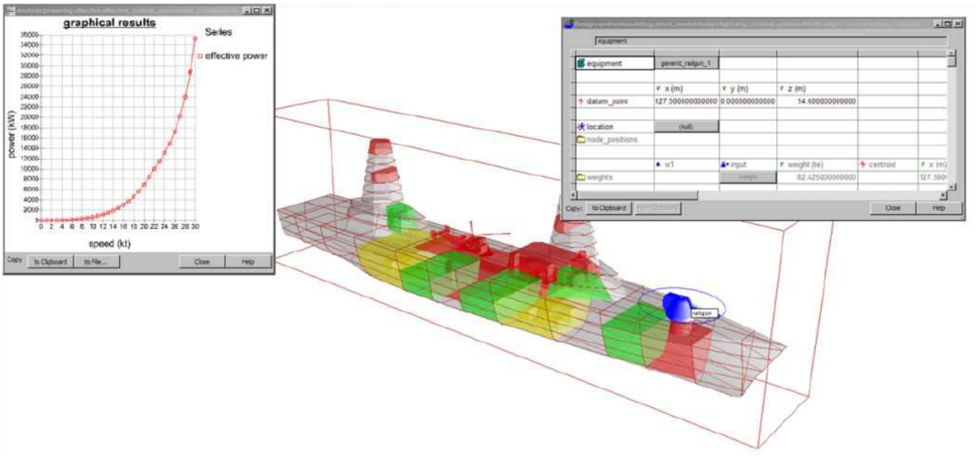



**Figure 2.3:** Example of the graphical screen of the DBB approach, retrieved from Andrews et al. (2012)

individual designs as scatter plots for two (or more) design variables, such as damage length, displacement, or cost. By inspecting these scatter plots and subsequent interactive steering of concept generation, the designer can identify which parts of the design space are feasible, and why. An example of such scatter plots, including visual representations of requirements, is provided in Figure 2.5. Despite this relatively high degree of automation, the Packing approach still relies on the designer for elucidating underlying reasons. For example, the designer needs to identify which scatter plots are relevant, and how they should be interpreted. In terms of knowledge, this means that some form of tacit knowledge of the designer is needed in addition to the explicit knowledge that the Packing approach aims to elucidate. For example: in a test case of Duchateau (2016), one scatter plot shows two distinct clusters for freeboard. The fact that these result from two distinct options for the number of decks has to be identified by the designer, by means of pre-conceived ideas on deck arrangements. In this case this was rather obvious, but for other, more complex interactions, this may be less trivial.

Another method for overall ship design originates from the Virginia Polytechnic Institute and State University, and is subject to ongoing developments and updates. It is known as a Combat, Power, and Energy Systems (CPES) assessment method. A recent overview of the method is provided by Parsons et al. (2019). Contrary to the DBB approach and the Packing approach, which use one model to describe overall ship characteristics, the CPES method uses various different models to describe the overall ship. For example, a network is used for the logical architecture, and a process flow chart is used for describing ship operations. The different models are integrated in an application called Model Center, which follows a pre-defined procedure to assess overall ship performance, cost, and risk. A flow chart of this procedure is provided in Figure 2.6. A considerable level of detail is required as input for the CPES assessment method. For example, the logical architecture that is used in the example

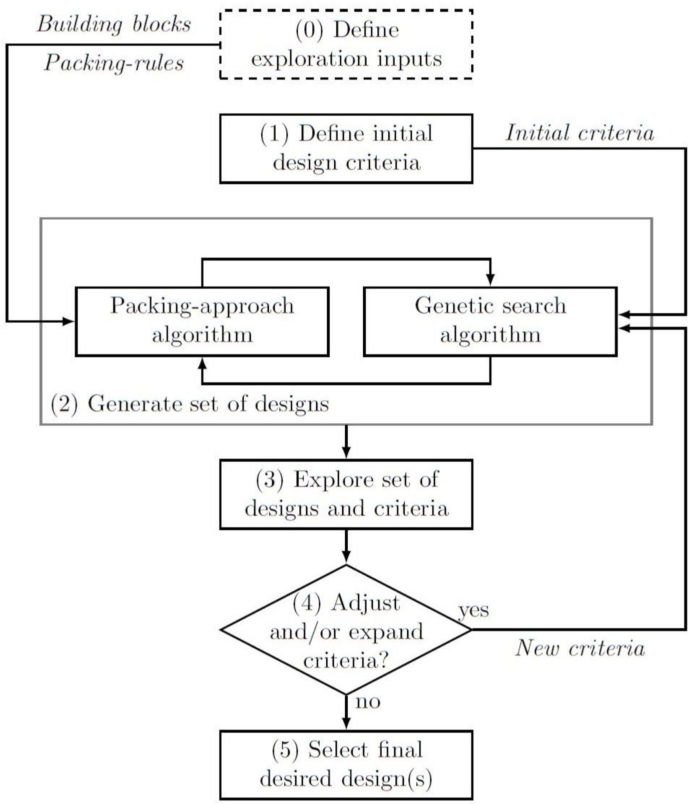



**Figure 2.4:** Work flow for concept exploration using the Packing approach. Figure retrieved from Duchateau (2016).

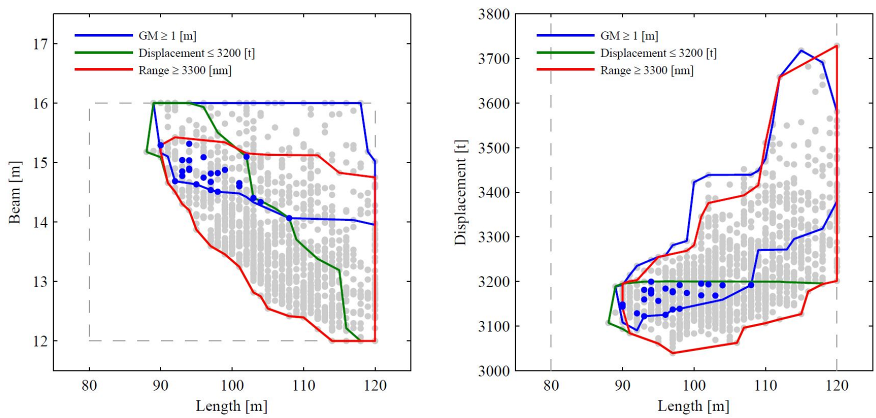



**Figure 2.5:** Example of scatter plots from the Packing approach, showing relations between design variables and requirements, retrieved from Duchateau (2016)

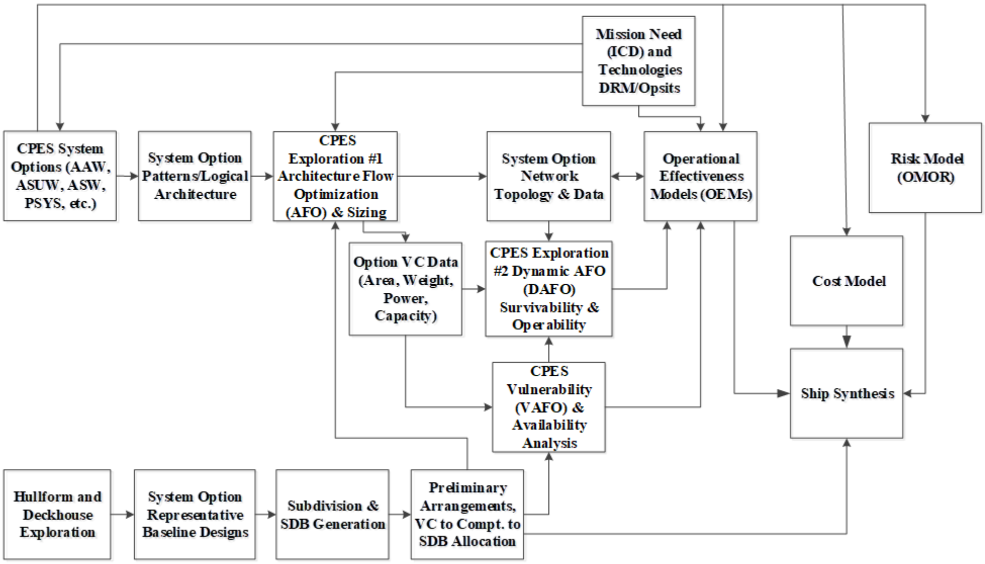



**Figure 2.6:** Flowchart of the CPES assessment method. Different models are available for different blocks in the flowchart. Figure retrieved from Parsons et al. (2019).

of Parsons et al. (2019) consists of more than ten different commodities (e.g. chilled water, lubrication oil, fuels, electricity), each of them consisting of several tens of nodes (i.e. components). Other modules provide e.g. a low-fidelity seakeeping analysis and propeller selection and optimisation. Compared to the DBB approach and the Packing approach, this method covers a broader spectrum of the overall design activity. Due to the required input, the method is best suited for the later part of early stage design, such as concept definition.

The focus on power and energy systems is also used in the method S3D, which stands for Smart Ship System Design. This is a tool for overall ship design with a specific focus on electric ships (Chalfant et al., 2012). The tool has been developed in response to the increasing complexity and sophistication of military systems, and is designed to facilitate collaboration between different design disciplines (e.g. electrical, mechanical, thermal, and naval architecture). The tool has been designed to consider one ship model at the time. The different design disciplines can work simultaneously on this model. Each discipline has its own view on the model, thus eliminating designer overload with non-relevant information. An example of the view for electrical engineers is provided in Figure 2.7. The tool is linked to the Leading Edge Architecture for Prototyping Systems (LEAPS), which is a common ship design data repository for the US Navy (Chalfant et al., 2017). Similar to the Design Building Block approach, the level of detail grows as the design process advances.

The examples of overall ship design methods discussed above have all been developed within - but are not necessarily limited to - the context of naval ship design. An

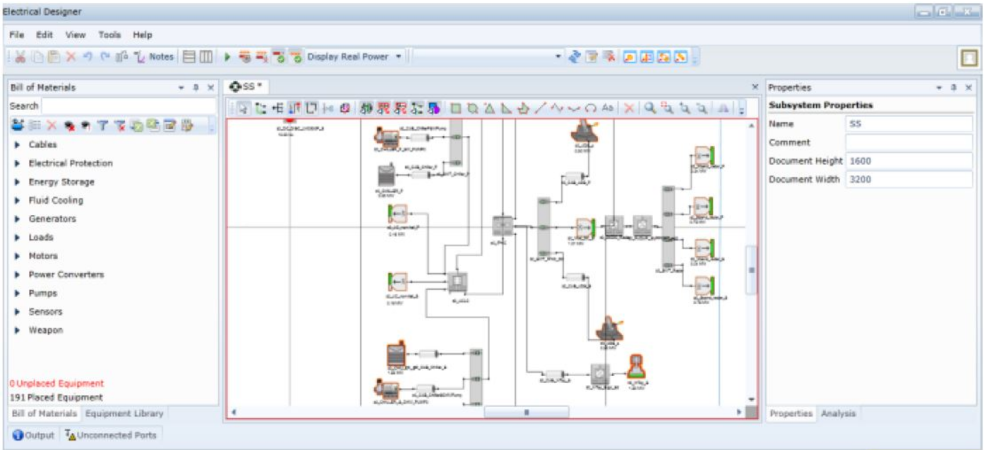



**Figure 2.7:** Example of the electrical engineering view of S3D, with a materials library from LEAPS at the left. Figure retrieved from Chalfant et al. (2017).

**Table 2.1:** Summary of ship design methods discussed in Section 2.2.

| **Method** | **Area of focus** | **Level of detail** |
|---|---|---|
| Design Building Block | Overall layout | Variable |
| Packing | Overall sizing | Low |
| CPES | Power and energy systems | Medium |
| S3D | Electric ships | Variable |
| Holistic ship design | User-defined variables of interest | Medium |

example of a non-naval approach for overall ship design is the holistic ship design optimisation method developed by Papanikolaou (2010). Similar to the Packing approach, it uses an optimisation algorithm to explore different design solutions that are subject to a set of constraints. One of the major differences is that the ship's particulars and loading conditions are assumed to be known. An optimisation effort is carried out within the scope of those fixed parameters. For example, in one of his test cases, Papanikolaou (2010) optimises for maximum transport capacity, a maximum subdivision index and minimum structural weight for a Ro-Ro vessel. Hence, this type of optimisation is carried out in a slightly later design stage than the Packing approach, when overall sizing is known.

The methods described above are summarised in Table 2.1. It can be observed that though all methods aim to facilitate early stage design in the overall ship design context, every method has a specific area of focus. In addition to that, the level of detail of all three methods is different, covering the full scope from concept exploration to concept definition.

## 2.3 Review of vulnerability reduction

Chapter 1 has explained that the challenges related to the interdependency between concepts (related to specific information) and requirements (related to generalised knowledge) manifest itself in particular in vulnerability of naval ships. To that end, this section elaborates on design methods and tools that already exist to address these challenges. Before these methods are discussed in more detail, several general considerations for vulnerability reduction are discussed first.

### 2.3.1 General considerations for ship vulnerability reduction

A key feature of vulnerability requirements is that they are usually formulated in relation to the impact level of a hit (or other damage). In other words: the required residual capability depends on how severe the damage is. It is undesirable that a low-cost weapon with minor impact disables a significant part of the ship (known as a 'cheap kill'), so for minor damage, it is likely that the requirements prescribe a certain ability to fight hurt. Likewise, it is unrealistic to require that full fighting capabilities remain after severe damage - in those cases it is more likely that the focus shifts towards evacuation, or leaving the theatre in an orderly fashion. This concept is known as 'graceful degradation'. The type of threat is a key element in graceful degradation. Usually, a distinction is made between a symmetric threat and and asymmetric threat (Wilson, 2010). The former relates to situations where both parties have comparable weapons and combat power (e.g. a ship against a ship), while the latter refers to situations where weapons and combat power are significantly different (e.g. a ship against a drone). In case of a symmetric threat, a high impact level is more likely to refer to a single hit with a large damage extent. For an asymmetric threat, a high impact level could potentially also result from many hits with smaller damage extents. Hence, both types of threat could result in the same impact level, while the associated damage is distinctly different. Especially in recent yeas - that is, after the Cold War - asymmetric threats have been a great area of concern (Wilson, 2010).

In order to facilitate graceful degradation, the vulnerability requirements are operationally oriented, as discussed by e.g. Reese et al. (1998) and Liwang and Jonsson (2015). An example of the relation between impact level and residual capabilities, expressed in a matrix, is provided in Figure 2.8. Reese et al. (1998) also provide approaches for quantifying vulnerability requirements, making a distinction between absolute and probabilistic terms. A requirement in absolute terms is expressed in a deterministic fashion, where the requirement must be met with a probability of 1. This type of formulation is particularly applicable if meeting the requirement is essential for success of the mission. With the probabilistic approach, the likelihood of meeting the requirement is expressed as a probability. This approach accounts for the perspective that a certain degree of loss of capability may need to be accepted. The probabilistic formulation also has benefits for hit modelling. Though ship signatures, such as the infrared signature, can influence the location of a hit (Schleijpen, 2010), hits can occur at any location, potentially in unexpected scenarios. Especially in the concept exploration phase, the vulnerability of the ship as a whole, regardless

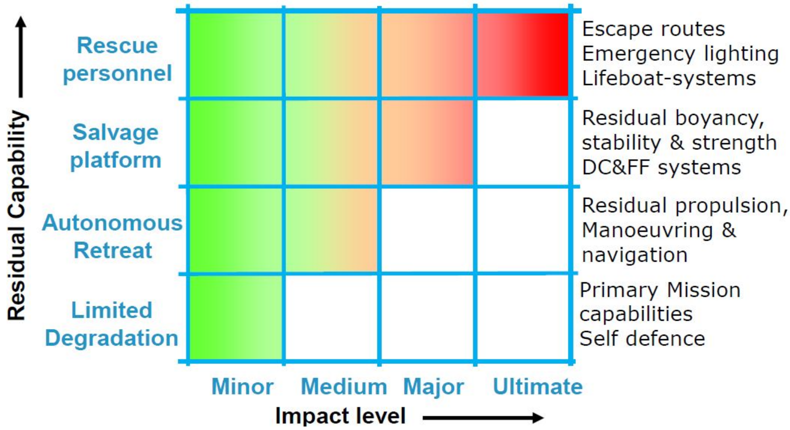



**Figure 2.8:** Example of the relation between residual capabilities and impact level for a support ship. Figure retrieved from van Meurs (2019).

the exact location of a hit, is of interest. A probabilistic approach in modelling hits supports such a generalised assessment.

The operationally oriented formulation of vulnerability requirements relate to how the ship and the distributed systems are used. However, other aspects are relevant as well, such as how various components of distributed systems are connected, and where they are located. In order to facilitate a comprehensive approach for designing distributed systems, in particular with a focus on low vulnerability, Brefort et al. (2018) have established a framework that describes these distributed systems. This framework is not a design method in itself, but highlights the different characteristics of distributed systems that need to be addressed for survivable design. This framework will be used in Section 2.3.2 to classify various methods for vulnerability reduction, and is now discussed in more detail.

Brefort et al. (2018) define three main characteristics of distributed systems: the physical architecture, logical architecture, and operational architecture. The characteristics are named 'architectures' because they express the conceptual structure of distributed systems, from different representations. The framework is graphically shown in Figure 2.9. The architectures are defined as follows:

- Physical architecture: The spaces in the configuration of the ship, as well as the physical attributes of components of the distributed systems, located in those spaces.

- Logical architecture: The functional characteristics of the system, as well as the links between the various components of the distributed systems.

- Operational architecture: The way in which the distributed systems are used over time, including what systems are needed in which order, or what processes are carried out with the distributed systems.

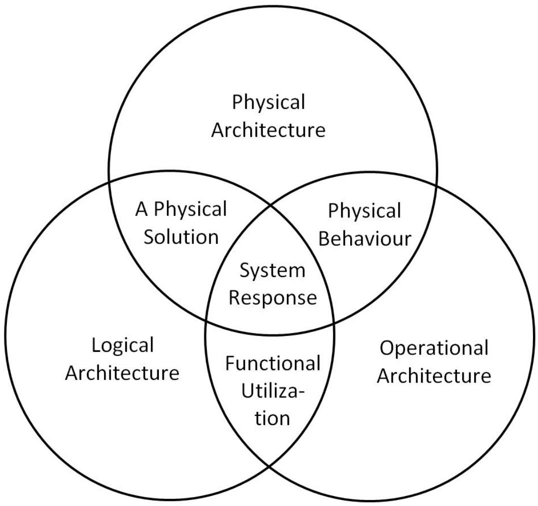



**Figure 2.9:** Architectural framework for representing distributed systems. Figure retrieved from Brefort et al. (2018).

Each architecture can be expressed in its own form. The physical architecture, for example, can be represented as a general arrangement, while a single-line diagram is suitable for describing a logical architecture. Note that this is independent of the level of detail. The operational architecture is more abstract to capture in a representation. In terms of vulnerability, a part of the operational architecture are the operationally oriented vulnerability requirements, as provided in Figure 2.8. However, system management procedures included in the platform handbook of a ship also represent the operational architecture.

A key feature of the architectural framework are the overlaps between the three main architectures. These overlaps capture characteristics of the distributed systems that are not captured by solely one of the architectures. The overlaps are defined as follows:

- Physical solution: The description of what the system components look like in the physical space of the ship, including connection elements, such as cabling, piping, or shafts.
- Functional utilisation: The resource flow required between system components in order to fulfil a mission of interest.
- Physical behaviour: The characteristics of a physical layout for a mission of interest.

Similar to the main architectures, these intersections have their own way in which they can be represented. A physical solution is typically represented as a routing scheme, that links connections to actual locations in the ship. The functional utilisation can be expressed by means of a load balance, potentially over time. The physical behaviour is less straightforward to capture in a representation. However, Brefort et al. (2018) give two examples of physical behaviour: the electromagnetic interferences that occur if an operational scenario requires high electrical loads, and the fact that the appropriate size of a generator depends on the operational profile of that generator.

The combination of all primary architectures and overlaps results in the system response, which describes the performance of a system for a certain layout, certain relations between components, and a certain mission of interest. It can be seen as the overall description of one or more distributed systems. This also implies that for comprehensive and survivable design of these systems, all architectures need to be addressed. To that end, this framework is used to evaluate various existing vulnerability methods in the next section.

### 2.3.2 Methods for ship vulnerability reduction

Various method and tools exist for ship vulnerability assessments. Some of these methods are aimed to be used in practical ship design by navies or shipyards, while others are developed from a more fundamental research perspective. Examples of the former type include the commercially developed tools RESIST (TNO, 2018), SURVIVE (Schofield, 2009) and SURMA (Surma Ltd., 2018). Many of these tools have been developed within the context of a specific country and/or navy. For example, the tools mentioned above have been developed in The Netherlands, the United Kingdom, and Finland, respectively. The tools provide high fidelity assessments of a ship exposed to one or more hits. They assess damage effects such as structural failure and fire. The results of these tools comprise overviews of the damage stability, availability of critical systems, and structural integrity after one or more hits. The computations in these tools are in some cases based on first principles, but in other cases on more detailed techniques. RESIST, for example, uses algorithms that hold an intermediate position between Finite Element Methods (FEM) and Computational Fluid Dynamics (CFD), in addition to analytical and empirical formulas. Because of this level of fidelity, detailed plans such as a general arrangement, a structural arrangement, and a logical architecture for distributed systems are needed as input for these tools. This makes them highly useful for detailed design stages. For the early design stage they are of limited use, due to the required level of detail. However, some tools have a simplified version for the early design stage, such as SURVIVE Lite (Schofield, 2009). This version can be used for more generic layouts and a reduced level of subdivision. Another tool, called PREVENT (Heywood and Lear, 2006) applies a similar level of detail. Two examples of different levels of fidelity are given in Figure 2.10.

Early-stage focussed methods for assessing vulnerability exist as well. Many of these have a more fundamental or scientific background. Piperakis (2013) has developed a method that is specifically aimed at the early design stage. It integrates susceptibility, vulnerability, and recoverability in a method for assessing overall survivability. The method is layout-based. It combines existing tools with a newly developed recoverability method. The method is suitable for assessing a relatively low number of alternatives, but at a relatively high level of detail. This fits well in the concept definition phase. A comparable level of detail is considered by Goodfriend and Brown

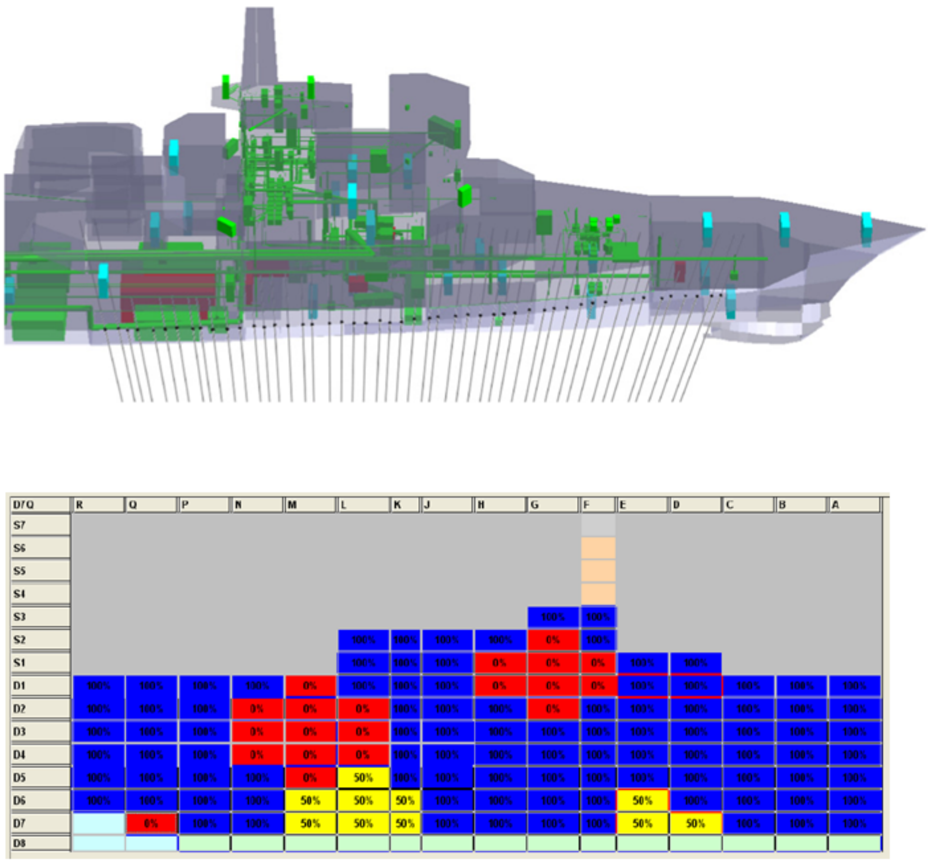



**Figure 2.10:** Examples of different levels of detail for vulnerability methods: high (RESIST, top) and low (PREVENT, bottom).

(2017). They only consider vulnerability, with a specific focus on distributed systems. Their method uses a multi-objective genetic algorithm to explore the design space, with high effectiveness, low cost, and low risk as objectives. The method has an exploratory nature, though it still requires a level of detail that may be more suitable for later design stages. The work of Goodfriend and Brown (2017) feeds into the CPES assessment method that is discussed in Section 2.2.

A method with a lower level of detail has been developed by van Oers et al. (2012). Their method uses an genetic optimisation algorithm that generates 2D physical solutions (i.e. routings) of distributed systems, where low vulnerability is one of the objective functions, quantified by minimising the loss of capability after one or more hits. The method only considers variations on the shortest path. In a follow-up study, Duchateau et al. (2018) also consider physical solutions that may be longer, but potentially less vulnerable. Their method is in 3D, though the transverse direction

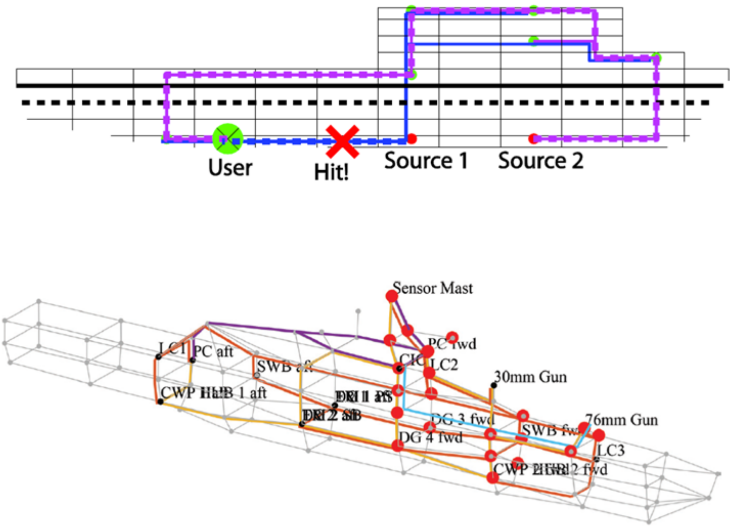



**Figure 2.11:** Example of two early stage vulnerability methods with a focus on routing: van Oers et al. (2012) (top) and Duchateau et al. (2018) (bottom).

only makes a distinction between port side and starboard. They also use a genetic optimisation algorithm. Visual examples of these methods are provided in Figure 2.11, where it can be observed that the level of detail is significantly lower than for e.g. RESIST. On a similar level of detail, the vulnerability of distributed systems is considered by Kim and Lee (2012). However, their aim is not to generate physical solutions, but to evaluate the availability of critical systems after one or more hits in a probabilistic fashion. They investigate a binomial method, a Poisson method, a tree diagram, and a Markov chain. Their method can be used with a limited level of detail, but the mathematical set-up becomes complex when the number of redundant components is increased. Furthermore, their method is well suited for evaluating predefined concepts, but does not provide guidance towards other - potentially better - concepts. Another method for assessing physical solutions in the context of vulnerability is provided by Shields et al. (2016). Their method has a slightly different perspective than the methods described above. The method is not a design tool in itself, but provides an estimation of the complexity of physical solutions. This estimation can be used for evaluating how well a concept is understood, rather than for generating concepts.

In addition to genetic algorithms and probabilistic models, networks are used as well for vulnerability assessments of distributed systems in the early design stage. Goodrum et al. (2018a) combine two networks, one describing the compartments of the ship (i.e. the physical architecture), and one describing the logical architecture for distributed systems, to compute an operability score for damaged compartments. This is done at three levels of fidelity, in increasing order: based on connectedness, based in connectedness in the right direction, and based on network flow. All compartments are considered individually for damage. The network flow assessment partially considers operational architecture, but no translation from the operability score to residual capabilities is made. Since their method is network-based, it is very robust and quick, allowing large numbers of layouts and damage scenarios to be considered. Networks are also applied by de Vos and Stapersma (2018), who have developed a tool that can automatically generate a vast number of logical architectures in order to explore the design space. A genetic algorithm is used to obtain logical architectures 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 the reconfigurability of a logical architecture as a critical aspect of vulnerability reduction, which can be realised by connecting hubs in the logical architecture. 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 logical architecture 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.

All above mentioned methods require some sort of modelling of the ship and its distributed systems, either with a significant or limited level of detail. However, guidance on vulnerability reduction can also be found in generic design guidelines that are based on experience and best practices. For example, the following design rules are in use at the Netherlands Defence Materiel Organisation (van Meurs, 2019):

1. Avoid platform distribution systems.
2. Avoid single points of failure in vital distribution systems.
3. Separate redundant sources.
4. Separate redundant paths.
5. Route vital distribution systems on the same paths.
6. Run feed and return lines of closed loop systems together.
7. Protect redundant sources within the sphere of weapon effects.
8. Protect redundant system runs within the sphere of weapon effects.
9. Arrange cross-overs close to critical users.
10. Arrange cross-overs close to system sources.
11. In general, ring-shaped systems are a preferred solution.

The advantages of these rules of thumb are that they have historically proved to be useful, and that they can be applied in the very earliest stages of vulnerability reduction. However, they are rather difficult to quantify, and provide no insight in potential trade-offs or compromises. For example, Rules 3 and 4 advise to separate redundant sources and paths, but it is not discussed how this should be done, or whether there is a practical limit to the amount of sources and paths that should reasonably be made redundant.

As mentioned in Chapter 1, vulnerability reduction of distributed systems is particularly important for ships with an IPS 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 IPS 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. IPS ships are also main topic of the work of Schuddebeurs (2014), who specifically considers advanced modelling and simulation techniques for de-risking IPS 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 IPS ships, while at the same time noting that the number of available suitable methods is limited. Doerry (2007) states that vulnerability in IPS 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 IPS ships need to operate adequately in normal operating conditions, which addresses the more internally oriented aspect of vulnerability, which focusses on internal systems failure rather than failure that result from weapon hits. 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 IPS ships are not the subject of this dissertation, but a more elaborate discussion can be found in e.g. (Logan, 2007) and (Menis et al., 2012).

A summary of the methods described in this section is provided in Table 2.2. It can be observed that the physical and logical architecture are considered in every method. The operational architecture seems to be considered to a lesser degree. If it is included, it is mostly in terms of network flow and capacity (i.e. functional utilisation), or in terms of recoverability.

The type of architecture that is considered in the various methods is not the only point of attention. It has been noted in Section 2.3.1 that asymmetric threats are

**Table 2.2:** Summary of vulnerability reduction methods discussed in Section 2.3. P = physical architecture, L = logical architecture, O = operational architecture.

| **Method** | **Architecture type** | **Level of detail** |
|---|---|---|
| RESIST, SURVIVE, SURMA | P, L, O | High |
| SURVIVE Lite, PREVENT | P, L | Low |
| Piperakis | P, L, O | Medium |
| Goodfriend and Brown | P, L | Medium |
| Van Oers et al. | P, L | Low |
| Duchateau et al. | P, L | Low |
| Goodrum et al. | P, L, O | Low |
| Kim and Lee | P, L | Low |
| Shields et al. | P, L | Low |
| De Vos and Stapersma | L | Low |
| Trapp | L, O | Low |
| DMO design rules | P, L | Very low |
| Cramer et al. | P, L, O | Medium |
| Schuddebeurs | L, O | High |
| Doerry | L, O | Medium |

a major area of focus. In order to deal with this type of threat during the design, a vulnerability reduction method needs to be able to account for multiple hits with smaller damage extents, rather than the more traditional single, but more severe hit. However, most of the methods of Table 2.2 use user-defined hit scenarios. This works well for a limited selection of hits, but quickly becomes cumbersome for combinations of multiple but smaller hits - especially because it is unknown where a hit will occur. This is taken into consideration in the gap analysis and selection of the associated mathematical approach, which will be discussed in Sections 2.4 and 2.5.

### 2.3.3 Methods for assessing vulnerability in other fields

Vulnerability assessments are also carried out in other fields of study. They are especially relevant for applications with resource flows through infrastructures, analogous with the resource flow through distributed naval ship systems. The number of applications is extensive, but three examples are discussed here briefly.

A typical example of a non-naval vulnerability assessment is is the design of land power grids. Liu et al. (2012) have defined an operational vulnerability index to investigate the possible benefits of decentralised power generation. In terms of this index, a good network with respect to vulnerability is one in which the long-distance large-capacity power transmission is minimal. A major difference with naval ship applications is that land power grids consider only one type of resource (electricity), while for naval ships interdependencies with other types of flow, e.g. chilled water, data, and fuels, need to be considered. Furthermore, the operational vulnerability index is not based on damage or loss of systems or compartments, but on the efficiency of the transmission.

**Table 2.3:** Difference in number of resources and operational scenarios considered for various vulnerability methods. (Naval) ships added for reference.

| Application | No. of resources | No. of operational scenarios |
|---|---|---|
| Electrical power grid | one | one |
| Highway | one | many |
| Health care facility | many | one |
| (Naval) ships | many | many |

Another non-naval ship design example of a vulnerability assessment is the work of El-Rashidy and Grant-Muller (2014), who have performed a vulnerability assessment on a highway network. This example also considers one type of resource (cars), but they have taken into account that the vulnerability depends on various operational and external factors, such as different threats or traffic speeds. This is done by defining vulnerability attributes that are calculated based on basic road traffic parameters, such as the number of lanes, the speed of the cars, and the congestion density.

The third example is the assessment of a health care facility. Arboleda et al. (2009) have developed a method for assessing the operational vulnerability of a health care facility during disaster events. In contrast to the two methods mentioned earlier, this method takes into account that the system, in this case a health care facility, is dependent on different types of resources, such as water, power, and the transportation of medical supplies. However, it takes into account only one default operational scenario.

The characteristics of these vulnerability methods are summarised in Table 2.3. It can be observed that the applications considered in this section are of a different nature than naval ships. For these applications only one type of resource and/or one operational scenario is considered, while for naval ships both could be many. Note that this is no measure for the quality of the vulnerability methods for other applications, as different problems require different solutions. It is pointed out, however, that existing methods for vulnerability assessments in other fields may not be directly applicable to naval ship design.

## 2.4 Gap analysis

Based on the review of Sections 2.1 to 2.3, a research direction can be obtained from identifying where a research gap still exists. This is done from both an overall ship design perspective, as well as a vulnerability reduction perspective.

In terms of the overall ship design perspective, it can be stated that some methods aim to develop a concept that can be used as a starting point for the remainder of the design process. In other words: the methods focus on concept definition, usually with a considerable level of detail. Though this step is indispensable for a successful design process as a whole, it does not necessarily address the issue of the strong interdependency between requirements and solutions (i.e. the wicked problem). In other words: the methods do not directly provide design knowledge that is needed for identifying the driving factors and finding directionality towards better concepts. To address this issue, another - earlier - step needs to take place: developing concepts for the sake of *understanding* these concepts. This is done during concept exploration. Of the methods discussed in Section 2.2, Packing and the Design Building Block approach mostly comply with this perspective. However, both methods require a considerable level of human input for interpreting why the results are as they are. This is not necessarily a bad thing. However, a more formalised, mathematics-based approach for identifying underlying reasons for the ship's performance may be helpful for more complex interactions between concepts and performance.

In terms of the vulnerability perspective, it can be stated that the physical and logical perspective on distributed systems is well present in existing vulnerability methods. However, the operational architecture leaves room for further exploration. Especially the need for operationally oriented formulations of vulnerability requirements (i.e. the fact that residual capability needs to be linked to impact level) is not yet considered in existing vulnerability methods that are aimed at the early stage. The ability to quantify and understand graceful degradation, including the driving factors and interdependencies between the different levels of degradation, would greatly enhance design knowledge on the operational perspective on vulnerability. This knowledge can be used to obtain design recommendations for distributed systems. This supports the purpose the concept exploration phase, i.e. obtaining generalised estimations of the vulnerability trends of the ship as a whole (see Table 1.1). Based on this assessment, the designer can decide which direction is most promising for further design efforts. A typical, notional result of such an assessment could be (see Chapter 4 for an actual test case on this topic):

*"Based on the likelihood that the levels of residual capability will be met after damage, a concept with an integrated power system seems more appropriate than a concept with separate, mechanical propulsion. Further design efforts could focus on relocating the aft switchboard and its associated electricity cables, as they have shown to be most decisive for the level of vulnerability."*

As such, the new method helps the designer deciding in which direction to proceed for less vulnerable (i.e. better) concepts. It is not intended to identify the least vulnerable concept at this stage. Since more detailed will be added later on, the least vulnerable concept in concept exploration is not necessarily the least vulnerable concept after detailed design and engineering. Summarising: the design decisions and associated methods for the concept exploration stage are all about *directionality*, in this case on where to physically place the distributed systems, and why.

Combining the research gaps from the overall ship design perspective and the vulnerability perspective, the new method needs to comply with the following requirements:

- A focus on understanding concepts in the early stage, rather than generating one or more concepts that can be used for further steps in the design process.

- A formalised, mathematics-based approach for identifying underlying driving factors for the performance (in this case: vulnerability) of the ship.
- Providing design recommendations on how the concept can be improved, using the knowledge obtained from the original concept.
- The ability to quantify graceful degradation, considering different levels of residual capability.

These requirements are the main requirements that follow directly from the gap analysis. However, based on the review of this chapter, several additional requirements arise as well:

- Different design disciplines need to be integrated early on, as discussed in Section 2.1. In terms of vulnerability, this means that different types of resources in distributed systems, such as electricity, chilled water, and data, need to be addressed simultaneously.
- The method needs to be able to do an assessment in a rapid and generalised fashion, to align with the purpose of concept exploration.
- The level of detail needs to be aligned with concept exploration, i.e. limited, but sufficient enough to provide a meaningful result.
- The vulnerability needs to be assessed in a probabilistic fashion, because 1) it is unknown where hits (or other damage) will occur, and 2) the concept of graceful degradation can not ensure a probability of 1 that certain systems will be available after damage.
- The way in which hits are modelled needs to be able to represent asymmetric threats, i.e. multiple hits with smaller damage extents, in addition to existing methods that mostly consider single hits with a large damage extent.

Based on these requirements, an appropriate mathematical approach for the new method can be selected. This is done in the next section. Subsequently, the new method is developed. This method is intended to fill the specific gap outlined in this section. Hence, the method in itself provides a solution to a self-contained problem. The same holds for other methods discussed in this chapter. However, in order to fully outline the contributions of an individual method, it needs to be discussed how the method relates to other methods, and how the right method for the right problem at the right time can be applied. By doing so, individual methods can be used as leverage towards a common goal, in this case: designing survivable naval ships. As such, a final requirement for this research arises:

- The contributions of the method need to be outlined with contributions of other methods, resulting in a clear structure on when to use which method(s) for early stage design of survivable naval ships.

## 2.5 Selecting a mathematical approach

In order to find a mathematical tool or approach that meets the requirements for the new method, several options have been investigated. First, methods for modelling different types of resources, and their interdependencies, have been investigated, as the integrated nature has been identified as an important requirement for the method. An overview for modelling and simulating techniques for interdependent resources has been provided by Rinaldi (2004). He elaborates, amongst others, on aggregate supply and demand tools, dynamic simulations, agent-based models, and physical models. Though it is explained how these models consider the interdependency aspect, they are found to be less useful for the new method. Aggregate supply and demand tools can be highly useful for e.g. load balances (functional utilisation, in terms of the architectural framework), but that part of the operational architecture is not the topic of interest for the new method. In terms of linking residual capabilities to disruptions, dynamic simulations could be more suitable. However, they have a more deterministic nature, which conflicts with the requirements for a probabilistic approach. Physics-based models are useful for highly detailed assessments, down to the level of individual components, but this quickly becomes too detailed for the concept exploration phase, where the available design information is limited. Agent-based models also have a rather deterministic nature. However, one of their advantages is that they describe the state of components in a system, and they include the option that this state may change over time or after certain occasions. This is considered a useful characteristic for the method, and has been used for further investigation.

Combining the state description of components with a probabilistic assessment approach have lead to a closer investigation of network epidemics. This method is very useful for investigating how a failure propagates through a network, based on the probability that a hurt node contaminates its neighbours (discussed by e.g. van Mieghem (2014) in more detail). A typical application is epidemiology in public health. Within a ship design context, epidemiology shows similarities with cascading failures. However, the way in which epidemiology models failure (be it disease or another type of lost performance) does not entirely align with the ship design perspective. Cascading failures in a ship are based on logical relations. For example, if a generator supplies a switchboard, which in term supplies a critical user, loss of the generator will automatically result in loss of both the switchboard and the critical user. The probabilistic aspect in this situation considers how likely it is that the associated capability is still available. In network epidemiology, however, the contaminations themselves are based on probability. For example: if person A is infected by a disease, there is a certain probability - say 40% - that he contaminates another person in his network. This way of modelling does not outline with the logical relations between system components. It makes no sense to say that there is a 40% probability that the switchboard will be off if the generator is off. Their direct relation has a more logical nature: components are either on or off. Hence, network epidemics are of limited use as well.

Subsequently, Markov theory has been investigated. Similar to epidemics, Markov theory describes the different states of a system, and the probability that this state changes. However, the state transitions are not dependent on a contamination probability, but on user-defined transition probabilities that occur on either discrete instances for a discrete-time Markov chain, or with certain rates for a continuous-time Markov chain (also discussed in more detail by e.g. van Mieghem (2014)). The discrete approach introduces the opportunity to link the state description (in the case of the ship: the level of residual capability) to hits (discrete events). This aligns well with the requirement to quantify graceful degradation. The probabilistic nature of a discrete-time Markov chain also allows for simulating multiple smaller hits instead of one large hit, which is needed to simulate asymmetric threats. As for the other requirements, Markov theory is expected to be applicable as well. Its computations involve vector-matrix multiplications, which can be carried out in a rapid fashion. Interdependencies between the different types of resources can be addressed though the definition of the states, and matrix decomposition can help in expressing the vulnerability of the ship in a formalised, mathematics-based way. Hence, Markov theory has been selected as the mathematical basis for the new method. More specifically, a discrete-time Markov chain will be used, as it allows for modelling individual hits or failures. Continuous-time Markov chains inherently provide the steady state for a system that is subject to transition rates over a longer period of time. Since recoverability and repair are not considered in this thesis, this by definition results in the state where all capabilities are eventually lost. This is a trivial result that has no practical meaning, especially because the way in which that state is obtained does not matter due to the 'averaged' nature of the continuous time approach. Hence, for this application, continuous-time Markov chains are not suitable. Nevertheless, they have been applied in another early stage ship design research effort, where the importance of components in a distributed systems network has been investigated (Mooren, 2018). Since continuous-time Markov chains are not considered in this dissertation, a discrete-time Markov chain will simply be referred to as 'Markov chain' for the remainder of this dissertation.

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 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 these examples, the Markov chain is mainly used for analysis purposes. Identifying driving factors and obtaining design recommendations - which are requirements of the new method - are not covered in these studies. 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 component-based assessment is less applicable for the capabilities perspective that is required for the new method, as one capability may require multiple components, or one component may support multiple capabilities. The set-up of the Markov chain in this dissertation therefore differs from the set-up used by Kim and Lee (2012). Other applications of a Markov chain in maritime technology exist as well. Most of them consider aspects of ship operations, in some cases connected to ship design. For example, Pruijn (2020) applies a Markov chain for estimating port waiting times for vessels. Kana and Harrison (2017) provide decision-support on when to implement new (environmental-proof) technologies on board, such as dual fuel engines, in the light of uncertain future emission regulations. This is done with a Markov Decision Process, which is a stochastic control process that uses a Markov chain. Niese et al. (2015) also investigate policy-making under uncertain emission regulations, and link this to analysing different alternatives for concepts in the early design stage. Strom et al. (2018) use a Markov Decision Process to develop a contingency plan for a ship faced with uncertainties in future missions, business strategies, and market states.

# Chapter 3

# Early stage vulnerability assessment method

In response to the gap analysis and method requirements discussed in Chapter 2, this chapter presents the principles of a new method for assessing vulnerability in the early design stage. In Section 2.5, Markov theory has been selected as the mathematical basis for the new method. Section 3.1 gives a brief explanation on Markov theory. Subsequently, Section 3.2 discusses how Markov theory is applied in the set-up of the new method. Section 3.3 explains which computations are carried out by the method. The results of these computations are discussed in Section 3.4. These sections use a simple, conceptual physical solution to prove the concept. Subsequently, Section 3.5 lists several steps that need to be taken to extend the method from the proof of concept to a more practical setting. Together, these sections provide a method for assessing the vulnerability. This is the first part of the research objective. In addition to that, the second part of the research objective states that the driving factors for the vulnerability, and design recommendations towards better solutions need to be obtained. Section 3.6 explains how this can be achieved. A brief summary of the method is provided in Section 3.7.

## 3.1 Mathematical principles of Markov theory

The basis of a Markov chain consists of a state vector $\mathbf{s}$ and a transition matrix $T$. Let $n$ be the number of all possible states that the system can be in. The state vector $\mathbf{s}$ is a row vector of length $n$. The values of the elements of $\mathbf{s}$ represent the probability that the system is in that specific state. Hence, the sum of $\mathbf{s}$ equals 1. The initial state is represented as $\mathbf{s}(0)$. The probability of transferring between states at discrete time steps is described by $T$. The dimensions of $T$ are $n \times n$. Element $T_{i,j}$ denotes the probability of transferring from state $i$ to state $j$. For each row in $T$ the sum equals 1. An example of a system with two states is provided in Figure 3.1. An example of an associated initial state vector is given in Equation 3.1. It is assumed here that the

Parts of this chapter are based on Habben Jansen et al. (2018, 2019, 2020a).

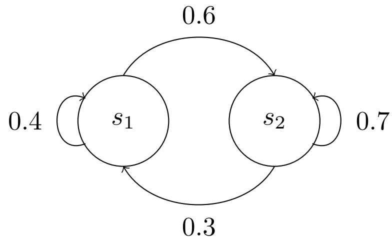



**Figure 3.1:** Example of a system with two states

system initially is in state 1. The associated transition matrix is given in Equation 3.2.

$$\mathbf{s}(0) = \begin{bmatrix} 1 & 0 \end{bmatrix} \tag{3.1}$$

$$T = \begin{bmatrix} 0.4 & 0.6 \\ 0.3 & 0.7 \end{bmatrix} \tag{3.2}$$

The behaviour of the system over time can be calculated by multiplying $\mathbf{s}$ with $T$. For example, for the first two time steps, the state probabilities become as follows:

$$\mathbf{s}(1) = \mathbf{s}(0) \cdot T = \begin{bmatrix} 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0.4 & 0.6 \\ 0.3 & 0.7 \end{bmatrix} = \begin{bmatrix} 0.4 & 0.6 \end{bmatrix} \tag{3.3}$$

$$\mathbf{s}(2) = \mathbf{s}(1) \cdot T = \begin{bmatrix} 0.4 & 0.6 \end{bmatrix} \cdot \begin{bmatrix} 0.4 & 0.6 \\ 0.3 & 0.7 \end{bmatrix} = \begin{bmatrix} 0.34 & 0.66 \end{bmatrix} \tag{3.4}$$

In general, this can be expressed for any time step $h$ as:

$$\mathbf{s}(h) = \mathbf{s}(h-1) \cdot T \tag{3.5}$$

If $T$ does not change over time, this can be simplified to:

$$\mathbf{s}(h) = \mathbf{s}(0) \cdot T^h \tag{3.6}$$

In some cases, depending on $T$, the system may reach a steady state after a certain amount of time steps, i.e. $\mathbf{s}(h+1) = \mathbf{s}(h)$. If this happens, Equation 3.5 becomes (Lay, 2006):

$$\mathbf{s} = \mathbf{s}T \tag{3.7}$$

This is in fact the eigenvector equation:

$$\mathbf{x}A = \lambda\mathbf{x} \tag{3.8}$$

under the condition $\lambda = 1$. This property is independent of $\mathbf{s}(0)$, and only holds if $\lambda_{max} = 1$ is unique. In other words, if other eigenvalues equal 1 as well, a steady state may not be reached (Lay, 2006). This property has proven to be highly relevant for the new method, as the eigenvalues of the transition matrix can be used to link the level of vulnerability to specific parts of the physical solution. This will be explained further in Section 3.6. Another property of a Markov chain is the fact that the time steps $h$ do not necessarily have to represent actual time steps in seconds or any other time unit. They are event-based, meaning that they represent occasions where an event occurs that may lead to a change in the state vector, i.e. a change in the condition of the system. This general nature of the time steps is used as well for the set-up of the new method.

## 3.2 Set-up of the method

Chapter 1 has mentioned that the compartments of the ship and the logical architecture of the main components of the distribution system are assumed to be known for the vulnerability assessment. In other words: a physical solution needs to be available. At the same time, the concept exploration phase exists to find out what is wanted. It may sound contradictory that something needs to be known at this stage already. However, at this stage, concepts are generated for the sake of exploring and understanding the design space. Converging to an actual solution is done afterwards, in the concept definition stage. Hence, the starting point for concept exploration does not need to be closely related upfront to what the eventual concept that results from concept definition will look like. In other words: there is a certain amount of freedom to choose the starting point for concept exploration, as long as the scope, limitations and assumptions of the concept exploration methods are acknowledged. The importance of the latter is demonstrated by Jaspers (2017), who has shown for a particular test case that clusters found in alternative ship design concepts were based on the computational starting point, rather than on actual ship design related parameters, such as length or displacement. Summarising: the starting point matters, but while considering the scope of the applied methods, concept exploration allows freedom in choosing the starting point.

A suitable rule of thumb for starting an exploration effort is that the starting point should be representative for what needs to be investigated. For example, if the advantages and disadvantages of an IPS over a conventional concept need to be investigated (such as in the test case of Chapter 4), the two associated logical architectures needs to be sufficiently detailed to capture that difference, without containing abundant details. In the very early stages this could even be done by hand, where (automated) tools can provide concepts later on. This is also discussed in Chapter 5.

If a basic physical solution of the ship is available, a Markov chain such as described in Section 3.1 can be used to do an early stage vulnerability assessment. In terms of the new method, the states represent the availability of systems. If $n_s$ is the number of systems, and each system can either be on or off, the total number of possible states is $2^{n_s}$. In State 1 all systems are on, in State $2^{n_s}$ all systems are off, and the intermediate states contain all possible combinations of several systems being on and several systems being off. Hence, the state vector $\mathbf{s}$ has length $2^{n_s}$, and the transition matrix $T$ has size $2^{n_s} \times 2^{n_s}$. The transition probabilities can be derived from the physical solution of the ship, which is assumed to be available. The ship is subdivided in compartments. Let $n_c$ be the number of compartments. It is now assumed that the ship gets hit, and that the hit will disable one of the compartments, while all other compartments remain intact. The hit probability is assumed to be equal for all compartments and for any time step in the Markov chain. Hence, each compartment has a probability of $1/n_c$ to get hit. In other words: hit scenarios consist of multiple hits with one damaged compartment per hit, which aligns with the requirement to account for asymmetric threats. Based on which systems and routings are located inside a hit compartment, a transition to another state may occur. Repair of systems is not considered, which means that it is not possible to transfer to states where systems that were already off, are on again. The reason for leaving out repairs is that recoverability is mainly - though not exclusively - an operational aspect, and is mostly dealt with by the crew rather than the designer. Nevertheless, the mathematical set-up of the Markov chain relies on user-defined transition probabilities, so repairs could also be accounted for with a Markov chain, as long as repair probabilities are known or estimated.

At $t = 0$ all systems are assumed to be on (State 1). At $t = 1$ the first hit occurs in an arbitrary compartment. If no systems or routings are located in the compartment that was hit, there is no transition to another state. In all other cases, there will be a transition to another state. Which state this is, depends on which systems and/or routings are located in that compartment. The probability of transferring to another state after a hit can be derived from the number of compartments that a system occupies. It is not needed to know the exact location of the hit, as this method considers all possible hit locations. In this fashion the first row of $T$ can be constructed. For all other rows, a similar procedure can be followed. However, for these rows it needs to be assumed that the corresponding systems are already down. The number of hits that happened previously to end up in that state does not matter. In state $2^{n_s}$ all systems are down. Since there is no possibility to hit any more systems, the probability of staying in that state is 1. Once the transition matrix has been built, the probabilities for each state can easily be determined for any number of hits with Equation 3.6.

## 3.3 Method computations

The set-up of the method described in Section 3.2 is now demonstrated by means of three physical solutions of a conceptual nature. These physical solutions are referred to with the abbreviation PS. Consider a square grid with $3 \times 3$ 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 systems are placed in the grid in various ways. In PS 1 the routings cross each other in one compartment. In terms of the architectural framework, this is an overlap in the physical architecture. In PS 2 the systems share the power source, so there is an overlap in the logical architecture. In PS 3 the systems do not overlap, and they share no components. Hence, there is no physical or logical relation between the two systems. The three physical solutions are presented in Figure 3.2.

For each physical solution, there are two systems, that can be either on or off. This results in four possible states for the availability of systems:

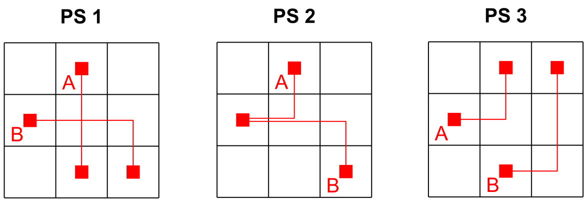



**Figure 3.2:** Three conceptual physical solutions for the vulnerability assessment, with a physical relation (PS 1), a logical relation (PS 2), and no relation (PS 3). Figure adapted from Habben Jansen et al. (2018).

- State $s_1$: Systems A and B are both on
- State $s_2$: Only system A is on
- State $s_3$: Only system B is on
- State $s_4$: Both systems are off

Hence, $\mathbf{s}$ has length 4, and $T$ has size $4 \times 4$. In the initial state all systems are on, so:

$$\mathbf{s}(0) = \begin{bmatrix} 1 & 0 & 0 & 0 \end{bmatrix} \tag{3.9}$$

The transition matrix is dependent on the physical solution. PS 1 is considered first. 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 are 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 a combination of them is 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 off. 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 for PS 1:

$$T_1 = \begin{bmatrix} 3/9 & 3/9 & 2/9 & 1/9 \\ 0 & 6/9 & 0 & 3/9 \\ 0 & 0 & 5/9 & 4/9 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{3.10}$$

For PS 2 and PS 3, $T$ can be obtained in a similar fashion. The transition matrices for PS 2 and PS 3 are given in Equations 3.11 and 3.12, respectively. Their first rows are different, which illustrates that $T$ is a function of the physical solution.

$$T_2 = \begin{bmatrix} 4/9 & 2/9 & 1/9 & 2/9 \\ 0 & 6/9 & 0 & 3/9 \\ 0 & 0 & 5/9 & 4/9 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{3.11}$$

$$T_3 = \begin{bmatrix} 2/9 & 4/9 & 3/9 & 0 \\ 0 & 6/9 & 0 & 3/9 \\ 0 & 0 & 5/9 & 4/9 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{3.12}$$

The probability of being in any state after any number of hits can now be calculated by multiplying $\mathbf{s}(0)$ with $T^h$, where $h$ is the number of hits.

In order to highlight the need for an approach where all systems are assessed together, such as the Markov-based method described above, a comparison is made with the situation where all systems are assessed individually, as would be done if the problem would be decomposed to individual systems to assess their vulnerability independently. For example, the availability of the systems would then merely be the product of the probabilities that each individual system is available (see Figure 3.3), because in standard probability theory, the probability that multiple events happen at the same time equals the product of the probability of separate, independent events (Dekking et al., 2005). With this approach, system A has a probability of 6/9 to be available after a hit, and system B a probability of 5/9. For $h$ hits, the probabilities for each state then become:

$$Pr(s_1) = (6/9)^h \cdot (5/9)^h \tag{3.13a}$$

$$Pr(s_2) = (6/9)^h \cdot (1 - (5/9)^h) \tag{3.13b}$$

$$Pr(s_3) = (1 - (6/9)^h) \cdot (5/9)^h \tag{3.13c}$$

$$Pr(s_4) = (1 - (6/9)^h) \cdot (1 - (5/9)^h) \tag{3.13d}$$

Since this approach does not account for the fact that the systems may overlap or share components, the probabilities in Equation 3.13 are independent of the physical location of the systems. For reference, the explicit mathematical expressions of the vector-matrix multiplication of the Markov method for PS 1 are given in Equation 3.14. These equations are found by diagonalising $T$ (see e.g. Lay (2006) for more details on diagonalising matrices. This technique has also been applied in further developments of the method, see Section 3.6.). These equations are dependent on the transition matrix, and thus on the physical solution. For PS 2 and PS 3 the transition

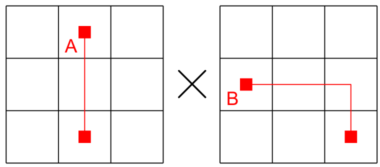



**Figure 3.3:** PS 1 if the systems are assessed in a decomposed fashion. Figure retrieved from Habben Jansen et al. (2018).

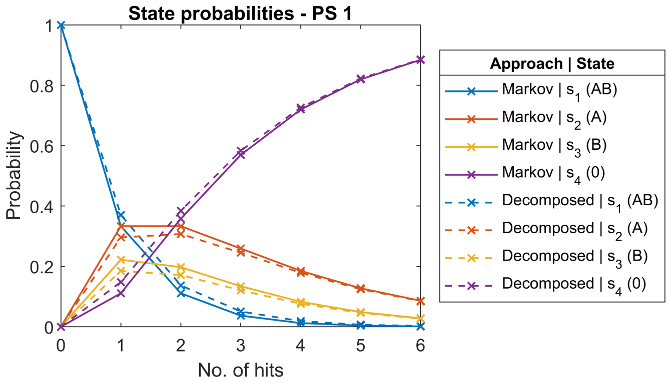
matrix and equations change. They can be obtained in a similar fashion as for PS 1, such as described above. The difference in the equations for the decomposed approach and the Markov method is a subtle but important property of this method, that highlights the need for an integrated approach. The implications of this characteristic are discussed in Section 3.4.

$$Pr(s_1) = (1/3)^h \tag{3.14a}$$
$$Pr(s_2) = -(1/3)^h + (2/3)^h \tag{3.14b}$$
$$Pr(s_3) = -(1/3)^h + (5/9)^h \tag{3.14c}$$
$$Pr(s_4) = (1/3)^h - (2/3)^h - (5/9)^h + 1 \tag{3.14d}$$

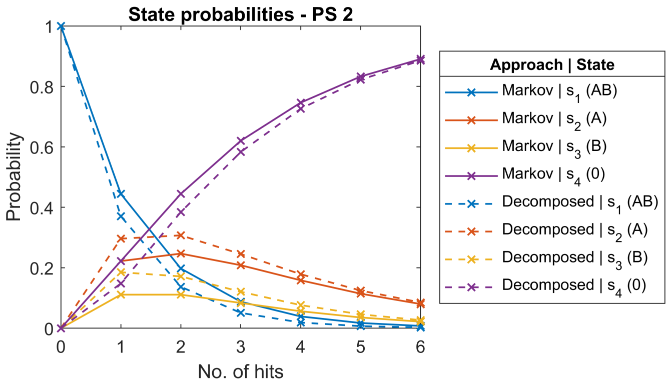
## 3.4 Method results

The results of the calculations of Section 3.3 are curves that represent the probability for every state after any number of hits. For this test case, results are calculated up to 6 hits. The amount of hits is not decisive for the complexity of the computation, as all hit scenarios are inherently included in the transition matrix. The reason for selecting 6 hits is that it spans the scope from zero to serious damage, in order to investigate what happens in between. The results are presented in Figures 3.4. For PS 1, small differences between the Markov method and the decomposed approach can be observed, but the deviation from the decomposed approach is small. For PS 2, the deviation from the decomposed approach is larger. The most distinct deviation from the decomposed approach occurs for PS 3. This is an interesting result, as PS 3 is the only physical solution where there is no overlap between system A and system B.

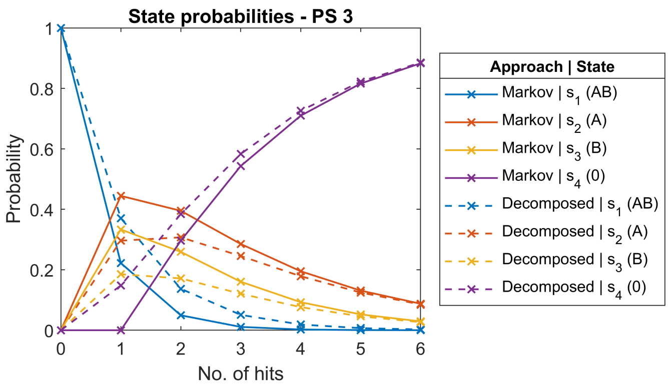
The difference between the Markov method and the decomposed approach has already been mathematically derived in Section 3.3. In addition to that, the differences can also be interpreted rationally. Consider for example PS 3. In this physical solution, only 2 out of 9 compartments are empty (see Figure 3.2). With the decomposed approach, the number of empty compartments is 6 (for system A) and 5 (for system B). Hence, the decomposed approach overestimates the number of empty compartments. Due to this, the probability for $s_1$, where both systems are on, is overestimated. The probability for $s_4$, where both systems are off, is overestimated as well. As the systems do not overlap, at least 2 hits are needed to arrive in this state. However, this is not considered in the decomposed approach, where the two systems are independent.




**(a)** PS 1




**(b)** PS 2




**(c)** PS 3

**Figure 3.4:** State probabilities for PS 1, PS 2, and PS 3. Figure adapted from Habben Jansen et al. (2018).

Following the same argumentation for $s_2$ and $s_3$, it can be derived that the probabilities for these states are underestimated.

The absolute difference between the two methods is listed in Table 3.1. A positive difference means a higher probability for the Markov method, while a negative difference means a higher probability for the decomposed approach. By definition the state probabilities for the Markov approach and the decomposed approach both sum to one for every number of hits. Subsequently, the underestimations and overestimations of the decomposed approach always sum to one as well. Furthermore, the absolute values of the difference are always the same. This is because the numbers of hits and compartments are discrete integers, leading to discrete fractions that form the probabilities. For example, the probability for $s_1$ after one hit for PS 3 is 14.81% (i.e. 4/27) higher for the decomposed approach than the Markov method. This can also be seen in Figure 3.4. Table 3.1 shows that the differences are the largest for one hit, regardless of the physical solution. For an increasing number of hits, the differences become smaller, which indicates that there is eventually no longer any difference between the results of the Markov method and the decomposed approach. This aligns with the expectations, because for (very) large numbers of hits, the probability for $s_4$ eventually approaches 1 (and 0 for the other states), regardless if the Markov method or the decomposed approach is used. This is also supported by the equations for the numbers in Table 3.1. For PS 1, this leads to Equation 3.15, which is the difference between Equations 3.14 and 3.13:

$$dPr(s_1) = (1/3)^h - [\,(6/9)^h \cdot (5/9)^h] \tag{3.15a}$$

$$dPr(s_2) = -(1/3)^h + (2/3)^h - [\,(6/9)^h \cdot (1 - (5/9)^h)] \tag{3.15b}$$

$$dPr(s_3) = -(1/3)^h + (5/9)^h - [\,(1 - (6/9)^h) \cdot (5/9)^h] \tag{3.15c}$$

$$dPr(s_4) = (1/3)^h - (2/3)^h - (5/9)^h + 1 - [\,(1 - (6/9)^h) \cdot (1 - (5/9)^h)] \tag{3.15d}$$

In all these equations, except for 3.15d, all bases of the exponent are smaller than 1, which results in an approximation of zero for $h \rightarrow \infty$. In Equation 3.15d two terms with value 1 occur, but as they have a positive and negative sign, respectively, this yields zero as well. Translated to actual physical solution, this means that Equation 3.15 is a metric for the interdependency between the two systems, which is highest for a low number of hits, and decreases for higher numbers of hits.

Though these results are rather straightforward due to the relative low complexity of the physical solutions, two interesting conclusions can be drawn with respect to the vulnerability of on-board distributed systems:

1. Need for an integrated approach: The method shows that the vulnerability needs to be assessed in an integrated fashion. If systems are considered separately with the decomposed approach described above, a major assumption of probability theory is violated, namely that the systems are independent. This is not the case in reality. Though the need for an integrated approach appears to be generally known to designers of distributed systems, it may happen in practice that systems are designed separately. For example, if designer X designs a survivable electrical distribution system, designer Y designs a survivable fire-fighting

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| **s1** | 0.0000 | -0.0370 | -0.0261 | -0.0138 | -0.0065 | -0.0029 | -0.0012 |
| **s2** | 0.0000 | 0.0370 | 0.0261 | 0.0138 | 0.0065 | 0.0029 | 0.0012 |
| **s3** | 0.0000 | 0.0370 | 0.0261 | 0.0138 | 0.0065 | 0.0029 | 0.0012 |
| **s4** | 0.0000 | -0.0370 | -0.0261 | -0.0138 | -0.0065 | -0.0029 | -0.0012 |

**(a)** PS 1

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| **s1** | 0.0000 | 0.0741 | 0.0604 | 0.0370 | 0.0202 | 0.0104 | 0.0051 |
| **s2** | 0.0000 | -0.0741 | -0.0604 | -0.0370 | -0.0202 | -0.0104 | -0.0051 |
| **s3** | 0.0000 | -0.0741 | -0.0604 | -0.0370 | -0.0202 | -0.0104 | -0.0051 |
| **s4** | 0.0000 | 0.0741 | 0.0604 | 0.0370 | 0.0202 | 0.0104 | 0.0051 |

**(b)** PS 2

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| **s1** | 0.0000 | -0.1481 | -0.0878 | -0.0398 | -0.0164 | -0.0064 | -0.0025 |
| **s2** | 0.0000 | 0.1481 | 0.0878 | 0.0398 | 0.0164 | 0.0064 | 0.0025 |
| **s3** | 0.0000 | 0.1481 | 0.0878 | 0.0398 | 0.0164 | 0.0064 | 0.0025 |
| **s4** | 0.0000 | -0.1481 | -0.0878 | -0.0398 | -0.0164 | -0.0064 | -0.0025 |

**(c)** PS 3

**Table 3.1:** Difference between the results of the Markov method and the decomposed method for PS 1, PS 2, and PS 3. The rows denote the four states, the columns denote the number of hits.

system, and designer Z designs a survivable chilled water distribution system, it does not necessarily imply that the combination of these three survivable systems lead to a survivable ship as a whole.

2. Systems in one physical solution are related: it can be concluded from this proof-of-concept that the fact *that* systems are placed together in one physical solution (i.e. in one ship) already relates them from a vulnerability perspective. This also holds if there is no physical or logical overlap between the systems. This is a further reinforcement of the need for an integrated approach for vulnerability, even if systems are seemingly unrelated.

## 3.5 Extended features of the method

The method described in Sections 3.2 to 3.4 has a conceptual nature. The physical solution that has been used to illustrate the method has little complexity and is not representative for a concept that is used during practical early stage design. Hence, extended features are needed to make the method useful for that purpose. These methods are discussed in this section. First, Section 3.5.1 explains how the logical architecture can be scaled up in complexity. Subsequently, Section 3.5.2 elaborates on how different hit probability distributions can be incorporated. Section 3.5.3 explains how a transition from individual systems to higher-level ship capabilities can be made. Finally, Section 3.5.4 explains how the transition matrix is automatically generated for larger, more complex physical solutions.

### 3.5.1 Scaling up in complexity

The logical architecture 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 logical architecture of distributed systems 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 distributed systems, such as a chilled water unit, which is a consumer for electrical distribution, but a supplier for chilled water distribution. A different definition of systems is therefore needed.

Consider the example of a logical architecture in Figure 3.5. The system components are the nodes, and the connections between them are the edges. Because this logical architecture 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. Likewise, if Consumer 1 is hit, Connections 1 and 3 are on, and Connection 2 is off.

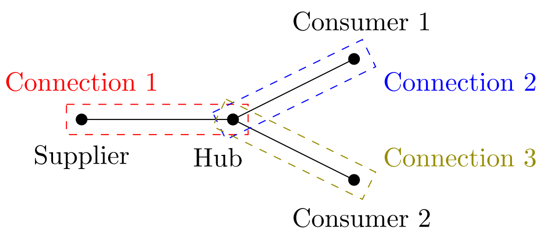



**Figure 3.5:** Definition of connections as used for the new method. Figure adapted from Habben Jansen et al. (2020a).

In addition to the increased complexity of the logical architecture, the number of compartments in the ship increases as well for practical applications of the method.

However, this does not impose complications for the computation. The size of the transition matrix is independent of the number of compartments. The number of compartments only influences the values of individual entries in the transition matrix.

### 3.5.2 Hit probabilities

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, weight factors can be applied.

In order to apply a Markov chain for the 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 3.16:

$$w_1 \cdot \frac{1}{n_c} + w_2 \cdot \frac{1}{n_c} + \ldots + w_{n_c} \cdot \frac{1}{n_c} = 1 \tag{3.16}$$

This leads to:

$$\sum w_1 \ldots w_{n_c} = n_c \tag{3.17}$$

Any combination of values that complies with the scaling method of Equation 3.17 can be used within the 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 4.2.

### 3.5.3 Systems to capabilities

Paragraph 3.5.1 has explained why systems need to be broken down in individual connections to apply the new method on a larger scale. However, the eventual question is whether critical capabilities are still available after hits, rather than which 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 connections to thinking in capabilities. These main capabilities 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. 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 fighting capability may no longer be fully relevant, and the focus may be with float. The relation between residual capability and impact level is visualised in Figure 3.6. These various levels of capabilities may be interdependent (Liwang and Jonsson, 2015). Optimising for a certain level of residual capability may compromise other levels of residual capability, which results in a trade-off that is typically investigated during concept exploration (see Section 1.1). This will also be shown with a test case in Section 4.3. In terms of the architectural framework of Brefort et al. (2018), the required residual capability is part of the operational architecture.

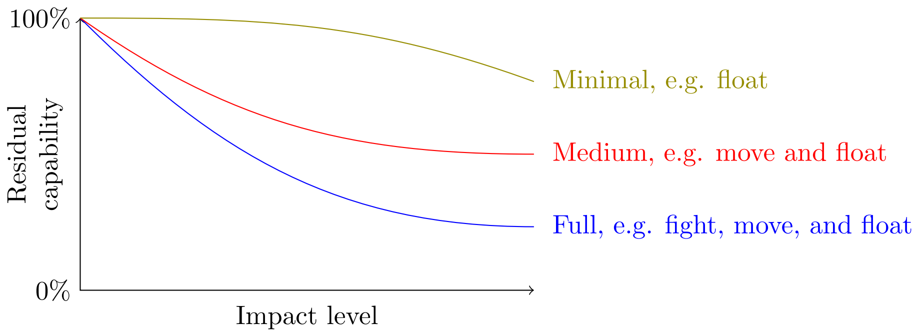



**Figure 3.6:** Example of the relation between residual capability and impact level. The higher the impact level, the lower the level of required residual capability. Figure adapted from Habben Jansen et al. (2019).

It may sound contradictory that there is a need for thinking in high-level capabilities, while Paragraph 3.5.1 advocated for a method where distributed systems are broken down into individual connections. However, these connections are needed because of the supplier-hub-consumer structure of the logical architecture of the distributed systems. For example, consider the distributed system of Figure 3.5 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 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 and their interdependencies are needed.

To make the transition from connections to capabilities, states of the Markov chain that contribute to a capability need to be clustered, and their state probabilities need to be added together. Logical relations should be taken into account while doing this. If it is still assumed that Consumers 1 and 2 of Figure 3.5 are redundant CIWSs, the self-defence capability is present if at least Connections 1 and 2 OR Connections

**Table 3.2:** All possible states for the example network of Figure 3.5. The red states represent states that contribute to the self-defence capability.

| State number | Connection 1 | Connection 2 | Connection 3 |
|---|---|---|---|
| **1** | **1** | **1** | **1** |
| **2** | **1** | **1** | **0** |
| **3** | **1** | **0** | **1** |
| 4 | 1 | 0 | 0 |
| 5 | 0 | 1 | 1 |
| 6 | 0 | 1 | 0 |
| 7 | 0 | 0 | 1 |
| 8 | 0 | 0 | 0 |

1 and 3 are on. As can be seen in Table 3.2, States 1, 2, and 3 contribute to this capability. The probability for the self-defence capability can thus be obtained from individual state probabilities as follows, regardless of the number of hits:

$$Pr(\textit{self-defence}) = Pr(s_1) + Pr(s_2) + Pr(s_3) \tag{3.18}$$

The same procedure can be followed for any capability of any concept that is considered for a vulnerability assessment.

### 3.5.4 Automatic generation of the transition matrix

Section 3.2 explained that the size of the transition matrix is $2^{n_s} \times 2^{n_s}$. For the proof-of-concept, with two systems, this has resulted in a $4 \times 4$ matrix, which was derived manually from the physical solution. This manual derivation serves the purpose of explaining the method set-up, but quickly becomes cumbersome for larger numbers of systems. Hence, an algorithm has been developed for automatic generation of the transition matrix. This has been done in the form of a function in MATLAB. This programme has been used for all computations described in this dissertation. The function follows the same rationale as the manual derivation. The physical solution is assumed to be available as matrix $PS$, which consists of $n_s$ rows and $n_c$ columns, where $n_c$ is the number of compartments. If system $i$ is located in compartment $j$, element $\{i, j\}$ of $PS$ equals 1, otherwise it equals zero. Hence, a row of $PS$ describes in which compartments a connection is located. Subsequently, the transition matrix is derived with the procedure of Algorithm 1.

The total number of elements in the $T$ equals $2^{2n_s}$. This very strong increase in size limits the number of connections that can be considered. For standard settings of MATLAB, the maximum allowable number of connections is 13. In that case, $T$ consists of about 6.7e+07 elements, which equals 5.4e+08 bytes. This is reasonably below the maximum memory (~2.8e+10 bytes). This way, the duration for generating the transition matrix remains reasonable (in the order of several minutes). In addition to that, sufficient memory for the rest of the computations remains. The practical consequences of this limitation for an actual design effort are discussed in more detail in Section 4.1.

**Data:** Physical solution matrix (PS)
**Result:** Transition matrix

Derive number of connections ($n_s$) from physical solution matrix;
Generate a vector of all possible states ($2^{n_s}$), expressed as binary numbers;
Generate a matrix ($2^{n_s} \times 2^{n_s}$) that describes the difference between all states;
**foreach** *state* **do**
  Count how many compartments need to be hit to go to the other states;
  Divide that number by total number of compartments ($n_c$)
**end**

**Algorithm 1:** Pseudo-code for automatic generation of the transition matrix

## 3.6 Eigenvalue analysis

Chapters 1 and 2 have highlighted the need for design methods that not only assess the performance of a concept, but also elucidates the driving factors for that performance. In terms of the new method, this means that it is not only relevant to know the shape the vulnerability curves of Figure 3.4, but also to understand why the curves are shaped that way. With the latter, driving factors and potential trade-offs can be understood more completely. It has already been shown in Equation 3.14 that the vulnerability curves can be formulated explicitly with matrix diagonalisation. This section shows how this technique contributes to understanding the shape of the vulnerability curves.

It has already been explained that the state probabilities can be obtained by multiplying the initial state vector with the $h^{th}$ power of the transition matrix. For higher powers of $h$ it quickly becomes cumbersome to write out all matrix entries explicitly. However, higher powers of the transition matrix can also be expressed as:

$$T^h = PD^hP^{-1} \tag{3.19}$$

which is by definition the equation for matrix diagonalisation (Lay, 2006). In this equation, $D$ is a diagonal matrix with the eigenvalues of $T$ on the diagonal, and $P$ contains the respective right eigenvectors. This holds if and only if all eigenvectors of $T$, i.e. all columns of $P$, are linearly independent (Lay, 2006). This dissertation does not contain a proof that this universally holds for the transition matrix of any physical solution in general. However, it can be checked upfront if a transition matrix is diagonalisable by computing the rank of its associated matrix $P$. If the rank of $P$ equals its size, $T$ is indeed diagonalisable. This has turned out to be the case for all cases described in this dissertation, which indicates - but does not prove - that $T$ is always diagonalisable in the new method.

In addition to $P$, the diagonal matrix $D$ needs to be constructed as well. This requires the eigenvalues of $T$. Since the vulnerability assessment only considers damage of systems, and not repairs, $T$ is always an upper triangular matrix. Hence, the eigenvalues of $T$ are the entries on its diagonal. As a result, the diagonal of $D$ contains the same values as the diagonal of $T$. For PS 1, which was also considered in Section 3.3, this leads to:

$$D = \begin{bmatrix} \lambda_1 & 0 & 0 & 0 \\ 0 & \lambda_2 & 0 & 0 \\ 0 & 0 & \lambda_3 & 0 \\ 0 & 0 & 0 & \lambda_4 \end{bmatrix} = \begin{bmatrix} 3/9 & 0 & 0 & 0 \\ 0 & 6/9 & 0 & 0 \\ 0 & 0 & 5/9 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{3.20}$$

The associated right eigenvectors are the columns of $P$:

$$P = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{3.21}$$

The rank of $P$ is 4, so the columns of $P$ are linearly independent. As such, matrix diagonalisation is indeed possible, so the state probabilities can indeed be expressed explicitly. The inverse of $P$ matrix is needed as well for this:

$$P^{-1} = \begin{bmatrix} 1 & -1 & -1 & 1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{3.22}$$

Hence, Equation 3.19 becomes:

$$T^h = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} \lambda_1^h & 0 & 0 & 0 \\ 0 & \lambda_2^h & 0 & 0 \\ 0 & 0 & \lambda_3^h & 0 \\ 0 & 0 & 0 & \lambda_4^h \end{bmatrix} \begin{bmatrix} 1 & -1 & -1 & 1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{3.23}$$

Writing this out, this leads to:

$$T^h = \begin{bmatrix} \lambda_1^h & -\lambda_1^h + \lambda_2^h & -\lambda_1^h + \lambda_3^h & \lambda_1^h - \lambda_2^h - \lambda_3^h + \lambda_4^h \\ 0 & \lambda_2^h & 0 & -\lambda_2^h + \lambda_4^h \\ 0 & 0 & \lambda_3^h & -\lambda_3^h + \lambda_4^h \\ 0 & 0 & 0 & \lambda_4^h \end{bmatrix} \tag{3.24}$$

Finally, the state probabilities can be found by multiplying $T^h$ with the initial state vector, which is (see Equation 3.9):

$$\mathbf{s}(0) = \begin{bmatrix} 1 & 0 & 0 & 0 \end{bmatrix} \tag{3.25}$$

For PS 1 this leads to:

$$Pr(s_1) = \lambda_1^h = (3/9)^h \tag{3.26a}$$
$$Pr(s_2) = -\lambda_1^h + \lambda_2^h = -(3/9)^h + (6/9)^h \tag{3.26b}$$
$$Pr(s_3) = -\lambda_1^h + \lambda_3^h = -(3/9)^h + (5/9)^h \tag{3.26c}$$
$$Pr(s_4) = \lambda_1^h - \lambda_2^h - \lambda_3^h + \lambda_4^h = (3/9)^h - (6/9)^h - (5/9)^h + 1 \tag{3.26d}$$

The right hand side of these equations is equal to Equation 3.14. Hence, it is shown that the state probabilities are only dependent on the eigenvalues of $T$. A major advantage is that this holds for any physical solution with two systems, regardless of the number of compartments or the physical location of the systems in the compartments. In other words: for PS 2 and PS 3 these eigenvalue equations still hold, only the actual numeric values of the eigenvalues become different.

With this assessment, a specific, pre-defined physical solution can be used to generate generalised design knowledge. This, in turn, can be used to search for alternative solutions, and to evaluate the interdependencies between the states. Consider for example the situation where there is a desire to maximise the probability that both systems are on, i.e. to maximise $Pr(s_1)$. This probability is dependent on $\lambda_1$ only. This is element $\{1, 1\}$ of the transition matrix, i.e. the probability to remain in $s_1$ given that the previous state was $s_1$ already. In this example, this probability is 3/9, corresponding to the number of compartments where no systems are located. To increase the probability, this value needs to be increased. This implies that more compartments need to be empty, i.e. systems A and B need to be concentrated more, which is sensible from a physical perspective. However, this comes at a cost, as increasing $\lambda_1$ has a negative effect on the probabilities for $s_2$ and $s_3$. Hence, this leads to an increased probability that both systems are on after one or more hits, but the probability that at least one of the systems is on, reduces. Though this result seems rather straightforward for this conceptual physical solution, this method can be extended to larger, more complex physical solutions as well, enabling a better understanding of the trade-off between ship capabilities. Following the systems to capabilities procedure of Section 3.5.3, the probabilities of individual states that contribute to a capability need to be clustered and added together. The associated equation is:

$$Pr(c_i) = \sum_{k=1}^{n} f_k \cdot \lambda_k^h \tag{3.27}$$

where $c_i$ denotes the $i^{th}$ capability level, $\lambda_k$ denotes the $k^{th}$ eigenvalue of the transition matrix, where $k$ runs from 1 to the number of states, $h$ is the number of hits, and $f_k$ is an integer factor that states how strong the contribution of $\lambda_k$ is, and which sign it has. For example, in Equation 3.26b $f_k = -1$ for $\lambda_1$ and $f_k = 1$ for $\lambda_2$. Depending on which states are added together, $f_k$ is positive, negative, or zero. If $f_k$ is zero, the associated eigenvalue $\lambda_k$ has no influence on the level of vulnerability. Chapter 4 elaborates on this in more detail with a test case.

## 3.7 Method summary

This chapter has provided a proof-of-concept for a method for an early stage assessment of the vulnerability of distributed systems. A basic physical solution is assumed to be available at this stage. The method provides a quantitative metric for the vulnerability by means of a discrete time Markov chain. By means of the eigenvalues of the associated transition matrix, the level of vulnerability can be linked to specific parts of the physical solution. Due to the generalised nature of the eigenvalue assessment, one physical solution is representative for all physical solutions, given a fixed logical architecture. Using this, the designer can obtain guidance and directionality towards other, potentially better, physical solutions. The proof-of-concept has been compared to a vulnerability assessment where the physical solution is decomposed into individual systems. The latter violates the assumption that the individual systems are independent. The results of this decomposed approach deviate considerably from the Markov approach, which inherently assesses the vulnerability in an integrated fashion. This even holds if systems in a physical solution have no physical or logical overlap. This enhances the need for an integrated approach. Finally, several extended features are added to the method to make it better suited for a practical early stage vulnerability assessment of distributed systems on board a naval ship.

# Chapter 4

# Test case: Oceangoing Patrol Vessel

This chapter illustrates the new method by means of a test case with a notional Oceangoing Patrol Vessel (OPV). This chapter assesses vulnerability in terms of hits, i.e. for situations where the physical solution is relevant (see Section 3.2). Vulnerability in terms of complex distributed systems, i.e. for situations where the logical architecture is relevant, is discussed in Chapter 6. The goal of this test case is to demonstrate how the new method contributes to the research objective, which was outlined in Chapter 1:

*Develop a knowledge-providing early stage ship design method that assesses the performance of a concept, identifies the driving factors for that performance, and provides design recommendations towards better solutions, in the context of vulnerability reduction of naval ships.*

Several steps are taken to show the contributions of the method. First, the test case set-up is discussed in Section 4.1. Subsequently, various hit types are assessed in Section 4.2 and design guidance for making trade-offs in residual capability is obtained Section 4.3. These sections also reflect the test case results against the research objective. Finally, Section 4.4 elaborates on the validity of the method compared to other methods.

## 4.1 Test case set-up

The test case assesses different levels of residual capability of a notional OPV. The test case uses an existing OPV model that has previously been used in other early stage vulnerability research (Duchateau et al., 2018; de Vos et al., 2018). Using the existing model limits the test case development time and keeps options for (future) integration of different vulnerability research efforts open. The physical architecture of the OPV is presented as a 3D model in Figure 4.1. Figure 4.2 provides the physical

Parts of this chapter are based on Habben Jansen et al. (2020a, 2019).

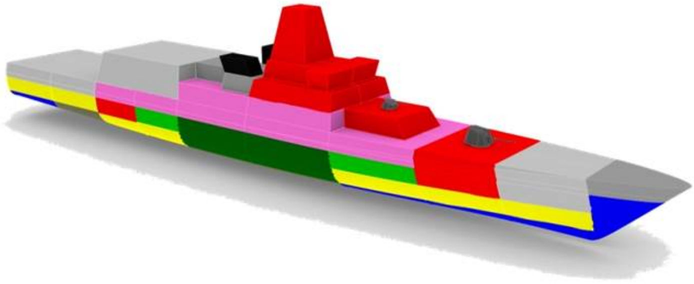


**Figure 4.1:** Physical architecture of the notional OPV used for the test case, visualised as a 3D model. Figure retrieved from Duchateau et al. (2018).

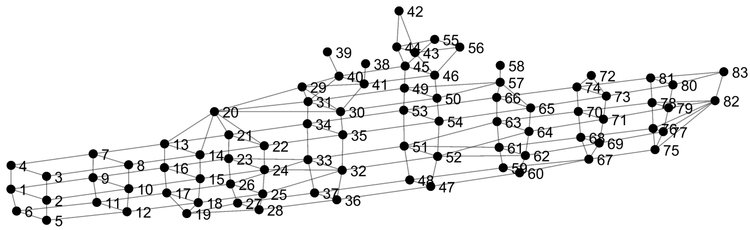


**Figure 4.2:** Physical architecture of the notional OPV used for the test case, visualised as a network. Each node represents the geometric centre a compartment. Each edge denotes a physical adjacency between compartments, i.e. the compartments are located on both sides of the same deck or bulkhead. Figure retrieved from Habben Jansen et al. (2020a).

architecture in terms of a network. This format is suitable as input for the computations.

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, one on port side (PS) and one on starboard (SB). The level of capability that is required after damage depends on the impact level of the damage. For low impacts, practically no loss of capability is accepted, while for high impacts the 'fight' capability does not have priority any longer, and the focus shifts towards 'move'. 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 4.1. To ease the discussion of the results, a short qualitative term is provided for each level of required residual capability.

**Table 4.1:** Residual capability for impact levels (Habben Jansen et al., 2020a).

| **Impact level** | **Required residual capability** | **Qualitative capability 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 |

A distributed systems network enables these capabilities by providing 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 (SWBs). In addition to that, chilled water units (CWs) provide chilled water to the weapons.

2. Integrated Power System (IPS) 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 logical architectures of these powering concepts are visually presented in Figure 4.3. Figure 4.4 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 3.5.4, the number of connections that can be considered with this method is 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 applied type of the damage scenarios differs from various existing methods: many hits with a small damage radius, contrary to few hits with a large damage radius (Figure 4.5). The computations of this test case go up to 8 hits. Due to the probabilistic way of modelling damage, this results in 8 separate hits in most cases. However, it also includes scenarios where the 8 hits are clustered in 8 adjacent compartments, or even where 8 hits all damage the same compartment. Though it is acknowledged that some of these scenarios may be more likely than others to occur, the goal of this method is to assess the vulnerability in a probabilistic way, taking into account asymmetric

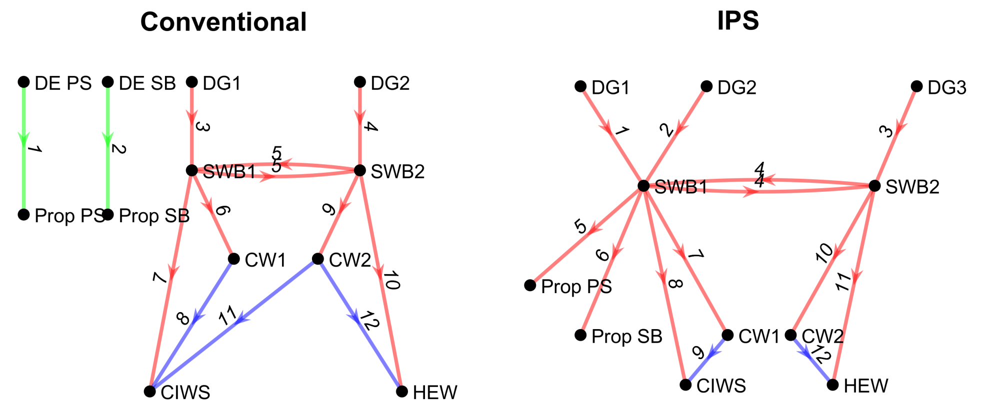



**Figure 4.3:** Logical architectures for the two powering concepts, with mechanical energy (green), electrical energy (red) and chilled water (blue). Figure retrieved from Habben Jansen et al. (2019).

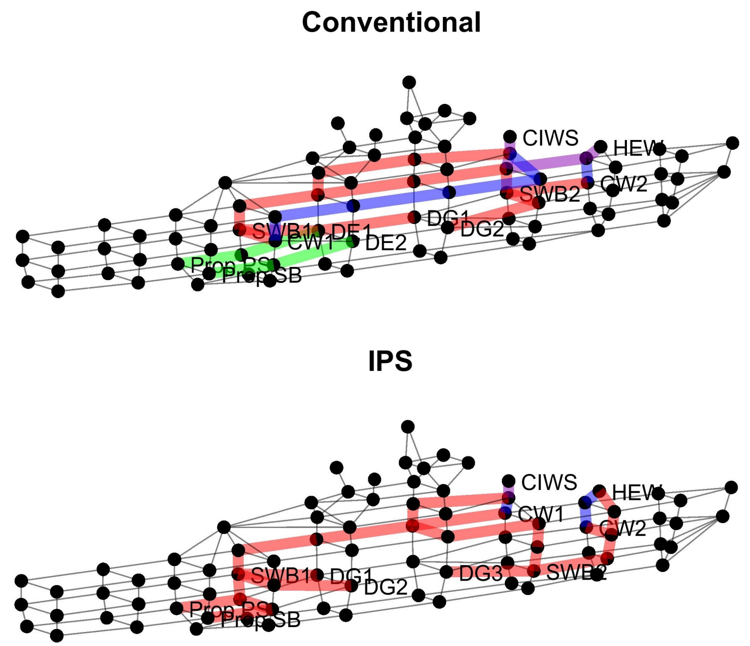



**Figure 4.4:** Physical solutions for the notional OPV. Purple lines represent routings of both chilled water and electricity through the same compartments. Figure retrieved from Habben Jansen et al. (2019).

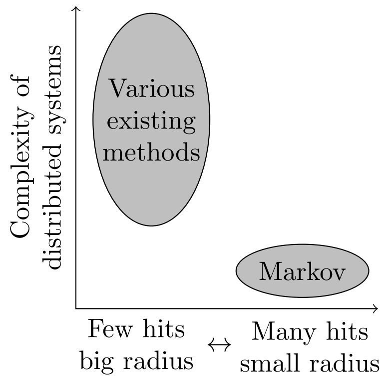



**Figure 4.5:** Relation between existing vulnerability methods and the new Markov method, in terms of the type of damage scenarios and the complexity of distributed systems. Figure adapted from Habben Jansen et al. (2020a).

threats. This gives an indication of the general vulnerability, rather than the specific vulnerability for certain damage scenarios. This is in contrast with other methods, that often focus on a smaller number of hits, but with more severe damage per hit.

## 4.2 Hit type assessment

With the test case set-up described in Section 4.1, the vulnerability method can be tested. Both the conventional concept and the IPS concept are tested in three ways:

1. Uniform hit distribution over all compartments, similar to the proof-of-concept (see Chapter 3).
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 3.16 and 3.17 is used. The projected lateral areas of the compartments, which are required for Option 2, are presented in Figure 4.6. 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 logical architectures that are considered in this test case use the engine rooms for several vital components and routings, which is expected 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 4.7. 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.

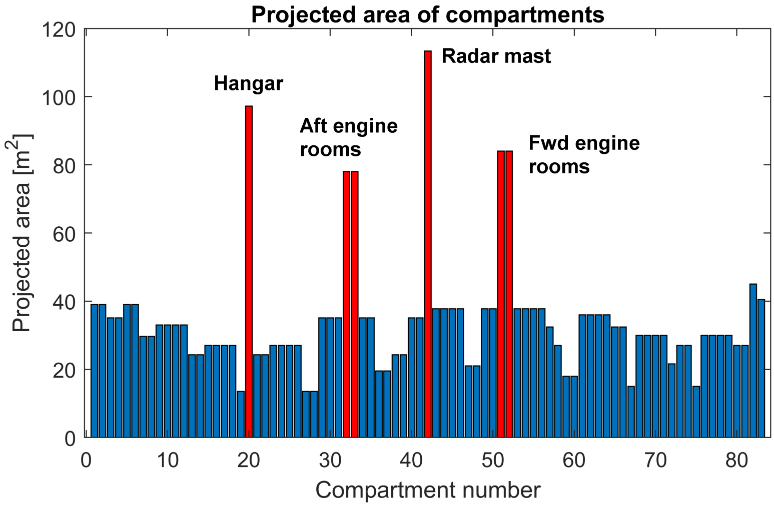



**Figure 4.6:** Projected lateral areas for all compartments. Figure retrieved from Habben Jansen et al. (2020a).

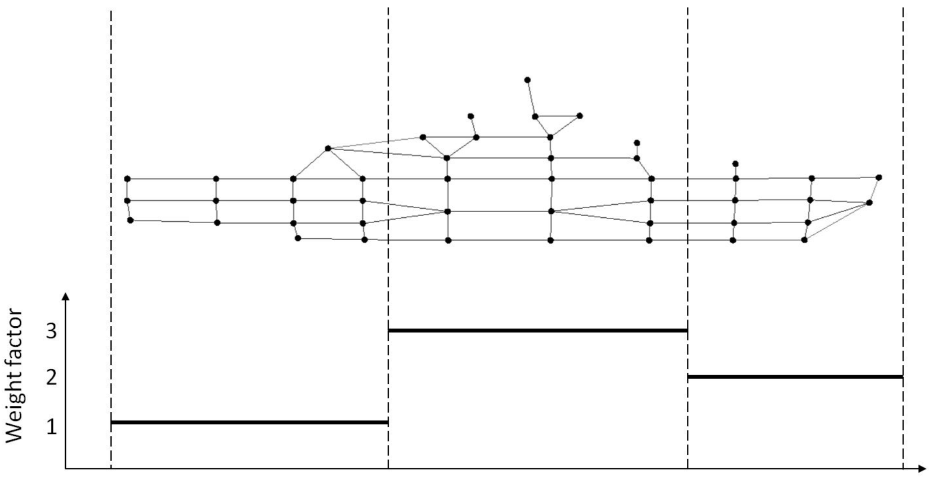



**Figure 4.7:** Weight factors for different longitudinal zones. Projected lateral areas for all compartments. Figure adapted from Habben Jansen et al. (2020a).

**Table 4.2:** Logical architecture connections required for different types of resources. Prop = propulsion, E = electricity, CW = chilled water, & = AND, | = OR

<table>
<tr><th></th><th>Required connections in conventional concept</th><th>Required connections in IPS concept</th></tr>
<tr><td>Prop PS</td><td>1</td><td>5 & (1 | 2 | (3 & 4))</td></tr>
<tr><td>Prop SB</td><td>2</td><td>6 & (1 | 2 | (3 & 4))</td></tr>
<tr><td>E CIWS</td><td>7 & (3 | (4 & 5))</td><td>8 & (1 | 2 | (3 & 4))</td></tr>
<tr><td>E HEW</td><td>10 & (4 | (3 & 5))</td><td>11 & (3 | (4 & (1 | 2)))</td></tr>
<tr><td>CW CIWS</td><td>(6 & 8 & (3 | (4 & 5))) |<br>(9 & 11 & (4 | (3 & 5)))</td><td>9 & 7 & (1 | 2 | (3 & 4))</td></tr>
<tr><td>CW HEW</td><td>9 & 12 & (4 | (3 & 5))</td><td>12 & 10 & (3 | (4 & (1 | 2)))</td></tr>
</table>

**Table 4.3:** Resources required for the various levels of residual capability

<table>
<tr><th>Residual capability</th><th>Required resources</th></tr>
<tr><td>Full</td><td>Prop PS & Prop SB & E CIWS & E HEW & CW CIWS & CW HEW</td></tr>
<tr><td>Considerable</td><td>Prop PS & Prop SB & E CIWS & CW CIWS</td></tr>
<tr><td>Moderate</td><td>(Prop PS | Prop SB) & E CIWS & CW CIWS</td></tr>
<tr><td>Minimal</td><td>Prop PS | Prop SB</td></tr>
</table>

### 4.2.1 Comparison of hit types

Using the physical solutions and the weight factors, the vulnerability assessment can be carried out, following the set-up explained in Chapter 3 and Section 3.5. As explained there, 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 levels of Table 4.1. In order to cluster the states, it is first determined which connections in the logical architecture are needed for a certain type of resource (propulsion, electricity, or chilled water). This overview is given in Table 4.2. Subsequently, it is determined which resources are required for the various levels of residual capability. These logical relations are given in 4.3.

Figure 4.8 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,

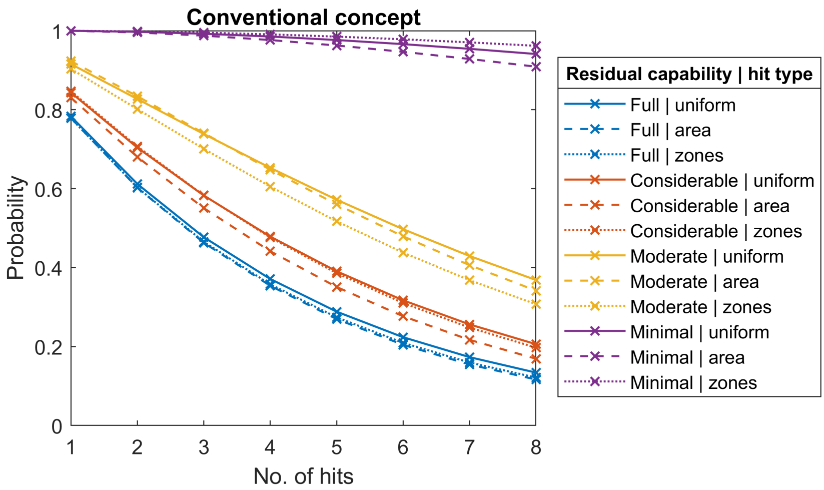



**Figure 4.8:** Probability of availability of main capabilities for the conventional concept. Figure adapted from Habben Jansen et al. (2020a).

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 4.9 shows a similar graph for the IPS 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 hit type yields more optimistic results than the uniform hit type. This holds for all residual capabilities. The zonal hit type leads to significantly 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 IPS 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

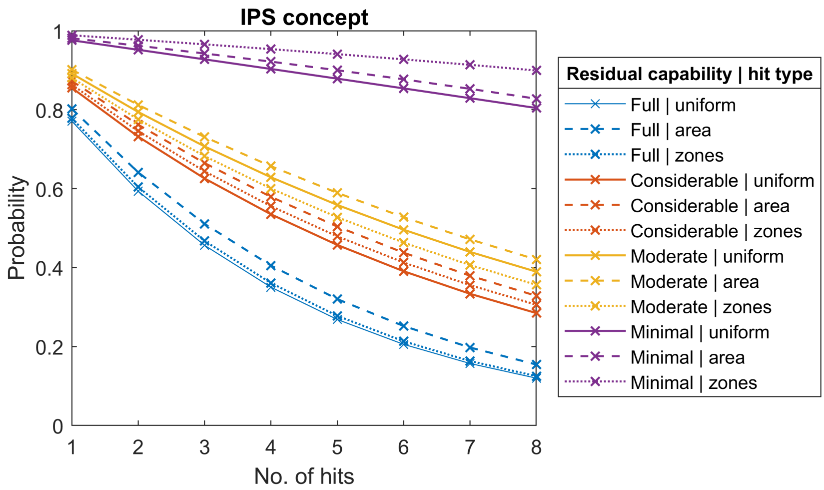



**Figure 4.9:** Probability of availability of main capabilities for the IPS concept. Figure adapted from Habben Jansen et al. (2020a).

hit type with the uniform hit type gives an indication of the vulnerability given a susceptibility context.

### 4.2.2 Comparison of concepts

In addition to comparing the results of different hit types for a given concept, such as in Figures 4.8 and 4.9, it also possible to compare the results of the two concepts for a given hit type. Figure 4.10 presents these results. The curves represent the absolute difference between the two concepts. A positive difference indicates that the IPS 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 IPS concept has a 10% higher probability of having that capability available. 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 IPS concept. However, the area and zonal hit types enlarge the hit probability for the diesel engines and generators. Since the IPS 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 of compartments that are needed, and thus the conventional concept is still preferred.

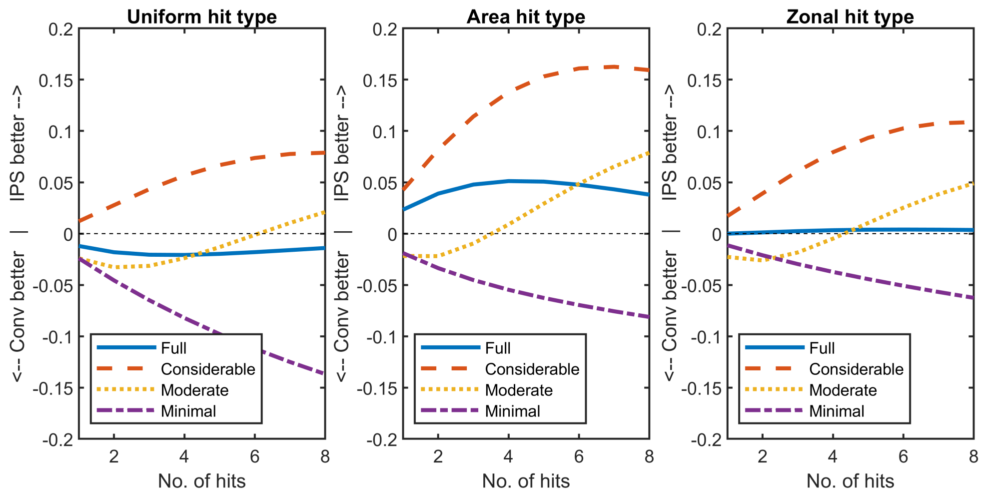



**Figure 4.10:** Difference in probability of availability of main capabilities for both concepts. Figure retrieved from Habben Jansen et al. (2020a).

- 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 IPS 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 IPS 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 IPS 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 IPS 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 IPS 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 IPS 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 IPS 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 or IPS 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 for vulnerability.

### 4.2.3 Conclusion

If the hit type assessment is reflected against the research objective, it can be seen that it partially fulfils the objective. It assesses the performance of a concept (in this case: the vulnerability), but is does not directly identify the underlying reasons for that performance. In terms of the main requirements for the method, it is able to quantify graceful degradation, but is does not yet provide a formalised, mathematics-based approach for identifying why the vulnerability is as it is. Hence, the focus on understanding rather than generating results needs further attention. In terms of the DIKW pyramid (see Chapter 1) it provides information, but not necessarily knowledge. As discussed in the previous two sections, the shape of the capability curves can be explained by manual interpretation. Furthermore, the shape of the curves confirms expectations that were already present upfront. A better, more formalised understanding of the curves can be obtained with the eigenvalue assessment as described in Section 3.6. This is considered in the next section. However, that does not negate the usefulness of this section's results. The fact that they align with upfront expectations endorses the the quality of the method.

## 4.3 Capability trade-off assessment

In order to make the transition from calculating the vulnerability to understanding the vulnerability, the eigenvalue assessment needs to be carried out. This can be done using any hit type, so it does not matter whether a uniform hit distribution or weight factors are used. However, for the sake of explaining the eigenvalue assessment, it is easier to use a uniform hit distribution. Hence, this distribution will be used for the eigenvalue assessment of this section.

As this section focusses on a uniform hit distribution, not all curves in the results of Figures 4.8 (conventional concept) and 4.9 (IPS concept) are addressed. More specifically, the only curves of interest are the solid curves of these figures. For clarification purposes, these curves have been included in a new visualisation, which is given in Figure 4.11. Both the conventional concept and the IPS concept are assessed in more detail in this section. First, matrix diagonalisation needs to be applied. This is only possible if the rank of $P$ equals its size, i.e. if the rank of $P$ is 4096. Using MATLAB, this is found to be the case for both the conventional concept

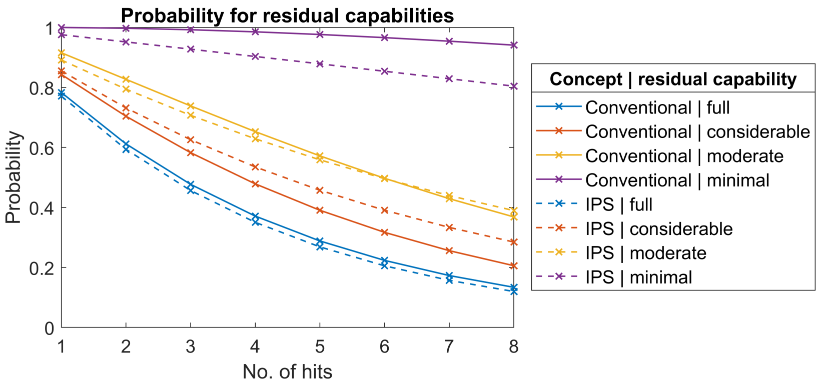



**Figure 4.11:** Probabilities for the four levels of residual capability for the conventional and IPS concept, for uniform hit probability. Figure retrieved from Habben Jansen et al. (2019).

and the IPS concept. Hence, the curves of the different levels of residual capability can be expressed as (see also Equation 3.27):

$$Pr(c_i) = \sum_{k=1}^{n} f_k \cdot \lambda_k^h \tag{4.1}$$

where $c_i$ denotes the $i^{th}$ capability level (in this test case $i$ runs from 1 to 4), $\lambda_k$ denotes the $k^{th}$ eigenvalue of the transition matrix (in this test case $k$ runs from 1 to 4096, which is $n$, the number of states), $h$ is the number of hits, and $f_k$ is an integer factor that states how strong the contribution of $\lambda_k$ is, and which sign it has. This factor results from the fact that individual states have been clustered to capabilities, using the method described in Section 3.5.3, and the logical relations of Tables 4.2 and 4.3. For the uniform hit distribution, all values of $f_k$ are integers, either positive or negative. If weight factors for the hit distribution are included, $f_k$ may take other values as well. This makes no difference for the procedure described in this section.

### 4.3.1 Conventional concept

The expression of Equation 4.1 can be set up for each individual vulnerability curve. Table 4.4 gives the eigenvalues and factors for the curve that represents the probability for full residual capability of the conventional concept, as presented in Figure 4.11 (the blue solid line). The corresponding state definitions are included as well, where the numbers 1-12 relate to the individual connections in the concept, as defined in Figure 4.3. Several observations can be made:

- Though there is a total of 4096 states, only 12 states have eigenvalues that contribute to the probability for full residual capability of the conventional concept.
- Some eigenvalues have a positive contribution, while others have a negative contribution. Many of these eigenvalues occur in pairs that cancel each other

out. For each pair, connection 11 is off in one of the corresponding states, while connections 7, 10, and 12 are on. This state is physically not possible, as connection 11 shares routings with these other connections through the same compartments. The meaning of the corresponding eigenvalues is strictly mathematical in this case. Nevertheless, they should not be ignored. If modifications to connection 11 are made in such way that it no longer routed together with other connections, the pair-wise cancellation may no longer be present.

- For every eigenvalue, the corresponding state includes the availability of at least connections 1, 2, 7, 9, 10, and 12. Relating this back to the distributed systems network of Figure 4.3, it turns out that these are all non-redundant connections.

- For some states, connections 6 and 8 are off. Their unavailability is related; individual availability of either connection 6 or connection 8 does not occur. For every state where connections 6 and 8 are off, there is a fellow state where connection 11 is off.

- For most states, either connection 3, 4, or 5 is off, but no combinations of these states.

**Table 4.4:** The eigenvalues, and their corresponding factors and state definitions, that contribute to the curve of full residual capability for the conventional concept. The numbers 1-12 in the state definitions relate to the individual connections in the concept, as defined in Figure 4.3. Table retrieved from Habben Jansen et al. (2019).

| $k$ | $\lambda_k$ | $f_k$ | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 0.6747 | 2 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 3 | 0.6747 | -2 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 |
| 81 | 0.7349 | -2 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 1 |
| 129 | 0.6867 | -1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 131 | 0.6867 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 1 |
| 209 | 0.7470 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 1 |
| 257 | 0.6988 | -1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 259 | 0.6988 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 |
| 337 | 0.7590 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 1 |
| 513 | 0.6867 | -1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 515 | 0.6867 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 |
| 593 | 0.7470 | 1 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 1 |

These observations are the result of assessing this specific concept, but are not restricted to this physical solution. In other words: for every physical solution the same eigenvalues are decisive for the vulnerability, provided that the logical architecture itself does not change. With this generalised description, the concept can now be better understood and improved. In order to do this, the results of the eigenvalue assessment need to be translated into actual design recommendations for the concept. The following procedure is proposed for this:

1. From all curves representing the various levels of residual capability, select one to study in more detail. For this test case, the curve of full residual capability for the conventional concept is investigated.

2. Check how many eigenvalues contribute to the shape of that curve. This may be decisive for how the further assessment is carried out. In this case, 12 eigenvalues contribute to the curve. The number of contributing eigenvalues is no metric for the vulnerability - it can therefore not be stated that either more or less eigenvalues is 'better'. However, a smaller number of eigenvalues allows the designer to do a manually-oriented assessment, while for a larger number of contributing eigenvalues the assessment may require a more computational approach. This test case illustrates a manual approach.

3. Check for repetitions or pairs in the contributing eigenvalues. For this test case, four pairs with connection 11 occur, leading to eigenvalues that cancel each other out. As such, only four eigenvalues contribute to the shape of the curve. They will be addressed in this test case.

4. Change the remaining connections in such way that the eigenvalues with positive factors increase and the eigenvalues with negative factors decrease. In order to increase an eigenvalue with a positive factor, the connections that are on in that state need to be reduced in size or concentrated. In order to decrease an eigenvalue with a negative factor, the connections that are off in that state need to be reduced in size or concentrated. From a mathematical point of view it could also be an option to increase the size of the routings of the other connections, but that would lead to increased vulnerability of those connections for the sake of a lower relative vulnerability of the other connections. As such, recommendations of size reduction and concentration of routings are preferred.

This can be applied to this test case. Consider the situation where there is a desire to increase the probability that there is full residual capability after one or more hits. The eigenvalues $\lambda_{81}$, $\lambda_{209}$, $\lambda_{337}$ and $\lambda_{593}$ have the strongest influence on this, as they are not cancelled out by other eigenvalues. More specifically, $\lambda_{81}$ needs to be decreased, and $\lambda_{209}$, $\lambda_{337}$ and $\lambda_{593}$ need to be increased. For all these eigenvalues, connections 6 and 8 are off. In order to decrease $\lambda_{81}$, the routings of these connections should be made smaller or more concentrated. However, in order to increase $\lambda_{209}$, $\lambda_{337}$ and $\lambda_{593}$, it is the other way around. This is a mathematical representation of conflicting requirements that result from interdependencies between the connections. However, a closer look at $\lambda_{209}$, $\lambda_{337}$ and $\lambda_{593}$ shows that either connection 3, 4 or 5 is off in their associated states. In order to increase these eigenvalues, the probability to remain in any of these states should be increased. This indicates that all routings related to connections other than 3, 4, 5, 6 or 8 need to be made smaller, or more concentrated. Connections 1 and 2 are related to propulsion, and are not easy to modify for the conventional concept. However, for connections 7, 9, 10, 11 and 12, two modifications are proposed:

1. Bring CW2 above SWB2, closer to the CIWS. This concentrates the routings of connections 9, 10 and 12, and reduces the routing length of connection 11.

2. Concentrate the routing from SWB1 to the CIWS (connection 7) with the routing between SWB1 and SWB2 (connection 5). This reduces the number of compartments solely occupied by the routing of connection 7.

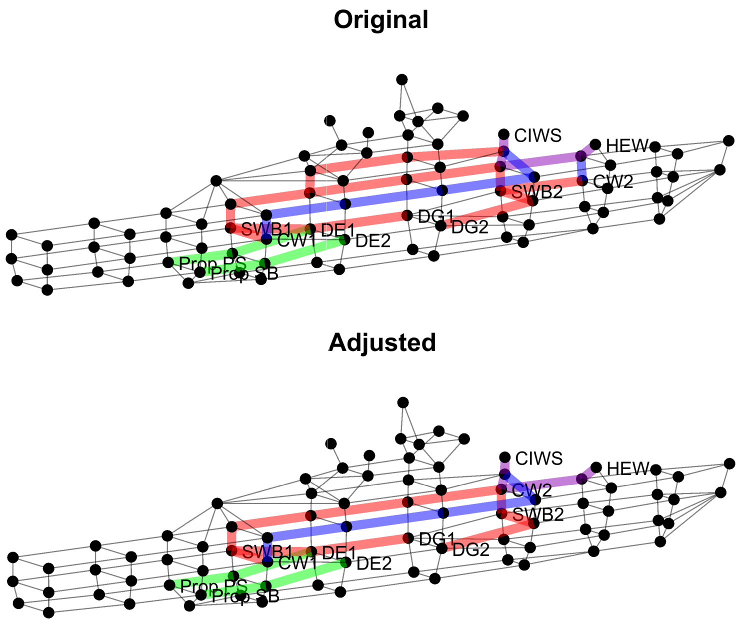



**Figure 4.12:** Physical solution of the adjusted conventional concept. The original concept is given for reference. Figure adapted from Habben Jansen et al. (2019).

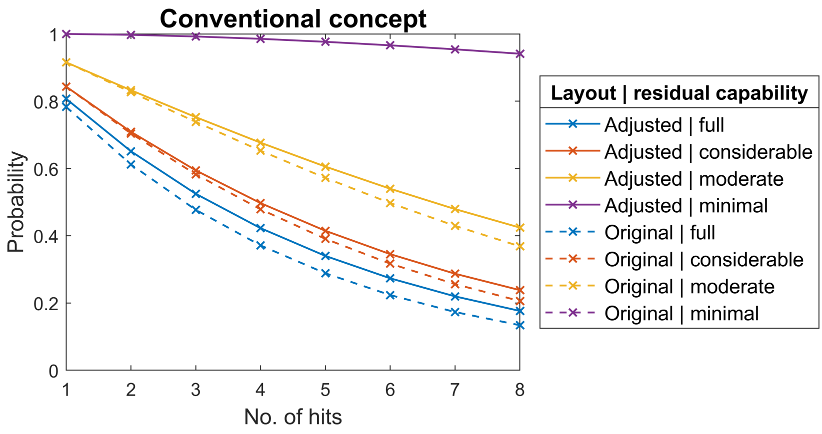



**Figure 4.13:** Probabilities for the four levels of residual capability for the adjusted conventional concept. Figure retrieved from Habben Jansen et al. (2019).

The concept is adjusted accordingly, such as presented in Figure 4.12. The results of this adjustment are given in Figure 4.13. It can be observed that the adjustments have the desired effect, as the curve for full residual capability lies higher, indicating a higher probability for having this level of residual capability after one or more hits. At the same time the curves for moderate and considerable residual capability have increased as well. Hence, the positive effect of the modification goes beyond the level of residual capability that was originally considered. In this case this effect is positive. However, for other cases the residual capability of other levels may drop if the residual capability of the level that was originally considered is increased. This method elucidates and quantifies these interdependencies.

### 4.3.2 IPS concept

The same procedure can be applied to the IPS concept. Figure 4.11 shows that the probability for minimal residual capability, i.e. at least propulsion at one side, is significantly lower for the IPS concept (purple dashed curve) than for the conventional concept. Consider the situation where there is a desire to increase this probability. The eigenvalues and factors that determine the shape of this curve are presented in Table 4.5. For this case all factors are either 1 or -1, so in order to determine the eigenvalues with the largest influence, the magnitude of the eigenvalues need to be considered. The largest eigenvalues, i.e. the eigenvalues with the largest influence on the curve, are $\lambda_{1920}$, $\lambda_{1984}$ and $\lambda_{2944}$. The corresponding factor is 1 for all these eigenvalues, so they make a positive contribution to the curve. Hence, the probability for minimal residual capability increases when the magnitude of these eigenvalues increase.

The state definitions associated with these eigenvalues show that connections 1, 2, 5, and 6 are on, while the other connections are off. In order to increase the probability for minimal residual capability, the number of compartments associated with these connections needs to be reduced, and concentration and/or separation of the associated system components and routings may be beneficial. To that end, SWB1 is relocated one compartment lower compared to the original IPS concept that was presented in Figure 4.4. As a result, the distance between SWB1 and both propellers reduces. In addition of that, only one compartment is a single point of failure, instead of two compartments for the previous situation. Since SWB1 has been relocated, the routings from DG1 and DG2 need to be adjusted as well. As a result, the routing from DG2 to SWB1 now has a partial overlap with the routing between SWB1 and the starboard propeller. However, this does not affect the power supply to the port side propeller, so the requirement to have a large probability for propulsion at one side at least is still met. Propulsion power can also be supplied via DG3 and SWB2, i.e. connections 3 and 4. However, the results of the eigenvalue assessment shows that these connections have a smaller influence on the shape of the curve. These connections are therefore left unchanged.

The adjusted layout is presented in Figure 4.14. The associated result is given in Figure 4.15. It can be seen that the probability for having at least minimal residual capability has increased significantly. Hence, the proposed solution has the desired effect. For the other levels of residual capability, the curves remain unchanged, so no trade-off needs to be made. This is because the capability that is considered, i.e. propulsion at one side at least, does not include components or routings of other systems.

**Table 4.5:** Eigenvalues, factors, and state definitions that contribute to the curve of minimal residual capability for the IPS concept (Habben Jansen et al., 2019).

| $k$ | $\lambda_k$ | $f_k$ | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 64 | 0.8072 | -1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 128 | 0.8313 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 192 | 0.8193 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 832 | 0.9036 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 896 | 0.9277 | -1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 960 | 0.9157 | -1 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1088 | 0.8313 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1152 | 0.8554 | -1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1216 | 0.8434 | -1 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1856 | 0.9277 | -1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1920 | 0.9518 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1984 | 0.9398 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2112 | 0.8193 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2176 | 0.8434 | -1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2240 | 0.8313 | -1 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2880 | 0.9157 | -1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2944 | 0.9398 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3008 | 0.9277 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3136 | 0.8434 | -1 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3200 | 0.8675 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3264 | 0.8554 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |

### 4.3.3 Conclusion

The results from the capability trade-off assessment align with the research objective. Whereas the hit type assessment assessed the vulnerability of a concept, the eigenvalue assessment also provides the underlying driving factors. A major benefit of the method is that its results are not only applicable to the concept that is modelled, but to any concept with the same logical architecture. Hence, direction towards other, potentially better concepts can be obtained. In terms of the DIKW pyramid, the eigenvalue assessment adds knowledge to the problem. More specifically, the vulnerability curves themselves can be categorised as information, but the mathematical equation that links the curves (performance) to actual parts of the ship (Equation 4.1) builds upon that information and provides knowledge. This also aligns with the main requirement that a formalised, mathematics-based approach for identifying driving factors and design recommendations is needed.

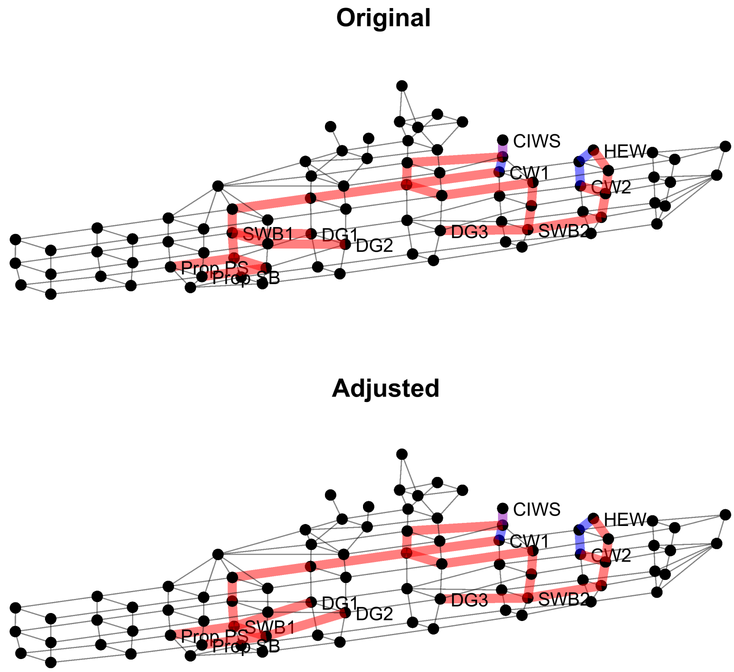



**Figure 4.14:** Physical solution of the adjusted IPS concept. The original concept is given for reference. Figure adapted from Habben Jansen et al. (2019).

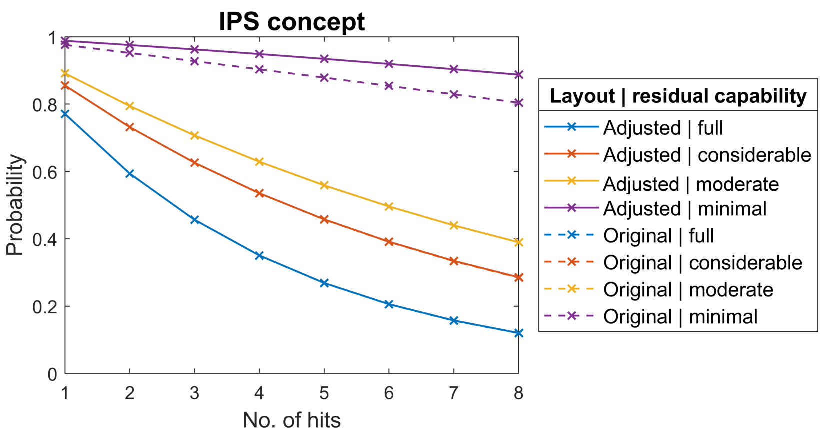



**Figure 4.15:** Probabilities for the four levels of residual capability for the adjusted IPS concept. The curves for considerable, moderate, and minimal residual capability are similar for the adjusted and the original concept. Figure retrieved from Habben Jansen et al. (2019).

It should be noted that the eigenvalue assessments described in this section have led to *a better* physical solution for both the conventional concept and the IPS concept. However, this says nothing about whether it is *the best* solution. If desired, such an analysis can be done by coupling the eigenvalue assessment to an optimisation algorithm. However, the level of detail and the purpose of this assessment need to be considered before doing this. As explained, this method aims to elucidate driving factors for vulnerability for the purpose of getting insight, not for the purpose of further development of the concept. This means that there is no strict need to obtain the best solution at this stage.

## 4.4 Verification and validation

The test case in this chapter has demonstrated that the new method is able to provide an estimation of underlying driving factors for the vulnerability of a naval ship, in a formalised, quantitative fashion. As such, it can be stated that the method complies with its requirements. In other words: it has been verified. This means that the method fulfils its purpose in the right way, but not necessarily that the method fulfils the right purpose. As such, another step - validation - needs to take place.

Validation is typically mostly based on logical induction and/or deduction. This fits well for validating mathematics-based models, which are often used in engineering. However, the method of this dissertation is a design method for an engineering context. Though it is mathematics-based, it includes a large share of subjective statements. Examples include questions like: “Which levels of residual capability to include?” or “When are the vulnerability characteristics good/sufficient?”. Due to these subjective issues, traditional validation can become problematic. This is discussed in considerable detail by Pedersen et al. (2000). In response to this issue, they propose a method for validating design methods that involve subjectivity: the validation square. This square is provided in Table 4.6. The method of this dissertation and the test case are validated based on this square, using its validation steps.

The first quadrant of the validation square is theoretical structural validity. This concerns whether the set-up of the method is correct. The first step of this method is:

**Table 4.6:** The validation square of Pedersen et al. (2000), intended for validation of design methods that involve subjectivity

| | |
|---|---|
| Theoretical structural validity (step 1 and 2) | Theoretical performance validity (step 6) |
| Empirical structural validity (step 3) | Empirical performance validity (step 4 and 5) |

1. Accepting the construct's validity.

In this step, a 'construct' is a building block of the method. A method may incorporate multiple constructs. The proposed activity for the first step is literature review. In the case of the method of this dissertation, the main constructs are a Markov chain and network metrics. The suitability of a Markov chain has been discussed in Section 2.5, where a justification for using a Markov chain is given. Section 2.3.2 explains that networks are a commonly and accepted used representation for distributed systems. As such, it can be stated that Step 1 is fulfilled. The next step is:

2. Accepting the method consistency.

This step aims to build confidence in the way in which the constructs of the method are put together. Flowcharts that describe information flow are proposed for this. However, in the case of the method of this dissertation, a more mathematical approach can be used. A main claim about using Markov theory in combination with a network description of distributed systems is that this approach assesses vulnerability in an integrated way, and that decomposing the network into individual pieces yields an incorrect result. This claim has been justified with the comparison between the integrated and decomposed approach, of which the results are provided in Figure 3.4. Further confidence can be gained by repeating this comparison for the OPV considered in this chapter. Using the same computations as described in Section 3.3, the results of Figures 4.16 and 4.17 are obtained. These figures show that the decomposed approach deviates distinctly from the integrated Markov approach, especially for the IPS concept. The decomposed approach estimates lower probabilities for the residual capabilities, i.e. higher vulnerability. Though it can be argued that this is on the conservative - thus safe - side, a mathematically correct approach is preferred over a safe approach. Hence, Step 2 of the validation square has also been fulfilled. This means that the theoretical structural validity of the method has been confirmed.

Subsequently, the empirical structural validity needs to be assessed. This is the second quadrant of the validation square. This quadrant aims to assess the appropriateness of the example problem(s) that are used to verify the the usefulness of the method. The according step is:

3. Accepting the example problems.

The proposed activity consists of documenting answers and associated data for the following two questions:

1. Is the example problem similar to the problems for which the method is intended?

2. Is the example problem similar to the actual problems that need to be solved?

As for the first question: the method of this dissertation is meant for assessing complex damage scenarios for logical architectures with a small number of edges (up to 13). The example problem of the OPV has deliberately been kept below that number. The second question is a more serious issue. It has been stated in Section 4.1 that

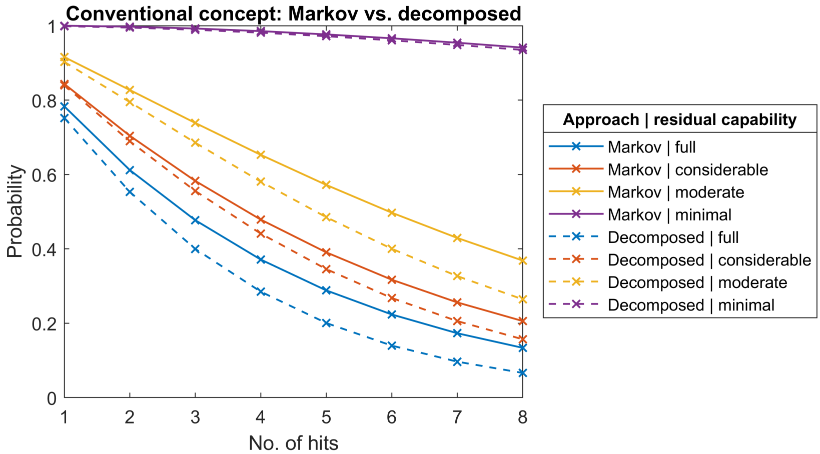



**Figure 4.16:** Vulnerability of the conventional concept if individual connections are decomposed and assessed individually

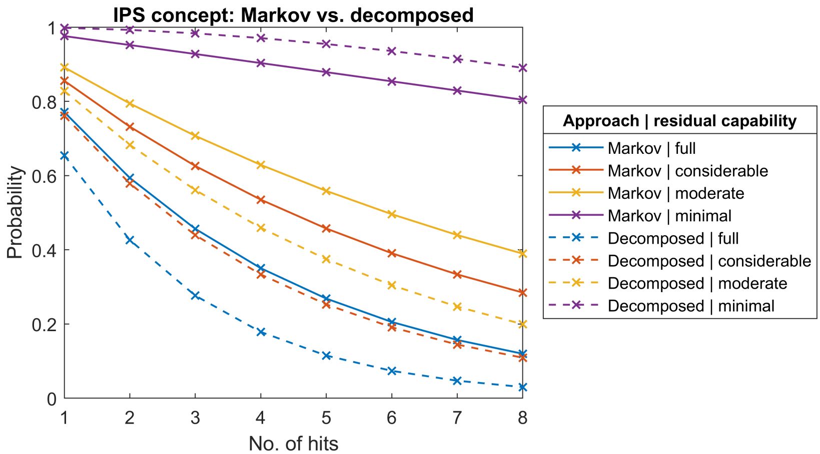



**Figure 4.17:** Vulnerability of the IPS concept if individual connections are decomposed and assessed individually

a typical early stage logical architecture consists of about 10-100 nodes. Hence, the method of this dissertation only supports the utmost lower end of that spectrum. In addition to that, the 10-100 nodes logical architecture is already a simplification made for the purpose of early stage design. Logical architectures of actual ships have numbers of nodes in several higher orders of magnitudes. A full validation would therefore also comprise a comparison with an early stage and a final vulnerability assessment of a fully defined ship. This is not considered in this dissertation, since such a model was not available. It must therefore be concluded that Step 3 can not be entirely fulfilled. Nevertheless, the other quadrants of the validation square can be applied, while keeping this limitation in mind.

The third quadrant of the validation square is the empirical performance validity. In this square, the performance of the design solutions and the method are assessed with respect to the example problem. First, Step 4 is needed for this:

4. Accepting the usefulness of the method for some example problems.

The proposed activity for this is to use representative example problems. The degree to which the purpose of the method has been achieved for the example problem is a metric for method usefulness. Note that this step is similar to the verification step that has been addressed at the beginning of this section. Since the method fulfils its previously defined requirements, it can be stated that it is useful within the scope of the example problem. This leads to Step 5:

5. Accepting that usefulness is linked to applying the method.

For this step it is proposed to compare the results of the method with existing methods. As explained in Section 2.3.2, several vulnerability reduction methods exist. However, none of these does the same as the method of this dissertation - which is the very reason the new method has been developed. Comparing the new method with existing method is therefore not straightforward. However, the DMO design rules provide an opportunity for a comparison with the new method. Recall that for the conventional OPV, the power cable to the CIWS and the crossover between the switchboards have been concentrated. This aligns with Rule 5: Route vital distribution systems on the same paths. Furthermore, the forward chilled water plant was relocated onto the path of the power cable of the high-energy weapon. This also aligns with Rule 5. For the IPS concept, the length of the power cables needed for propulsion was reduced by letting it run through a smaller number of compartments. Furthermore, a reduction in overlap between the starboard and port side routing was obtained by this measure. This aligns with Rule 4: Separate redundant paths. This separation has also reduced the number of single points of failures, though these were not entirely removed. This aligns with Rule 2: Avoid single points of failure in vital distribution systems.

From this assessment it can be concluded that the new method aligns with previously existing design rules. Not all rules have been covered by the new method. Since the method does not make changes to the logical architecture, it will for example not generate additional crossovers, which is an advice provided by Rules 9 and 10. The other way around, however, the new method provides knowledge that is not covered for in the rules. For example, the interdependency between the different levels of residual capability can be quantified. Hence, the conclusion of this step is that the new method aligns with existing design knowledge, while it is distinctly different from existing methods. This is regarded as a satisfactory conclusion for Step 5.

The last quadrant of the validation square is the theoretical performance validity, which is about the performance of the designs solutions and method beyond the example problems. The step associated with this quadrant is:

6. Accepting usefulness of the method beyond example problems.

Contrary to the first five steps, there is no proposed activity for this step. Instead, it is argued that a successful implementation of Steps 1-5 ensures generality - thus an ‘assurance’ that the method is useful beyond its example problems. It is also noted, however, that validation eventually rests on (subjective) belief and faith. Hence, Steps 1-5 provide confidence for full validation, but do not guarantee it.

Summarising the results of Steps 1-5 of the new method, it can be stated that Step 3 has not yet led to a satisfactory result. As such, it must be concluded that validation of the new method has not yet been fully established. Yet, all other steps have been covered. This suggests that it is difficult to state that the method is either validated or not validated - it is a more gradual interpretation. The conclusion for the new method is therefore that it has been validated to the reasonably largest extent possible. Recommendations that result from this statement will be provided in Chapter 7.

# Chapter 5

# Integration of the method into early stage design

The method introduced in this dissertation has been developed for a specific vulnerability context in early stage ship design. Yet, vulnerability and ship design as a whole encompass a broader scope of problems and methods to solve these problems. As such, this chapter discusses the integration of the new method in early stage ship design. First, Section 5.1 elaborates on the advantages and challenges for managing design knowledge in general. Subsequently, Section 5.2 discusses how the new method can be combined with other early stage vulnerability methods, and how this affects the work flow during the design process. Over the course of these two sections, it turns out that the field of managing (design) knowledge is highly subjective and unspecific. To that end, Section 5.3 provides several considerations to keep in mind for research in this field.

## 5.1 Management of design knowledge

The method described in this dissertation has been developed as a specific solution to a specific problem with respect to assessing vulnerability in early stage ship design. This specific vulnerability problem, in turn, results from a generalised early stage design problem: the interdependency between concepts and solutions (see Chapter 1). It could be stated that the specific solution contributes to the generalised problem *through* the specific problem. Though this reasoning is correct in itself, it does not exploit the full potential of the specific solution. More specifically, a translation of how the specific solution can be translated into a generalised solution could potentially make the new knowledge applicable in a broader scope, enabling re-use of that knowledge. This is schematically presented in Figure 5.1. Simply stated: the top right box of the figure still has to be filled.

The translation from the specific solution to the generalised solution is not necessarily as straightforward as taking the new Markov method (i.e. the specific solution) and

Parts of this chapter are based on Habben Jansen et al. (2020b).

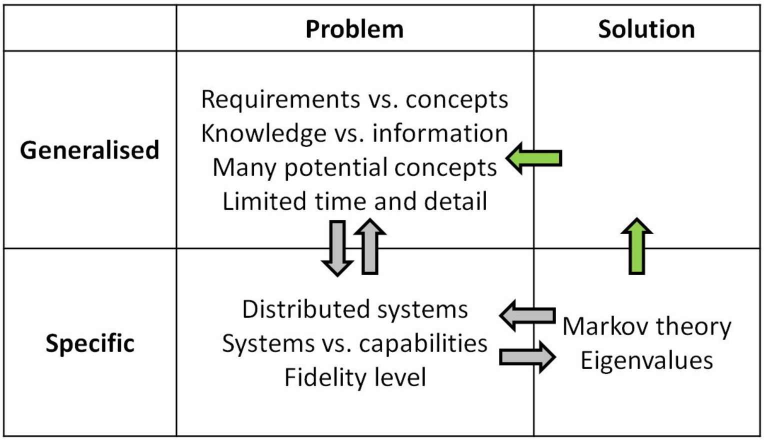



**Figure 5.1:** Envisioned translation from the specific solution to the generalised solution, presented with green arrows. The grey arrows denote the 'shortcut', which in itself is not wrong, but does not fully exploit the potential of the method.

applying it to more problems (i.e. the generalised solution). The Markov method has been developed as a solution for a specific vulnerability problem, which has been defined first. In itself there is nothing wrong with turning this order around, i.e. finding new problems for which the Markov method can be applied as a solution, as long as it does not 'solve' a problem for which another solution is already available. This is considered in Chapter 6, but in this chapter, the translation from the specific solution to the generalised solution is envisioned as an effort where different methods and tools are integrated, that together provide knowledge that is 'better' than the knowledge supplied by the methods individually. A major point of attention is that this is highly subjective and hard to measure: when is combined knowledge from methods 'better' than knowledge from separate, individual methods?

This topic relates to the field of knowledge management, and is not limited to the ship design application. This section aims to outline the benefits and challenges of knowledge management in the context of this dissertation's topic. Nevertheless, several general considerations for knowledge management are now discussed first.

The first question that arises in this discussion, is: "What is knowledge?". Section 1.1 has already introduced this topic by means of the DIKW pyramid. As stated in that section, knowledge is associated with a higher degree of understanding, but it is less specific and rather difficult to capture or program. In addition to that, there is a difference between explicit knowledge and tacit knowledge. In terms of this dissertation, the vulnerability method with its eigenvalue assessment provides explicit knowledge: it states why the vulnerability is as it is, what the driving factors are, and what can be done to make it better. Tacit ship design knowledge, however, is ship designer's knowledge through experience, rather than ship design knowledge through equations. This is also discussed by Andrews (2007), who argues that there is an aspect of art in ship design. He makes a distinction between art as by an artisan, and art as by an artist, and concludes that the former remains present in ship design, even in the light of computer aided design. Hence, both explicit and tacit knowledge are present in ship design.

To capture knowledge in organisations, knowledge management systems were introduced around the 1990's. Alavi and Leidner (1999) have defined knowledge management systems as:

*"information systems designed specifically to facilitate the codification, collection, integration and dissemination of organisational knowledge".*

Such systems are typically computer or ICT systems. Alavi and Leidner (1999) have also investigated the perceived benefits and challenges for the - back then - early application of knowledge management systems. The perceived benefits include, but are not limited to saving time, enhancing communication, better serving the client, and better accountability. The perceived challenges include the ability to convince people to volunteer their knowledge, the responsibility for managing the knowledge, confidentiality and security. Another topic of concern was how to implement knowledge management systems effectively.

The effective implementation is discussed in more detail by Walsham (2001). He argues that leveraging knowledge through ICT systems is hard to achieve, due to the very nature of knowledge. Using the distinction between explicit and tacit knowledge, it can be stated that knowledge captured in knowledge management systems is explicit knowledge. He argues that this is only useful if it connects well to the tacit knowledge of the users of such systems, and states that this can not be replaced by personal communication and relationships. This leads him to concluding that ICT-based knowledge management systems can be beneficial to human activities as long as their benefits and limitations are carefully kept in mind.

An example of a knowledge management effort related to ship design is the work of DeNucci (2012), who has developed a tool to capture design rationale. It is not an ICT system in itself, but a procedure to extract and re-use ship designer's knowledge on general arrangements and layouts. This was done by presenting a set of concept designs, including unorthodox concepts, to a group of ship designers. The designers were asked to identify what was *not* good on the layout of these concepts, and why. By means of avoiding these aspects, or doing the *opposite* of what is not good, a set of 'best practices' for ship design, i.e. design rationale, is captured. Examples of rationale captured with this procedure include:

*"If the fan rooms are too far forward, the suction of green water in rough seas is possible."*

and

*"Boat launch and recovery is easier and safer when the boat and davit are near waterline."*

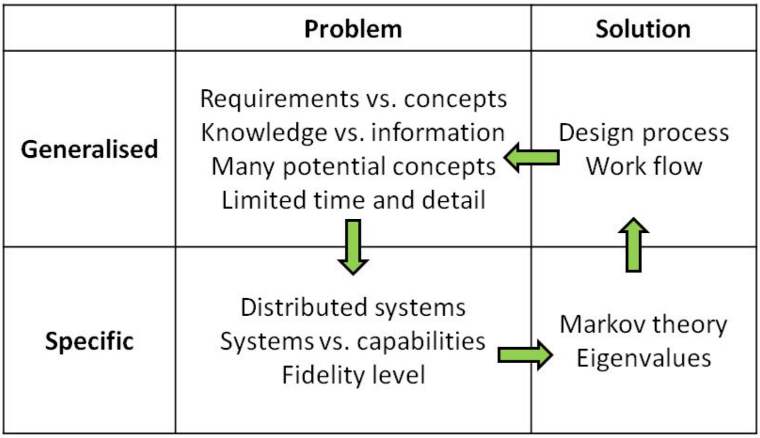



**Figure 5.2:** A design process and associated work flow as generalised solution for the generalised problem

A key finding of this research is that the majority of the captured rationale is re-usable, i.e. independent of the ship type or specific project. Hence, future design and/or acquisition projects could use this rationale, which saves time and prevents loss of knowledge if the designers who came up with this rationale are no longer available. In terms of the definitions of knowledge, this type of rationale capturing is an example of explicit knowledge: it is clearly formulated and documented, and can easily be transferred to other (potential) users.

With this reflection on knowledge management, several directions for integrating the new method in early stage ship design can be formulated, i.e. the translation from the specific solution to the generalised solution can be made. The knowledge obtained from the new method is explicit knowledge. Simply stated, that is nothing more than factual statements. In that sense, they are comparable to the rationale of DeNucci (2012): statements of knowledge that are generalised and re-usable, but not necessarily actionable. In order to actually apply the knowledge, it needs to be transferred into actionable tasks for a design effort. At the same time, the deep, tacit knowledge that is the foundation for the explicit knowledge - regardless whether it is from the method of this dissertation or another ship design or vulnerability method - is unlikely to be captured in language or an ICT system. Hence, the transition from the specific solution to the generalised solution can best be achieved by formulating an adequate design process, that includes the method of this dissertation, as well as other methods. This confirms what was outlined at the beginning of this section. Hence, the solution to the generalised design problem, is a generalised design process. This does not only include an overview of which methods provide which results, but also a work flow that can be acted upon during a design effort. This fills the final quadrant of the problem and solution addressed in this dissertation, and is schematically presented in Figure 5.2. Section 5.2 outlines what the design process and work flow are.

## 5.2 Relation of method to other early stage vulnerability methods

The proposed new method, of which the details have been discussed in Chapters 3 and 4, has been developed in response to a gap that has specifically been identified for this method. The same holds for other methods, especially the ones that have been developed in a scientific research context. As such, multiple early stage design methods exist that have all been developed as stand-alone methods. Yet, they all cover a part of the same topic, in this case early stage design of distributed systems, with a focus on vulnerability. Hence, proper integration of the methods into early stage design as a whole is essential.

The need for integrating design methods in early stage design of distributed systems is not new, and has previously been discussed by e.g. de Vos (2018). He subdivides early stage design of distributed systems in a set of steps that together form a work flow. This work flow is taken as a starting point, and is worked out below in more detail to consider multiple design methods. More specifically, the work of de Vos (2018), Duchateau et al. (2018) and the Markov method described in this dissertation are combined into an early stage design framework, and an updated work flow. The selection of these three methods results from the practical fact that all these methods have been developed by researchers from the same university. However, the application of the framework is not limited to these three methods.

### 5.2.1 Method integration framework

A key feature of integrating multiple design methods is using the right method at the right time. Chapter 1 has already made a distinction between concept exploration and concept definition in early stage design, that both have specific focus areas and levels of detail. Also, Section 2.3.1 has identified three types of architecture for distributed systems: the physical, logical, and operational architecture. Hence, two 'dimensions' in design of distributed have been identified: it matters where in the design process you are, and what perspective on distributed systems you consider. These dimensions are included in the framework, which is presented in Table 5.1. This table shows that the physical, logical and operational architectures have been condensed into two perspectives: the system perspective and the ship perspective. The systems perspective has a stronger focus on fundamentals of marine engineering, such as assessments of capacities, flows, and (thermo)dynamics, using the logical architecture. The ship perspective has a stronger focus on geometric aspects, such as weights, volumes, and locations, using the physical solution. However, these are not strictly separate things. A logical architecture may for example also include information on zoning or the location of components. This occurs for instance when 'switchboard aft' and 'switchboard forward' are included as two nodes in the logical architecture. Hence, the framework uses the terms 'system' and 'ship' as perspectives.

The selected methods have been allocated to specific parts of the framework. All methods exist of a way in which vulnerability can be assessed. Max-flow-between-

**Table 5.1:** Framework for integrating early stage distributed systems design methods, with a focus on vulnerability. Table retrieved from Habben Jansen et al. (2020b).

<table>
<tr><td colspan="2"></td><td colspan="3">Design stage</td></tr>
<tr><td colspan="2"></td><td>Concept exploration</td><td>Concept definition</td><td>Detailed design & Engineering</td></tr>
<tr><td rowspan="2">Perspective</td><td>System</td><td>Max-flow-between-hubs</td><td>Hurt state percolation / logical architecture</td><td>GES, S3D</td></tr>
<tr><td>Ship</td><td>Markov</td><td>Hurt state percolation / physical solution</td><td>RESIST, SURVIVE, SURMA</td></tr>
<tr><td colspan="2"></td><td colspan="2">Methods considered for integration in this dissertation</td><td>Examples of other methods and tools</td></tr>
</table>

hubs is used by de Vos (2018). The max-flow-between-hubs approach aims to improve reconfigurability of system designs. This approach requires only a logical architecture. No routing or location information is required. Logical architectures are thus analogous to e.g. system block diagrams or single line diagrams that are used in practice. The idea behind focusing on logical architectures first, before addressing the actual location of components and connections in the ship, is to filter the design space from the perspective of operational performance of the systems; i.e. an energy flow perspective. It makes little sense to place and route systems that are deemed infeasible or inoperable as such a system will never be realised. Theoretically, the actual lay-out of connections (length, diameter, number of bends, etc.) has an effect on operational performance of the systems, but in ship systems this effect is typically very small and can be neglected. This is the reason the idea of focusing on logical architectures first holds and why max-flow-between-hubs is particularly useful for concept exploration.

The mathematical definition and explanation of max-flow-between-hubs is given by de Vos and Stapersma (2018). Note that this vulnerability metric is fundamentally different from probabilistic methods to assess vulnerability. The metric is designed to focus on a specific aspect of vulnerability which is considered the most elusive aspect from the viewpoint of a logical architecture. As such, max-flow-between-hubs is more like a designers rule-of-thumb; it does not require the ‘simulation’ of the ship or system being hit and therefore does not require as much computational capacity than the other vulnerability assessment methods discussed in this section. Three robustness measures that are used in practice to decrease the vulnerability of systems from an operationally oriented perspective have been identified by de Vos (2018):

1. Increasing redundancy by duplicating functionally similar components, either as full back-up or with performance degradation, or by different type of components (similar function, different working principle) such as accumulators.

2. Introducing separate ‘islands’ in the logical architecture (i.e. zoning). The islands are able to operate as stand-alone systems in critical operations (islands

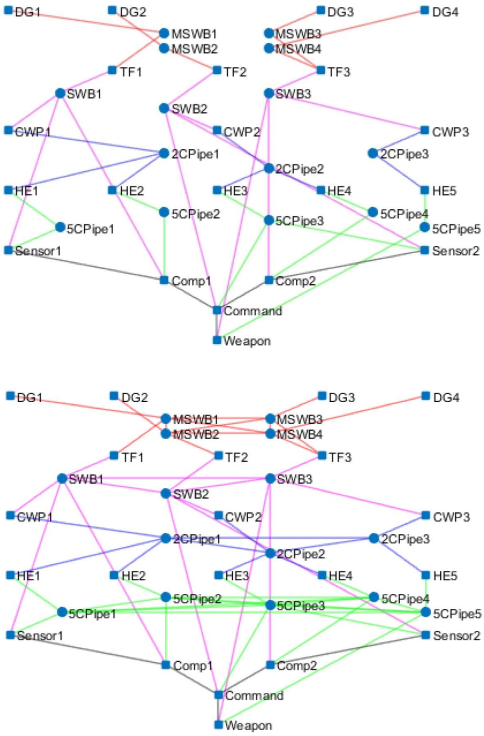



**Figure 5.3:** Two possible solutions for the logical architecture. The bottom solution is preferred by max-flow-between-hubs. Figure retrieved from de Vos and Stapersma (2018).

should then also be physically separated; i.e. located in different zones in the ship separated by blast-resistant and watertight bulkheads).

3. Increasing reconfigurability of the distribution systems by increasing the number of paths between suppliers and users. This is achieved by additional supply lines to vital users and by interconnecting the afore-mentioned islands by cross-overs.

Max-flow-between-hubs focusses on the last measure: reconfigurability of distributed systems as arguably the most important and elusive aspect of system vulnerability. It is assumed that reconfigurability of distributed systems is improved by increasing the interconnectivity between the (most) central distribution points of the systems; i.e. the hubs. By improving the maximum flow between hubs specific connection patterns, like ring distributions, are preferred in conceptual system design solutions as depicted in Figure 5.3.

Max-flow-between-hubs is allocated to the concept exploration of phase of the systems perspective, due to its designer's rule-of-thumb nature. It is a quick, low fidelity metric that provides a first estimation of the vulnerability of a logical architecture. For concept definition, hurt state percolation is proposed. This way of addressing vul-

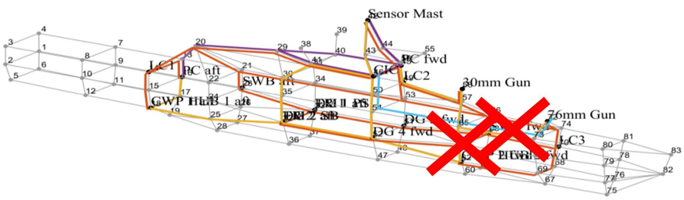



**Figure 5.4:** Example of a deterministic hit scenario with one hit covering two compartments, as used in the hurt state percolation method. Figure adapted from Duchateau et al. (2018).

nerability is used by Duchateau et al. (2018). With this approach, the consequences of a hit are determined by systematically removing parts of the system design, which represents damage cases. For each of these individual damage cases it is checked which system components are still connected, and whether these connections can provide the required resources to (vital) users. A hit is defined as an occasion where a compartment, bounded by bulkheads and decks, is disabled. A hit in one compartment also affects the adjacent compartment in transverse direction (i.e. port side or starboard), if applicable. It is user-defined whether the compartments above, below, before, and aft of the hit compartment are affected as well. For small hits this is not the case, while for large hits it is included. The damage of such a hit is assumed not to propagate through blast-resistant bulkheads. An example of a hit scenario with one small hit is provided in Figure 5.4. It comprises both the port side and starboard compartment, but the damage does not propagate through decks of transverse bulkheads. All compartments have equal hit probability, so the method does not account for signatures such as hot spots at this stage. Nonetheless, the method can account for this, if desired.

The deterministic hit simulating approach makes the method suitable for the concept definition stage. The approach can be used both on a system topology or a fully routed topology throughout the ship. The difference between these two is the hit-state information. If a topology is used as the system design, nodes or edges will be hit and removed accordingly. If a routed topology is used, one or more compartments will be hit, and thereby the associated nodes and edges of the topology. A depth-first tree search algorithm on the damaged system topology forms the basis of this approach. Each node in the network is checked for their individual supply requirements. The results give insight into where bottlenecks in the system design occur once hit.

For single or dual hit cases it is possible to simulate all possible hit cases within the order of seconds for a concept comparable up to about 40-45 edges in the logical architecture. For more than two hits a combinatorial explosion of possible hit location combinations occurs. Assessing such scenarios requires a finite number of random cases. The vital users that are assessed can also be grouped into capabilities, such as Anti-Air Warfare (AAW) or Anti-Surface Warfare (ASuW). This comes at the cost of adding more simulations, as multiple combinations of systems may exist for a single function. The hurt state percolation approach does not take into account remaining network capacity. Hence, a connected network in this method does not necessarily imply a working network in reality - it is a necessary but not sufficient condition.

The Markov method of this dissertation is allocated to concept exploration of the ship perspective. As stated in Section 2.4, the method aims to identify driving factors of vulnerability in a probabilistic fashion. This particularly suits the concept exploration phase. As explained in Chapter 3 the method has been developed for the ship perspective, though it could in principle also be applied to the systems perspective. For detailed design and engineering, various other methods exist. They have already been discussed in Section 2.3. Methods like RESIST, SURVIVE and SURMA take layout into account, and can be allocated to the ship perspective. Section 2.2 has discussed S3D. Though intended for the early design stage, this tool allows for higher levels of fidelity as well, and is thus allocated to detailed design and engineering in this framework. GES is a similar tool, specifically designed within the context of the Netherlands, by the same developers as RESIST (TNO, 2019).

### 5.2.2 Work flow for early stage design of distributed systems

The second part of the integration effort consists of further development of the list of steps of de Vos (2018). The first steps, that lead up to the possibility of defining / generating a logical architecture, are given below:

1. Define vital, mission-related components, i.e. end-users.
2. Define support components (suppliers) and distributed systems that the end-users require to function.
3. Define hubs in each distributed system.
4. Generate or define by hand topologies that provide the logical relations in the distributed systems, i.e. the connections between the components.
5. Assess performance of logical architectures (design solutions for interdependent distributed systems) with respect to different design objectives including vulnerability.

The first four steps are independent of the system or ship perspective or design stage. They precede any assessment and/or further development of the ship or system design. Step 5 is the first time that the vulnerability of the logical architecture is assessed. According to the framework, max-flow-between-hubs could typically be used for this step. After this step, the distinction between the ship perspective and the systems perspective starts to play a role. Once a logical architecture has been developed, it needs to be routed through the ship (ship perspective) and the capacity and dimensions of components need to be established (system perspective). These two steps can be carried out in parallel. For the ship perspective, the procedure continues with:

6. Define the location of nodes in the ship.
7. Generate or define by hand the routing of edges through the ship compartments.

8. Assess performance of routed design solutions of interdependent distributed systems with respect to. different design objectives including vulnerability.

Step 8 comprises a vulnerability assessment of the logical architecture that is now routed through the ship, i.e. a physical solution. The level of detail is still limited, and at this stage it still matters *why* the vulnerability is as it is. Hence, for this step, the Markov method can be used. Parallel to steps 6-8, the systems perspective continues with:

9. Determine the amount of power (effort and flow) the users need in the operational conditions of interest.

10. Determine the individual capacity of the suppliers in order to balance total power supply and demand.

11. Determine the principle dimensions and weights of all components.

Though steps 9-11 are allocated to the system perspective, they are not strictly isolated from the ship perspective. Determining the dimensions and weights of components, for example, needs to be carried out in close cooperation with the more physically oriented ship perspective. However, the two tracks have deliberately been separated because of the fundamentally different goals of the tracks. Similar to the ship perspective, the system perspective needs a vulnerability assessment (Step 12). This assessment needs to include capacity and load balancing. The methods described in this section do not yet support this. Other methods can provide this, such as S3D or GES. However, as indicated by the framework, these methods are typically applied in a later design stage. Hence, a gap remains for a capacity assessment in the early design stage. Chapter 7 gives several brief recommendations for this gap. After Step 12 the ship perspective and system perspective are brought together to ensure adequate integration of these perspectives (Step 13: concept definition). At this stage the concepts (one or multiple) have grown to a considerable level of detail, and a more detailed vulnerability assessment is required (Step 14), such as hurt state percolation. A summary of this list of steps, that together form the proposed integration of the methods, is provided in Figure 5.5.

### 5.2.3 Computational integration

In Sections 5.2.1 and 5.2.2 three early stage methods for distributed systems design have been integrated from a design process perspective. Yet, they are still individual, stand-alone methods. Therefore, further integration on a computational level could be beneficial in terms of efficiency. Computational integration itself does not necessarily result in better designs, but it may make the transitions between the methods easier and faster. Though the methods are currently still self-contained, they rely on the same type of information: a logical architecture of distributed systems with nodes and edges, either or not including a physical routing. This common feature may offer opportunities for integration of these methods. An important consideration for method integration is the size of the system model, i.e. the number of nodes and edges in the logical architecture or physical solution. The max-flow-between-hubs method requires a certain minimum number of nodes (especially hubs) to provide a

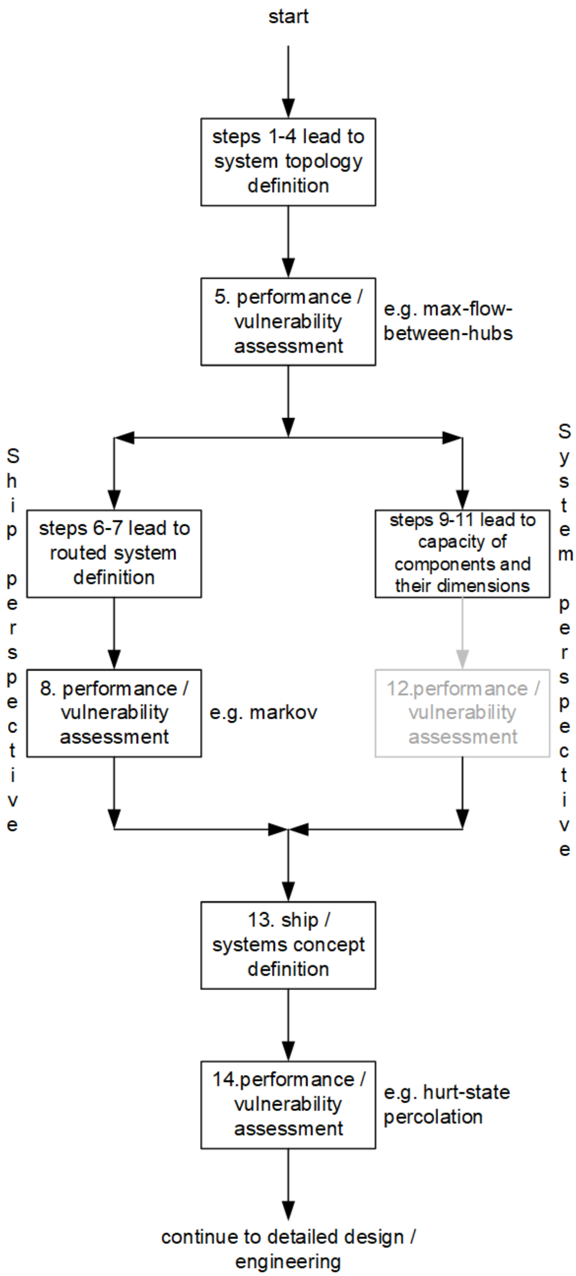



**Figure 5.5:** Proposed integration of methods in ship and systems design process. Figure retrieved from Habben Jansen et al. (2020b).

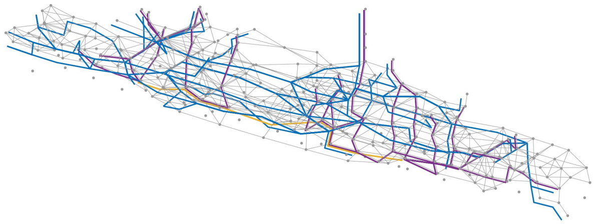


**Figure 5.6:** Example of a scaled-up test case of the hurt state percolation method. Figure retrieved from Habben Jansen et al. (2020b).

meaningful result, and has been applied for a test case with 36 nodes (de Vos and Stapersma, 2018). For the Markov method of this dissertation, the number of edges is determinative for the computational effort. In Chapter 4 a test case with 12 nodes and 12 edges has been carried out. For the hurt state percolation the number of nodes and edges is less relevant. A test case considers about 20 nodes (Duchateau et al., 2018), but the method has been applied with up to 100 nodes, such as presented in Figure 5.6. The computational effort is determined by the number of hits, which is currently limited to two. Larger numbers of hits require a random selection of representative hits.

The typical number of nodes and edges for these methods are summarized in Table 5.2, along with the earlier discussed design stages and system modelling types. In general it can be stated that the earlier an assessment is carried out, the less information it should consider. The vulnerability methods of this chapter follow this statement. Markov and max-flow-between-hubs, which are meant for concept exploration, require indeed less nodes and edges than hurt state percolation, which is meant for concept definition. However, it is also important to consider the two types of modelling systems. Though the system perspective (logical architecture) and the ship perspective (physical soluition) on distributed systems may contain the same type of information, as discussed in Section 5.2.1, a clear sequential approach can be identified: there needs to be a logical architecture before it can be routed through the ship (physical solution). Hence, in the ideal situation, the logical architecture that has been assessed with max-flow-between-hubs can be used to make the physical solution that can be assessed with the Markov method. However, in their current status, the methods do not support the ideal situation because of a difference in their required number of nodes and edges. For a full integration of assessing both the logical architecture and the physical solution in concept exploration, the number of nodes and edges for Markov needs to be increased, or the number of nodes for max-flow-between-hubs should be decreased. For concept definition this issue is less relevant, as hurt state percolation is not limited by the number of nodes and edges, but by the number of hits.

The discrepancy in required number of nodes and edges for Markov and max-flow-between-hubs may be addressed by considering the way in which the codes and algorithms have been written. This has not yet been addressed, as there was little need to do so when the methods were developed as to be self-contained. This dissertation

**Table 5.2:** Overview of main characteristics of the vulnerability methods for distributed systems design. Table retrieved from Habben Jansen et al. (2020b).

| Method | Typical no. of nodes / edges | Design stage | System model type |
|---|---|---|---|
| Markov | <12 | Concept exploration | Physical solution |
| Max-flow-between-hubs | >36 | Concept exploration | Logical architecture |
| Hurt state percolation | 20 - 100 | Concept definition | Logical architecture / Physical solution |

does also not consider this topic, as computational integration is not a goal in itself. It needs to be carried out within the context of the design process of Figure 5.5. This is left as a recommendation for future research, and is discussed in more detail in Chapter 7.

## 5.3 Final considerations for design knowledge

This chapter's discussion on design knowledge management only considers a small part of this vast field. The challenge with design knowledge is that it is highly unspecific and hard to capture or quantify. Section 5.1 posed the question: "When is combined knowledge from methods 'better' than knowledge from separate, individual methods?" Though Section 5.2 has provided a design process and work flow for combining this dissertation's method with other vulnerability methods in early stage ship design, a definite answer to this question has not been established. Consider for reference Figure 5.7. It schematically shows the problem space for design of distributed systems. Furthermore, it shows three separate, smaller parts of this problem space, that have been addressed in this chapter. These three smaller problems all have a separate solution, that are part of the solution space. But how much of the total problem and solution do these methods form together? Are the three problems for example 10%, 40% or 70% of the total problem? How can this be determined? Can it be measured in percentages at all? Are the combined solutions a smaller or bigger portion of the solution space than the combined problems of the problem space? Furthermore: design of distributed systems is only one of the fields in which the generalised problem of this dissertation (i.e. the relation between requirements and concepts, and knowledge and information) presents itself. This dissertation does not address - to mention a few - general arrangements, structures, or hydromechanics. Then what is the boundary of the problem, and the associated solution?

These are a lot of important and relevant questions, but due to the unspecific and subjective nature of knowledge, it is unlikely that definite answers will ever be provided. However, the inability to define *definite* answers does not mean that there are no

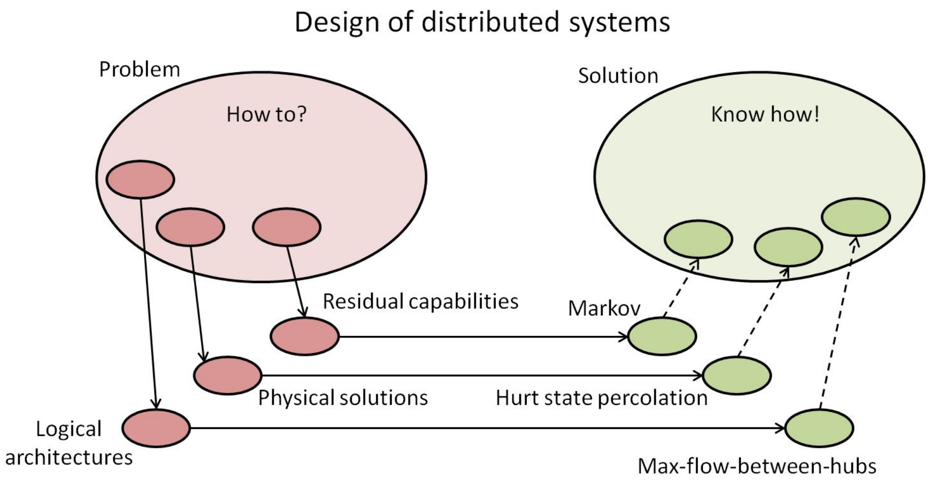



**Figure 5.7:** Relation between problems and solutions discussed in this chapter.

*useful* answers. This issue does not only arise within the context of this chapter. It stretches far beyond the topic of distributed systems design, and relates to the very nature of research in the field of design and engineering, and the associated knowledge that is sought. For ship design research, the following question arises:

*Should ship design research be scholarly or useful, or can the two be combined?*

This question continues to be a subject for ongoing debate, and is for example discussed by Edstrom (2017). She focusses on engineering education, which is different from ship design (though ship design can also benefit from insights in the field of engineering education, as discussed by Kana et al. (2016)). However, what is relevant for this discussion, is Edstrom's review of different types of research. A distinction is made between a method-led research tradition, that focusses on proving something with truth as the main criterion, and a problem-led research tradition that focusses on selecting questions that are significant for real-world problems, and providing useful insights that are relevant for these problems. In terms of these two traditions, ship design research is mostly problem-led. This does not mean that methodology is not important for ship design research, but the priority is more on usefulness and less on scholarliness. Edstrom (2017) provides no advice on how to overcome this tension, but instead argues to embrace it to enable a productive dialogue. Though there is in general no preference for either usefulness or scholarliness, she recommends to have mechanisms to uphold standards, in order to ensure that research efforts are neither scholarly nor useful are filtered out. In terms of ship design, this can be supported by peer review in both scientific and practitioner communities. The focus, however, remains on usefulness, due to the problem-led nature of ship design.

Another issue to keep in mind is that all knowledge provided in this dissertation - or publications in general - is inherently explicit knowledge: it has been coded or calculated, documented, and can be transferred. Yet, the tacit knowledge of ship design, embedded in designers' experience, insights, or intuition, is by definition not yet captured. Though it is possible to translate tacit knowledge into explicit knowledge, the fact remains that there is a component of art in ship design, as already discussed by Andrews (2007) (see Section 5.1). What eventually matters, is whether knowledge - either explicit or tacit - supports advances in ship design - either on a scholarly or practitioner level. This problem-led approach should be a key driver for ship design related research efforts.

# Chapter 6

# Extended opportunities of the method

Chapters 3 and 4 have introduced a new method for an early stage vulnerability assessment. The relation of this method to the early stage design process has been discussed in Chapter 5. Though these chapters form the main body of this dissertation, the opportunities that the new method offers, are not necessarily restricted to these applications. As such, this chapter introduces other applications of the method. The major difference between this chapter and the previous chapters is that the previous chapters have defined a new solution to an existing problem, while this chapter aims to apply the existing solution to a new problem. These different perspectives are discussed by e.g. Kossiakoff et al. (2011), who argue that both perspectives are acceptable for developing new systems, products, or methods. They differentiate between operational deficiencies and technological opportunities. The former is needs-driven, and is comparable to what is done in the previous chapters. The latter is technology-driven, and compares with the approach of this chapter.

This chapter discusses three further applications of the method. Section 6.1 provides an alternative way for defining residual capability levels, which can be used to evaluate graceful degradation and worst case scenarios. Subsequently, Section 6.2 discusses how the method can be used to assess the quality of the logical architecture, in addition to the physical solution. Section 6.3 discusses an opportunity to a smaller part of a logical architecture at a higher level of detail. Several closing remarks are provided in Section 6.4

## 6.1 Separate residual capability levels

As discussed in Section 2.3.1, the concept of graceful degradation is highly important for defining requirements for residual capabilities after damage. This concept is incorporated in the test case of Chapter 4. The definitions for the residual capability levels for the various impact levels have been provided in Table 4.1, and are repeated in

Parts of this chapter are based on Habben Jansen et al. (2020a).

**Table 6.1:** Residual capability for impact levels (Habben Jansen et al., 2020a).

| Impact level | Required residual capability | Qualitative capability 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 |

Table 6.1 for the sake of this section's discussion. The table shows that higher levels of residual capability always include lower levels of residual capability. For example, if moderate capability is available, minimal capability is available as well. Similarly, if considerable capability is available, moderate and minimal capability are available as well. In other words: the capability levels build upon each other, with the idea that an increasing impact level gradually results in loss of less important capabilities, while the vital capabilities remain available.

The residual capability levels in Table 6.1 do not contain all residual capabilities that are possible. For example, the capabilities 'two-shaft propulsion, but no weapons' and 'only the offensive weapon' fall out of the scope of the required levels. This indicates that such capabilities do not follow the concept of graceful degradation. For example 'two-shaft propulsion, but no weapons' is more than minimal residual capability, but less than moderate residual capability, since the defensive weapon is not available. Similarly, 'only the offensive weapon' contains the first system for which loss is accepted, while it does not contain other, more important systems. Hence, in terms of graceful degradations, these are 'odd' capabilities. Yet, they could be the result of certain hit scenarios. Assessing the residual capabilities separately, rather than built upon each other, indicates how good graceful degradation can be facilitated. In order to separate the different residual capabilities, new definitions of the required resources for the different levels are needed. These are provided in Table 6.2. Compared to the original definitions of the capability levels, two extra levels have been added. The level 'zero' indicates that no residual capability at all is left. This level was not included in the original definitions, as the probability to have at least zero capability is always 100% and thus trivial. The level 'other' contains all capabilities that do not follow the concept of graceful degradation, such as the two examples given previously.

These separate definitions of the capability levels are applied to the same notional OPV that has been used in Chapter 4 (the original concept, before design modifications were made as a result of the eigenvalue assessment). The results for both the conventional concept and the IPS concept are provided in Figure 6.1. For each number of hits, the probabilities of all levels sum to 1. This means that the ship is in *only* one of the levels, rather than in *at least* one of the levels. The curves for full residual capability are the same as the original test case of Chapter 4. This makes sense, because 'full residual capability' is the same is 'at least full residual capability'. The probabilities for the considerable, moderate, minimal, and zero level are

**Table 6.2:** Required resources for each capability level for the separate level definition. The original level definition (see Table 4.1) is added for reference. & = AND, | = OR, $\oplus$ = XOR, $\sim$ = NOT

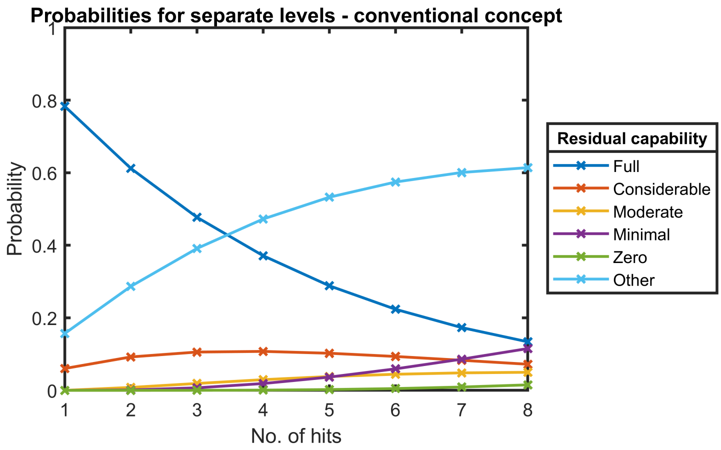
| **Residual capability** | **Required resources (original)** | **Required resources (separate)** |
|---|---|---|
| Full | Prop PS & Prop SB & E CIWS & E HEW & CW CIWS & CW HEW | Prop PS & Prop SB & E CIWS & E HEW & CW CIWS & CW HEW |
| Considerable | Prop PS & Prop SB & E CIWS & CW CIWS | Prop PS & Prop SB & E CIWS & CW CIWS & ~(E HEW & CW HEW) |
| Moderate | (Prop PS \| Prop SB) & E CIWS & CW CIWS | (Prop PS ⊕ Prop SB) & E CIWS & CW CIWS & ~(E HEW & CW HEW) |
| Minimal | Prop PS \| Prop SB | (Prop PS ⊕ Prop SB) & ~(E CIWS & CW CIWS) & ~(E HEW & CW HEW) |
| Zero | N/A | ~Prop PS & ~Prop SB & ~(E CIWS & CW CIWS) & ~(E HEW & CW HEW) |
| Other | N/A | Everything else |

relatively small, where the considerable level has the largest probability of this set. A remarkable result are the probabilities for other levels for both concepts. These are about 15% for one hit and increase to 55-60% for higher numbers of hits. This indicates that there is a substantial probability that the associated capability levels are not met. However, this statement comes with two important remarks:

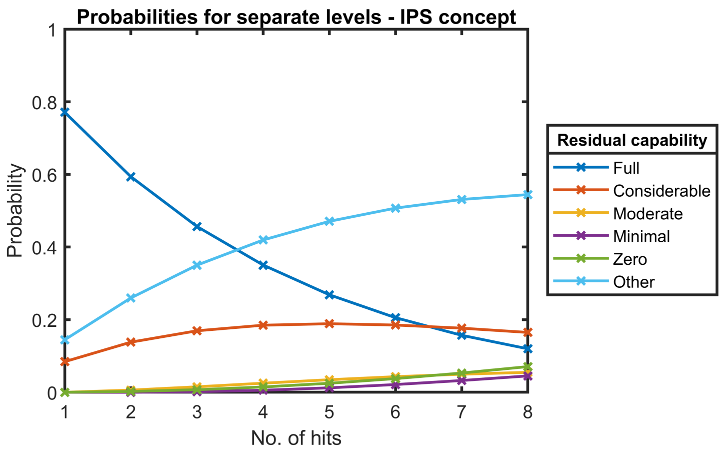
1. *Other* levels of residual capability are not necessarily *bad* levels of residual capability. Capabilities that fall outside the pre-defined levels may still be useful. For example, if full propulsion but no weapons are left (which is one example of an 'other' level), the propellers can still be used to leave the theatre in a rapid fashion. How useful this is, is very much dependent on the circumstances.

2. It is not known how these figures compare to existing ships that have been designed in accordance with graceful degradation. The concept that is used for this assessment, has very much been simplified compared to existing ships. If Figure 6.1 is made for existing ships, the probability for other capability levels may be lower. It may also be similar or even higher, due to the fact that damage does not always occur in the way that it is 'wanted' or planned for. A validation with an existing design needs to be carried out in order to assign the right value to these results.

Though these two remarks provide some reservations for drawing strong conclusions from this assessment, the result in itself provides an interesting direction for further




**(a)** Conventional concept




**(b)** IPS concept

**Figure 6.1:** Probability for the separate capability levels, using the notional OPV of Chapter 4.

investigations. Similar to the test case of Chapter 4, the curves that form the capability levels can be expressed in terms of the eigenvalues of the transition matrix. As such, the driving factors for the level of other residual capability can be identified. Subsequently, design recommendations for decreasing this curve can be obtained. This eventually results in a modified concept, which can then be evaluated with the procedure of Chapter 4. Hence, this approach provides a second way in which graceful degradation can be assessed.

A second interesting feature of the separate capability levels is the ability to investigate what is *not* left, instead of what is left. The curve for zero residual capability indicates the likelihood for the worst case scenario, i.e. the scenario where there is no

**Table 6.3:** States that lead to the worst case scenario for the conventional concept.

| State | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3719 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 1 |
| 3841 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 3981 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 |

residual capability at all. Though Chapter 1 has explained that such specific scenarios are usually considered after the concept exploration phase, an early assessment may already indicate weak spots in the logical architecture or physical solution. For the conventional concept, the probability for this state is zero for 1 and 2 hits. In other words: full loss of capability occurs only at 3 hits or more. For 3 hits, the probability for the worst case scenario is 0.00013, i.e. 0.013%. This is a very small probability, but it is still interesting to investigate when this happens, as it indicates the hit scenario for which the ship is most vulnerable. The states that contribute to this probability are listed in Table 6.3. One of the three hits that contribute to this state, is always in the starboard drive train, as it shares no compartments with other parts of the physical solution. For State 3719, the additional two hits are in SWB1 aft, and the compartment above SWB2 forward, as electricity and chilled water routings are located together there. For State 3841, the combination of DE1 and DG2 leads to the worst case scenario, and for State 3981 the combination of DE1 and SWB2. Hence, from the perspective of the worst case scenario, DE1 has an unfortunate location. If it is hit, it does not only disable the port side drive train, but also the electricity supply from DG1, as its routing runs through the same compartment. A hit over there, combined with a hit in the starboard drive train and a hit in or near the forward SWB2 compartment disables the entire physical solution. This indicates that particularly the locations of the aft engine and routings may need to be reconsidered.

For the IPS concept, only 2 hits are needed to obtain the worst case scenario. This is because the propulsion is not separated in this concept. The probability for the worst case scenario after 2 hits is 0.0023, i.e. 0.23%. This is more than a factor 10 higher than the conventional concept, though still a very small probability. The states that contribute to the worst case scenario for the IPS concept are listed in Table 6.4. Compared to the conventional concepts, more states contribute to the worst case scenario. Yet, a closer observation shows that for all those states, Connections 1, 2, 4, 5, 6, 7, and 8 are off. This only happens if SWB1 (aft) gets hit. This single hit directly disables both propellers and the CIWS. If a second hit occurs forward, where the HEW is located, the entire ship is disabled. Hence, SWB1 is a highly critical part of this concept. This is not necessarily because of the physical solution, i.e. the way in which the routings are located inside the ship. Even with just the logical architecture itself, SWB2 is already critical. Hence, the advice here would be to modify the logical architecture, rather than to apply the method of this dissertation to obtain a better physical solution. A better physical solution can not make up for a poor logical architecture.

**Table 6.4:** States that lead to the worst case scenario for the IPS concept.

| State | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3570 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 |
| 3571 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 |
| 3572 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 |
| 3574 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 |
| 3575 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 |
| 4087 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 1 |

## 6.2 Hits vs. failures

Up to now, this dissertation has considered vulnerability in terms of a man-made hostile environment. As such, damage has been modelled probabilistically by a multitude of hits that each disable one compartment. However, Chapter 1 has outlined that vulnerability may also result from increasing complexity and interdependency of the distributed systems themselves. The strong interdependencies between components of the distributed systems may result in cascading failures that have not been envisioned or modelled before. Contrary to hits, these type of failures are not necessarily associated to physical locations in the ship. In other words: the damage occurs in a system or component, not in a compartment. Though systems and components are located in actual compartments, this is a fundamentally different perspective on damage. As such, the more generic term 'failure' is used to describe such damage, rather than 'hits'. The method of this dissertation can also be used to assess this type of vulnerability. Instead of hits in the physical solution, failures in the logical architectures need to be modelled.

Some of the assumptions made for modelling failure instead of hits are slightly different than the original assumptions of the method. What remains similar, is that one failure occurs at every time step in the Markov chain. In addition to that, a failure is still assumed to encompass one connection in the logical architecture at the time. Similar to the original situation, a connection also includes the nodes at both ends (see Figure 3.5). However, the consequences of this assumption are different. For original situation it is possible that a multitude of connections is disabled by one hit. This happens for example if a compartment where a switchboard is located, gets hit. This hit disables both the connections from the generators to the switchboards, as well as the connections from the switchboard to the users. It is also possible that a hit occurs where no system is located, which results in no (further) loss of capabilities. For the new situation this is different. A failure that results from complexity of the distributed systems is inherently related to those systems. As such, it makes no sense to include the option where a failure occurs that does not result in loss of connections. In addition to that, it needs to be ensured that an increasing number of failures represents an increasing impact level. For the OPV test case this was related to the number of hits - be it with minor or major impact dependent on the location of the hit - but the present test case is not based on hits. As such, the increasing impact level is represented by an increasing number of lost connections. Also, connections

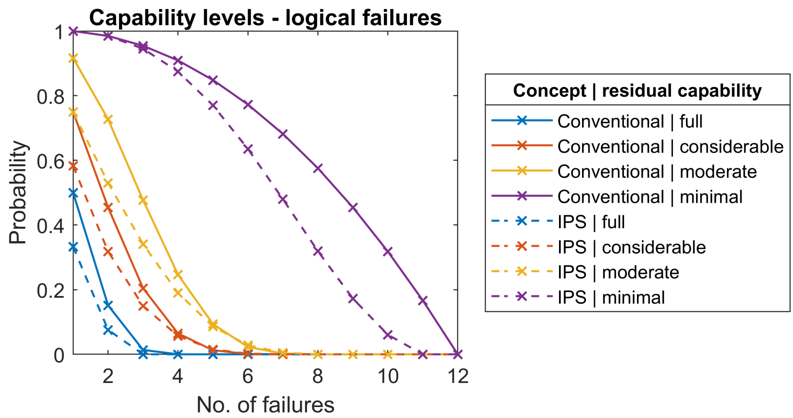



**Figure 6.2:** Probability for capability levels based on failures in the logical architecture, using the notional OPV of Chapter 4.

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. This way of modelling is similar to edge removal in network science (Ruths and Ruths, 2013). Note that node removal is not accounted for in this case, since one node may be connected to multiple edges, while only one edge is removed at the time.

As can be derived from this discussion, the residual capability of a logical architecture is very much dependent on how the failure is modelled. The assumption that one connection is disabled at the time has no relation to how likely it is that this failure scenario will actually occur. However, as this dissertation considers vulnerability, not susceptibility, the starting point is the fact that failures *will* occur, and that there is a need for an early assessment of the consequences of these failures. As these failures may also be unexpected or may never have happened before, the bias on how likely it is that a failure occurs has deliberately been left out.

This way of modelling failures in a logical architecture has been applied to the notional OPV, again with a conventional concept and an IPS concept. Similar to Section 6.1, the original concepts are used, before adjustments were made based on the obtained design recommendations. The residual capability levels have been calculated up to 12 failures. Since both logical architectures consist of 12 connections, this is the situation where all connections have failed. Hence, this range spans the full scope from zero to maximum failure. The results are presented in Figure 6.2. The results show that for all capability levels, the curves for the IPS concepts are lower than for the conventional concept. In other words: the logical architecture of the IPS concept is more vulnerable. This connects to the conclusion of Section 6.1.

The curves of this way of modelling failure are mostly for analysis purposes, rather than for obtaining design knowledge. Where the curves of the hit modelling type could be expressed as explicit equations with eigenvalues of the transition matrix, this is not possible for the failure modelling type. This is because of the mathematical set-up of the transition matrix. For the hit modelling type, it is possible that hits occur in compartments where no system or routing is located. This results in no (further) loss of capability, and is expressed as the probability to remain in the same state. This probability is by definition an element on the diagonal of the transition matrix, which corresponds to an eigenvalue. These eigenvalues are needed to understand the shape of the curve. For the failure modelling type, however, it is not possible that a failure occurs that does not disable one of the connections. Hence, all values on the diagonal of the transition matrix are zero, except for the final state where all connections are off (where the diagonal value is 1). Under these conditions, the rank of the matrix does not equal its size, so matrix diagonalisation is not possible. Hence, the curves can be used for an analysis, but not for obtaining design recommendations towards improved logical architectures. Despite this limitation, this assessment, together with the assessment type of Section 6.1 provides a metric for the quality of the logical architecture itself. This is an addition to the original set-up of the method, which considered the physical solution for a given logical architecture.

## 6.3 Level of detail in logical architectures

It has previously been noted in Section 3.2 that the logical architectures that can be used for the method are limited to 13 edges. At the same time, there may be a desire to perform a vulnerability assessment on a higher detail level than the OPV test case discussed in Chapter 4. A compromise can be established by considering a smaller part of the logical architecture, but in more detail. This is done in this section, where only the chilled water distributed system is considered. In the OPV test case of Chapter 4 the chilled water distributed system was limited to two or three connections. This can now be increased to thirteen connections. However, this comes at the cost of not including other parts of the distributed systems, such as the electrical power system. As explained in Chapter 2, this violates the principle that an integrated approach for vulnerability assessments (and design in general) is needed. Hence, the focus on a single but more detailed distributed system should not be a stand-alone assessment. It is envisioned that such an assessment is carried out after an integrated assessment of the distributed systems as a whole. This first integrated assessment should capture the main principle of distributed systems design (e.g. describe whether a conventional, IPS or hybrid concept is investigated), but does not need to include more detail than that. After more detailed assessments of individual distributed systems, which can also be done with the method described in this dissertation, a second iteration of an integrated assessment can be carried out. With the current specifications of the method, it is advised to use another method for that second iteration, for example the hurt state percolation approach of Duchateau et al. (2018) (see Chapter 5).

A second test case is set up to investigate the possibility to assess more detailed logical architectures of a single type of resource. 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

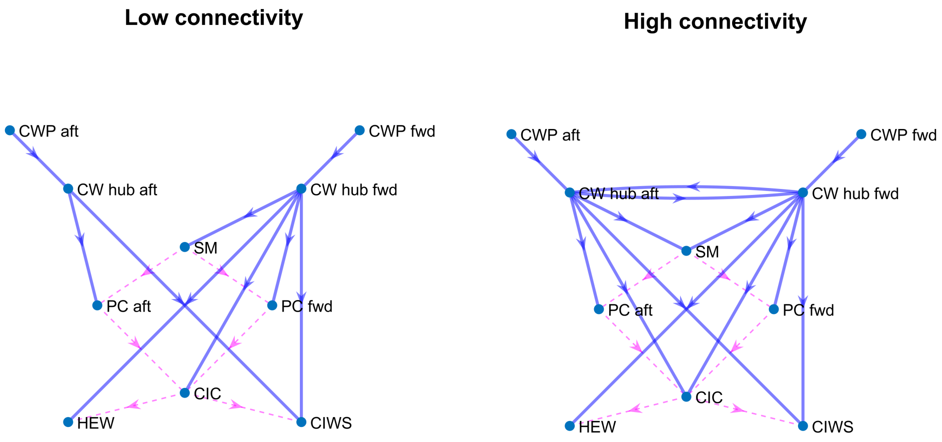



**Figure 6.3:** Two logical architectures for the chilled water distribution system, adapted from de Vos (2018). The dotted lines in magenta represent the data network, which is not considered in this test case, but which needs to be supplied with chilled water. Figure retrieved from Habben Jansen et al. (2020a).

both weapon systems is supplied by two chilled water plants (CWP's) 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 center (CIC). Hence, the logical architecture consists of 10 nodes.

Two versions of connecting the 10 nodes are compared. These have been adapted from de Vos (2018), and are presented in Figure 6.3. 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 backward 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 separ-

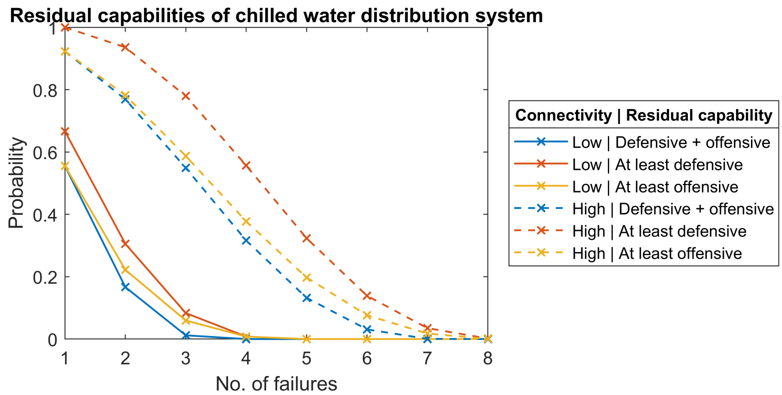



**Figure 6.4:** Probability of availability of the main capabilities for the chilled water distribution plant. Figure retrieved from Habben Jansen et al. (2020a).

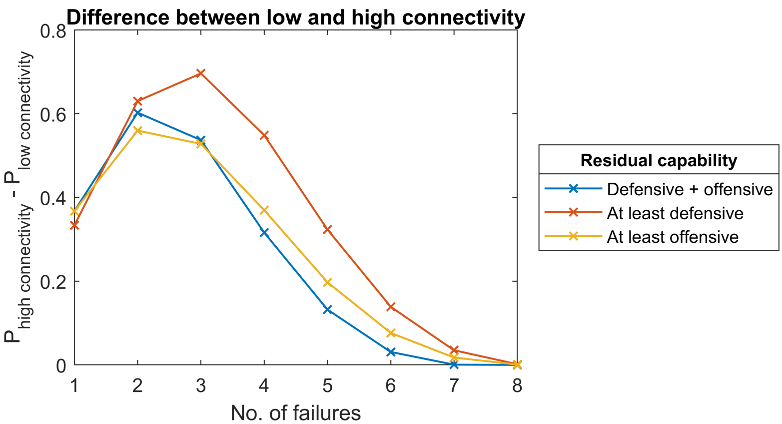



**Figure 6.5:** Difference in the probability of availability between the high and low connectivity architectures, in favour of the high connectivity version. Figure retrieved from Habben Jansen et al. (2020a).

ate zones. The interdependencies between zones is an important point of attention for such an assessments. Though the zones are designed to be independent, this can't be fully realised in practise, since distribution elements such as a main pipeline run through multiple zones. However, a full investigation on linking multiple zones together is not included in this dissertation.

Similar to the OPV test case, damage can be modelled as either hits or failures. Since hits have already been discussed in considerable detail throughout this dissertation, this test case applies failures, similar to Section 6.2. The results of the test case can be visualised in a similar way as the OPV test case. However, 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.

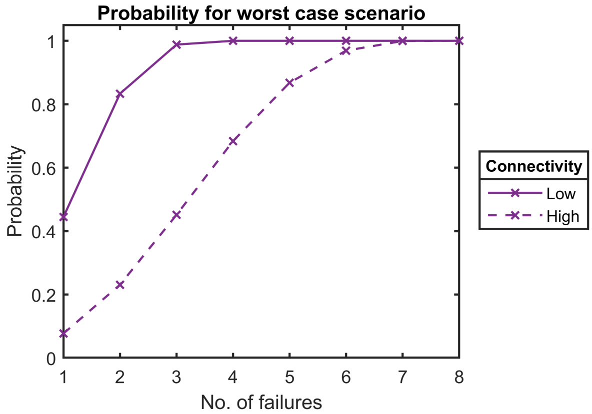



**Figure 6.6:** Probability for the worst case scenario for the high and low connectivity architectures. Figure retrieved from Habben Jansen et al. (2020a).

The results are presented in Figure 6.4. 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 2-4 failures. This is further illustrated by Figure 6.5, which shows the absolute difference in probability of availability between the low connectivity and high connectivity version. 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, similar to Section 6.1. This is the same as the inverse of the previous curves, but provides a different 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 6.6. 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 actual states contribute to the worst case scenario, and how they can be avoided.

## 6.4 Closing remarks

This chapter has presented extended opportunities for applications of the Markov-based vulnerability method. Where the previous chapters have defined a ship design problem for which the method is a solution, this chapter has applied the opposite perspective: the method was taken as a starting point, and has been applied to other problems. The discussions on the three extended applications of this chapter are meant as a starting point for further investigations. As mentioned in Section 5.1, defining new problems for an existing solution has the potential risk that it 'solves' problems for which other solutions are already available. As such, the three problems discussed in this chapter (separate residual capability levels, the vulnerability of logical architectures, and the level of detail, respectively) need to be defined more precisely. Furthermore, existing alternative solutions need to be analysed. Subsequently, the potential of the new method for extended applications can be exploited in a suitable and relevant fashion.

# Chapter 7

# Conclusions

This chapter forms the closing part of this dissertation. First, the research objective of Chapter 1 and requirements of Chapter 2 are revisited in Section 7.1, after which a final research conclusion is drawn. Section 7.2 explicitly lists the contributions of this dissertation. The societal context and impact of this research are discussed in Section 7.3. Finally, recommendations for future research, in terms of vulnerability reduction, distributed systems design, and ship design as a whole, are provided in Section 7.4.

## 7.1 Conclusions

In order to draw conclusions from this research, the research objective needs to be revisited. This has been defined as (see Chapter 1):

*Develop a knowledge-providing early stage ship design method that assesses the performance of a concept, identifies the driving factors for that performance, and provides design recommendations towards better solutions, in the context of vulnerability reduction of naval ships.*

This research objective is based on the underlying problem that during concept exploration generalised design knowledge is needed to generate feasible concepts, while this knowledge actually depends on information from those specific concepts. Hence, an incompatibility between generating concepts on the one hand, and assessing concepts on the other hand occurs. This problem applies to early stage ship design in general, but for naval ships it manifests itself in particular in vulnerability reduction, which is the context of this research.

The different parts of the research objective have been considered throughout this dissertation. A method to assess the vulnerability of a concept has been developed in Sections 3.2 to 3.5. The method uses a discrete time Markov chain, which allows for describing various conditions of a system (in this case: a ship) and the probability that these conditions change over time. The development of a new method was not a goal in itself, since other vulnerability methods exist as well, but the integration of all parts of the research objective needs a method that differs from existing methods. This particularly links to the second and third part of the research objective, i.e. the ability to identify driving factors and obtain design recommendations for vulnerability reduction. This has been discussed in Section 3.6, which provides a way to link the vulnerability of a concept to specific parts of the physical solution. This is done through matrix diagonalisation and an eigenvalue assessment of the Markov chain, which is the very reason that Markov theory has been selected as the mathematical basis for the new method. The eigenvalue assessment provides a derivation of which specific routings in the physical solution have the strongest influence on the vulnerability, and how these can be modified to improve a concept. Based on these considerations, it can be concluded that the research objective has been met. However, the additional requirements for the method (see Section 2.4) need to be checked in order to evaluate *how good* the new method meets the research objective:

1. Different design disciplines need to be integrated early on. In terms of vulnerability, this means that different types of resources in distributed systems, such as electricity, chilled water, and data, need to be addressed simultaneously.

This is supported by the new method. Every connection in the logical architecture has its own type of resource. By means of logical relations, individual connections can be combined to form capabilities. The method has shown that the fact *that* distributed systems are placed together in one ship already relates them from a vulnerability perspective. This also holds if there is no physical, logical, or operational overlap between the systems.

2. The method needs to be able to do an assessment in a rapid and generalised fashion, to align with the purpose of concept exploration.

This requirement is met. For vulnerability assessments comparable to the test case of Chapter 4, the computational time is in the order of several minutes. Up to several additional hours are needed to make the translation from systems to capabilities and to interpret the results. The total assessment takes less than one day to carry out. This supports a fast and interactive dialogue that iterates between requirements and concepts. The generalised nature of the eigenvalue assessment makes the results of a single assessment applicable for any concept with the same logical architecture.

3. The level of detail needs to be limited, but sufficient enough to provide a meaningful result.

This requirement remains a topic of attention. As stated in the research objective, this method is intended for the early design stage, more specifically, the concept exploration stage (see Section 1.1). In order to evaluate if the method supports this stage, a test case has been carried out in Chapter 4. During this test case, it turned out that the method supports logical architectures up to 13 edges, which in on the lowest end of what is typically assessed in the concept exploration stage. Integration of the method with other vulnerability methods showed that the different levels of detail of the different methods do not yet fully align.

4. The vulnerability needs to be assessed in a probabilistic fashion, because 1) it is unknown where hits (or other damage) will occur, and 2) the concept of graceful degradation can not ensure a probability of 1 that certain systems will be available after damage.

The probabilistic approach is inherently provided by the Markov chain. The method considers all damage scenarios at once, rather than modelling and aggregating individual damage cases. The results are expressed in probabilities that certain levels of residual capability are still met after damage.

5. The way in which hits are modelled needs to be able to represent asymmetric threats, i.e. multiple hits with smaller damage extents, contrary to single hits with a large damage extent.

Every hit scenario that is assessed probabilistically, consists of multiple hits (up to 8 for the test case, but other numbers of hits could be realised as well) for which the damage is contained within one compartment. This aligns with the nature of asymmetric threats. Hence, this requirement is met.

6. The contributions of the method need to be outlined with contributions of other methods, resulting in a clear structure on when to use which method(s) for early stage design of survivable naval ships.

The new method has been combined with two other methods in a procedure for early stage design of distributed systems. This procedure combines the ship perspective and the systems perspective for distributed systems design, which places the three individual methods into larger contexts than what they were originally developed for. At the same time, it is acknowledged that it is hard to measure or quantify the knowledge that is obtained from this combination of methods. Due to the problem-led nature of ship design, it is of particular importance that this knowledge can be used. This has been accounted for by making the three methods actionable in a work flow for distributed systems design.

From these six requirements, the third one is currently limiting for the applicability of the method. Hence, the overall conclusion is that the research objective has been met, provided that the method currently is restricted to a logical architecture with limited size and complexity. Recommendations to overcome this challenge are provided in Section 7.4.

## 7.2 Contributions

This dissertation has provided the following contributions to the field of early stage ship design:

- A probabilistic vulnerability assessment method on a residual capability level has been developed. Distributed systems on board ships provide capabilities. However, the relation between systems and capabilities is not one-to-one. The new method takes this translation into account for assessing vulnerability. This is done at a probabilistic level, which suits the purpose of the concept exploration stage, and accounts for the fact that graceful degradation of systems can not be expressed in a deterministic way.

- An eigenvalue assessment of the transition matrix of the Markov chain has been developed, which identifies driving factors for the vulnerability. Some routings in a physical solution have a stronger influence on the vulnerability than others. By means of the eigenvalue analysis of the method, the routings that are most decisive for the vulnerability can be identified. This includes an assessment on whether this influence is positive or negative. Using the fact that the eigenvalue analysis holds for any physical solution for a given physical and logical architecture, direction towards better (i.e. less vulnerable) physical solutions (i.e. routings) can be obtained.

- A quantification of interdependencies between various levels of residual capability has been developed, based on the eigenvalue assessment. If one level of residual capability is improved by adjusting the physical solution, other residual capability levels could change as well due to interdependencies between the different levels. This change could be an improvement as well, but it could also be an impairment compared to the original physical solution. Since the method inherently takes interdependencies into account, the consequences of a modification of the physical solutions for *all* levels of residual capability are elucidated.

- An improved work flow for early stage design of distributed systems has been developed, allocating the right vulnerability methods to the right problems. The new method has been developed as a solution to a clearly bounded, self-contained problem. Yet, this problem is part of early stage design of distributed systems as a whole. As such, the new method, along with two other methods, are combined in an existing procedure for early stage design of distributed systems. This procedure has been updated to include these methods, and to distinguish between steps that can be taken serial and in parallel.

## 7.3 Societal context and impact

The method described in this dissertation has been developed in the context of naval ships. Since these are government owned ships that are financed from public resources, this research has a direct link to the society as a whole. This research has the potential to impact society in two ways:

1. More survivable naval ships. The method discussed in this dissertation provides directionality and design recommendations on vulnerability reduction in the early design stage. If applied successfully, the basis for less vulnerable, i.e. more survivable ships can be established at this stage. Combined with more detailed vulnerability assessment in later stages, this can lead to more survivable ships. The more survivable naval ships are, the stronger the strategic advantage over adversary parties is. Hence, more survivable ships are better in protecting the nation's interests.

2. Cost savings. The design recommendations for less vulnerable ships that this research provides are applicable to the early design stage. This is where most of the eventual costs of the project are locked in (see also Chapter 1). If the method of this research is successfully applied, the design can converge faster towards a concept with the required vulnerability characteristics. This saves time, and prevents costly design modifications in later, more detailed design stages. As a result, less public resources are required for the project.

The method discussed in this dissertation is not the only method that can contribute to more survivable ships and cost savings. Many other factors - both technical (*what* to design) and organisational (*how* to design it) - impact the performance and costs of a naval ship as well. Hence, it is not straightforward to express the advantages of the method in actual monetary value or other performance indicators. As such, the relation of the new method to the ship design process as a whole remains a key factor of interest. This also holds for other research and design efforts. Dialogue between different disciplines therefore continues to be indispensable, and needs to be applied at both research and practitioner level.

The naval focus of this dissertation means that this work is envisioned to contribute to defence activities. This can - not necessarily, but at least optionally - involve warfare. The act of warfare is highly politically sensitive, and could have severe and devastating consequences. The question whether warfare can be justified, and in which cases, is a field of research and dialogue in its own, and is not considered in this dissertation. Despite the violent-laden nature of warfare, this research seeks to minimise consequences of weapon effects. The aim is to increase survivability, primarily in terms of materiel systems, but indirectly also for personnel on board. Hence, the focus of this research lies on surviving, not on engaging. Nevertheless, this ethical aspect should not be passed over carelessly.

Despite the naval focus, this research can also be used for civil applications. Vulnerability reduction is also of interest to commercial ships. The difference with naval ships is that vulnerability of commercial ships likely doesn't result from weapon effects, but from other factors, such as rough seas, collisions, or insufficient system reliability. As a result, the method of this dissertation can also be applied to commercial ships, in particular those that rely strongest on distributed systems. Relevant ship types include cruise ships and autonomous vessels. With the method described in this dissertation, these ships can be designed more survivable and less costly as well, just like naval ships. This mainly leads to benefits for the shipyard or shipping company, such as competitive advantage. However, it can also contribute to enhanced overall safety for (passenger) ships, for example in the context of the Safe Return to Port regulation of the International Maritime Organisation (as discussed by e.g. Vicenzutti et al. (2016)).

## 7.4 Recommendations

Throughout this dissertation, various topics for further research have been touched upon. As such, the following recommendations are proposed:

With respect to the new method:

- Make the method applicable to larger, more complex logical architectures. The allowed size and complexity of the logical architectures is the key limitation of the method in its current status. The ability to include more connections in the logical architecture would align better with the purpose of the concept exploration phase and the integration with other vulnerability methods. However, due to the set-up of the method, the Markov transition matrix becomes four times larger for every connection that is added. As such, efforts to include another connection have currently been of limited use, as the same problem arises again for the next connection. A solution to this problem would be of great value for the usability of the method. A solution with a computational nature is proposed. The code has been developed to provide correct calculations, but not to be particularly efficient. In other words: memory space could be saved by a smarter set-up of the code. This is particularly the case because the more connections are included in the logical architecture, the more sparse the transition matrix becomes. Hence, the number of elements in the transition matrix that actually matter, increases much slower than the size of the matrix itself. If the complexity of the logical architecture is increased, the ability to interpret the results needs to be considered as well. In other words: it is not only about enabling a bigger transition matrix. Defining a procedure to handle the additional information that it provides, is equally important.

- Compare the results of the method with a detailed vulnerability assessment of a fully defined ship. During the verification and validation of the method, it turned out that one of the steps in the validation process could not be completed fully. This concerns the question whether the example problem of the test case is similar to the actual problems that need to be solved. It has already been noted that the method uses a highly simplified version of actual logical architectures on board ships (see also the previous recommendation). In order to determine the consequences of this simplification, the results of the test case need to be compared to the results of a more detailed vulnerability assessment with a ship model where the logical architecture is fully defined. Such a model could for example be a model in RESIST, SURVIVE, SURMA or a comparable tool that is meant for the detailed design and engineering stage (see also Section 2.3.2). First, it needs to be checked if differences between such a tool and the new method occur. If so - which is likely - the cause for these differences needs to be found. Based on this result, the level of confidence of the new method can be estimated, which completes the verification and validation.

- Explore options to apply the method for other problems where capabilities of different components and connections in a network are relevant. The new method has been developed for assessing the vulnerability of distributed systems on board ships. However, there are numerous other applications where components and connections in a network provide certain capabilities. The new method could potentially be useful to such other applications as well. Several opportunities have already been discussed in Chapter 6. Another example is fleet management, where individual ships provide specific capabilities. In a naval fleet, a submarine could for example provide intelligence, a frigate provides offensive power, and a replenishment vessel provides fuels and other resources. The performance of a fleet as a whole depends on the availability and status of individual ships. This situation is very similar to the distributed systems context for which the new method has been developed. As such, the method could potentially be interesting for this example as well. Applications may also be found beyond the scope of (naval) ship design. It should be kept in mind, however, that finding new problems for an existing solution is not a goal in itself, because these new problems may already have their own solutions. What matters, is whether the method can provide a useful contribution.

With respect to the design process for distributed systems:

- Develop an early stage method for capacity assessment of distributed systems. The updated work flow for early stage design of distributed systems has shown that a method for a capacity assessment is still lacking (see Section 5.2.2). However, if a network is connected, it does not necessarily mean that sufficient resources are available. As such, an early stage capacity assessment is a valuable contribution to the design process for distributed systems. This recommendation has previously been made by de Vos (2018), who mentions that additional knowledge on the load balance and decision-making for power division is required for this. These issues are still to be solved for completing the work flow.

- Enable computational integration of the new method with other vulnerability methods. In order to integrate the new method with other methods discussed in this dissertation (particularly in Chapter 5), computational compatibility is required. This can be established by e.g. uniform descriptions of variables and the physical solution, for example as a matrix, a graph, or a combination of both. This is mostly a practical matter related to tool development. It does not necessarily lead to better concepts, but it makes the design process faster and easier.

- Explore options to include operational doctrine in the design of distributed systems. Factors related to operational doctrine are usually not extensively included in the product-oriented process of ship design. Yet, they can influence the vulnerability, and other performance characteristics. For example, in case of a threat, the crew may position the ship in such a way that an incoming weapon is likely to hit the ship from a certain angle (M. van Diessen, personal communication, December 2019). This makes some compartments of the ship more likely to be hit than others. Though the new method allows for user-defined hit probabilities, this operational view on hit probabilities has not yet been included. Also for other methods this point of view could be used to improve the quality of the results. Other examples of operational aspects include priority-setting in which threats to encounter first (in case of multiple threats) and how to divide the remaining resources over the users after damage. The latter also relates to the first recommendation of this set.

With respect to ship design in general:

- Support non-digital knowledge transfer between designers. This research, along with various other ship design research efforts, has aimed to generate explicit, specific and re-usable design knowledge. Though such knowledge is indispensable for advancing the field of ship design, it has also been acknowledged that some of the design knowledge is contextual and personal, i.e. tacit knowledge. In order to transfer such knowledge, personal contact is needed, such as having contextual discussions or sharing design experiences. By definition, these are hard to capture and do not always lend themselves for formalisation in (ICT related) documents or procedures. As such, it is recommended to create and/or maintain an environment where transfer of such tacit knowledge is valued, encouraged, and facilitated. This could apply to both teaching environments, such as universities, as well as professional communities, companies, and organisations.

- Consider both scholarliness and usefulness in ship design research, while keeping in mind that the latter is eventually decisive. The problem-led nature of ship design research tends to be in tension with the method-led principle of other, more fundamental sciences such as mathematics or physics. Yet, ship design also relies on such sciences to succeed. Since the two are not necessarily mutually exclusive, it is recommended to combine both views in future research topics for ship design. This could mean that some findings may not instantaneously lead to better ships or better design procedures. Yet, the very nature of ship design - which is about designing real-world products for real-world problems - should make the aspect of usefulness superior over the aspect of scholarliness.

# References


Alavi, M. and Leidner, D. (1999). Knowledge Management Systems: Issues, Challenges, and Benefits. *Communications of the Association for Information Systems*, 1:1–28.

Andrews, D. (1981). Creative Ship Design. *Transactions of RINA*, 123:447–471.

Andrews, D. (2007). The Art and Science of Ship Design. *International Journal of Maritime Engineering*, 149(A1):1–14.

Andrews, D. (2011). Marine requirements elucidation and the nature of preliminary ship design. *International Journal of Maritime Engineering*, 153:A23–A39.

Andrews, D. (2018). The Sophistication of Early Stage Design for Complex Vessels. *International Journal of Maritime Engineering, Special Edition.*

Andrews, D., Duchateau, E.A.E., Gillespie, J.W., Hopman, J.J., Pawling, R.J. and Singer, D. (2012). State of the art report - Design for layout. *Proceedings of the 11th International Marine Design Conference (IMDC)*. Glasgow.

Andrews, D., Kana, A., Singer, D. and Romanoff, J. (2018). State of the art report on design methodology. *Proceedings of the 13th International Marine Design Conference*, pp. 3–16. Helsinki.

Arboleda, C., Abraham, D., Richard, J. and Lubitz, R. (2009). Vulnerability assessment of health care facilities during disaster events. *Journal of Infrastructure Systems*, 15(3):149–161.

Ball, R. and Calvano, C. (1994). Establishing the Fundamentals of a Surface Ship Survivability Design Discipline. *Naval Engineers Journal*, 106(1):71–74.

Bandecchi, M., Melton, B., Gardini, B. and Ongaro, F. (2000). The ESA/ESTEC Concurrent Design Facility. *Proceedings of EuSEC*, pp. 329–363. Munich.

BBC (2018). Helge Ingstad: Norway's warship collides with tanker in fjord. URL `https://www.bbc.com/news/world-europe-46136564`.

Bolton, M., Waterworth, S. and McClurg, R. (2018). Enabling, Equipping and Empowering the Support Enteprise through Digital Transformation. *Proceedings of the 14th International Naval Engineering Conference*, pp. 607–613. Glasgow.

Boulougouris, E. and Papanikolaou, A. (2004). Optimisation of the Survivability of Naval Ships by Genetic Algorithms. *Proceedings of COMPIT'04*. Siguenza.

Boulougouris, E., Winnie, S. and Papanikolaou, A. (2017). Assessment of Survivability of Surface Combatants after Damage in the Sea Environment. *Journal of Ship Production and Design*, 33(2):156–165.

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

Brouwer, R. (2008). A Framework for Systems Engineering in Ship Design from a NATO Specialist Team Perspective. *Engineering the Total Ship*. Falls Church, VA.

Brown, A. and Thomas, M. (1998). Reengineering the naval ship concept design process. *From research to reality in ship systems engineering symposium, ASNE*.

Brown, D. (1991). *The future British surface fleet*. Conway Maritime Press, London.

Calvano, C., Jons, O. and Keane, R. (2000). Systems Engineering in Naval Ship Design. *Naval Engineers Journal*, 112(4):45–57.

Chalfant, J. (2015). Early stage design for electric ship. *Proceedings of the IEEE*, 103(12):2252–2266.

Chalfant, J., Langland, B., Abdelwahed, S., Chryssostomidis, C., Dougal, R., Dubey, A., El Mezyani, T., Herbst, J., Kiehne, T., Ordonez, J., Pish, S., Srivastava, S. and Zivi, E. (2012). A collaborative early-stage ship design environment. *ESRDC 10th anniversary meeting*. Austin, TX.

Chalfant, J., Langland, B., Rigetrink, D., Sarles, C., McCauley, P., Woodward, D., Brown, A. and Ames, R. (2017). Smart Ship System Design (S3D) Integration with the Leading Edge Architecture for Prototyping Systems (LEAPS). *IEEE Electric Ship Technologies Symposium*. Arlington.

Clayton, D., Sudhoff, S. and Grater, G. (2000). Electric ship drive and power system. *Conference Record of the 2000 Twenty-fourth International Power Modulator Symposium*, pp. 85–88. Norfolk.

Cramer, A., Sudhoff, S. and Zivi, E. (2011). Performance Metrics for Electric Warship Integrated Engineering Plant Battle Damage Response. *IEEE Transactions on Aerospace and Electronic Systems*, 47(1):634–646.

Dekking, F., Kraaikamp, C., Lopuhaa, H. and Meester, L. (2005). *A Modern Introduction to Probability and Statistics - Understanding Why and How*. Springer, London.

DeNucci, T. (2012). *Capturing Design - Improving conceptual ship design through the capture of design rationale*. Ph.D. thesis, Delft University of Technology.

Doerry, N. (2006). Zonal Ship Design. *Naval Engineers Journal*, 118(1):39–53.

Doerry, N. (2007). Designing Electrical Power Systems for Survivability and Quality of Service. *Naval Engineers Journal*, (119):25–34.

Doerry, N. (2015). Naval Power Systems: Integrated power systems for the continuity of the electrical power supply. *IEEE Electrification Magazine*, pp. 12–21.

Dougal, R. and Langland, D. (2016). Catching it early - Modeling and simulating distributed systems in early stage design. *SNAME Marine Technology*, pp. 63–69.

Duchateau, E. (2016). *Interactive evolutionary concept exploration in preliminary ship design*. Ph.D. thesis, Delft University of Technology, Delft.

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

Edstrom, K. (2017). The role of CDIO in engineering education research: Combining usefulness and scholarliness. *European Journal of Engineering Education*.

El-Rashidy, R. and Grant-Muller, S. (2014). An assessment method for highway network vulnerability. *Journal of Transport Geography*, 34:34–43.

Elgot, J. (2016). British warships need multimillion-pound refit to stop power failures. URL `https://www.theguardian.com/uk-news/2016/jan/29/royal-navy-warships-multimillion-pound-refits-power-cuts`.

Erkel, A., Luyten, J. and Galle, L. (2002). TNO-PML developments of blast resistant doors and walls. *Proceedings of the RTO Applied Vehicle Technology Panel (AVT) Symposium*. Aalborg.

Evans, J. (1959). Basic Design Concepts. *Journal of the American Society for Naval Engineers*, 71(4):671–678.

Frické, M. (2019). The Knowledge Pyramid: the DIKW Hierarchy. *Knowledge Organization*, 46(1):33–46.

Gaspar, H. (2013). *Handling Aspects of Complexity in Conceptual Ship Design*. Ph.D. thesis, NTNU - Norwegian University of Science and Technology.

Geertsma, R. (2019). *Autonomous control for adaptive ships*. Ph.D. thesis, Delft University of Technology.

Gonsoulin, D. (2018). *Distributed Energy Management UtilizingModel Predictive Control for Naval Ship Applications*. Ph.D. thesis, Florida State University.

Goodfriend, D. and Brown, A. (2017). Exploration of System Vulnerability in Naval Ship Concept Design. *Journal of Ship Production and Design*, 33(3):1–17.

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

Goodrum, C., Taylordean, S. and Singer, D. (2018b). Understanding initial design spaces in set-based design using networks and information theory. *Proceedings of the 13th International Marine Design Conference*, pp. 385–394. Helsinki.

Gortney, W. (2010). Dictionary of Military and Associated Terms. United States Department of Defense as amended through February 2016. Technical report.

Habben Jansen, A., Duchateau, E., Kana, A. and Hopman, J. (2020a). Assessing complex failure scenarios of on-board distributed systems using a Markov chain. *Journal of Marine Engineering & Technology*, 19(sup1):45–61.

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

Habben Jansen, A., Kana, A. and Hopman, J. (2019). A Markov-based vulnerability assessment for the design of on-board distributed systems in the concept phase. *Ocean Engineering*, 190.

Habben Jansen, A., de Vos, P., Duchateau, E., Stapersma, D., Hopman, J., van Oers, B. and Kana, A. (2020b). A Framework for Vulnerability Reduction in Early Stage Design of Naval Ship Systems (in press). *Naval Engineers Journal*.

Heywood, M. and Lear, T. (2006). PREVENT  A tool to reduce vulnerability early in the design. *Proceedings of Warship 2006*. London.

Janssen, J., Butler, J., Worthington, P., Geertsma, F. and den Hartog, M. (2016). Autonomous, adaptive, aware: DINCS. *Proceedings of the 13th International Naval Engineering Conference*. Bristol.

Jaspers, T. (2017). *Elucidating families of ship designs using clustering algorithms*. MSc thesis, Delft University of Technology.

Jung, H.C. (2019). Research of Power and Propulsion System Using Improved Gas-Turbine for DDG-51 Flight III. *Naval Engineers Journal*, 131(1):125–131.

Jung, J., Liu, C., Tanimoto, S. and Vittal, V. (2002). Adaptation in Load Shedding Under Vulnerable Operating Conditions. *IEEE Transactions on Power Systems*, 17(4):1199–1205.

Kana, A. and Harrison, B. (2017). A Monte Carlo approach to the ship-centric Markov decision process for analyzing decisions over converting a containership to LNG power. *Ocean Engineering*, 130:40–48.

Kana, A., Shields, C. and Singer, D. (2016). Why is naval design decision-making so difficult? *Warship*. Bath.

Kim, K. and Lee, J.H. (2012). Simplified vulnerability assessment procedure for a warship based on the vulnerable area approach. *Journal of Mechanical Science and Technology*, 26(7):2171–2181.

Koskela, L. (2007). Concurrent Engineering in Constructing Projects. C. Anumba, J. Kamara and A.F. Cutting-Decelle (Editors), *Foundations of Concurrent Engineering*, pp. 12–29. Taylor & Francis Group, 1st edition.

Kossiakoff, A., Sweet, W., Seymour, S. and Biember, S. (2011). *Systems Engineering Principles and Practice*. Wiley, Hoboken, New Jersey, 2nd edition.

Koufteros, X., Vonderembse, M. and Doll, W. (2001). Concurrent Engineering and its consequences. *Journal of Operations Management*, 19(1):97–115.

Lay, D. (2006). *Linear Algebra and Its Applications*. Pearson Education, Boston, 3rd edition.

Liu, C., Xu, Q., Chen, Z. and Leth Bak, C. (2012). Vulnerability Evaluation of Power System Integrated with Large-scale Distributed Generation Based on Complex Network Theory. *Proceedings of the 47th international Universities Power Engineering Conference (UPEC)*. Uxbridge.

Liwang, H. and Jonsson, H. (2015). Comparison between different survivability measures on a generic frigate. *International Journal of Maritime Engineering*, 157(A2):125–134.

Logan, K. (2007). Intelligent Diagnostic Requirements of Future All-Electric Ship Integrated Power System. *IEEE Transactions on Industry Applications*, 43(1):139–149.

Marineschepen.nl (2012). Vuurgevecht Hr.Ms. Rotterdam met piraten. URL `https://marineschepen.nl/nieuws/Vuurgevecht-Rotterdam-met-piraten.html`.

Mark, J. (2018). The Hittites. URL `https://www.ancient.eu/hittite/`.

Mavris, D. and DeLaurentis, D. (2000). Methodology for examining the siultaneous impact of requirements, vehicle characteristics, and technologies on military aircraft design. *Proceedings of the 22nd Congress of the International Council on Aearonautical Sciences (ICAS)*, pp. 145.1–145.10.

Menis, R., da Rin, A., Vicenzutti, A. and 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*. IEEE, Bologna.

van Meurs, R. (2019). Integrating Vulnerability in Ship Design - TNO Resilient Ship Design course notes.

van Mieghem, P. (2014). *Performance Analysis of Complex Networks and Systems*. Cambridge University Press, Cambridge.

Ministerie van Defensie (2018). Marine bereidt zich voor op gevecht tot in hoogste geweldsspectrum. URL `https://www.defensie.nl/actueel/nieuws/2018/04/24/marine-bereidt-zich-voor-op-gevecht-tot-in-hoogste-geweldspectrum`.

Ministerie van Defensie (2019). Joint logistic Support Ship (JSS). URL https://www.defensie.nl/onderwerpen/materieel/schepen/joint-logistic-support-ship-jss.

Mooren, M. (2018). *A Markov chain based study on the availability of ship systems of a naval vessel*. MSc thesis, Delft University of Technology.

NATO Naval Group 6 on Ship Design (2004). Working paper on small ship design.

Nederlandse Omroep Stichting (2015). Verstekelingen op Nederlands ebolahulpschip. URL https://nos.nl/artikel/2014342-verstekelingen-op-nederlands-ebolahulpschip.html.

Nederlandse Omroep Stichting (2016). Nederlands fregat redt bootvluchtelingen. URL https://nos.nl/artikel/2111217-nederlands-fregat-redt-bootvluchtelingen.html.

Niese, N., Kana, A. and Singer, D. (2015). Ship design evaluation subject to carbon emission policymaking using a Markov decision process framework. *Ocean Engineering*, 106:371–385.

van Oers, B. (2011). *A packing approach for the early stage design of service vessels*. Ph.D. thesis, Delft University of Technology.

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

van Oers, B., Takken, E., Duchateau, E., Zandstra, R., Cieraad, S., van den Broek - de Bruijn, W. and Janssen, M. (2018). Warship Concept Exploration and Definition at The Netherlands Defence Materiel Organisation. *Naval Engineers Journal*, 130(2):61–82.

Ostergard, T., Jensen, R. and Maagaard, S. (2016). Building simulations supporting decision making in early design  A review. *Renewable and Sustainable Energy Reviews*, 61:187–201.

Papanikolaou, A. (2010). Holistic ship design optimization. *Computer-Aided Design*, 42:1028–1044.

Parsons, M. (2004). Parametric Design. *Ship Design and Construction vol. 1*, chapter 11. SNAME.

Parsons, M., Robinson, K., Kara, M., Stinson, N., Snyder, D., Woodward, D. and Brown, A. (2019). Application of a Distributed System Architecture Framework to Naval Ship Concept and Requirements Exploration (C&RE). *Proceedings of the Intelligent Ships Symposium*. Philadelphia.

Pawling, R., Percival, V. and Andrews, D. (2017). A Study into the Validity of the Ship Design Spiral in Early Stage Ship Design. *Journal of Ship Production and Design*, 33(2):81–100.

Pedersen, K., Emblemsvag, J., Bailey, R., Allen, J. and Mistree, F. (2000). Validating design methods & research: the validation square. *Proceedings of DETC 00*. Maryland.

Pei, Y., Song, B. and Han, Q. (2006). A Generic Calculation Model for Aircraft Single-hit Vulnerability Assessment Based on Equivalent Target. *Chinese journal of aeronautics*, 19(3):183–189.

Piperakis, A. (2013). *An Integrated Approach to Naval Ship Survivability in Preliminary Ship Design*. Ph.D. thesis, University College London.

Piperakis, A. and Andrews, D. (2012). A comprehensive approach to survivability assessment in naval ship design. *International Journal of Maritime Engineering*, 156:333–352.

Pruijn, J. (2020). Using Markov Processes to Investigate Dry Bulk Port Congestion. *Maritime Supply Chains*, chapter 5. Elsevier, 1st edition.

Raptodimos, Y. and Lazakis, I. (2019). Application of NARX neural network for predicting marine engine performance parameters. *Ships and Offshore Structures*.

Reese, R., Calvano, C. and Hopkins, T. (1998). Operationally Oriented Vulnerabiliity Requirements in the Ship Design Process. *Naval Engineers Journal*, 110(1):19–34.

Renzi, C., Leali, F. and Di Angelo, L. (2017). A review on decision-making methods inengineering design for the automotive industry. *Journal of Engineering Design*, 28(2):118–143.

Rinaldi, S. (2004). Modeling and simulating critical infrastructures and their interdependencies. *Proceedings of the 37th Conference on System Sciences*. Hawaii.

Roberts, N. (2000). Wicked problems and network approaches to resolution. *International Public Management Review*, 1(1):1–19.

Rowley, J. (2007). The wisdom hierarchy: representations of the DIKW hierarchy. *Journal of Information Science*, 33(2):163–180.

Ruths, J. and Ruths, D. (2013). Robustness of Network Controllability under Edge Removal. *Complex Networks IV - Proceedings of the 4th Workshop on Complex Networks CompleNet 2013*, pp. 185–193. Berlin.

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

Schleijpen, R. (2010). Toolset for evaluating infrared countermeasures and signature reduction for ships. *Proceedings of SPIE 7836, Technologies for Optical Countermeasures VII*. Toulouse.

Schofield, J. (2009). SURVIVE and SURVIVE Lite - survivability assessment from concept to operational support. *Proceedings of the American Society of Naval Engineers Day*. Maryland.

Schuddebeurs, J. (2014). *De-risking Integrated Full Electric Propulsion (IFEP) vessels using advanced modelling and simulation techniques*. Ph.D. thesis, University of Strathclyde.

Schulte, J. (1994). *An analysis of the historical effectiveness of anti-ship cruise missiles in littoral warfare*. MSc thesis, Naval Postgraduate School.

Shields, C. (2017). *Investigating Emergent Design Failures Using a Knowledge-Action-Decision Framework*. Ph.D. thesis, University of Michigan.

Shields, C., Sypniewski, M. and Singer, D. (2016). Understanding the relationship between naval product complexity and on-board system survivability using network routing and design ensemble analysis. *Proceedings of PRADS2016*. Copenhagen.

Singer, D. and Doerry, N. (2009). What is Set-Based Design? *Naval Engineers Journal*, 121(4):31–43.

Strom, M., Rehn, C., Pettersen, S., Erikstad, S., Asbjornslett, B. and Brett, P. (2018). Combining Design and Strategy in Offshore Shipping. *Proceedings of the 13th International Marine Design Conference*. Helsinki.

Surma Ltd. (2018). SURMA survivability analysis. URL `http://survivability.fi/surma/demo/`.

TNO (2018). RESIST Lite. URL `https://www.tno.nl/media/1644/resist_lite.pdf`.

TNO (2019). Geïntegreerde Energiesystemen (GES). URL `https://www.tno.nl/media/8083/geïntegreerde_energiesystemen_ges.pdf`.

Trapp, T. (2015). *Shipboard Integrated Engineering Plant Survivable Network Optimization*. Ph.D. thesis, Massachusetts Institute of Technology.

United Nations Security Council (2010). Letter dated 4 June 2010 from the Permanent Representative of the Republic of Korea to the United Nations addressed to the President of the Security Council.

Vicenzutti, A., Bucci, V., Sulligoi, G. and Pelaschiar, R. (2016). Impact of Safe Return to Port rules on passenger ships power systems design. *2016 AEIT International Annual Conference (AEIT)*, pp. 1–7. Capri.

de Vos, P. (2018). *On early-stage design of vital distribution systems on board ships*. Ph.D. thesis, Delft University of Technology.

de Vos, P. and Stapersma, D. (2018). Automatic topology generation for early design of on-board energy distribution systems. *Ocean Engineering*, 170:55–73.

de Vos, P., Stapersma, D., Duchateau, E. and 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)*, pp. 463–481. Pavone.

Walsham, G. (2001). Knowledge Management: the Benefits and Limitations of Computer Systems. *European Management Journal*, 19(6):599–608.

Weinberger, D. (2010). The Problem with the Data-In-formation-Knowledge-Wisdom Hierarchy. URL `https://hbr.org/2010/02/data-is-to-info-as-info-is-not`.

Wilson, B. (2010). Responding to Asymmetric Threats in the Maritime Domain: Diplomacy, Law and Naval Operations. *Maritime Affairs: Journal of the National Maritime Foundation of India*, 5(2):68–85.

# Acknowledgements

After four years of research work, I am proud to present you my dissertation. By definition a dissertation is a product of one person. Nevertheless, I could never have come to this point without the help of numerous other people, to whom I am greatly indebted, and to whom I would like to express my sincere gratitude.

First and foremost, I would like to thank the United States Office of Naval Research, and Ms. Kelly Cooper in particular, for making my PhD project financially possible through a NICOP research grant. Many thanks also go to my colleagues - both PhD candidates and senior scientific staff - from our fellow universities in the NICOP project: University of Michigan, Virginia Polytechnic Institute and State University, and University College London. It was wonderful to discuss our work, to share ideas, and to philosophise about (future) naval ship design. Thank you for your hospitality in hosting our meetings, and for the great times we have had at various conferences.

Many thanks go to my supervisors: professor Hopman and Austin Kana. Professor Hopman, thank you for your trust in me as a PhD candidate, and for your advice throughout the various stages of my PhD project. Austin, you have been truly important to me as daily supervisor. Thank you for all the (long) time you have devoted to me and my work. I feel very fortunate to have had such a committed supervisor. Many thanks also go to the members of the doctoral committee, who have carefully read this dissertation.

My colleagues from the Delft University of Technology have made a significant contribution to my PhD project with listening ears and constructive conversations. Thank you for sharing your time during work, during breaks, and during all kinds of (social) events. Koen, it was you, above all, with whom I have shared the office almost every single day. I am highly grateful for the good times we have had, in all respects, and whatever the circumstances were. It made all the difference. Joan, it was great to share the office with you as well. I am sure your PhD project will be a successful one. Good luck! Peter, our discussions on distributed systems have been highly helpful and clarifying to me, thank you! As for Erik Ulijn: thanks for all our long coffee and tea breaks, during which we could ventilate our thoughts and discuss miscellaneous topics. If those discussions had ever been recorded, I am sure some of the world's problems would have been solved by now. To Erik Rotteveel: thank you for your cordiality and good advice during the first stage of my PhD, which have really encouraged me. Of course, students play a large role in university life as well. Special thanks go to

Maurice, whom I have supervised with his MSc graduation project. Thank you for being patient with me while I was trying to find out what to do just as much as you did. I hope you look back on your graduation project with pleasure and some pride.

I have had a great time with my colleagues of the Bureau of Life Cycle Management of the Maritime Systems Division of the Defence Materiel Organisation. Thank you for offering me a second work place and many interesting conversations on practical issues with respect to designing and operating naval ships. I particularly remember our team activity in June 2019, where I learned that asking "What could possibly go wrong?" indicates limited understanding of susceptibility, not only in a naval context, but also for canoeing with colleagues. I am very grateful to all of you, but Etienne, I would like to address you specifically. What you have meant to me and my work has been truly invaluable. I could never do that full justice within these few sentences, but I know you will understand.

There are many people who have not directly contributed to this dissertation, but who have offered many indispensable moments of leisure time and distraction from my work. Many thanks go to my fellow musicians of the Koninklijke Harmoniekapel Delft (Royal Delft Wind Orchestra). It was not uncommon that only five minutes of playing with you at our weekly rehearsals were sufficient to let go of a full week of work-induced worries. I have often misused our after-rehearsal drinks and other occasions for bothering some of you (especially Wouter, sorry!) with endless PhD stories; thank you for bearing with me.

I have received a great deal of joy from my friends from Delft: Roderik, Sietske, Marja, Rob, and Thomas. I vividly remember our trips to Zeeland, Corsica, the Ardennes, Texel, and many more destinations. Thank you for our nice activities (120 kilometres of cycling in Limburg's hills is just too intense for me), good conversations (in French, Sietske?), and 30 Seconds games (where Rolls Royce was not a luxury car brand, but a manufacturer of gas turbines). I am looking forward to sharing many more moments together with you.

To my parents, my brothers, my sister, my grandparents, and my family-in-law: thank you for encouraging me ceaselessly. Home will always be home, and the fact that you are there, has been and will continue to be of great support to me in all respects.

Finally, but undisputedly most important, I would like to thank Maarten. Thank you for your love, your patience and your support during the past years. I am so grateful for having you at my side, and I look forward to continuing our journey and adventures together forevermore.

# Curriculum Vitae

Agnieta Habben Jansen was born on July 18, 1993 in Alphen aan den Rijn, The Netherlands. After completing her pre-university education at CSG Groene Hart in Alphen aan den Rijn in 2010, she started her BSc education in Marine Technology at the Delft University of Technology. She obtained her BSc degree in 2014, after which she continued her education in Marine Technology with an MSc programme at the same university. She specialised in ship hydromechanics, obtaining her MSc degree in 2016 with her graduation project on the influence of the bow shape of inland ships on the resistance. This graduation project was conducted in collaboration with Damen Shipyards and MARIN.

After obtaining her MSc degree, Agnieta commenced her PhD research on vulnerability reduction of distributed ship systems at the Delft University of Technology. This research was carried out in collaboration with the Office of Naval Research of the United States Navy and the Defence Materiel Organisation of the Netherlands Ministry of Defence. For her research she received the Sir Donald Gosling Award in 2018, and she was nominated for the Maritime Designer Award in 2019. In addition to her research work, she was involved in teaching the MSc course *Design of Complex Specials*, and she supervised an MSc student with his graduation project.

# Publications

## Journal publications

1. **Habben Jansen, A.C.**, de Vos, P., Duchateau, E.A.E., Stapersma, D., Hopman, J.J., van Oers, B.J., Kana, A.A. (2020). A Framework for Vulnerability Reduction in Early Stage Design of Naval Ship Systems (in press). *Naval Engineers Journal*.

2. **Habben Jansen, A.C.**, 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 & Technology*, 19(sup1):45-61.

3. **Habben Jansen, A.C.**, Kana, A.A., Hopman, J.J. (2019). A Markov-based vulnerability assessment for the design of on-board distributed systems in the concept phase. *Ocean Engineering*, 190, 106448.

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

## Conference publications

1. **Habben Jansen, A.C.**, de Vos, P., Duchateau, E.A.E., Stapersma, D., Hopman, J.J., van Oers, B.J., Kana, A.A. (2019). A Framework for Vulnerability Reduction in Early Stage Design of Naval Ship Systems. In *Proceedings of the Intelligent Ships Symposium*. Philadelphia.

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

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

# Magazine publications

1. **Habben Jansen, A.C.** (2019, January). Designing Survivable Naval Ships. *SWZ Maritime*, 17-19.