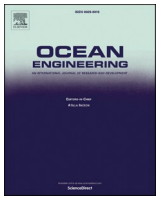
Ocean Engineering 225 (2021) 108731

Contents lists available at ScienceDirect

Ocean Engineering

journal homepage: www.elsevier.com/locate/oceaneng



A multilayer network approach to vulnerability assessment for early-stage naval ship design programs

Luke C. Brownlow [a,*], Conner J. Goodrum [b], Michael J. Sypniewski [b], James A. Coller [a], David J. Singer [a]

[a] University of Michigan, Department of Naval Architecture and Marine Engineering, Ann Arbor, MI, USA
[b] Navatek LLC, Ann Arbor, MI, USA

ARTICLE INFO

Keywords:
Network theory
Vulnerability
Ship design
Early-stage design
Naval engineering
Survivability

ABSTRACT

Vulnerability is a crucial facet of a naval ship's operational capability in a hostile environment. Naval combatants are among the most complex and densely packed distributed systems created today. These shipboard distributed systems are defined by their layout and componentry. Vulnerability assessments of these systems are therefore derived from failures of the integrated componentry layout due to hostile weapon impacts. In late-stage design programs, these vulnerability assessments are accomplished via detailed modeling and computationally expensive simulation. During early-stage design, this level of detailed modeling is unavailable, but integrated system failure analysis remains essential for thorough vulnerability assessment. The authors resolve this issue by utilizing an adaptable network-based approach to reduce the design fidelity needed for modeling and simulation. The approach allows for the development of a novel vulnerability assessment method for early-stage design. The approach is demonstrated through a representative naval case study.

1. Introduction

Vulnerability is a naval ship's hit tolerance or hardness – the ability to withstand the impact of a hostile weapon (Ball, 2003; Goodfriend, 2015). Lower vulnerability for naval ships means increased mission efficacy, capability, and crew safety. Vulnerability assessments analyze the architectural weaknesses in a ship's design due to a hostile weapon impact. These assessments are part of the greater survivability analysis consisting of susceptibility, vulnerability, and recoverability. Identifying critical weaknesses in a design provides indispensable information to design program decision makers and operators.

In many engineering disciplines, the first products off the assembly line can be destructively tested for vulnerabilities, but large-capital naval programs do not have this luxury, as the first product (ship) must perform. Instead, naval vulnerability assessments turn to physics-based models and knowledge of weapon envelopes — the volumetric area of a weapon's blast and damage radius. Through probabilistic modeling and simulation of weapon impacts, an assessment can be conducted (Ball, 2003).

1.1. Challenges of current vulnerability assessments

Vulnerability studies are historically executed late in the naval design process after the major design characteristics have been determined, since they require extensive modeling and probabilistic simulation. Jansen et al. (2019) provide a discussion of high fidelity vulnerability assessment tools for late-stage design and highlight the need for early-stage design stage tools. These computationally expensive simulations provide excellent results but require a detailed knowledge of the ship design. This need for detailed design severely limits traditional vulnerability assessments' ability to explore the unsolidified early-stage design space. They are similarly challenged in comparing multiple design variants due to the amount of modeling and computational expense.

Traditional vulnerability studies provide valuable information, but often so late in the design stage that architectural fixes are inefficient and extremely expensive (Molland, 2008). The exponential relationship between stages in a design program and the cost to alter the design is illustrated in Fig. 1 (McKenny, 2013). Ideally, vulnerability should be integrated into early-stage design in order to produce more effective naval ships.

* Corresponding author.
E-mail address: brownlow@umich.edu (L.C. Brownlow).

https://doi.org/10.1016/j.oceaneng.2021.108731
Received 24 August 2020; Received in revised form 7 January 2021; Accepted 7 February 2021
Available online 28 February 2021

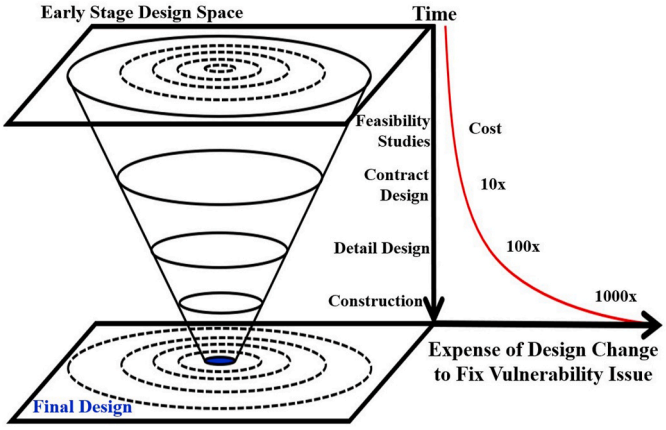


Fig. 1. A depiction of the design space narrowing throughout the ship's design program and its relationship to exponential increase in cost to change the design. The cost increase relationship is derived from McKinney (2013).

As Navy Postgraduate Professor Robert E. Ball states in his textbook on survivability analysis and design:

'Vulnerability reduction is most effectively accomplished early in the design. . . when component sizes, locations, materials, construction, and redundancies are being studied and selected' (Ball, 2003).

Late-stage vulnerability reductions are not only inefficient, but also extremely costly when changing ship architecture. This expense relationship results in decision makers having to weigh program budget concerns against detrimental vulnerability shortcomings. In order to minimize these vulnerability pitfalls, decision makers need to be informed of the vulnerability implications of their design decisions as early as possible in the design program. The earlier vulnerability issues are identified in a ship program, the easier it is to deliver a more economical, less vulnerable ship.

As a design program progresses, its increasing cost pressure incentivizes decision makers to prefer insufficient add-on vulnerability reduction features, as opposed to architectural changes that fix vulnerable design issues. While sometimes unavoidable, these add-on vulnerability reduction features often increase weight and cost (e.g. ballistic panels to shield vulnerable components) and are not as effective as eliminating the vulnerability issue completely (e.g. relocation of vulnerable components). A method of conducting an efficient vulnerability assessment during early-stage design is needed to properly address the vulnerability implications of architectural decisions.

1.2. Objectives

Effective early-stage vulnerability reduction requires an early-stage vulnerability assessment. The research presented in this paper provides a novel vulnerability assessment method for ship design managers by analyzing the architectural systems they are considering in the early-stage design space. The following three objectives for such a vulnerability assessment have been identified as necessary to effectively integrate into the early stage design phase and to provide meaningful information to naval decision makers:

1) Identify leading indicators for vulnerability issues arising from implications of architectural decisions. The physical system, logical system, and combined integrated system architectures should be evaluated.
2) Compare the vulnerabilities of competing design variants in the early-stage design space.
3) Adapt and assess rapid design modifications inherent in proper exploration of the early stage design space.

All three of these objectives are required to better inform decision makers earlier in the ship design program and form the motivation for this research.

Network theory will be used to create a framework for this vulnerability assessment of the design space in order to meet the three objectives. Network theory provides a flexible approach that is adaptable to the information gradient of the knowledge space without the need for a traditional vulnerability assessment's detailed modeling and simulation. It additionally allows for quick re-routing, substitution, and elimination of components and their connections in naval design (Rigterink, 2014; Goodrum et al., 2018).

A novel four-layer network framework for vulnerability assessments is created and demonstrated in this paper. The framework allows for identification of leading indicators for vulnerability issues early in the design process. This allows for proactive low vulnerability design influence instead of reactive vulnerability reduction techniques on a near-complete ship design. A case study utilizing the four-layer network framework is presented on the integration of a cargo elevator system for a representative T-AKE class ship arrangement.

1.3. Not a replacement for traditional methods

The need for a vulnerability assessment method that can efficiently assess designs during conceptual design has been previously identified and several approaches proposed in recent years. These approaches have included but are not limited to genetic optimization (Parsons 2019, Goodfriend and Brown 2017), Markov chains (Jansen 2019), and network science relationship frameworks (Goodrum et al., 2018; Shields, 2017a,b). Focus on naval distributed system design and assessment has further been explored over the past decade with the rise in demand on ship power systems (Doerry 2007; Chalfant 2015; Brefort et al., 2018).

The work presented here builds on the network science approach by providing a novel framework to assess the interdependencies of the logical architecture of a ship with that of the physical system within the realm of vulnerability.

The network framework and case-study implementation strategy presented are not meant to replace the later-stage vulnerability assessments based on computer models of detailed design. A discussion of these more traditional vulnerability assessment models and tools can be found in Stevens (2016) where it is noted that all these methods are designed to be used later in the design process than conceptual design. Those intensive vulnerability assessments provide important insights that are not attempted to be replaced by a network implementation. Instead, this research is meant to help bridge the gap between early-stage naval design and vulnerability analysis in order to better inform decision makers and procure more effective, more dependable naval ships.

2. Vulnerability programs and implementation

The vulnerability of a ship is directly derived from the architectural layout of its vital components (Piperakis, 2013). The ship's componentry and architectural layout make up the ship's distributed service systems (Brefort et al., 2018). As described by Goodrum et al. (2018):

'… the overall architecture of distributed ship service systems can be discussed in terms of physical architecture, logical architecture, and operational architecture'.[1]

The physical architecture is the spatial relationship in the general arrangements of the ship. The logical architecture is the relationship between vital components that generates system functionality. The operational architecture is the use of distributed systems over time. Vulnerability focuses on the physical and logical systems; this research will therefore also focus on the interconnectivity of the physical and logical systems. In order to account for both systems' architecture, a vulnerability program should therefore accomplish three tasks (Ball, 2003):

1) Identify the vital components and their kill modes.
2) Assess the vulnerability.
3) Reduce the vulnerability of the ship through feedback to the designers

A reactive vulnerability program will analyze a ship design when it is close to completion and then recommend vulnerability reduction features. A proactive vulnerability program will analyze a ship design early and continuously throughout the design program. The proactive program cycles feedback from leading indicators that the vulnerability assessment provides back to the architectural designers of the ship's distributed systems. The designers can then make informed revisions regarding the vulnerability implications of their architectural layouts and logic. Traditional vulnerability programs are heavily reactive due to their assessments requiring large amounts of precise information for complex modeling and simulations.

2.1. Identification of vital components and kill modes

Vital components are the critical parts required for a system to properly function. Kill modes are the ways in which the system fails due to damage or failure of one or more vital components in the system (Ball, 2003). In order to conduct the vulnerability assessment, it is imperative to know what types of componentry damage will result in a kill mode.

Naval ship kill modes are either related to a mission capability or a navigational capability. A mission kill mode results in a ship no longer being able to accomplish a critical mission mode (e.g. a weapon system failure). A navigational kill mode results in a loss of steering or propulsion. These two types of kill modes are not exclusive, as most navigational kill modes also result in a mission kill mode.

2.2. Naval vulnerability assessment

Probabilistic simulation of weapon effects on a computer model of the ship design results in vulnerability metrics. The metric commonly used in quantifying a design's vulnerability is the probability of kill upon hit, often denoted in literature as P_k (Farris and Stuckey, 2000; Ball, 2003). This metric is typically calculated via probabilistic shotlines and evaluation of a design's kill modes (Smith, 2010). Once an assessment calculates the vulnerability metrics, the results can be used to determine a down-selection of competing design variants, help inform the policy of operational leadership, or revise the design. Design revisions can either alter the architecture or add a vulnerability reduction feature. Revision of the design allows for vulnerability reduction through iterative vulnerability assessments, which is best conducted early. This is illustrated in Fig. 2.

2.3. Vulnerability reduction

There are two methodologies for reducing the vulnerability of naval design. The first and most effective method is through an architectural change in the design of the system. This option allows for re-location of compartments and vital components, which results in better placement and separation of redundant components. Unfortunately, architectural changes are often not possible due to the cost of delaying and redesigning part of the ship. For this reason, architectural design changes should be done during early-stage design when redesign is possible.

The second methodology for vulnerability reduction is adding a vulnerability reduction feature. These methods provide smaller reductions than architectural changes, but do not delay the design production. An example addition is ballistic paneling. Ballistic paneling helps protect vital componentry within a compartment from weapon fragments, but also adds significant weight to the ship design. A more effective approach is to move the vulnerable componentry away from the vulnerable area through an architectural change during early-stage design.

2.3. Vulnerability assessment implementation

Traditional vulnerability assessments are limited in being able to provide the vulnerability reduction options during early-stage design, but network-based assessment reduces the design detail needed for analysis. A network-based vulnerability assessment can make use of an iterative approach based on leading indicators derived from analysis of the network with an example implementation strategy, as seen in Fig. 3. This vulnerability information feedback loop allows design decision makers to make vulnerability-conscious decisions earlier in the design process. The metrics and constants shown in Fig. 3 are developed in Section 3 of this paper.

3. Vulnerability assessment via networks

Networks allow for the reduction of the design detail needed to

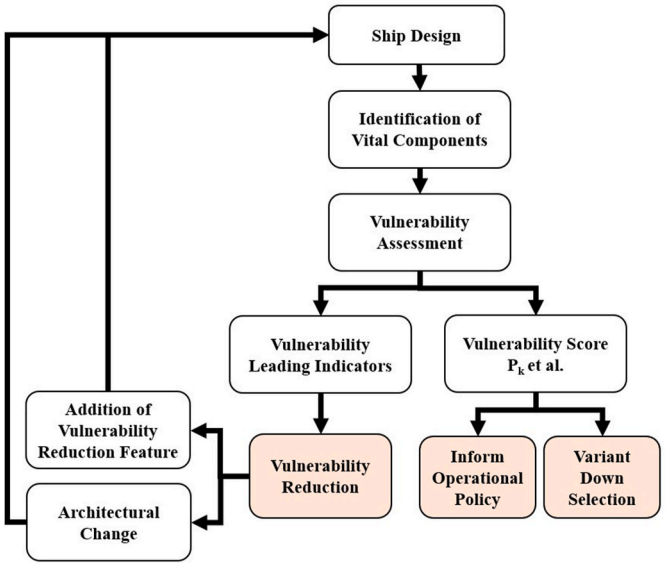


Fig. 2. A vulnerability program and the products of a vulnerability assessment. The highlighted boxes are the three types of actions that can be taken after analysis of a vulnerability assessment. Note the ability to do an iterative vulnerability reduction loop via leading indicators before moving a design along in the total ship design program.

[1] This description reflects the findings of an ongoing research program on the design of naval distributed systems. Research collaborators include students, researchers, and faculty at The University of Michigan, Virginia Polytechnic Institute and State University, The University College London, and Delft University of Technology. This program is supported by U.S. Office of Naval Research, Grant No. N00014-15-1-2752.

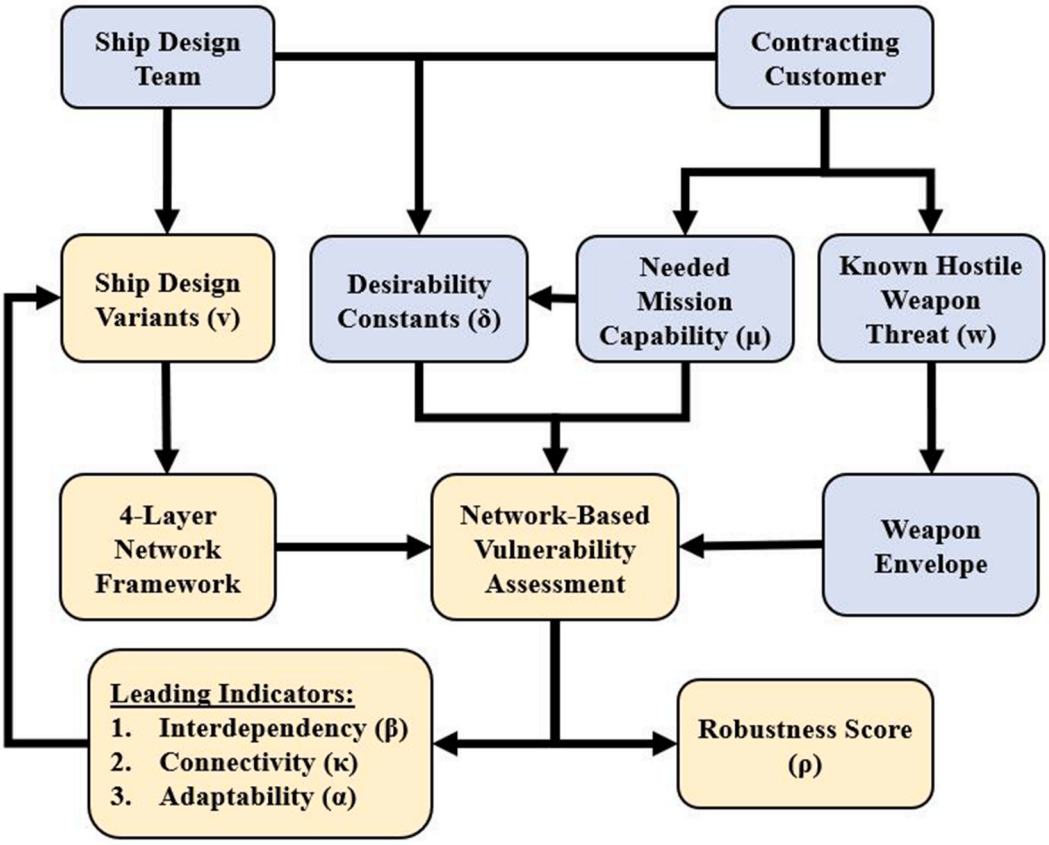


Fig. 3. The knowledge flow of a network-based vulnerability assessment. A box points to what it determines and from what it is derived. The lighter shaded boxes represent the iterative loop of vulnerability information up the decision ladder to influence new ship design variants based on the vulnerability leading indicators of the previous design cycle. See Fig. 2 for a closer look at the vulnerability assessment portion.

perform analysis on the architectural systems of a naval ship. Network theory stems from mathematical graph theory and has been widely applied to the sciences and engineering. Networks have more recently been applied to ship design as a tool for modeling and examining naval design spaces through information duals and shipboard distributed systems (Chalfant et al., 2017; Shields et al., 2015; Rigterink, 2014; Goodrum et al., 2018). For a detailed presentation of network theory, the reader is encouraged to consult the references of Newman (2018) and Barabási (2016). For an explicit mathematical representation of multi-layer networks, refer to the reference De Domenico et al. (De Domenico et al., 2013).

Networks are made up of nodes, which are the entities being modeled, and edges, which are the relationships between the nodes. Two nodes that have a relationship are then said to be linked by an edge. The addition or deletion of an edge or node is instantaneous, which makes networks adept at examining a changing, complex design space. A network containing multiple types of nodes can be broken into multi-layer networks, where each layer contains one type of node. The level of detail modeled is up to the designer, but clear rules for creating edges between nodes is essential to provide an accurate representation of the system being modeled.

3.1. Multilayer network approach

A multilayer network was selected to allow for evaluation of both the coupled and decoupled physical and logical systems on a ship. A four-layer network is utilized and divided into two node layers for the physical system (Openings and Compartments) and two layers for the logical system (Vital Components and Functional Links), as seen in Fig. 4. The four layers are:

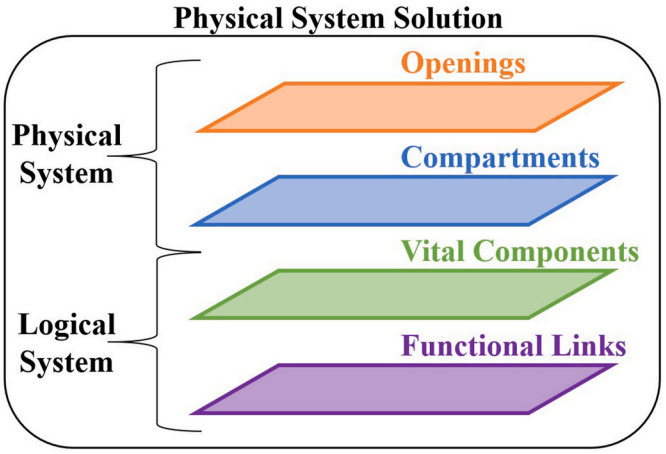


Fig. 4. A depiction of the four-layer network framework created for vulnerability assessments. The four layers together represent the Physical System Solution (Goodrum et al., 2018).

1) Openings Layer

Contains nodes that represent physical openings between compartments (e.g. doors, hatches).

2) Compartments Layer

Contains nodes that represent physical compartments (e.g. bridge,

stairway, ballast tank).

3) Vital Components Layer

Contains nodes that represent vital components of a logical system (e.g. generator, control panel, pipe).

4) Functional Links Layer

Contains nodes that represent the functional links between vital components (e.g. rotate, transmit).

This four-layer framework allows for separation and integration between the physical and logical architectures. While nodes exist on each layer, edges connect physical or logical relationships between nodes. An example of mapping the physical and logical systems' relationships is depicted in Fig. 5.

The framework's integrated, yet separated, organization allows for assessments to be executed on an individual system as well as on integrated systems. The integration of the physical and logical systems creates the Physical System Solution (Goodrum et al., 2018).

An important, flexible advantage of modeling a ship with this four-layer network framework is that even with vastly different physical architecture between multiple variants, there are common reusable nodes for modeling. For example, only one node needs to be created for a ship's galley even if the competing design variants are a monohull and trimaran. This galley node can be reused time and time again throughout the design program and only have its edges changed for analysis. The efficient reuse of nodes is also true for a logical system's vital components, as often only the relationship changes between design variants, not their entire componentry. This level of modeling adaptability is unattainable in a CAD model, where new models must be built for each variant.

3.2. Modeling damage/failure in the network

In order to evaluate the architectural implications due to damage cases, nodes are removed. Nodes can be removed one at a time or in groups to simulate different types of damage or failure. Each layer's type of node results in the removal of a subset of the nodes and edges in the four-layer network. Like in classical network theory, when a node is removed from a network, all edges associated with that node are also removed. This allows for quick simulation of damage to the ship design without the need for probabilistic shotlines and intensive computer modeling simulations.

Let the following sets of nodes be defined as O the openings, C the compartments, V the vital components, and F the functional links. Let ψ_0 represent the original set without removed nodes, as shown in (1), and ψ be the new set of nodes post damage.

$$\Psi_0 = O \cup C \cup V \cup F \tag{1}$$

Let the subscript d denote the set of damaged nodes of the type that the subscript is acting on. (e.g. C_d = set of compartment nodes damaged). The removal logic thus follows the following four rules using set notation:

1) Failure of an *opening*.

Remove opening node from network, as seen in (2).

$$\Psi = \Psi_0 \not\ni C_d \tag{2}$$

2) Failure of a *compartment*.

Remove compartment and remove vital components within compartment from network, as seen in (3).

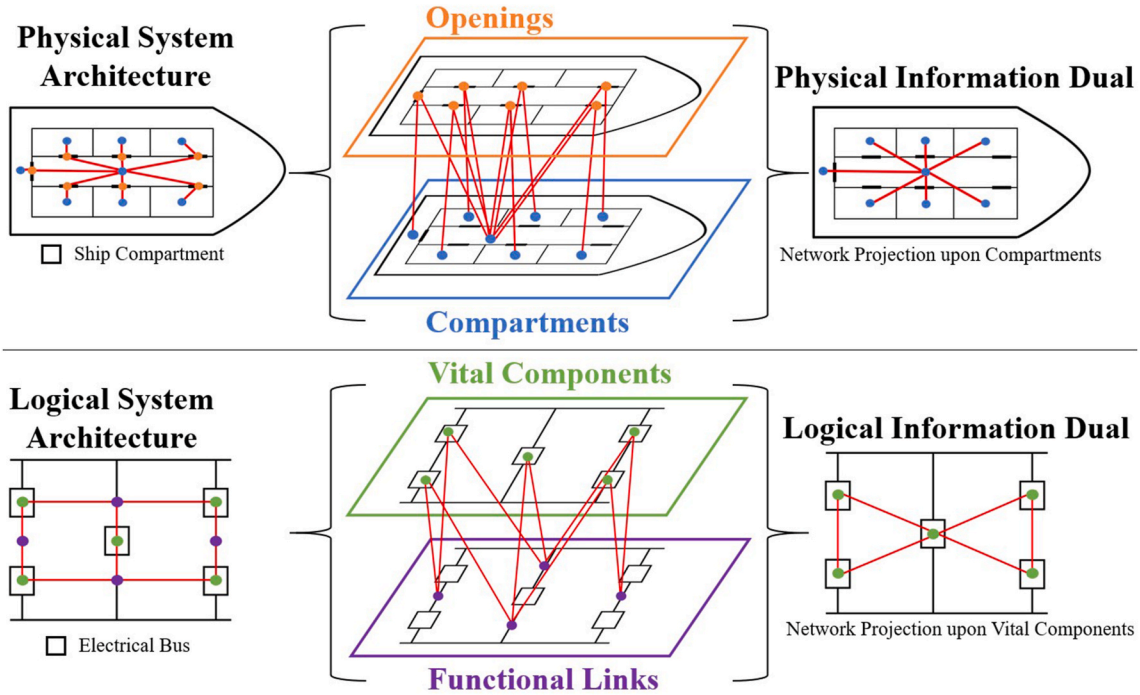


Fig. 5. System architecture network mapping examples. A 2D collapsed view of the system is shown on the left (bipartite network), an expanded 3D view of the layers in the middle (multi-layer network), and a network projection into an information dual on the right. The duals are formed by projecting one layer's nodes and the interlayer edges upon the other layer. Top: An illustrative example of a ship physical system architecture network mapping method. The compartments and openings of a ship are nodes (circles), and the relationships between them are edges (lines). A compartment is related to another compartment through an opening. Bottom: An illustrative example of a small electrical logical system network mapping method. The vital components and electrical links are the nodes (circles), and the relationships between them are edges (lines). A component is related to another component through a link.

$$\Psi = \Psi_0 \not\ni (C_d \cup V_d) \tag{3}$$

3) Failure of a *vital component.*

Remove vital component and remove its functional links from network, as seen in (4).

$$\Psi = \Psi_0 \not\ni (V_d \cup F_d) \tag{4}$$

4) Failure of a *functional link.*

Remove functional link from network, as in (5).

$$\Psi = \Psi_0 \not\ni F_d \tag{5}$$

3.3. Network projections and information duals

Networks that have two types of nodes, like the physical and logical systems in Fig. 5, are called bipartite networks. These two types of nodes can be split into two layers and then projected upon each other. The network projection upon a layer replaces the inter-layer edges and nodes of the projection layer with edges on the projected upon layer. This results in a single layer representation with intra-layer edges and only one node type. The simpler projected layers are useful for efficient calculation and representation of a more complicated system (Shields et al., 2015). These network projections are examples of information duals or network duals. A depiction of two network projections and information duals is shown in the right side of Fig. 5.

Information duals are beneficial to complex distributed system analysis, as they represent the recipients and transmitters of signals in the system without modeling the complex steps involved to send the signal (Rosvall, 2005). Information duals have proved useful in naval architecture by discovering interdependencies between distinct ship-board systems (Shields et al., 2015).

3.4. Vulnerability leading indicator network-based metrics

A focus on leading indicators is an essential characteristic of an effective engineering product development metric (Reinertsen, 1997). Three network theory derived vulnerability metrics based on leading indicators are presented. The metrics are intended to aid designers in understanding the vulnerability implications of architectural decisions at the physical system, logical system, and integrated physical system solution levels. The three metrics of interdependency, connectivity, and adaptability provide leading indicators of vulnerable areas in the architectural design of the systems. The metrics assess the importance of a node's role in the overall function of that network; the higher the importance of a node, the higher the risk, as the system is too reliant on that single node for operations. The leading indicator metrics therefore allow designers to address vulnerability issues in early design revisions in order to create a more capable ship for the customer.

3.4.1. Interdependency, β

Interdependency quantifies a network's reliance on certain nodes. Interdependency is based on a measure of the network's betweenness centrality. The average betweenness centrality of a node, β_i, informs the number of the shortest paths between all node pairs that travel through that node, as in (6) and (7) (Newman, 2018). Let g_{st} be the total number of shortest paths from source to target nodes.

$$\beta_i = \sum_{st} \frac{x_{st}^i}{g_{st}}, where\{ \begin{matrix} i = individual\ node \\ s = source\ node \\ t = target\ node \end{matrix} \tag{6}$$

$$x_{st}^i = \{ \begin{matrix} 1, node\ i\ on\ shortest\ path\ between\ s\ and\ t \\ 0, otherwise \end{matrix} \tag{7}$$

This metric is zero if the node is not on any shortest paths and proportional to the average rate at which traffic passes through a node (Newman, 2018). Interdependency provides a useful leading indicator by identifying nodes that are crucial to the successful operation of a network. Nodes with high interdependency act as a conduit for physical or logical traffic through the network. For example, in a physical system a stairway or elevator compartment is a high-traffic area through a ship's decks and levels.

3.4.2. Connectivity, κ

Connectivity identifies the nodes in the network that have a high number of edges. This is based on a node's degree centrality, which is the number of neighboring nodes a node is attached to (Newman, 2018). The degree of a node, and thus its connectivity score, is shown in (8) and (9).

$$\kappa_i = \sum_{j=1}^{n} A_{ij}, where\{ \begin{matrix} i = node\ being\ inspected \\ n = all\ nodes\ in\ network \\ A_{ij} = node\ adjacency\ matrix \end{matrix} \tag{8}$$

$$A_{ij} = \{ \begin{matrix} 1, edge\ exists\ between\ i\ and\ j \\ 0, otherwise \end{matrix} \tag{9}$$

This metric is bounded between a minimum of zero, where the node is not connected to another node, and n where the node is connected to all other nodes in the network. A high degree is related to a greater importance in the network's function because it identifies nodes with hub-like properties in the network. These network hubs, like a ship power panel, are potential leading indicators of vulnerable componentry that need to be preserved to maintain a ship's capability.

3.4.3. Adaptability, α

Adaptability is the system's flexibility in changing routings between two nodes. This is a direct measure of redundancy because it evaluates how many nodes are required to make a certain system or task fail. A water pump that can be routed to two generators requires both to fail instead of only being connected to one – hence a greater number of nodes must be removed from the network. This behavior is captured in the network by the max-flow min-cut theorem, which states that the number of independent paths, the number of nodes to remove connection between two nodes (the minimum cut set), and the maximum flow between two nodes are all equal (Newman, 2018). The average adaptability of a node can therefore be defined as seen in (10) and (11).

$$\alpha_i = \frac{\sum_{j=1}^{n} x_j}{n}, where\{ \begin{matrix} i = individual\ node \\ n = all\ nodes\ in\ network \end{matrix} \tag{10}$$

$$x_j = \{ \begin{matrix} 1, node\ j\ in\ minimum\ cut\ set \\ 0, otherwise \end{matrix} \tag{11}$$

This metric is bounded by a minimum of zero, where the node does not exist in any minimum cut set, and a maximum of one which is that all shortest paths in the system run through the node. A high adaptability means high redundancy for that task, but a low adaptability can highlight areas and systems that need further vulnerability reduction in subsequent design revisions.

3.5. Vulnerability assessment robustness metric

A robustness metric has been developed for operational evaluation of a ship design's ability to withstand a hostile weapon impact. Robustness tests a network's redundancy and separation in case of componentry failure. It examines how much of the network is still operational after damage. Damage is simulated by the removal of nodes and edges from the network. Kill modes can then be analyzed and evaluated for operability (see Section 2 on kill modes). The design's robustness, ρ, can thus be calculated as shown in (12). Several competing design variants denoted by the subscript v can be compared through this metric to help

inform decision makers.

$$\rho_v \mid w = \sum_i \frac{\sum_n \delta_n^i \mu_n^i}{\sum_n \delta_n^i}, where\{ \begin{array}{l} v = design\ \ variant \\ w = weapon\ \ threat \\ i = \ weapon\ \ impact\ \ run\ \ number \\ \delta = desireability\ \ coefficient \\ n = number\ \ of\ \ evaluated\ \ missions \\ \mu = mission/task \end{array} \quad (12)$$

The desirability constant, δ, allows for consideration of the necessity versus desirability of a given mission or capability. The desirability constant can be adapted throughout the ship's design from being used to address the separate capabilities the customer wishes the conceptual ship to have in combat to more refined performance parameters later in detail design. An example desirability constant table is shown in Table 1.

A possible assessment method when implementing the desirability constant for evaluation is to implement a baseline rule. For example, the failure of three or more compartments below the waterline can disable hydrostatic stability. Similarly, one node and two node removal can prove useful in examining the result of individual or dual componentry failure, while a removal of a large segment can provide information on the network's capability to handle a large weapon impact. The given weapon, *w*, determines the weapon envelope due to its charge size and generalized blast damage equations. The weapon envelope in turn determines the number of nodes removed from the network for simulating damage.

The robustness metric gives the vulnerability assessment director flexibility in choosing to run an assessment based on specific weapon envelopes and/or to evaluate the entire system at an individual componentry level. An example flowchart, Fig. 3 of Section 2 of this paper, shows how the network framework and vulnerability assessment can be integrated into the ship design program to provide leading indicators and design variant comparisons for decision makers.

4. Representative case study

In this case study, an assessment was conducted on a representative naval ship design and its cargo elevator system as shown in Figs. 6 and 7. The representative ship design and physical system takes influence from the Military Sealift Command's T-AKE dry cargo/ammunition ship class. The logical architecture examined six of the naval cargo elevators like that on the T-AKE class ship (NASSCO). The functionality of the cargo elevators is imperative for the ship's primary mission as a supply and replenishment vessel (United States Navy Fact File Online). Cargo elevator systems provide a useful case study, as they exemplify the characteristics of many important shipboard systems. Complex shipboard systems require routing through many compartments and have supply and demand needs in the same manner as cargo elevators. The products these shipboard systems deliver are their main difference (e.g. cargo, electricity, chill water, etc.).

Naval cargo elevators have proven a mission essential system in not only cargo vessels but also aircraft carriers. Most recently, the USS Gerald R. Ford has made the news after encountering extensive delays due to issues with the installation of its munitions elevators (Capaccio, 2019).

Table 1
Example desirability constants for use in vulnerability assessments in determining the robustness of a ship design.

Post impact desirability constant, δ	Must accomplish task to maintain ability for:
1.0	Hydrostatic Stability
0.9	Power & Navigation
0.7	High Importance Mission/Task
0.5	Medium Importance Mission/Task
0.3	Low Importance Mission/Task

4.1. Construction of the ship design's four-layer network

First, a model set of general arrangements was created and then converted into the physical system network in the manner shown in Fig. 5. Then, the logical system architecture of the cargo elevators was mapped based on the Naval Ship's Technical Manual Ch. 772 on Cargo and Weapon Elevators (Naval Sea Systems, 1998). Six cargo elevators were placed into the logical system architecture with their functions and links mapped as shown in the right side of Fig. 6, with an illustrative depiction of the general system on the ship in Fig. 7. Redundancy is built into the logical system, as pairs of cargo elevators serve one cargo hold on each deck. Pairs of cargo elevators were linked to a single cargo hold space on each below main-deck level of the ship. The cargo elevator logical system architecture was then integrated with the physical system architecture by placing edges between vital components and the compartments they reside within. This results in the completed four-layer network as shown in the center of Fig. 6.

4.2. Case study vulnerability leading indicators

The physical system, logical system and the integrated four-layer network were assessed using the leading indicator metrics described in Section 3. The networks used are shown in Fig. 6 and show how a lower fidelity, early-stage, design can be assessed using the integrated four-layer framework. For an unbiased, accurate framework, the integrated four-layer network analysis used only the compartments and openings that affect the cargo elevator logical system. This ensures that unrelated physical architecture does not skew the results of the three metrics. For example, the measure of how many independent paths run between the bridge and the engine room is not relevant to the cargo elevator system being analyzed. All the physical system elements can be incorporated if all shipboard systems were to be analyzed. Fig. 8 shows the pairwise comparison graphs of the three network leading indicators on each network analyzed. The diagonal plots within Fig. 8 represent the kernel density plots. These plots show that most nodes score low, near zero for each metric, and only a small subset of nodes are shown to score high. This small subset of high scoring individuals are the nodes that the rest of the system depends on and therefore the most important for vulnerability protection. This behavior is indicative of a power law distribution or Pareto distribution (Newman, 2018; Barabási, 2016).

4.2.1. Physical system observations

The physical system was seen to demonstrate the connectivity and interdependency of its hallways and stairwell compartments. The top right score on the pairwise comparison of these two metrics in Fig. 8 for the physical system was the superstructure's hallways. This result correctly illustrates expectations, as halls and stairs are the main source of personnel movement throughout the ship's spatial layout. Low adaptability of low deck spaces and single passage doorways was also found to be consistent to expectations. For example, the lower deck ballast tanks make up part of the group of the adaptable physical system nodes scoring around zero throughout Fig. 8. The scores of the cargo elevator compartments within the physical system were unremarkable, as they fell below the middle of the results. This shows that without the context of the logical system, the cargo elevators do not appear as important as they are to operations.

4.2.2. Logical system observations

The importance of the cargo elevator platforms is seen in the logical system indicators. The platforms are clustered together in the top right of Fig. 8 pairwise comparison plots for connectivity and interdependency. The electrical connections and control panels scored the highest in low adaptability. The leading indicators are therefore showcasing their intended characteristics, as the electrical componentry and control panels have no redundancy in this case study.

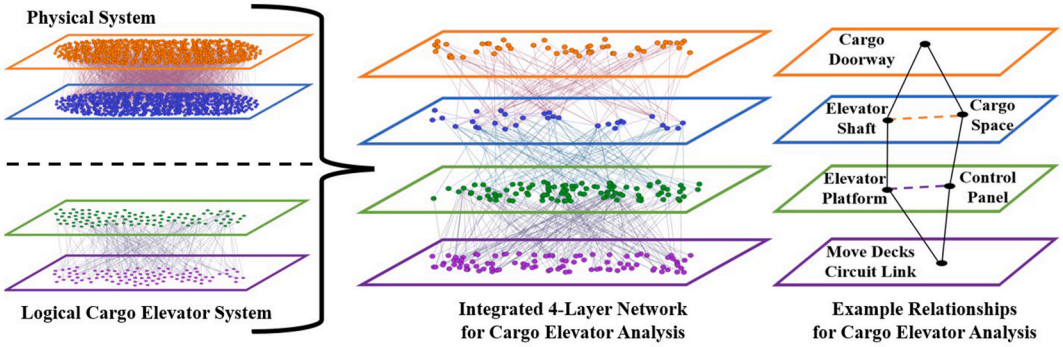


Fig. 6. A depiction of the detailed physical and logical systems is on the left. The case study's integrated four-layer network for the cargo elevator system is shown in the center. The physical system network has 1742 nodes and 1902 edges (upper left). The logical system network has 194 nodes and 188 edges (lower left). The integrated system network has 276 nodes and 394 edges (center). This integrated network has the compartments and openings that its vital components are in to avoid improperly skewing results of the leading indicator analysis. On the right is an example relationship between nodes in the network. The black dots are nodes, and the black solid lines are edges. The dashed lines represent projections of the physical and logical system into network information duals as described in Section 3. Network duals are useful in reducing a large, complex system to its fundamental content (Shields et al., 2015).

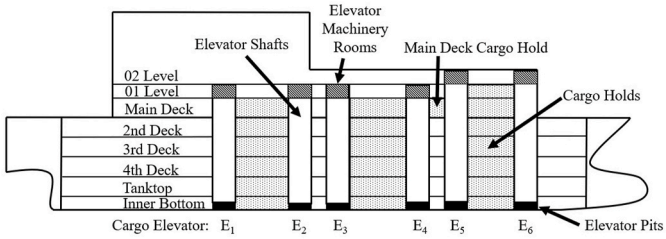


Fig. 7. A depiction of the six cargo elevators' layout that was used in the case study. Cargo elevators open on each deck toward their respective cargo holds. Pairs of cargo elevators are shown to service a set of cargo holds. The Main Deck cargo hold is serviced by the forward four cargo elevators. A machinery room for each cargo elevator is on the 01 Level or 02 Level on top of each elevator shaft. These machinery rooms contain the mechanical components needed to raise/lower the elevators. The operability of each cargo elevator is analyzed after damage as part of the vulnerability assessment.

4.2.3. Integrated 4-layer network observations

The integrated network's leading indicators highlight vulnerable areas not seen by examining the physical or logical system. Cargo elevators, elevator platforms, machinery rooms, and electrical sources scored high in at least one of the three indicators. Control panels, mechanical linkages, and electrical linkages were seen to have high adaptability scores as part of the highest adaptability scoring group in Fig. 8.

The Main Deck cargo hold emerged as the dominant high scoring outlier and the maximum score in connectivity and interdependency; it is plotted in Fig. 8 as the peak value for both these metrics. This result is previously unseen by the physical or logical network model, where the cargo hold's score was unremarkable in the pairwise comparisons.

4.2.4. Outlying top scores

The highest scoring nodes in Fig. 8 for the integrated network based on the three leading indicators are shown in Table 2.

These identified nodes are crucial to the successful operation of the integrated network and thus need vulnerability reduction and protection. Design decision makers can now be informed of these vulnerable areas for improvement via revisions based on the vulnerability reduction techniques discussed in Section 2. An assessment of the hardness of the design in response to a weapon threat can further highlight vulnerable areas within the environment of a hostile weapon impact. This is demonstrated through a calculation of the case study design's robustness, which is the other result of the network-based vulnerability assessment as shown previously in Fig. 3.

4.2. Calculating robustness

A set of representative missions was developed to demonstrate the robustness metric and the network-based vulnerability assessment program illustrated back in Fig. 3. The six cargo elevators' ability to move cargo from holds to on deck for transference were analyzed. Three missions, one for each pair of cargo elevators, were created. All three missions were given a high importance and a high desirability constant from Table 1. Table 3 shows the missions and desirability constants used in the case study.

Each mission's kill mode was defined as a failure of being able to move cargo from below decks to main deck. If any pair of cargo elevators were unable to provide operational capability, their respective mission is killed. Combining the missions and a weapon threat analysis allows for calculation of the robustness of the ship design.

Air explosion threats (AIREX) are a common hostile threat to naval ships that need to be addressed in a vulnerability assessment (Smith, 2010). To simulate an AIREX weapon, a simulation was run on the network where every exterior compartment above the waterline, between 2nd Deck and 02 Level, was considered the point of impact. For each exterior touching compartment in this ranges, runs were conducted to simulate the damage. In each run, the impact compartment was removed from the integrated network. The impact compartment's neighboring compartment nodes and their neighbors through openings were also removed to represent severe damage spreading. This could be due to fire, fragmentation, or blast from the impact. The integrated network was then modified in accordance with the rules stated in Section 2. The integrated network was then analyzed for its ability to carry out its critical missions.

Under this weapon threat selection, only three impacts resulted in a cargo elevator failure; this is shown in Fig. 9. The impacts of the machinery rooms of Elevator 1 and Elevator 2 both resulted in failure of those elevator platforms. The network model correctly captured this damage case. Failure of the platforms is to be expected if the cargo elevator loses its mechanical and/or electrical system. Since these two machinery rooms were directly exposed on the topside of the ship to the impact, they are more vulnerable. However, since each pair of elevators is redundant and only one fails in these cases, then the three missions defined in this case study are satisfied. This highlights the network framework's ability to model redundancy.

The only compartment weapon impact in this scenario that resulted in a mission failure was to the cargo hold on the Main Deck. This cargo hold on the Main Deck is serviced by Elevators 3, 4, 5, 6, which are the four that failed in this damage case. This results in two out of three mission kills. A high robustness score ($\rho_v \mid \text{AIREX} = 0.996$) for this given

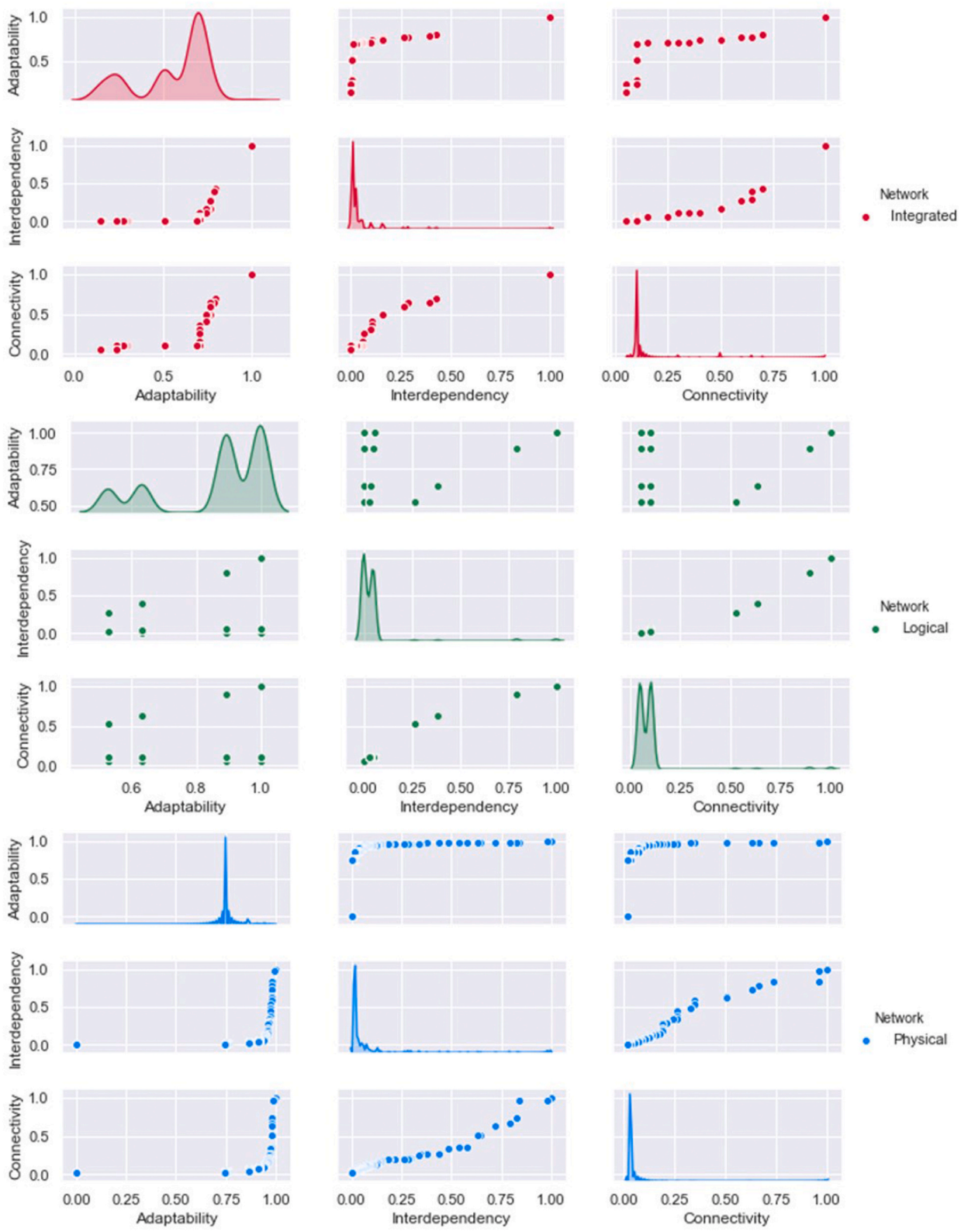


Fig. 8. A matrix of pairwise comparison graphs for the three vulnerability leading indicator metrics. Each case study network (physical, logical, and integrated) is represented with different colors and symbols in the plots. The diagonal plots are kernel density plots of the respective metric. Each vulnerability metric is normalized to its respective maximum within each network. The maximums of leading indicators and their pairwise comparisons in the graph are the nodes that should be considered by decision makers for vulnerability reduction. Note: In order to maintain comparison between leading indicator maximums, adaptability is plotted as the one minus the normalized adaptability metric described in Section 3. (For interpretation of the references to color in this figure legend, the reader is referred to the Web version of this article.)

Table 2
Case study top ten nodes for the three vulnerability leading indicators for the integrated four-layer cargo elevator network.

Rank	Interdependency (Highest)	Connectivity (Highest)	Adaptability (Lowest)
1	Main Deck Cargo Hold	Main Deck Cargo Hold	Elevator 5 Machinery Room 01 Level
2	Elevator 2 Shaft	Elevator 1 Platform	Elevator 6 Machinery Room 01 Level
3	Elevator 1 Shaft	Elevator 2 Platform	Elevator 5 Machinery Components
4	Elevator 2 Platform	Elevator 3 Platform	Elevator 5 Electrical Source
5	Elevator 1 Platform	Elevator 4 Platform	Elevator 6 Machinery Components
6	Elevator 3 Shaft	Elevator 1 Shaft	Elevator 6 Electrical Source
7	Elevator 4 Shaft	Elevator 2 Shaft	Elevator 5 Mechanical Winch
8	Elevator 3 Platform	Elevator 5 Platform	Elevator 5 Electrical Source Linkage
9	Elevator 4 Platform	Elevator 3 Shaft	Elevator 6 Mechanical Winch
10	Elevator 1 Main Deck Arch	Elevator 4 Shaft	Elevator 6 Electrical Source Linkage

Table 3
Cargo elevator mission definitions for case study analysis.

Mission	Desirability	Kill Mode
μ_1	$\delta_1 = 0.7$	E_1 and E_2 unable to service their cargo holds.
μ_2	$\delta_2 = 0.7$	E_3 and E_4 unable to service their cargo holds.
μ_3	$\delta_3 = 0.7$	E_5 and E_6 unable to service their cargo holds.

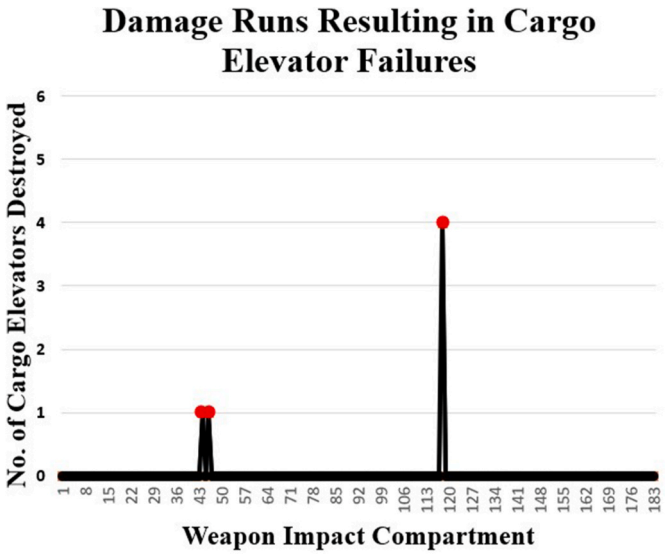


Fig. 9. A depiction of the physical and logical systems used in the case study is on the left. The integrated 4-layer network for the cargo elevator system is on the right. This integrated network only has the compartments and openings that its vital components are in contact with to avoid skewing results of the leading indicator analysis. There are 183 compartments and 6 cargo elevators analyzed.

threat and specific three missions can then be calculated for this design as shown in (12). This analysis represents one of many threats that could be examined. The robustness can then be compared to another variant's performance under the same weapon threat to inform designers.

The logical system and the physical system individually did not show this Main Deck cargo hold to be vulnerable, but the integrated four-layer cargo elevator network directly pointed to this compartment as being the most vulnerable node in the network. The Main Deck cargo hold is shown as ranking the highest in two out of the three leading indicators seen in Table 3. This shows the power of the vulnerability assessment network method presented in being able to uncover vulnerability issues and rapidly compare results with other variants.

5. Conclusion

This paper has demonstrated how a network-based vulnerability assessment can be implemented in early-stage design to better inform decision makers. The use of the novel multi-layer network framework to represent a ship design for vulnerability assessments helped to extend vulnerability assessments at a lower level of design fidelity than required for traditional methods. A set of vulnerability leading indicator metrics were developed and illustrated in this research through a case study of a representative naval ship. The case study further examined the effectiveness of the metrics in identifying important components in a distributed naval ship design. The four-layer network approach was also able to uncover previously unforeseen vulnerability issues by integrating a ship's logical and physical system for vulnerability analysis.

The research enables decision makers to understand the vulnerability implications of their design choices earlier in the design program, thereby empowering the designers to deliver safer, more effective ships to the operators on the front line.

The framework developed provides utility in the design space but does not extend to the operations domain. Future work on this research could examine dynamic time-stepping for expansion into operation-based analysis. It could also integrate probabilistic failures for recoverability analysis or component lifespan investigation. The addition of dynamics to the network could prove useful in identifying other types of weaknesses in a design that can further inform naval decision makers.

CRediT authorship contribution statement

Luke C. Brownlow: Writing - original draft, Writing - review & editing, Data curation, Software, Conceptualization, Project administration, Formal analysis. **Conner J. Goodrum:** Writing - review & editing, Methodology, Conceptualization, Resources. **Michael J. Sypniewski:** Writing - review & editing, Methodology, Conceptualization, Resources. **James A. Coller:** Writing - review & editing, Methodology, Conceptualization, Resources. **David J. Singer:** Writing - review & editing, Resources, Methodology, Conceptualization, Supervision, Project administration.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors. We would like to thank the Science, Mathematics, and Research for Transformation Program funded by the Department of Defense for providing general academic support during the course of this project.

Appendix A. Supplementary data

Supplementary data to this article can be found online at https://doi.org/10.1016/j.oceaneng.2021.108731.

References

Ball, R.E., 2003. The Fundamentals of Aircraft Combat Survivability Analysis and Design, second ed. American Institute of Aeronautics and Astronautics, Inc.

Barabási, A., 2016. Network Science. Cambridge University Press.

Brefort, D., Shields, C.P.F., Jansen, A.H., Duchateau, E., Pawling, R., Droste, K., Jasper, T., Sypniewski, M.J., Goodrum, C.J., Parsons, M., Kara, M., Roth, M., Singer, D.J., Andrews, D.L., Hopman, H., Brown, A., Kana, A.A., Jan. 2018. An architectural framework for distributed naval ship systems. Ocean Eng. 147, 375–385.

Capaccio, A., 2019. On Costliest U.S. Warship Ever, Navy Can't Get Munitions on Deck, Bloomberg. July 30, 2019.

Chalfant, J., 2015. Early-stage design for electric ship. Proc. IEEE 133 (12), 2252–2266.

Chalfant, J., Chryssostomidis, C., Synder, D., Parsons, M.A., Brown, A., 2017. Graph Theory Application in Focus-Compliant Ship Designs. IEEE Electric Ship Technologies Symposium, Arlington, VA.

De Domenico, M., Solé-Ribalta, A., Cozzo, E., Kivelä, M., Moreno, Y., Porter, M.A., Gómez, S., Arenas, A., Dec. 2013. Mathematical formulation of multi-layer networks. Phys. Rev. X 3, 4.

Doerry, N., 2007. Designing electrical power systems for survivability and quality of service. Nav. Eng. J. 119 (2), 25–34.

Farris, R.S., Stuckey, C.B., 2000. A ship Defense analysis process. Johns Hopkins APL Tech. Dig. 21 (3).

Goodfriend, D.B., 2015. Exploration of System Vulnerability in Naval Concept Design. M. S. thesis. Dept. Ocean Engineering, Virginia Polytechnic Institute and State Univ.

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

Jansen, A.C.H., 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 Eng. 190.

McKenny, T.A., 2013. An Early-Stage Set-Based Design Reduction Decision Support Framework Utilizing Design Space Mapping and a Graph Theoretic Markov Decision Process Formulation, Ph.D. Dissertation, Naval Architecture and Marine Engineering. Univ. of Michigan, Ann Arbor, MI.

Molland, A.F., 2008. Vulnerability studies. In: The Maritime Engineering Reference Book. Butterworth-Heinemann, Oxford, England, pp. 69–70 ch. 2, sec. 5.6.

NASSCO. General dynamics. Lewis and Clark (T-AKE 1) class dry cargo/ammunition ship Fact sheet. San Diego, CA, USA. https://nassco.com/pdfs/T-AKE-Fact-Sheet.pdf (last accessed on 31 March 2020).

Naval Sea Systems, Dec. 1998. Naval Ships' Technical Manual, Ch. 772 - Cargo and Weapons Elevators, Rev. 2.

Newman, M., 2018. Networks, second ed. Oxford University Press.

Parsons, M.A., 2019. M.S. thesis. In: Network-Based Naval Ship Distributed System Design Using Architecture Flow Optimization. Ocean Engineering. Virginia Polytechnic Institute and State Univ., Blacksburg, VA.

Piperakis, A.S., 2013. An Integrated Approach to Naval Ship Survivability in Preliminary Ship Design. Ph.D. dissertation. Dept. of Mechanical Engineering, University College London, London, England.

Reinertsen, D.G., 1997. Managing the Design Factory, first ed. Free Press.

Rigterink, D.T., 2014. Methods for Analyzing Early Stage Naval Distributed Systems Designs, Employing Simplex, Multislice, and Multiplex Networks, PhD. Dissertation, Naval Architecture and Marine Engineering. Univ. of Michigan, Ann Arbor, MI.

Rosvall, M., Trusina, A., Minnhagen, P., Sneppen, K., 2005. Networks and cities: an information perspective. Phys. Rev. Lett. 94.

Shields, C.P.F., 2017a. Investigating physical solutions in the architectural design of distributed ship service systems. Ocean Eng. 135, 236–245.

Shields, C.P.F., 2017b. Investigating Emergent Design Failures Using a Knowledge-Action-Decision Framework. Ph.D. dissertation. Naval Architecture and Marine Engineering. Univ. of Michigan, Ann Arbor, MI.

Shields, C.P.F., Rigterink, D.T., Singer, D.J., 2015. The information dual network and its applications to naval architecture. In: 12th International Marine Design Conference Proceedings. Tokyo, Japan.

Smith, R.M., 2010. Using Kill-Chain Analysis to Develop Surface Ship CONOPS to Defend against Anti-ship Cruise Missiles. thesis. Navy Postgraduate School, Monterey, CA.

Stevens, A.P., 2016. Naval Ship Preliminary Arrangements for Operability and Reduced Vulnerability. M.S. thesis. Ocean Engineering. Virginia Polytechnic Institute and State Univ., Blacksburg, VA.

United States Navy Fact File Online. Dry cargo/ammunition ships T-AKE. https://www.navy.mil/navydata/fact_display.asp?cid=4400&tid=500&ct=4 last accessed 31 March 2020.