Ocean Engineering 150 (2018) 36–47

Contents lists available at ScienceDirect

Ocean Engineering

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

Understanding cascading failures through a vulnerability analysis of interdependent ship-centric distributed systems using networks

Conner J. Goodrum *, Colin P.F. Shields, David J. Singer

University of Michigan, USA

ARTICLE INFO

Keywords:
Distributed systems analysis
Ship vulnerability
Interdependent networks
Cascading failures
Early stage-ship design (ESSD)
Vessel operability

ABSTRACT

System vulnerability is of critical concern when evaluating the operational performance of a naval vessel. The identification of system failures as well as subsequent cascading failures of related systems is required to understand if the vessel's distributed systems can survive a damage scenario through the prevention of large scale failures. In late-stage ship design, high-fidelity system analysis and scenario simulations can identify this type of emergent failure. However, in early-stages when distributed system design information is limited, vulnerability analysis typically focuses on component damage and vessel layout. Without considering the effect of distributed system design, the identification of cascading failures can not be identified early in the design process. To address this problem, the authors describe a distributed system model and corresponding vulnerability analyses to consider how vessel layout and distributed system configuration impact vessel performance under damage with limited information. The approach uses network-based methods to reduce the design detail required for distributed system modeling and vulnerability analysis. This approach is demonstrated on illustrative cases and a naval ship concept example to illustrate the importance of identifying cascading failures in early stage design.

1. Introduction

Increased connectedness and interdependence of distributed systems on-board naval vessels compounds the ever-growing potential for emergent system failures. System-wide failures driven by damage propagation through distributed systems are a critical factor in vessel vulnerability. While many emergent behaviors are beneficial, such as in the case of the functionality of the Internet and artificial intelligence (Mitchell, 2009); other behaviors such as cascading failures are detrimental, even catastrophic (Buldyrev et al., 2010). Cascading failures start in a small section of a system and quickly spread through interdependencies between system components rendering large portions of the system non-functional. Notable examples include the blackouts experienced in the eastern United States as well as Italy in 2003 (Dobson et al., 2007). Cascading failures are also present in the naval domain:

- The USS Yorktown was a U.S. Navy guided-missile cruiser which incorporated high-powered radars, computer systems, and new automation technology. On September 21, 1997 an error in the main monitoring computer caused a ship control system fault to spread through LAN switches, into the engine controllers and ultimately caused the ship to go dead in the water (Slabodkin, 1998).
- U.K. Royal Navy's newest vessels, Type 45 destroyers, have suffered complete power failures in warm climates. When outside temperatures rise, intercoolers providing chilled air to the primary turbines become overloaded. This causes the turbines to overheat and shutdown, leading to a significant power load to smaller diesel generators which in turn fail, leaving the vessel with no sources of power or propulsion (Project Napier sees twin-, 2016) (Brown, 2016).

These examples show how relatively small amounts of damage spread rapidly through all of the integrated shipboard systems. Failure propagation of this sort presents serious operational and vulnerability concerns, especially in the face of increasing complexity and interdependence of systems and components (Piff, 2013; Piperakis, 2013; Rigterink et al., 2013; Trapp, 2015). Studies have analyzed and proposed qualitative system design solutions that attempt to minimize the opportunity for cascading failures in naval power systems (Amy, 2002; Doerry, 2006, 2014). However, many cascading failures are a function of multiple systems and thus can only be identified through an interdependent analysis paradigm.

Interdependent systems present the opportunity for failures to cascade through the coupling of components spatially (Asztalos et al., 2014) and functionally (Issacharoff et al., 2008; Carreras et al., 2014).

---

* Corresponding author.
E-mail address: cgoodrum@umich.edu (C.J. Goodrum).

https://doi.org/10.1016/j.oceaneng.2017.12.039
Received 1 August 2017; Received in revised form 20 November 2017; Accepted 17 December 2017

Naval ship systems are coupled in both space and functionality, which can result in extreme vulnerabilities, and exhibit cascading failures under limited damage (Bashan et al., 2013). Strong spatial coupling occurs when system components or their supporting distribution systems are co-located in the vessel. High degrees of functional coupling result from the limited number of components within a vessel and the self-contained nature of naval operations. Increasing system density and the interdependence of automation and component functions in all-electric warship designs will continue to drive both spatial and functional coupling in the future. This makes the early identification and prevention of emergent catastrophic failure modes a critical design activity (Dougal and Langland, 2016).

Measuring the performance of interdependent ship systems has been approached through simulation of system dynamics (Whitcomb, 1992; Cramer, 2007; Fang et al., 2009; Cramer et al., 2011) and linear programming analysis of network flows (Butler et al., 2001; Cramer et al., 2009; Trapp, 2015). These methods require significant modeling effort to represent various types of resource flow, primarily electrical and chilled water, through their respective conduits. However, in the concept design phase, the requisite level of detail may not be available without making significant assumptions, may be unknown due to concurrent technology development, or may incur unsustainable computation effort when applied across a large design space (Kassel et al., 2010). The disconnect between the information available in early design stages and in the information required to model these systems limits their utility.

In an effort to introduce system performance analysis earlier in the design process, naval distributed ship service systems are approached from an architectural perspective. The overall system behavior can be decomposed into interactions between architectures defining the system environment, the functional interdependencies between system components, and how those components are used. Thus the overall architecture of distributed ship service systems can be discussed in terms of *physical architecture*, *logical architecture*, and *operational architecture*.[1] Physical architecture describes the system environment, defined as the spatial relationships within the vessel. For example: how compartments are geometrically related and component locations. Logical architecture describes the relationships between vessel components that are required to generate system functionality (e.g. generator provides power to a radar). Operational architecture defines how the distributed system is utilized through time for a given scenario.

Here we analyze the system response by defining the physical, logical, and operational architectures. The intersection of the physical and logical architectures create a physical solution, which describes the material manifestation of components within the vessel and distributed system routings between components. Specifically, a physical solution representing an early-stage design of an all-electric warship is considered. In the following study, we focus on vulnerability analysis, which considers how damage to the physical solution impacts the overall system functionality. Vulnerability of the vessel is analyzed under three different operational architectures based on network measures.

Understanding the vulnerability characteristics of a distributed system design earlier in the design process can complement and guide existing higher fidelity analyses. Identifying critical damage scenarios and non-robust designs will enable designers to apply high fidelity analyses where needed. This limits the significant modeling and computation effort required by complex scenario modeling and provides a new early-stage design differentiator. Traditionally, engineers address this in concept design with component damage analyses that identify how probabilistic attacks result in component failures. This overlooks system vulnerabilities which may exist in the connectivity between components, and limits observable failure modes.

Concept design survivability analysis relies on reliability diagrams and proximity-based damage of shipboard components (Doerry, 2007). These analysis methods apply probabilistic damage scenarios to the physical architecture, remove hit components, and calculate the corresponding functionality loss in the logical architecture (Brown and Waltham-Sajdak, 2015). Using recently developed network-based representations of systems and vessel arrangements this can now be expanded to include physical connectivity between components (Rigterink, 2014; Shields et al., 2016). Including distributed system representations when applying traditional methods will help identify critical cascading failure modes during concept design using only rudimentary network analysis.

This paper describes and demonstrates a method to extend early-stage naval system vulnerability analysis to include the connectivity effects of distribution systems within the vessel. This extension is shown to identify cascading failures which cannot be identified through component-based reliability analysis or high-fidelity analysis of systems independently. First, a recursive damage propagation algorithm and three network-based damage analyses are presented. The algorithm and methods are demonstrated in two illustrative cases and applied to a representative naval combatant concept design. Results and analysis are used to discuss the capabilities provided by a connectivity-based approach and to compare the proposed analysis methods.

2. Analyzing damage in naval design

In this section, networks are introduced as tools to define physical and logical design relationships at preliminary design stages. Networks can be used to both represent functional and physical relationships between system components without the need for high fidelity models or detailed system design parameters. They also provide the ability to conduct various analyses on multiple distributed subsystems coupled by physical and logical relationships.

Informally, a network is a set of objects (nodes) which are linked to one another through relationships (edges). The generality of defining what the nodes and edges represent provides immense flexibility in network applications. Examining the way nodes are connected to one another, which comprises the network's *structure*, allows better understanding of the relationships between individual nodes and the system response. In the naval domain, networks have been used to model both geometric and distributed system structures (Shields et al., 2017) with limited information. For a comprehensive overview of network theory, see (Newman, 2010).

The most fundamental network structure is a ‘Simplex Network’ in which a set of N nodes are connected by K edges. In general, edges are ‘undirected’ - meaning connections exist between nodes but no additional information about the nature of their connection. Edges can also be ‘directed’, which limits the relationships between nodes to a single direction. At an additional level of detail, nodes can be given values of demand, which allows them to be treated as a source or sink. The edges in this case become ‘pipes’ through which demand can flow; the edges are assigned capacities. This enables an additional level of analysis from the conventional connectivity case.

Fig. 1 illustrates a ‘Multiplex Network’, in which the aforementioned simplex networks are expanded into n layers. This creates a network of networks. Each of these n layers have the same set of N nodes, but can have different numbers of edges. These edges represent different functional representations and relationships between the nodes (Kurant and Thiran, 2006). Each duplicate node in a subsequent layer is connected across all layers to the same node, which represents interdependencies across the network plexes (shown in the figure as grey lines between layers).

The vulnerability analysis conducted in this paper follows the flow chart shown in Fig. 2. The process begins by representing the physical

---

[1] This description reflects the findings of an ongoing research program studying 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. The program is supported by the U.S. Office of Naval Research, Grant No. N00014-15-1-2752.