A triple-network-layer method for designing high resilience system architectures

Giota Paparistodimou[1] MEng MSc PhD CEng MIET MINCOSE, Philip Anthony Knight[2] BSc MSc PhD, Malcolm Robb[1] BEng PhD AMIMECHE, Gail Hughes[1] BEng PhD CEng MIET.

[1] *BAE Systems,* [2]*University of Strathclyde*

[1] Corresponding Author. Email: giota.paparistodimou@baesystems.com

Synopsis

Complex multi-domain engineering systems are at the heart of modern warfare. The very nature of complexity means that the interactions between elements of such systems can lead to unforeseen consequences that are difficult to understand and predict. This is particularly true when there are varied types of disruption that can take place, such as component failure or deliberate attacks. The ability to analyse and assess how complex systems recover from disruption is critical for understanding resilience, especially as automated control design aspects are increasing. This paper proposes a triple-layer network methodology that is based on the physical, functional, and control layers of a complex system. The number of controllers and connections between controllers and functional nodes are varied for different design options, and resilience is evaluated. By identifying the control design features that have the greatest influence on resilience, the preferred design option can be chosen, ensuring that resilience meets the design objectives in the early stages with only the necessary redundancy elements. The method is suggested to be integrated into the overall process of designing high resilience monitored and controlled system architectures ultimately allowing to design for recoverability

Keywords: resilience, recoverability multi-layer network analysis, early-stage system architecture design, control systems.

1. Introduction background

1.1. Research motivation

The complexity and interconnectedness of modern engineering systems are caused by their increasing size, the amount of data they manage, and the introduction of new and more sophisticated technologies, such as automation and platform management with their increased monitoring and control elements. This has made engineering systems more vulnerable to expected and unexpected disruptions during their lifecycle. INCOSE (2023) defined the purpose of the system architecture process as "to generate system architecture alternatives, select one or more alternatives(s) that address stakeholder concerns and system requirements, and express this in consistent views and models". In this way, system architecture process is an appropriate process to address resilience concerns and the resilience requirements, therefore, having appropriate system architecture method to address resilience is valuable.

1.2. Resilience

The resilience concept seeks to address the ever-changing vulnerability of engineering systems, necessitating the design and development of resilience systems. Resilience is defined by (Haimes 2009) as the "ability of a system to withstand a major disruption within acceptable degradation parameters and to recover with a suitable time and reasonable costs and risks". A typical resilience curve is shown in Figure 1 displaying the system performance plotted against time prior, during and post disruption.

Resilience is impacted by the topology of the system, thus the interconnectivity of the constituent components of the system (Bertoni et al. 2021). Similarly, (Office of the Assistant Secretary of Defense for Homeland Defense and Global Security 2015) specifies resilience as an inherent property of a system architecture, recommending that it should be analysed and defined during the system architecture process alongside other design variables. Redundancy in the system architecture is an important aspect of designing a resilient system.

Author's Biography

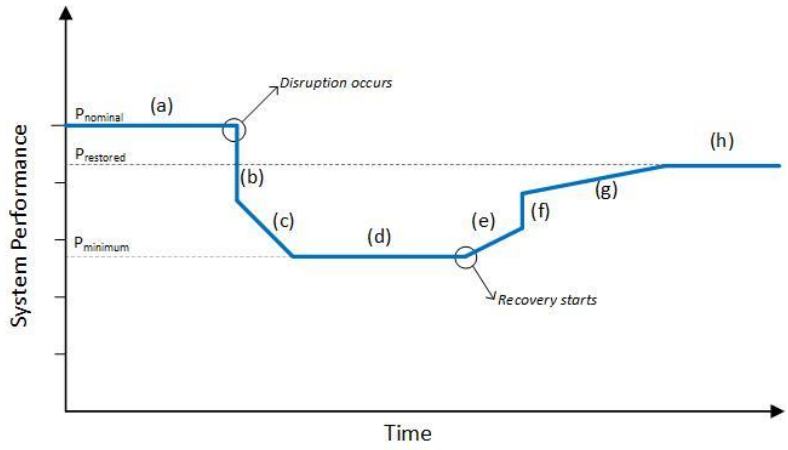
Giota Paparistodimou works as a Model Based Systems Engineer with BAE Systems. She is a Chartered Engineer, has completed a PhD in System Engineering and has a number of academic publications in the area. She has worked internationally, as a newbuilding ship Classification Surveyor in South Korea, Project Engineer in Brazil and Norway, and as a Principal System Engineer in the UK. Philip Knight is a Senior Lecturer in Mathematics at the University of Strathclyde. His primary research interests are in applied linear algebra, encompassing a wide range of topics in network analysis. He has written a number of highly cited papers on matrix algorithms and is co-author of the well-regarded textbook "A First Course in Network Theory". Malcolm Robb is a Research and Technology Engineering Manager for BAE Systems' Future Business and Technology Team. He has worked for BAE Systems for twenty-six years on a wide variety of warship designs and projects. Malcolm holds a PhD in composite materials. Gail Hughes, a Chartered Engineer, is a Principal Research and Technology System Engineer and has a PhD in control system design.

 https://doi.org/10.24868/11188

Redundancy improves recovery capabilities by creating different routes that aid in preserving system performance when disruptions take place (Yodo and Wang 2016). (Paparistodimou et al. 2020) in a structural viewpoint stated design for redundancy involves “architectural (components and their connections) options in the instantiated system architecture that are capable of satisfying the same function”.

Meanwhile, (Wied et al. 2020) mentions that the difference between a resilience and a predictive approach is that the first prepares, monitors, responds, rebounds, whereas the second forecasts, assesses, plans and prevents. Particularly, resilience relates to the ability to respond (Hollnagel et al. 2011).

Facets of resilience are related to the system's ability to monitor its operations, anticipate potential failures, and respond to such failures (Yodo and Wang 2016).



(a) Normal operation phase, system operates at nominal operation performance ($P_{nominal}$).
(b) Immediate degraded state.
(c) Subsequent degrading state
(d) Resulting disrupted state, system operates at minimum disrupted performance ($P_{minimum}$).
(e) Recovery improved state.
(f) Resulting recovered state.
(g) Repairing state
(h) Final stable state, system operates at stable restored performance ($P_{restored}$).

Figure 1: Generic resilience curve

1.3. Monitor and control systems relationship with resilience

Today's complex engineering systems have extensive monitoring and control over the behaviour of their constituent components, which adds to the complexity of modern systems as the number of components and intertwined interactions grows. A high level of monitoring and control helps to manage the system's behaviour better under normal conditions, as well as detect degradation behaviour before it becomes completely incapacitated, allowing control systems to initiate and complete the recovery pathway. Monitoring and control architecture supports complex systems' resilience behaviour by detecting early signs of degraded behaviour and facilitating quick and intelligent corrective actions to recover system performance to normal. As a result, monitoring and control are essential for enabling the resilience recovery path, but they can also increase system vulnerability in the event that they are unable to support the system's recovery.

In this way, monitoring and control have become key parts of complex systems, but also have become great causes of vulnerabilities, as failures of sensors or controllers are becoming key causes for loss of total system functionality. Thus, when sensors or controllers fail, the entire system's resilience suffers. The recent cases of sensor failures that contributed to total system failure demonstrate the inherent interdependence between designing resilient systems and resilient of monitoring and control architectures. According to (Yoo et al. 2020) sensors cause problems and downtime in various aerospace engineering systems and have even contributed to plane crashes. These are key characteristics in the automated system making it even more important that they be studied early and in-depth.

Control systems increase the size and therefore the complexity of systems, and have a key involvement in initiating recovery in modern systems, particularly those that are automated. As a result, selecting the control system design that initiates recovery by designing the right connectivity between control and redundant nodes in a system is a significant consideration that has a direct impact on the system's resilience. System architecture methods and tools that focus on the control-redundancy-resilience requirements are needed because performing such analysis is not a simple task.

 https://doi.org/10.24868/11188

1.4. Research gap and aim

Network science approaches have been proposed in naval ship engineering literature to analyse vulnerability of ship distributed systems (Rigterink 2014, de Vos and Stapersma 2018, Paparistodimou et al. 2018, Brownlow et al. 2021). However, these existing methods do not offer a method that focusses on a dynamic analysis upon the resilience of the interwoven physical, functional, and control layers of a ship distributed system.

The aim of the paper is to support the system architectures process by creating a method that models the physical, functional, and control layers of systems together, facilitates the generation of options for system architectures, and provides a resilience assessment calculation. The results of the proposed method can help guide decisions about resilience, functional redundancy, and control architecture design during the system architecture process. The following Section 2 details the proposed method and illustrates the concept in Figure 2.

2. Methodology

The method proposed in the paper employs a triple layer network (physical, functional, and control). The physical layer represents the spatial system architecture, with disruption occurring at the physical layer and the consequences extending to the functional layer. The functional layer represents the functional flows and includes standby redundancy nodes, which are designed to recover in the event of a disruption. The control layer represents the control nodes. Standby redundant nodes initiate recovery only when they receive control node instructions via the network connectivity. A resilience metric is proposed for evaluating resilience at the functional layer. In the methodology presented herein, the experiments focus on the controlling aspects of the system. The function of a control node is to trigger the start-up of standby redundant nodes at the functional layer. The method enables the variation of the number of control nodes; their connectivity to the standby redundancy nodes enables the experimentation to identify improved resilient design solutions. Questions to be investigated include the placement of controllers and the interlinking of controllers and standby systems to optimise a measure of resilience subject to constraints on the level of redundancy. The resilience of the network is assessed by simulating disruptions at the functional layer in an exhaustive fashion. Post disruption control nodes trigger the start-up of standby redundant nodes at the functional layer. The resilience of the different control design options is assessed based on a resilience metric that measures if the required performance (specified by the user in terms of components whose function is essential) is satisfied post disruption. The methodology identifies control layouts at an early stage of the design process that can offer benefits for resilient behaviour.

2.1. Methodology Stages

Figure 1 illustrates the triple layer modelling approach with a simplistic example to aid the understanding of the methodology.

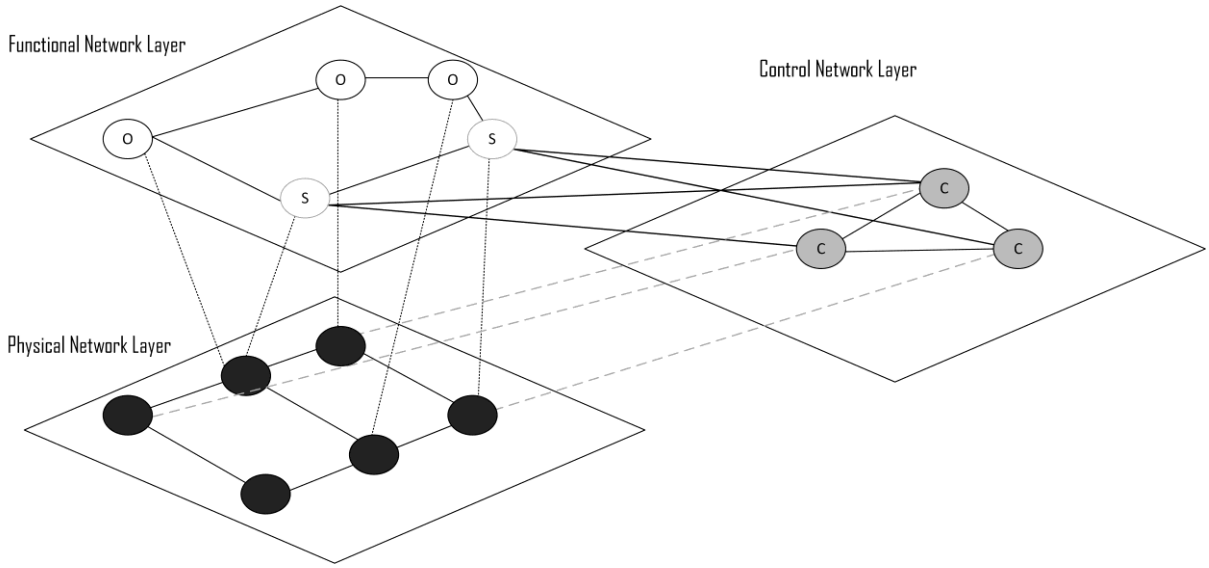


Figure 2: Triple layer modelling approach

 https://doi.org/10.24868/11188

The nodes in the functional network layer annotated with letter S indicate the standby redundant components, and the nodes annotated with the letter O show the operational components prior to disruption. The nodes annotated with the letter C in control network layer represent controllers. Table 1 presents an overview of the stages of the methodology which are implemented in MATLAB software environment.

Table 1: Methodology stages overview

	METHODOLOGY STAGE	EXPLANATION	INPUTS/OUTPUT
1	Definition of the functional network layer	Representing the functional elements and their links; a common approach to model system architectural functionality is using Design Structure Matrix. (Eppinger and Browning 2012, Paparistodimou et al. 2017).	***Input*** a. Number of functional elements. b. Interconnectivity of elements c. Construct Design Structure Matrix. d. Definition of standby redundant and operational functional elements. e. Definition of source and sink elements. f. Essential dependencies between sinks and sources for satisfactory and normal performance.
	Definition of the physical network layer	Representing the spatial dimensional layer as a grid network	***Input*** Number of potential sites in each dimension under consideration.
3	Definition of the control network layer	Representing the controllers as a network layer	***Input*** Total number of controllers (nc).
4	Definition of the standby links between control network layer and functional network layer	Representing the standby links between controllers and standby components ➢ Default Option is to assign standby links from standby components to their physically nearest controller(s). ➢ When increasing the standby links for a standby component the tool selects the additional standby link from the next physically nearest controller.	***Input*** Number of standby links between each standby component in the functional layer to each controller (s_{nc}) at the control layer.
5	Definition of the links between control network layer and physical layer.	Representing the location (as connectivity) of controllers on physical network. ➢ The controllers represent the centre of areas within the ship that a particular controller is controlling. ➢ Default strategy is to place controller physically near the neighbourhood of the standby redundant components they control.	***Input*** Physical locations for each of the controllers according to deck/zone.
6	Simulation of physical disruptions	Simulating disruption by removing the disrupted nodes (functional components and controller) and any associated edges of that node. ➢ Default controller disruption approach: the tool removes an increasing number of controllers from 1 to n_c, and measures the effect on resilience, producing the resilience curves.	***Input*** Number of components to disrupt in the functional layer in a combinatorial exhaustive approach, which means, for example for two components every possible combination of two components is disrupted in the functional network.
7	Simulation of recovery	Simulating recovery by a default approach that is a controller starts up standby redundancy post disruption.	***Output***
8	Calculation of resilience	Calculating resilience by a measurement measured based on the proportion of disruptive events for which performance is restored within an acceptable time. ➢ The proposed resilience metric measures performance in terms of level connectivity between sources and sinks previously defined by Paparistodimou et al. (2020a).	***Output***

 https://doi.org/10.24868/11188

2.2. Assumptions

A number of assumptions and simplifications are adopted to develop the proposed methodology. It is assumed that all controllers are linked to sensors receiving real time information. Sensors are not modelled in the methodology, but it is assumed that each physical node has a sensor attached to it. In addition, it is assumed that each controller receives timely information from sensors, and that controllers are immediately activated on receipt of a message from a sensor.

3. Case Study & Results

The case study presented herein models the power and propulsion systems of a generic naval ship with the addition of controllers (Figure 3) and is based on a medium redundancy technical system architecture as previously presented in Paparistodimou et al. (2020b). In Figure 3 components illustrated in black colour (annotated in white) show standby components and the standby links from controllers to standby components are annotated in grey colour. The number of controllers and number of standby links are the two design variables that are investigated in the case study.

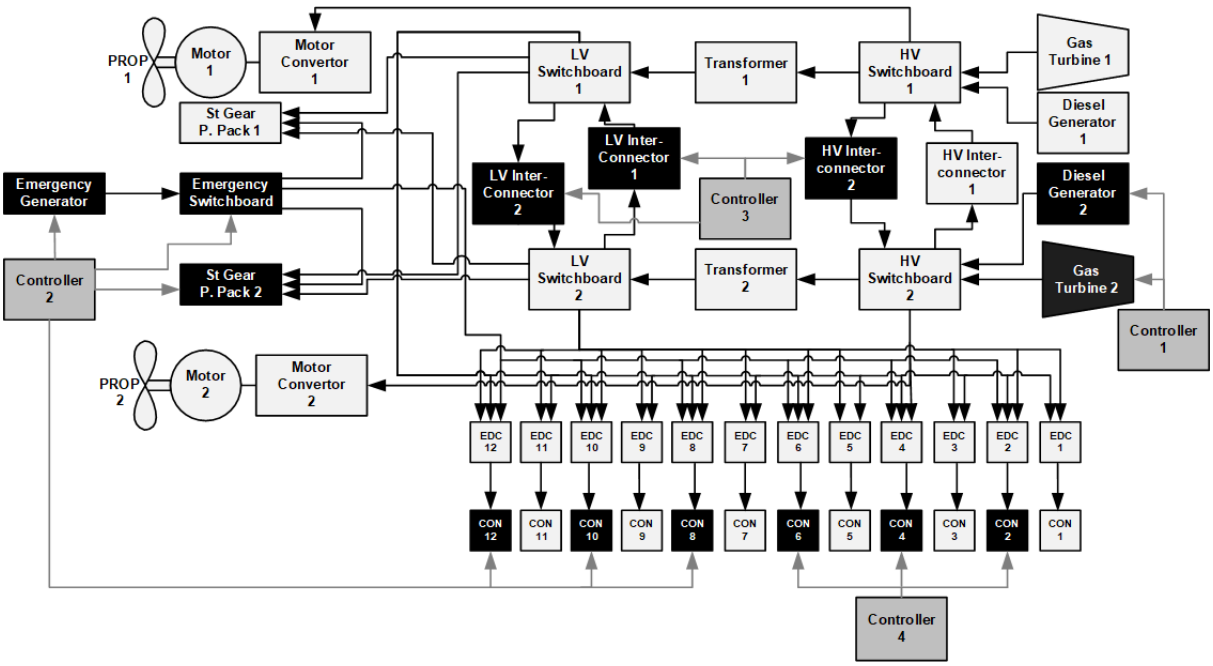


Figure 3: Generic power and propulsion system architecture (design option 1) adapted from Paparistodimou et al. (2020b)

In Figure 3 the generic power and propulsion system architecture design (design option 1) is varied systematically to create various design options based on Design of Experiment approach. The number of controllers is defined as Variable 1 and the standby connectivity between controllers and standby redundant components is defined as Variable 2 as shown in Table 2.

Table 2: Definition of Variable 1 & 2

Transformer	**Value 1**	**Value 2**	**Value 3**
Variable 1: Number of Controllers(n_c)	4	6	8
Variable 2: Standby links (s_{nc})	1	2	3

 https://doi.org/10.24868/11188

Based on the above definition of control system architecture variables, the following nine design options are devised. The resilience for each design option presented in Table 3 was calculated based on the resilience metric under combinatory physical disruptions. The resilience measure is an average of the resilience score as 1, 2, 3…n_c controllers are removed after the system suffers 3 components disruption (all combinations of components disruption are considered). The controllers are removed in several different patterns to give a better picture of what's happening.

Table 3: List of Generated Design Options

Transformer	**Variable 1**	**Variable 2**	**Resilience metric**
Design Option 1	n_c =4	s_{nc} = 1	0.5196
Design Option 2	n_c =4	s_{nc} = 2	0.6545
Design Option 3	n_c =4	s_{nc} = 3	0.7266
Design Option 4	n_c =6	s_{nc} = 1	0.5494
Design Option 5	n_c =6	s_{nc} = 2	0.6732
Design Option 6	n_c =6	s_{nc} = 3	0.7357
Design Option 7	n_c =8	s_{nc} = 1	0.5573
Design Option 8	n_c =8	s_{nc} = 2	0.6795
Design Option 9	n_c =8	s_{nc} = 3	0.7417

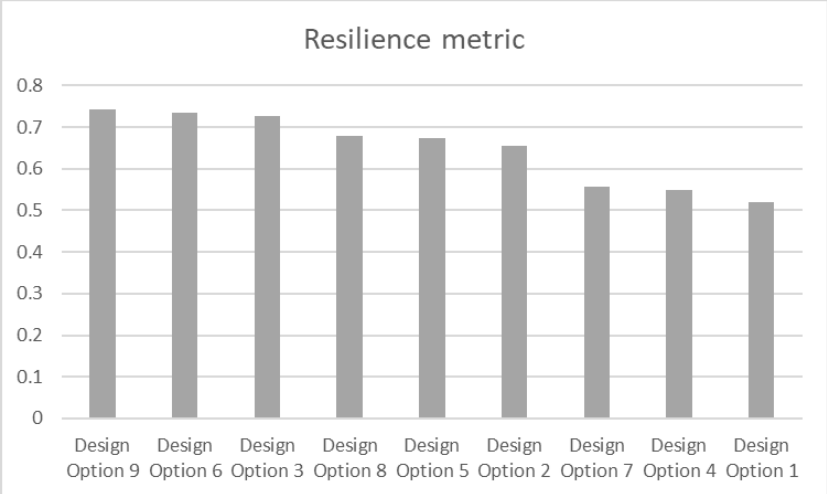


Figure 4: Resilience metric results for design option 1-9

Design option 9 in Figure 4 is shown to be the most resilient option which is as expected as it has the highest number of controllers and interconnections between controllers and standby components. Similarly, the least resilient option occurs with the least numbers of controllers and minimal connectivity. There is a difference in the effect on resilience between increasing the number of controllers and increasing the standby links. For example, the resilience between options 3, 6, 9 does not increase significantly even though the number of controllers increased, whereas the resilience of options 7, 8, 9 increases more notably with increase in the number of standby links between controllers and standby redundancy. Furthermore, while options 3 (n_c =4, s_{nc}=3) and 5 (n_c =6, s_{nc}=2) have exactly the same total number of links between controllers and components (3*4=6*2=12) there is a marked difference in resilience. Option 3, that has minimum number of controllers combined with maximum level of standby links, outperformed Option 5, that has the higher number of controllers with medium level of connectivity between standby redundant and controllers.

 https://doi.org/10.24868/11188

To illustrate these differences, Main Effects and Interaction Plots of Means were produced using Minitab, shown in Figure 5 and Figure 6 below.

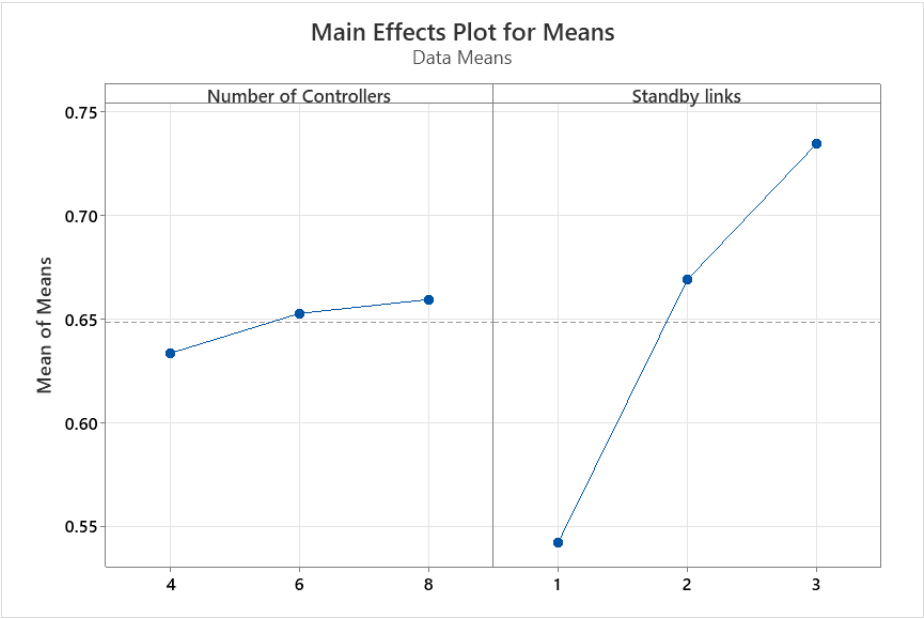


Figure 5: Main Effect Plots for Means

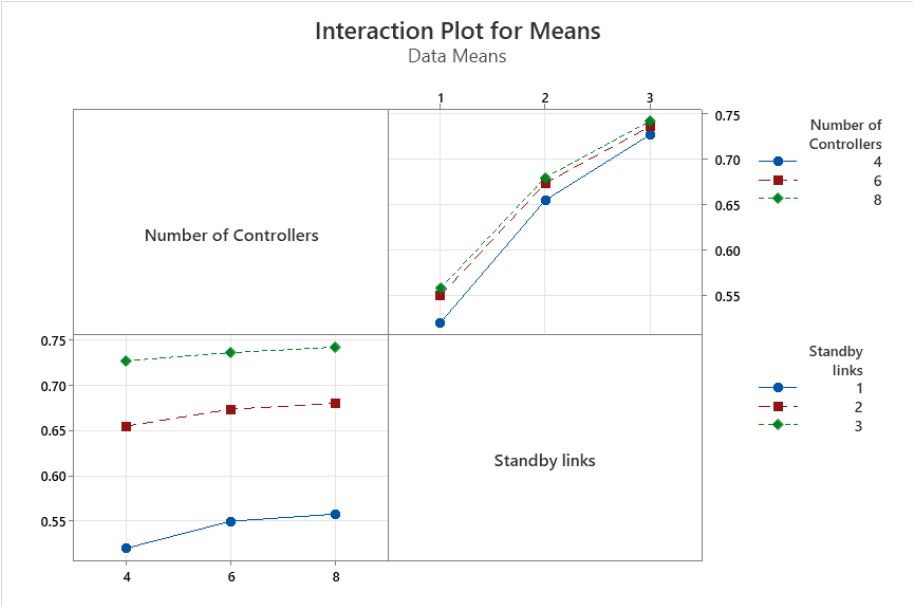


Figure 6: Interaction Plot for Means

In summary, the resilience results show that the level of interconnectivity between controllers and standby redundancy has a greater impact than the number of controllers. Such findings can provide useful insights during the early stages of design, when key design decisions are made, such as determining the number of control components and the number of standby connections between controllers and standby redundant components. This method is centred on the standby linkage, which is an important enabler of the post-disruption recovery process because it allows for reconfiguration, and thus improves system resilience.

Designing redundancy in system architecture centres on which parts to denote as redundant, the amount of redundancy at the component and interconnection, and the type of redundancy. Such redundancy decisions are made alongside other design considerations (Chen and Crilly 2014). The proposed method aids system engineering discussions by providing quantitative indicators for identifying design approaches that will provide the most

 https://doi.org/10.24868/11188

benefit in terms of redundancy at the lowest possible cost, as well as avoiding incorporating designs that will provide no significant benefit in terms of resilience.

The proposed methodology is suggested for use during the early design decision phase, before detailed information is available. The findings are limited to the system architecture under investigation and are not intended for generalisation. It is expected that any design options developed early on based on the method's results will be thoroughly examined using a multi- physics analysis approach.

4. Conclusions & Future Research

The paper describes a method for assessing resilience in the early stages of design by modelling the complex system using a triple-layer network approach. The method considers the physical, functional, and control aspects of the system. This paper applied the method to a generic naval system power and propulsion case study, with control elements included. The case study presented experiments with different numbers of controllers and levels of connectivity between controllers and standby redundant components. The goal was to examine how the control aspect influences the system's resilience. The findings revealed that increasing connectivity between controllers and standby redundancy had a greater impact on resilience than increasing the number of controllers.

The method is intended to help at the very early stages of design, when important decisions are made, but detailed analysis tools are not available. The results of applying the method can help designers choose systems that meet the design objectives without introducing ineffective additional redundancy and the associated costs.

The case study presented in this paper is simple but provides early evidence that the multilayer design approach can give a speedy indication of the benefits of different design option approaches. The study suggests that there is value in exploring further how best to arrange the controllers in the design, both in terms of their interconnections and also in terms of how the controllers are associated with each individual standby component. In this study, the assignment was performed on the basis of physical location of the various components, however it is possible to explore other approaches.

Future research will focus on combining resilience optimisation strategies on multiple levels, such as within the functional and/or controller layer, and simultaneously positioning components in these two layers with reference to the physical layer. This will allow for the identification of optimal multilayer architecture patterns at a very early stage of design. Another potential future direction is to improve resilience metrics to capture different stages of the recovery process while also incorporating various reconfiguration approaches.

5. References

Bertoni, V.B., Saurin, T.A., Fogliatto, F.S., Falegnami, A., and Patriarca, R., 2021. Monitor, anticipate, respond, and learn: Developing and interpreting a multilayer social network of resilience abilities. Safety Science, 136 (October 2020), 105148.

Brownlow, L.C., Goodrum, C.J., Sypniewski, M.J., Coller, J.A., and Singer, D.J., 2021. A multilayer network approach to vulnerability assessment for early-stage naval ship design programs. Ocean Engineering, 225, 108731.

Bertoni, V.B., Saurin, T.A., Fogliatto, F.S., Falegnami, A., and Patriarca, R., 2021. Monitor, anticipate, respond, and learn: Developing and interpreting a multilayer social network of resilience abilities. Safety Science, 136 (October 2020), 105148.

Brownlow, L.C., Goodrum, C.J., Sypniewski, M.J., Coller, J.A., and Singer, D.J., 2021. A multilayer network approach to vulnerability assessment for early-stage naval ship design programs. Ocean Engineering, 225, 108731.

Chen, C.C. and Crilly, N., 2014. Modularity, redundancy and degeneracy: Cross-domain perspectives on key design principles. In: 8th Annual IEEE International Systems Conference, SysCon 2014 - Proceedings. IEEE, 546–553.

Eppinger, S.D. and Browning, T.R., 2012. Design Structure Matrix Methods and Applications. Cambridge, MA, USA: MIT Press.

Estrada, E. and Knight, P., 2015. A First Course in Network Theory, 272.

Haimes, Y.Y., 2009. On the definition of resilience in systems. Risk Analysis.

Haley, B., 2014. Evaluating complex engineered systems using complex network representations.

Hollnagel, Erik, Pariès, J., Woods, D., and Wreathall, J., 2011. Resilience engineering in practice: A guidebook. Resilience Engineering in Practice: A Guidebook. Ashgate Gower.

INCOSE ed., 2023. INCOSE systems engineering handbook. John Wiley & Sons.

Office of the Assistant Secretary of Defense for Homeland Defense and Global Security, 2015. Space Domain Mission Assurance: A Resilience Taxonomy White Paper. Federation of American Scientists, (September), 1–10.

Paparistodimou, G., Duffy, A., Knight, P., Whitfield, I., Robb, M., and Voong, C., 2018. Network-based metrics for assessment of naval distributed system architectures.

 https://doi.org/10.24868/11188

Paparistodimou, G., Duffy, A., Voong, C., and Robb, M., 2017. System Architectures Assessment Based On Network Metrics. In: 19th International Dependency and Structure Modeling Conference, DSM. Aalto University Design Factory, Finland.

Paparistodimou, G., Duffy, A., Whitfield, R.I., Knight, P., and Robb, M., 2020a. A network tool to analyse and improve robustness of system architectures. Design Science, 6, e8.

Paparistodimou, G., Duffy, A., Whitfield, R.I., Knight, P., and Robb, M., 2020b. A network science-based assessment methodology for robust modular system architectures during early conceptual design. Journal of Engineering Design, 31 (4), 179–218.

Rigterink, D., 2014. Methods for Analyzing Early Stage Naval Distributed Systems Designs, Employing Simplex, Multislice, and Multiplex Networks. The University of Michigan.

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

Wied, M., Oehmen, J., and Welo, T., 2020. Conceptualizing resilience in engineering systems: An analysis of the literature. Systems Engineering, 23 (1), 3–13.

Yodo, N. and Wang, P., 2016. Engineering resilience quantification and system design implications: A literature survey. Journal of Mechanical Design, 138 (11).

Yoo, M., Kim, T., Yoon, J.T., Kim, Y., Kim, S., and Youn, B.D., 2020. A resilience measure formulation that considers sensor faults. Reliability Engineering and System Safety, 199 (September 2017), 106393.

 https://doi.org/10.24868/11188