A Framework for Resilience-Informed Decision-Making in Early Design

Daniel Hulse

Oregon State University, Corvallis, OR
hulsed@oregonstate.edu

ABSTRACT

Early in the design process, informed decisions must be made to ensure that the developed system will be resilient—that is, capable of preventing, mitigating, or recovering failures. However, at this phase of design, many options exist to achieve resilience, each with different effects on the system's fault response, performance, and difficulty to implement. As a result, it is important to be able to quantify the value of a design's resilience so that it can be traded off against these other concerns. Advancements in the capabilities of Prognostics and Health Management, fault-tolerant control and related technologies have enabled a variety of novel prevention and recovery features that require an understanding of the system's structure and available functions during operation to consider properly. This work aims to develop modelling and design frameworks enabling the consideration of these features, such as system reconfiguration, functional redundancy, operational failure avoidance, and goal change early in the design process. Such design frameworks will show which designed features are most appropriate in the system and will account for the uncertainty of assumptions made in early design phase.

1. PROBLEM STATEMENT

There has been a recent push to increase the resilience of engineered systems, due to perceived shortcomings in traditional reliability engineering. While reliability engineering focusses on the avoidance of risks, it has not provided approaches to mitigating unavoidable or difficult-to-avoid risks (Clark-Ginsberg, 2016). Engineering resilience has been put forward as a more comprehensive approach to risk in which, instead of attempting to avoid failure at all costs (at the expense of system complexity, performance, and capital costs), the system is designed to additionally mitigate and recover from faults when they occur (Haimes, 2009). Increasing the resilience of engineered systems accordingly could lead to more economical systems, when appropriate.

Simultaneously, recent developments in prognostics and health management technology have led to new paradigms about how engineering assets can be managed to avoid failure. Systems with online condition monitoring can now be controlled to proactively avoid failures through active maintenance and changes to usage patterns, rather than setting fixed maintenance and replacement schedules (Kim, An, & Choi, 2017). Designing engineered systems for resilience as a result requires not just a consideration of recoverability in the system, but of the ability of PHM systems to manage risk on-line (Yodo & Wang, 2016).

In the design of new complex engineered systems, the consideration of resilience must happen early in the design process, when there is most freedom to explore design alternatives. Design research has shown that early system-level design decisions about system functionality, architecture, and requirements have large impacts on the future success of the project, since the resulting design is locked-in to these high-level choices (Tan, Otto, & Wood, 2017). Since system resilience is critical to the economy of the engineered asset and its ability to meet external reliability and availability requirements, resilience should be considered in the early design phase rather than attempting to add-on resilience post-design.

This research will approach the problem of incorporating resilience in the early design of engineered systems. The goal is to provide a framework that will allow designers to consider alternative design options and functionalities, such as PHM systems, failure or fault-tolerant controllers, automated safety systems, or traditional redundancy circuits to determine which is most appropriate for the given design problem. The main challenges for early resilient design include representing and modelling system resilience and the effect of different system functionalities, making resilience-informed decisions that account for the trade-offs between design effort, failure risk, recovery, and performance, and ensuring that the results of design process are not overly hindered by the significant uncertainties present in the early design phase.

2. EXPECTED CONTRIBUTIONS

The overarching contribution of this work is a design process to incorporate resilience in the early design of an engineered system. This research will pursue three major questions:

- How can a system be modelled in the early design phase to incorporate resilience?

A variety of techniques to design for risk for early design have been put forward in previous research that generate the fault response of a system based on its functional model—an early design representation—for automated functional hazard assessment (McIntire, Keshavarzi, Tumer, & Hoyle, 2016). However, these techniques have not incorporated important properties required to model the effect of different design options on overall system resilience. A contribution of this research will be to incorporate the modelling tools required to make this decision, by incorporating rate and severity information to determine the effect of monitoring and proactive maintenance approaches enabled by PHM, including both preventative and repair actions the system may perform to mitigate the fault and the effect of potential errors introduced by these systems when faulty.

- How can resilience be incorporated in the decision-making process to choose between different design solutions?

To incorporate trade-offs between cost, risk, and performance in decision-making, decision-based and value-driven design processes have put forward expected utility (Hazelrigg, 1998) and expected cost (Collopy & Hollingsworth, 2011) as comprehensive metrics for decision-making. A contribution of this work will be the adaptation of these methods to quantify the costs associated with resilience-informed fault model results and to trade the resilience of the system against design effort and performance. This design process will further showcase the ability for these methods to find the fault management strategy most appropriate for a given design solution among many.

- What must be known about a system to make resilience-informed design decisions without the results of the decision being overly prone to underlying uncertainty in the information?

An important topic of study in design research currently is the validation of design methods. While many risk-based design and modelling approaches have been presented, there has been skepticism about whether decisions can be meaningfully made given the many uncertainties present in the early design phase (Fadel, Summers, Mocko, & Paredis, 2016). A contribution pursued in this research will be providing a framework to check whether resilience-based design processes were meaningful by quantifying the effect of uncertainty on the decision process by adapting the value of perfect information metric presented by (Bradley & Agogino, 1994). This approach will allow designers to determine when an early design process was effective and when more information should be sought out before making a final decision.

3. RESEARCH PLAN

Each of the previously mentioned research questions will be approached as individual tasks and then brought together in a single unifying case study in the final dissertation. While a significant amount of work has been performed towards the development of this method (both completed and in progress) regarding the design decision-making process and uncertainty consideration, more work needs to be performed to develop the underlying modelling framework to allow consideration of the resilience of a variety of different novel design features. Further work may enable the adaptation of these tools for novel design practices, such as multidisciplinary design optimization.

3.1 Work Performed

Work has already been performed towards quantifying the cost of different design solutions for use in a design decision-making process. A general framework for optimization and design selection was provided based on the expected cost of fault model results (Hulse, Hoyle, Goebel, & Tumer, 2018a). Preliminary results have shown that incorporating failure-mitigating features in the design can drastically increase design value when the cost of failure is high, justifying the use of risk-based design processes in the early stages of design (Hulse, Hoyle, Goebel, & Tumer, 2018b). This work is complete and has been published. Ongoing work is using the quantified uncertainty in these expected cost measures in the context of a design selection process to show which design decisions in a system are meaningful and which require more information to be made appropriately. Preliminary work and a case study have been developed for this approach in the context of continuous parameter uncertainty, and ongoing work is developing the method for uncertainty about discrete assumptions. This work is expected to be complete by Fall 2019.

3.2 Remaining Work

The remaining work is to develop the resilience-informed modelling approach, demonstrate the overall modelling, design and validation framework in a detailed case study, and adapt the framework to design processes. Developing the modelling approach will involve modifying current function-based fault modelling tools to incorporate resilience and is

expected to be complete by Winter 2020. It is expected that the development of this modelling framework will culminate in a publicly available toolkit for fault propagation and resilience assessment that will enable future collaboration. A detailed case study will be developed concurrently with the modelling approach to showcase both the capabilities of the modelling approach and provide a single reference application that can be followed through each step of the design process in the final dissertation manuscript. This case study is expected to be complete by Spring 2020. Finally, there are novel design framework applications and modelling considerations that may be addressed in this work, including applications of multidisciplinary design optimization and decomposed design processes in risk-based design and the incorporation of human-PHM interactions in resilience models. The development of these approaches is ongoing and expected to be complete by Summer 2020 when the work is complete.

4. CONCLUSION

This work will find methods to design resilience into engineered systems in the early phases of design. Much work in the prognostics and health management fields has focused on the use of the technology to retrofit existing systems. However, in the design of new systems, there is much to gain from considering failure and risk-mitigating features early in the design process to enable the integration of these features with the rest of the system. This work will study the methods required to model resilience in a system and make decisions based on this quantified resilience about which features to add in a system, with a focus on ensuring that the process is not overwhelmed by the uncertainty associated with early design assumptions. The expected result of this framework is that designers will be able to rationally justify the use of PHM systems and other resilient features in the design process to enable the design of these systems to occur concurrently with the rest of the system in an integrated way.

REFERENCES

Bradley, S. R., & Agogino, A. M. (1994). An Intelligent Real Time Design Methodology for Component Selection: An Approach to Managing Uncertainty. *Journal of Mechanical Design*, *116*(4), 980–988. https://doi.org/10.1115/1.2919508

Clark-Ginsberg, A. (2016). What's the Difference between Reliability and Resilience? *Stanford University, Tech. Rep*.

Collopy, P. D., & Hollingsworth, P. M. (2011). Value-driven design. *Journal of Aircraft*, *48*(3), 749.

Fadel, G., Summers, J., Mocko, G., & Paredis, C. (2016). *The Circle of Design: An NSF sponsored workshop on Education, Validation and Dissemination, and Research Directions in Engineering Design and Systems Engineering held at Clemson University, Clemson, South Carolina.* (p. 34). Retrieved from Clemson Engineering Design Applications and Research website: http://www.clemson.edu/centers-institutes/design/workshop/docs/The%20Circle%20of%20Design.pdf

Haimes, Y. Y. (2009). On the Definition of Resilience in Systems. *Risk Analysis*, *29*(4), 498–501. https://doi.org/10.1111/j.1539-6924.2009.01216.x

Hazelrigg, G. A. (1998). A Framework for Decision-Based Engineering Design. *Journal of Mechanical Design*, *120*(4), 653–658. https://doi.org/10.1115/1.2829328

Holling, C. S. (1996). Engineering resilience versus ecological resilience. *Engineering within Ecological Constraints*, *31*(1996), 32.

Hulse, D., Hoyle, C., Goebel, K., & Tumer, I. Y. (2018a, August 26). *Optimizing Function-Based Fault Propagation Model Resilience Using Expected Cost Scoring*. V02AT03A052-V02AT03A052. https://doi.org/10.1115/DETC2018-85318

Hulse, D., Hoyle, C., Goebel, K., & Tumer, I. Y. (2018b). Quantifying the Resilience-Informed Scenario Cost Sum: A Value-Driven Design Approach for Functional Hazard Assessment. *Journal of Mechanical Design*, *141*(2), 021403-021403–021416. https://doi.org/10.1115/1.4041571

Kim, N.-H., An, D., & Choi, J.-H. (2017). *Prognostics and Health Management of Engineering Systems*. https://doi.org/10.1007/978-3-319-44742-1

McIntire, M. G., Keshavarzi, E., Tumer, I. Y., & Hoyle, C. (2016). Functional Models With Inherent Behavior: Towards a Framework for Safety Analysis Early in the Design of Complex Systems. *ASME 2016 International Mechanical Engineering Congress and Exposition*, V011T15A035–V011T15A035. American Society of Mechanical Engineers.

Tan, J. J. Y., Otto, K. N., & Wood, K. L. (2017). Relative impact of early versus late design decisions in systems development. *Design Science*, *3*. https://doi.org/10.1017/dsj.2017.13

Yodo, N., & Wang, P. (2016). Engineering Resilience Quantification and System Design Implications: A Literature Survey. *Journal of*

Mechanical Design, *138*(11), 111408-111408–
111413. https://doi.org/10.1115/1.4034223