Function-Based Failure and Flow State Reasoning for Robust PHM Development

David C. Jensen, Advisor: Irem Y. Tumer [1]

[1] *Complex Engineering Systems Design Lab Oregon State University, Corvallis, OR, 97331, USA*
jensend@onid.orst.edu and irem.tumer@oregonstate.edu

1 OVERVIEW

The role of health management can be dissected into identifying faults and then acting to mitigate the impact of faults. Often the approach taken to developing a prognostics and health management subsystem occurs after the rest of a system design has been refined to a high level of precision. While this can be beneficial to fault identification goals of PHM in that many components have known failure characteristics, this post-design approach is also limiting. When PHM considerations are included in the design of the system it is possible to make system design decisions based on failure detectability as well as mitigation effectiveness. The difficulty of incorporating PHM considerations into early design is mainly due to the lack of specific fault information and system-level failure characterizations. The field of function-based failure analysis has been developed in recent years to provide designers with information on system failures in the early stages of system development that can be used to make risk-informed design decisions. Recent advancements in this field have extended the ability of function-based failure analysis to include the effects of failures propagating through a system. Considering these advancements, the information gained from a failure propagation analysis in the design stage can be used to develop PHM systems. The benefits of this type of approach could apply to both the PHM system and the physical system. PHM subsystems would benefit by reducing development costs when designed concurrently with the rest of the system. Early component failure information would assist fault identification and PHM fault mitigation procedures can be simulated to evaluate the effectiveness of the fault response. The system development would benefit from this approach by optimizing physical design for failure detectability, reduced failure impact, and fault mitigation effectiveness.

2 FUNCTION FAILURE AND FLOW STATE REASONING

Previous work has identified function-based failure analysis as a means for determining risk and fault impact in the design stage. Refinement of these methods have led to the ability to identify and simulate the impact failures that propagate through the system. This has been achieved with a modeling and simulation framework that maps specific component fault modes to failed states of the designed system functions by means of function failure reasoning. While function failure reasoning has been shown to be a useful tool for evaluating the propagation and impact of failures, part of this research has identified a key limitation of this type of approach.

Implicit in the concept of failure propagation is that there are specific paths that a failure can be described as following, affecting one component and then another. Design stage approaches that investigate failure propagation use the nominal operating system representation to model both the system and the failures that affect that system. Failure propagation analysis that is limited to the designed (expected) flows in the system representation fails to capture potential flow paths. For example a failure in one component might reasonably be expected to affect the next nominally connected component; function failure reasoning can capture the effect of this propagation. However, many failures can propagate to components that would not be connected in the nominal system representation, such as in the case of a fluid leak, short circuit, or an explosion. While some of these failures are rare, the potential impact warrants their inclusion into a thorough risk analysis framework. As part of this research the Flow State Logic (FSL) reasoning method was developed to meet this short coming in function-based failure propagation analysis methods.

Flow State Logic reasoning identifies and characterizes energy, material, and signal (EMS) flows as part of a failure simulation by characterizing both potential and designed flows(those represented in the nominal system representation). Additionally this method defines component behavioral models based on operating mode changes that occur as a result of input

EMS flow types and levels. The combination of these two elements into a function failure reasoning method provides meaningful results for a number of different types of failure scenarios. For example, a known failure mode for a generic valve component is defined as a ”leak.” Including the FSL methodology into an analysis would provide results on the impact of the material leak when it affects other components in the system. Further, with the FSL methodology, a failure state could be identified and analyzed of when the system experiences specific EMS flows from its environment.

3 APPLICATION OF INITIAL RESULTS TO PHM

Initial research has applied this methodology to a simple electrical power system and an initial controlled liquid fueled rocket engine design. The electrical power system was designed to be similar to the Advanced Diagnostic And Prognostics Testbed (ADAPT) and provides numerous sensor outputs. Expected future work will demonstrate how these sensor values can be compiled early in the design stage to give PHM developers a library of failure characterizations. Apply the FSL methodology to the liquid fueled rocket engine design provided many useful insights into the use of FSL and function-based failure analysis for PHM. Specifically, a simple software control subsystem was incorporated into the system simulation. The results of applying failure scenarios to the simulation revealed the impact of the control behavior from a functional perspective. This simple controller can be seen as a PHM subsystem. These results show that incorporating PHM responses to sensor data into the simulation would provide designers with a means of evaluating responses and optimizing PHM reactions. Related to this area of expected future work is the inclusion of expected human behavior and the evaluation of operating protocols with respect to fault mitigation.

4 FUTURE DEVELOPMENTS

Future work for this research will include the design and development of an electrico-mechanical actuator testbed. The methodology discussed in this abstract will be used to identify all of the failure modes and effects for the actuator component as well as optimize the testbed for fault detectability. When the testbed is physically completed actual failure results will be compared to those predicted by the initial simulation. Additionally the simulation results are expected to show how mitigation of actuator failures affects system functionality. These results will also be verified with real observations.

An additional area of continuing research is the inclusion of time to failure and PHM reaction time. At the current state of this research failure scenarios consist of a set of discrete time steps and failures either exist and are propagated or they have not yet been injected into the simulation. An important next step is addressing PHM response to failure is the inclusion of the relative time a failure takes to propagate through a system. PHM response can be developed to incorporate the a concept of relative time to impact.

Finally, part of effective health management is the reaction to failures with the goal often being autonomous repair. The initial work described here has focused on specific subsystems that would normally be part of a larger, more complex system. An area of interest for this research is the ability to provide designers with top-level PHM response evaluation. The goal of this aspect of the research would be to identify optimal PHM response to failure considering the overall functions of the system. For example, this might include comparing repair of a subsystem versus utilizing a different subsystem to achieve the same functionality. Further expansion of this work may even provide designers with suggested failure responses based on natural or previous designed systems.

5 CONCLUSION

This research has developed the Flow State Logic (FSL) reasoning method to complete a function-based failure propagation analysis in the design stage. The initial results from an electrical power system testbed and controlled liquid fueled rocket engine designs indicate that PHM development would benefit from early system failure information. Alternatively, these results indicate that inclusion of health management into early failure propagation analysis can be use to optimize both the PHM response as well as the physical system with respect to risk. Future work will demonstrate these benefits by incorporating PHM subsystem into design. However, several important factors related to evaluating PHM response have yet to be incorporated into the current methodology. Addressing these unfulfilled areas and refining the method with respect to PHM represent the future work of this research.

6 RESEARCH PUBLICATIONS

The research leading to this abstract has resulted in three conference papers and one journal paper. Papers have been accepted to the 2008 ASME International Mechanical Engineering Congress and Exposition and the 2009 International Design Theory and Methodology Conference as part of the ASME Design Engineering Technical Conferences. Papers are in review for the 2009 Prognostics and Health Management Conference and the Journal of Research in Engineering Design.

ACKNOWLEDGMENTS

This research is supported by the Air Force Office of Scientific Research under Grant Number AFOSR FA9550-08-1-0158. Any opinions or findings of this work are the responsibility of the authors, and do not necessarily reflect the views of the sponsors or collaborators.