Design of an Electrical Power System using a Functional Failure and Flow State Logic Reasoning Methodology

David C. Jensen [1], **Irem Y. Tumer** [1], **and Tolga Kurtoglu** [2]

[1] *School of Mechanical, Industrial, and Manufacturing Engineering, Oregon State University, Corvallis, OR, 97331, USA*
jensend@onid.orst.edu and irem.tumer@oregonstate.edu
[2] *Mission Critical Technologies, NASA Ames Research Center, Moffett Field , CA, 94035, USA*
tolga.kurtoglu@nasa.gov

ABSTRACT

Knowledge about failures and failure propagation paths in early design can benefit Prognostics and Health Management (PHM) system development by identifying expected system failures, determining adequate system monitoring, and improving system reliability through hardware configurational changes. Function-based failure analysis provides a means for early system representation that can provide meaningful results for failure analysis. Function-based failure analysis methods model failures propagating between components based on shared energy, material, and signal (EMS) flows. Limiting these connections to the designed system representation limits the scope of failure impact and propagation analysis. This paper presents a method of defining and reasoning on flow states for designed and potential EMS flows and using this information to determine impact and propagation behavior for failures based on early design information. To demonstrate the value of this approach, an electrical power system design is developed and analyzed as a case study. The initial results presented in this paper specifically benefit the development of PHM by providing simulated system behavior for a wide scope of propagation paths and by identifying the impact of failures with respect to system functions.

1 INTRODUCTION

Prognostics and health management (PHM) provides complex systems with the ability to mitigate the effect of failures, thereby reducing the risk of failure and improving reliability. The role of PHM can be dissected into identifying faults and then acting to mitigate the impact of faults. Often the approach taken to developing a 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 the lack of specific fault information and system-level failure characterizations.

While numerous methods exist for analyzing and quantifying the risk and reliability of systems, the greatest benefit in terms of failure mitigation comes from reliability methods that are applied in the design stage. Combining early failure analysis with PHM development offers two advantages. First, PHM development benefits from the failure state characterization results from reliability analysis. Second, system component and configuration design can be optimized to reduce risk with less expense in the design stage compared to any other stage of product development. Including PHM considerations into design stage reliability analysis increases the importance of the concept of failure propagation within the system. Since, health management techniques are generally applied to the system level, design stage failure analysis must provide results at the system level and not be limited to single point failures.

To realize the mutual benefits of early PHM development and system reliability analysis, methods of design stage failure analysis are beginning to be developed (Kurtoglu *et al.*, 2008). Most methods of design stage failure analysis utilize a functional approach to system representation models (Kurtoglu and Tumer, 2008a; Jensen *et al.*, 2008; Huang and Jin, 2008; Hutcheson *et al.*, 2006; Krus and Grantham Lough, 2007; Kurtoglu and Tumer, 2008b; Grantham-Lough *et al.*, 2008; Meshkat *et al.*, 2007; Stone *et al.*, 2005; Tumer and Stone, 2003). In their traditional use, these models capture the transformation of energy, material and signal (EMS) flows within a system under operational or nominal conditions. This presents a fundamental limitation for function-based system models to be used for reliability analysis, which focuses not on the nominal, but almost completely on the fail-

ure design space. This paper asserts that methods of failure analysis that are limited to nominal state system representation generally fail to capture the failure propagation paths not explicitly identified in the design representation. For many real failures this representation is inadequate to reflect faults that propagate along unidentified EMS paths. For example real material leaks and electrical shorts introduce EMS flows in a system that are not reflected by the nominal state representation of the functional model. Some design research work has focused on formalizing the language of functional representation (Functional Basis) (Hirtz *et al.*, 2002). The function-flow relationship of new EMS flows created by failures can not be formally described from the functional perspective as there is no consistent logical construct of how a function changes when acting on different EMS flows.

The goal of this paper is to address the limitation of this nominal system behavior representation by tracking the state of all flows in a system. In this light, this paper introduces the Flow State Logic (FSL) method, which provides a method of logic reasoning based on EMS flows to capture failure propagation along paths that are not considered in the original design. The FSL method in this paper is shown to augment an existing function-based failure analysis method to capture effects of failures following EMS flow paths beyond those represented in the functional model. The Function-Failure Identification and Propagation (FFIP) framework introduced in prior work (Kurtoglu and Tumer, 2008a) to provide the foundation for assessing the impact of component level failures at the functional level. Augmenting this approach with the FSL method provides a more complete picture of system reliability in the design stage. Furthermore, the results from this analysis can be used to design effective health management responses to faults. In this way system design and health management development can have a symbiotic relationship with the overall goals of lower risk and safer system operation. Implementing this type of approach in the design stage allows the system architecture to be optimized in order to reduce the effect of failure. Further, health management systems can be provided information in the design stage necessary to mitigate failures beyond what can be addresseed through hardware and configurational optimization.

1.1 Overview

In the following sections, we first review the related work in reliability methods and fault mitigation approaches to summarize the current state of the art. The underlying concept of Flow State Logic (FSL) is the classification of Flow States which is outlined in the next section. The resulting flow characterizations allow for flow state failure analysis. With this groundwork in place, we then present the methodology of tracking failure propagation along failure-induced flow paths. To demonstrate the benefits of implementing the FSL methodology for PHM development, an example Electrical Power System (EPS) is developed and analyzed using the presented framework. The EPS system is based on the Advanced Diagnostic and Prognostics Testbed (ADAPT), and the analysis results provide insight to guide PHM development.

2 RELATED WORK

2.1 Approaches to Health Management

For health management systems to be capable of fault mitigation they must first be capable of correctly diagnosing faults. Fault diagnosis is the process of determining the cause of any abnormal or unexpected behavior in a complex system (Patterson-Hine, 2005). The field of fault identification and mitigation used for health management systems has developed in two ways. (de Kleer and Kurien, 2003). The first is a high-level approach using model-based diagnosis (MBD), where a system is monitored and a comparison is performed of observed and expected behavior of the system to detect anomalous conditions usually with the goal of run-time repair (Patton *et al.*, 1998). MBD is based largely on early work in qualitative physics and qualitative reasoning (Weld and de Kleer, 1987; Forbus, 1984; Kuipers, 1986; Struss, 1988) The second aspect is a research community that focuses on fault detection and isolation. This area is primarily concerned with analyzing diagnosability and testability of the system and what instrumentation is needed to accomplish diagnostic functionality. Testability analysis is usually performed before any tests are designed and is based on the physical topology of the system and proposed instrumentation locations. Tools in this field use models, which capture the physical connectivity of system components and map failure modes and instrumentation points onto a dependency graph (Deb *et al.*, 1995). Expert systems are extensively used in diagnosis, where knowledge acquired from human experts is formulated in different ways such as if-then rules or decision trees (Giarratano and Riley, 2004), and statistical and probabilistic classification methods are applied where physical behavioral is difficult to model in analytical form (Yairi *et al.*, 2001; Berenji *et al.*, 2003).

2.2 Function-Based Approaches to Reliability

To enable the analysis of failure potential during early design, functional modeling has been introduced in prior work as a basis for system representation for the majority of design stage reliability methods. Functional modeling is a system representation method, developed as a means to enhance the concept generation stage of product design (Pahl and Beitz, 1996). Using this approach, designers identify specific functions that a product must accomplish and connect these functions in a block diagram with the EMS flows that are transformed by the functions. Functional modeling has also been used in reverse engineering methods

such as the Force Flow Analysis (Greer *et al.*, 2004; Otto and Wood, 2001). This method dissects products into components and the forces acting on and between components and finally into the functions that components embody. Most of the function-based methods in the research community make use of the Functional Basis (Hirtz *et al.*, 2002; Stone and Wood, 2000) in order to provide a standard taxonomy for concept design and avoid the use of designer specific function and flow descriptions. Based on the usefulness of functional modeling for system representation in early design, it has also been used as part of the system representation in many early design reliability methods.

The first method that proposed a function-based approach to failure analysis was the Function Failure Design Method (FFDM) (Tumer and Stone, 2003; Stone *et al.*, 2005). In FFDM, the functional model is developed to represent the system design, which serves as a basis for generating configuration concepts of component implementations of function. Based on historical failure data for these types of components, it is then possible to establish likely failure modes for a given function. However, because historic failure data for components is configuration-specific, failure propagation is difficult to incorporate into an analysis, limiting the method to single, independent faults.

Several other methods built upon the FFDM methodology. Hutcheson et al. introduced a methodology to enable the design of health monitoring modules concurrently with system conceptual design to reveal, model, and eliminate associated risks and failures (Hutcheson *et al.*, 2006). Also the Risk in Early Design (RED) methodology determined functional-failure likelihood and consequence-based risk assessment to identifying high-risk and low-risk function-failure combinations (Grantham-Lough *et al.*, 2008).

Connecting component failure and risk to a functional model for design stage reliability was also shown by Meshkat et al. using a commercial systems engineering tool, CORE (Meshkat *et al.*, 2007). Using this method, functional models are related to dynamic fault trees to correlate historic risk and failure mode data of components to implemented functions. As with previous empirical approaches, model accuracy in this work is directly related to depth and applicability of historical data.

2.3 Failure Propagation Analysis in Design

A limitation of these previous methods is the singular and independent nature of the failure capable of analysis. To overcome this limitation, other research efforts have focused on including the propagation of failure in the analysis. As a direct extension of FFDM and RED introduced above, a failure propagation method was introduced by Krus and Grantham-Lough (Krus and Grantham Lough, 2007) to develop failure propagation mapping based on historical data using a functional model for system representation. This method adapted the element of common interfaces from change prediction (Clarkson, 2004) to apply to the functional level. This method explicitly defines failures as propagating along the designed flow paths.

A related approach (Wang and Jin, 2002) presented a Bayesian network analysis tool for evaluating the properties of function structures based on dependencies between flows and functions. In this method, the causation relationship is identified between a flow and every functional failure for each identified high-level function. Failure propagation is analyzed using a Function Event Network of all possible causation relationships in the function structure. This type of approach allows for a probabilistic analysis by applying a statistical reliability to the failure of each function in the function structure. An extension of this work is the Conceptual Stress and Conceptual Strength Interference Theory (CSCSIT) method (Huang and Jin, 2008), where the conceptual strength of a function is the ability of a function to continue to operate while under normal energy, material and signal (EMS) flows. In this method, conceptual stresses are the EMS flows in the function structure. The application of interference theory is used to define functional faults as when the output flow from a function is out of a specified normal range.

Finally, the Function-Failure Identification and Propagation (FFIP) framework was introduced (Kurtoglu and Tumer, 2008a; 2008b) as a design stage method for reasoning about failures based on the mapping between components, functions, and nominal and off-nominal behavior. The goal of the FFIP method is to identify failure propagation paths and map component failure states to function health. This approach does not rely on a historical database but instead uses a failure simulation method for determining fault propagation paths and the risks associated with them, providing the designer with the possibility of analyzing functional and component failures and reasoning about their effects downstream in a design based on their nominal and failed state behavior. In this paper, FFIP is used as a starting point, and hence will be explained in more detail in the next section.

As an extension of the FFIP method, the Function-Failure Reasoner (FFR) method was developed to quantify the effect of failures and compare design alternatives (Kurtoglu and Tumer, 2008b). This method introduces Function Failure Impact (FFI) as the quantitative description of FFIP scenario results, providing designers with a means to indicate the relative importance of each function. In this paper, the impact of fault scenarios simulated with the FSL method use FFI values to quantify the results.

3 FLOW STATE LOGIC METHODOLOGY

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 rep-

resentation 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 impact warrants their inclusion into a thorough risk analysis. As part of this research, the Flow State Logic (FSL) reasoning method was developed to meet this shortcoming in function-based failure propagation analysis methods.

Flow State Logic reasoning, introduced in this paper as an effective means to design PHM systems, identifies and characterizes energy, material, and signal (EMS) flows as part of a failure simulation, 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 when the system experiences specific EMS flows from its environment.

3.1 System Representation

In this paper, FFIP, discussed in Section 2.3 (Kurtoglu and Tumer, 2008a), is used as a starting point to provide the system representation, including the functional and configurational layouts. The goal of the FFIP framework is to link failure propagation to the ability of a design to provide the desired functionality. Therefore, the first step of the FFIP method is to decompose design requirements into a functional model (FM). This functional decomposition is elaborated to the point where generalized components can be identified to embody all functions. The generalized components are modeled using a component Configuration Flow Graph (CFG) which is related to the FM by the Energy, Material, and Signal (EMS) flows. That is, the EMS flows that connect functions in the FM are identical to the EMS flows between the generalized components that embody those functions. A simulation of the system is then created by linking behavioral models for each component according to the configuration identified in the CFG. The final module of the FFIP framework is the Function Failure Logic (FFL) reasoner. This reasoner evaluates the input and output flows of a component behavioral model and relates these to the operative state of the functions that the component embodies. With this framework in place, critical scenarios or failures of interest to the designer can be simulated to provide information about the functional health of the system (Kurtoglu and Tumer, 2008a).

This paper also uses some of the quantifiers that were introduced as part of the FFR method , described in Section 2.3 (Kurtoglu and Tumer, 2008b). Specifically, the Function Failure Impact (FFI) is calculated as the cost of a function's state multiplied by the function's criticality rating, summing over all functions in the system. Function Criticality Ratings (FCR) are defined by designers based on relative importance and can be assigned in the functional decomposition and the FM. The relative cost of function states is assigned by designers and is analogous with the cost/difficulty of returning that function to a nominal state. In the case study, the impact of fault scenarios simulated with the FSL method use FFI values to quantify the results.

The system representation and function failure reasoning elements of the FFIP framework and the impact reasoning of the FFR method provide a foundation for the FSL method. The goal of the FSL method is to determine the functional impact of failures that occur because of unanticipated EMS flows (or alternatively, the impact of new flows caused by failures). The coupling of the functional and component representations from the FFIP framework provide a means of relating components to the functions those components embody based on matching EMS flows. The FFL reasoning produces the results from simulating possible failure scenarios with the FSL methodology, while the cost and function state evaluation from the FFR methodology provide a means for evaluating the FFL results. Combined, these elements provide a means for representing the designed system and outputting and evaluating the results of failure simulations. The following FSL methodology completes this analysis by creating a means to simulate faults in a system when considering EMS flows that are not modeled in the nominal system representation.

3.2 Flow State Characterization

This paper asserts that failure events can lead to unanticipated Energy, Material, and Signal (EMS) flows in a system, which must be considered when designing a PHM system. If failure propagation is assumed to follow EMS flow paths then a complete failure analysis of a design must also include potential flows. From a failure standpoint, any flow between components and from components is possible. Similarly, any flow from the environment to the component is also possible. It is therefore necessary to distinguish between designed flows and non-designed, or potential flows. Figure 1 illustrates the difference between designed flows and one potential flows that may exist in a fault specific

fault scenario.

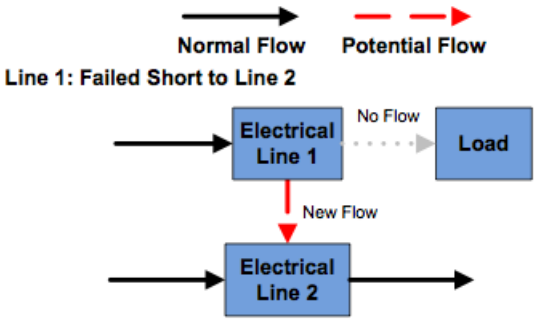

Figure 1: An example failure in an Electrical Power System with an unaccounted EMS flow.

Non-designed flows are the cause and/or effect of certain failure events. To capture the possibility of failure propagation of these potential flows, the Flow State Logic (FSL) reasoner was introduced (Jensen *et al.*, 2009) which identifies the state of any flow in the system of interest for any given system state. To begin the discussion, it is first necessary to define the concept of a flow's state, which is to be differentiated from a flow's actual value. Flow states can be separated as one normal state representing the designed flow and three states representing non-nominal flow.

The new flow states are described as follows:

1. *Normal Flow:* Flow is consistent with the original design
2. *New Flow:* Flow exists but was not designed to exist
3. *No Flow:* Flow does not exist but was designed to exist
4. *Reversed Flow:* All aspects except direction of flow are as designed

By categorizing the flow states of all flows that appear in a system, and using a critical event simulation, it is possible to identify the failures that propagate along both designed and potential EMS flow paths.

3.3 Flow State Logic

To map failure propagation along new system EMS flows, the Flow State Logic (FSL) reasoner has been developed and is introduced here to provide more complete and accurate results about the state of failures. Implementing the concept of Flow State Logic into FFIP requires a reasoner which evaluates the port values of the behavioral models. Ports are the input and outputs of a component behavioral model. The behavioral models for components have input and output ports for the designed flows as identified in the CFG and input and output ports for potential flows that might exist in a failed state. As can be seen Figure 2, FSL reasoning modules are created to evaluate flows by comparing the ports of nominally connected components as well as the potential ports. Figure 3 shows the logic used by the FSL for potential and designed flows. The Flow State Logic for designed flows evaluates the output and input ports *A.1* and *B.1*. The example potential flow logic evaluates the environmental input port *E-P.1* and potential component input port *A-P.1*.

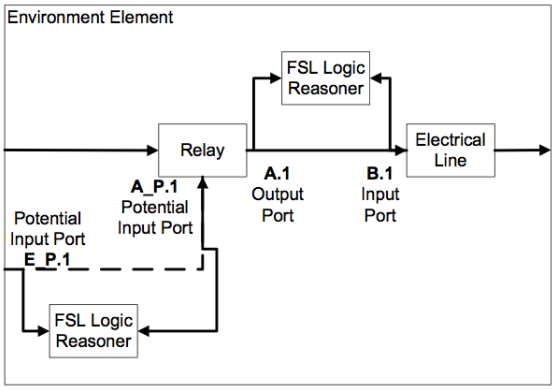

Figure 2: FSL modules reason on the input and output of component behavioral models.

3.4 Propagation-Based Behavioral Models

To accommodate the addition of the FSL reasoner, the behavioral model of a system must be formulated differently than the previous FFIP work. The first new element is the addition of a model element that corresponds to the environment around the system. Previous methods of defining component behavior identify the relationship between known input and output flows based on component mode (Kurtoglu and Tumer, 2008a; 2008b). To be flexible enough to analyze failure scenarios with new unknown flow types, this method uses a systematic approach to flow propagation to create component behavioral models. This is done by establishing a relationship between the component behavior mode and the propagation characteristics of a flow. The types of flows used in this method are the secondary level of flow as specified by the Functional Basis (Hirtz *et al.*, 2002; Stone and Wood, 2000), summarized in Figure 4.

For a component, the behavioral model is created by defining the relationship between designed input and output EMS flows based on component mode. Then for each type of potential flow that is considered, a designer specifies the critical level at which a component mode would change. If a critical level exists, then the component mode change is specified. Finally, some components do not have any means to propagate a type of flow to other system components. Therefore, the Boolean options of propagation or no propagation are specified for each potential flow type. In this way nominal and potential flow event behaviors are inte-

Flow Type	Considered for Example EPS System as:
Human Energy	Work performed by a person
Acoustic Energy	Fluid or solid vibration
Electrical Energy	Combined EMF and current flows
Electromagnetic Energy	Light and associated heat
Human Material	Contact by person
Gas material	Uncontained flow of normally contained gas
Liquid Material	Uncontained flow of normally contained liquid
Solid Material	Contact that includes energy of impact
Plasma Material	High temperature electro-neutral ionic gas

Figure 4: Flow types considered for an Electrical Power System.

Designed Flow

```
if A.1==B.1
    if A.1=="Zero"
      Flow="No Flow"
    else
        Flow="Normal"
else
    Flow="Reverse Flow"
```

Potential Flow

```
if E_P.1==A_P.1
    if E_P.1=="Zero"
      Flow="Normal"
    else
        Flow="New Flow"
else
    Flow="New Flow"
```

Figure 3: Example logic used for potential and designed flows for the FSL reasoner.

grated into a single component behavioral model. Ideally component behavior would reflect behavior associated with multiple simultaneous potential flows that occur in a failure. The current stage of this research limits the behavior to a single potential flow input and output, resulting in the designer choosing the potential flow of interest for failure analysis.

For example, a generic electric motor is nominally designed to have an input flow of electrical energy and an output flow of rotational energy. Using this methodology to develop the behavioral model of this component, the potential flow of liquid material would be considered. Exposure to liquid from the motor's environment may or may not cause a failure based on expected type of motor component used in this application. Therefore, designer knowledge is necessary to create the behavioral models. This systematic approach can be taken with each type of flow to determine component behavior to potential flows.

4 APPLICATION TO THE DESIGN OF AN ELECTRICAL POWER SYSTEM

The Advanced Diagnostic and Prognostics Testbed (ADAPT) at NASA Ames Research Center is used in this paper as a case study to illustrate the benefits of the proposed PHM design methodology. ADAPT provides a representative aerospace vehicle electrical power system (EPS) that enables automated diagnosis of faults in a physical software-hardware testbed. The testbed enables the injection of faults to determine the ability of various diagnostic software to determine failure type, location, and time. The physical implementation of the EPS is designed to deliver power to select loads, which might represent subsystems such as propulsion, life support, and thermal management systems, and contains basic functionality common to many aerospace applications: power storage, power distribution, and operation of loads (Poll *et al.*, 2007). The EPS testbed was originally designed using the Function Failure Based Design (FFDM) methodology at the early concept design phase (Hutcheson and Tumer, 2005). For this reason, the testbed represents an ideal case study for applying the function-based failure analysis presented in this paper to directly determine the benefit to the field of health management.

4.1 System Representation

The approach for this case study will be from the perspective of designing the ADAPT EPS testbed for the first time. To generate an initial design it is necessary to specify the design requirements. The high-level requirements for this design are to store and supply power in a controlled manner to operate three representative loads, namely a light, a fan, and a liquid pump. Applying the FFIP framework for system representation in this example begins with the functional decomposition into a functional model (FM). These are shown in two different levels of detail in Figure 5 and Figure 6 respectively. Function Criticality Ratings (FCR) are assigned for each function in the system based on the designer's expert opinion. Additionally the function state costs are assigned based on designer opinion and for this example are defined as the following:

1. $Operative = 0$
2. $Degraded = 1$
3. $LostRecoverable = 2$
4. $Lost = 3$

A set of generalized components are created based on the FM and are represented in the Configuration Flow Graph (CFG), shown in Figure 7. Included in the CFG is a block identified as the environment that this system operates within. This block represents an environmental behavioral model that can interact with components within the system through potential and designed EMS

flows. After using the FFIP framework for system representation, the Function Failure Logic (FFL) modules for each system function are created. The combined FFL reasoner modules provide function health states for each component based on behavioral model nominal inputs and outputs.

4.2 Implementing the FSL methodology

In order to create the behavioral model for each component the designed behavior is first specified based on discrete modes of the component. Then, to address both the designed behavior and the behavior associated with new flows, the following three questions for each of the EMS flows identified in Figure 4 are answered:

1. What qualitative level for each flow is necessary to change the mode of the component? (This is called the critical level.)
2. Does this component have the physical means to propagate this flow to nominally connected components?
3. How will each flow at its critical level affect component mode?

The answers to these three questions are used to derive the behavior model for each component. Combining the behavioral models together forms a system simulation model. The final addition is the inclusion of FSL reasoning modules to evaluate the state of flows as described above. Figure 8 illustrates the behavioral mode changes for a generic relay component with respect to the designed and potential EMS flows.

4.3 Results

The results from simulating failures using this approach is a quantified relative functional impact for each failure scenario. System simulation using this method can provide a means for failure propagation analysis of single and multiple component faults. Example scenario set one, illustrates the fault impact analysis capabilities of this method for single and multiple faults. The second example set shows how the scope of failure analysis is expanded using the FSL reasoning.

The first critical fault scenario is a single fault of the Pump Load. When the pump failure of a blocked flow is simulated the result is a higher than nominal current draw, causing Circuit Breaker 1 to trip. Functionally, the impact of this failure is significant because of the loss of electrical flow to multiple down stream components. The function states determined by the FFL reasoner for this are presented in Figure 9. While single failures may be of higher likelihood than multiple component failures it may be of interest for designers to know the impact of multiple faults, especially when considering failures to system safeguards. For this reason the results of the previous example can be compared with the same fault to the pump load but also considering the impact of Circuit Breakers 1 and 2 failing to trip with the high current flow. The result is that electrical energy is still provided to the loads. However, the high current draw of the pump limits the available electrical energy to the light load causing it to operate in a degraded state. The impact of this failure is presented in Figure 10.

The following set of examples provide insight into some of the benefits to the presented method. Considering again the effect of the blocked flow pump failure but with a different system load state. When the light load is not active (but the Fan load is active) the result of the pump fault is that the pump operates in a degraded state. The functional impact of this is presented in Figure 11. FSL reasoning provides the capabilities of analysis of new EMS flows created as a result of failures as well as new flows that might cause failures. For the final scenario, the same pump failure can generate a new EMS flow in the system of Liquid Material. When the Fan Load is exposed to a Liquid Material flow the Fan operates in a degraded state. This added a new functional failure as seen in Figure 12.

5 DISCUSSION

This paper presents an analysis of an Electrical Power System (EPS) using a Flow State Logic reasoning method. The main contribution of the FSL reasoning to the example system was to expand the scope of the failure scenarios for analysis. The benefit to PHM development is the same for this practical example. However, the fundamental concept behind the FSL method, that potential EMS flows that can exist in failed states that are not captured in nominal system representation, may provide insight into model-based reasoning approaches. For example, to simulate the impact of unanticipated EMS flows with this method generates a model that can be used for model-based reasoners. Additionally, the approach of recognizing a limited set of potential flows expands the system failure models used by the diagnostic reasoners.

For PHM development, the results indicate future contributions in two areas. First, this method applied to the PHM system provides a means to perform a function-based failure propagation behavior and impact analysis. Because the EPS sensor suite was also modeled in the simulation, a set of sensor characteristics readings was created for each failure. This information could be used to develop initial fault diagnostic reasoning. Secondly, comparing these fault sensor maps for uniqueness provides a metric for determining fault detectability and can provide designers with information on sensor placement.

A significant limitation of this current simulation methodology is the lack of time-to-failure analysis. For example, the fourth scenario given as an example in the previous section simulated failure propagation from the pump component to the fan component. The results are presented at an end state, however, a real failure of this type would have a certain time to impact

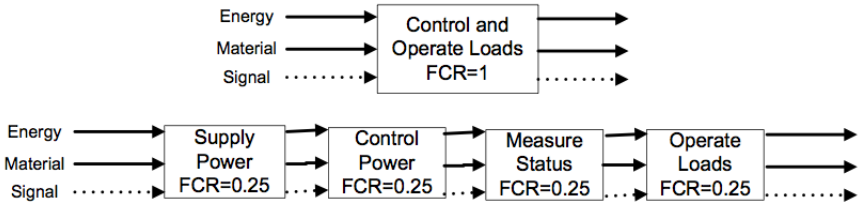

Figure 5: Functional Decomposition of an Electrical Power System.

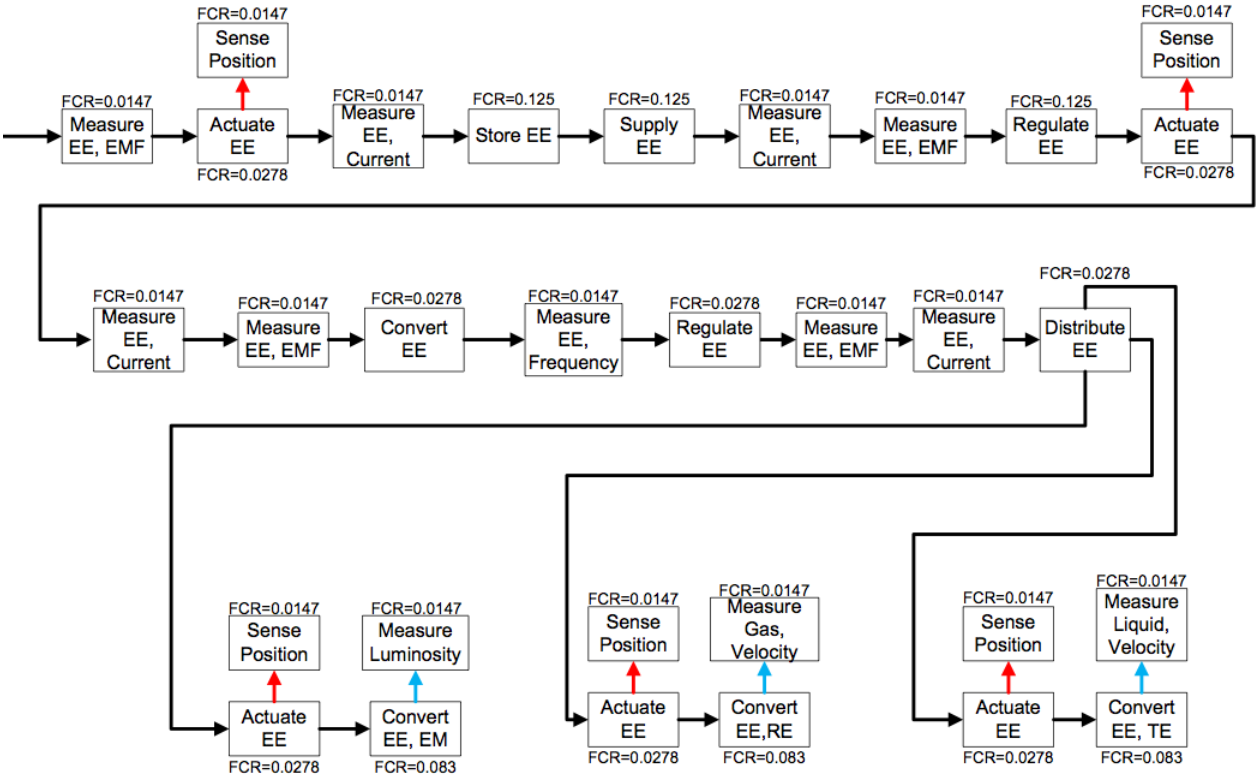

Figure 6: Functional Model of an Electrical Power System.

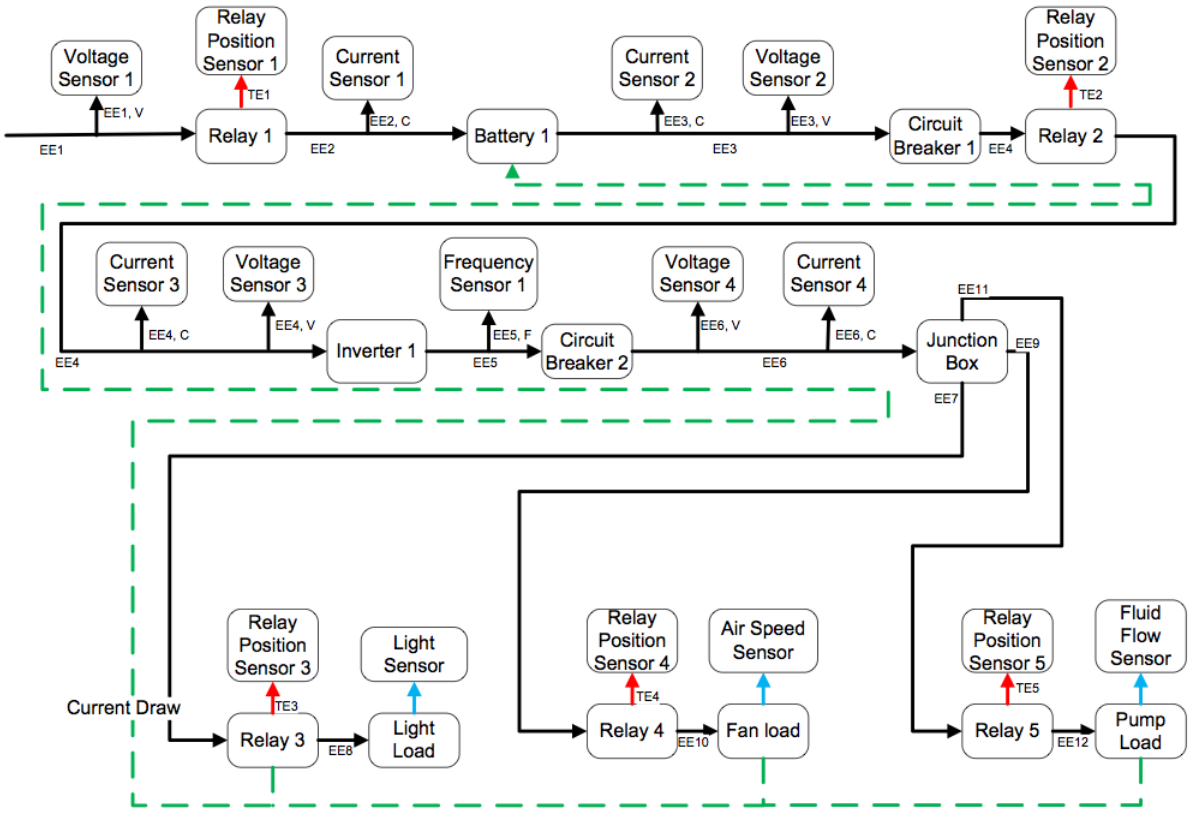

Figure 7: Component configuration and EMS flow diagram.

Relay			
Flow	Critical Level	Propagates?	Mode Change
Designed			
Electrical Energy	none	yes	none
Control Signal	Open/Close	yes	Open/close
Potential			
Human Energy	low	no	stuck open
Acoustic Energy	high	no	stuck open
Electrical Energy	high	yes	open/short
Electromagnetic Energy	high	no	stuck open
Human Material	low	no	stuck open
Gas material	none	no	none
Liquid Material	low	no	stuck open
Solid Material	low	no	stuck open
Plasma Material	low	no	stuck open

Figure 8: Example mode changes used to define component behavioral model.

Function	Component	FCR	State	FFI
Actuate EE	Relay 2	0.0278	Lost Recoverable	0.0556
Convert EE	Inverter 1	0.0278	Lost Recoverable	0.0556
Regulate EE	Circuit Breaker 2	0.0278	Lost Recoverable	0.0556
Actuate EE	Relay 3	0.0278	Lost Recoverable	0.0556
Convert EE, EM	Light Load	0.0833	Lost Recoverable	0.1666
Actuate EE	Relay 4	0.0278	Lost Recoverable	0.0556
Convert EE, RE	Fan Load	0.0833	Lost Recoverable	0.1666
Actuate EE	Relay 5	0.0278	Lost Recoverable	0.0556
Convert EE, TE	Pump Load	0.0833	Lost Recoverable	0.1666
			Sum	0.8334

Figure 9: Function failure results of scenario 1, Pump Load failure of ”Blocked Flow”.

Function	Component	FCR	State	FFI
Regulate EE	Circuit Breaker 1	0.0278	Lost	0.0834
Regulate EE	Circuit Breaker 2	0.0278	Lost	0.0834
Convert EE, EM	Light Load	0.0833	Degraded	0.0833
Convert EE, TE	Pump Load	0.0833	Degraded	0.0833
			Sum	0.3334

Figure 10: Function failure results of scenario 2, Pump Load failure of ”Blocked Flow” and Circuit Breakers 1 and 2 failure of ”No Trip”.

Function	Component	FCR	State	FFI
Convert EE, TE	Pump Load	0.0833	Degraded	0.0833
			Sum	0.0833

Figure 11: Function failure results of scenario 3, Pump Load failure of ”Blocked Flow” with no Light Load.

Function	Component	FCR	State	FFI
Convert EE, RE	Pump Load	0.0833	Degraded	0.0833
Convert EE, TE	Pump Load	0.0833	Degraded	0.0833
			Sum	0.1666

Figure 12: Function failure results of scenario 4, Pump Load Failure of ”Blocked Flow” with new liquid flow to Fan Load.

associated with it. Future work will examine explicitly defining failure propagation timing for both designed and potential flow paths. Additionally, this approach has focused on the mechanical component design and how the analysis results can benefit PHM design. Including the PHM control subsystem as part of the simulation provides a means of quantifying health management response with respect to function state. Future work will demonstrate a simple health management system design for the EPS presented in this paper and evaluate the response of that PHM system to failures caused by unanticipated EMS flows. Including the PHM control subsystem in the simulation would demonstrate the effectiveness of health management approaches, future work will investigate the inclusion of human interaction with the system. This extension could be used for evaluating the effectiveness of operator responses to failures for human-in-the-loop systems.

6 CONCLUSION

The symbiotic benefits of designing the PHM and physical system concurrently can be achieved when failure analysis is applied in the early stage of design. To this end a functional approach to failure analysis is used in this paper to design a conceptual Electrical Power System (EPS). The Function Failure Identification and Propagation (FFIP) method has been used in previous work to analyze the impact of failure and asses failure propagation with respect to system function. In this paper, the Flow State Logic (FSL) method was shown to expand the failure reasoning space to include potential flows not accounted for in the nominal system representation. Further this paper demonstrates that using this function-based failure impact reasoning can provide initial design information beneficial for the PHM development.

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.

REFERENCES

(Berenji *et al.*, 2003) H. Berenji, J. Ametha, and D. Vengerov. Inductive Learning For Fault Diagnosis. In *Proceedings of the 12th IEEE International Conference on Fuzzy Systems*, pages 726–731, 2003.

(Clarkson, 2004) Simons C. Eckert C. Clarkson, P. Predicting change propagation in complex design. *Journal of Mechanical Design*, 126:788, 2004.

(de Kleer and Kurien, 2003) J. de Kleer and J. Kurien. *Fundamentals of model-based diagnosis*. Safe Process, 2003.

(Deb *et al.*, 1995) S. Deb, K. R. Pattipati, V. Raghavan, M. Shakeri, and R. Shrestha. Multisignal flow graphs: a novel approach for system testability analysis and fault diagnosis. *IEEE Aerospace and Electronics Systems Magazine*, 10:14–25, 1995.

(Forbus, 1984) K. Forbus. *Qualitative Process Theory*. Artificial Intelligence, 24, 85-168, 1984.

(Giarratano and Riley, 2004) J. C. Giarratano and G. D. Riley. *Expert Systems: Principles and Programming*. PWS, Boston, MA, 2004.

(Grantham-Lough *et al.*, 2008) K. Grantham-Lough, R. B. Stone, and I. Y. Tumer. Implementation Procedures for the Risk in Early Design (RED) Method. *Journal of Industrial and Systems Engineering*, 2(2):126–143, 2008.

(Greer *et al.*, 2004) J. Greer, D. Jensen, and K. Wood. Effort flow analysis: a methodology for directed product evolution. *Design Studies*, 25(2):193–214, 2004.

(Hirtz *et al.*, 2002) J. Hirtz, R. Stone, D. McAdams, S. Szykman, and K. Wood. A Functional Basis for Engineering Design: Reconciling and Evolving Previous Efforts. *Research in Engineering Design*, 13:65–82, 2002.

(Huang and Jin, 2008) Z. Huang and Y. Jin. Conceptual Stress and Conceptual Strength for Functional Design-for-Reliability. In *Proceedings of the ASME Design Engineering Technical Conferences; International Design Theory and Methodology Conference*, 2008.

(Hutcheson and Tumer, 2005) R. Hutcheson and I. Y. Tumer. Function-based design of a spacecraft power subsystem diagnostics testbed. In *Proceedings of the ASME International Mechanical Engineering Congress and Exposition*, 2005.

(Hutcheson *et al.*, 2006) R. Hutcheson, D. McAdams, R. Stone, and I. Y. Tumer. FACE A function-based methodology for analyzing critical events. In *Proceedings of the ASME Design Engineering Technical Conferences*, 2006.

(Jensen *et al.*, 2008) D. Jensen, I. Y. Tumer, and T. Kurtoglu. Modeling the propagation of failures in software-driven hardware systems to enable risk-informed design. In *Proceedings of the ASME International Mechanical Engineering Congress and Exposition*, 2008.

(Jensen *et al.*, 2009) D. Jensen, I. Y. Tumer, and T. Kurtoglu. Flow State Logic (FSL) for analysis of failure propagation in early design. In *Proceedings of the ASME Design Engineering Technical Conferences; International Design Theory and Methodology Conference*, 2009.

(Krus and Grantham Lough, 2007) D. Krus and K. Grantham Lough. Applying function-based failure propagation in conceptual design. In

Proceedings of the ASME Design Engineering Technical Conferences; International Design Theory and Methodology Conference, 2007.

(Kuipers, 1986) B. J. Kuipers. Qualitative Simulation. *Artificial Intelligence*, 29/3:289–338, 1986.

(Kurtoglu and Tumer, 2008a) T. Kurtoglu and I. Y. Tumer. A graph-based fault identification and propagation framework for functional design of complex systems. *Journal of Mechanical Design*, 130(5), 2008.

(Kurtoglu and Tumer, 2008b) T. Kurtoglu and I. Y. Tumer. A risk-informed decision making methodology for evaluating failure impact of early system designs. In *Proceedings of the ASME Design Engineering Technical Conferences; International Design Theory and Methodology Conference*, 2008.

(Kurtoglu *et al.*, 2008) T. Kurtoglu, S. Johnson, E. Barszcz, J. Johnson, and P. Robinson. Integrating system health management into early design of aerospace systems using functional fault analysis. In *Proc. of the International Conference on Prognostics and Heath Management, PHM08*, 2008.

(Meshkat *et al.*, 2007) L. Meshkat, S. Jenkins, S. Mandutianu, and V. Heron. Automated Generation of Risk and Failure Models during Early Phase Design. In *Proceedings of the IEEE Aerospace Conference*, 2007.

(Otto and Wood, 2001) K. N. Otto and K. L. Wood. *Product Design: Techniques in reverse engineering and new product development*. Prentice Hall, 2001.

(Pahl and Beitz, 1996) G. Pahl and W. Beitz. *Engineering Design: A Systematic Approach*. Springer-Verlag, London, UK, 1996.

(Patterson-Hine, 2005) Narasimhan S. Aaseng G. Biswas G. Pattipati K. Patterson-Hine, A. A review of diagnostic techniques for ishm applications. In *1st Integrated Systems Health Engineering and Management Forum.*, 2005.

(Patton *et al.*, 1998) R.J. Patton, P. Frank, and R. Clark. *Fault Diagnosis in Dynamic Systems: Theory and Applications*. Prentice Hall, Hertfordshire, UK, 1998.

(Poll *et al.*, 2007) S. Poll, A. Patterson-Hine, J. Camisa, D. Garcia, D. Hall, C. Lee, O. Mengshoel, C. Neukom, D. Nishikawa, J. Ossenfort, A. Sweet, S. Yentus, I. Roychoudhury, M. Daigle, G. Biswas, and X. Koutsoukos. Advanced diagnostics and prognostics testbed. In *18th International Workshop on Principles of Diagnosis*, 2007.

(Stone and Wood, 2000) R. B. Stone and K. L. Wood. Development of a functional basis for design. *Journal of Mechanical Design*, 122(4):359–370, 2000.

(Stone *et al.*, 2005) R. B. Stone, I. Y. Tumer, and M. VanWie. The Function Failure Design Method. *Journal of Mechanical Design*, 14:25–33, 2005.

(Struss, 1988) P. Struss. Mathematical Aspects of Qualitative Reasoning. Int. J. Artificial Intelligence in Engineering. *Int. J. Artificial Intelligence in Engineering*, 3(3):156–169, 1988.

(Tumer and Stone, 2003) I. Y. Tumer and R. B. Stone. Mapping Function to Failure during High-Risk Component Development. *Research in Engineering Design*, 14:25–33, 2003.

(Wang and Jin, 2002) K. Wang and Y. Jin. Applying function-based failure propagation in conceptual design. In *Proceedings of the ASME Design Engineering Technical Conferences; International Design Theory and Methodology Conference*, 2002.

(Weld and de Kleer, 1987) D. Weld and J. de Kleer. *Readings in qualitative physics*. Morgan Kauffman, 1987.

(Yairi *et al.*, 2001) T. Yairi, Y. Kato, and K. Hori. Fault Detection by Mining Association Rules from House-keeping Data. In *Proceedings of the SAIRAS*, 2001.

David Jensen is a PhD student and graduate research assistant at Oregon State University. He earned both a Bachelor and Master of Science from Oregon State University in Mechanical Engineering in 2008 and 2009 respectively. His research to date has focused on function-based failure simulation and analysis. He has worked as a summer intern with the Advanced Diagnostic and Prognostic Testbed (ADAPT) as part of the Intelligent System Division at NASA Ames Research Center. Previous work in complex software-hardware product design and testing has provided him with a background and interest in failure identification and mitigation. His research has been published in the ASME International Mechanical Engineering Congress and Expo, ASME's International Design Theory and Methodology Conference, and at the Prognostics and Health Management Conference.

Dr. Irem Tumer is an Associate Professor at Oregon State University. Her extensive experience at NASA and in the Engineering Design community has led to over 20 journal publications and over 80 refereed conference publications, focusing on risk and failure analysis and engineering design theory and methodology. Prior to accepting a faculty position at OSU, Dr. Tumer led the Complex Systems Design and Engineering group in the Intelligent Systems Division at NASA Ames Research Center, where she worked from 1998 through 2006 as Research Scientist, Group Lead, and Program Manager. She has been extensively funded through various NASA programs while leading the Complex Systems Design group during her time at NASA Ames Research Center between 1998 and 2006, and through NSF and AFOSR since moving to Oregon State University in 2006. Dr. Tumer has

been Conference Chair for ASMEs Design for Manufacturing and the Lifecycle conference in 2000, and Technical Program Chair for IEEE Reliability Societys Prognostics and Health Management Conference in 2008, and Symposium Organizer and Chair for Integrated Systems Engineering at ASME's Computers in Engineering Conference in 2008 and 2009. She received her Ph.D. in Mechanical Engineering from The University of Texas at Austin in 1998.

Dr. Tolga Kurtoglu is a Research Scientist with Mission Critical Technologies at the Intelligent Systems Division of the NASA Ames Research Center working for the Systems Health Management group. His research focuses on the development of prognostic and management systems, model-based diagnosis, design automation and optimization, and risk and reliability based design. He received his Ph.D. in Mechanical Engineering from the University of Texas at Austin in 2007 and has an M.S. degree in the same field from Carnegie Mellon University. Dr. Kurtoglu has published over 40 articles and papers in various journals and conferences and is an active member of ASME, ASEE, AIAA, and AAAI. Prior to his work with NASA, he worked as a professional design engineer at Dell Corporation in Austin, Texas.