



## Scholars' Mine

---

Masters Theses

Student Theses and Dissertations

---

Spring 2008

# Fault propagation timing analysis to aid in the selection of sensors fro health management systems

Jeremy Johnson

Follow this and additional works at: [https://scholarsmine.mst.edu/masters\\_theses](https://scholarsmine.mst.edu/masters_theses)

 Part of the [Mechanical Engineering Commons](#)

Department:

---

### Recommended Citation

Johnson, Jeremy, "Fault propagation timing analysis to aid in the selection of sensors fro health management systems" (2008). *Masters Theses*. 4614.

[https://scholarsmine.mst.edu/masters\\_theses/4614](https://scholarsmine.mst.edu/masters_theses/4614)

This thesis is brought to you by Scholars' Mine, a service of the Missouri S&T Library and Learning Resources. This work is protected by U. S. Copyright Law. Unauthorized use including reproduction for redistribution requires the permission of the copyright holder. For more information, please contact [scholarsmine@mst.edu](mailto:scholarsmine@mst.edu).



FAULT PROPAGATION TIMING ANALYSIS TO AID IN THE SELECTION OF  
SENSORS FOR HEALTH MANAGEMENT SYSTEMS

by

JEREMY RYAN JOHNSON

A THESIS

Presented to the Faculty of the Graduate School of the

UNIVERSITY OF MISSOURI-ROLLA

In Partial Fulfillment of the Requirements for the Degree

MASTER OF SCIENCE IN MECHANICAL ENGINEERING

2008

Approved by

---

Dr. Daniel McAdams, Co-Advisor

---

Dr. Robert Stone, Co-Advisor

---

Dr. Robert Landers

© 2008

Jeremy Ryan Johnson

All Rights Reserved

## ABSTRACT

Sensor data is processed to assess performance and health of complex systems. Proper sensor selection, placement, and implementation are critical to build an effective health management system. For complex systems in which the timely assessment of the health is desired to avoid expensive consequences of failure, sensor placement is vital. The ability to identify a critical failure early is completely dependent on sensor location within the fault propagation path. A strategy for assessing a sensor suite with respect to timely critical failure detection is presented in this thesis. To illustrate the strategy, Fault Propagation Timing Analysis (FPTA) will be performed on the Rocketdyne RS-68 rocket engine.

The strategy consists of building directed graphs to represent the architecture and flows of the system. These graphs identify potential fault propagation paths for any selected failure mode located at a node. Fault propagation times are then generated for each arc and node within the propagation path. Locations where the fault propagation terminates are identified as critical effect nodes within the system. Candidate sensor suites may then be inserted into the graph. Time to detect is then compared to the time to criticality in order to assess sensor suite effectiveness.

## ACKNOWLEDGMENTS

I would like to thank Dr. Robert Stone, and Dr. Daniel McAdams for providing me with the opportunity to work with them. The experience that they offered me was instrumental not only in the completion of this thesis but also in my decision to enroll in UMR's masters program.

Working with the Functional Fault Analysis (FFA) group at NASA Ames Research Center has been the cornerstone of the work that this thesis presents. I would like to thank Dr. Stephen Johnson for providing this interesting and engaging project to work on.

I would like to acknowledge my contracting company USRA-RIACS for providing the funding for completing my course work and research for the thesis.

Finally I would like to thank my family for the support they offered me during the completion of my work.

## TABLE OF CONTENTS

	Page
ABSTRACT.....	iii
ACKNOWLEDGMENTS .....	iv
LIST OF ILLUSTRATIONS .....	vii
LIST OF TABLES .....	viii
NOMENCLATURE .....	ix
1. INTRODUCTION.....	1
2. LITERATURE REVIEW .....	5
2.1. SENSOR SELECTION EVALUATION.....	5
2.2. OPTIMIZATION PROCESS .....	6
2.3. REVIEW OF SENSOR SELECTION PROCESSES.....	8
2.3.1.Observability .....	8
2.3.2.Sensor Reliability/Sensor Fault Robustness.....	10
2.3.3.Fault Detectability/Fault Discriminability .....	12
2.4. FAILURE ANALYSIS METHODS.....	15
2.5. PROPOSED APPROACH .....	16
3. RESEARCH METHOD .....	18
3.1. STEP 1: BUILD DIRECTED GRAPH .....	18
3.2. STEP 2: IDENTIFY POTENTIAL FAILURE MODES.....	19
3.3. STEP 3: INSERT SENSORS.....	21
3.4. STEP 4: IDENTIFY CRITICAL FAILURE POINTS .....	22
3.5. STEP 5: IDENTIFY FAULT PROPAGATION PATHS.....	23
3.6. STEP 6: IMPLEMENT TIMING ANALYSIS.....	23
4. RS-68.....	26
4.1. INTRODUCTION TO THE RS-68.....	26
4.2. STEP 1: BUILD RS-68 DIGRAPH.....	28
4.3. STEP 2: IDENTIFY FAILURE MODES OF RS-68 .....	29
4.4. STEP 3: INSERT CANDIDATE SENSOR SUITE .....	30
4.5. STEP 4: IDENTIFY CRITICAL FAILURE POINTS OF THE RS-68 ....	31

4.6. STEP 5: IDENTIFY FAULT PROPAGATION PATHS .....	32
4.7. STEP 6: IMPLEMENT RS-68 TIMING ANALYSIS .....	33
4.8. RS-68 FPTA CONCLUSIONS .....	34
5. CONCLUSIONS.....	36
APPENDIX.....	38
BIBLIOGRAPHY .....	39
VITA .....	42



**LIST OF ILLUSTRATIONS**

Figure	Page
1.1. Time to Criticality Timeline.....	3
2.1. Fault Trajectory Space for Two Sensors Described by Santi, et al. (2005).....	13
3.1. Directed Graph Example.....	18
4.1. RS-68 Operating Characteristics .....	27
4.2. RS-68 Operating Schematic.....	27
4.3. RS-68 Digraph.....	29
4.4. RS-68 Digraph Snapshot With Sensors .....	31
4.5. RS-68 Digraph Snapshot With Critical Point.....	32
4.6. RS-68 FTP Head Efficiency Loss Propagation Path .....	33
4.7. RS-68 Propagation Path With Times Included .....	34

**LIST OF TABLES**

Table	Page
2.1. Sensor Selection Optimization Techniques and References .....	7
3.1. Characteristic Propagation Times.....	25
4.1. Example Candidate Red-line Sensor List for the RS-68.....	30

**NOMENCLATURE**

HMS	Health Management System
FPTA	Fault Propagation Timing Analysis
FOM	Figure Of Merit
NLP	Nonlinear Program
MINLP	Mixed Integer Nonlinear Program
MFD	Multiple Fault Diagnosis
QDG	Quantified Directed Graph
FMEA	Failure Modes and Effects Analysis
FTA	Fault Tree Analysis
EELV	Evolved Expendable Launch Vehicle
CaLV	Cargo Launch Vehicle
FTP	Fuel Turbo Pump
MCC	Main Combustion Chamber

## 1. INTRODUCTION

Effective design of health management systems for complex systems represents an important challenge in engineering. Health management deals with the timely detection, diagnosis and correction of abnormal behavior caused by faults in a system. Early detection and diagnosis of faults while the system is still operating in a controllable environment may help avoid progression of faulty behavior to a critical point. The Space Shuttle Columbia accident represents a strong case for the effective design of health management systems. If the effects of the foam strike were detectable and diagnosable before the shuttle attempted reentry the catastrophe might have been avoided.

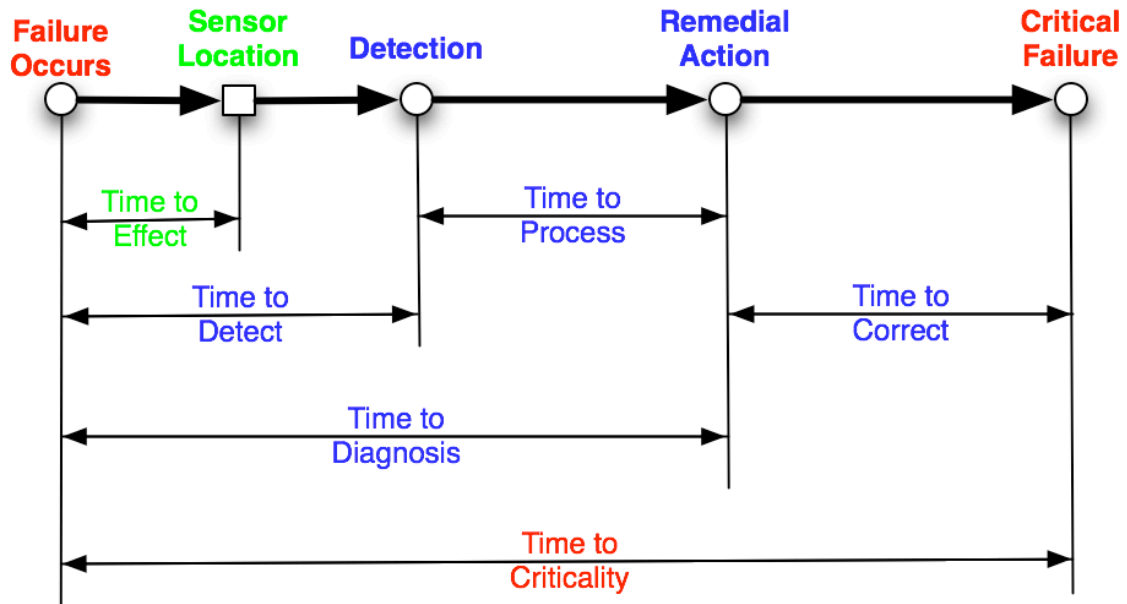
The input data that Health Management Systems (HMS) require to make assessments of the status of a system originates from sensors. Positions of sensors, along with implementation define the range of potentially critical failures that a HMS may isolate. Isolation of critical failures is required for a HMS to potentially compose a corrective action. The corrective action may take the form of switching to a redundant channel, activating a mitigation mechanism, or sending notification to an interested source. In all cases, the corrective action must take place before a fault propagates to a critical situation. Making a diagnosis of the system in a timely manner requires sensors to be located at or near the point of fault origination. It is desired to have the ability to analyze candidate sensor suites with respect to the ability to sense critical failure modes in a timely manner.

Complex systems, such as aerospace systems, are developed through a series of design reviews. Within each design cycle different design considerations are studied. All components under consideration must demonstrate a clear added value to the system.

The costs and risks associated with the complex system drive the design cycles to eliminate any components that are not able to demonstrate their value to the design.

When considering sensors to contribute to an effective HMS system the challenge is to be able to justify each measurement's existence in terms of added value to the system.

There are a myriad of tradeoffs when considering an optimal sensor suite for any given system. Parameters such as weight, cost, time constants, etc., have to be compared against each other to assemble a candidate sensor suite with the goal of meeting the requirements imposed upon the system. The sensor suite evaluation strategy described in this thesis primarily addresses a time to detect requirement. The evaluation provides for time to criticality to be assessed as well, allowing a comparison between the two times to identify sensor suite effectiveness. There exists a race condition between HMS being able to sense and react to a failure, and the time for off-nominal behavior caused by that failure to propagate to a critical condition. A timeline that defines the events that lead up to criticality is shown in Figure 1.1. The goal, in this thesis, is to select a sensor suite that can minimize the time to detect.



**Time to Effect** - The time for the symptom of a fault to become potentially detectable.

**Time to Detect** - This time includes the time to effect and all sensor latencies associated with sensor time constants, red lines, etc.

**Time to Process** - The time for all processing of sensor data and decision making.

**Time to Correct** - The time that a remedial action may take place to avoid a critical failure.

**Time to Criticality** - Time from onset of failure to when the effects of that failure propagate to a expensive consequence.

Figure 1.1. Time to Criticality Timeline

The Rocketdyne RS-68 rocket was selected to demonstrate the sensor suite evaluation strategy. The RS-68 is the first new U.S. engine certified to fly since the Space Shuttle Main Engine over 20 years ago. The RS-68 has also been selected to boost the first stage of the Ares V Cargo Launch Vehicle that is part of the next generation of launch vehicles in NASA's exploration vision. Fault Propagation Timing Analysis

(FPTA) is performed on the RS-68 to demonstrate how a hypothetical sensor suite performs with respect to the time to detect.

Chapter 2 is a literature review of sensor selection strategies that have been developed. Failure identification and analysis methods are also described. Deficiencies of these concepts are identified and represent the opportunity for improvement that FPTA offers in being able to evaluate a sensor suite and its ability to detect faults in a timely manner. Chapter 3 describes the FPTA method and how it is implemented to evaluate a sensor suite. FPTA is then implemented on Rocketdyne's RS-68 rocket engine in chapter 4. Lastly, the conclusions and future work are presented in the final section.

## 2. LITERATURE REVIEW

Sensor selection strategies for complex systems are numerous and have a broad range of approaches to meet each individual system's needs. The intended purpose for each of the sensor suites implemented in these systems dictates the aspects that need to be addressed during the selection process. Maul, et al. (2007) describe the sensor selection process in two parts: an evaluation module and an optimization module. These modules will be used to demonstrate past sensor selection strategies.

### 2.1. SENSOR SELECTION EVALUATION

The effectiveness of a particular sensor suite is evaluated by identifying the requirements that need to be addressed within a system, and the ability of the selected sensors to meet those requirements. The degrees to which a sensor selection meets those requirements can be defined as the Figures of Merit (FOMs) of the system. A set of FOMs reflects the objectives of the sensor suite selection process. Sensor selection strategies described in this section will be presented with regard to how they address the following figures of merit identified by Maul, et al. (2007).

- **Observability:** This category considers how well the sensor suite will provide information about the given system process, which parameters that are directly observed, and which parameters can be inferred.
- **Sensor Reliability/Sensor Fault Robustness:** This category addresses sensor reliabilities and how sensor availability impacts the overall sensor suite performance.



- **Fault Detectability / Fault Discriminability:** This category specifically addresses whether the sensor suite can detect and discriminate system failures.
- **Cost:** This category can include development, purchase, and maintenance costs for the sensors as well as resource and communication costs.

## **2.2. OPTIMIZATION PROCESS**

Sensor selection problems addressing the before mentioned FOMs require fast approximate search solutions to produce results in a timely manner. There are several methods that have been developed which refine searches through identification of possible candidates to find the optimal solution. The following is an introduction to some of these general optimization strategies.

- Debouk, et al. (1999), apply constraints on an objective function to streamline the optimization process.
- Worden (2001) applies advanced artificial analysis techniques such as genetic algorithms and simulated annealing algorithms.
- Eberhart (1995) proposed particle swarm optimization that is a population based stochastic technique.
- Osorio (2004) describes a cutting and surrogate constraint analysis that uses constraint pairing and an initial integer solution to combine the dual surrogate constraint with the objective function to generate new constraints.

This list is a representation of the variety of algorithms available to produce an optimized solution. Optimizations techniques are not reviewed in detail here, but the methods have been well documented by Fletcher (1987). A set of sensor selection

optimization techniques and the associated references are listed in Table 2.1 that was generated by Maul, et al. (2007).

Table 2.1. Sensor Selection Optimization Techniques and References

Optimization technique	Researcher
Constrain-Based Search	Narasimhan, et al. (1998), Mushini (2005)
Exhaustive/Brute Force Search	Debouk, et al. (1999), Mushini (2005), Narasimhan, et al. (1998), Madron (1992), Worden (2001)
Genetic Algorithms	Musulim, et al. (2005), Mushini (2005), Spanache, et al. (2004), Sen, et al. (1998), Santi, et al. (2005), Worden (2001)
Particle Swarm Optimization	Zhang (2005)
Graph Theory: Spanning Trees and Cutsets	Ali (1993 and 1995), Bagajewicz (1997 and 1999)
Cutting and Surrogate Constraint Analysis	Azam, et al. (2004)
Mixed Linear Integer Programming	Bagajewicz (2000, 2002, and 2004), Chemielewski, et al. (2002)
Simulated Annealing Algorithm	Worden (2001)

## 2.3. REVIEW OF SENSOR SELECTION PROCESSES

The first three Figures of Merit (FOMs) that Maul, et al. (2007) describe are used to guide the review of sensor selection processes that have been developed. The fourth FOM, cost, is a straightforward penalty driven group and may be included in the concepts that address each of the three FOMs discussed. The FOMs that are covered are observability, sensor reliability/sensor fault robustness and fault detectability/fault discrimination.

**2.3.1.Observability.** A system's ability to provide information about its state with respect to performance monitoring, health assessment, and control of the system is of paramount importance. Some strategies define the degree of observability by analyzing a state space model that represents the process of interest. Van den Berg, et al. (2000) define the criteria for degrees of observability by determining the amount of signal received by a sensor for a system configuration of a tubular chemical reactor. Optimal sensor locations for the reactor are found by specifying scalar measures on the observability Gramian integral from the linear least-squares state estimation problem. Muller (1972), similarly, develops scalar metrics from the observability matrix to define the degree of observability for linear dynamical systems. Dochain, et al. (1997) identify a criterion that is the condition number of the observability matrix of the linearized tangent model of the discretized model of fixed bed bioreactors.

Other approaches to display degrees of observability use graph-based approaches that capture the architectural information of a given system. Two graph-oriented algorithms for observability and redundancy classification were proposed by Kretsovalis (1987). Luong, et al. (1994) establish an incidence matrix using graph-based analysis.

The incidence matrix related process relationships to the state variables qualitatively. Identification of unmeasured variables and determination of whether a measured variable was redundant is accomplished by the decomposition of the incidence matrix. Bagajewicz (1999) describes the degree of estimability that incorporates degrees of observability and redundancy to assess system variables that may be estimated by measurements. A variable that is not measured is observable if it can be identified in at least one way from the measurements. Similarly, a measurement is redundant if it can be found in at least one way from the remaining measurements.

There is a large body of work that focuses on identifying observability in structural type problems. Papadopoulos (1998) proposes a scheme that selects the most linearly independent impulse responses at all candidate sensor locations from a Gram-Schmidt orthogonalization procedure. Also proposed is a scheme based on a principal component analysis and iteratively removes sensors that do not contribute significant information to the Fisher information matrix. Hac (1993) uses quantitative measures of observability based on gramians to determine sensor locations in motion control of flexible structures. By determining eigenvalues, obtained in closed form from corresponding gramians in each optimization step, an optimality criterion is established.

Some strategies for assessing system observability include utilizing prediction of error of a given sensor suite with respect to various parameters of interest. Chmielewski, et al. (2002) propose a Nonlinear Program (NLP) that is independent of all decision variables. The NLP can then be converted into a convex program through the use of linear matrix inequalities. Using the results, sensor placement is established by standard interior-point and branch-and-bound search algorithms. Musulin, et al. (2005) identify

sensor suite observability by maximizing Kalman filtering performance. The measurement noise and observation matrices are manipulated to produce the parameters. Similarly, Mushini (2005), proposed maximizing a Kalman filter performance by utilizing a metric defined as a function of the steady state error-covariance and the cost of the selected sensors. The optimal measurement sets for an aircraft gas turbine engine are then estimated. Madron (1992) uses multiple Gauss-Jordan elimination of the system of linear mathematical model equations to generate classifications of observability for sensor suites.

**2.3.2.Sensor Reliability/Sensor Fault Robustness.** Observability and detectability become useless if measurements are not available to make the detections. Being able to identify how reliably a system can make detections for fault diagnosis is of considerable importance. Therefore it is important to be acquainted with strategies for assessing the reliability and fault robustness of sensors.

Considerable consideration has been made for assessing the performance of a sensor network in the presence of sensor faults. Bagajewicz (1997) defines qualifying constraints that relate to certain requirements of data reconciliation with the goal of minimizing cost. Error detectability is defined as the ability of the sensor network to detect sensor faults. Availability is defined as the precision after a failed sensor is removed. Resilience is defined as precision in the presence of a sensor fault. These constraints define the ability of a sensor network to perform in the presence of a sensor fault. Bagajewicz (2002) then extends this research to include explicit Mixed Integer Nonlinear Program (MINLP) formulation. Hardware redundancy is then taken into account as an extension of the theory represented in this work.

Some researchers define the reliability of an instrumentation system as the probability that information required for control are available through measurements or deduction during a given time period. Using this definition, Loung, et al. (1994) compute the number of sensor failures conserving the observability of the variables required for control. This is done by classification of various parameters needed for control. Competing networks are compared by integration of the time profile for each sensor network.

Yet other researchers identify the concept of sensor reliability as the reliability of the availability of measurements to provide system state estimations. Ali (1993) focuses on identifying how robustly a sensor network can handle failures and still estimate a variable. Using a graph-theoretic algorithm, globally optimum solutions are generated for realistic processes. Later, Ali (1995) adds to the algorithm to identify the optimal design for a redundant sensor network for linear processes. This algorithm accounts for specifications of measurable variables. Sen, et al. (1998) use genetic algorithms to allow for multiple performance metrics to be evaluated along with the optimization of objective functions with a single criterion. Similarly, Bagajewicz (2000), used MINLP to provide for multiple metrics, such as cost to be optimized along with reliability.

**2.3.3. Fault Detectability/Fault Discriminability.** While observability provides information about state parameters required for making a system health diagnosis, fault detection and discriminability define the sensor network's ability to distinguish off nominal from nominal operation and the ability to distinguish these faults from each other, respectively. Observability, detectability and discriminability are all necessary to be able to process sensor data and to make a system health diagnosis.

Some research focuses on using system behavioral models and reliability data to assess sensor placement. Azam, et al. (2004) propose using such a model along with fault probabilities and effects of faults on observable system parameters to evaluate a sensor suite. Fault effect information is translated into cause-effect dependencies and detection probabilities are then computed. Multiple Fault Diagnosis (MFD) algorithms search for the most likely candidate fault subset that best explains the set of observed discrepancies from the bipartite graph model. Optimal sensor allocation is then performed after a set of performance measures are calculated using the candidate fault subset. The optimization was performed using surrogate cutting and constraint pairing-based method.

Santi, et al. (2005) propose a detection strategy for rocket propulsion systems in which thresholds are used to determine off-nominal behavior. Measurements from multiple sensor sources must exceed a prescribed threshold limit for reliable fault detection. A minimum measurement deviation level for that fault detection within a defined false alarm limit is designated as the detection threshold limit. Figure 2.1 shows the detectable fault zone that is the measurement space area where the outputs from two

sensors exceed a detection threshold limit. A fault becomes detectable when its measurement level reaches the trajectory location that intersects the detection threshold.

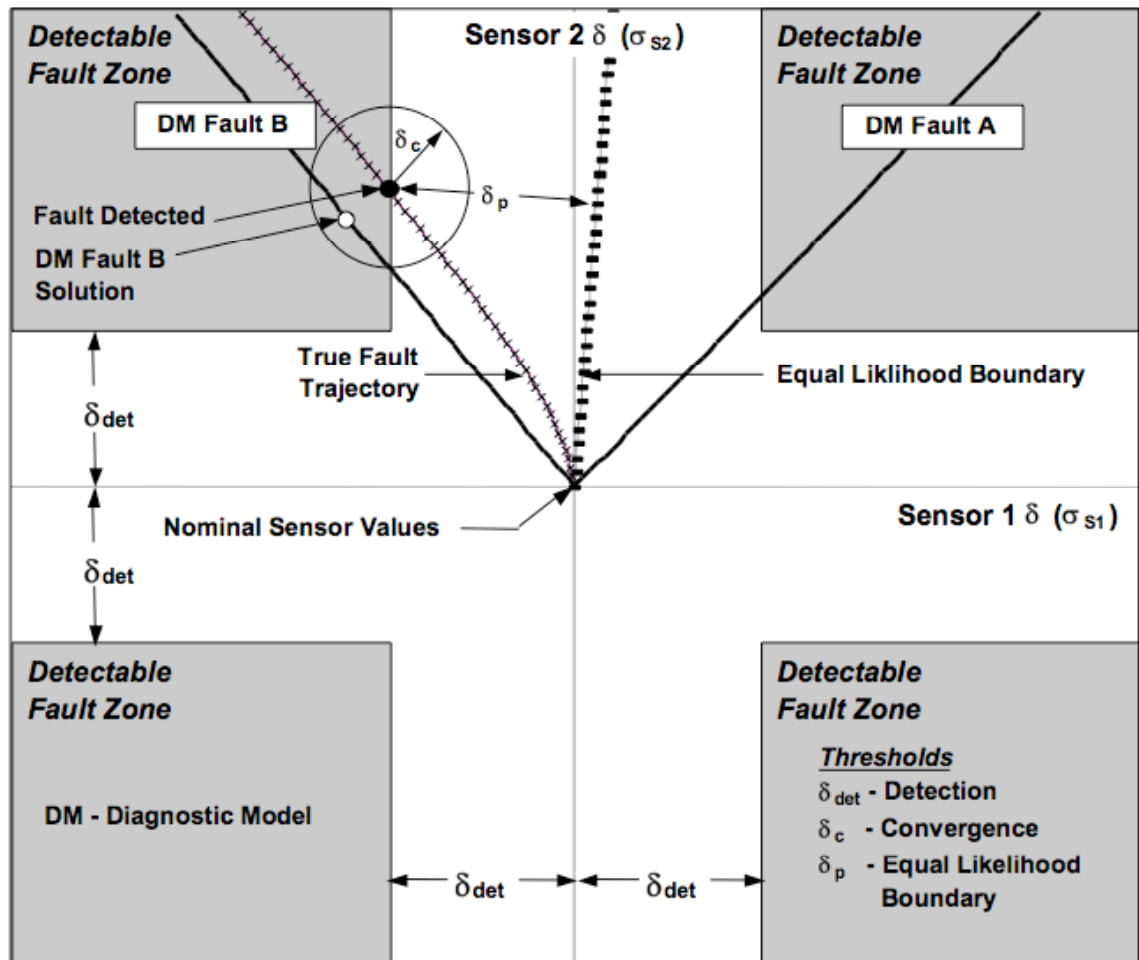


Figure 2.1. Fault Trajectory Space for Two Sensors Described by Santi, et al. (2005)

There is much research that focuses on assessing detectability by qualitatively analyzing the fault propagation process. Several researchers including Raghuraj, et al (1999), Bushan (2000), and Bagajewicz, et al. (2004) use directed graphs, or digraphs, to



represent faults in a system. Faults are related to sensors through dependencies modeled by the digraphs. This graph provides an indication of which sensors should respond to which faults. Spanache, et al. (2004) capture the behavior of a system through a series of constraints that represent the limitations imposed on the evolution of the variables. The constraints and fault signatures that are assigned to failed components are then used to establish a component oriented fault signature matrix. Similarly, Narasimhan, et al. (1998) identify qualitative fault signatures by establishing temporal causal graphs derived from a bond graph model. The temporal causal graph is a directed graph, where vertices are the system variables and the edges represent the causal relationship between these variables qualified by the temporal characteristics of the relation.

Yan (2004) uses the CAD environment to implement a diagnosability analysis for sensor placement. In this work the fault signature matrix is found by projections of different operation modes on observable variables. While these qualitative methods represent a straightforward strategy for relating system faults to effects, there are several researchers that chose to incorporate more fault information in hopes of augmenting these useful techniques. Zhang (2005) proposes a Quantified Directed Graph (QDG) in hopes of capturing quantitative information to model the behavior of a system. In a QDG, each node represents a sensor location with a signal to noise ratio. A sensor detectability measure was then calculated for each sensor and then evaluated against an assigned lower bound. The qualitative methods presented here are ideal for identification of fault signatures to analyze sensor placement during the early design stages of complex systems. These methods are also preferable because they are less expensive than hardware and software simulation techniques.

## 2.4. FAILURE ANALYSIS METHODS

Failure Analysis is an integral part of identifying a sensor suite's ability to detect fault in a system. Being able to identify the ways in which a failure mode manifests itself as a fault within a system yields information about what measurements need to be taken to isolate the failure. There are a couple of failure analysis techniques that are regarded as the standard in failure assessment in the aerospace industry. Tumer (2003) points out that Failure Modes and Effects Analysis (FMEA) is the standard failure analysis method used in design. FMEA is a risk assessment technique for systematically identifying potential failures in a system or process. System experts identify failure modes for each component within a system. Effects are also recorded for each of these failure modes. One of the shortfalls of the FMEA approach is that there is little attempt at assessing failure propagation times for each of the failure modes. When fault propagation time numbers are identified they are usually too coarse to make design decisions with. FMEA may indicate time to criticality as instant, seconds, minutes, hours, or even longer periods of time. This provides an idea of how fast a fault propagates to a critical condition, but does not give any exact numbers.

Another failure analysis approach commonly implemented for complex systems during the design stages is Fault Tree Analysis (FTA). Bahr (1997) indicates that fault trees are widely used not only in reliability analysis, but also in safety analysis because of their ability to account for failure beyond single part malfunctions. FTA is a failure analysis in which a critical state of a system is indicated as the top node in the tree. Using Boolean logic the top node event trees out to lower level events that are causes of

the higher level events. While FTA represents an invaluable tool for evaluating the events that lead up to a failure, they fall short in that they do not address how fast these events ultimately manifest themselves as the undesired situation.

On the other end of the spectrum of strategies for identifying propagation times is physics based simulation. These simulations yield precise numbers that may be used to accurately assess a system's ability to handle candidate failure scenarios. Simulations that have the fidelity to produce these numbers are usually very expensive and time consuming to produce. Another shortfall in the implementation of these simulations is that there has to be a great deal of design information available for production of a model that can yield the type of timing information that is desired to evaluate a sensor suite's ability to detect a fault.

## **2.5. PROPOSED APPROACH**

All of the failure analysis techniques mentioned are not necessarily implemented during the early stages of design. A sufficient level of design maturity is needed to be able to generate both FMEA, FTA and physics based simulation. FMEA usually requires more information about the components to be able to accurately identify the ways in which specific components may fail. Physics based simulation needs more information to be able to generate equations to accurately represent the system.

The proposed approach, Fault Propagation Timing Analysis (FPTA), may be implemented during the early design stages of a system to make evaluations of sensor suites. During conceptual development when there is an idea of the type of components

that a system might have, these configurations may be represented in directed graphs and an FPTA analysis can be completed to evaluate sensor placement.

FPTA is an augmentation of some of the directed graph approaches mentioned in section 2.1.1.3. of this thesis and contributes directly to the detectability evaluation of a sensor suite. Previous digraph approaches did a good job of relating faults to sensors through modeled dependencies, but failed in providing a sense for how much time it took for that fault to reach a sensor. This research outlines an approach for assigning propagation times to the dependencies of the digraph in order to evaluate how long it takes for a fault to become detectable by a sensor. A natural addition to this concept is that a propagation time can be identified for a fault to reach a critical condition. Comparison of the time to criticality and the time to detect allows for a quantitative evaluation of a candidate sensor suite's ability to detect a failure mode.

### 3. RESEARCH METHOD

To support sensor suite assessment with respect to a system's ability to identify off-nominal behavior before a critical state is reached I propose Fault Propagation Timing Analysis (FPTA). The analysis is presented as a series of steps to follow for sensor suite evaluation implementation on a system.

#### 3.1. STEP 1: BUILD DIRECTED GRAPH

To complete an FPTA, a directed graph must be built for the system to be instrumented. Inputs that are needed to build the graph include, but are not limited to, system schematics, drawings, illustrations, concept of operations, and expert solicitation. The nodes of the graph represent the components of the system that have the potential for failure. The arcs represent fault propagation paths of the system. Components are arranged and connected to model the interactions that represent the functional dependencies of the system. For instance, an electric motor generates mechanical energy to be transferred through a gearbox to a wheel. The directed graph for this system is illustrated in Figure 3.1.



Figure 3.1. Directed Graph Example

Fault propagation paths can be a superset of two types of flows within a system. There are nominal system flows and flows that may occur as a result of off-nominal behavior. The nominal system flows are usually easy to identify. These nominal flows might be the energy, signal, or mass flows that are functionally intended to flow between components to provide for overall system functionality. The nominal flows usually represent the majority of paths that a fault may propagate within a system. For example, if an electrical wire breaks, electricity will fail to transfer to the appropriate components within the system. The effects of the failed wire would propagate through the system following nominal paths, that is, there will be a lack of power to downstream components. The off-nominal system flows that occur as a result of a failure are usually more difficult to identify. These flows must be represented by arcs to directly address the effect of that failure. For example, if a battery overheats and explodes, an off-nominal system flow might be modeled as an arc from the battery to any components that may be affected by the explosion. If the system was working the way it was intended to perform, there would be no arcs from the battery to these components. The objective is to capture all potential fault propagation paths that may occur within a system.

### **3.2. STEP 2: IDENTIFY POTENTIAL FAILURE MODES**

FPTA analysis relies on understanding the ways a system may fail. The extent to which failure modes are identified within a system is dependent on the desired capability of the candidate sensor suites. When completing FPTA analysis on complex systems that have potentially expensive consequences of failure, it is desired to comprehensively

identify failure modes with the goal of assessing sensor suite detection capabilities for any given failure scenario. Failure modes are identified for each of the components that are modeled. Any off-nominal condition that the component has the possibility of encountering may be considered a failure mode. The condition is identified as a failure mode when the failure effects cause off-nominal behavior to be seen at components that are located downstream from the failed component in the digraph.

Failure Modes and Effects Analysis (FMEA) is an excellent source of this type of failure information that is generally available for complex systems. FMEA is a risk assessment technique for systematically identifying potential failures in a system or process. Failure modes are identified for each component within a system. Effects are also recorded for each of these failure modes. These effects aid in the identification of fault propagation paths.

While FMEA offers a valuable bottom-up approach to potential system failure identification, Fault Tree Analysis (FTA) is a top-down method. FTA identifies a critical event that is defined as the “top event” and then trees out to reveal potential causes of that event. Paths of the tree pass through Boolean logic gates that define which lower level events may lead to the “top event”. The lower levels of the fault tree that identify potential failure sources that lead to the critical event are then related to component failures that may be represented in the FPTA digraph.

Once failure modes are identified, using whichever approach deemed appropriate, fault propagation paths may be developed. The failure modes represent the initiation of a given fault propagation path. The faults that result from these failure modes also define which dependencies represented in the digraph are valid propagations. The determination

of these paths is made from understanding the effects of each of the failure modes and is discussed in section 2.4 of this thesis.

### **3.3. STEP 3: INSERT SENSORS**

After a directed graph is completed that models all of the components and dependency paths of a system, candidate sensor suites may be inserted. A sensor is seen as another component in a directed graph of a system. The arcs, or fault propagation paths, that are inputs to the sensors follow the same conventions as described earlier. Any signal, energy, or mass flow that a given sensor is intended to measure is drawn as an arc from a component in the system to that sensor. The component that the arc is drawn from may be the component where that sensor is physically located, or it may be a component that the sensor is intended to directly measure. Sensors will sometimes not have outputs because faults caused by failure modes in the system will usually propagate along nominal flow paths. Sensor nodes may have output ports if there are failure modes that need to be taken into account for the system due to the existence of the sensor. For instance, a pressure sensor located on a combustion chamber represents a potential gas leakage point if failure occurs. A significant consideration has to be made for the sensor failing to make a detection as well. This failure may manifest itself in several ways such as a detection failing off-scale or sensor drift. These types of failures can be common and should therefore be accounted for.

While sensors have the possibility of failing, the ability of a system to overcome a sensor failure in order to make a failure determination is out of the scope of this work. There have been several strategies developed for allocating sensors and for processing



data from those sensors to accurately diagnose a system's health in the presence of sensor faults. The goal of this work is to be able to assess how well a given sensor suite can detect a critical fault in a timely manner. The strategy described in this thesis takes into account the time for a fault to propagate to a sensor, and the time it takes for any given sensor to realize that the fault has occurred. The time for a sensor to identify the fault in the system incorporates all sensor latencies associated with time constants, red lines, etc. It is not intended to be able to assess the time it takes to process the data to make a health status determination.

#### **3.4. STEP 4: IDENTIFY CRITICAL FAILURE POINTS**

It is desired to assess sensor placement to identify failures before the fault leads to an expensive consequence. If time to criticality is known, it may be compared to the time to detect to make a determination of sensor suite effectiveness. FPTA analysis allows for a time to criticality assessment. It is necessary to understand the way the system can fail and what the effects of these failures will be to identify points of criticality. Points of criticality represent locations within a system that off-nominal behavior will manifest itself as an expensive consequence. For instance, when a valve fails to open, the immediate effects associated with that valve failing may not be critical. But when a combustion chamber downstream of that valve fails to receive fuel, this represents a point of criticality. The scenario becomes critical when the combustion chamber behavior becomes off nominal because those consequences are more significant than upstream effects of the failure.

The points of criticality may be modeled as nodes in the directed graph. The input is any flow that may demonstrate the symptoms of off-nominal behavior from a component. There will usually be no outputs of the points of criticality because these nodes represent where a propagation path will terminate. There are scenarios though where there may be two critical failures that can lead to a more crucial consequence. In such a case one could model fault propagation paths from each of the critical failures to another point of criticality that represents the more crucial consequence.

### **3.5. STEP 5: IDENTIFY FAULT PROPAGATION PATHS**

To identify which sensors have the opportunity of detecting off-nominal behavior of a system due to a failure, it is necessary to know the path in which a given fault may propagate. Propagation paths are generated by tracking dependency paths that are modeled in the directed graph of a system. Any failure that occurs in a component, or node, of the graph will propagate along the arcs that point to downstream components that are affected by the propagation of the fault. For any fault of interest, a path may be traced from the component along the arcs and nodes until a critical point is reached.

### **3.6. STEP 6: IMPLEMENT TIMING ANALYSIS**

The timing analysis identifies the time it takes from initiation of the failure mode to the manifestation of the critical fault. The analysis also identifies the time it takes for the off-nominal flows of the system to be detected by a given sensor suite. The failure propagation path is populated with times that represent how fast the fault propagates

through the system. Times are identified for each arc and node in the graph. Times that are identified for the arcs represent the time it takes for a fault to propagate from the output of one component to the input of the next component. Times that are identified for a module represent the time it takes for a fault to propagate from the input of a component to the output of that component.

Depending on the goals of the timing analysis, there are several strategies for producing these propagation times. During the early design process the numbers may be generated by expert solicitation. The digraph represents an early conceptual formulation of a system and a subject matter expert may be asked how long it would take a fault to propagate from one point to another. The times would be inserted into the digraph and the timing analysis would identify potential issues that may be resolved during subsequent design cycles.

In order to accurately assess a sensor suite with respect to its ability to detect faults in a timely manner it is desired to use a high fidelity approach to producing the propagation times for insertion to the digraph. Such an approach would include physics based simulation of a system. A fault condition may be simulated and the propagation time can be identified by analyzing the simulation parameters that are located downstream of the component that failed. Accurate propagation times may also be produced from calculations that take system characteristics into account. For instance, a propagation time can be identified for a system where liquids flow through conduit by dividing the speed at which the liquid is moving by the length of conduit.

There is a notion of characteristic propagation times as well. If the underlying physical mechanisms by which the faults propagate are known there may be a

characteristic time of propagation that accurately captures the way the system behaves. For example, electrical faults typically propagate at speeds determined by the transportation of electrons through wire. Some characteristic times for various functional flows are shown in table 3.1.

Table 3.1. Characteristic Propagation Times

<b>Functional Flow</b>	<b>Characteristic Time</b>
Electrical Energy	1-10 milliseconds
Data computation	10-100 milliseconds
Fluid flow	5-30 milliseconds
Radiative Heat Transfer	Minutes to hours
Gas flow	10 milliseconds – seconds

Regardless of what fidelity is needed for the propagation times that are inserted into the graph, an evaluation of a sensor suite may be performed to identify its ability to identify faults before they become critical. Times identified for each of the arcs and nodes are summed as the propagation path is followed. Conclusions may then be drawn as to which sensors have the ability to detect a fault before it leads to a critical event.

## 4. RS-68

The Rocketdyne RS-68 rocket engine is presented here to demonstrate Fault Propagation Timing Analysis (FPTA). According to Wood [2002] the RS-68 is the first new U.S. engine certified to fly since the Space Shuttle Main Engine over 20 years ago. The RS-68 powers the Delta IV Evolved Expendable Launch Vehicle (EELV). It is planned to use 5 RS-68 engines to power the Ares V Cargo Launch Vehicle (CaLV) of NASA's Project Constellation. The RS-68 is a complex system with expensive consequences of failure. FPTA is performed to assess candidate sensor suites with respect to timely critical failure detection within the RS-68. The analysis follows the steps outlined in the previous chapter.

### 4.1. INTRODUCTION TO THE RS-68

The RS-68 burns liquid hydrogen and liquid oxygen in a gas generator cycle. The engine has the capability of transitioning between full power and a minimum power level as commanded from the vehicle. The engine supplies gasses to pressurize the fuel and oxidizer propellant tanks. The RS-68 also provides for thrust vector and roll control by gimbaling the thrust chamber and the fuel turbine exhaust roll control nozzle. Turbo-pumps are directly powered through a single shaft by turbines. A gas generator powers the turbines in parallel with high-pressure hot gas combusted from propellants tapped off after the pumps. The engine has an ablative nozzle with a lining that is designed to burn away as the engine runs, dissipating heat. The RS-68 engine operating characteristics and schematic are shown in Figure 4.1 and 4.2, respectively.

	Full Power	Minimum Power
Thrust, vac (KN) (K kg-f/Klb-f)	3,341 341/751	1,922 197/432
Thrust, s/l (KN) (K kg-f/Klb-f)	2,918 299/656	1,499 153/337
Chamber pressure (MPa) (psia)	9.79 1,420	5.62 815
Engine mixture ratio	6.0	
$I_{sp}$ , vacuum (sec)	409	
$I_{sp}$ , sea level (sec)	357	




Figure 4.1. RS-68 Operating Characteristics

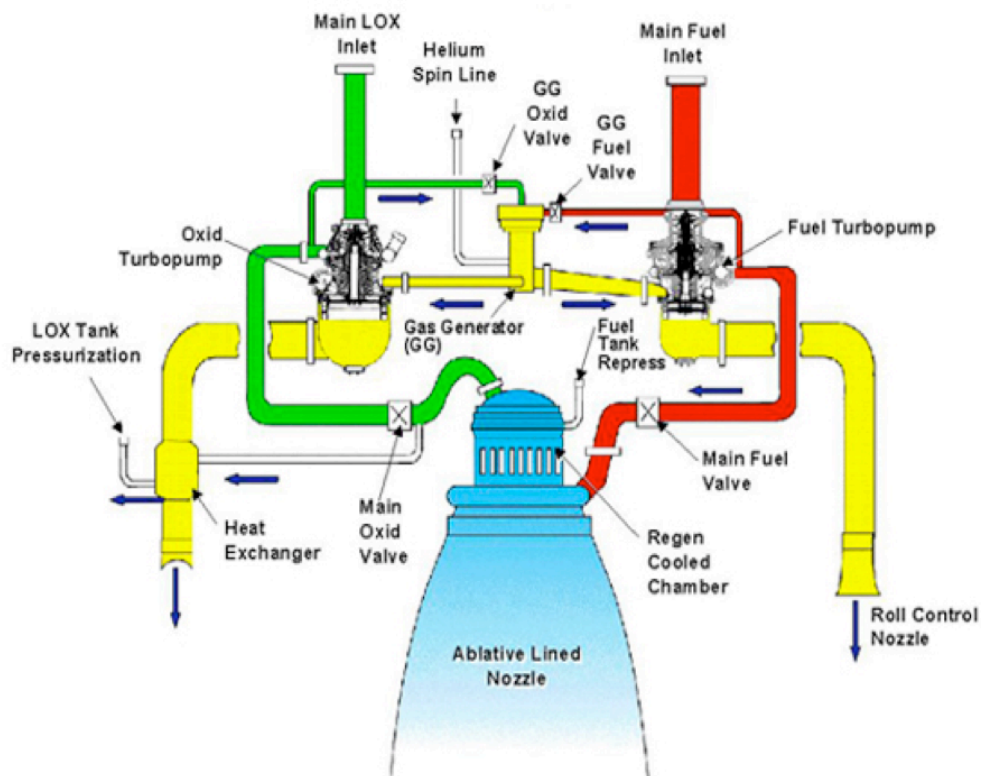


Figure 4.2. RS-68 Operating Schematic

## 4.2. STEP 1: BUILD RS-68 DIGRAPH

FPTA analysis is initiated on the RS-68 by building a directed graph, or digraph, to represent the architecture of the rocket engine. Components that represent failure sources for the engine are the nodes of the graph. Nominal flow paths between the components are modeled as the arcs of the digraph. These flows represent the functional dependencies between the components of the engine. The arcs are distinguished into three categories of flow types. Flows representing energy dependencies between components such as electrical and mechanical energy flows are represented by thin solid arrows. Thick solid arrows represent mass flows such as solid, gas, or liquid flows. Thin dashed arrows represent data flows that signify control signals or sensor data. A digraph that models the architecture of the RS-68 is shown in Figure 4.3.

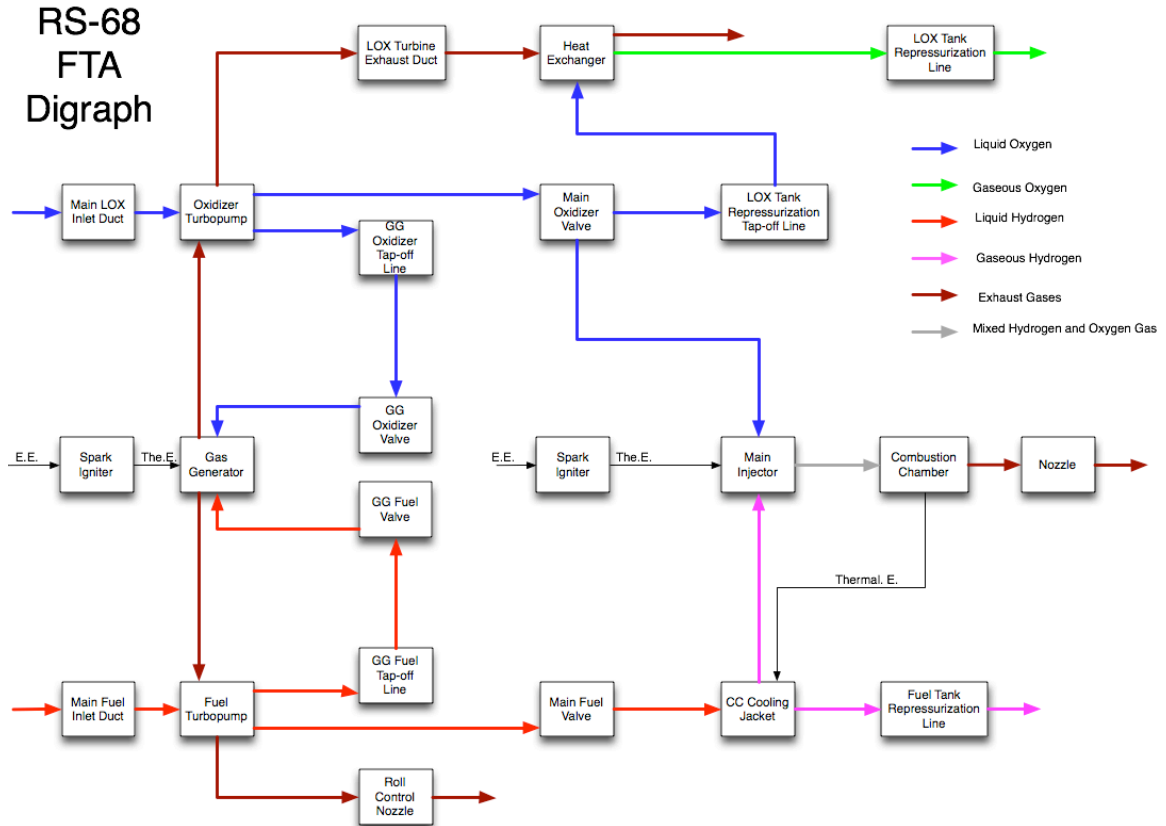


Figure 4.3. RS-68 Digraph

#### 4.3. STEP 2: IDENTIFY FAILURE MODES OF RS-68

To analyze fault propagation times of the RS-68, it is essential to identify the ways in which the system may fail. Failure modes are identified for each of the components that are modeled. A list of failure modes and effects associated with some of the components identified in the RS-68 digraph are presented in Table 1 of the Appendix. Immediate, downstream, and end effect are identified for each of the failure modes in this example FMEA. The failure mode and effect information is used to guide the FPTA process as the propagation paths and effect nodes are analyzed.



#### 4.4. STEP 3: INSERT CANDIDATE SENSOR SUITE

Candidate sensor suites may now be inserted into the digraph. An example sensor suite implemented on a rocket engine in order to initiate a shutdown in response to a critical failure is shown in table 4.1. A snapshot of the RS-68 digraph with the fuel pump discharge pressure and Fuel Turbo-Pump (FTP) shaft speed sensor inserted is displayed in Figure 4.4. The arcs that connect a component to the sensor represent the flow that is measured. For instance, the FTP shaft speed sensor measures the mechanical energy of the turbine shaft. Therefore a link that represents that mechanical energy is drawn from the turbo-pump to the sensor.

Table 4.1. Example Candidate Red-line Sensor List for the RS-68

Sensor	Location
Fuel Pump Discharge Pressure	FTP discharge duct just after the pump
Fuel Turbine Temperature	Hot gas inlet duct to the fuel turbine
Main Combustion Chamber Pressure	At the top of the combustion chamber
Fuel turbo-pump shaft speed	FTP
Oxidizer turbo-pump shaft speed	OTP

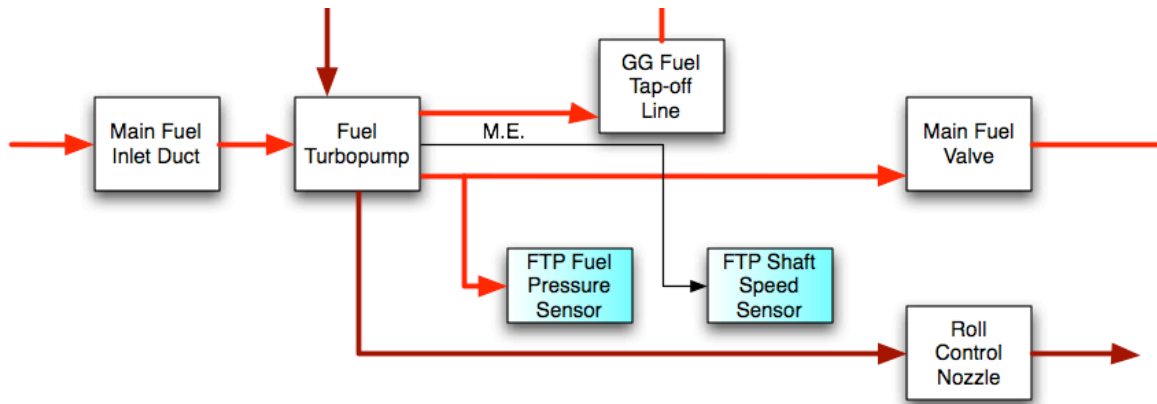


Figure 4.4. RS-68 Digraph Snapshot With Sensors

#### 4.5. STEP 4: IDENTIFY CRITICAL FAILURE POINTS OF THE RS-68

To identify fault propagation paths it is desired to identify the critical failure points that represent the costly consequences of a failure within a system. The example RS-68 FMEA located in Appendix A is a source of information that may facilitate the identification of the critical points in the digraph. For example, when the gas generator fuel valve exhibits the failure mode of being stuck closed, there is no fuel flow to the gas generator combustion chamber. This condition potentially leads to an explosion at the chamber due to oxygen rich conditions because the oxidizer valve allows oxidizer to flow without the fuel needed for complete combustion. This represents a critical consequence and may be indicated by another node in the digraph as shown in Figure 4.5.

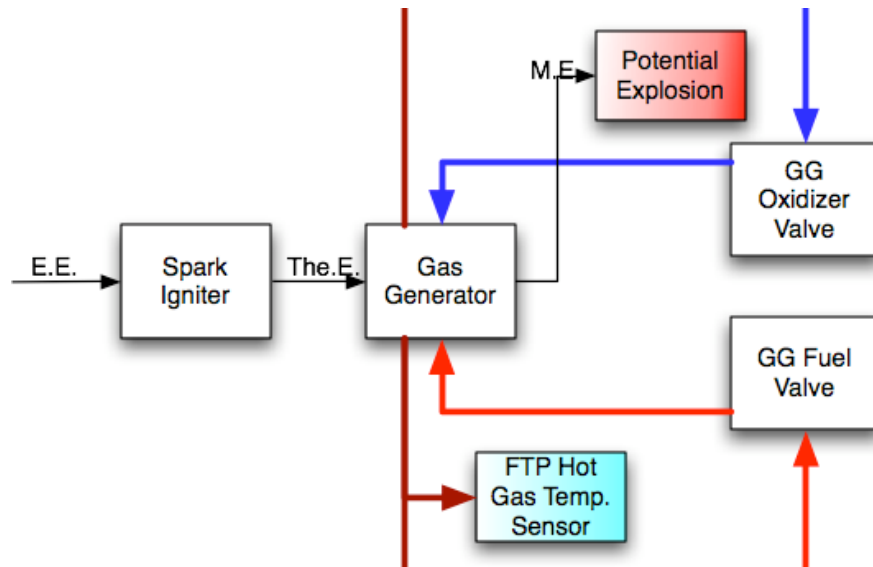


Figure 4.5. RS-68 Digraph Snapshot With Critical Point

#### 4.6. STEP 5: IDENTIFY FAULT PROPAGATION PATHS

The RS-68 digraph now has the essential elements that are needed to identify fault propagation paths that may then be used to initialize the timing analysis. A component along with a failure mode is chosen to implement the timing analysis. A failure of interest might be the pump head loss of the oxidizer turbo-pump. The effect of this failure eventually leads to a low thrust condition of the engine. The propagation path begins with the fuel turbo-pump and follows the flow dependencies modeled in the system to the critical failure point of low thrust that would be seen as an output of the nozzle. The propagation path may be seen in Figure 4.6. The propagation path indicates that there are potentially three sensors that can pick up the fault at different points in the system.

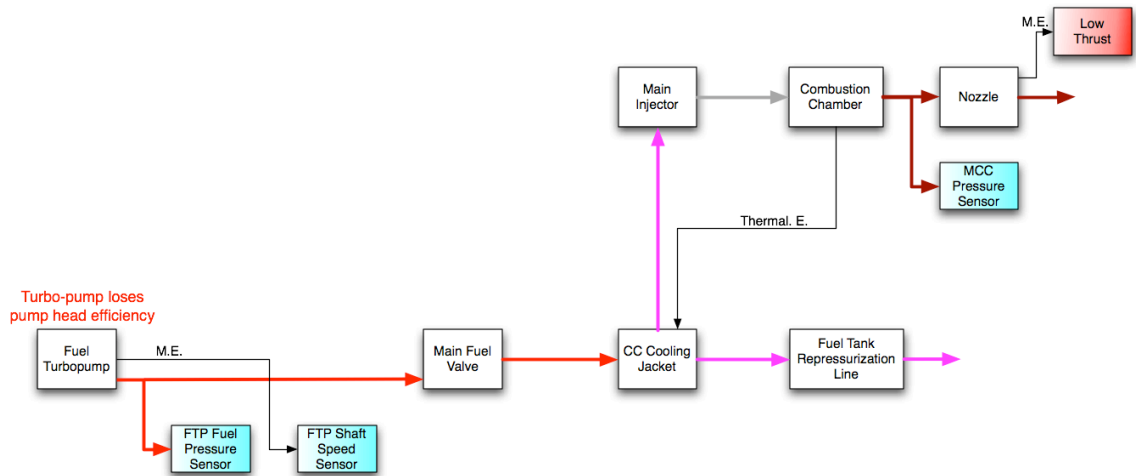


Figure 4.6. RS-68 FTP Head Efficiency Loss Propagation Path

#### 4.7. STEP 6: IMPLEMENT RS-68 TIMING ANALYSIS

To implement FPTA timing analysis the graph must be populated with fault propagation times for each arc and node. These propagation times will allow for determination of the time it takes for a fault to reach each component, sensor, and effect node in the graph. The fault propagation path for the RS-68 fuel turbo-pump head loss efficiency failure with propagation times identified is shown in Figure 4.7. A propagation time of 28 ms is indicated for the hydrogen flow from the fuel turbo-pump to the main fuel valve. The 28 ms represents the time from when the head loss first occurs to when the off-nominal pressure could be seen at the main fuel valve.

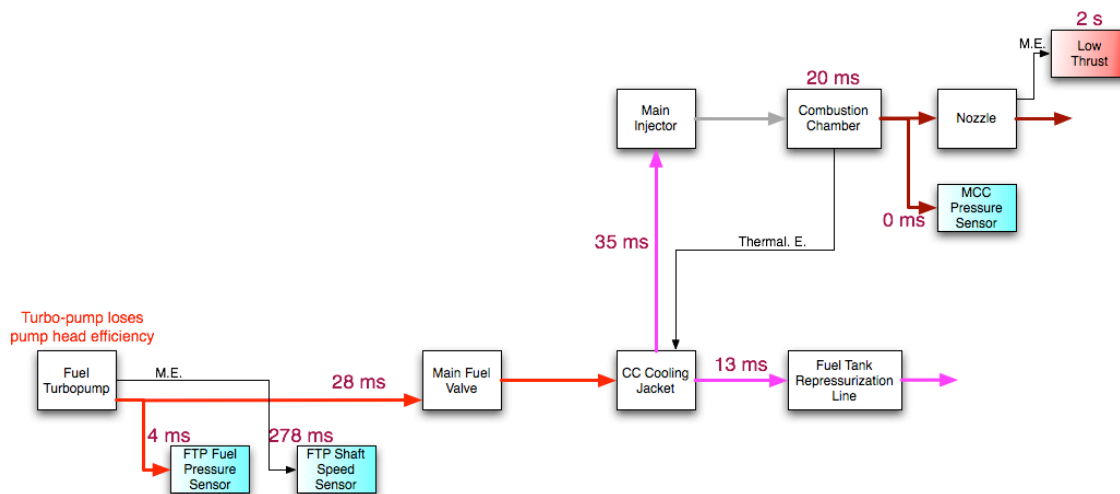


Figure 4.7. RS-68 Propagation Path With Times Included

#### 4.8. RS-68 FFTA CONCLUSIONS

There are several conclusions that may be drawn from the FFTA analysis of the RS-68 fuel turbo-pump head loss. First, there are several sensors in the propagation path that should have the ability of detecting the fault before it becomes critical. The off-nominal pressure may be sensed by the FTP fuel discharge pressure sensor within 4 ms of failure. The fault is sensed by the MCC pressure sensor 83 ms after the failure. This is not the end of the story for the sensors though. There are time constants that must be taken into account. In most cases the off-nominal flow will have to exceed a red-line before a fault will be recognized. This represents another latency that must be accounted for to complete an accurate assessment of detectability. These times may then be included in the digraph and the resulting sensor suite assessment will provide a time to detect measure. The FFTA analysis indicates that it takes 2.083 seconds for there to be a critical loss of thrust due to the FTP failure. The FFTA analysis allows for the time to

detect to be compared to the time to criticality for several sensor suites, therefore providing system designers with a strategy for assessing sensor suites with respect to their ability to detect faults in a timely manner.

## 5. CONCLUSIONS

In this thesis, a strategy for evaluating a sensor suite's effectiveness in detecting faults before they become critical has been presented. Fault Propagation Timing Analysis (FPTA), is a flexible approach to evaluating sensor placement for a system during various stages of design. Complex systems that have expensive consequences of failure, such as those in the aerospace industry, benefit from the concepts that are presented. FPTA was performed on Rocketdyne's RS-68 rocket engine to illustrate how the strategy may be implemented to compare the time to detect to the time to criticality.

The work presented in this thesis describes FPTA as an augmentation to several detectability evaluation strategies that may be implemented through the use of directed graphs. While previous approaches using digraphs were able to relate faults to sensors, FPTA goes further by attaching fault propagation times to the dependencies modeled in the graph. The propagation times may then be analyzed to identify time to detect and time to criticality. These metrics allow for an evaluation of a sensor suite's ability to detect a fault before it becomes critical.

FPTA is being utilized to assess the detection capabilities of NASA's Ares I launch vehicle. The analysis has successfully produced results that are being accounted for in the vehicle's design cycles. Details of outputs derived from the analysis are proprietary and are therefore not available in this work.

There are several challenges that exist in the further development of FPTA. While the analysis described in this thesis can identify the time it takes for off-nominal behavior of a system due to a failure to be sensed by a given sensor suite, there is no assessment of a time to process and provide a response to the failure. An extension to the

fault propagation timing work would be development of a strategy for identifying the time from failure detection to corrective action initiation as well as the time it takes for the corrective action to take place. The identification of these propagation times would allow a designer to make a comprehensive assessment of a system's ability to respond to any failure with the goal of avoiding critical consequences.

The successful implementation of FPTA is dependent on the failure data that is available for a system. An area of work that can support the development of useful FPTAs would be the development of a systematic approach to identifying cross subsystem failure modes. While modeling dependency paths in a digraph that represent nominal system behavior is usually straightforward, the identification of dependencies representing off-nominal failure propagation is a challenging proposition. Cross subsystem failures are very commonly not accounted for because of the nature of current design practices. If there were a strategy to account for these potential failures, an FPTA may be augmented to catch a comprehensive set of off-nominal conditions.



## APPENDIX

Table 1: RS-68 Example FMEA

Component	Failure Mode	Immediate Effect	Downstream Effect	End Effect
GG Fuel Valve	Stuck Closed	no flow to gg	oxyqen rich GGCC	Possible Explosion
	Stuck Open	none	none	none
	Stuck Partial	partial flow to gg	off-nominal combustion leading to lower engine thrust	Low Thrust
	External Leakage	none	oxygen rich environment	Possible Explosion
Fuel Turbopump	Friction	Efficiency Loss	low fuel flow to cc leading to lower thrust level	Low Thrust
	Turbine Blade Loss	Efficiency Loss	low fuel flow to cc leading to lower thrust level	Low Thrust
	Bearing Failure	no flow to cc	oxygen rich cc	Possible Explosion
	Pump Head Loss	Efficiency Loss	low fuel flow to cc leading to lower thrust level	Low Thrust
Main Fuel Valve	Stuck Closed	no flow to cc	oxygen rich CC	Possible Explosion
	Stuck Open	none	none	none
	Stuck Partial	partial flow to gg	off-nominal combustion leading to lower engine thrust	Low Thrust
	External Leakage	none	oxygen rich environment	Possible Explosion
GG Oxidizer Tap-off Line	External Leakage	low flow to gg	oxygen rich environment/off-nominal combustion leading to lower engine thrust	Possible Explosion/Low Thrust
	Rupture	Oxygen rich environment	Oxygen rich environment	Possible Explosion
	Clog	no flow to gg	incomplete combustion at gg leading to lower thrust level	Low Thrust

## BIBLIOGRAPHY

1. Wood, B.K., "Propulsion for the 21<sup>st</sup> Century—RS-68," *38<sup>th</sup> Joint Liquid Propulsion Conference*, AIAA 2002-4324, 2002.
2. Debouk, R., Lafortune, S., and Teneketzi, D., "On an Optimization Problem in Sensor Selection for Failure Diagnosis," *Proceedings of the 38<sup>th</sup> Conference on Decision & Control*, vol. 5, IEEE, 1999, pp. 4990-4995
3. Worden, K., and Burrows, A., "Optimal Sensor Placement for Fault Detection," *Engineering Structures*, vol. 23, 2001, pp. 885-901.
4. Eberhart, R., and Kennedy, J., "A New Optimizer Using Particle Swarm Theory," *IEEE Sixth International Symposium on Micro Machine and Human Science*, IEEE, 1995, pp. 39-43.
5. Osorio, M., and Hernández, E., "Cutting Analysis for MKP," *IEEE Proceedings of the Fifth Mexican International Conference in Computer Science*, ENC'04, IEEE, 2004, pp. 298-303.
6. Fletcher, R., *Practical Methods of Optimization*, 2<sup>nd</sup> ed., John Wiley & Sons, Chichester, 1987.
7. Narasimhan, S., Mosterman, P., and Biswas, G., "A Systematic Analysis of Measurement Selection Algorithms for Fault Isolation in Dynamic Systems," *Proceedings of the 9<sup>th</sup> International Workshop on Principles of Diagnosis*, DX-98, 1998, pp. 94-101.
8. Mushini, R., and Simon, D., "On Optimization of Sensor Selection for Aircraft Gas Turbine Engines," *Proceedings of the 18<sup>th</sup> International Conference on Systems Engineering*, ISCEng'05, IEEE, 2005, pp. 9-14.
9. Madron, F., and Veverka, V., "Optimal Selection of Measuring Point in Complex Plants by Linear Models," *American Institute of Chemical Engineering Journal*, vol. 38, no. 2, 1992, pp. 227-236.
10. Musulin, E., Benqlilou, C., Bagajewicz, M., and Puigjaner, L., "Instrumentation Design Based on Optimal Kalman Filtering," *Journal of Process Control*, vol. 15, no. 6, 2005, pp. 629-638.
11. Spanache, S., Escobet, T., and Travé-Massuyès, L., "Sensor Placement Optimisation Using Genetic Algorithms," *Proceedings of the 15th International Workshop on Principles of Diagnosis*, DX-04, 2004, pp. 179-183.

12. Sen S., S. Narasimhan and K. Deb, "Sensor Network Design of Linear Processes Using Genetic Algorithms," *Computers and Chemical Engineering*, 1998, vol. 22, 1998, pp. 385–390.
13. Santi, L.M, Sowers, T.S. and Aguilar, R.B., "Optimal Sensor Selection for Health Monitoring Systems," NASA/TM—2005–213955, 2005.
14. Zhang, G., "Optimum Sensor Localization/Selection in a Diagnostic/Prognostic Architecture," Ph.D. Dissertation, Electrical and Computer Engineering Dept., Georgia Institute of Technology, 2005.
15. Ali, Y., and Narasimhan, S., "Sensor Network Design for Maximizing Reliability of Linear Processes," *American Institute of Chemical Engineering Journal*, vol. 39, no. 5, 1993, pp. 820–828.
16. Ali, Y., and Narasimhan, S., "Redundant Sensor Network Design for Linear Processes," *American Institute of Chemical Engineering Journal*, vol. 41, no. 10, 1995, pp. 2237–2249.
17. Bagajewicz, M., "Design and Retrofit of Sensor Networks in Process Plants," *American Institute of Chemical Engineering Journal*, vol. 43, no. 9, 1997, pp. 2300–2306.
18. Bagajewicz, M., and Sanchez, M., "Design and Upgrade of Nonredundant and Redundant Linear Sensor Networks," *American Institute of Chemical Engineering Journal*, vol. 45, no. 9, 1999, pp. 1927–1938.
19. Azam, M., Pattipati, K., and Patterson-Hine, A., "Optimal Sensor Allocation for Fault Detection and Isolation," *IEEE International Conference on Systems, Man and Cybernetics*, vol. 2, IEEE, 2004, pp. 1309–1314.
20. Bagajewicz, M., and Sanchez, M., "Cost-optimal Design of Reliable Sensor Networks," *Computers and Chemical Engineering Journal*, vol. 23, 2000, pp. 1757–1762.
21. Bagajewicz, M., and Cabrera, E., "New MILP Formulation for Instrumentation Network Design and Upgrade," *American Institute of Chemical Engineering Journal*, vol. 48, no. 10, 2002, pp. 2271–2282.
22. Bagajewicz, M., Fuxman, A., and Uribe, A., "Instrumentation Network Design and Upgrade for Process Monitoring and Fault Detection," *American Institute of Chemical Engineering Journal*, vol. 50, no. 8, 2004, pp. 1870–1880.
23. Chmielewski, D., Palmer, T., and Manousiouthakis, V., "On the Theory of Optimal Sensor Placement," *American Institute of Chemical Engineering Journal*, vol. 48, no. 5, 2002, pp. 1001–1012.

24. Kretsovalis, A., and Mah, R., "Observability and Redundancy Classification in Multicomponent Process Networks," *American Institute of Chemical Engineering Journal*, vol. 33, no. 1, 1987, pp. 70–82.
25. Luong, M., Maquin, D., Huynh C., and Ragot, J., "Observability, Redundancy, Reliability and Integrated Design of Measurement System," *Proceedings of 2<sup>nd</sup> IFAC Symposium on Intelligent Components and Instruments for Control Applications*, SICICA'94, 1994.
26. Dochain, D., Tali-Maanar, N., and Babary, J.P., "On Modeling, Monitoring and Control of Fixed Bed Bioreactors," *Computers and Chemical Engineering*, vol. 21, 1997, pp. 1255–1266.
27. Muller, P., and Weber, H., "Analysis and Optimization of Certain Qualities of Controllability and Observability for Linear Dynamical Systems," *Automatica*, vol. 8, 1972, pp. 237–246.
28. Van den Berg, F., Hoefsloot, H., Boelens, H., and Smilde, A., "Selection of Optimal Sensor Position in a Tubular Reactor Using Robust Degree of Observability Criteria," *Chemical Engineering Science*, 2000, vol. 55, 2000, pp. 827–837.
29. Papadopoulos, M., and Garcia, E., "Sensor Placement Methodologies for Dynamic Testing," *AIAA Journal*, vol. 36, no. 2, 1998, pp. 256–263.
30. Hac, A., and Liu, L., "Sensor and Actuator Location in Motion Control of Flexible Structures," *Journal of Sound and Vibration*, vol. 167, no. 2, 1993, pp. 239–261.
31. Raghuraj, R., Bhushan, M., and Rengaswamy, R., "Locating Sensors in Complex Chemical Plants Based on Fault Diagnostic Observability Criteria," *American Institute of Chemical Engineering Journal*, vol. 45, no. 2, 1999, pp. 310–322.
32. Tumer, I., Stone, R., Bell, D. (2003) Requirements for a Failure Mode Taxonomy for Use in Conceptual Design, *Proceedings of the International Conference on Engineering Design, ICED 2003 – 1612*.
33. Bahr, Nicholas J., 1997, *System Safety Engineering and Risk Assessment: A practical approach*, Washington, D.C.: Taylor and Francis.

## VITA

Jeremy Ryan Johnson, son of Greg and Rebecca Johnson, was born on September 27, 1980 in Vienna, Austria. Jeremy attended several Austrian grade schools before completing fifth grade at the Vienna Christian School in Vienna, Austria. At the age of 12 his family moved to Salina, Kansas, where he graduated from Salina Central High School. After high school, Jeremy attended Garden City Community College on a football scholarship and was a member of Phi Theta Kappa, graduating with an A.S. in Science. He then transferred to the University of Missouri-Rolla on a football scholarship to pursue a B.S. in Mechanical Engineering and continued on to receive his M.S. in Mechanical Engineering in May 2008.

While an undergraduate at UMR, Jeremy worked with Dr. Robert Stone and Dr. Daniel McAdams as a research assistant on a project where he built functional models of many electro-mechanical devices for population of a design repository in the summer of 2004. After Jeremy's football career came to a conclusion at the end of the fall semester of 2004, he continued to work with Dr. Stone and Dr. McAdams to populate the repository until he was accepted for an internship at NASA Ames Research Center (ARC) in the summer of 2005. At ARC Jeremy worked with Dr. Irem Tumer to build functional models of complex aerospace systems. He then returned to UMR to attend graduate school under advisers Dr. Stone and Dr. McAdams for the fall semester of 2005. Jeremy then accepted a full time position at ARC to work on modeling of the Ares I Launch Vehicle in January of 2006. Jeremy continued to fulfill the requirements for his degree while working at ARC and in May 2008 he graduated with a M.S. in Mechanical Engineering from UMR.

Jeremy married Joanne Marie Thornburg on May 31<sup>st</sup> 2003. On July 20<sup>th</sup> 2006, they welcomed the birth of their daughter, Hayley Marie Johnson. Jeremy continued to work at NASA Ames through 2008.