A DESIGN APPROACH TO A RISK REVIEW FOR FUEL CELL-BASED DISTRIBUTED COGENERATION SYSTEMS

A Thesis

by

KRISTIN LYN LUTHRINGER

Submitted to the Office of Graduate Studies of
Texas A&M University
in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

May 2004

Major Subject: Mechanical Engineering

A DESIGN APPROACH TO A RISK REVIEW FOR FUEL CELL-BASED DISTRIBUTED COGENERATION SYSTEMS

A Thesis

by

KRISTIN LYN LUTHRINGER

Submitted to Texas A&M University
in partial fulfillment of the requirements
for the degree of

MASTER OF SCIENCE

Approved as to style and content by:

Thomas Lalk (Chair of Committee)	
John Appleby (Member)	Rodger Koppa (Member)
William Schneider (Member)	Dennis O'Neal (Interim Head of Department)

May 2004

Major Subject: Mechanical Engineering

ABSTRACT

A Design Approach to a Risk Review for Fuel Cell-Based Distributed Cogeneration Systems. (May 2004)

Kristin Lyn Luthringer, B.S., Texas A&M University

Chair of Advisory Committee: Dr. Thomas Lalk

A risk review of a fuel cell-based distributed co-generation (FC-Based DCG) system was conducted to identify and quantify the major technological system risks in a worst-case scenario. A risk review entails both a risk assessment and a risk analysis of a designed system, and it is part of risk engineering. Thorough literature reviews and expert interviews were conducted in the field of fuel cells. A thorough literature review of the risk engineering field was also conducted. A procedure for a risk review of the FC-Based DCG System was developed. The representative system design was identified by the current DCG design technology. The risk assessment was carried out, identifying the system components and potential failure modes and consequences. Then, using probabilities of failure for the various system components, the risk associated with a particular system design was determined.

A Monte Carlo simulation on the total system reliability was used to evaluate the potential for system failure at a time of 1 hour, 5 hours, 10 hours, 50 hours, 100 hours and 500 hours of continuous operation. The original system was found to be acceptable at the initial times, but after 100 hours was predicted to fail. The components which consistently contribute significantly to the overall system risk are the membrane electrode assembly (MEA) and the nickel-metal foam flow fields. A revised system was analyzed with the reliability of the MEA and the Ni-foam set to 100%. After the revision, the components which contributed significantly to the system risk were the pumps. Simulations were run for several alternative systems to provide feedback on risk management suggestions. The risk engineering process developed with the design approach for this research is applicable to any system and it accommodates the use of many different risk engineering tools.

ACKNOWLEDGEMENTS

I would like to thank my committee chair, Dr. Thomas Lalk, for his insights and determination to see this research done completely and described to the lowest level of detail. I would also like to thank the members of my thesis committee, Dr. John Appleby, Dr. Rodger Koppa, and Dr. William Schneider for their insights and patience. I am honored that such great engineers as these would encourage me during my course of study and lead me in the right direction as I struggled to unlock the vast subjects before me.

Special thanks are extended to my coworkers and fellow graduate students Erik Snyder and Arthur Thomason for all their help answering my questions and to James Schaefer for his editing assistance. A gracious acknowledgement is made to the Center for Electrochemical Systems and Hydrogen Research for funding this research project, and to the Department of Mechanical Engineering for supporting my education by providing a departmental fellowship.

Finally, I would like to thank all the friends and family who supported and inspired me to see this through to the end and who prayed for me all the way there.

TABLE OF CONTENTS

Page

LIST OF FIGURES

LIST OF TABLES

INTRODUCTION

The current primary system for creating electricity in the United States is by generation at centralized large-scale power plants, using various methods. Electricity delivery presently occurs as allocation from the central plant through a grid of power lines, a power conditioning system, and transmission-boosting substations to the end user. Since deregulation of the energy market took effect the electric companies have argued over who will maintain this aging grid infrastructure and few are willing to heavily invest in repairs or in expansion. The centralized power plants have very high capital costs to build and have long lead-times to install and bring up to full capacity so there is a reduced incentive to build new plants. So, as the demand for electricity keeps increasing, the centralized system is slow to respond. Another reason that centralized power plants are not being built is that the traditional thought process of NIMBY, or not in my backyard, has moved to BANANA, or build absolutely nothing anywhere near anybody, due to the widespread public fear of living near high-voltage power lines. Still, Americans have grown used to having their electricity readily available and do not like being subjected to "brown-outs" or periods of no/low power due to a peak in electricity demand or a problem with the grid. One method proposed to boost electrical generation without the stigma of centralized plants and to provide better availability for the small, residential consumer is through the use of distributed generation – small-scale electricity generation for the individual residence or for a small group of users. With the smaller transmission distance between the source and the end user it becomes cost-effective to use the waste energy from the distributed electricity generation processes at the residence. This dual use leads to the term distributed co-generation (DCG) system, alternatively called a combined heat and power system, and it can lead to a higher thermal efficiency. Since FC-Based DCG is an emerging market in the energy industry, having a means to determine whether or not a particular system's configuration and implementation will likely be successful while still in the design stages would be invaluable as far as the costs and person-hours potentially saved from a "lessons-learned" experience. One method to evaluate the system design is to use risk.

The objective of this research was to utilize risk engineering in order to determine the current FC-Based DCG design parameters and operating conditions that contribute the

---

This thesis follows the style and format of Journal of Power Sources.

most to the technological system risk. This was accomplished by using the design approach to organize, systematize, and clarify all the background information for risk engineering and then applying the risk review portion of the risk engineering process to an example FC-Based DCG system.

This thesis is structured in order to discuss the pertinent aspects of the risk review for a FC-based DCG system which is a part of the larger risk engineering process. The characteristics of the risk engineering process will be noted using a design approach. Then, the current status of FC-Based DCG systems will be explored. Next, the specific functions and procedure for the two research focus areas will be presented as the risk engineering process is applied for FC-Based DCG. Finally, the results will be discussed and conclusions drawn.

Characteristics of Risk Engineering

The general objective of the risk engineering process is to understand what events can happen to a designed system, how likely it is that the events might happen, the consequences that could occur if the events happen, and the confidence in predicting the answers. Risk engineering is a useful tool because it reduces waste of product, raw materials, and human resources. It can increase the chance of remaining in business and making a profit in the market by potentially preventing failure through design, improving overall safety, and increasing reliability of equipment. By identifying areas where the risk can be controlled, essentially where the possibility of failure can be reduced and/or where the consequences of the failures can be mitigated, risk reviews feed information to risk management. It is risk management that is then charged with ensuring the risk associated with the design is acceptable. When implemented correctly, the risk engineering process will result in improved public image and in avoidance of possible legal problems by increasing product reliability.

There are several key benefits that a risk engineering process can specifically bring to DCG. The benefits include providing comparisons of alternative configurations in order to create a better design of the system, providing identification of alternative procedures, and providing documented and logical evaluation of trade-offs involved in the decision making process. These benefits would allow the risk management portion of the engineering process to provide the emerging DCG market with a design tool that can be used to

troubleshoot the system design before creating the beta-test (preproduction) prototype for initial trials. The risk review portion of risk engineering should enable identification of which of the technical barriers can be overcome (failure prevention) and which are the most likely failure modes that should be mitigated. The risk management portion of risk engineering should present suggestions to make the system more reliable and safer. Many industries use risk engineering as a tool in their daily operations and planning operations because of its many benefits. [1] Table 1 below lists several industries that currently use some form of risk engineering in their decision making process.

Table 1: Industries that Use Risk Engineering [1]

Aerospace	Construction
Consulting	Education
Energy, Oil & Gas	Environmental
Finance & Financial Planning	Facilities
Government	Insurance
Medical Devices & Healthcare	Military
Project & Cost Management	Pharmaceutical
Public Policy Research	Real Estate
Semiconductor & Microelectronics	Technology
Telecom	Utilities

Defining "risk" is difficult because the general meaning is vague. Everyone has his or her own interpretation of what is "risky"! A literature review of the field of risk analysis demonstrates that there is not much consensus even among the experts. Much discussion centers around defining what the relevant risks are for the different situations to be analyzed and what weight to put on the values that will ultimately be used to evaluate those risks. There is also dissention on which is the best method to use in a certain situation. The methodology of an engineering design approach should be a very useful tool in combining the risk engineering knowledge into a cohesive process. Since most risk personnel agree upon the principles of risk engineering but disagree on the details, the systematic design approach can give a framework of issues to address in risk engineering while leaving open the choice of tools to use when implementing the risk assessment, risk analysis, or risk management.

One key idea to take from the experts is to define upfront the type of risks at which one is looking and the magnitudes of the potential consequences. An important fact to keep in mind is that different kinds of risk exist, and it is the perception of those risks that is reality. The actual risks pertaining to a design can be overstated or understated by how the design is viewed. Many of the aspects surrounding a technology, such as market pressure from consumers or product/company safety records, can change how the public views the risk associated with a particular design. Figure 1 below graphically demonstrates the external pressures that affect how the public perceives a risk.

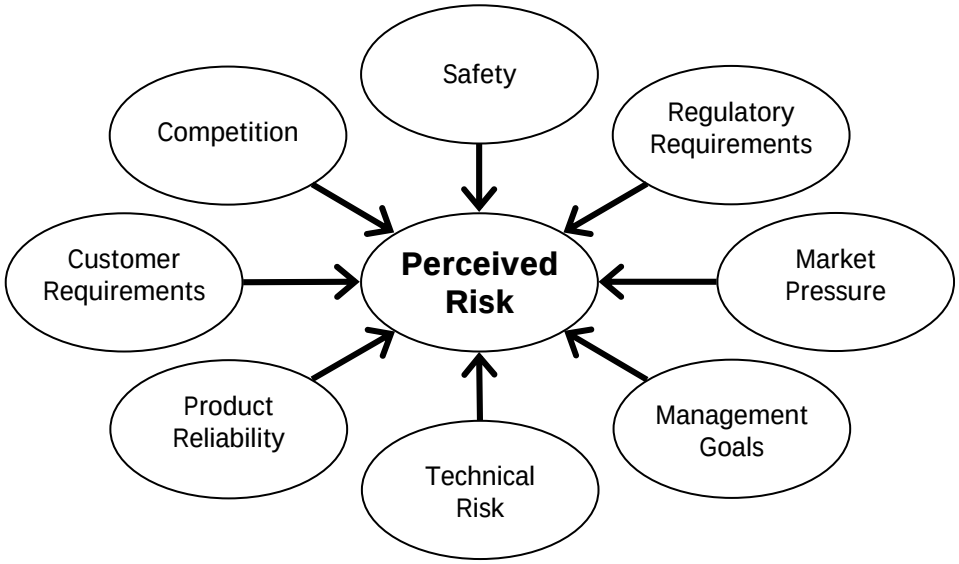

Figure 1: Factors Affecting the Perception of Risk [2]

The difficulty in defining risk is compounded further because several types of risk exist. There is technical risk – associated with the equipment, technology, and science of systems; programmatic risk – including operational hazards and safety of designs; supportability risk – associated with marketability and viability concerns; cost risk – connected with financial impact in all aspects of the system; schedule risk – including the time impact of the design lifecycle; and political risk – associated with public opinion and governmental regulations. All types of risk can be factored into the relative riskiness of a project. A general engineering division would be primarily focused on technical risk and to some extent programmatic risk.

Even so, engineers must be aware of the other types of risk as they may also affect the total perceived risk of a project much like the aforementioned pressures on public risk perception.

Specific definitions of key vocabulary are needed in order to minimize confusion among risk engineers, who are the practitioners of risk assessment, risk analysis or risk management in an engineering design company. Risk is defined to be the probability of occurrence and the consequences of an undesirable event, part of which can be reduced by design, part of which can be reduced by transfer, and the remaining residual, or "leftover", risk that must be less than some tolerable level. [2] When this residual risk is greater than the tolerable level, the project is too risky to pursue. Still, some other measures of risk control may exist that, when implemented, would reduce that residual risk to acceptable levels. The undesirable event is defined to be the occurrence of a failure, a partially unsuccessful occurrence, a problem, an accident, a loss, damage, or danger. The probability is defined to be the likelihood of occurrence, and the consequences are defined to be the effects of the occurrence. The harmful effects of the occurrence of an undesirable event are usually of concern to engineers trying to prevent failure of their designs, whereas the non-harmful effects are not given a priority. This identifies an important point commonly misunderstood by the public – if an undesirable event is not harmful, then it is not a true risk. Likewise a hazard, or unsafe condition, is only a risk if someone or something is exposed to it. [3] Risk engineering is defined to be all the paraphernalia, procedures, tools, representations, and actions that involve the application of a broad spectrum of sciences in order to solve problems that must accomplish multiple, contradictory goals. [4]

A design approach to the risk engineering process has been taken to determine the best procedure to adopt. This entails taking the need for risk engineering, determining the top-level functions required to fulfill that need, and decomposing those top functions into lower-level functions. The function structure is a useful device to accomplish the functional decomposition in which the relationships between the necessary functions can be easily observed. It is also constructive to determine what needs to be done before deciding on how to proceed. This format potentially allows for the use of different risk-related tools when evaluating various designs in diverse situations. The function structure also displays the chronological process of risk engineering when read left to right.

It is useful to note the differences between risk engineering from a design approach and traditional risk methodologies. In the traditional way of conducting risk engineering, information is widely scattered and tool-specific (focused on PRA, FMEA, etc.). The documentation must be consciously generated and isn't always organized but is definitely needed for traceability and legal defenses. Some risk engineers have a dedication to specific risk tools with which they are very familiar. This sometimes results in information from which risk management is not easily carried out. On the other hand, this design approach to risk engineering allows entrants to risk engineering to understand what is needed (in analysis), to learn and apply the tools rapidly, and to minimize inadvertent omission of key points. A logical, defensible display of the risk engineering decisions is easily obtained. Also, this approach ensures the risk review produces information that is usable in risk management.

It is also useful to note some important differences in risk assessment and analysis as defined here and the words as defined by the prominent risk methodology prescribed by the United States Environmental Protection Agency (EPA). For this research, the focus is on a company's design risk as it would be addressed within a department and risk assessment describes the first, qualitative part of a risk review while risk analysis refers to the second, quantitative part. The EPA is primarily focused on human health risk and therefore the EPA risk assessment guidelines (RAGS) treat assessment and analysis as interchangeable words. The four functions under an EPA-prescribed risk assessment are hazard identification, toxicity (or dose-response) assessment, exposure assessment, and risk characterization. The EPA focus is also more on the cancer and non-cancer (illness) effects of anthropogenic and natural chemicals in the environment, whereas the risk engineering process looks for all the potential end states of the design and tries to ensure a successful system. [3] While this format works for a remedial situation where the damage is already done, it is not very useful for trying to troubleshoot a design in order to prevent damage.

Returning to the design approach, the three major functions of a risk engineering process necessary to achieve the objective are reviewing risk in the design, creating documentation of the risk, and managing (optimizing) the risk. Reviewing risk in the system entails both assessment and analysis.

Creating documentation entails first understanding what is useful information, then obtaining, organizing, and presenting that information in a constructive manner. This second top function is necessary to ensure the data and ideas from the risk review function are useable by the risk management function and that the potential design solutions to optimize the risk from the risk management have enough information to be checked by another risk review. If the other two top functions are done properly, this documentation can fall right out of the work without much effort. Care must still be taken when presenting the risk information because if the documentation is improperly done, this can become a liability.

Risk management entails evaluation of the risk data generated by the risk review, control of risk through prevention or mitigation (i.e. changing the system if the risk is unacceptable), and monitoring both the non-design elements of risk reduction and the residual (i.e. "leftover") risk. Since risk reduction by decreasing the occurrence of the effects is weighed against cost, an alternate way of looking at risk management is to think of it as implementing risk optimization. Recommendations for design improvements should result from the risk review; however, the management function must be carried out by the implementer of the FC-Based DCG system (or the company owning the evaluated technology) according to their own values, practices, and policies.

One of the major reasons for separation of the management function from the review function is to prevent bias in the risk review. This could happen if by knowing that the company can only spend a certain amount of money in fixing a problem, a reviewer stopped assessing the system risk once a certain number of problems were found. The functions as discussed to this point are relevant to all designs on which the risk engineering process can be used. Further decomposition of the risk assessment and risk analysis functions under the risk review will be specific to the example FC-Based DCG design being reviewed and will illustrate the differences between the two processes. Figure 2 on the following page is a function structure displaying the top functions and their relationships to one another as well as the breakdown on the risk engineering process as it could be applied to any system.

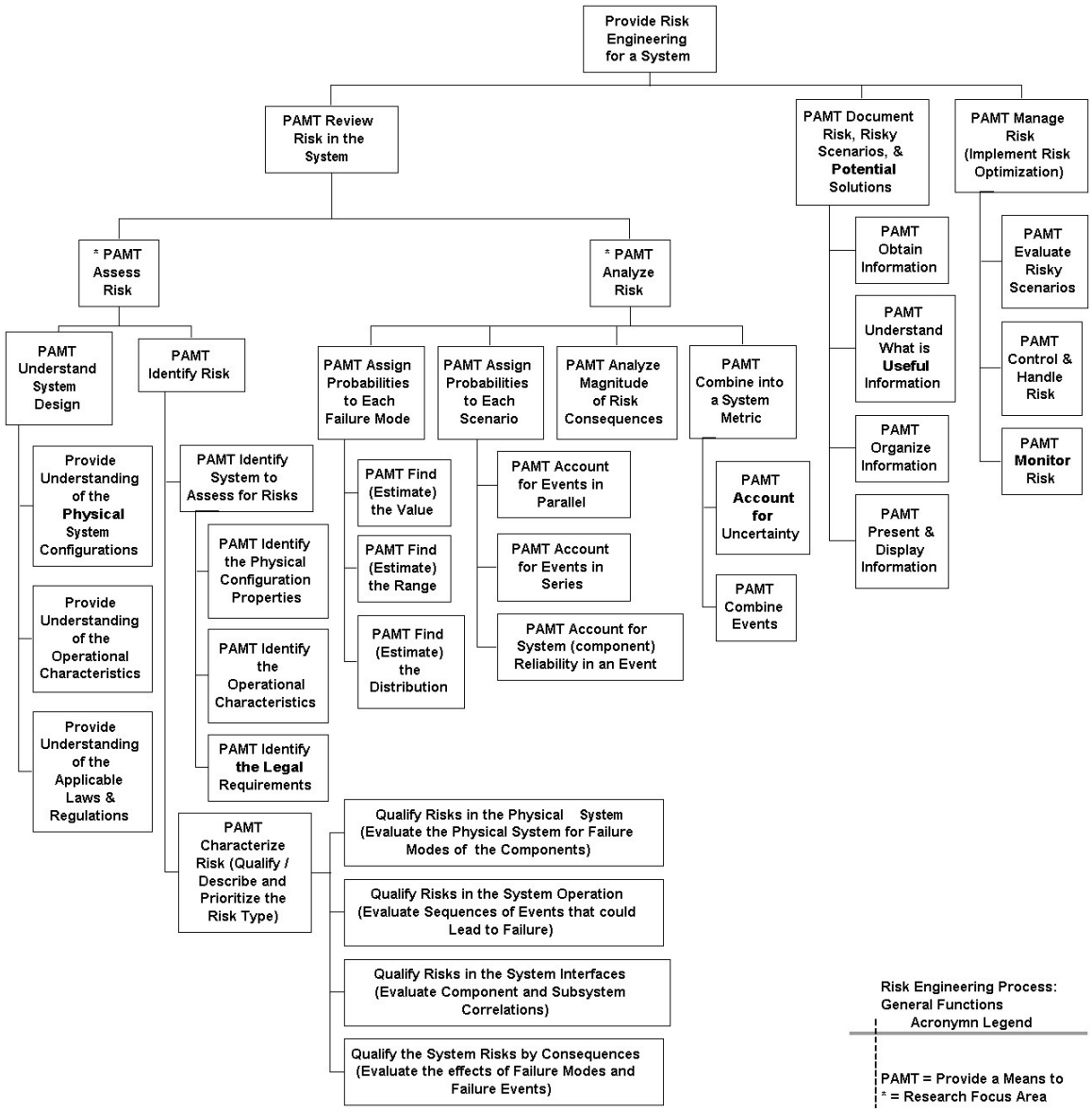

Figure 2: Functions of the General Risk Engineering Process

Now, one of the utilities of the function structure can be appreciated. As can be readily seen in Figure 2, the function structure allows for design iterations (or "looping") between risk management and risk review through the risk documentation.

As part of the risk review, the functions of assessing risk and analyzing risk are the focus areas and will be discussed more in the research section of this thesis. Recalling that when the risk review and the risk management functions are fulfilled properly the risk documentation naturally is completed, the next portion of the risk engineering process to

discuss is the risk management functions from Figure 2. The three functions necessary in order to optimize risk are: evaluation of the risk review information, control of the calculated risks of concern, and monitoring both the changes and the residual risk in the system design. Risk evaluation connotes deciding what tolerable risk is. The identification and decision of acceptability limits for the system design must be made within societal norms and with respect to the background levels of risk currently accepted by potential users of the design. At this point in the process, potential trade-offs in the system are identified. Risk control is preventing or mitigating the risks of concern for the system. Design mitigation changes try to ameliorate the effects of the failure but do not change the failure mode, like adding redundancy. For example, an air bag does not prevent the car wreck but rather tries to ensure passenger safety during one. On the other hand, design prevention changes modify the probability of the failure or even eliminate the failure mode itself, like adding a safety factor for ensuring material strength. The identification of alternatives or other changes is decided upon at this stage. Risk monitoring involves tracking the non-design risk reduction methods and the residual risk. During this portion of the risk engineering process, such things as inspections, maintenance schedules, tracking checklists, or other procedural changes to transfer risk would be implemented. It is important to identify the residual risk – the level of risk that is "leftover" once all design and non-design reduction methods have been implemented. As mentioned previously, it is this residual risk that must be at or below the tolerable level determined in the risk evaluation portion in order to continue with the project. The expected result of risk management is a system design optimized for the minimal risk with respect to minimal cost. [5] The trade-off criteria and the design changes to optimize risk will have been identified. Alternative configurations and/or components will have been proposed and the best ones chosen for implementation. The controls to optimize the systems risk, such as inspections, procedures, tracking, etcetera, will have been proposed. The final task to complete the risk engineering process objectives – the risk management portion – is truly one for an implementer of the system as only they are able to determine how much risk reduction is worth the cost to them.

Before discussing the background information for FC-Based DCG, it is necessary to note that there is a large issue to consider when creating and performing a risk review. This is summed up by the following quote:

> Many risk-related decisions are driven by perceptions, not necessarily objective risk as defined by [calculations]. Perceptions of consequences tend to grow faster than the consequences themselves — that is, several small accidents are not perceived as strongly as one large one, even if fatalities are identical. [5]

Two major implications can be gleaned from this quote. First, it is necessary not only to create a risk review of the system, but to do it right! Sloppy work will lead to negative perceptions of the system, which is not good for either the design or the company producing the design. It will also increase the difficulty in improving the design if risk managers try to use information generated by a poor risk review. Second, risk engineers must use their hearts as well as their minds, especially when making judgments between alternatives. If we omit from consideration the public perception of our work, a grounded engineering decision may appear to be without base.

Characteristics of FC-Based DCG

The method for boosting electrical generation and providing better availability for the small, residential consumer that is the focus of this research is distributed generation. Several current technologies already exist for the power plant of a DCG system, including the popular internal combustion (IC) engine. If the IC engine were to be widely used for the power plant of a DCG system, the IC engine system would only increase the nation's current dependence on foreign oil and it could potentially increase the well-known detrimental environmental effects by proliferation of IC engines. Therefore, the research impetus has been for a fuel cell-based power plant in DCG systems due to the fact that fuel cell systems produce low emissions of pollutants and that water is the only byproduct. Ideally, hydrogen fuel gas would be derived from electrolyzed water (with the electricity generated from renewable resources like solar, wind or geothermal); however it is currently reformed from natural gas or methanol. The fact that the current government administration has shown great interest in a "hydrogen economy" has also added to the interest in FC-Based DCG.

Several types of fuel cells exist today as option for use in DCG including Alkaline FCs, Phosphoric Acid FCs, Molten Carbonate FCs, Solid Oxide FCs, Regenerative FCs, Zinc Air FCs, and Protonic Ceramic FCs. There are several advantages & disadvantages for each type of FC explained in [6]. The Center for Electrochemical Systems and Hydrogen Research (CESHR) at Texas A&M University has chosen the platform of the Polymer Electrolyte

Membrane, alternately called a Proton Exchange Membrane, for its fuel cell-based distributed co-generation (PEM FC-Based DCG) system using reformate fuel gas. The CESHR system is the example design used in this risk review, therefore the characteristics of only the PEM FC are discussed. How a typical PEM FC-Based DCG system would work starts with a description of the acid-based fuel cell itself. An electrolyte that only allows the passage of hydrogen ions would be placed between an anode to which hydrogen gas is fed and a cathode to which oxygen is fed. Hydrogen ions on the anode side of the cell would pass through the electrolyte while the electrons would pass through an electrical circuit. On the cathode side of the electrolyte, the hydrogen ions would recombine with oxygen and the electrons forming water. [6] This typical system operation for a proton electrolyte is depicted by the anode & cathode reactions in Figure 3 below.

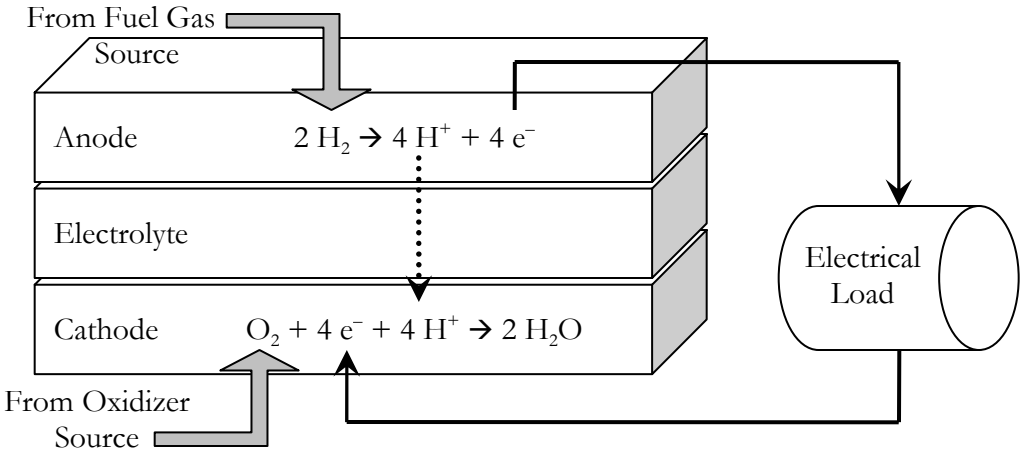

Figure 3: Reaction Schematic for a Single Acid-Based Fuel Cell

The anode-electrolyte-cathode layers in the diagram of Figure 3 create the membrane electrode assembly (MEA) for the FC. One is able to combine a fuel cell in a series connection called a "stack" to increase the voltage output, but the current remains the same. A method of cell stacking employs a layer of conductive material known as a bipolar plate to join the anode side of one MEA to the cathode side of the next MEA in series. This allows fuel channels to be machined onto both sides of the bipolar plate to feed the fuel gas and oxidizer to the appropriate sides of the MEA as well as cooling channels to be machined

throughout the plate. When fuel cells are stacked, a means to distribute that fuel gas and the oxidizer over the electrodes is needed to ensure that all areas of the MEA are utilized to generate electricity. This has been accomplished in the past with graphite plates. A combination of bipolar plates and nickel metal foam allows greater fuel/oxidizer distribution over electrode by providing a better flow field without losing efficiency in the series connections. The CESHR system uses such a combination bipolar plate and Ni-Foam for its flow field and series connections. The balance of plant (BOP) is all the remaining peripheral equipment used in the system such as: pumps, blowers, and/or compressors; intercoolers, pre-heaters, and/or heat exchangers; power conditioning, direct current (DC) to DC converters, a DC to alternating current (AC) inverter, and/or electric motors; fuel processing system (reformer, desulfurization, etc.); fuel storage system; control valves and pressure regulators; and controllers. Top-level functions for the DCG system are the same regardless of the type of FC used as its power plant. The system must: intake fuel, reform fuel to hydrogen/fuel gas/reformate, control fuel cell operation, condition generated power to clean AC, output power, interface with a grid network, provide energy storage for start-up and excess loads/peaks for when not connected to a grid, and provide a marketable alternative to other, centralized power sources. [7]

A further look into the CESHR DCG system design shows much more than a single PEM FC. Figure 4 on the following page depicts the parts of the fuel cell stack that CESHR will use for its DCG System, including bipolar plates, nickel foam assemblies, and MEA, where the MEA consists of a polymer electrolyte, and two electrodes.

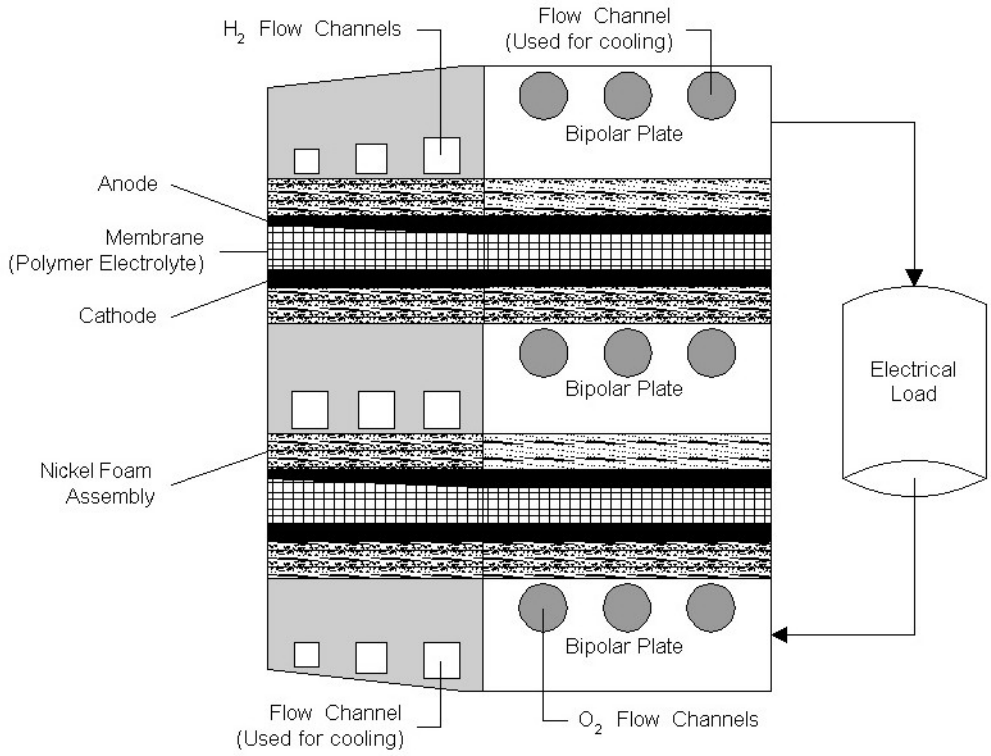

Figure 4: Fuel Cell Stack Schematic

The current general BOP configuration for the CESHR system consists of a reformed methane (natural gas) fuel supply system, a bipolar plate-delivered water-glycol cooling system for cogeneration, and a DC/AC power conditioning inverter system. The full system schematic in Figure 5 on the following page displays all the equipment needed, minus the control system. A full prototype commercial unit has not yet been built, so the diagram that follows is simply the planned system.

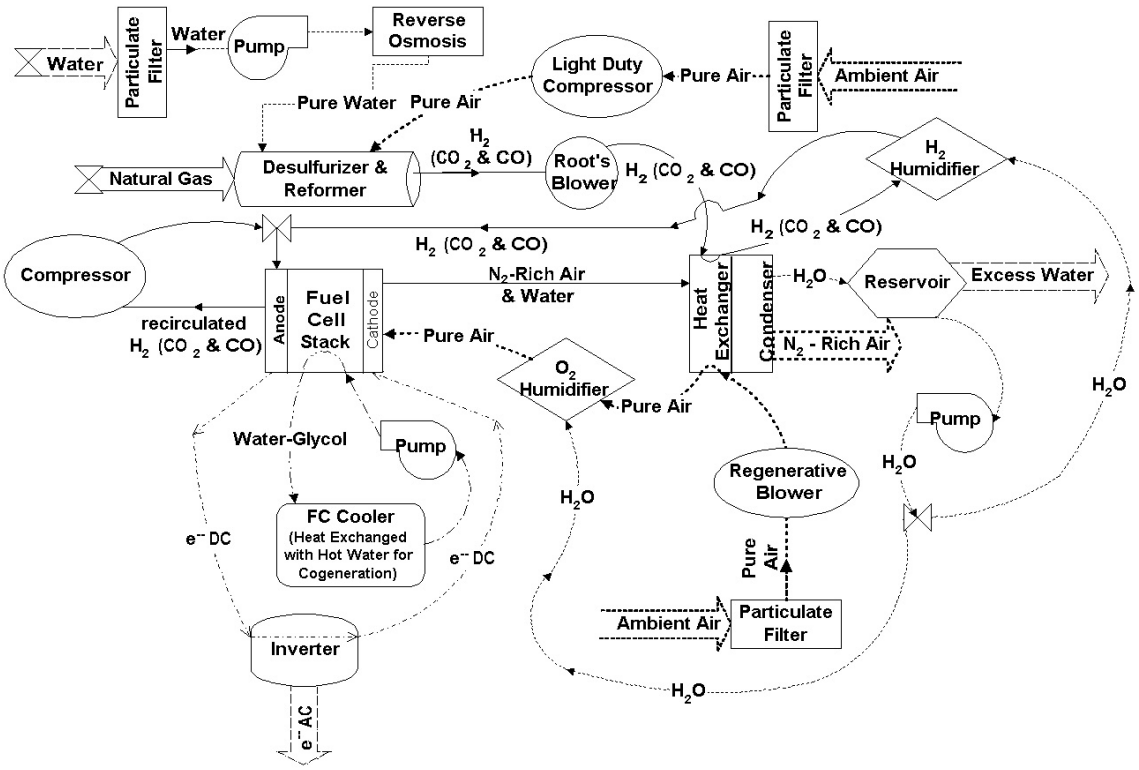

Figure 5: Distributed Cogeneration System Schematic

Currently, there exist many benefits and barriers for DCG systems in general and specifically for FC-Based DCG systems. Some of the many benefits for DCG systems are: reliability, cogeneration, site flexibility, peak power shaving, emergency/back-up power, and short lead times. Some advantages with respect to FC-based DCG applications are: minimal noise/vibration, power quality, high power densities, fuel flexibility, modularity, popularity, and some FC types have a quick response to load variations. Some of the barriers to implementation of DCG systems are: grid interface, ownership, safety, auxiliary energy storage, and possible regulatory barriers. Some disadvantages with respect to FC-Based DCG applications are: technical barriers, high cost (use of platinum, "prototype" manufacturing), sensitivity to fuel impurities, and maintenance. [7] These issues are mostly self-explanatory for those involved with fuel cells. For the novice, the reference by Lariminie or the one by McKinley will provide further insight. The FC-Based DCG system is still in the design stages and therefore makes an ideal system to apply the benefits of the risk engineering process. That is, the risk engineering process can be most effective before the design is finalized.

FUNCTIONS & PROCEDURE

To reiterate, the objective of this research was to utilize risk engineering in order to determine the current FC-Based DCG design parameters and operating conditions that contribute the most to the technological system risk. The first step in organizing the risk engineering process with the design approach is to understand what the goals of risk engineering are. Most experts in all fields of risk engineering will agree upon the following three aims. The general purposes for the risk engineering process are to identify the risks involved in the system, to categorize those risks by consequences and likelihood, and to effect changes, if necessary, thereby reducing the risks below background levels. The focus of this research project will be only on the first two, identifying and categorizing risks, rather than on the final aim, implementing risk reduction for the system design. Applying the design process at this point, the research objective and risk purposes are therefore stated as dual aspects of the following need statement for the CESHR example system:

> There exists a need to identify the risks involved with a fuel cell-based distributed co-generation system using reformed natural gas and to categorize those risks in order to use them as a decision tool for selecting between different design configurations.

The necessary tasks to satisfy the need are: (1) to identify the necessary elements of a risk engineering process, (2) to develop a procedure for reviewing risk, (3) to perform both a risk assessment and a risk analysis on at least one example system configuration to test the procedure, and (4) to make recommendations according to the data generated from the analysis.

The first task, identification of the necessary elements of the risk engineering process, has already been completed with the aforementioned functions of risk engineering. Figure 6 on the following page shows the top-level functions only.

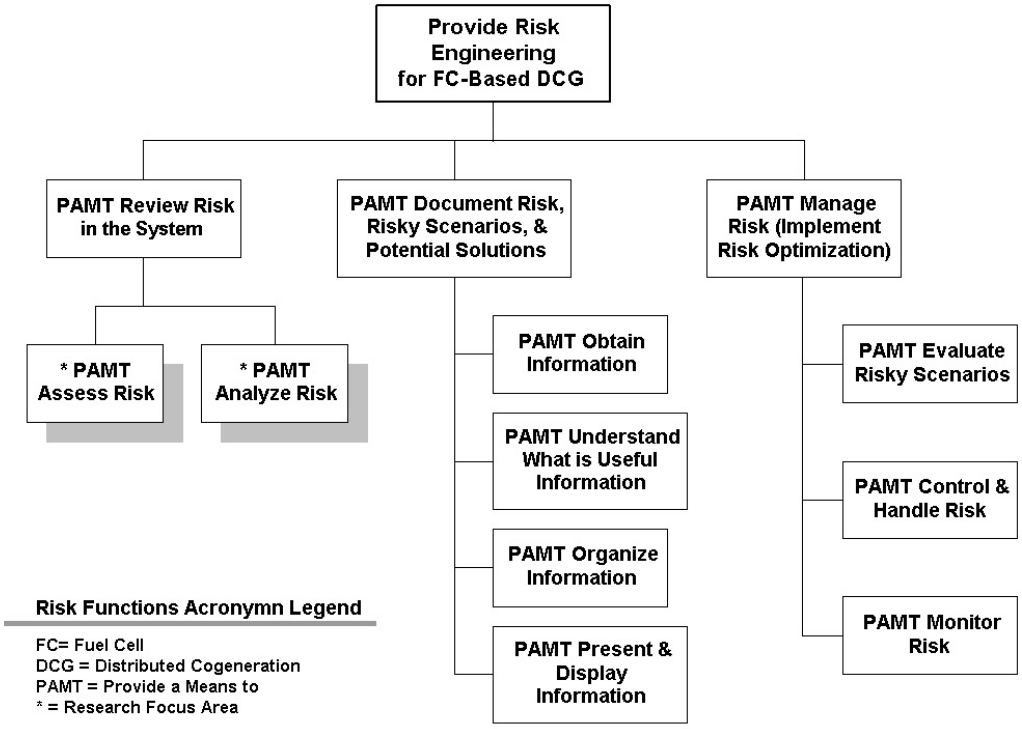

Figure 6: Top-Level Functions of the Risk Engineering Process

While advocating some changes to the process used by the EPA and traditional methodologies, this risk engineering process holds true to the objectives and allows for creativity in finding the problems and solutions in a system. The initial part of the risk engineering process is the risk review, which is the research focus so it will only be briefly discussed here. In any system, the risk review must start by identifying and categorizing risks in order to meet the process objectives. So, the risk review is further broken into assessing risk and analyzing risk as to what needs to be done in order to identify and categorize the risk associated with the alternative system configurations for FC-Based DCG. A literature review of current Department of Energy (DOE) and industry risk practices for fuel cells turned up only a utility function for a solid oxide fuel cell [8], so there are no published precedents for a risk review specific to this system of FC-Based DCG. The next two subsections show the completion of the second and third tasks for the risk assessment and the risk analysis, respectively. Any recommendations generated by the risk review in completion of the fourth task feed directly into the risk management portion of risk engineering.

Risk Review Assessment Procedure & Example Application

The risk engineering procedure for risk assessment, as shown by the functional decomposition in Figure 7 below, centers on the idea that assessment is a qualitative measure of a system's risk. A "top-down" identification and characterization of an example risky scenario was conducted using a literature review of current FC-Based DCG technology system configurations and operational characteristics as well as informal interviews of the CESHR personnel. The function structure below is a dissection of the risk assessment function discussed in Figure 2 as it applies to FC-Based DCG. This function structure illustrates the utility of the top-down design process for risk engineering, in that it allows for a determination of what needs to be considered before deciding how to handle it.

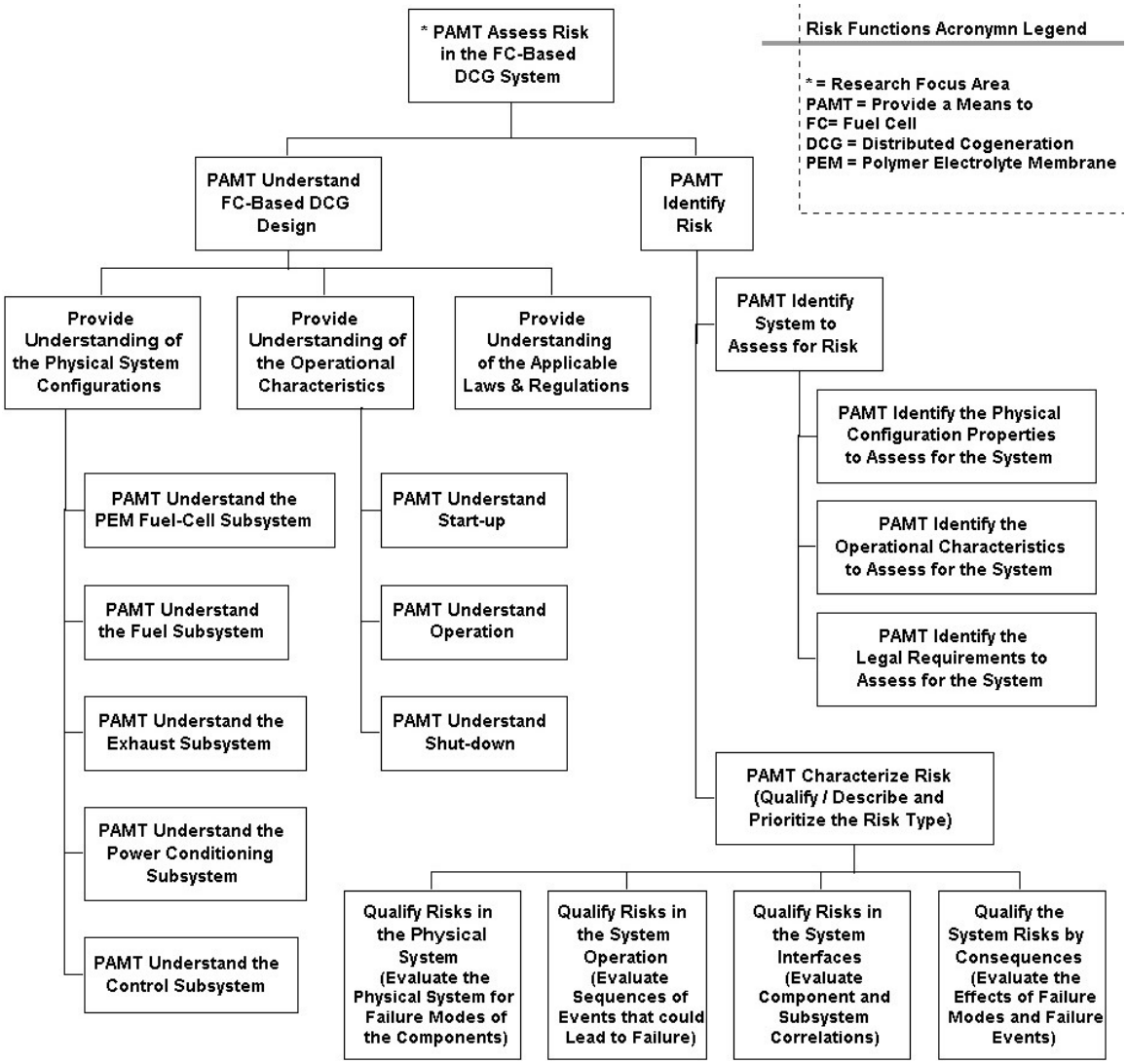

Figure 7: Risk Review Assessment Functions (Research Focus)

Some typical methodologies employed for this stage of a risk review are: fault tree analysis, potential failure modes and effects analysis, expert interviews, risk templates, and lessons learned.

Since there are currently many different ways that could be used to configure and operate the FC-Based DCG, each scenario from the risk assessment should be of the form of a set of specific physical system configurations (PC), operating characteristics (OC), legal requirements (LR), failure modes (FM), failure events (FE), and potential failure consequences (PFC). On way to represent this is using the set in Equation (1) where each capital letter combination is the set of characteristics (or failures) for the specific design for which the risk is to be determined.

$$\{PC, OC, LR, FM, FE, PFC\} \tag{1}$$

So, the physical system configuration set is of the form of Equation (2) for N such parameters needed to define the design that will be analyzed.

$$PC = \{pc_1, pc_2, \ldots, pc_N\} \tag{2}$$

At this point in the design of a risk review process, the identification of the system to be analyzed begins. The function structure shown in Figure 7 provides a logical hierarchy of steps to identify the system risks. Beginning with the system identification, the PCs must be identified from the understanding of the system design for the physical configuration. However, the function structure as shown in Figure 7 is not yet at its lowest level for the design of the subsystems of the FC-Based DCG system. The functions for the understanding of the physical system need to be broken down (decomposed) further to get specific functions that need to be satisfied by the DCG system. This method allows for different components to be used, so the procedure could be applied to systems other than the CESHR example presented here.

Following the procedure outlined by the breakdown in Figure 7 above, the next series of figures will depict the design functions (i.e. what would need to be addressed in the physical system design). From the design, the CESHR system components for each respective subsystem will be identified.

This process brings up an interesting characteristic of function structures in that a single component may fulfill more than one function or multiple components may be needed to

perform one function. Multi-functional components may have a lower reliability than single function ones, as this increases the complexity of the system and introduces more potential failure modes. The first subsystem design to understand is the fuel cell subsystem. This subsystem design is represented by Figure 8 below.

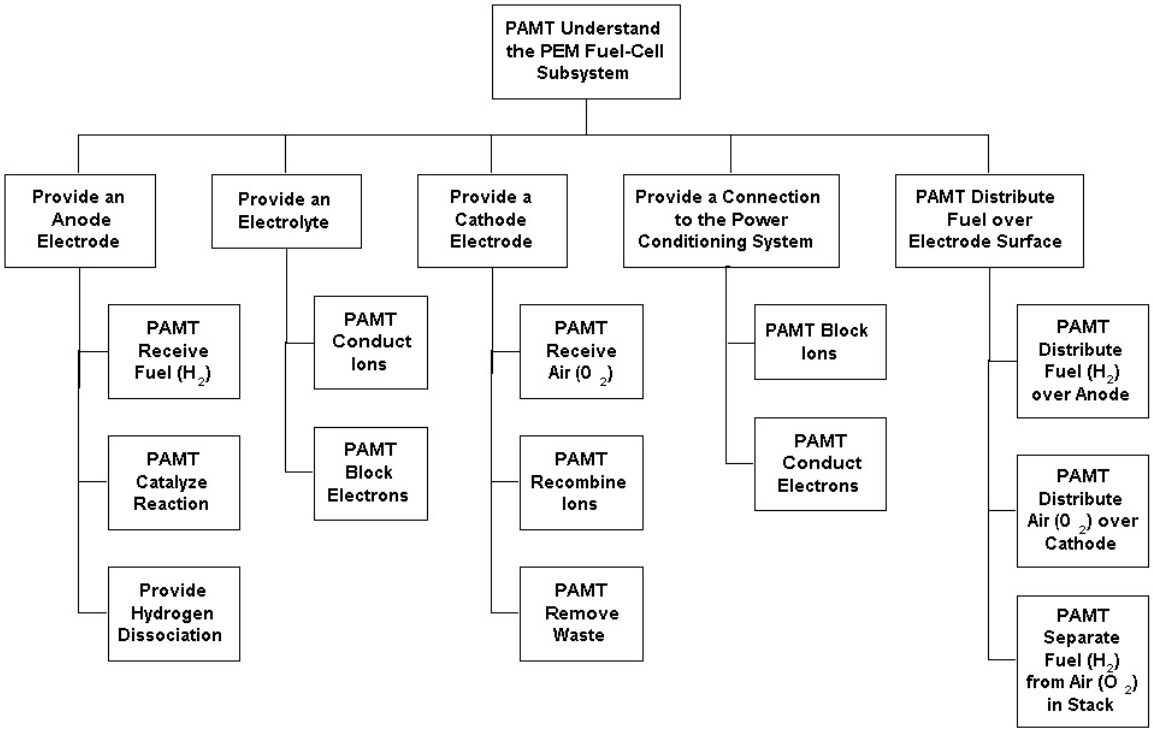

Figure 8: PEM Fuel Cell Stack Subsystem Functions

The second subsystem design to understand is the fuel subsystem. This subsystem design is represented by Figure 9 on the following page.

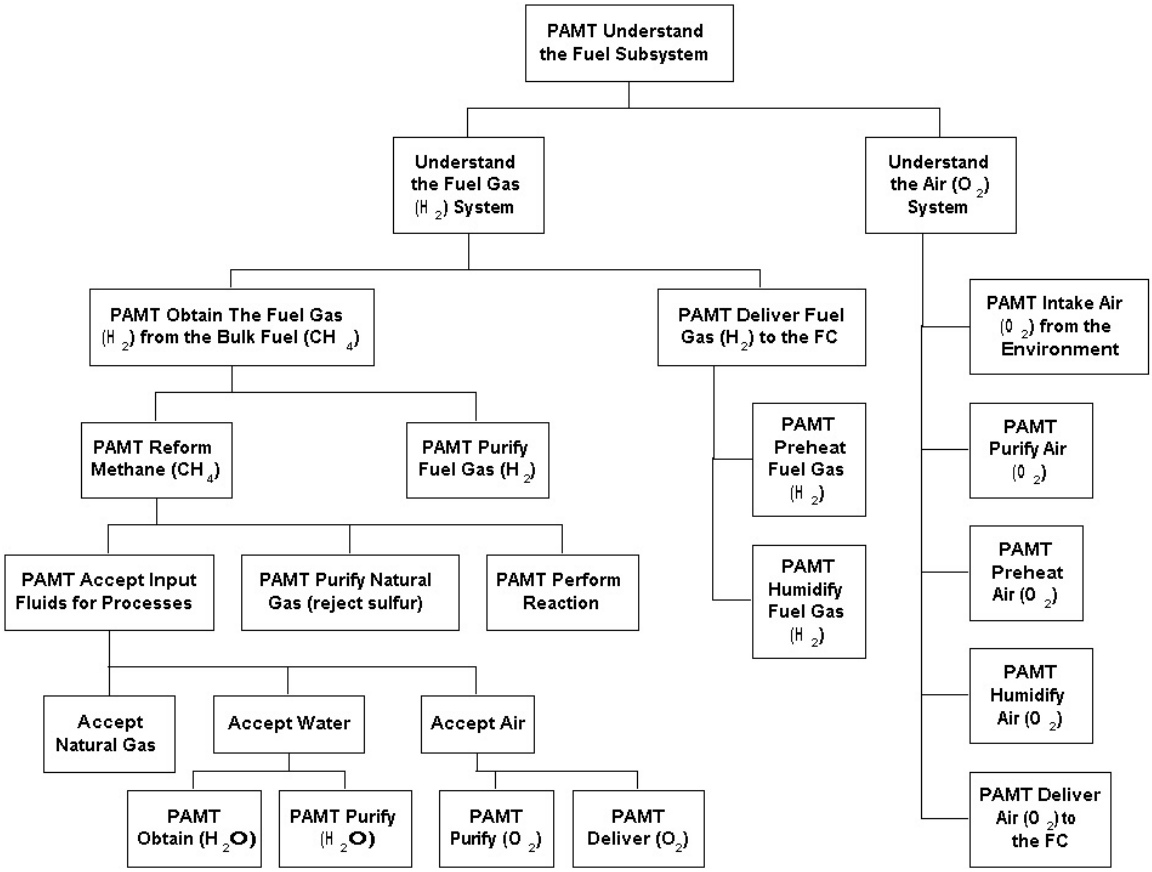

Figure 9: Fuel Subsystem Functions for Fuel Gas & Oxidizer

The third subsystem design to understand is the exhaust subsystem. This subsystem design is represented by Figure 10 on the following page.

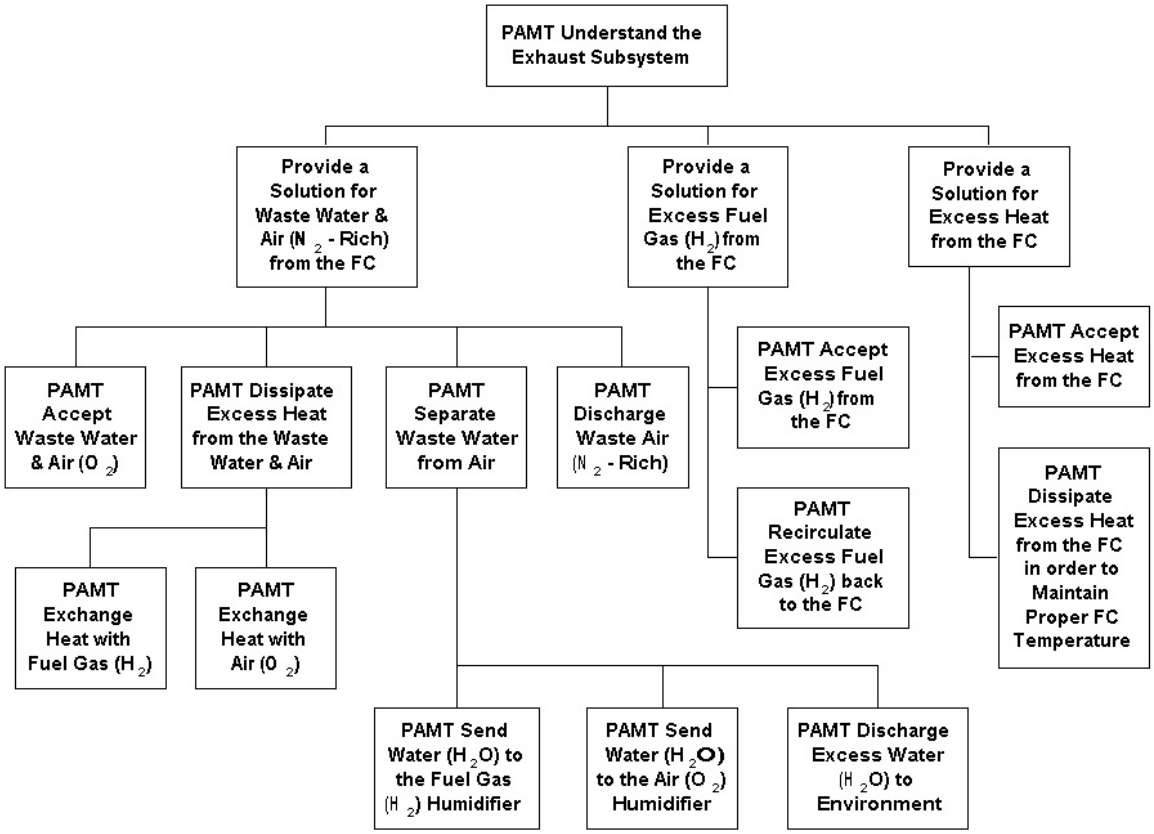

Figure 10: Exhaust Subsystem Functions

The fourth subsystem design to understand is the power conditioning subsystem. This subsystem design is represented by Figure 11 below.

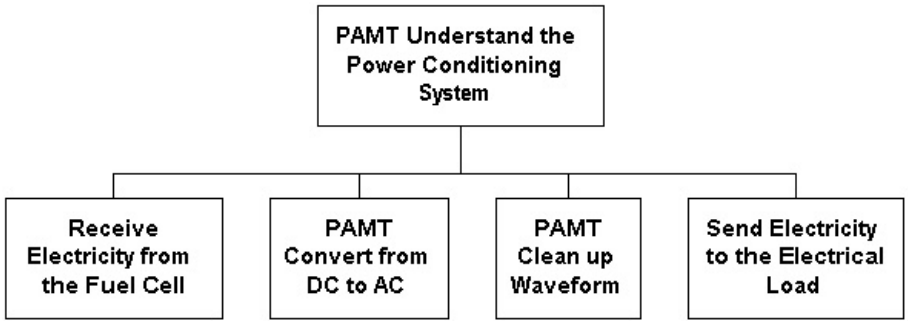

Figure 11: Power Conditioning Functions

The final subsystem design to understand is the control subsystem. This subsystem design is represented by Figure 12 on the following page.

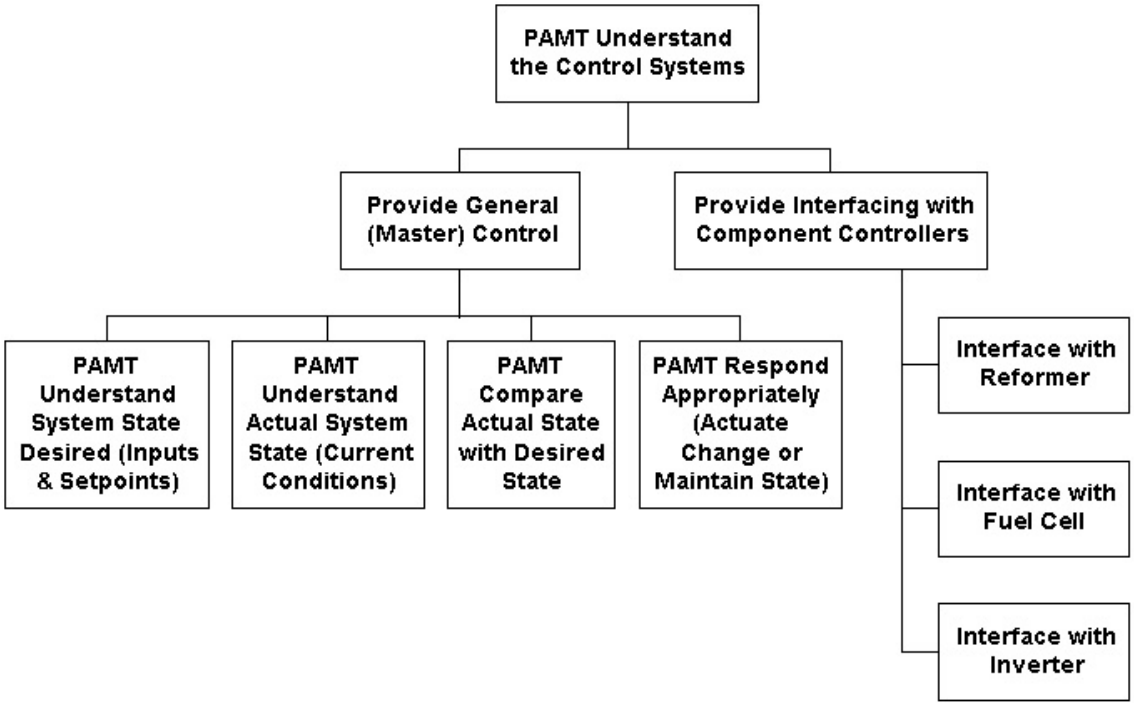

Figure 12: Control Systems Functions

Notice that by defining what each subsystem must do before defining the components of the system to be analyzed, the system design shown by Figures 8 through 12 allows for future parametric analysis where the components can be changed to determine the effect on the system reliability. This demonstrates the utility of the design approach to risk engineering.

The best way to describe all the PCs (physical configurations) of the FC-Based DCG System is to break down the components into their subsystems. The diagram in Figure 13 on the following page shows the same schematic of the DCG System shown in Figure 5, except that the shapes are now pattern-coded to highlight which components belong to what subsystem.

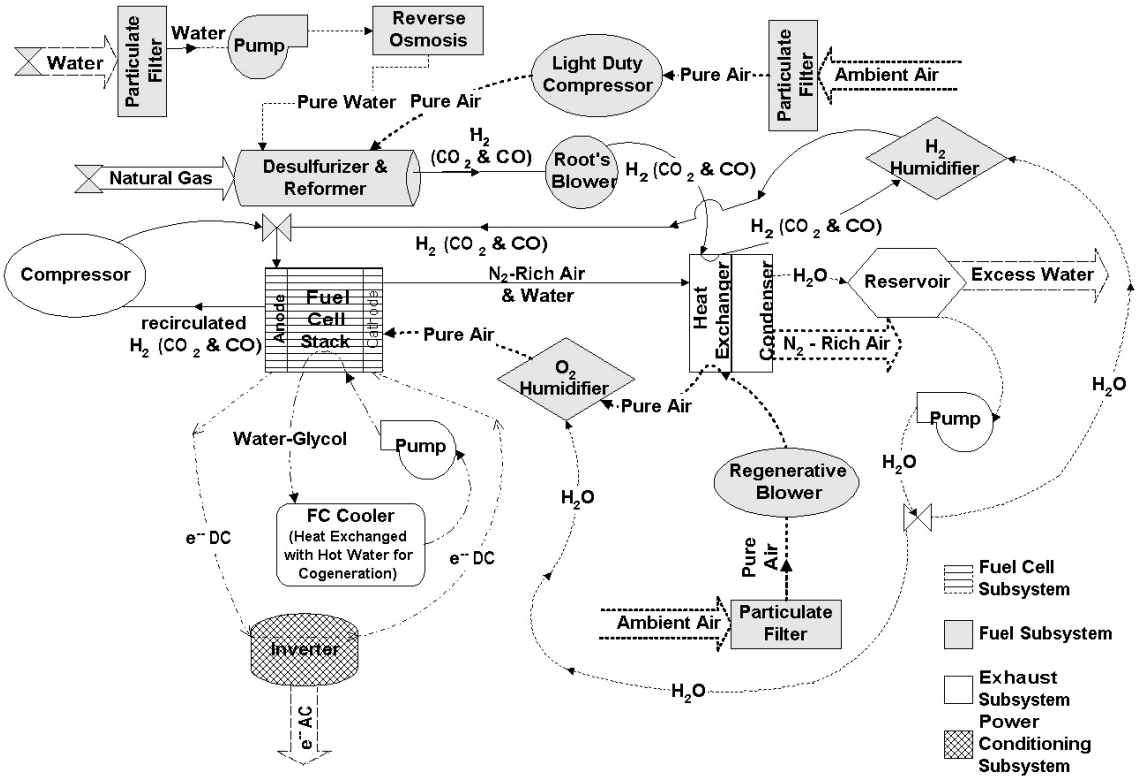

Figure 13: Subsystems of the FC-Based DCG System

The system schematic of Figure 13 is useful, but it is obviously not in the form of a function structure. The components of the FC-Based DCG system grouped by subsystem are shown as part of the risk assessment PC identification function structure in Figure 14 on the following page. The function structure and the components are discussed below.

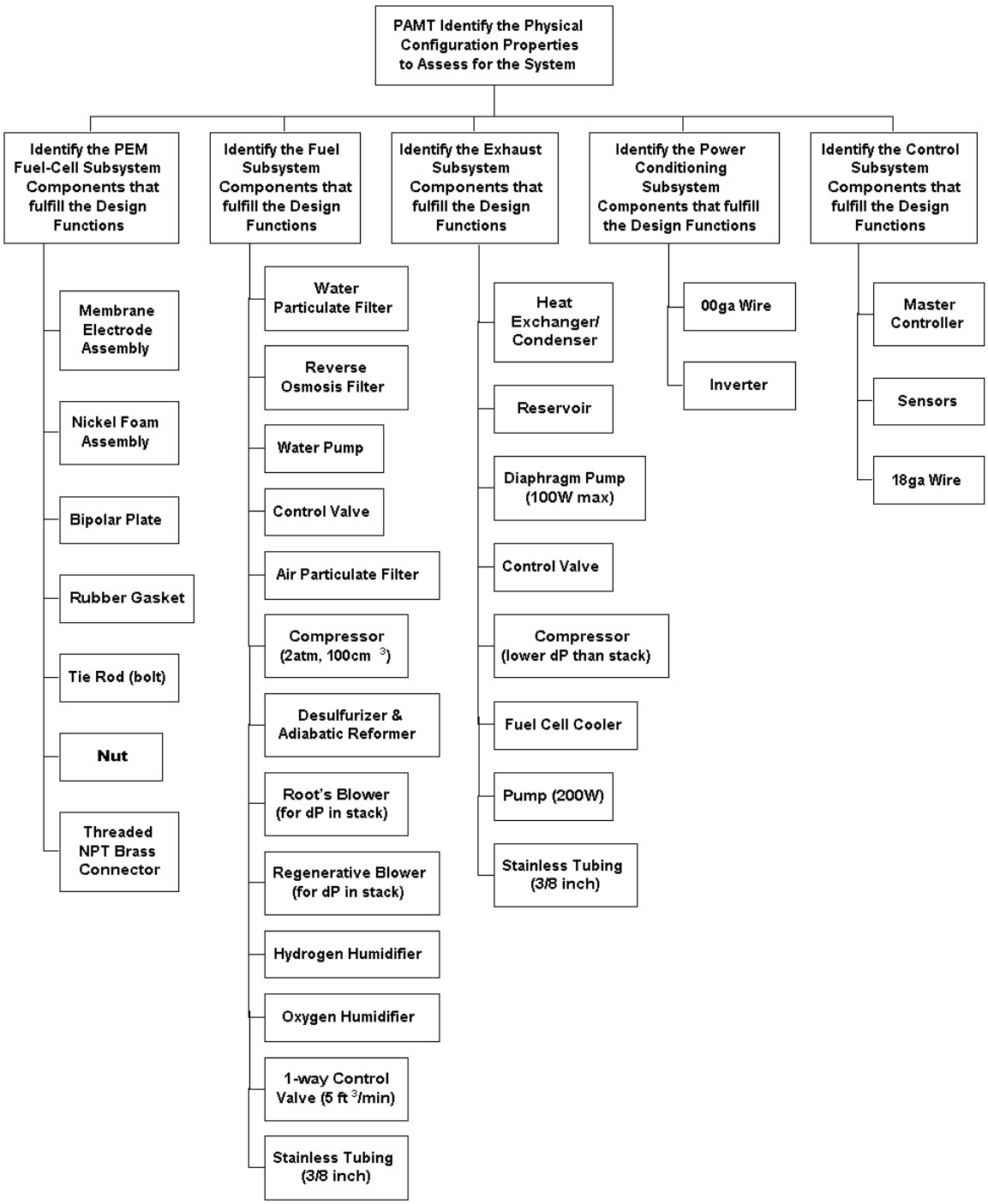

Figure 14: Identifying Physical Configuration of the FC-Based DCG System

For ease of tracking the components, looking to a future analysis of other failure modes and/or operating conditions, each component is given a number (pc_i). To start with the fuel cell subsystem, which are the striped components in Figure 13 and all components shown in

the fuel cell stack schematic of Figure 4, there are seven PCs. In the CESHR system, a Membrane Electrode Assembly (MEA) performs the anode, electrolyte, and cathode functions. Therefore pc_1 is the MEA. A nickel foam flow field assembly performs the functions of distributing the fuel gas and the oxidizer over the surface of the electrodes and of providing the connection to the power conditioning system. Therefore, pc_2 is the Ni-Foam, where there are two for each MEA as shown previously in Figure 4. Bipolar plates perform the functions of distributing the fuel (& air on the other side) and of conducting the electrons as a connection to the power conditioning system. Therefore, pc_3 is a bipolar plate, where there are one more plates than there are MEAs. Gaskets & stack fasteners perform the function of blocking the reactants (i.e. not permitting the gases to leak out of the bipolar plates). Therefore, pc_4 is a rubber gasket, pc_5 is a bolt and pc_6 is a nut. Currently, twelve nuts and bolts hold the CESHR FC stack together, so that will be the amount used in the analysis following. Threaded connections provide the means to receive the fuel gas and air, as well as the removal of waste air-water mixture. Therefore, pc_7 is three threaded connectors.

The PC identification continues with the fuel subsystem, which is represented by all the grey components of Figure 13. There are fourteen PCs depicting the fuel gas and air supply. In the CESHR system, a particulate filter and a reverse osmosis filter perform the functions of purifying the water used in the reforming processes. Therefore pc_8 and pc_9 are a water particulate filter and a reverse osmosis filter, respectively. A pump is needed to input the water to the sulfur-rejection and natural gas (methane) reforming processes and two valves are needed to control the amount of water sent as well as the amount of natural gas sent. Therefore, pc_{10} is a pump and pc_{11} is two control valves. A particulate filter performs the function of purifying the air used in the reforming processes. A second particulate filter is used for the air needed by the fuel cell, but it is the same kind as is used by the reformer. Therefore pc_{12} is two air particulate filters. A light-duty compressor is used to deliver the purified air to the reformer. Therefore pc_{13} is a light-duty compressor. A desulfurizer within the reformer removes the sulfurous acid (H_2SO_3) from the natural gas thereby purifying the fuel gas. In the CESHR system, an adiabatic reformer performs the functions of reforming and purifying the methane (CH_4) into the fuel gas (H_2). Therefore pc_{14} is a desulfurizer & reformer. A Root's Blower is used to deliver the fuel gas to the fuel cell. Therefore pc_{15} is a Root's blower. A regenerative blower performs the function of delivering the air to the fuel

cell. Therefore pc_{16} is a regenerative blower. A humidifier is used to humidify the fuel gas before it is sent to the fuel cell. A second humidifier is used to humidify the air. Therefore pc_{17} and pc_{18} are a hydrogen humidifier and an oxygen humidifier, respectively. A 1-way control valve meters the amount of fuel gas that is delivered to the fuel cell so that the stack runs rich. Therefore pc_{19} is a 1-way control valve. Tubing is the pathway for all the process fluids in the fuel (fuel gas and air) system. Therefore pc_{20} is tubing. A heat exchanger that is part of a condenser takes the heat from the cathode waste stream and uses it to separately preheat the fuel gas and the air. This component is a part of the exhaust system components and demonstrates how a single component can interface with the various parts of the function structure.

For the components of the exhaust subsystem, which are white in Figure 13, there are eight PCs. In the CESHR system, a heat exchanger/condenser takes the excess heat from the waste water & air and uses it to separately preheat the intake air & fuel gas as it condenses out the water from the waste stream. This water is then available to perform the function of humidifying the warmed air and fuel gas. Therefore pc_{21} is a heat exchanger/condenser. In the CESHR system, a reservoir performs the function of ensuring the amount of water needed by the humidifiers is collected and the excess is discharged to the environment. Therefore pc_{22} is a reservoir. A pump performs the function of sending water to the humidifiers and a control valve ensures the correct amount is sent. Therefore pc_{23} is a pump and pc_{24} is a control valve. A compressor takes the excess fuel gas and feeds it back to the fuel cell through the 1-way control valve. Therefore pc_{25} is a compressor. In the CESHR system, a fuel cell cooler performs the function of accepting and removing FC heat using a pump to circulate a water-glycol mixture as the working fluid. This is the component that allows for cogeneration to occur by exchanging the excess heat from the FC with water for the end user to create hot water. Therefore pc_{26} is a fuel cell cooler and pc_{27} is a pump. Tubing is the pathway for all the process fluids in the exhaust system. Therefore pc_{28} is tubing.

In the power conditioning subsystem, which is represented by the hatched components in Figure 13, there are two PCs. In the CESHR system, electrical wire and soldered connections perform the functions of receiving the electricity from the fuel cell at the bipolar plates and sending the electricity to the electrical load. Therefore pc_{29} is wire. In the

CESHR system, an inverter performs the functions of converting direct current to alternating current and cleaning any noise from the waveform. Therefore pc_{30} is an inverter.

Considering the control subsystem components, which are not in the schematic in Figure 13, there are three PCs. A master controller performs the functions of general control and interfacing with the component controllers. The reformer subsystem, the fuel cell subsystem, and the inverter subsystem all are manufactured with their own controllers so the master controller would be in charge of sensing the positions of the various control valves and flow rates of the various pumps and blowers in order to ensure that all subsystems are interacting appropriately for the desired operating condition. Therefore pc_{31} is a master controller and pc_{32} is the various sensors. The actuators (control valves, compressors and pumps) have already been identified within their respective subsystems. In the CESHR system, electrical wire and soldered connections perform the functions of interfacing (i.e. sending and receiving the electrical signals) the controllers to the components. Therefore pc_{33} is wire.

Now, to explain a few notes on the procedure that was just used. In the example system, pc_1 through pc_7 refer to the type of fuel cell used, which was a Polymer Exchange Membrane in this case, but it could have been any of the other types, such as Solid Oxide. This process also works for different components within the PEM type fuel cell; instead of a nickel foam flow field assembly, a graphite plate could have been used. Similarly, pc_8 through pc_{20} refer to the type of fuel gas system, which was reformate in this case, but it could have been pure hydrogen.

Continuing with the identification of the system to be analyzed, the conditions in which the system is operating must be identified. There are several operating conditions (variable OC) in which the FC-Based DCG system could be evaluated for the risk assessment. There is the operating condition of startup, or the initial run, which is of interest because the system or its components can have "infant mortality" due to such causes as manufacturing defects. The next operating condition is that of constant running, where excess electricity is fed back to the grid or to a battery bank for peak shaving. This is the OC of choice for the example FC-Based DCG system. Another operating condition is that of intermittent running; where the DCG system acts like an air conditioner which cycles on when needed and off when the demand has been met. The final operating condition that could be

consider is shut down, or decommissioning. Several systems require a very specific set of shut-off procedures when they will not be used again, and this may be the case with the DCG system. The following Figure 15 shows all the OCs for the FC-Based DCG system, where the research focus of continuous operation is shadowed and the operational sequence for that function is further decomposed.

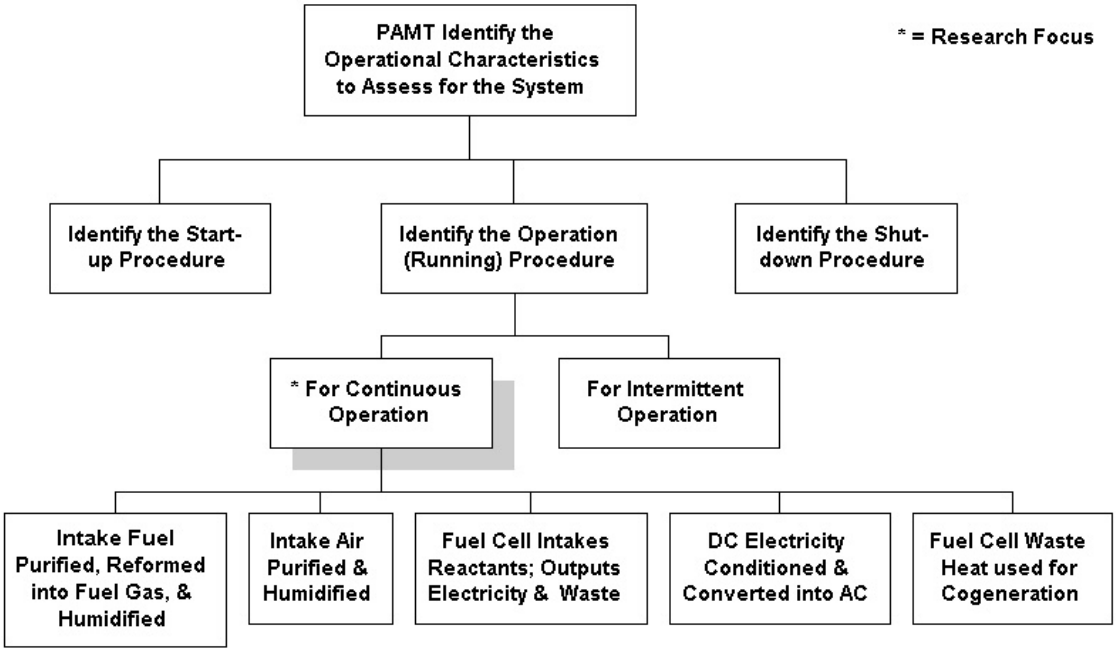

Figure 15: Identifying Operating Characteristics & Research Focus

The next attribute to identify in the system for the risk assessment are the legal requirements (variable LR), which are primarily a programmatic risk dealing with whether or not the system is in compliance with all applicable laws and regulations. For this research, the current CESHR configuration is assumed to be in compliance with all governing laws and regulations. If the laws were to change, then the PCs or the OCs would change to meet the new demands, and a new risk review would need to be performed on the new configuration.

Following the hierarchy of steps to identify the system risks, as shown in Figure 6, several parts must be completed in order to characterize the system risk. Failure modes of the components, sequences of events that could lead to failure, component and subsystem

correlations, and the effects of the failure modes and failure events; all must be identified for the operating conditions of the system. An obvious failure mode for the components identified in the system is wearing out, and another one is simply not working. For this research, the focus for all components is FM = not working (no functionality of the part). Using a handbook of failure rates will let this qualitative failure mode easily translate into a quantitative one for the next section, risk analysis. The following function structure in Figure 16 would serve to help identify many more failure modes for each component in future analyses.

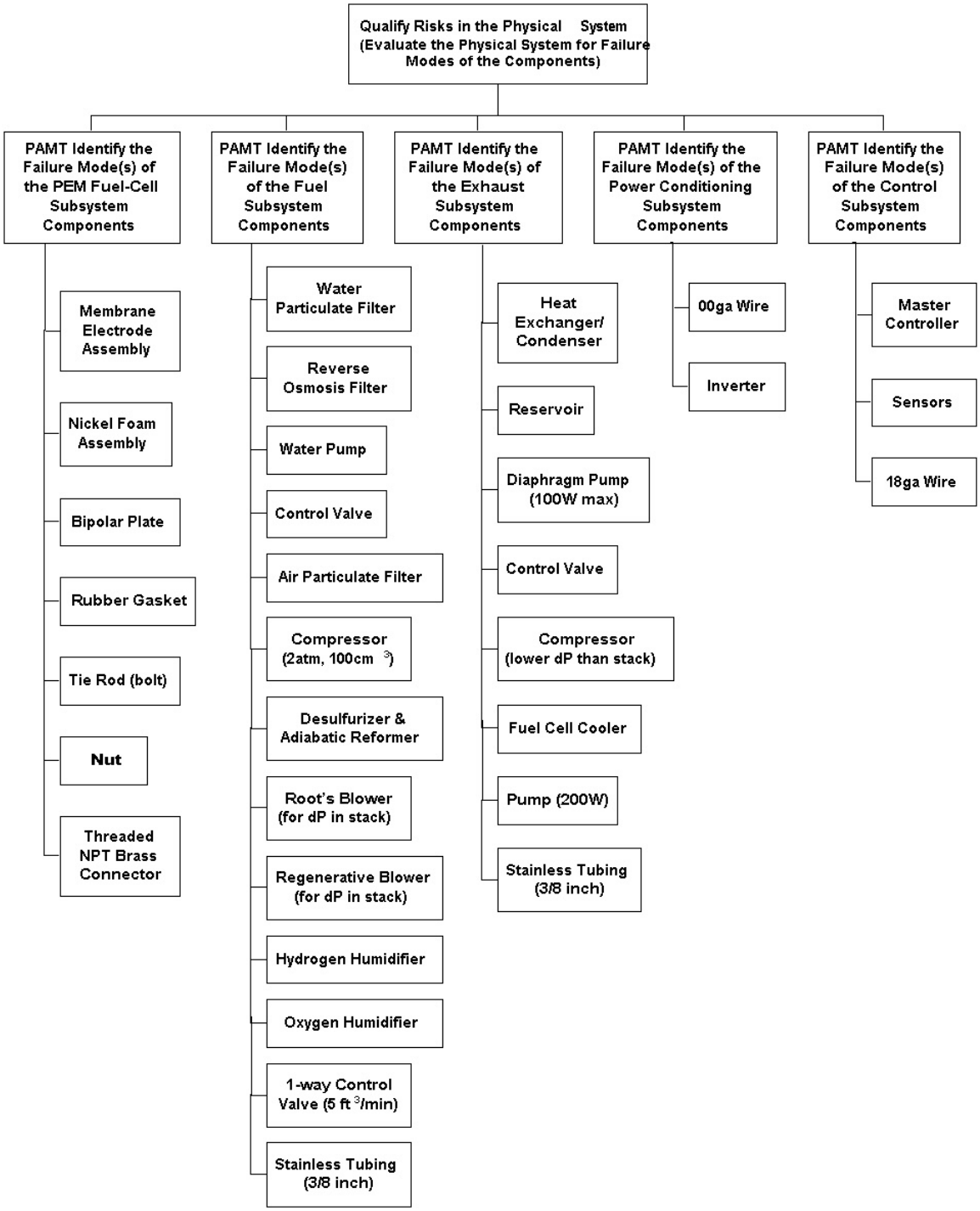

Figure 16: Identifying Component Failure Modes

The components may be salvageable with this FM of ceasing to operate as intended or the components may need to be replaced as with other FMs. The FMs identified as part of the

procedure represented by Figure 16 should guide the risk engineer towards potential consequences of the failure modes (which is a subsequent step to define the PFCs for FMs).

For the chosen OC, continuous operation, there is a timeline of events that must occur for successful operation of the DCG system. Originally, an event tree was to be constructed, but due to the FC-Based DCG system having no redundancy or parallel reliabilities and the focus on an FM of simply ceasing to operate (rather than other kinds of failure with myriad consequences), the operation sequence was sufficient. Essentially, this means that all individual component failures would lead to total system failure. The risk information gathered from the subsequent risk analysis will therefore be a "worst-case" scenario that will be useful in determining where CESHR should focus future research to bring the FC-Based DCG system to market. The following Figure 17 should be more useful for organizing the event trees (or other risk methodologies) for other FC-Based DCG systems with redundancy.

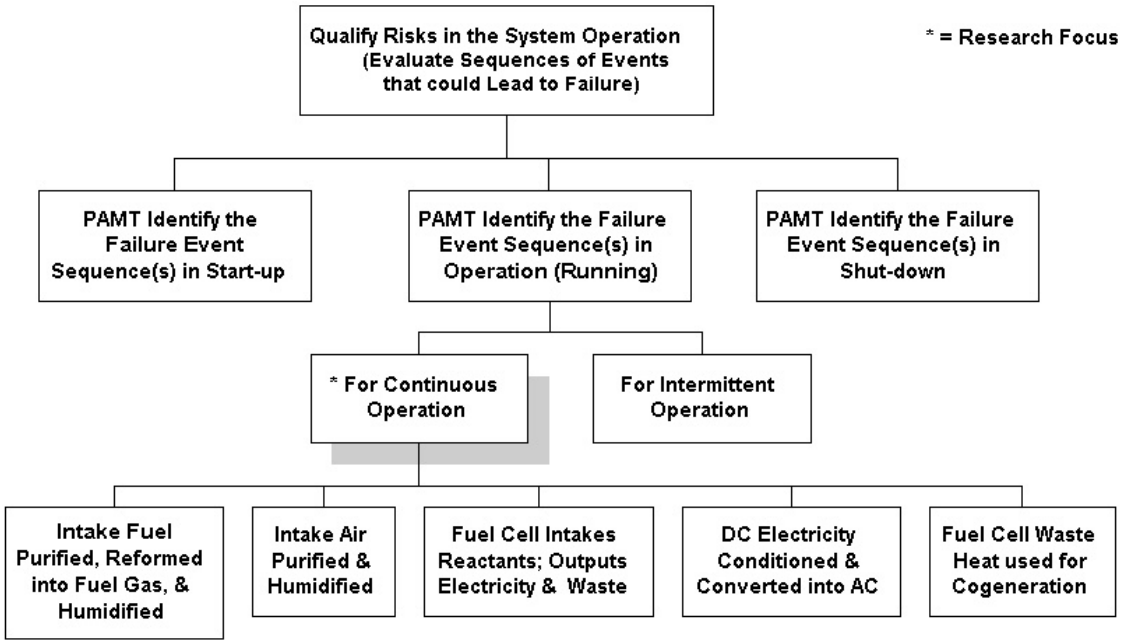

Figure 17: Identifying Failure Events

The components acting in this operation sequence are depicted on the following page in Figure 18, where the "and" gates show that although some of the components act in parallel, all branches are necessary to the operation of the next component in the operational flow.

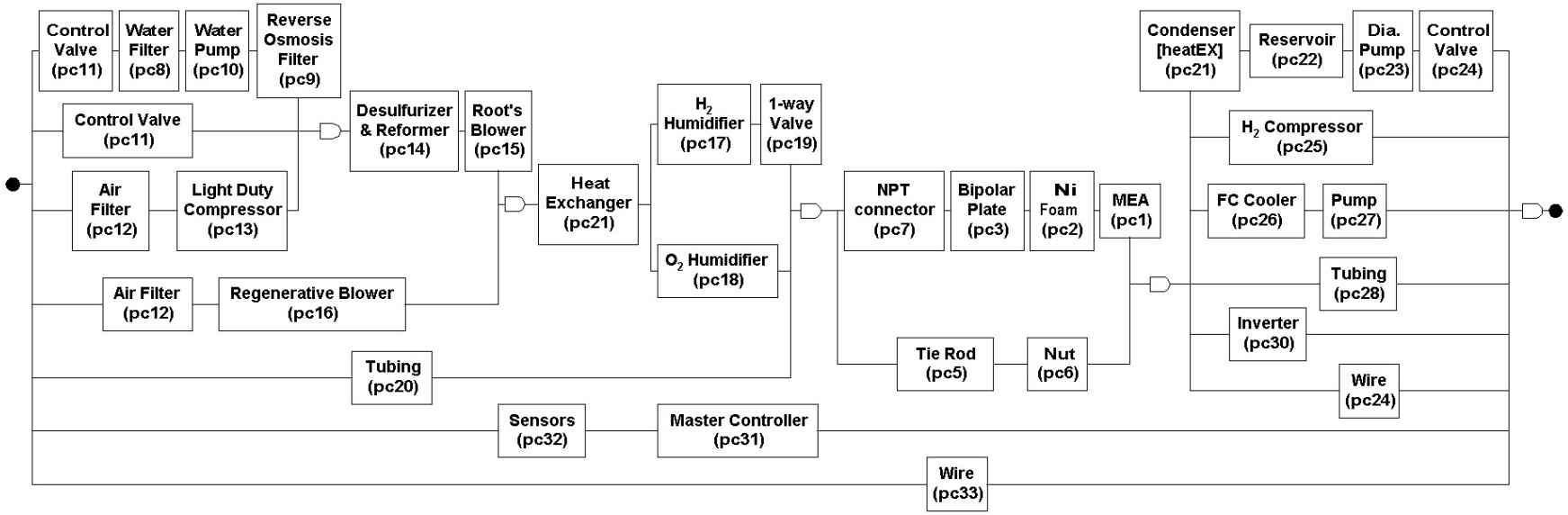

Figure 18: FC-Based DCG Operation Sequence for Normal, Continuous Operation

Following the last two steps from the risk assessment function structure depicted previously in Figure 7, the system interfaces and the system risk consequences must be qualified. Due to the simplifying assumptions previously discussed, interfaces are dealt with internal to the system. As mentioned before, there is not much redundancy in the chosen FC-based DCG system; the consequences of the individual components not working are usually total system failure (PFC = system shutdown). Even though there can be more than one failure consequence for a failure mode, other consequences will not be considered here. The results of the risk assessment portion are discussed in the next section following the discussion of the risk analysis procedure as applied to FC-Based DCG.

Risk Review Analysis Procedure & Example Application

The risk engineering procedure for analysis, as shown by the functional decomposition in Figure 19 on the following page, centers on the idea that analysis is a quantitative measure of a system's risk. This gives the risk reviewer an idea of what needs to be addressed in order to perform the risk analysis for the completion of the second task. A "bottom-up" rating for each scenario previously identified by the assessment will be conducted at this point using standard risk industry practices. Here the magnitude of the consequences is combined with the event likelihood to give a metric for each scenario, which can then be combined to a total system metric. Some typical methodologies employed for this portion of the risk review are: event trees, failure rates, probabilistic risk analysis, scheduling network analysis, Monte Carlo simulations, reliability ranges for each component, Ishikawa "fishbone" diagrams, hazard analysis, and trade-off studies. The function structure below is a decomposition of the risk analysis function discussed in Figure 2 as it applies to FC-Based DCG. Like the assessment function previously discussed, it also illustrates the utility of the top-down design process for risk engineering by allowing for a determination of what should be considered before deciding how to analyze it. The dashed analysis functions shown on the diagram in Figure 19 on the following page are performed repetitively for each component & operation found in the previous assessment.

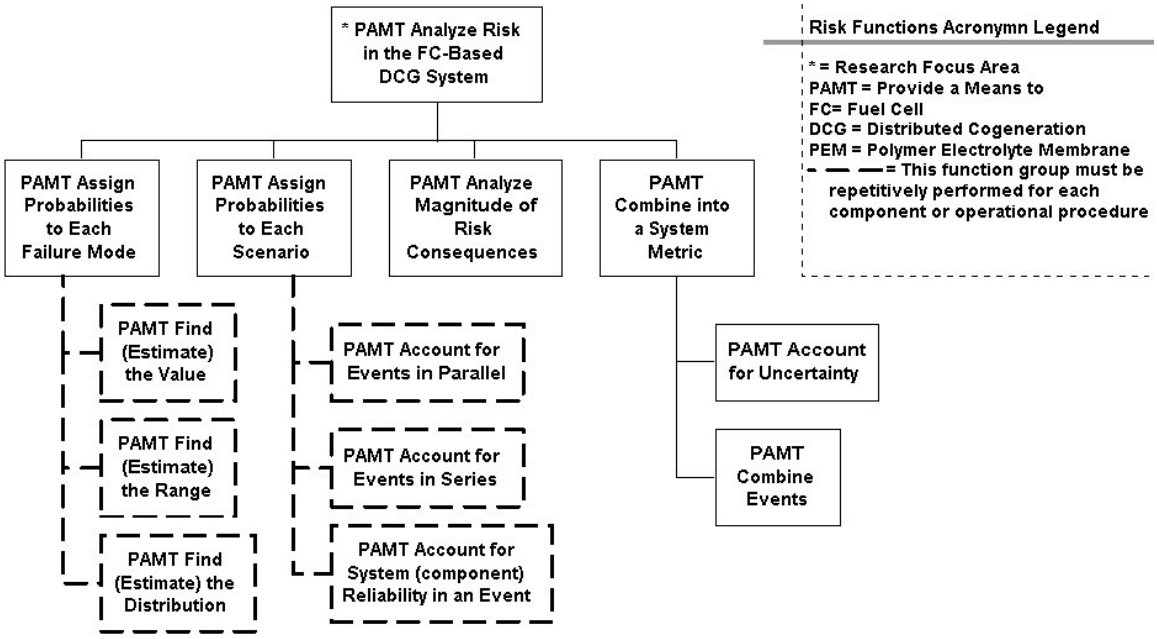

Figure 19: Risk Review Analysis Functions (Research Focus)

Before discussing the assignment of probabilities to the failure modes and then to the failure events, the last two functions from Figure 19 will be discussed. First, the magnitude of the risk consequences are all that no electricity will be delivered to the end user and no heat will be exchanged with the site water. This gives the "worst-case" scenario for the operational sequence. There can be more than one magnitude of failure for a potential failure consequence. Second, the combination into a system metric will be done with standard reliability equations while a Monte Carlo simulation will account for uncertainty. A Monte Carlo simulation runs several "what-if" scenarios by iterating the system variables (in this case, failure data) through a range of values according to a specified distribution. The random generation of these bounded data will change the output of interest (in this case, system reliability). [1] By simulating the model over 1,000 times a statistical feel for the likelihood of the outcome is developed.

The calculations following in Equations (3) through (5) demonstrate some of the probability principles that were useful in finding an overall value of risk for the system. As all products degrade over time (t), the probabilities are shown as functions of time. First, the sum of the probability of failure ($P_f(t)$) & of success ($P_s(t)$) will always be unity.

$$P_f(t) + P_s(t) = 1 \tag{3}$$

Second, as most component data will be of the form of the mean time between failure (MTBF) of tested parts or in the form of failure per million hours (fpmh), some way to convert this into a probability is needed. This allows for a Monte Carlo simulation to then turn component failure data into a reliability (R) or a probability of the success for the system by randomly choosing the fpmh from a specified range and distribution for each uncertain value and then tracking the effect of these variations on the system reliability. The generally accepted equation to convert from fpmh or MTBF to a probability of success is as follows:

$$R = P_{success} = e^{-\frac{t^* fpmh}{10^6}} \quad where \quad fpmh = \frac{10^6}{MTBF} \tag{4}$$

Last, many systems today are very complex, creating rather complex event structures leading to failures. If the sub-events are independent, i.e. no common causes, a means to account for the complexity of these sub-events is to multiply each sub-event probability. Alternately, if all sub-events have the same probability, raise the success probability for a single event to a power equal to the number of sub-events (N). This development may also be applied to the total probability from a number (n) of the same components in a system of several (N) different types of components.

$$P_{complex}(t) = \prod_{i=1}^{N} P_s(t)_i \quad \text{or} \quad P_{complex}(t) = [P_s(t)]^N \tag{5}$$

$$P_{components}(t) = \prod_{i=1}^{N} \left([P_s(t)]^n \right)_i$$

Figure 20 on the following page shows the first repetitive subgroup from Figure 19 applied to the FM for each PC previously identified by the risk assessment. Since there was only one FM of not working, finding the value of the probability of failure for the standard components is relatively easy as there exists many sources of failure data. On the other hand, the failure data for the new components will have to be estimated from experience. One could perform experiments to obtain the failure data of new components, however that is outside of the scope of this research. Estimates are widely used and accepted as standard engineering practice.

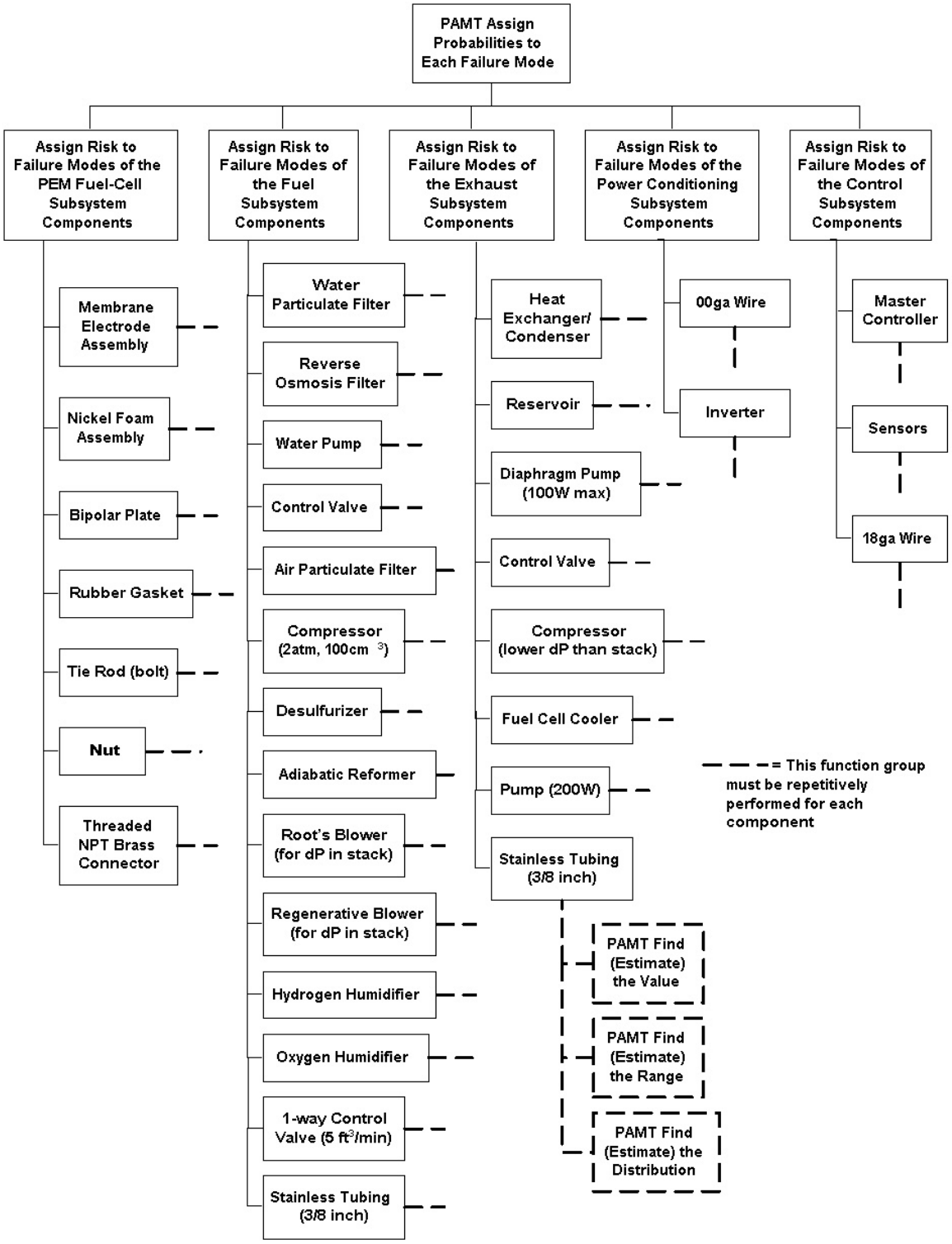

Figure 20: Analysis of Component Failure Modes

At this point in the risk engineering process the failure data, which is when the component would not work as intended, for the individual components was gathered. Most component

data for the BOP and some parts of the fuel cell stack were obtained as failures per million hours (fpmh) from the Nonelectronic Parts Reliability Data Handbook and are repeated here with the significant figures shown in the handbook in the unshaded cells. [9] However, since this handbook did not cover the reliability of the MEA, Ni-Foam, bipolar plates, and the reformer, these components were estimated from laboratory experience of the MTBF in the shaded cells. Table 2 gives the failure values found for normal operation.

Table 2: FC-Based DCG Component Failure Data for Normal Components

Variable	Component Name	Subsystem	# of Comp.	Median fpmh
pc1	membrane electrode assembly	Fuel Cell	80	200
pc2	nickel foam	Fuel Cell	160	100
pc3	bipolar plate	Fuel Cell	81	0.1
pc4	rubber gasket	Fuel Cell	160	0.0597
pc5	tie rod (bolt)	Fuel Cell	12	2.7835
pc6	nut	Fuel Cell	12	0.5744
pc7	threaded NPT brass connector	Fuel Cell	3	5.9243
pc8	water particulate filter	Fuel	1	17.4825
pc9	reverse osmosis filter	Fuel	1	49.519
pc10	water pump	Fuel	1	342.377
pc11	control valve	Fuel	2	107.346
pc12	air particulate filter	Fuel	2	51.2821
pc13	light-duty compressor (2atm, 100cu.cm)	Fuel	1	193.7094
pc14	desulfurizer (CH4 & N2) & reformer (adiabatic)	Fuel	1	20
pc15	Root's blower (size for dP in stack)	Fuel	1	3.3029
pc16	regenerative blower (just for dP)	Fuel	1	3.3029
pc17	hydrogen humidifier	Fuel	1	33.435
pc18	oxygen humidifier	Fuel	1	33.435
pc19	1-way control valve (5 cu.ft./min)	Fuel	1	107.346
pc20	(90 ft) stainless (or Cu) 3/8 inch tubing	Fuel	1	2.047
pc21	heat exchanger/condenser	Exhaust	1	9.9894
pc22	reservoir	Exhaust	1	3.37
pc23	diaphragm pump (100W max)	Exhaust	1	342.377
pc24	control valve	Exhaust	1	107.346
pc25	compressor (lower dP than pc16)	Exhaust	1	16.0894
pc26	fuel cell cooler	Exhaust	1	9.9894
pc27	pump (200W)	Exhaust	1	342.377
pc28	(11 ft) stainless3/8 inch tubing	Exhaust	1	2.047
pc29	(2 ft) 00 wire	Pwr Cond	1	0.1877
pc30	inverter	Pwr Cond	1	5.0851
pc31	master controller	Control	1	0.0486
pc32	sensors	Control	50	3.6125
pc33	(50 ft) 18 wire	Control	1	0.2203

Obtained from NPRD-95

Calculated from MTBF estimate

To turn these failure data from Table 2 into reliabilities, Equation (4) presented above was used to calculate the most likely reliability for each PC. For analysis of the system, a triangular distribution was assumed for each component with a ± 50% range of failure values. Other distributions could have been chosen, such as the Weibull distribution, the uniform distribution, or the Gaussian (normal) distribution. The following Figure 21 depicts the most likely value, the range and the distribution for pc_1 as used in the subsequent analysis. The risk analysis distribution and values (range and most likely) for the other PCs are included in Appendix A.

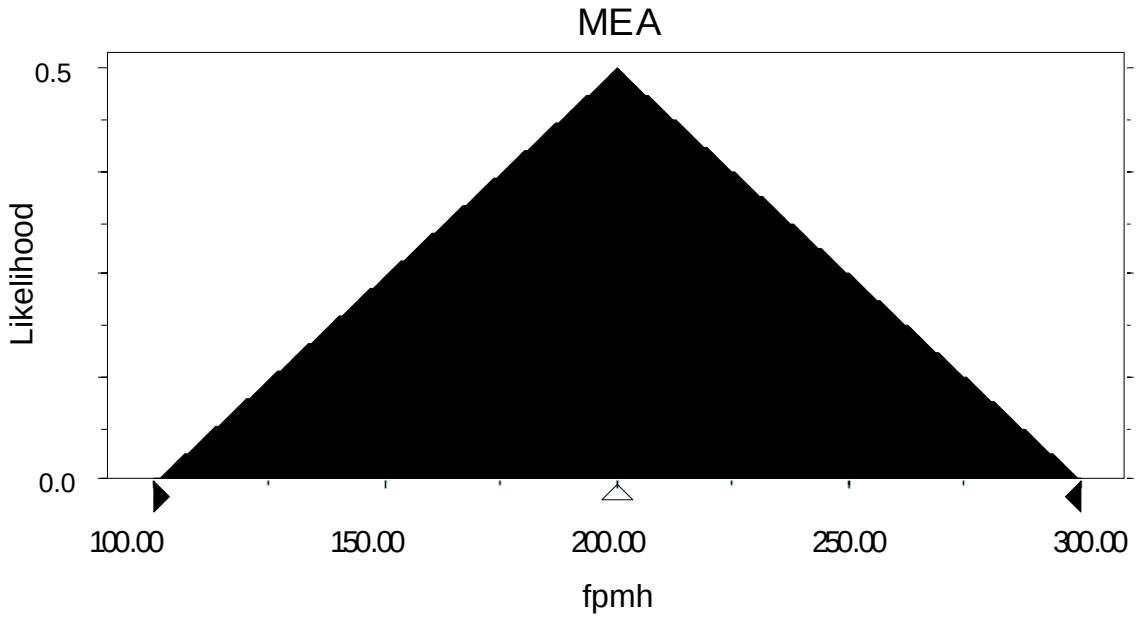

Figure 21: Risk Analysis Values & Probability Distribution for pc_1

Figure 22 on the following page shows the second repetitive subgroup of the risk analysis function structure from Figure 19 applied to the FEs previously identified from the risk assessment.

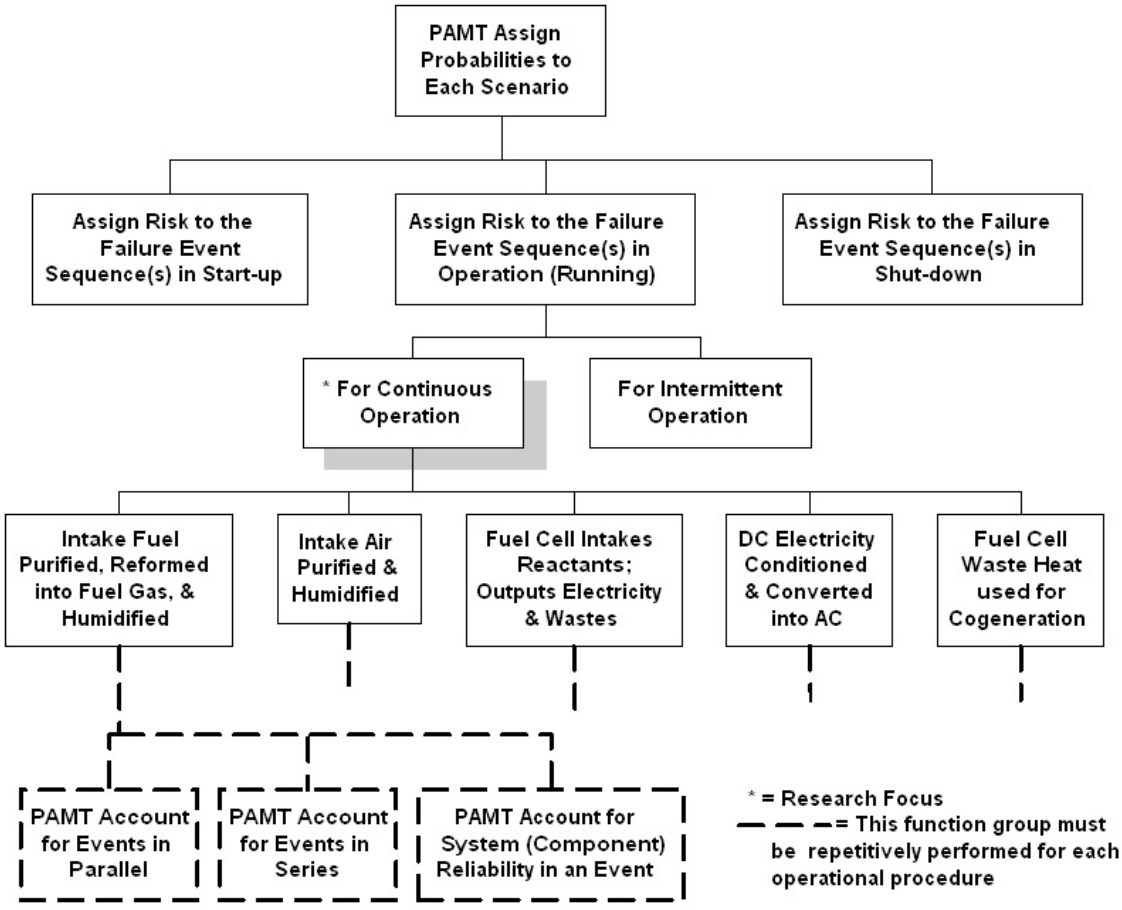

Figure 22: Analysis of Operational Failure Events

Care must be taken in combining individual component reliabilities into system reliabilities because the combination changes depending on if the components are in series, in parallel, or are redundant components. For independent components in general, the reliabilities for components in series are multiplicative, the reliabilities for components in parallel are inversely additive, and the reliabilities for redundant components in parallel additive are added with the multiplied reliability subtracted. A standby redundant system, where the operation switches from the failed component to start operating a new component, uses a Poisson process and is not applicable to the current research. [10] This is illustrated with the following three Equations (6) through (8).

$$R_{series} = \prod_{i=1}^{n} R_i \quad \text{for n reliabilities in series} \tag{6}$$

$$R_{parallel} = \left(\sum_{i=1}^{n} \frac{1}{R_i} \right)^{-1} \quad \text{for n reliabilities in parallel} \tag{7}$$

$R_{redundant} = R_1 + R_2 - R_1 * R_2$ for two continuously redundant reliabilities in parallel (8)

For example, take the following four components, A, B, C, and D. Components B and C are redundant for each other, and this combination is in series with both components A and D. This is illustrated graphically in Figure 23 below.

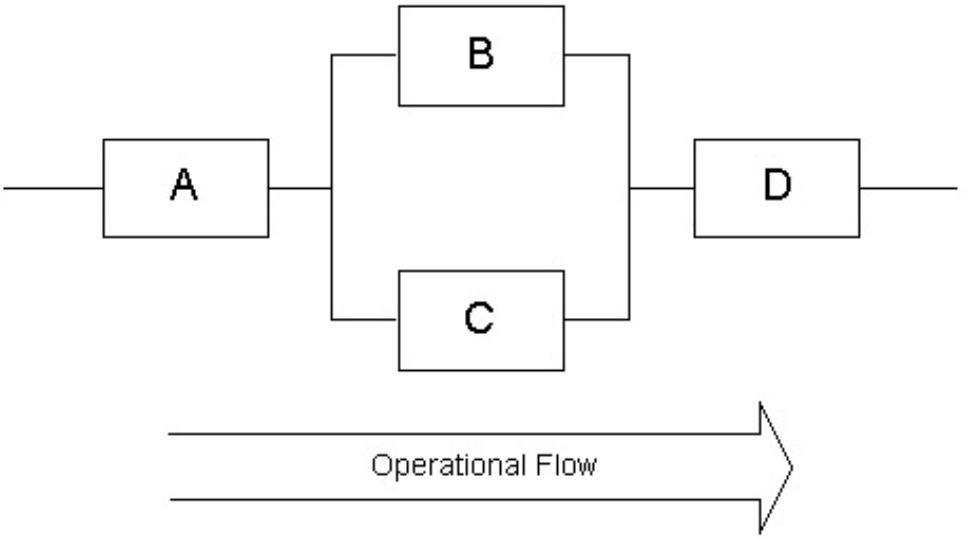

Figure 23: Reliability Example

Applying Equations (6) and (8), the total reliability for this simple system is $R_{system} = (R_A)(R_B + R_C - R_B R_C)(R_D)$. However, if B and C had been reliabilities in parallel with each other, Equation (7) would have been used in place of Equation (8). Thus, the total reliability for the system would have been $R_{system} = (R_A)\left(\frac{1}{R_B} + \frac{1}{R_C}\right)^{-1}(R_D)$. [10]

In the case of the FC-Based DCG, no redundancy and no parallel reliabilities exist for the original, non-risk controlled case. Therefore, the total system reliability is calculated by applying the principle discussed above for Equation (6) and for Equation (5). This results in the following Equation (9) where N = 33 PCs in this case and n is the number of component i in the system design.

$$R_{sys} = \prod_{i=1}^{N}\left[\left(R_{pc_i}\right)^n\right] \quad (9)$$

The times chosen for evaluation were t = 1 hour, 5 hours, 10 hours, 50 hours, 100 hours and 500 hours of continuous operation. The approach used for finding the deterministic risk of the system was simply to apply the series reliability equation to the "most likely" median values of the transformed failure data for the components at each desired evaluation time. However, this deterministic reliability is not able to give a likelihood of the system actually having that value. At most it would give a bound on the system limits by plotting the low and high reliability combinations as a measure of the uncertainty band.

The approach for finding the probabilistic risk of the system was to use the Crystal Ball (CB) software from Decisioneering in Excel to perform 5,000 Monte Carlo trials for each evaluation time. The range (high and low reliability values) and distribution were defined for each of the failure rates for the components (pc_1 through pc_{33}), and the total system reliability for each time evaluated was set as a "forecast value". This meant that whenever the CB package randomly chose the values for each component, the resulting effect on the total system reliability was recorded. [1] This allowed for a probability of the reliability of the system (or the probability of system success) at each evaluation time. The following Figure 24 shows the reliability recorded at the second evaluated time (t = 5 hours) by CB where the predicted reliability of the system is 84% with the possibility of a reliability value ranging from 79% to 89%. The standard deviation of the system reliability at this evaluated time is 0.02.

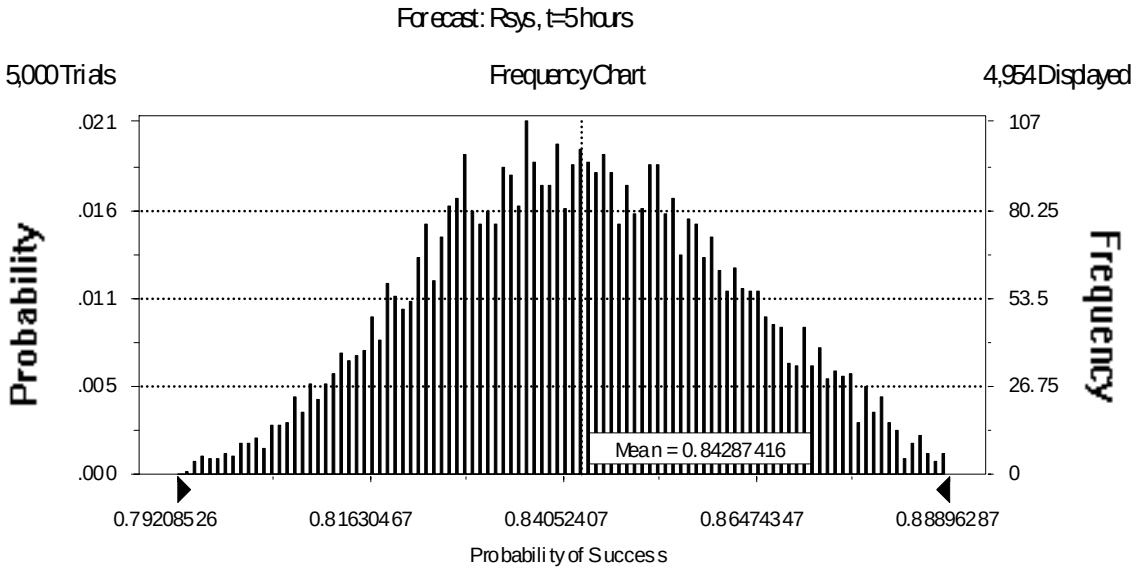

Figure 24: Distribution of Reliability for t = 5 hours

All other forecast values have similar graphs and data statistics (standard deviation, range) presented in a report generated by CB. The Excel spreadsheet setup and the CB report are included in Appendix A. The analysis in the appendix includes the deterministic evaluation of the system reliability mentioned previously. Figure 25 below depicts the reliability of the current configuration of the FC-Based DCG system with the 100% confidence bands for the evaluated times. Incidentally, CB does not allow for significant figure changes to the axis.

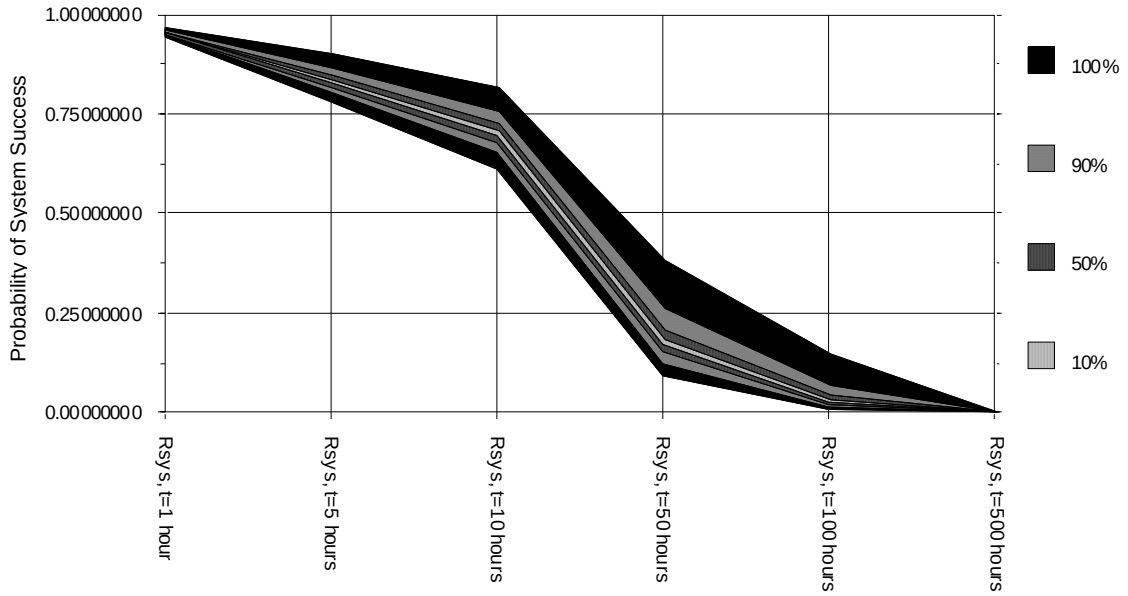

Figure 25: Variation of FC-Based DCG System Reliability with Evaluated Operating Times

This trend diagram takes the distribution of the reliability for each time and plots the information as a vertical band of confidence according to the pattern scheme depicts to the right of the graph. For instance, since the predicted reliability of the system recorded at the second evaluated time (t = 5 hours) by CB is 84% the 10% confidence band is centered at an 84% probability of system success. Since the evaluated time had the possibility of a reliability value ranging from 79% to 89%, the 100% confidence band stretches from 79% to 89% of the system reliability.

As can be seen from the trends, the major problem with the FC-Based DCG system is that the original system with normal component failure values is certain to have system failure after 400 hours of use (275 hours by the deterministic method which did not use

Monte Carlo simulation and from which no likelihood of the reliability could be determined). The system is essentially unacceptable after 100 hours of use. This could be due to the fact that the system has no redundancy and to the quality of the components (i.e. high fpmh data). Also the CB sensitivity analysis showed the MEA to be the most risky component at each evaluation time. This is evidenced by the information in Table 3 following showing the top four correlations to the system reliability. Essentially, the closer the correlation value is to unity, the more effect that component has on the total system reliability for that evaluated time. The FC-Based DCG system is so sensitive to the value of the fpmh for the MEA and Ni-Foam due to the fact that there are so many of those two components types.

Table 3: FC-Based DCG System Sensitivity Analysis

Components	Rsys, t=1 hour	Rsys, t=5 hours	Rsys, t=10 hours	Rsys, t=50 hours	Rsys, t=100 hours	Rsys, t=500 hours
Original System						
MEA	-0.71	-0.71	-0.71	-0.71	-0.71	-0.71
Ni-Foam	-0.69	-0.69	-0.69	-0.69	-0.69	-0.69
Control Valve (fuel)	-0.04	-0.04	-0.04	-0.04	-0.04	-0.04
Bipolar Plate	0.03	0.03	0.03	0.03	0.03	0.03
Reformer	-0.03	-0.03	-0.03	-0.03	-0.03	-0.03
Sensors	-0.03	-0.03	-0.03	-0.03	-0.03	-0.03
Diaphragm Pump	-0.03	-0.03	-0.03	-0.03	-0.03	-0.03
Water Pump (fuel)	-0.03	-0.03	-0.03	-0.03	-0.03	-0.03

This information is valuable; however experience with PEM FCs has shown that when properly humidified and fueled with pure hydrogen, an MEA does not stop working. The MEA will only fail if some other component fails and then disturbs the conditions under which the MEA needs to operate. Also, the Ni-Foam, when gold-plated, seems to resist corrosion rather well. Further investigation was needed to determine the other components that affect the total system reliability since the MEA and the Ni-Foam dominate this sensitivity analysis.

In order to better understand how the BOP affects the total system reliability, a revised system was created where, instead of calculating a reliability as before, the reliability of the MEA and the Ni-Foam were set to unity (R=1, 100% reliable). The failure data was still that of normal quality for the other components (calculated R). The Excel spreadsheet setup and

the CB report are included in Appendix B. The analysis in the appendix also includes a deterministic evaluation of the revised system reliability. Figure 26 following depicts the reliability of the revised configuration of the FC-Based DCG system, with the 100% confidence bands for the evaluated times.

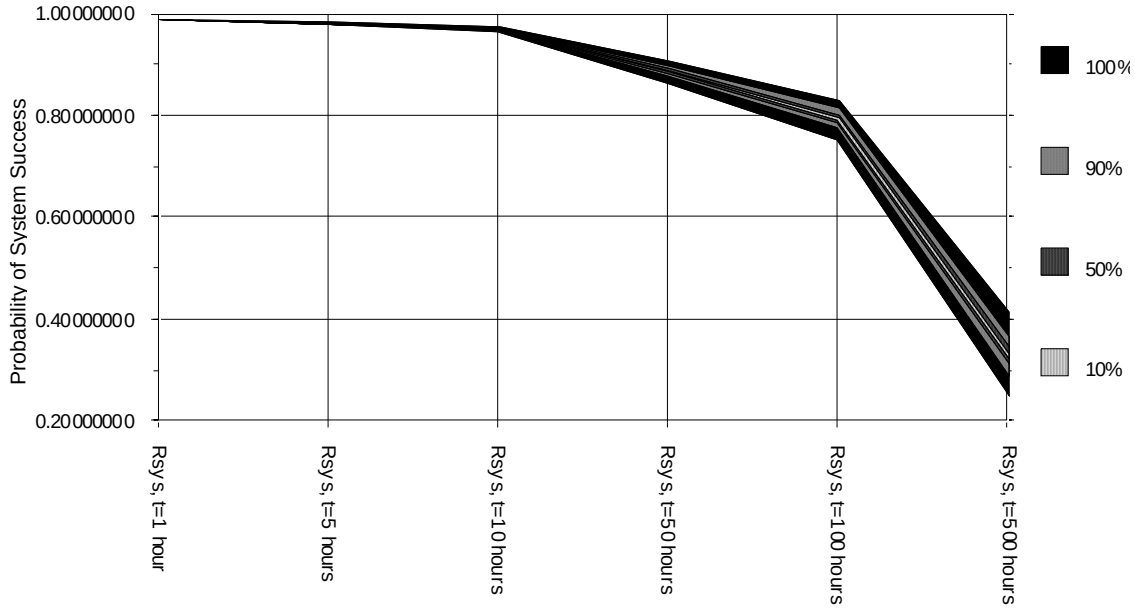

Figure 26: Variation of Revised System Reliability with Evaluated Operating Times

As can bee seen by comparing Figure 25 with Figure 26, the variability (width of the uncertainty band) of the FC-Based DCG system is greatly reduced and it should be acceptable at and under 100 hours (average R_{100} = 80%). The reliability at the 500 hour evaluated time is still disappointing at an average of approximately R_{500} = 33%. The CB sensitivity analysis now tells a different story, without the MEA and Ni-Foam in the Monte Carlo simulation. The top six most correlated components are the pumps and valves, which are also those components with the highest failure rates (fpmh values), as well as the sensors which is the most numerous component type still in the simulation. This is evidenced by the data in Table 4 on the following page.

Table 4: Revised System Sensitivity Analysis

Sensitivity Data	Rsys, t=1 hour	Rsys, t=5 hours	Rsys, t=10 hours	Rsys, t=50 hours	Rsys, t=100 hours	Rsys, t=500 hours
Revised System						
Diaphragm Pump	-0.47	-0.47	-0.47	-0.47	-0.47	-0.47
Pump (exhaust)	-0.45	-0.45	-0.45	-0.45	-0.45	-0.45
Water Pump (fuel)	-0.45	-0.45	-0.45	-0.45	-0.45	-0.45
Control Valve (fuel)	-0.28	-0.28	-0.28	-0.28	-0.28	-0.28
Compressor (fuel)	-0.27	-0.27	-0.27	-0.27	-0.27	-0.27
Sensors	-0.25	-0.25	-0.25	-0.25	-0.25	-0.25

The results for the risk analysis portion of risk engineering for this FC-Based DCG system are discussed in the next section. The results and recommendations section below will also give some suggestions on how to manage this system reliability, which is still poor after the revision of the MEA and Ni-Foam individual reliabilities. Repeated CB simulations will also be presented and discussed to show the potential impacts of the proposed changes to the FC-Based DCG system.

RESULTS & DISCUSSION

From the necessary tasks to satisfy the objectives several results have followed from this research. From the first task, to identify the necessary elements of a risk engineering process, the functions of risk engineering were determined and compared with the literature in the field. A major result for this research came from the fulfillment of second task, to develop a procedure for reviewing risk, and that procedure should be followed for future risk reviews of FC-Based DCG. Figures 7 and 19 showed the functional decomposition of what needed to be addressed in order to perform the risk assessment and risk analysis, respectively, for part of the completion of the second task.

After creating the procedure for both risk assessment and risk analysis, the procedure was tested with an example system based on the one used by CESHR in completion of the third task. The results for the risk assessment portion are: a set of components, a developed component sequence of operation, a potential mode of failure to be evaluated, and a scenario (with several more suggested) for analysis. The results for the risk analysis portion are: a set of two end states for the chosen continuous operation scenario ranging from complete success to total failure, the probabilities associated with the scenario, and the distribution of that probability (relating to the confidence in the system's risk rating) for the evaluated times. The original system gave extremely high sensitivities to two components that, in common practice, do not normally fail on their own. That is, the MEA and Ni-Foam usually fail as a result of some BOP component failure. Therefore, a revised system with the reliability of those two components set to 100% was also analyzed.

Three risk reduction activities were chosen to improve overall system reliability for the revised system: 1) to add a redundant Fuel Cell to the revised system, 2) to make the FC-Based DCG system more robust by using higher quality components, and 3) to do both (add redundancy and robustness). When adding a redundant FC to the revised system, the probability of system success improves incrementally (averages R_{100} = 80.7% and R_{500} = 34%) while the uncertainty band narrows slightly. This trend can readily be seen by Figure 27 on the following page and by noting its similarity to the previous Figure 26.

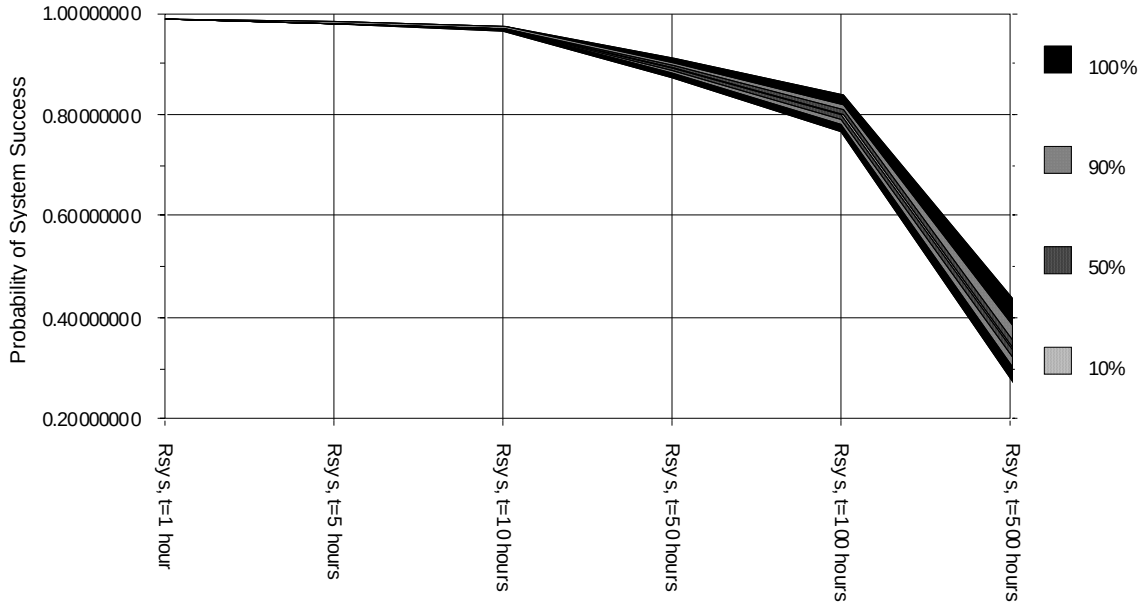

Figure 27: Variation of Reliability for Revised, Redundant FC System with Evaluated Times

The Excel spreadsheet setup and the CB report are included in Appendix C. The analysis in the appendix also includes a deterministic evaluation of the revised, redundant FC system reliability.

The failure rate data for the FC-Based DCG system high quality components is listed on the following page in Table 5, where the shaded cells in the "Variable" column showcase the changed components and the shaded cells in the median fmph column still signify a calculated failure value from an estimated MTBF. The unshaded cells in the median fpmh column still represent data gathered from NPRD-95, with the significant figures repeated here as they were reported in the handbook. [9]

Table 5: FC-Based DCG Component Failure Data for High Quality Components

Variable	Component Name	Subsystem	# of Comp.	Median fpmh
pc3	bipolar plate	Fuel Cell	81	0.01
pc4	rubber gasket	Fuel Cell	160	0.0597
pc5	tie rod (bolt)	Fuel Cell	12	2.7835
pc6	nut	Fuel Cell	12	0.5744
pc7	threaded NPT brass connector	Fuel Cell	3	5.9243
pc8	water particulate filter	Fuel	1	6.8112
pc9	reverse osmosis filter	Fuel	1	2.6455
pc10	water pump	Fuel	1	181.3384
pc11	control valve	Fuel	1	0.2912
pc12	air particulate filter	Fuel	2	0.078
pc13	light-duty compressor (2atm, 100cu.cm)	Fuel	1	10.3061
pc14	desulfurizer & reformer (adiabatic)	Fuel	1	10
pc15	Root's blower (size for dP in stack)	Fuel	1	0.5294
pc16	regenerative blower (just for dP)	Fuel	1	0.5294
pc17	hydrogen humidifier	Fuel	1	0.6261
pc18	oxygen humidifier	Fuel	1	0.6261
pc19	1-way control valve (5 cu.ft./min)	Fuel	1	0.2912
pc20	(90 ft) stainless (or Cu) 3/8 inch tubing	Fuel	1	0.7415
pc21	heat exchanger/condenser	Exhaust	1	9.9894
pc22	reservoir	Exhaust	1	2.2483
pc23	diaphragm pump (100W max)	Exhaust	1	181.3384
pc24	control valve	Exhaust	1	0.2912
pc25	compressor (lower dP than pc16)	Exhaust	1	16.0894
pc26	fuel cell cooler	Exhaust	1	9.9894
pc27	pump (200W)	Exhaust	1	181.3384
pc28	(11 ft) stainless (or Cu) 3/8 inch tubing	Exhaust	1	0.7415
pc29	(2 ft) 00 wire	Pwr Cond	1	0.1877
pc30	inverter	Pwr Cond	1	5.0851
pc31	master controller	Control	1	0.0486
pc32	sensors	Control	50	3.6125
pc33	(50 ft) 18 wire	Control	1	0.2203
Normal quality				Obtained from NPRD-95
Higher quality				Calculated from MTBF estimate

When increasing the robustness of the FC-Based DCG System by using higher quality components, the overall system reliability improves. With these changes, the system might now be acceptable between 100 and 500 hours. This trend is evidenced by Figure 28 on the following page, note the change of scale resulting in an average $R_{500} = 65\%$.

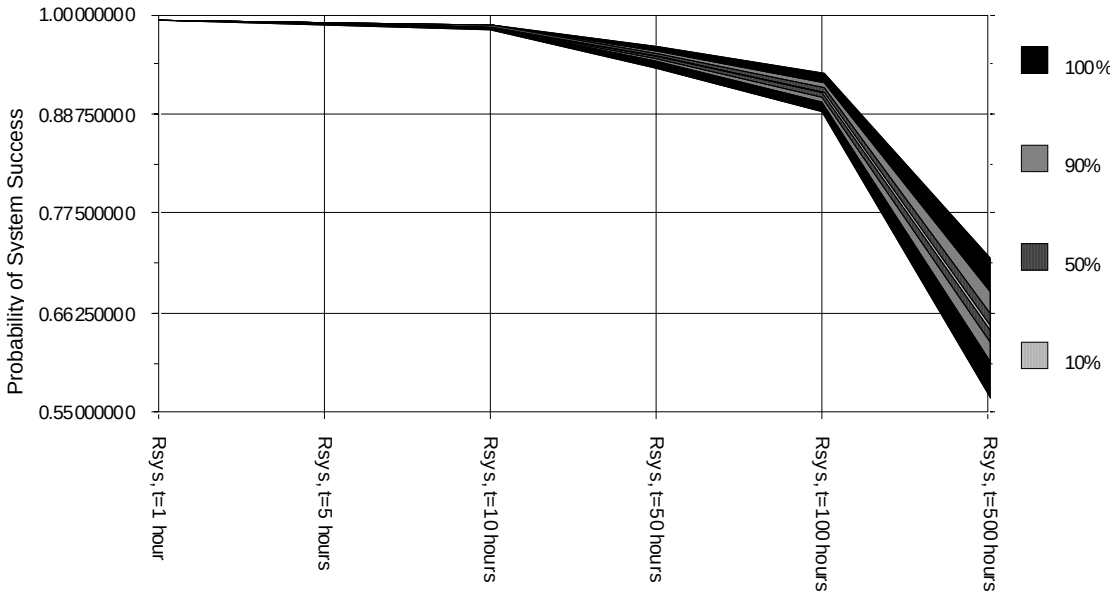

Figure 28: Variation of Reliability for Robust System with Evaluated Times

The Excel spreadsheet setup and the CB report are included in Appendix D. The analysis in the appendix also includes a deterministic evaluation of the robust system reliability.

When increasing robustness of the revised FC-Based DCG system as well as adding a redundant FC, not only do the reliability values improve over the revised system (R_{500} = 66.9%), but also the uncertainty band decreases slightly. The reliability of the robust, redundant system is not greatly improved over the robust system alone. This trend is evidenced by Figure 29 on the following page.

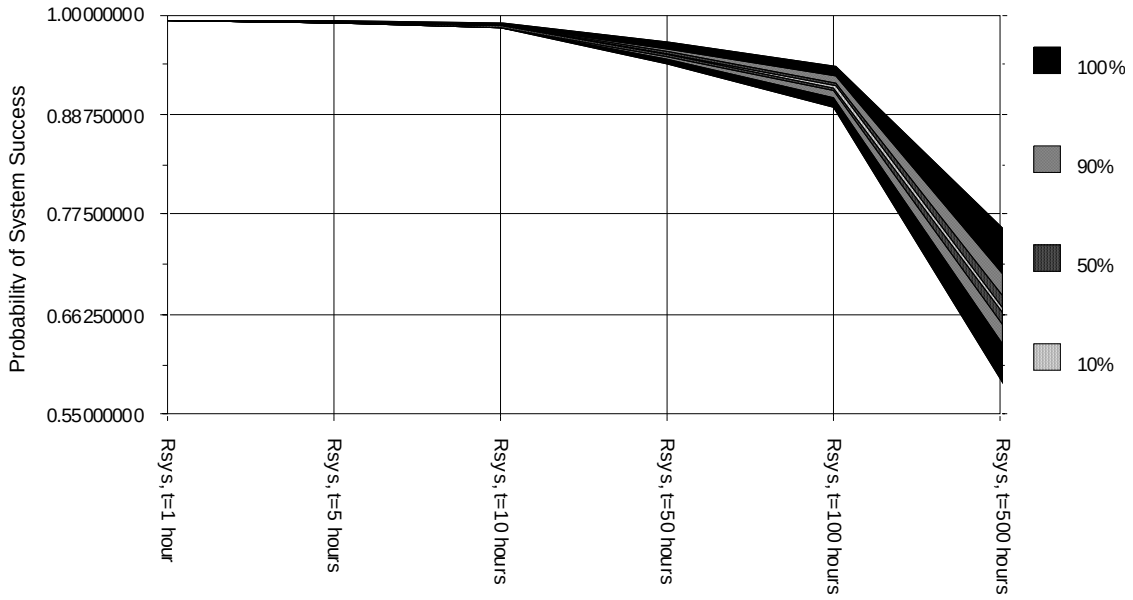

Figure 29: Variation of Reliability for Robust, Redundant FC System with Evaluated Times

The Excel spreadsheet setup and the CB report are included in Appendix E. The analysis in the appendix also includes a deterministic evaluation of the robust, redundant FC system reliability.

The information in Table 6 on the following page lists the results of the sensitivity analysis on the system: the top six correlations for each suggested risk control scenario. The sensitivity in some situations had more than one component with the same correlation, so for some scenarios more than six correlated components are shown.

Table 6: Sensitivty Analysis for Risk Control Scenarios

Sensitivity Data	Rsys, t=1 hour	Rsys, t=5 hours	Rsys, t=10 hours	Rsys, t=50 hours	Rsys, t=100 hours	Rsys, t=500 hours
Revised, Redundant FC System						
Water Pump (fuel)	-0.49	-0.49	-0.49	-0.49	-0.49	-0.49
Pump (exhaust)	-0.46	-0.46	-0.46	-0.46	-0.46	-0.46
Diaphragm Pump	-0.45	-0.45	-0.45	-0.45	-0.45	-0.45
Control Valve (fuel)	-0.32	-0.32	-0.32	-0.32	-0.32	-0.32
Compressor (fuel)	-0.26	-0.26	-0.26	-0.26	-0.26	-0.26
Sensors	-0.25	-0.25	-0.25	-0.25	-0.25	-0.25
Robust System						
Sensors	-0.49	-0.49	-0.49	-0.49	-0.49	-0.49
Pump (exhaust)	-0.49	-0.49	-0.49	-0.49	-0.49	-0.49
Water Pump (fuel)	-0.48	-0.48	-0.48	-0.48	-0.48	-0.48
Diaphragm Pump	-0.48	-0.48	-0.48	-0.48	-0.48	-0.48
Tie Rod	-0.10	-0.10	-0.10	-0.10	-0.10	-0.10
Gasket	-0.07	-0.07	-0.07	-0.07	-0.07	-0.07
Robust, Redundant FC System						
Pump (exhaust)	-0.49	-0.49	-0.49	-0.49	-0.49	-0.49
Diaphragm Pump	-0.48	-0.48	-0.48	-0.48	-0.48	-0.48
Water Pump (fuel)	-0.48	-0.48	-0.48	-0.48	-0.48	-0.48
Sensors	-0.48	-0.48	-0.48	-0.48	-0.48	-0.48
Compressor (exhaust)	-0.03	-0.03	-0.03	-0.03	-0.03	-0.03
Tubing (exhaust)	-0.02	-0.02	-0.02	-0.02	-0.02	-0.02
Air Filter	-0.02	-0.02	-0.02	-0.02	-0.02	-0.02
Tie Rod	-0.02	-0.02	-0.02	-0.02	-0.02	-0.03
Control Valve (fuel)	0.02	0.02	0.02	0.02	0.02	0.02
Bipolar Plate	-0.02	-0.02	-0.02	-0.02	-0.02	-0.02
Connector	-0.02	-0.02	-0.02	-0.02	-0.02	-0.02

A brief review of the trends in the probabilistic system risk diagrams, as shown in Figures 25 and 26 presented in the previous "Risk Review Analysis" section as well as Figures 27 through 29, allows for the following findings to be stated. Adding a continuously redundant FC to the revised system slightly improves the FC-Based DCG system. This is demonstrated by the slightly decreased slope ranging from the 10 hour through the 500 hours evaluations, and a small decrease in the width of the uncertainty band. Adding robustness improves the FC-Based DCG system more than simply adding redundancy, which is evidenced by the increase in actual reliability values in all time ranges evaluated. Therefore, system robustness would be recommended to the implementers of FC-Based DCG over FC redundancy.

From the sensitivity analysis provided by Crystal Ball and presented in Tables 3, 4, and 6 several findings may be extracted (full sensitivity analyses are supplied in the appendices of this report with the system to which they pertain). The MEA was the component to which the risk was most sensitive at all times evaluated for the original system. The pumps were the components which were highly correlated with the system risk in the revised system and in all risk control strategies. It is therefore recommended that CESHR investigate using redundancy, both continuous and standby, for these components in order to see what that risk control strategy would do to the system risk.

The probability of each scenario, when combined with its consequences, allows risk engineers to discover the most important risks about which something must be done. What to do about them is precisely what the risk management function should determine. The initial part of the fourth task, to make recommendations according to the data generated from the analysis, is as far as this research goes. It is a company's responsibility to complete the management in order to complete the risk engineering process and is outside the scope of this research. One of the scenarios presented here would need to be decided upon and implemented in order to fulfill the risk management for a FC-Based DCG system.

By no means does this thesis cover the end of research in this area. It is more like a first step towards a better, more marketable system. More simulations should be run on other failure modes for the current operating condition, and on other operating conditions, which would require the development of more operational sequence diagrams. The risk control strategy of redundancy for other components, such as the pumps, should be investigated. Also, more research is needed in order to obtain more accurate estimates for the reliability of the Ni-Foam assembly, the bipolar plates, and the reformer, which could also lead to a better understanding of other failure modes for these components. It is recommended that CESHR therefore focus on improving the performance of the system by using high quality components. The performance of the system as a whole could be improved by adding redundancy for components other than the FC; it is recommended to investigate both continuous and standby redundancy.

SUMMARY

Completing the first task needed to reach the research objectives provided the identification of the necessary elements of the risk engineering process. Completing the second task, CESHR was provided with a procedure for reviewing risk specifically in FC-Based DCG systems, which should be an invaluable deliverable. In completion of the third task, a complete example system configuration has a documented risk assessment and a risk analysis. The deliverables from this risk review are that it should be easy to understand the procedure for one familiar with the subject with a fully worked out example and that the procedure was verified by being applied to an example. The risk review produced probabilities associated with two of the various possible end states of the system – from complete success to total failure of the FC-Based DGC – and the details of how each element of the system contributes to these probabilities. System design change recommendations were made according to the data generated from the risk analysis for the system identified with the risk assessment and included possible changes to the elements that contributed the most to the risk. However, completing the final task, system design changes, would have to be performed by an implementer of the system as only they are able to determine how much risk reduction is worth the cost to them. The major deliverables from this research are the useful conclusions which CESHR will be able to draw in terms of the design configuration of physical and operating characteristics for a FC-Based DCG system which will be the least technologically risky.

The design approach was indeed able to organize, systematize, and clarify all the background information for risk engineering and simplify the application to an example FC-Based DCG system. The current FC-Based DCG design parameters in the operating condition of continuous running that contribute the most to the technological system risk of not working were the MEA, the Ni-foam flow field, and the pumps. By making the system more robust, essentially by using high quality components, the FC-Based DCG system reliability improves significantly over the original and over the revised system.

CONCLUSIONS

From the information presented in the results and discussion section above as well as in the appendices several conclusion may be drawn from this research.

The reliability of the typical FC-Based DCG system should be relatively constant and acceptable initially and then drop off significantly to an unacceptable level after a certain point in time. The system design will need to ensure that this decrease in reliability occurs after the end user is ready to purchase a new system or design some maintenance schedule to prolong the acceptable reliability period.

The MEA and the Ni-Foam are the two components that should contribute the most to the system reliability since there exists such a great number of those components in the FC-Based DCG system. When considering the MEAs and Ni-Foam assemblies to be 100% reliable, the next components to which the system reliability is most sensitive are the pumps. Thus, any improvements to the pumps will improve the entire FC-Based DCG system. The sensitivity of the system to various components may or may not vary with time.

The improvement of the robustness of the individual components should have a positive impact on system reliability, with the most impact resulting from improving those components to which the system is most sensitive. Adding redundancy for the fuel cell system provides a minimal improvement to the FC-Based DCG system reliability; however other redundancy options for other components like the pumps should be explored to fully understand how redundancy affects the system.

The design approach will continue to be useful in assessing, analyzing, and managing risk large complex systems, such as FC-Based DCG, since it collapses the overarching goals into smaller, accomplishable portions.

ACRONYMS

ABBREVIATION	MEANING
AC	Alternating Current
BANANA	Build Absolutely Nothing Anywhere Near Anybody
BOP	Balance of Plant
CB	Crystal Ball® (by Decisioneering®)
CESHR	Center for Electrochemical Systems and Hydrogen Research
CHP	Combined Heat and Power
DC	Direct Current
DCG	Distributed (Power & Heat) Cogeneration
DOE	Department of Energy
EPA	United States' Environmental Protection Agency
ETA	Event Tree Analysis
FC	Fuel Cell
FE	Failure Events
FM	Failure Modes
FMEA	Failure Modes and Effects Analysis
fpmh	Failures per Million Hours
FTA	Fault Tree Analysis
IC	Internal Combustion
LR	Legal Requirements
MEA	Membrane Electrode Assembly
MTBF	Mean Time Between Failures
Ni-Foam	Nickel-Metal Foam Flow Field Assembly
NIMBY	Not in My Backyard!
OC	Operating Characteristics
PAMT	Provide a Means To…
PC	Physical System Configurations
PEM	Polymer Electrolyte Membrane (also: Proton Exchange Membrane)
PFC	Potential Failure Consequences
PRA	Probabilistic Risk Assessment
R	Reliability
RAGS	Risk Assessment Guidelines

REFERENCES

[1] Decisioneering, Inc. Accessed on July 22, 2002. http://www.decisioneering.com/risk-analysis-print.html

[2] A. Wilson, Risk Analysis Methods for Medical Devices, Biomedical Engineering Seminar (2002) Texas A&M University.

[3] R.V. Kolluru, S.M Bartell, R.M. Pitblado, R.S. Stricoff, Risk Assessment and Management Handbook for Environmental, Health, and Safety Professionals, McGraw-Hill, St. Louis, MO, 1996.

[4] A.V. Gheorghe, R. Mock, Risk Engineering: Bridging Risk Analysis with Stakeholder Values, Kluwer Academic Publishers, Boston, MA, 1999.

[5] NASA Systems Engineering Handbook, NASA SP-610S, (1995) NASA Special Publications, Washington, DC.

[6] J. Larminie, A. Dicks, Fuel Cell Systems Explained, Wiley, New York, NY, 2000.

[7] N. McKinley, A Summary of the 2001 Developmental and Market Status of Fuel Cell Based Distributed Power Generation, MEEN 685 Report (2002) Texas A&M University.

[8] K.L. Seip, B. Thorstensen, H. Wang, Environmental impacts of energy facilities, J. Power Sources 35 (1991) 37-58.

[9] W. Denson, G. Chandler, W. Crowell, A. Clark, P. Jaworski, Nonelectronic Parts and Reliability Data, NPRD-95, Reliability Analysis Center, Rome, NY, 1994.

[10] B.S. Blanchard, W.J. Fabrycky, Systems Engineering and Analysis, 3rd Ed., Prentice Hall, Upper Saddle River, NJ, 1998.

Supplemental Sources Consulted

Bahnmaier, W.W., Editor, Risk Management Guide for DoD Acquisition, 5th Ed., Department of Defense & Defense Acquisition University Press, Fort Belvoir, VA, 2002.

DeGaspari, J., Risky Business, Mechanical Engineering, July 2002, 42-44.

Del Campo, C.S., Effects of Electrode Compression on the Performance of a Solid Polymer Electrolyte Fuel Cell, Thesis, Texas A&M University, 1997.

Department of Defense Systems Management College, Systems Engineering Fundamentals, Defense Acquisition University Press, Fort Belvoir, VA, January 2001, Chapter 15.

Kumamoto, H., Henley, E.J., Probabilistic Risk Assessment and Management for Engineers and Scientists, 2nd Ed., IEEE Press, New York, NY, 1996.

Lalk, T.R., McConnell, J.B., Spence, C.A., Robotic Mars Sample Return Risk Assessment and Analysis, NASA Report, Houston, TX, August 2000.

NASA Procedures and Guidelines, NASA Program and Project Management Processes and Requirements, NPG: 7120.A, Washington, DC, April 1998.

Niwa, K., Knowledge Based Risk Management in Engineering: A case study in human-computer cooperative systems, Wiley, New York, NY, 1989. 3-24.

Parkin, J., Engineering Judgment and Risk, Thomas Telford, London, England, 2000.

Reinschmidt, K.F., Introduction to Project Risk Management: CVEN 689-603 Course Notes, TEES Copy Center, Texas A&M University, August 2003.

Smith, D.J., Distributed generation: the power to choose, Power Engineering, (March 1999) 32-35.

APPENDIX A

Original System

In the accompanying zip file there is a Microsoft Excel file named "AppendixA Calculations.xls". The worksheets within the Excel file use the Crystal Ball add-in software from Decisioneering to evaluate the original system reliability at the evaluated times of t=1, 5, 10, 50, 100, and 500 hours. This system uses normal quality components. There are also worksheets which evaluate only the low, median, and high values of the system reliability at the same times, representing a deterministic approach.

APPENDIX B

Revised System

In the accompanying zip file there is a Microsoft Excel file named "AppendixB Calculations.xls". The worksheets within the Excel file use the Crystal Ball add-in software from Decisioneering to evaluate the revised system reliability at the evaluated times of t=1, 5, 10, 50, 100, and 500 hours. This system uses normal quality components, with the MEA and Ni-Foam Assembly reliability revised to 1. There are also worksheets which evaluate only the low, median, and high values of the system reliability at the same times, representing a deterministic approach.

APPENDIX C

Revised, Redundant FC System

In the accompanying zip file there is a Microsoft Excel file named "AppendixC Calculations.xls". The worksheets within the Excel file use the Crystal Ball add-in software from Decisioneering to evaluate the revised, redundant FC system reliability at the evaluated times of t=1, 5, 10, 50, 100, and 500 hours. This system uses normal quality components, with the MEA and Ni-Foam Assembly reliability revised to 1 and an additional, continuously redundant, FC. There are also worksheets which evaluate only the low, median, and high values of the system reliability at the same times, representing a deterministic approach.

APPENDIX D

Robust System

In the accompanying zip file there is a Microsoft Excel file named "AppendixD Calculations.xls". The worksheets within the Excel file use the Crystal Ball add-in software from Decisioneering to evaluate the robust system reliability at the evaluated times of t=1, 5, 10, 50, 100, and 500 hours. This system uses high quality components, with the MEA and Ni-Foam Assembly reliability revised to 1. There are also worksheets which evaluate only the low, median, and high values of the system reliability at the same times, representing a deterministic approach.

APPENDIX E

Robust, Redundant FC System

In the accompanying zip file there is a Microsoft Excel file named "AppendixE Calculations.xls". The worksheets within the Excel file use the Crystal Ball add-in software from Decisioneering to evaluate the robust, redundant FC system reliability at the evaluated times of t=1, 5, 10, 50, 100, and 500 hours. This system uses high quality components, with the MEA and Ni-Foam Assembly reliability revised to 1 and an additional, continuously redundant, FC. There are also worksheets which evaluate only the low, median, and high values of the system reliability at the same times, representing a deterministic approach.

VITA

Kristin Lyn Luthringer was born in Sugarland, Texas, in August of 1979 to Robert L. and Kathleen B. Luthringer. Upon graduating from James E. Taylor high school in 1997, Kristin attended Texas A&M University in College Station, Texas, in order to pursue a degree in engineering. Recognizing that the growing globalization of the economy would necessitate clear communication with other cultures, Kristin added a minor in Spanish to her degree, along with a study abroad in Monterrey, Nuevo León, México at Instituto Tecnológico y de Estudios Superiores de Monterrey (ITESM) during the spring of 1999. During the summers of 2000 and 2001, she interned with the Facilities department of Texas Instruments in Dallas and Houston, respectively. She was also a participant in the Engineering Scholars Program.

In December of 2001, Kristin graduated magna cum laude with her Bachelor of Science degree in Mechanical Engineering with a minor in Spanish. She immediately began pursuit of another degree in engineering at Texas A&M University to learn more about systems engineering, mechanical design, and design analysis so that she would be able to make a greater impact upon entering the workforce full time. Kristin completed her degree requirements in January of 2004 and obtained a Master of Science degree in Mechanical Engineering in May 2004. She is a member of the American Society of Mechanical Engineers and is certified as an Engineer-in-Training by the Texas Board of Professional Engineers.

Kristin currently resides with her new husband in Tyler, Texas, and works as a design engineer for Trane, Residential Systems. The permanent mailing address is as follows: Mrs. Kristin L. Schaefer, 14922 County Road 285, Tyler, Texas 75707.