Spring 2012

The risk mitigation strategy taxonomy and generated risk event effect neutralization method

Daniel A. Krus

Department: Mechanical and Aerospace Engineering

THE RISK MITIGATION STRATEGY TAXONOMY AND GENERATED RISK EVENT EFFECT NEUTRALIZATION METHOD

by

DANIEL ADAM KRUS

A DISSERTATION

Presented to the Faculty of the Graduate School of the

MISSOURI UNIVERSITY OF SCIENCE AND TECHNOLOGY

In Partial Fulfillment of the Requirements for the Degree

DOCTOR OF PHILOSOPHY

in

MECHANICAL ENGINEERING

2012

Approved
Katie Grantham, Advisor
Shun Takai
Lokeswarappa Dharani
Susan Murray
Jeff Thomas

PUBLICATION DISSERTATION OPTION

This dissertation consists of the following five articles that have submitted for publication as follows:

Pages 3-27 have been published in the JOURNAL OF FAILURE ANALYSIS AND PREVENTION

Pages 28-64 have been submitted to the journal RESEARCH IN ENGINEERING DESIGN

Pages 65-96 have been submitted to the JOURNAL OF ENGINEERING DESIGN

Pages 97-128 have been submitted to the journal ARTIFICIAL INTELLIGENCE FOR ENGINEERING DESIGN, ANALYSIS AND MANUFACTURING

Pages 129-161 have been submitted to the JOURNAL OF FAILURE ANALYSIS AND PREVENTION

Appendices A, B and C have been added for purposes normal to dissertation writing.

ABSTRACT

In the design of new products and systems, the mitigation of potential failures is very important. The sooner in a product's design mitigation can be performed, the lower the cost and easier to implement those mitigations become. However, currently, most mitigations strategies rely on the expertise of the engineers designing a product, and while models and for failure modes do exist to help, there are no guidelines for performing product changes to reduce risk. To help alleviate this, the risk mitigation strategy taxonomy is created from an empirical collection of mitigation strategies used in industry for failure mitigation, creating a consistent set of definitions for electromechanical risk mitigation strategies. By storing mitigation data in this consistent format, the data can be used to evaluate and compare different mitigation strategies. Applying this, the Generated Risk Event Effect Neutralization (GREEN) method is used to generate mitigation strategies for a product during the conceptual design of the product, where changes are the easiest to implement and cost the least. The GREEN method then compares and selects the best strategy based on the popularity, likelihood change, and consequence change that result from implementing the strategies.

ACKNOWLEDGMENTS

I would like to thank my advisor, Dr. Katie Grantham, for all of her help throughout my research here at MS&T. Her teaching, pushing, prodding, and sound advice have brought me to this point, and I could not have asked for a better advisor throughout my time as a graduate student.

I would also like to thank Dr. Shun Takai, Dr. Lokeswarappa Dharani, Dr. Susan Murray, and Dr. Jeff Thomas for serving on my Advisory Committee, and offering helpful comments throughout my career.

I would also like to thank Delvrick Bozeman, Yoon Hyung Lee, and the other members of the R.I.S.K. by Design Lab for their assistance on this project.

Finally, I would like to thank my friends and family for their support throughout this journey. Without their kind words and criticisms, I would not be at this point in my life, and would have fallen behind long ago. I would like to dedicate this work to them, who have kept me on this long and difficult road, even when I was ready to give up. My greatest thanks to all of you; this work is thanks to you.

TABLE OF CONTENTS

Page

LIST OF ILLUSTRATIONS

LIST OF TABLES

1. INTRODUCTION

Failure prevention in a product is an important consideration in the design of a new product. Focusing on prevention during the conceptual stage of design can have a great impact on the cost of the product, as the largest changes can be made with the least overall cost. However, this process is often difficult, as communicating risk mitigation strategies are often difficult.

When trying to communicate risk mitigations strategies, proper communication of the context of the strategy is important. Information on the risk, the change, and its effects must be clearly stated, in a way that others can understand and implement the strategy. Further, in order to store data on those strategies, there needs to be a clear set of attributes that can be used to define a mitigation strategy.

These attributes allow for the creation of a consistent language of mitigation strategies to be created. This risk mitigation strategy taxonomy is a collection of 42 defined electromechanical mitigation strategies, derived from case studies of successful mitigation strategies. Using this set of defined strategies, mitigation can be performed on a product by identifying failure modes, and then selecting potential mitigation strategies that have been used to correct the failure in the past.

Further, the taxonomy can be used as a tool to help collect data and use it to generate mitigation strategies based on the parameters the strategies have changed, and the parameters that correspond to the failure modes they mitigate. This method, the Generated Risk Event Effect Neutralization method, allows mitigation strategies to be generated during the conceptual stage of design, and integrated into the product from the very beginning. Also, the method allows those with minimal experience in risk

mitigation to mitigate failures in a product, and supplements the experience of those who are already experienced in risk mitigation.

This dissertation presents the construction of the risk mitigation strategy taxonomy, and its use in risk mitigation. Further, it demonstrates the use of the taxonomy along with failure mode parameters and the failure mode taxonomy to allow the generation of mitigation strategies during the conceptual design, the Generated Risk Event Effect Neutralization (GREEN) method. Finally, it covers how to collect and populated the GREEN knowledgebase, so as to improve its performance.

PAPER I

A STEP TOWARD RISK MITIGATION DURING CONCEPTUAL PRODUCT DESIGN: COMPONENT SELECTION FOR RISK REDUCTION

Daniel Krus

Department of Mechanical Engineering

Missouri University of Science and Technology

Katie Grantham, Ph.D.

Assistant Professor of Engineering Management and Systems Engineering

Missouri University of Science and Technology

ABSTRACT

The objective of this paper is to introduce a method that will mitigate product risks during the conceptual design phase by identifying design variables that affect product failures. By using this comprehensive, step-by-step process that combines existing techniques in a new way, designers can begin with a simple Functional Model and emerge from the conceptual design phase with specific components selected with many risks already mitigated. The Risk in Early Design (RED) method plays a significant role in identifying failure modes by functions, and these modes are then analyzed through modeling equations or lifespan analyses, in such a manner that emphasizes variables under the designers' control. With the valuable insight this method provides, informed decisions can be made early in the process, thereby eliminating costly changes later on.

Keywords: concept selection, risk analysis, lifespan analysis

1 INTRODUCTION

Failure in a product is an important point to consider in the design of a new product. Despite being designed by teams of trained engineers using risk analysis tools such as Failure Modes and Effects Analysis (FMEA), fault tree analysis, and event tree analysis, many products in today's market experience failure during use. These products that can pose a safety risk are recalled after production by organizations like the Consumer Product Safety Commission (CPSC) or the Federal Aviation Administration (FAA). In 2008 alone, the CPSC recalled 563 different products, numbering almost 60.8 million units [1].

Further, the conceptual design phase can have a great impact on the overall cost of the product. This portion of the design phase, which tends to cost only 5 percent of the design cost, can change the cost of a product by up to 50 percent [2]. Finding a way to limit the failures during this early, very cost efficient portion of the design process would be beneficial to the company, as well as the eventual customer for the product.

During the initial stages of design, different concepts for a product are created through a variety of means. These product concepts can use a variety of components, each having different modes of failure. Choosing or designing the best component for the product is often a long, subjective process requiring several iterations. However, by applying analytical methods, such as the one suggested in this paper, potential solutions can be selected or designed for a product with a focus on limiting the potential failure. The method presented in this paper presents a means to select or design components to remove or limit the failures with the greatest likelihood and consequence of occurrence.

In this paper, a means of using existing failure information to help select and design components for use in a new product through the means of combining the Risk in Early Design method and models of failure is shown. This method is then demonstrated through the case study of a wind turbine unit.

2 BACKGROUND

2.1 Concept Selection

The conceptual stage of design focuses on identifying actions that the system or product must perform, organizing those actions into a logical model of the product, and then develop potential product concepts by selecting or designing components. This process generates many potential concepts, and then evaluates them based on design criteria. These concepts are refined many times until a final, single concept is decided upon [2].

Several different concept generation techniques exist. Selection design uses components that currently exist to design a new product, while configuration design focuses on the configuration of existing components to improve the design. Parametric design changes aspects of a design to create new products, whereas original design is the creation of new products that are different from those that currently exist [3].

These types of concept generation can be assisted by a number of tools, such as using multiple members of a design team to create ideas, and then expand on them. Some of these tools are the 6-3-5 method, which calls for each member of the team to create three ideas, and then spend time adding to each other's ideas [4], or the Theory of Inventive Problem Solving (TRIZ), which uses the concept that the current problem to be solved by this product has been solved in another design for an unrelated reason [5].

Another set of these tools are morphological methods, where specific components are matched to the actions a product must perform. These methods can be accomplished through brainstorming using the above tools to identify as many solutions as possible for a given action, or by using a digital design repository and design structure matrices to determine the components [4, 6].

Recently, a computational tool called MEMIC was introduced by Arnold, Stone, and McAdams. This tool takes a model of the new product's actions and uses an online design repository to create a morphological matrix based on existing solutions to those actions. As the user selects component solutions, the program will also remove incompatible solutions from further down the list, allowing a novice engineer to generate concepts based on morphological methods [7]. However, none of these design methods involve risk analysis in their approach.

2.2 Risk Analysis

To aid the designer in finding potential risks to a system, there are several methods available. Fault Tree Analysis (FTA) uses backwards logic to trace a failure in a mature system to its possible causes. Beginning with this failure, called the "top fault," potential other faults that could cause or contribute to the top fault occurrence are determined. The potential causes for these faults are then determined, repeating this step until all of the potential root faults are located. Then, using team experience, the probability of each potential fault occurring is determined, allowing an overall probability for a given chain of faults occurring [8, 9].

Similarly, Event Tree Analysis (ETA) traces a chain of failure from a single initiating event, although unlike FTA, this method uses forward logic [10]. Starting from

the “initiating event,” paths are created showing the possible events that can occur in the system, leading to the ultimate failure. Each path is a binary choice, though in some cases both choices can have the same outcome. Like Fault Tree Analysis, it requires a mature system, and uses the experience of the engineer performing the analysis to generate probabilities of the individual events occurring [11].

Failure Modes and Effects Analysis (FMEA) describes areas of potential failures in a system and their severities. Each potential failure mode lists the component affected, the consequences of the failure, and potential solutions to either mitigate or eliminate that failure mode [12].

The Risk in Early Design (RED) method uses historical failures to determine potential failures of a new product. Using a historical database of failures, RED calculates the likelihood and consequence of an action of the product failing by a particular failure mode. RED can be performed during the conceptual phase of design as if focuses on the actions a product performs rather than the components that make up the product [13].

Function-failure identification and propagation (FFIP) uses a combination of two models of a system to trace potential failures through a system. The first functional model is built based on the actions the system must perform, the second model is a configuration model based on the configuration of components in the system. Based on these two models, potential failures are tied to the actions they perform, and a simulation is run using a starting failure. Based on that starting failure and the relationships taken from the configuration model, it predicts what other actions may fail, and by what means [14].

Like FFIP, function-based failure propagation uses a functional model to predict the likelihood of a chain of failures occurring. This method uses RED to detect the actions of a new system most likely to start a chain of failures, and traces all of the potential chains that lead to actions the system is most dependant on. Using historical failure propagation data collected from failure reports [15], the likelihood of each chain of failures occurring is calculated using Boolean operations, allowing the designer to find the chains of failures most likely to occur [16].

Throughout all of these function-failure based methods, a consistent language of failure modes should be used. This failure mode taxonomy originally consisted of only mechanical failure modes [17, 18], but in recent years, has been expanded to cover electrical failure modes as well [19, 20]. This taxonomy provides a single, consistent language of failures, and can be used to quantify data uniformly, as well as meaningfully communicate those results to other engineers.

While all of these methods aid in the finding of potential or already existing failures in products, they lack a technique to limit that failure. For this purpose, risk mitigation methods are required. By combining these methods with risk mitigation methods, better products can be designed.

2.3 Risk Mitigation

Reliability prediction strategies, such as penalty functions, show methods to determine further risk analysis methods that should be applied for different systems, or which systems are most reliable. Penalty functions can be used alongside genetic algorithms to find an optimal design solution based on reliability and cost. From an initial set of solutions, child solutions are created and then rated for their feasibility. This

adapting penalty function eliminates the most unfeasible solution, and the remaining feasible solutions are used to generate new children until an optimal solution appears [21].

The system reliability prioritization method proposed by Coit uses the uncertainty of different methods to determine which components need additional analysis. From certain cases, the uncertainty of a particular component will have little effect on the prediction of the reliability of the entire system. By using the normalized variance of the system reliability, the components that add the most variance to the system can be identified for further analysis [22].

These methods are not the only ways that potential failures for a product can be found. Sometimes, the mode of failure is known, and only how long it will take for the failure to manifest is unknown. In these cases, lifespan analysis can be used to provide an estimate of the life of the product based on a particular failure mode.

2.4 Lifespan Analysis

Lifespan analysis performs testing on a product to analyze its expected working life and behavior over the course of that life. Statistical lifespan analysis tests the life of a product by running at its intended standard operating conditions, or at much harsher conditions in an accelerated life test. This purposely allows units to fail in controlled conditions, and then uses the data from those failures to fit an appropriate probability distribution over the life of the product. That data can then be used to evaluate other useful reliability information about that product. Existing data from such tests can be used to perform a Monte Carlo simulation, which can be used as a start to plan new tests for similar products [23]. These simulations use random inputs from a defined set and

run a deterministic calculation on them [24]. Using this method, the previous failure data determines the outcomes based on the random inputs, giving a simulated lifespan test. These tests, while useful, still contain uncertainty. These uncertainties can be parametric where they come from finite test elements or subjective interpretation of the data, or modeling uncertainties where errors in modeling or approximation create uncertainty in the data [25].

While lifespan analysis provides a picture of the life of a system based on a single failure mode, there are often many potential failure modes in a new system that must be considered. Combining lifespan analysis with other methods to determine the risk of failure can allow for a more thorough risk mitigation process.

3 RISK MITIGATION IN CONCEPTUAL DESIGN

By using existing failure models alongside risk analysis tools, a method for mitigating the potential failures of a new product can be realized. This method involves applying RED to the functional model to determine the potential failure modes and corresponding functions have the greatest likelihood and consequence of occurrence. These function-failure mode pairs are then further analyzed through the means of existing failure models and lifespan analysis to provide a beginning point for further failure mitigation.

During the conceptual phase of design, there are many possible forms that a product design can take. While the components that make up the product are yet unknown, the actions the product must perform are known. Performing a RED analysis on the system identifies potential failure areas in the system. The actions and the

corresponding failure modes are ranked by consequence and likelihood into low, moderate, and high risk failures. This initial analysis identifies the high risk areas of the product that should be focused on to minimize failure.

Once these highest risk areas of the design are known, the components that correspond to those functions have to be evaluated against each other so that the component with the least risk can be selected for each. The actions used in the RED analysis correspond to potential components used in the different concepts. The potential components that fit the highest risk functions from RED are identified, as well as the failure modes that apply to those components. Different components can perform the same actions as each other, yet may not fail by the same failure modes.

Once the potential components that correspond to a given action and failure mode have been determined, a means to assess the failure modes of the different components is found, either in the form of an equation or statistical lifespan analysis.

For many mechanical failure modes, there exist mathematical models for failure based on the geometry, loading, and properties of the component. A literature review revealed many of the mechanical and electrical failure mode equations from the failure modes in the taxonomy. From these modeling equations, variables were divided into design parameters that is, those parameters that can be altered by the designer, and situational, or those parameters dependant on the situation the system is in, and the designer has limited control over. In these models, the design parameters are marked with a (D) and the situational parameters are marked with a (S).

For example, “high cycle fatigue” can be modeled using the Stress Life Method, shown in Table 1 [26]. In this model, the experimentally determined material parameters

C and *m* and the stress intensity factor *K* were deemed design parameters as the designer can choose the material used in the design, as well as the geometry of the component. The number of cycles, *N*, as well as the crack growth, *a*, were deemed situational parameters as the number of cycles of operation and the rate of crack growth are usually design requirements, and cannot be altered by the designer. These design parameters can be used as a starting point for selecting or designing new components. While the exact details may not exist until later in the design, the basic concepts from the model can be used to help the designer rule out or create appropriate solutions to a function.

Using this similar methodology, the design and situational parameters were determined for all of the found failure mode models. Using these equations can help design the component so that it will not fail under operation, will last as long as needed, or determine if the component is not feasible to the product. A complete current listing of modeling equations used in this method is presented in Appendix A.

Table 1. Collection of Some Mechanical Failure Mode Models

Failure Mode	Equation	Description
Fatigue (High Cycle, Impact, Surface, Thermal) [26]	Stress Life Method $\frac{\partial a}{\partial N} = C(\Delta K)^m$	a = crack growth (S) C & m = material properties (D) K = Stress intensity factor (D) N = number of cycles (S)
Fatigue (High Cycle, Impact, Low Cycle, Surface, Thermal) [26]	Strain Life Method $\frac{\Delta\varepsilon}{2} = \frac{\sigma'_f}{E}(2N)^b + \varepsilon'_f (2N)^c$	ε = strain (S) σ_f, b, ε_f, c = material constants (D) E = modulus of elasticity (D) N = number of cycles (S)
Galling [27]	$V = Klw/p$	V = volume lost (S) K = wear coefficient (D) l = sliding distance (D) w = normal load (S, D) p = indentation hardness (D)
Seizure [27]	$P_m \geq \sigma_{YP}$ or $\frac{W}{A_a} \geq \sigma_{YP}$	P_m = nominal contact pressure (S) σ_{YP} = uniaxial yield point stress (D) W = load (S) A_a = apparent contact area (D)

In certain instances, it is difficult for a single or set of mathematical equations to accurately model a failure mode. Some, such as "creep" or "undercurrent," are simply difficult to predict without testing. Others, such as "fretting fatigue," "corrosive wear," and "gate oxide breakdown" do not yet have a model or have yet to validate any existing models [27, 28]. Finally, some such as "fretting corrosion" and "radiation damage" vary greatly depending on the material undergoing the failure, and lack a single unified model [27, 29]. In cases such as this, lifespan analysis can be used to help predict the overall lifespan or degradation rate of the failure mode.

For this analysis, lifespan data regarding that component and failure mode can be used to simulate the behavior of that failure mode. This data can be found for similar

products that have had lifespan testing performed on them for a given failure mode, and consist of a type of lifespan distribution function and the corresponding parameters (such as the Weibull distribution), or the means to calculate these values.

Using this data, a Monte Carlo simulation can be run to give an idea of how the component behaved during a lifespan test. This data can be used as a basis to compare the overall lifetimes of components and their probability of failure at a particular time in their life. Based on the data from these models and the initial inclusion of RED, a component can be selected to give the product the minimum likelihood of failure as well as the desired length of life, to help eliminate the function-failure mode pairs of highest risk. As a further benefit to using this analysis, if further detail is required or a significant change to the component has been made during design, the simulation results can be used as the starting point for performing a lifespan test, which can be carried out later in the design process. In this way, historical data on a component can be used to predict its failure behavior for a given failure mode.

4 CASE STUDY

As an example of the application of this method, a case study of a wind turbine will be examined. For the purpose of this example, we will look at the wind turbine during the conceptual phase of the design. Since we are at the conceptual stage, the only thing that exists is a functional model of the turbine, as shown in Figure 1.

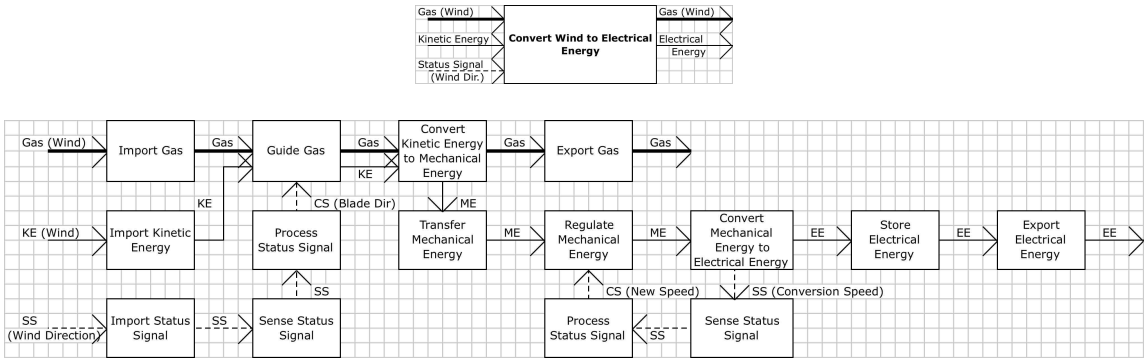
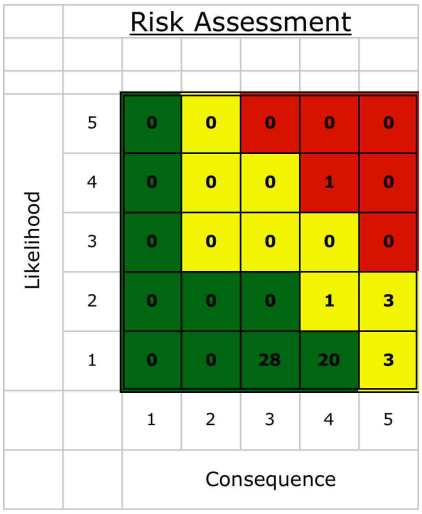


Figure 1. Functional Model of Wind Turbine

Using the functional model, a list of functions is generated and used to run a RED analysis. For this case study, the RED analysis returned fifty-six function-failure mode pairs. These results point toward the functions and failure modes that have the highest consequence and likelihood of failure. There was one high risk function-failure mode pair, "transfer mechanical energy fails due to high cycle fatigue," and seven moderate risk function-failure mode pairs as shown below in Figure 2. In the fever chart, the axes show the severity of the consequence and the likelihood, and the number in the cell is the number of function-failure mode pairs that have that likelihood and consequence combination.



Transfer Mechanical Energy fails due to High Cycle Fatigue	(4, 4)
Import Gas fails due to High Cycle Fatigue	(5, 2)
Guide Gas fails due to High Cycle Fatigue	(5, 2)
Export Gas fails due to High Cycle Fatigue	(5, 2)
Transfer Mechanical energy fails due to Impact Fracture	(5, 1)
Regulate Mechanical energy fails due to High Cycle Fatigue	(5, 1)
Regulate Mechanical energy fails due to Thermal Shock	(5, 1)
Transfer Mechanical energy fails due to Yielding	(4, 2)

Figure 2. RED Results for Wind Turbine (Consequence, Likelihood)

The current RED knowledge base is incomplete, and as such has no data on some failure modes, such as undercurrent. While it is not the purpose of this paper, a well-populated RED knowledge base would also include appropriate electrical failure modes as well. The example of undercurrent used here was chosen as data for this failure mode is easily available.

Once this portion of the analysis is completed, the analysis follows two different paths, one for failure modes that can be modeled by existing mathematical models, and one for those that either have no existing model or are difficult to model.

4.1 Analysis Based on Failure Mode Model

Once the potential failures of the turbine have been determined, a means of evaluating potential solutions by this failure mode must be found. Of these function-failure modes, the highest risk pair can be modeled using the "strain life method" to model the high-cycle fatigue. This model, shown in Eq. (1), relates the strain, modulus of elasticity, and the number of cycles to the material properties. Of the two models for high-cycle fatigue, this model is regarded as having the higher accuracy, and the better choice for this purpose.

$$\frac{\Delta\varepsilon}{2} = \frac{\sigma'_f}{E}(2N)^b + \varepsilon'_f (2N)^c \tag{1}$$

As shown in Table 1, for this model, the situational parameters are the strain, ε, and the number of cycles, N. The design parameters are the modulus of elasticity, E, and the material properties σ'_f, b, c, and ε'_f. For this particular instance, the strain and the number of cycles are set by the situation. Whatever component that will be used to answer the function "transfer mechanical energy" will be dependent on the load it will experience and the number of cycles that are required for its active life. To achieve those desired results, the material the component is made out of must be resistant to strain, possessing a balance of a high modulus of elasticity and strength. When selecting or designing the component, the material that it is made of should be selected with great care.

In current wind turbines, materials such as steel and aluminum are used in the drive train to transfer the mechanical energy from the blades to the generator. To determine the most suitable material, the material properties are used to calculate the strain amplitude ($\Delta\varepsilon/2$) for the different materials, for a given number of cycles. For the purposes of the wind turbine, the components are designed for very long life, such as $4x10^8$ cycles of life. The properties for 2024-T4 aluminum, 1018 steel, and 4142 quenched steel and the resulting strain amplitudes are collected in Table 2 [30]. As can be seen, the strain amplitude for the 1018 steel is an order of magnitude smaller than the aluminum, as 1018 steel is a softer low carbon steel. However, the hardness of the 4142 steel compares better to the aluminum for this example. For these three materials and these properties, the 4142 steel can withstand a higher strain for the same life, at high life spans as shown in Figure 3. The 4142 steel would be the best choice in this case. This method can be repeated for many more materials, in this same fashion, to select the material capable of handling the required load (strain) for the appropriate life.

Table 2. Analysis of Different Materials for Transfer Mechanical Energy

Material	**2024-T4 Aluminum**	**1018 Steel**	**4142 Quenched Steel**
E	70430 MPa	207000 MPa	200000 MPa
σ'_f	764 MPa	882 MPa	2549 MPa
B	-.075	-.118	-.078
C	-.649	-.412	-.436
ε'_f	.334	.16	.003
$\Delta\varepsilon/2$ for $N = 4x10^8$	.00233	.000414	.00258

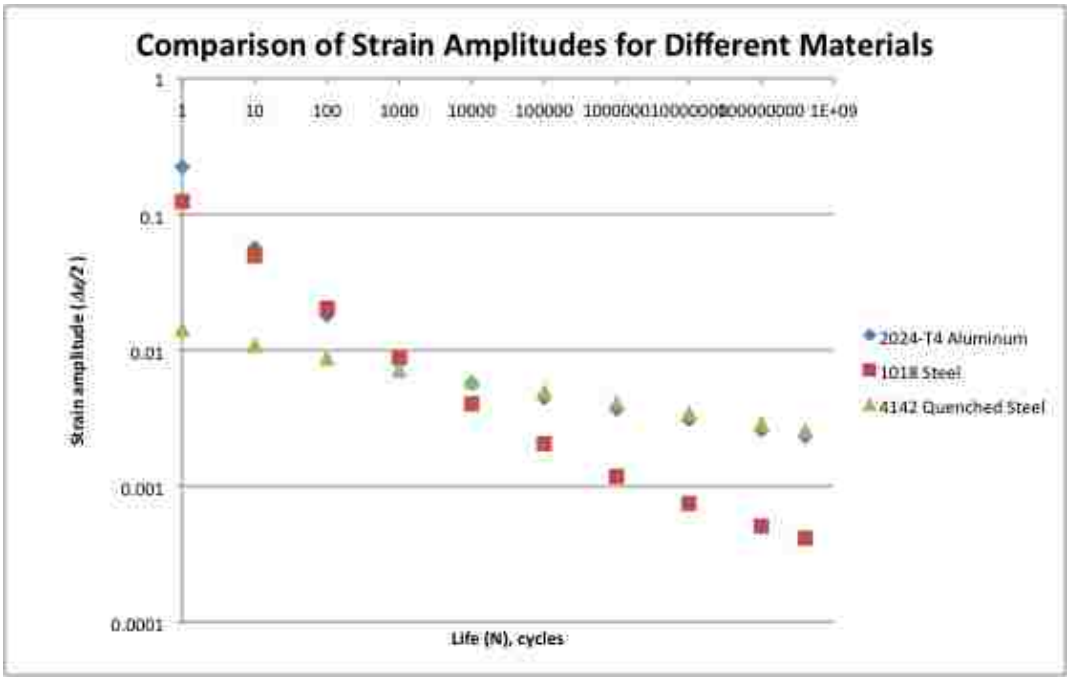


Figure 3. Comparison of Strain Amplitudes for 2024-T4 Aluminum, 1018 Steel, and 4142 Quenched Steel

4.2 Analysis Based on Lifespan Analysis

As a further example of the application of this method when no simple model exists, a case study of the action "store electrical energy" will be examined. For the turbine, one of the actions it must perform is "store electrical energy." After performing a RED analysis, one of the potential failure modes for this action is "undercurrent," where the electrical current in a device drops to the point that performance is affected or halted.

After the initial RED analysis, components that solve that action must be selected. For the action "store electrical energy" and the failure mode of "undercurrent," there exist several possible components. For this case study, three different batteries were considered as solutions to this action. These three batteries were lithium ion, sodium

sulfur, and nickel hydrogen. While it is understood that at least one of these batteries is unsuitable for the chosen application (lithium ion), these batteries were chosen as lifespan data was readily available for them. Each of these batteries differ in chemical composition. The failure mode for undercurrent has no simple model or mathematical formula to use for analysis, so a Monte Carlo simulation was performed using the data for the three batteries.

For these simulations, data was required. A literature search revealed that each of these three batteries can be modeled using a Weibull distribution with a positive shape parameter. For this distribution, shown in Eq. 2, the shape parameter, β, and the scale parameter, η, were used. These parameters correspond to the shape of the distribution and the overall size. The scale parameter corresponds to the .632 quantile at which 63.2% of the products have theoretically failed. Using the different parameters for each battery, 200 data points corresponding to theoretical failed units were generated using the Monte Carlo method. From that data, the cumulative distribution and hazard functions were created. These represent the percent of units failed at a given time and the propensity that a unit will fail in the next instant, respectively. For the hazard function, if *n* units are operating at time *t*, then *n* x *h(t)* is the approximate number of failures per unit time.

$$\Pr(T \le t;\eta,\beta) = 1 - \exp\left[-\left(\frac{t}{\eta}\right)^{\beta}\right], t > 0 \qquad (2)$$

The shape and scale factors for the lithium-ion batteries were 17.155 for β and 505 for η, as discussed by Park, *et al* [31]. For sodium sulfur batteries, the shape parameter β was 5, and η was 87600, based on information from Weaver *et al*. [32]. The

nickel hydrogen batteries used a shape parameter β of 12 and a scale parameter η of 46959, as stated by Simons, *et al* [33]. The scale parameter was obtained by converting the given mean of 45000 charge-discharge cycles using the Weibull mean involving the gamma function [23].

The simulations show that these batteries would theoretically not fail by undercurrent until approximately 370 hours of constant use, and the last should theoretically fail at approximately 550 hours of use. This constant use includes charging and discharging of the battery. The hazard function ranges from 0 to .15 during those hours. The lifespan of the sodium sulfur batteries are much greater than those of lithium ion, with failures due to undercurrent beginning to show up at 30000 hours and the last failing at approximately 130000 hours, or a little under 15 years. The hazard function ranges from 0 to .00027 across those ranges, much smaller than that of the lithium ion battery. The lifespan of the nickel hydrogen batteries are greater than those of lithium ion, but shorter than those of sodium sulfur. The first failures begin to appear at around 47000 hours, and the last fail at approximately 85000 hours, or just under 10 years. The failure probabilities from the hazard function ranged from 0 to 0.0013, higher than that of sodium sulfur. Comparisons for all three batteries' cumulative distribution and hazard functions are shown in Figures 4 and 5.

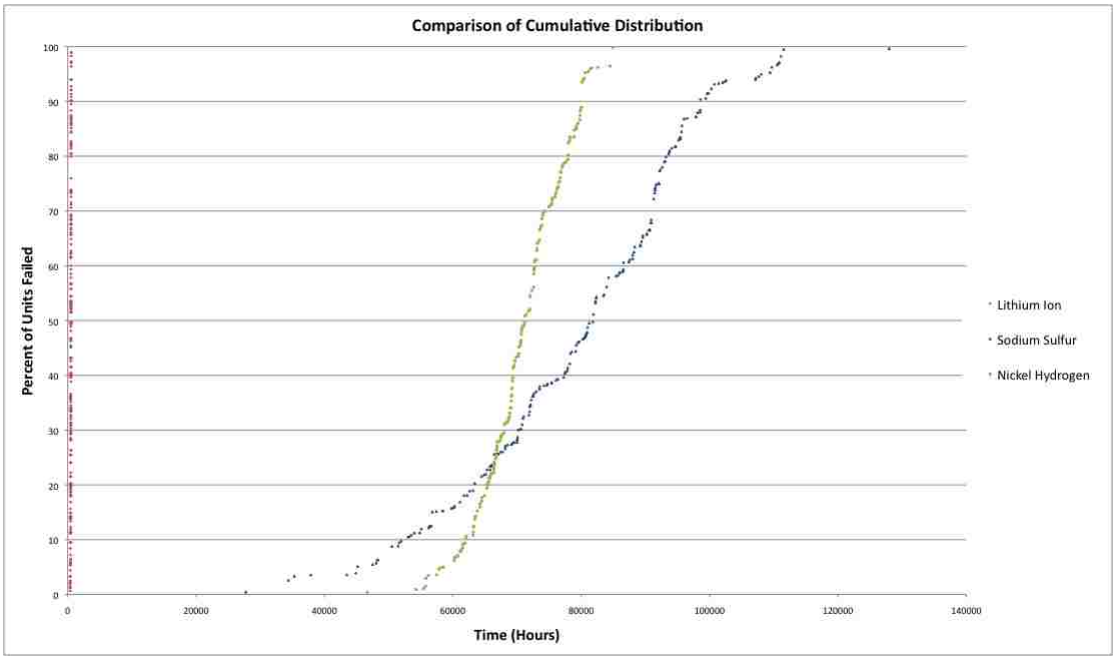


Figure 4. Comparison of Cumulative Distribution Functions for Lithium Ion, Nickel Hydrogen, and Sodium Sulfur Batteries

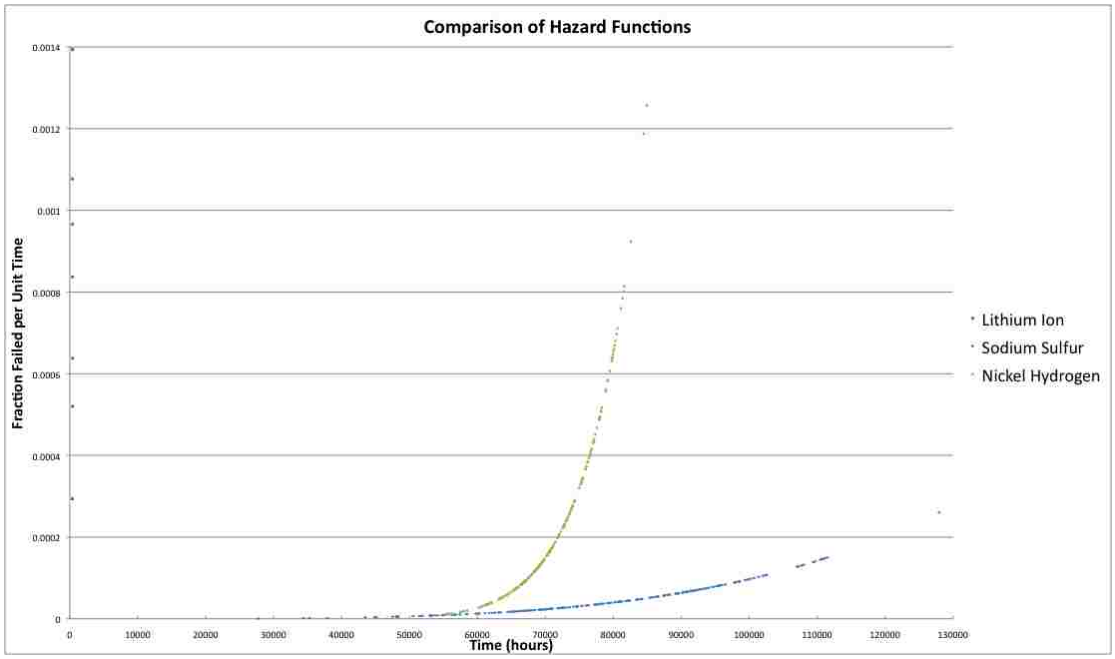


Figure 5. Comparison of Hazard Functions for Lithium Ion, Nickel Hydrogen, and Sodium Sulfur Batteries

4.3 Results

Based on these results, the appropriate component to limit failure can be selected. In the case of the function "transfer mechanical energy," a material with a good balance of strength and elasticity should be selected to ensure the required number of cycles in the components life, for the given strain. Once potential component have been selected, individual calculations can be carried out to determine the best possible selection using the model.

In the case of "store electrical energy," the lithium ion battery neither has the longest lifespan nor the lowest probability of failure in comparison to the other battery types. As shown in Figure 4, the lithium ion batteries climb very high, very early on the chart. While both sodium sulfur and nickel hydrogen batteries have a significantly fraction of failures for a given time than lithium ion over their entire lifetimes, they differ in the length of life and the fractions of units failed. For the purpose of our example wind turbine, which needs batteries that will last longer in the field and have a lowest number of failures, the sodium sulfur batteries are the optimal choice. The batteries should run failure free for about 4.6 years, and then require some monitoring for failed units from that point onward. If further data is required later in the design process, this data can be used to design further analysis, such as accelerated lifespan testing, to further clarify the component and identify specific failure times for the version of the component that has been selected.

5 CONCLUSIONS

As shown in the above example, the application of RED to determine potential failure modes and their models can help an engineer design a new product with a focus on reducing potential failures. Whether the model of the failure is an understood equation or requires statistical lifespan analysis, this comprehensive method can help the novice engineer design new components as well as select from existing ones. The use of existing failure mode models along with the RED analysis tool helps the designer to identify the important aspects of a component. Similarly, by analyzing the lifespan distributions of different components, an appropriate low-risk component can be selected or designed for the product based on the expected life of the component or the probability of failure at a given time. By using this method during the conceptual phase of design, new products with fewer potential failures can be designed.

6 FUTURE WORK

This work is the starting point for future risk mitigation methods. A further analysis of available risk mitigation methods, as well as their costs and measures of success, would add to the design parameters and lifespan analysis, as well as the design of a tool to help novice engineers select the best method to use.

ACKNOWLEDGMENTS

The authors would like to acknowledge the assistance of Even Laboube and Noroharivelo Randrianampy for their help on this project.

REFERENCES

[1] *2008 Performance and Accountability Report: Saving Lives and Keeping Families Safe*. U. S. Consumer Product Safety Commission, Editor. November 2008.

[2] Ullman, D. G. *The Mechanical Design Process*. 3rd Edition. 2003, Boston, McGraw Hill.

[3] Hyman, B. I. *Fundamentals of Engineering Design*. Upper Saddle River, NJ, 1998, Prentice Hall.

[4] Otto, K. N., and Wood, K. L., 2001, Product Design, Prentice-Hall Inc., Upper Saddle River, NJ.

[5] Altshuller, G., Creativity As An Exact Science, 1984. Gorden and Breach, Luxembourg.

[6] Bryant, C., et al. *Concept Generation from the functional Basis of Design* in *International Conference on Engineering Design*, *ICED 05*. 2005. Melbourne, Australia.

[7] Arnold, C.B., Stone, & McAdams. "MEMIC: An Interactive Morphological Matrix Tool for Automated Concept Generation. " *Proceedings of the 2008 Industrial Engineering Research Conference*. 2008.

[8] Vesely, W. E., et al., *Fault Tree Handbook*, United States Nuclear Regulatory Commission, Editor. 1981, U.S. Government Printing Office.

[9] Bedford, T and R. Cooke, *Probabilistic Risk Analysis: Foundations and Methods*. 2001, Cambridge: Cambridge University Press.

[10] Frank, M. V. *Reentry safety: probability of fuel release.* In ESREL '99. 1999.

[11] *Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, Appendix I: Accident Definition and Use of Event Trees*, United States Nuclear Regulatory Commission, Editor. 1975.

[12] *Procedures for performing failure mode, effects, and criticality analysis*, Department of Defense, Editor. 1980.

[13] Grantham Lough, K. A., "Risk in Early Design," *A Dissertation*, University of Missouri-Rolla, August 2005.

[14] Kurtoglu, T & I. Tumer. "A Graph-Based Fault Identification and Propagation Framework for Functional Design of Complex Systems*." Journal of Mechanical Design*, Vol. 130. May 2008.

[15] Grantham Lough, K & D. Krus. Breaking the cycle-preventing failures by

leveraging historical data conceptual design. *Proc. Flexible Automation and Intelligent Manufacturing '07*, Las Vegas, NV. 2007.

[16] Krus, D.A. and K. Grantham Lough. "Function-based failure propagation for conceptual design." *Artificial Intelligence for Engineering Design, Analysis and Manufacturing,* 23, pg 409-426. Cambridge University Press, 2009.

[17] Collins, J. A., Hagan, B. T. and Bratt, H. M., 1976, "The Failure-Experience Matrix: A Useful Design Tool," *Journal of Engineering for Industry*, 98 (3): 1074-1079.

[18] Collins, J. A., *Failure of Materials in Mechanical Design*, John Wiley & Sons, New York, NY U.S.A. 1993.

[19] Uder, S. J., Stone, & Tumer. "Failure Analysis in Subsystem Design for Space Missions." *Proc. of ASME Design Engineering Technical Conference '04.* Salt Lake City, 2004.

[20] Tumer, I. Y., R. B. Stone, D. G. Bell. "Requirements for a failure mode taxonomy for use in conceptual design." *International Conference on Engineering Design*, Paper No. 1612, Stockholm, Sweden. August 2003.

[21] Coit, D. W. & A. Smith. "Penalty Guided Genetic Search for Reliability Design Optimization." *Computers and Industrial Engineering*, Vol. 30, Num 4. 1996.

[22] Coit, D. W. "System Reliability Prediction Prioritization Strategy." *Proc. Annual Reliability and Maintainability Symposium*. IEEE, 2000.

[23] Meeker, W. Q. & L. A. Escobar. *Statistical Methods for Reliability Data*. John Wiley & Sons, Inc. New York, 1998.

[24] Metropolis, N. & S. Ulam. "The Monte Carlo Method." *Journal of the American Statistical Association*, Vol. 44, No. 247. pp. 335-341. Sep 1949.

[25] Kumamto, H. & E. J. Henley, *Probabilistic Risk Assessment and Management for Engineers and Scientists*. 2nd ed, ed. J.B. Anderson. 1996, Ney York: IEEE Press.

[26] Bannantine, Julie, Jess Comer, and James Handrock. *Fundamentals of Metal Fatigue Analysis*. Prentice Hall. 1990.

[27] Collins, J. A. *Failure of Materials in Mechanical Design: Analysis, Prediction, & Prevention.* John Wiley & Sons, New York. 1981.

[28] Azizi, Navid, and Peter Couras. *Gate Oxide Breakdown*. December 2, 2003.

[29] Agarwala, R.P. *Radiation Damage in Some Refractory Metals*. Trans Tech Publication, Ltd, Switzerland. 2005.

[30] eFatigue. eFatigue Material Property Finder, eFatigue LLC, 18 May 2010. <https://efatigue.com/probabilistic/strainlife/materials/>.

[31] Park, Jongin, et al. *Development of Accelerated Life Tests for Lithium Battery.* Proceedings of International Workshop on Reliability and Its Applications, 247-253. 2003.

[32] Weaver, Robert D., et al. Some reliability considerations of various networks of sodium/sulfur batteries. Proceedings of IECEC-89, Washington, DC, Aug. 6-11, 1989.

[33] Simons, Stephen N., Bryan C. Willhoite and Gert Van Ommering. *Energy Storage and thermal control system design status.* Proceedings of IECEC-89, Washington, DC, Aug. 6-11, 1989.

[34] Beer, Ferdinand, Russell Johnston, and John Dewolf. *Mechanics of Materials*, 3rd Ed. McGraw Hill, Coston. 2001.

[35] *ASM Handbook*, 10th Ed. Vol. 13, 13a, 13b, 13c. 1990.

[36] Graig, Benjamin D. *Material Failure Modes, Pt 2*. Material EASE AMPTIAC 30.

[37] Shigley, Joseph, Charles Mischke, and Richard Budynas. *Mechanical Engineering Design*, 7th Ed. McGraw Hill, Boston. 2004.

[38] Anderson, T.L. *Fracture Mechanics*, 3rd Ed. Taylor & Francis, Boca Raton. 2005.

[39] Lewis, R. *A modeling Technique for Predicting Compound Impact Wear*. Wear, Vol 262. Issues 11-12, pg 1516-1521. 10 May 2007.

[40] Tipler, Paul. *Physics for Scientists and Engineers*, 4th Ed. W.H. Freeman and Company, New York. 1999.

[41] *Quality and Reliability Handbook*. Sanyo Semiconductor Co, Ltd.

[42] Black, J.R. *Metallization Failures In Integrated Circuits*, RADC Technical Report, Vol. TR-68-243, October 1968.

[43] Zocholl, Stanley. *On the Protection of Thermal Processes*. April 2005.

PAPER II

TOWARDS FAILURE FREE DESIGN: AN ANALYSIS OF RISK MITIGATION COMMUNICATION

Daniel Krus

Department of Mechanical Engineering

Missouri University of Science and Technology

Katie Grantham

Department of Engineering Management and Systems

Engineering

Missouri University of Science and Technology

ABSTRACT

In order to ensure that risk mitigation strategies are properly communicated to and understood by those who would use them in future designs, a common language of risk mitigation should exist. This paper focuses on a set of elements for describing risk mitigation strategies based on a linguistic analysis of the information such strategies must communicate to the design team. Sample strategies are then decomposed into these attributes and evaluated using the Gricean cooperation principle, relevance theory, and functional analysis theories from the pragmatics sub-field of linguistics. Using the deficiencies found from this analysis, a format for risk mitigation strategies using the six risk mitigation attributes is formulated.

Keywords: risk mitigation, mitigation strategies, linguistic analysis

1 INTRODUCTION

In industry, planning for potential failures is an important part of designing a product. This failure mitigation takes the potential failures in a product, and creates measures to mitigate those risks, plan for any emergencies that may occur due to their failure, and control any residual risk that remains (Wang and Roush 2000). The risk mitigation strategies that are created are important, and must convey their information so that it is not just understood by the engineers who develop them, but that there is no confusion as to who will execute them and how they are to be executed. In particular, the mitigation strategies must clearly state the changes the strategy will make, and the effects those changes will have on the product, in addition to the failure being mitigated.

When trying to communicate a mitigation strategy, proper communication is important. For example, if a designer requires a change of the shaft diameter, the machinist needs to know what the new shaft diameter is, and in what dimensions. In the other direction, if a machinist needs to make a change to manufacture the product, those responsible need to know what effect that change will have on the risk of the design. If there is poor communication, the risk or its mitigation can be misunderstood and not dealt with efficiently, or wrongly, such as in the case of the Mars Climate Orbiter (NASA, 1999). Further, if two separate groups are trying to share strategies, they need to understand each other's terms if either wishes to use the other's strategies. At the very least, additional time is required to process the strategy into a form it can be used. If one wished to create a repository of such strategies, it would be next to impossible to search without proper terms and a language to organize and sort the database.

Currently, there is no common language for failure mitigation or its strategies known by the authors. As failure mitigation is currently handled within a design group and primarily based on that group's expert opinion, definitions of what is required for a risk mitigation strategy can very greatly between two different designers. Further, unless the terms, such as the environmental or design changes, are understood between the design team creating the plan and the manufacturer or customer that will implement the plan, there can be confusion between the different groups. Finally, without a common language, it becomes difficult to understand strategies used in the past, and determine if they are fit to use on current risks.

In order to promote greater communication of risk mitigation strategies, as well as allow them to be rated in terms of quality, this work seeks to better understand what must be communicated in a risk mitigation strategy, as well as providing a means for evaluating current mitigation strategies based on what must be communicated. It will begin with the identification of the important elements in a strategy. Using these elements, a linguistic analysis will be performed on several risk mitigation strategies to determine how well they communicate information. These elements will give a means to evaluate how well a risk mitigation strategy communicates its information to others. Finally, these elements and evaluations will allow for links to be formed between failure analysis methods such as the Risk in Early Design method (RED) (Lough 2007) and failure mitigation, as well as show how mitigation strategies can be improved.

2 BACKGROUND

2.1 Risk Mitigation

Risk mitigation is the process of removing, reducing, or transferring the risk in a system or product, as well as planning for unavoidable risks (Wang and Roush 2000). Risk mitigation develops risk mitigation strategies, which are then implemented on the product.

There are several tools to aid in the construction of these strategies. Cost-benefit analysis compares different choices based on their estimated or measured costs and benefits (Nas 1996). The costs and benefits of a given choice are quantified, usually into a monetary value. These values are then compared, and the best overall choice is selected based on those quantified costs and benefits. This allows different strategies to be rated against each other and the most fit strategy to be put into place for a given risk.

Failure Modes and Effects Analysis (FMEA), while not a risk mitigation tool itself, often requires the use of risk mitigation during analysis. FMEA collects and evaluates potential failures in a product by recording the occurrence, severity, and detection values. In addition to the ratings, it also requires an action item to handle the failure. Some versions also require recording a new occurrence, severity, and detection after implementing the action item (Department of Defense, 1949).

Adaptive management creates a strategy or strategies and tests them by applying them to the situation, and adapting the strategy as time passes (Brody et al. 2009). A successful strategy remains in place, while less successful strategies are changed to better answer the risk, or are replaced with entirely new strategies. Adaptive management is a

real time risk mitigation tool, useful for the changing of risk mitigation strategies over the course of their lives, but less useful on a system still in the early part of design.

The risk-based distributed allocation methodology (R-DRAM) focuses on the costs and benefits of risk mitigation across shareholders in a project, and determines the best spread of those resources to get the most benefit to the least cost with the lowest overall variance (Qiu et al. 2007).

Similarly, the antiterrorism risk-based decision aid (ARDA) determines the best means to mitigate potential terrorist attacks based on their cost-benefit analysis, by determining what resources are at risk and by what means. These are then evaluated based on the consequences and likelihood of the risk, and the costs saved by implementing the mitigation. These are then ranked to give the best mitigations for a given set of risks (Dillon et al. 2009).

While these tools exist to help designers determine the best ways to mitigate risks, they still rely on expert knowledge to generate the strategies, and have no consistent language between them. Two different groups attempting to mitigate the same set of risks may come up with different mitigation strategies, with different costs and benefits and effects on a product or system. In order to properly communicate these risk mitigation strategies, there needs to be some common language.

2.2 Risk Communication Pragmatics

The concept of using linguistic analysis to understand risk and how it is communicated is not new. Grantham Lough et al (2009) used linguistic analysis to examine risk elements, which are phrases that describe the failure, its scenario, causes,

and effects, as well as any issues or concerns related to that failure (Wie et al. 2005). Linguistic analysis was used to break these risk elements into attributes, such as Performance Parameters, Design Parameters, and Noise Parameters. These attributes were then used to evaluate 117 risk elements based on three theories of pragmatics, and then suggest a common method to report risk elements to capture as much information as possible (Grantham Lough et al. 2009).

Similar to the analysis of risk elements performed by Grantham Lough et al, when communicating risk mitigation strategies, the context of the strategy is important. This context refers to the details surrounding the strategy and how it applies to a product of system, such as the risk it is meant to mitigate or a change in a shaft diameter being made to the product. This focus on the context of a risk mitigation strategy lends itself to the sub-field of linguistics termed pragmatics, which focuses entirely on how statements are used to communicate and how they relate to the context of the discussion (Barsalou 1992, Wilson and Keil 1999). An analysis based on the pragmatics of communicating risk mitigation is appropriate as the focus of this work is on what is being communicated and how that communication can be improved.

This analysis will be based on three theories of pragmatics. Each of these theories gives certain conditions, and state that communication is successful when those conditions are met (Green 1996). These theories will then be applied to the communication of risk mitigation.

2.2.1 Gricean Cooperation Principle. The Gricean cooperation principle consists of four maxims that, unless the goal of the communication is to misinform,

should be followed for communication to be effective (Barsalou 1992). These four maxims describe cooperative interaction:

Quantity: *A statement should be as informative as possible, but not more than necessary*

Relevance: *A statement should be relevant to the goals of the conversation*

Quality: *A statement should be true and be based on sound evidence*

Manner: *A statement should be clear, unambiguous, and orderly*

As a risk mitigation strategy is communicating correct information and not trying to hide the information, it should follow all four maxims.

2.2.2 Functional Approach. The functional approach states that communication serves seven different functions (Green 1996). The instrumental function deals with satisfying needs, such as acquiring of goods and services. The regulatory function deals with the control of others, such as giving commands and orders to another person. The interactional function establishes interactions with others, such as giving a greeting or calling a person's name. The personal function applies to expressing awareness of one's self, such as a person's desires, feelings, and interests. The heuristic function is used to find out about the world, such as asking why the sky is blue. The imaginative function creates an imaginary environment, such as writing a fictional story. Finally, the informative function is used to convey information about the world, which must be done with language.

In the case of risk mitigation, the regulatory and informative functions are the most important. A risk mitigation strategy is giving a command or order to change a

product in some fashion that should be understood and followed. In addition, the strategy has to relate important information to those who need to enact it.

2.2.3 Relevance Theory. Relevance theory operates on two principles: that a statement creates positive cognitive effects and requires less processing effort (Wilson and Keil 1999).

If all other things are held equal, a statement that creates greater positive cognitive effects will be more relevant to the conversation. These cognitive effects can take the form of supporting existing information, contradicting existing assumptions, or interacting with existing information to create new conclusions. The more of these positive effects the statement has, the more relevant it is.

Similarly, if everything else is equal, then the statement with the lowest processing effort is the most relevant. This processing effort is the amount of effort that must be put into interpreting and understanding the statement, such as recalling relevant memory and inferences that must be created (Green 1996).

This implies that the information in a risk mitigation strategy should increase the understanding of the product and how the risk can be eliminated, and should be clear enough to understand with minimal effort.

3 RISK MITIGATION STRATEGY ATTRIBUTES

The dependence on expert opinion and knowledge for risk mitigation can create very informal risk mitigation strategies that are often difficult to understand or

implement. As the beginning of this research approach, risk mitigation strategies are investigated, and a set of risk mitigation attributes is developed.

3.1 Risk Mitigation Strategy Examples

Presented here are some of the risk mitigation strategies used in the analysis. These risk mitigation strategies are taken from the engine nacelle data for the Boeing 777 aircraft, as well as published general and case specific strategies from *Solutions to Equipment Failure* (Timmons 1999), and came in the form of a series of tables or a written description of the mitigation strategy. These data were selected both because of the different types of solutions that were generated, as well as its accessibility. These represent the different mitigation strategies, both general and taken from case studies, which were broken down into risk attributes. A complete listing of all mitigation strategies included in this analysis are shown in Appendix B.

Example Strategy #1: *Corrosion protection of aluminum aircraft parts by coating with pure aluminum.*

This strategy identifies a general failure mode, corrosion, and gives a design change by coating an aluminum alloy with pure aluminum to resist that failure mode. However, it does not discuss whether this will reduce likelihood or consequence of failure.

Example Strategy #2: *Reduce pitting corrosion by heat treatment of component to softer condition.*

Again, this strategy identifies the failure mode and the design parameters affected: the hardness of the material. Again, no mention of how this strategy reduces the risk of the failure is given.

Example Strategy # 3: *Reaming bolt holes and using interference-fit bushings.*

In this example, no mention of a failure mode is given, just a design change and no other mention of the design parameters affected or the affect on the risk of this failure mode.

Example Strategy # 4: *Better care in assembly to prevent dents and stress concentrations.*

This example gives an environmental change (the environment the product is being assembled in) but no information on which failure modes this is intended to mitigate, but does give a parameter that is affected, stress concentrations.

3.2 Risk Mitigation Strategy Attributes

Risk mitigation strategies share much in common with the risk elements they mitigate. In order to develop a set of risk mitigation attributes, several definitions from Glutch (1994), Kaplan and Gerrick (1981), Grantham et al. (2009), and Krus and Grantham (2010) were used to map the risk elements to corresponding risk mitigation attributes.

Kaplan and Gerrick describe risk in the three terms of the scenario of the failure, the likelihood of the failure, and its consequences (1981). For risk mitigation, comparable attributes would be the failure mode mitigated and the design parameters it corresponds to, which is the scenario the mitigation strategy applies to. The likelihood and consequence values correspond to the reductions in the likelihood and consequence in the product from applying the mitigation strategy.

Similarly, Glutch defines risk in terms of the context, probability of failure, and the impact of the failure (1994). The context surrounding the strategy links to the failure

mode and the design parameters, which describe the mitigation strategy. As above, probability maps to the change in the likelihood of risk, and the impact maps to a change in the consequence of failure.

Grantham et al. define a risk element with performance (a measurable indicator of the system's performance), design (parameters of the system that are defined by the design), and noise parameters (parameters that are beyond the control of the designer), as well as the failure mode and failure scenario (2009). The performance parameter can be mapped to the likelihood and consequence changes in a product, as those show the improvement in performance. The design parameters represent those parameters that a designer can change, and links to the changes a mitigation strategy call for. The noise parameters are parameters beyond the control of the designer, and can be equated to the environmental changes called for by a mitigation strategy. The failure mode is the same in both cases, being the failure mode that happens and the strategy intends to mitigate. Finally the failure scenario corresponds to the mitigation used in the strategy to limit the risk.

Krus and Grantham (2010) recommended looking at risk mitigation strategies by relating them to the parameters of the failure mode models. These design and situational parameters in the failure mode models related to the design and environmental changes that could be made to the system or its surroundings.

By mapping these four approaches to codifying risk elements, six risk mitigation elements can be derived. The first of those is the Failure Mode to be mitigated. This attribute covers the exact failure the mitigation strategy is to affect, such as high cycle fatigue, galling, or undercurrent. This attribute is important for understanding when a

strategy can be applied, and is a direct mapping of the failure mode discussed by Grantham et al.

The next parameter is Design Change. This is a change made to the design of a product with the intent of reducing a risk, and can be viewed as the product being physically different after the change is applied. These changes are the aspects of a design that the designer has a direct control over, such as a change in the shaft diameter, or the selection of a high strength steel to manufacture that same shaft. This is one of two attributes that tracks the parameters a mitigation strategy affects, and map to the scenario or context of the strategy.

Similarly, an Environment Change is a change made to the environment the product operates in or how it is manufactured, with the intent of reducing a risk. These are changes made to the environment that affect the product indirectly and do not physically change the design of the product, such as an operator instruction not to overpressure a tank, or overload a bridge. Like the Design change, this attribute tracks the parameters a mitigation strategy affects, and is a mapping of the context or scenario.

Next, the Likelihood Change is a change in the likelihood of the risk brought on by a mitigation strategy. These are the estimated or measured changes in the likelihood of a failure mode occurring because of the mitigation strategy. An example of this attribute would be a reduction in the likelihood of failure by 2% due to the change in the shaft diameter. This attribute is the first of two that tracks the performance of a mitigation strategy, and shows the reduction in risk that such a strategy seeks to accomplish. This maps to the consequence, impact, or performance of a risk element.

Like the Likelihood Change, Consequence Change is a change in the consequences of a risk brought on by a mitigation strategy. These are the estimated or measured changes in the consequence of a failure mode occurring because of the mitigation strategy. This attribute, too, tracks the performance of the mitigation strategy and demonstrates the reduction in risk. As Likelihood Change, this maps to the consequence, impact, or performance of a risk element.

The final attribute is the Design Parameter. This attribute covers the exact parameters that relate to the mitigation strategy and failure mode. These parameters are such things as the geometry of the product, its material fatigue properties, or its resistance to corrosion. This identifies the exact parameters that relate the failure mode and the mitigation strategy to the product. A strategy can have design parameters, and no design change. The design parameters are the physical aspects of the design that are affected by the strategy and failure mode. This attribute maps to the design and noise parameters, as well as the context or scenario.

Shown below in Table 1 is a summary of the six risk mitigation attributes, and where they were derived from, and why they are important to the communication of risk mitigation strategies.

Table 1. Risk Mitigation Strategy Attributes

Attributes	Definition	Example	Reference	Why?
Failure Mode (F)	The failure mode the mitigation strategy is meant to mitigate.	High Cycle Fatigue, Galling, Undercurrent	Grantham, et al, 2009; Kaplan and Garrick, 1981; Glutch, 1994	The exact failure mitigated is important. This also describes the situation the mitigation strategy is applicable. Tracks what strategy is supposed to mitigate.
Design Change (D)	A change that is made to the design of the product, with the intent of reducing the risk.	A change in the shaft diameter.	Krus and Grantham, 2009; Grantham, et al, 2009	Many mitigation strategies recommend changing the design of the product to achieve the desired goal. Variables from failure mode equations can be classified as design variables. Tracks the parameters the strategy affects.
Environment Change (E)	A change that is made to the environment the product operates in, with the intent of reducing the risk.	An operator instruction to not load the product more and 500 lbs.	Krus and Grantham, 2009; Grantham, et al, 2009	Many mitigation strategies recommend changing the way or how a product is used to achieve the desired goal. Variables from failure mode equations can be classified as environmental variables, that pertain to the environment the product works in. Tracks parameters the strategy affects.
Likelihood Change (L)	A change in the likelihood of the failure mode caused by the mitigation strategy.	Develop plan for concept design reduces Likelihood by 2%.	Boeing 777 Engine Nacelle Design Data; Grantham, et al, 2009; Glutch1994; Kaplan and Garrick, 1981	One of the major components of risk analysis is the likelihood of the failure. The likelihood reduction should be important to the mitigation strategy. Tracks the performance of the strategy. Boeing uses percent change in likelihood from a given change.
Consequence Change (C)	A change in the consequence of the failure mode caused by the mitigation strategy	Perform careful material selection reduces Consequence by 4%.	Boeing 777 Engine Nacelle Design Data; Grantham, et al, 2009; Glutch1994; Kaplan and Garrick, 1981	One of the major components of risk analysis is the consequence of the failure. The consequence reduction should be important to the mitigation strategy. Tracks the performance of the strategy. Boeing uses percent change in consequence for a given change.
Design Parameters (DP)	The parameters of the design that are affected by the failure mode.	The shaft diameter, the material properties of the shaft, the function of the component.	Grantham, et al, 2009; Kaplan and Garrick, 1981; Glutch, 1994	These parameters are the parts of the design that correspond to the failure mode, and that the Design Changes can impact. Tracks where changes can be made in the product.

4 PRAGMATICS ANALYSIS OF RISK MITIGATION STRATEGIES

In carrying out this analysis, two assumptions must be made. First, it must be assumed that the elicitation, discussion, and consideration of risk mitigation are all subject to the principles of pragmatics and that risk mitigation should be addressed in a manner consistent with these principles. The second assumption is that the risk mitigation attributes described in Section 3.2 are one potential valid solution toward specifying the context of risk mitigation, which is important to the discussion of risk mitigation. This second assumption demonstrates that this is only one potential way of looking at evaluating risk mitigation strategies, and there may be others. That is, these attributes are just one way to define mitigation strategies; there may be other, different, yet still valid sets of attributes that can define mitigation strategies.

What follows is the procedure and the pragmatic specific analyses that will be applied to the collected risk mitigation strategies.

4.1 Pragmatics Analysis Procedure

The sample risk mitigation strategies are decomposed into the risk mitigation attributes expressed above. These attributes will then be used to analyze the sample strategies using the three pragmatics approaches discussed in Section 2.2: the Gricean Cooperation Principle, Functional Analysis, and Relevance theory. This approach can be broken down into four steps:

Step 1: Relate each theory to the risk mitigation attributes. Each maxim is written in terms of general conversation, and needs to be transformed into one that deals specifically with risk mitigation. For this step, each mitigation strategy is broken down into the risk mitigation attributes by a group of experts (in the case of this paper, the authors, both of whom have a background in risk analysis and risk mitigation). This corresponds to the mappings column in Table 2, which show which attributes are related to given questions.

Step 2: Derive specific questions to relate the linguistic theories to the risk mitigation strategies. The maxims will be broken down into questions pertaining to the attributes of a given risk mitigation strategy. These questions will be used to evaluate if the strategy meets a particular maxim. These relate to the Question and Property Specific Question columns in Table 2.

Step 3: Derive logical relationships between the attributes and the maxims to determine if the criteria are satisfied. The relationship between the attributes and the questions pertaining to the maxims will be transformed into logical relations. A true value from the relation will mean that the attribute validates

that criterion. These correspond to the Logical Relationship column of Table 2.

Step 4: Evaluate each mitigation strategy. The mitigation strategies will then be evaluated using the attributes they were broken down into and the logical relations developed in step 3.

The specific questions for the given linguistic theories are presented in the following sections.

4.1.1 Gricean Cooperation Principle. For the maxim of quantity, the mitigation strategy should be informative and have only what is required. This translates to two questions: is the strategy informative, and does it only have what is required, as shown in Table 2. In terms of the mitigation attributes, an informative strategy should present the failure mode mitigated, the design or environment change, and the design parameters affected, which is the minimum amount of information needed to perform and evaluate the strategy. The second question states that the strategy should only deal with this failure mode(s) and not others; that is, this strategy should only relate to this failure and not have information about others. To answer this, the strategy should contain the failure mode(s) and design parameters specific to that strategy and contain no extraneous information; that is, design parameters or failure modes that don't relate to the mitigation strategy. The logical relationships that follow from these property specific questions are shown in the last column of Table 2. If these relations are both true, then the quantity maxim is true.

For relevance, the strategy should pertain to the failure mode and show that it will have an effect. In the terms of risk mitigation, the strategy should contain a failure mode it affects, a change in the likelihood or consequence of the failure. Containing the failure mode demonstrates the strategy being important to the topic, and the likelihood or consequence changes denote that this strategy will mitigate the risk, and have an effect on the failure mode. If the strategy contains at least one of those attributes, it is relevant to the conversation.

The quality maxim should address if the strategy can affect the risk and the product itself. These break down into three conditions. If the strategy contains a likelihood or consequence change, then the strategy will have an effect on the risk. Similarly, if it has a design or environment change, as well as corresponding design parameters, the strategy will affect the product. Finally, those design parameters must relate to the failure mode being mitigated in order to truly affect the risk. If all three conditions are met, then the quality maxim is met.

Finally, for the maxim of manner, the strategy should be clear and unambiguous. For clarity, the strategy must contain at least the failure mode to be mitigated and the design parameters that are affected by the changes. These are the items that must be present to understand what the strategy mitigates and how it does it. For the strategy to be unambiguous, it should report the likelihood or consequence change, the design or environment change, and the design parameters affected. These show what the mitigation strategy affects. If these are met, then the maxim of manner is satisfied.

4.1.2 Functional Analysis. For the regulatory function, the strategy should designate where the changes are to be made and give clear orders to follow. For this to

be understood, the changes to the design or environment and the design parameters must relate to the failure mode. Likewise, to prevent confusions and give clear orders, the design and environment changes must relate correctly to the design parameters. If both of these conditions are met, the strategy performs the regulatory function.

To answer the informative function, the strategy should give as much information as possible about the risk and how it will be mitigated. This can be accomplished if the strategy contains the failure mode to be mitigated, the design or environment changes that should be made to answer that failure mode, the likelihood or consequence changes that result from the mitigation, and the design parameters that will be affected. If all four of those attributes are accounted for, the strategy completes the informative function.

4.1.3 Relevance Theory. The positive cognitive effects should be answered by the strategy including as much information as is possible. To answer this category, as many of the possible attributes as possible should be included in the strategy. As more attributes are included, more conclusions about the strategy can be reached, and the exact information becomes clearer. The more of these elements reported, the better the strategy meets this criterion. This criterion is independent of the actual word length of the strategy, and only concerns the attributes present in the strategy itself.

From the processing effort portion, the strategy needs to have at least enough data to mitigate the risk. To do this, the strategy needs to meet the minimum amount of information about the mitigation. To meet this criterion, then, more than half of the potential attributes should be present in a strategy.

Shown in Table 2 is a summary of the criteria derived from these three approaches, which attributes correspond to each criteria, the exact question to be

answered, and the appropriate logical relationship posed by the question. These will be used to perform the pragmatics analysis on the collected risk mitigation strategies.

Table 2. Risk Mitigation Strategy Categories

Maxim	Description	Question	Mappings	Question	Property Specific Question	Logical Relationship
Gricean						
Quantity	Utterances should be as informative as possible but not more informative than required.	Is the strategy informative?	F, D, E, DP	Qn1	Does the mitigation strategy contain F, D or E, and DP?	IF(F and (D or E) and DP) THEN Qn1 True
		Does it only relate to this specific failure mode?	F, DP	Qn2	Does the specific DP and F relate to this particular mitigation strategy?	IF(F and DP are specific to the strategy) THEN Qn2 True
Relevance	Utterances should be relevant to the goals of the current conversation.	Does the strategy communicate the likelihood or consequence reduction of the failure mode?	F, L, C	R1	Does the strategy contain F, and L, or C?	IF(F and (L or C)) THEN R1 True
Quality	Utterances should be true and based on sound evidence.	Can the strategy reduce the risk?	L, C	Q1	Does the strategy contain L or C?	IF(L or C) THEN Q1 True
		Can the changes be made to the product or its environment?	D, E, DP	Q2	Does the strategy contain D and DP, or E?	IF((D and DP) or E) THEN Q2 True
Manner	Utterances should be clear, unambiguous, and orderly.	Is the strategy clear?	F, DP	M1	Does the strategy contain F and DP?	IF(F and DP) THEN M1 True
		Is the strategy unambiguous?	L, C, D, E, DP	M2	Does the strategy contain L or C, D or E, and DP?	IF((D or E) and (L or C) and DP) THEN M2 True
Functional						
Regulatory	Communicative means are used to control the behavior of others.	where the changes are to be made?	D, E, DP	Rg1	Does the strategy contain D and DP, or E?	IF((D and DP) or E) THEN Rg1 True
		Does the strategy give clear orders to follow?	D, E, DP	Rg2	Does the strategy contain D and DP, or E?	IF((D and DP) or E) THEN Rg2 True
Informative	Language is used to convey information to other people about things not visible in the immediate environment.	Does the strategy convey information about the mitigation?	F, D, E, L, C, DP	I1	Does the strategy contain F, D or E, L or C, and DP?	IF(F and (D or E) and (L or C) and DP) THEN I1 True
Relevance						
Positive Cognitive Effect	Other things being equal, the greater the positive cognitive effects achieved by processing an input, the greater the relevance of the input to the individual.	How well does the strategy address the mitigation of the product?	F, D, E, L, C, DP	C1	How many attributes does the strategy contain?	COUNT(F, D, E, L, C, DP)
Processing Effort	Other things being equal, the greater the processing effort expanded, the lower the relevance of the input to the individual at that time.	Does the strategy provide enough data to clearly mitigate the risk?	F, D, E, L, C, DP	P1	Does the strategy contain at least 4 of the six attributes?	IF(COUNT(F, D, E, L, C, DP)>=4) THEN P1 True

4.1.4 Example of Mitigation Strategy Evaluation. In this section, the step-by-step evaluation is shown for one of the mitigation strategies, "Better processing controls during etching and plating procedures to reduce potential pits chances of affecting material properties." First, the individual parameters contained within the strategy must be identified. When this strategy was collected from (Timmons, 1999), the strategy was cited as a solution for the failure mode fatigue, fulfilling the Failure Mode attribute. As the change would affect the manufacturing process, but not the design, it was identified as an Environment Change. However, no Design Change was reported, as no overall change was made to the design of the product. In the literature, no information was given regarding whether this change would affect the likelihood or consequence of change. However, the design parameters of material fatigue properties and the crack size were listed. So, for this mitigation strategy, a Failure Mode, Environment Change, and Design Parameters were identified, while the other three attributes were not.

After the attributes were collected, they were evaluated against the logical relations as shown in Table 2. For the Gricean Cooperation Principle, there are four maxims divided into seven relations. The first of those is Quantity, with two relations. The first asks if there is an adequate quantity of information, and contains a Failure Mode, either a Design or Environment Change, and Design Parameters. "Better processing controls" has three of these parameters (with the Environment Change fulfilling the OR condition), and is true for this first question. The second asks if the if the Failure Mode and Design Parameters are specific to this strategy. The Design Parameters relate to the Failure Mode, and are specific to this strategy, and so the second question is true. As both are true, this strategy satisfies the Quantity Maxim.

This process can be repeated for all of the other relations. For this given strategy, Relevance is false (no Likelihood or Consequence Changes), as is Quality (Q1 is false, again due to no Likelihood of Consequence, but Q2 is true as the strategy has an environment change). Manner is similarly false (M1is true, but M2 is false). The exact same procedure is carried out for Functional Analysis, with Regulatory being true, and Informative being false. Relevance is slightly different, as the Positive Cognitive Effect is a count of the number of attributes identified, which is three in this case. This is not enough for the Processing Effort to be true.

This procedure was repeated for all fifty of the collected mitigation strategies, with the results shown in the following section.

4.2 Analysis Results

The mitigation strategies used covered two different varieties: general strategies used to combat a class of failures, and specific strategies taken from the recommended actions of case studies. Presented here are the results of the analysis, demonstrating the variable nature of these mitigation strategies.

4.2.1 Gricean Cooperation Principle. Each strategy was subjected to the logical relationships presented in Table 2. If a relationship tested true, then that portion of the maxim was satisfied. If all questions were true, then the maxim was satisfied. The results of the Gricean analysis are shown in Figure 1. This figure shows that the maxim most satisfied is quality, followed by quantity, relevance, and manner. By examining the

exact results for each portion of these maxims, a better understanding of what is missing can be acquired.

For the maxim of quantity, two questions were asked. The first asked if the strategy was informative, and checked if the strategy reported the failure mode, a design or environmental change, and the design parameters affected by the failure. 23 of the 50 examined mitigation strategies met this criterion. The second question asked if the strategy contained only the information required to mitigate that risk. This strategy required that the design parameters and the failure mode appear only in this strategy. 19 of the examined strategies met this criterion. However, only 16 of the strategies shared these two criteria and met the quantity maxim. These results are shown in Figure 2.

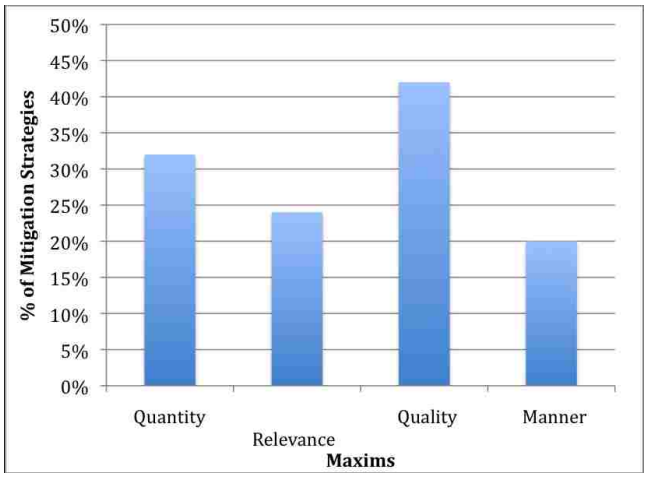


Figure 1. Gricean Mitigation Strategy Analysis

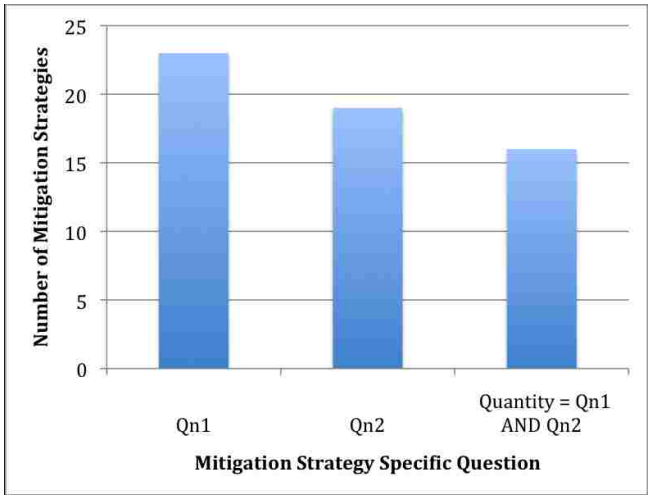


Figure 2. Gricean Mitigation Strategy Analysis – Quantity

The quality maxim also had two questions. The first question asked if the strategy could reduce the risk, and checked if there was a likelihood or consequence change reported. Over half the elements analyzed, 27, met this criterion. The second question was the most successfully met of the Gricean questions. This asked if the strategy could change the product, or its environment. 35 of the strategies met this criterion. Again, there was less overlap between these two questions, with only 21 strategies meeting both and satisfying the quality maxim. These results are shown in Figure 3.

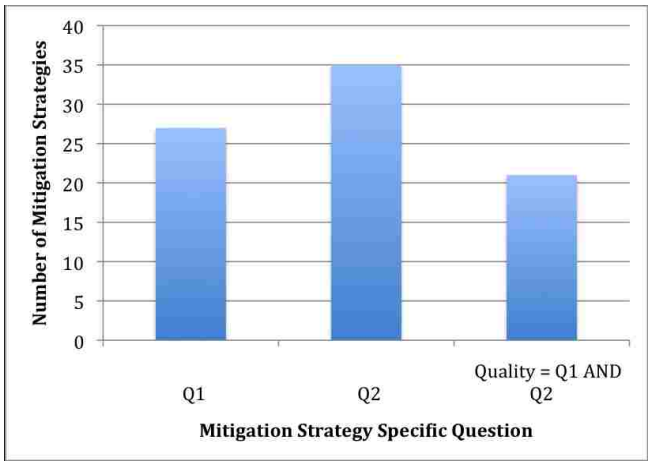


Figure 3. Gricean Mitigation Strategy Analysis – Quality

For the maxim of manner, the first question asked if the question was clear, and possessed a failure mode and the design parameters it affected. Just over half, 26, of the strategies met this. The second asked if the strategy was unambiguous, and had a change either in design or environment, the affect that change had to the likelihood or consequence, and the design parameters affected. This criterion had only 15 of the strategies meet it successfully. Much like the quality maxim, the manner maxim had only a small overlap between these two questions, with only 10 strategies shared between them. These results are shown in Figure 4.

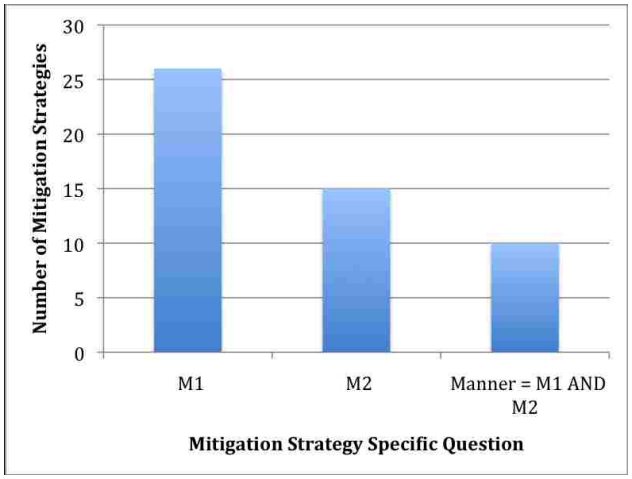


Figure 4. Gricean Mitigation Strategy Analysis – Manner

Overall, only 5 of the 50 mitigation strategies met all four maxims. Of those, 2 were from the Boeing strategies, and 3 were from the general strategies. None of the case study mitigation strategies met all four maxims. The most likely cause of this is that none of the case study samples possessed likelihood and consequence change attributes.

4.2.2 Functional Analysis. For the functional analysis portion, the mitigation strategies were subjected to the logical relationships presented into Table 2. If the relationship tested true, then the strategy met the requirements for that function. The results of the analysis are shown in Figure 5. Similar to the Gricean analysis, what follows is the individual breakdown of each of the two functions.

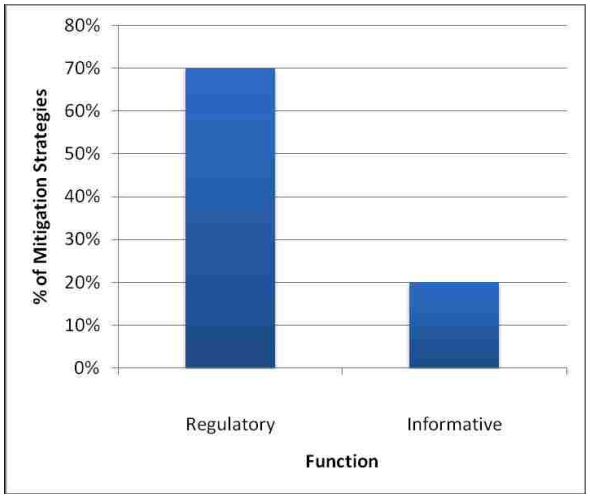


Figure 5. Functional Mitigation Strategy Analysis

For the regulatory function, there were two questions. These questions, does the mitigation strategy designate where the changes are to be made, and does it give clear orders. Both of these questions can be linked to the same logical relationship, asking is the strategy contained the Design Change and Design Parameters or the Environmental Change. For this relationship, 35 of the 50 strategies met this requirement; the most of any requirement save for the second quality question, which overlapped with this requirement.

The informative function asked that the mitigation strategy contained the failure mode, either a design or environmental change, either likelihood or consequence change, and the design parameters. 10 of the 50 strategies met this requirement. Those 10 strategies that met the informative function also met the Gricean maxims, as well as the regulatory function.

4.2.3 Relevance Theory. The relevance theory results are different from the other 2 analysis methods in that the first of the two questions performs a count of the

number of attributes that each strategy contained. This number of elements shows how much positive cognitive effect the strategy can create. Figure 6 shows the breakdown of the mitigation strategies by number of attributes shown. Most strategies contained either 2 or 3 of the attributes, while only 26% had 4 or more attributes.

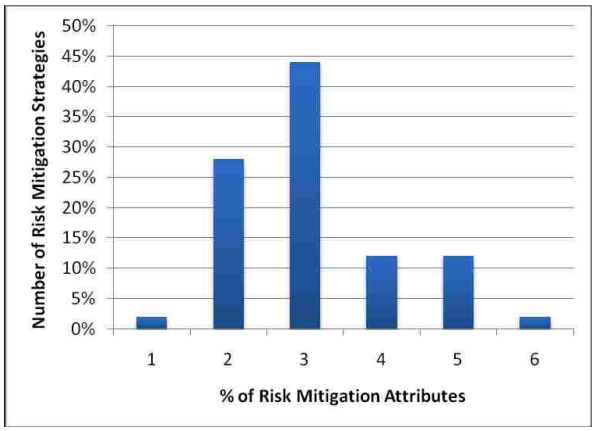


Figure 6. Relevance Mitigation Strategy Analysis – Positive Cognitive Effects

The second requirement, processing effort, required that the mitigation strategy contain at least 4 of the 6 attributes, that is, over half. As mentioned above, only 26% of the strategies met this criterion.

5 DISCUSSION OF RESULTS

Again, it is important to remember that all of the following conclusions are based on two assumptions. All of the discussion of risk mitigation and how those risk mitigation strategies are used is subject to the principles of pragmatics, and should be addressed in a manner consistent with those same principles. In addition, the presented risk mitigation attributes are one potential solution to showing the context of a risk

mitigation strategy. These two assumptions allow this analysis to show how well these mitigation strategies account for the attributes, and how well they conform to the principles of pragmatics.

The three principles of pragmatics used here each provide a different view of how the mitigation strategies are communicated. Throughout, two particular mitigation strategies, "corrosion protection of steel with cadmium" and "better manufacturing controls to remove fluids after hydrostatic testing," will be examined to show why they did or did not meet a particular criterion.

The Gricean Cooperation Principle analysis showed that the quantity maxim was met by 32% of the strategies. These strategies were informative, but only enough to deal with their mitigation strategy and no others. Strategies that met this maxim, such as "using fail-safe designs such as crack stoppers" possessed failure modes and design parameters, such as *fatigue* and *material toughness*, while those that didn't, such as "barrier coating with an insulating material" lacked one of those categories, such as the design parameters. For the two examples, "plating the steel with cadmium" contained the failure mode *corrosion*, gave the design change *plate the steel with cadmium*, and listed the *material properties* of the two materials as the design parameters affected. "Better manufacturing controls" listed the failure mode *stress corrosion* and the environment change of *increasing the controls on the product's manufacture* but did not list any design parameters affected by the failure mode or changes, causing it to not meet the criterion. For the same reason ("cadmium plating" gave design parameters and "better manufacturing controls" did not), the second quantity criteria went the same way.

“Better manufacturing controls” could have been improved by the addition of design parameters, such as what controls could be implemented.

Relevance was met by only 24% of the strategies. Only those were relevant to their failure mode, showing that there was an identified change in the likelihood or consequence of the risk; again, “fail-safe design” and “crack stopper” met this criterion, whereas “preparing a hole by cold-working and using a split sleeve” did not, as it lacked both a likelihood and consequence change. The “cadmium plating” strategy met this criterion by having both the failure mode, and explaining that such a strategy would reduce the likelihood of the failure by using a much more corrosion resistant material. “Better manufacturing controls” had a failure mode listed, but no change to either the likelihood or the consequence was given, causing it to not meet the criterion. Stating that the controls would reduce the likelihood of risk would have made the strategy pass.

42% of the strategies met the quality maxim, and thus gave true and sound information on the mitigation and the effects it would have. “Plating of high strength steels with cadmium to resist corrosion” passed this maxim, by having a design change and the design parameters the failure mode affected, while “fail-safe methods focused on multiple redundant parts” did not, because while it had a design change, it did not have design parameters. The “cadmium plating” here, as above, gave a likelihood change, showing it can reduce the risk, and by having a design change and design parameters showed that the strategy could affect the device. “Better manufacturing controls” lack a likelihood or consequence change, failing the first criterion, but meets the second criterion, by giving an environment change. Again, stating that the controls would reduce the likelihood of risk would have met this criterion.

Finally, manner only had 20% of the strategies meet its requirements of being clear, unambiguous, and orderly. "Making fail-safe designs and crack stoppers" met these criteria, as it contained all the attributes except a consequence change. In the other hand, "fail-safe methods of using redundant elements" was missing the design parameters affected, and thus did not adequately answer either question. "Cadmium plating" passed the first criterion, having both the failure mode and design parameters, while "better manufacturing controls" lack the design parameters, making it less clear as to where these controls should be used. The second criterion was also met by "cadmium plating," as it contained a design change, likelihood change, and design parameters, showing a very unambiguous strategy. As the "better manufacturing controls" lacked the design parameters and a likelihood or consequence change, it did not meet this criterion. Of all the strategies, only 10% met all four maxims, being informative, relevant, true, and clear. To have "better manufacturing controls" meet all four maxims, the likelihood change it would cause and the design parameters the failure mode and environment change affect would have to be stated.

The functional analysis results were a little different. The regulatory function had the best results of any of the criteria listed, at 70% of the mitigation strategies. This implies that for these mitigation strategies, they can communicate orders to control others well, by demonstrating where changes are to be made and giving clear orders. Virtually all of the Boeing strategies met these criteria, possessing both design parameters and design changes, or an environment change. Three quarters of the case studies, such as barrier coating with an insulating material, lacked those same design parameters or environmental changes. "Cadmium plating" and "better manufacturing controls" both

met the regulatory function, as both had either a design change and design parameters, or an environmental change.

The informative function, on the other hand, only had 20% of the strategies meet its requirements. "Coating high strength steel with cadmium" did meet this requirement, possessing a failure mode, the design parameters affected, a likelihood change, and a design change. In the case of the case studies, none had any likelihood or consequence changes stated, making it impossible for them to meet this function. This means that while these strategies can give clear orders, those orders do not successfully convey information about those orders. "Cadmium plating" passed as it contained all four asked for set of attributes (a failure mode, a design change, a likelihood change, and design parameters). "Better manufacturing controls" failed because it lacked the design parameters and the likelihood or consequence changes. Again, a likelihood change and design parameters would have caused "Better manufacturing controls" to satisfy both functional criteria.

The relevance theory results show a large number of the strategies, 74% had three or less attributes. Of the remaining, only a single strategy, "performing conformity and safety tests," had all six attributes. For these, the higher the number of attributes contained, the more positive cognitive effects can be generated and the more relevant a strategy is to the mitigation of the risk. Those same 74% did not meet the second requirement, by having half or less of the potential attributes. This means that for most of these strategies, an overly large amount of processing power is required to fill in the missing information, making them less relevant to the mitigation. "Cadmium plating" contained 4 attributes, and "better manufacturing controls" contained only 2. This lack of

information makes it difficult to reach the same kinds of conclusions as “cadmium plating,” and requires more effort to make those conclusions.

Based on these conclusions, risk mitigation strategies tend to be missing important pieces of information, most often the effects of implementing the strategies (Likelihood and Consequence Changes). Almost every single strategy had either a Design or Environment Change, as those changes are the core of the strategy. The supporting details, such as the Failure Mode they addressed or the corresponding Design Parameters, as well as the above Likelihood and Consequence changes tended to be the missing attributes.

These supporting pieces of data contain very useful information for a designer that would aid in the risk mitigation process. These attributes can lead the designer directly to mitigation strategies tailored for a given risk, and provide how effective that strategy will be. By not including those data, a designer has to determine the missing attributes on their own, and must sacrifice time to evaluate the best potential strategy. By having the missing attributes, a designer can decrease the amount of time required to evaluate and select the best possible mitigation strategy.

It should be mentioned that this is only one potential interpretation of the principles of pragmatics. A different interpretation of these principles could lead to different results, which is a possible source of error in this work. Further, each of the three theories is separate from the others, explaining why the relations for some of the maxims are the same. However, despite the three different approaches, they agree that these risk mitigation strategies clearly do not cover the attributes that are assumed to be important to the discussion of risk mitigation.

To rectify this problem, the consistency and descriptiveness of these mitigation strategies should be improved by adopting a format that requires specific attributes to be reported in a risk mitigation strategy. This format would remove inconsistencies between different groups of engineers, and allow different mitigation strategies to give the same level of information as any other. An example for the "cadmium plating" mitigation strategy is shown in Figure 7. It should be mentioned that in this format, the strategy can use either a likelihood or consequence change, or both. Similarly, it can contain either a design or environment change, or both. At a minimum, the strategy should contain at least 4 of the 6 attributes, consisting of the failure mode, design parameters, at least one design or environment change, and at least one likelihood or consequence change.

Corrosion that affects steels is mitigated by plating high strength steel with cadmium, which reduces the likelihood of failure by 5%					
(F)ailure Mode	(D)esign (P)arameter	(D)esign Change		(L)ikellihood Change	

Figure 7. Sample Risk Mitigation Strategy Format

Another potential use for this evaluation would be the creation of a knowledge base and taxonomy of mitigation strategies. With the current means of reporting and recording mitigation strategies, there is no set form to present or record data. Using the attributes presented here, mitigation strategies could be collected and evaluated using the method presented in this paper, and then sorted and categorized into a taxonomy. This taxonomy would contain the appropriate information that a product designer could use to implement these strategies in their design, based on the failure modes they have determined the product may suffer from. The Design and Environment Changes give different potential approaches to handling a given risk. Further, the inclusion of the

Likelihood and Consequence Changes would demonstrate what effects the strategy would have on the risk of those failure modes, and the Design Parameters would directly identify which aspects of the design need to be altered or maintained.

6 CONCLUSIONS AND FUTURE WORK

This paper focuses on how risk mitigation strategies are communicated. Six risk mitigation attributes were developed and an analysis of sample risk elements was performed. This analysis was based on the sub-field of linguistics called pragmatics, as pragmatics focuses on the context of the communication. The theories of Gricean Cooperation Principle, Functional Analysis, and Relevance theories were used to evaluate the attributes of the mitigation strategies, and they were found to be generally deficient. One solution to this deficiency was to improve the communication of the context of risk mitigation strategies was the use of the six mitigation attributes.

Using the mitigation attributes presented here can provide a means to store risk mitigation strategies to be used at a later date. Further, the design and environmental changes could be used along with the failure mode and design parameters to link the corresponding design parameters for a given failure mode, to help select appropriate risk mitigation strategies for a given failure mode. A knowledge base of collected mitigation strategies along with a means to link them to the important portions of a failure mode would allow a tool to help rapidly generate risk mitigation strategies for a new product.

ACKNOWLEDGMENTS

The authors would like to acknowledge the assistance of Steven Broussard, Josh Goldschmid, William Harkness, and Damon Slaughter for their assistance with collecting risk mitigation strategies.

REFERENCES

Barsalou LW, *Cognitive Psychology: An overview for Cognitive Scientists*: Lawrence Erlbaum Associates, Inc., 1992.

Brody SD*, et al.*, "Policy Learning for Flood Mitigation: AA Longitudinal Assessment of the Community Rating System in Florida," *Risk Analysis,* vol. 29, pp. 912-929, 2009.

Department of Defence, "Proceedures for performing failure mode, effects, and criticality analysis," 1949.

Dillon RL*, et al.*, "Risk-Based Decision Making for Terrorism Applications," *Risk Analysis,* vol. 29, pp. 321-335, 2009.

Gluch D, "A Construct for Describing Software Development Risks (CMU/SEI-94-TR-14)," Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA1994.

Grantham Lough K, "Detailed Risk Analysis for Failure Prevention in Conceptual Design: RED (Risk in Early Design) Based Probablistic Risk Assessments," in *International Design Engineering Technical Conference*, Las Vegas, NV, USA, 2007.

Grantham Lough K*, et al.*, "Promoting risk communication in early design through linguistic analyses " *Reserch in Engineering Design,* vol. 20, pp. 29-40, 2009.

Green DW, *Cognitive Science: An Introduction*: Blackwell Publishers Ltd, 1996.

Kaplan S and Garrick J, "On the Quantitative Definition of Risk," *Risk Analysis,* vol. 1, pp. 11-27, 1981.

Krus D and Grantham K, "A Step Toward Risk Mitigation During Conceptual Product Design: Component Selection for Risk Reduction," in *IDETC 2010*, Montreal, Qubec, 2010.

NASA, " Mars Climate Orbiter Mishap Investigation Board Phase I Report," November 10, 1999.

Timmins PF, *Solutions to Equipment Failures*. Materials Park, OH: ASM International, 1999.

Nas T, *Cost-Benefit Analysis: Theory and Application*. Thousand Oaks, CA: Sage Publications, Inc., 1996.

Qiu Y*, et al.*, "Risk-Based Resource Allocation for CollaborativeSystem Design in Distributed Environment," in *Internation Design Engineering Technical Conference*, Las Vegas, NV, USA, 2007.

Wang JX and Roush ML, *What Every Engineer Should Know About Risk Engineering and Management*. New York, NY: Marcel Dekker, Inc., 2000.

Wie MV*, et al.*, "Learning from Failures: Archiving and Designing with Failure and Risk," in *6th International Conference on Computer-Aided Industrial Design and Conceptual Design*, Delft, The Netherlands, 2005.

Wilson R and Keil F, *The MIT Encyclopedia of the Cognitive Sciences*. Cambridge, Mass: The MIT Press, 1999.

PAPER III

THE MITIGATION STRATEGY TAXONOMY: ORGANIZING AND CLASSIFYING RISK MITIGATION STRATEGIES

Daniel Krus

Department of Mechanical Engineering

Missouri University of Science and Technology

Katie Grantham, Ph.D.

Assistant Professor of Engineering Management and Systems Engineering

Missouri University of Science and Technology

ABSTRACT

The objective of this paper is to introduce the risk mitigation strategy taxonomy and demonstrate how it can link failure modes of a product to mitigation strategies, and then use those strategies along with failure mode models to refine the strategy for a given product. While models for failure modes are readily available in scientific textbooks and journals, a specific guideline for implementing product changes related to these models to reduce failures (i.e. mitigations) does not yet exist. Currently, most risk mitigation techniques rely on the expertise of the engineers on their team. The risk mitigation strategy taxonomy seeks to improve this situation by providing a set of mitigation strategies that can be easily linked to failure modes a product may experience. This taxonomy is created from an empirical collection of mitigation strategies used in industry for failure mitigation, storing the data in a consistent format that allows it to be used for future risk mitigation. By using this

taxonomy, an engineer can supplement their experience with historical mitigation data and more effectively mitigate risk.

Keywords: risk mitigation, failure analysis, conceptual design, risk linguistics

1 INTRODUCTION

The objective of this paper is to introduce a risk mitigation taxonomy that can be used during design to reduce risk of product failure. Throughout all fields of engineering, failure, especially unplanned, tends to be problematic for the product and its user. Unplanned product failures can be catastrophic, such as Toyota's many recent recalls. A simple design flaw which caused seizure and uncontrolled acceleration in the car caused 52 deaths and 32 injuries, lead to the recall of 4.5 million vehicles, and cost the company $900 million in repairs and $155 million in lost business after the recalls (CBS, 2010). Planning for failures like this from the beginning can save lives and cost such as this, and performing such an analysis during the initial stages of design costs the least and has the largest effect on the end product (Ullman, 2003).

Risk mitigation is the process of limiting risks, planning for potential emergencies, and measuring and controlling any remaining risk in the system (Wang and Roush, 2000). Risk mitigation methods involve the generation of plans that remove the risk from a product, reducing the risk by making it less likely to occur or reducing the consequence of its occurrence, or transferring the risk to a different, less vital system. For instances when the risk can't be completely removed, it also entails the design of plans for when the risk does occur, and measuring and controlling that remaining risk

(Wang and Roush, 2000). These plans, "risk mitigation strategies," tend to be created using the experience and expertise of the team that develop them, though some tools do exist to help with the task.

By performing risk and failure mitigation early, even great disasters can be reduced. In the recent earthquake and tsunami in Japan, the potential nuclear disaster at the Fukushima reactors was reduced by risk mitigation strategies in place before the earthquake took place. From the construction of the reactor itself keeping the radioactive material inside, to the use of boric acid to control reactions and keep heat down, every plan was in place before the accident. What could have easily spiralled out of control was kept in check by the defense-in-depth strategy used in the design of the reactors (World Nuclear, 2011).

As in the Fukushima case, it is desirable for mitigation plans to be in place and tested before accidents occur. In the case of the Deepwater Horizon oilrig operated by British Petroleum, many strategies that were either partially or totally ineffectual at capping the spilling oil were designed and used after the accident had occurred. From April 24 to September 21, 15 different mitigation strategies were attempted, with limited degrees of success, before finally closing the well (Guardian, 2010).

In light of disasters and failures such as these, this risk mitigation strategy taxonomy seeks to collect successful mitigation strategies and organize them into a common language. This common language, called the risk mitigation taxonomy, will enable efficient potential mitigation strategy identification for a product.

This taxonomy will classify historical failure mitigation strategies, and allow for the creation of a knowledge base of successful mitigation strategies that can be expanded

or tailored for different disciplines. This knowledge base will enable efficient mitigation of product failures during the earliest stages of the design process, when the changes can most easily be introduced at the least cost.

2 BACKGROUND

2.1 Risk Mitigation

There are only a few tools available to create risk mitigation strategies. Most, such as system reliability (Coit, 2000) evaluate strategies or analysis methods. These tools vary in their design and application, ranging from anti-terrorism (anti-terrorism risk-based decision aid, ARDA) (Dillon, et al., 2009) to weighing decisions across multiple stakeholders (risk-based distributed allocation methodology, R-DRAM) (Qiu, Ge, and Yim, 2007), both of which use a highly developed system and cost-benefit analysis to weigh the risks of a system, and determine the best strategies to employ. Others, such as adaptive management, measure and change strategies using the real world as an experiment, adapting to risks in real time rather than preparing a plan once (Brody, et al., 2009). Even some risk analysis tools, such as failure mode and effects analysis (FMEA), include risk mitigation in their execution, requiring an action plan for each identified risk (Department of Defense, 1949). For all of these tools, though, the individual strategies must be developed on their own, using expert knowledge, or require a well developed system which doesn't exist early during product design.

To promote risk mitigation it is necessary to identify a common language of mitigation strategies. This mitigation taxonomy would permit cataloging of engineering expertise and enable efficient risk mitigation.

2.2 Emerging Taxonomies

There are several languages that have recently been developed to aid with the design process and risk analysis. These languages, the functional basis, the component taxonomy, and the failure mode taxonomy, were used as guidelines for the population of the mitigation strategy taxonomy.

The functional basis, previously the function taxonomy, was brought about in an attempt to classify and standardize the terms used to conceptualize, define, or understand a product in terms of its function and purpose (Stone and Wood, 1999). Functional modeling, a process used to create models of a product's functions, suffered from a lack of precise definitions, making it difficult to reconcile functional models created by different designers. There have been several attempts to rectify this situation, dating back as far as the 1940s (Akiyama, 1991, Miles, 1972, VAI, 1993). Further, a common vocabulary is important in categorizing and archiving design knowledge. Collins et al. created a list of 105 functions to describe the mechanical functions of helicopters, and store failure data (1976). These early attempts lead the way for more organized and structured attempts. Pahl and Beitz, Hundal, Koch et al., and Kirschman and Fadel proposed breaking the functions and flows into groups or classes, using a variety of methods and strategies such as living systems theory, or a departure from the verb-object format (1988, 1990, 1994). By building off Pahl and Beitz's model to include functions and flows, a means to compare different products was developed. This functional basis was created through empirical study of over 100 products, and refined the categories set up by Pahl and Beitz to a higher degree, creating two more levels of detail (Kirschman

and Fadel, 1998, Little, Wood, and McAdams, 1997). Since its creation, the functional basis has undergone evolution and application, adding definitions for the flows (Stone, 1997), as well as applying to the creation of functional models, product similarity computations (McAdams, Stone, and Wood, 1999), design by analogy (McAdams and Wood, 2000), and functional tolerancing (McAdams and Wood, 1999). It is constructed primarily based on empirical studies, gained from studying a large number of existing products (Hirtz, et al., 2002). Even now, the basis is refined, such as the comparison to the NIST research efforts, used to find similarities and areas that the basis did not yet cover (Hirtz, et al. 2002).

The component taxonomy is a naming convention for mechanical parts (Kurtoglu, et al., 2005). This convention was developed as a way to abstract the complex components of a product down to a high level name to simplify information transfer and improve concept generation during the design process. The component taxonomy is based on the concept of a lexicon, which assumes that every artifact created has some function or purpose that it was created to fulfill (Chenhall, 1978). By using this thought, classifications for naming objects can be divided into three hierarchies: major categories, a controlled list of classification terms, and an open ended list of names. By using the controlled list of terms, a unique name can be generated for any object, similar to the Linnaean system of classifying species (Linnaei, 1937). The space breaks the mechanical objects into four categories: Functional form, components whose name is based on the function they perform, based on the functional basis; geometric shapes, components whose names are based on the geometry of the component; simple mechanics, components that are related to one of the seven simple machines (Greer, et al., 2003); and

nature, components whose names are based on their similarity to natural objects. Using these categories, 114 terms were collected from literature and technical publications, such as technical reference books, design texts, museum nomenclature, dictionaries, as well as the expertise of the creators (Greer, et al., 2003). By using the basis alongside functional modeling and tools such as the function component matrix (Strawbridge, McAdams, and Stone, 2002), a concept generator (Bryant, Stone, and McAdams, 2006) can be formed, allowing many potential designs to be easily generated from a single functional model.

The failure mode taxonomy attempts to do for the field of failure analysis what the functional and component basis did for the field of design. The failure mode taxonomy is a standardized collection of failure modes for electromechanical systems (Tumer, Stone, and Bell, 2003). It was created to add a consistent language to risk analysis and stemmed from the work of Collins, using his list of mechanical failures as the beginning (1976). From here, additional mechanical failure modes were added through empirical failure data from National Transportation Safety Bureau rotorcraft accident reports, as well as accident report from NASA's Jet Propulsion Lab (Tumer, Stone, and Roberts, 2003, Roberts, Stone, and Tumer, 2002). These were supplemented with electrical failure modes necessary to the highly automated systems used in NASA's projects. This electro-mechanical failure mode taxonomy can be used in conjunction with the functional and component basis to provide a means of detecting failure during the early portion of the design process. The Function Failure Design Method (FFDM) provided a way to link between the functions a product must perform and the failure modes they are likely to be susceptible to, by using the components that answer those functions and have failed by given failure modes as the common link (Stock, Stone, and

Tumer, 2003). Building on that, the Risk in Early Design method provided a means to rank the failure a product may experience into high, moderate, and low risks, based on the consequence and likelihood of the failure happening (Grantham Lough, 2005). In recent years, additional failure mode taxonomies have been developed for varied fields. Failure mode taxonomies have been developed for the business environment, dealing with the potential losses due to events and organization of the business itself (Patil, 2008). The chemical failure mode taxonomy deals with the risks of serious injury or damage caused by chemicals reacting in uncontrolled or unplanned ways (Ombete, 2009). Each of these taxonomies is still a work in progress, as there are failure modes that have not yet been discovered. As time progresses, these taxonomies will be populated with additional "new" failure modes, allowing these new modes to influence design of new products.

2.3 Linguistic Analysis of Risk Mitigation Strategies

Before being able to create a taxonomy for risk mitigation strategies, a linguistic analysis of available risk mitigation strategies must be performed. Based on a similar analysis of risk elements performed by Grantham Lough et al (2009), Krus and Grantham (2011) discuss one way of categorizing risk mitigation strategies based on the subfield of linguistics called pragmatics, as that field focuses on how statements are used to communicate and how they relate to the context of a discussion (Barsalou, 1992, Wilson and Kiel, 1999). The context of mitigation strategies were evaluated using three theories of pragmatics, the Gricean Cooperation Principle, the Functional Approach, and Relevance Theory. These mitigation strategies were broken into six potential attributes

and rated on the different maxims of each theory. These six attributes were the Failure Mode that the mitigation strategy was designed to fix, the Design or Environment Changes that were used to enact the fix, the Likelihood and Consequence Changes that are the effect of the strategy, and the Design Parameters that the engineer can directly affect. By determining which and how many of these six attributes a strategy contains, the number of maxims the strategy adequately meets can be determined (Krus and Grantham, 2011). This allowed for the quantification of valuable information contained in each risk mitigation strategy. This is the foundation that will be used to construct the mitigation strategy taxonomy and ensure that the language effectively communicates mitigation strategies.

2.4 Literature Summary

To meet the need for risk mitigation in engineering, a knowledge base of potential risk mitigation strategies will be collected to allow access to the collected knowledge of others and what has reduced risks for them. The knowledge base will be used to determine the risk mitigation taxonomy. This sort of taxonomy will follow in the footsteps of similar efforts, such as the functional basis (Stone and Wood, 1999), failure mode taxonomy (Kurtoglu, 2005), and the component taxonomy (Tumer, Stone, and Bell, 2003). These create a common language, which allows different designers to understand each other, reduce confusion, and better understand past applications of these terms, as well as perform mathematic operations on them. In the creation of this taxonomy, using the linguistic analysis suggested by Krus and Grantham (Krus and Grantham, 2011), it is hoped these helpful features can be brought to the field of risk mitigation.

3 THE MITIGATION STRATEGY TAXONOMY CONSTRUCTION PROCESS

This section details the terms in the mitigation strategy taxonomy and the strategies defined. Section 3.1 details how strategies were collected, classified into categories, and named. Section 3.2 presents the resultant taxonomy.

3.1 Mitigation Data Collection

The risk mitigation strategy taxonomy was created from an empirical collection of strategies from corporate data, engineering textbooks, and case studies. These sources contained failure case studies with detailed accounts of how a specific component or product failed, and recommendations on how to prevent such failures from occurring in the future. A total of 325 risk mitigation case studies were studied during the creation of the taxonomy. The ASM International's Handbook of Case Histories in Failure Analysis Volume 2 accounts for 168 of the strategies (Esakul, 1993), while Learning from Design Failures provided another 95 (Hatamura, 2009). A case study from NASA's redesign of the space shuttle's fuel tank was able to provide data for 22 mitigation strategies (Miller, 2011). Last but not least, corporate data from two companies was drawn upon to generate 40 of the strategies. Please note that it is the goal of the authors to continue investigating risk mitigation case studies to analyze and continuously improve both the taxonomy and knowledge base.

3.2 Mitigation Data Analysis

Mitigation techniques were collected and processed based on the six risk mitigation attributes identified by Krus and Grantham (2011), dividing the strategies into

a description, a failure mode, design parameters, environment and design changes, and likelihood and consequence changes. If information, such as the risk likelihood or risk consequence change due to employing the risk mitigation strategy was missing from a report under study, the analysts used their engineering experience to evaluate whether the strategy would have an affect on the consequence or likelihood of the risk.

3.2.1 Classifying Risk Mitigation Strategies. The risk mitigation strategies from the case studies analyzed were broken down into three basic categories, based on Wang and Roush's definition of how strategies affect risk: by making a change to reduce or remove the risk, by measuring or controlling the remaining risk, or by planning for a potential failure (2000). These categories can be further divided by whether the strategy affects a design or environment parameter. Of the 325 case studies, 152 made changes to reduce or remove risk; 108 were determined to be design changes, and 44 were environment changes. The remaining 173 strategies were either one of the other two categories, measuring and controlling a risk or planning for when the risk occurred, had no identifiable failure mode, or were a part of the design process, such as building a prototype. This categorization scheme was selected first due to similar environment and design parameters existing in failure mode models (Krus and Grantham 2010).

For this initial version of the taxonomy, only the strategies that make a change to reduce or remove a risk were focused on, leaving the other two categories for future work and additional strategies. These strategies were divided into Design changes and Environment changes, based on the parameter they affected. These parameters are taken from failure mode models, such as the stress life method and strain life method for

modeling fatigue. These models can be broken down into design parameters and environment parameters, based on whether or not the engineer has direct control over the parameter. Design changes are populated with strategies that change aspects of the design that the engineer has direct control over, such as "Shape Part" or "Convert Material," as the geometry of a part and the material it is made out of can be directly changed by the engineer (Krus and Grantham, 2010), resulting in a product or system that is different from the original design. Environment changes, on the other hand, are populated with strategies that don't change the product, instead focusing on changing the environment parameters of a failure mode. These strategies attempt to indirectly change the risk to a product by affecting the environment parameters, or the aspects of a design the engineer has no direct control over (Krus and Grantham, 2010), such as "Extract Contaminant" and "Stabilize Temperature," which involve trying to control what contaminants the product is exposed to and trying to maintain a constant temperature, both of which cannot be directly changed. These were considered beyond the scope of this initial taxonomy, and would be left for future work. With additional time and information, these two other categories can be added to the taxonomy.

A designer can use these categories to select mitigation strategies that are most applicable to their needs and situation. By separating the strategies into these categories, the taxonomy can help focus the engineer during risk mitigation.

3.2.2 Naming the Strategies. While collecting and cataloguing strategies, the descriptions collected varied greatly based on available resources. For instance, the length, radius, or even shape of a shaft could be altered all to fix the same failure mode of high cycle fatigue. To promote effective mitigation communication, it's important to create descriptive, encompassing names for similar strategies, much the same way as the component taxonomy groups together similar artifacts. Through a series of categorizations, the initial 325 case studies were grouped into the categories mentioned in the previous sections, and the 152 that were determined to be changes for reducing or removing the risk were further evaluated.

The first step in this effort was to group the strategies together based on similar types of changes. As discussed above, they were separated into design and environment categories. The initial grouping created 69 design categories and 59 environment categories, before excising mitigation strategies belonging to the other two groupings. For instance, all strategies that added a lubricant were grouped together and called "add lubricant." Similarly, groups like "change part geometry," where some geometric aspect of a part was altered, or "ensure part was cleaned properly," where the contaminants needed to be cleaned from a part before use. However, many of the separate groups contained only a single strategy, and could be seen as similar. In order to best use the strategies, consistent definitions needed to be established for the different strategies.

As part of this constant definition, the functional basis (Tumer, Stone, and Bell, 2003) was used. The functions from the functional basis provide clearly and consistently defined verbs that could be used to describe the actions the mitigation strategies performed. Each mitigation strategy was evaluated based on the function it performed to

mitigate the risk. These determined functions became the verbs used in the mitigation strategy taxonomy. For the objects, each strategy was evaluated to determine the object the above function operated on. These empirically determined objects were used as the objects for the mitigation strategy taxonomy. Using these two parts, each strategy can then be identified by a verb-object pair taken from these two sets. Using the above examples, "add lubricant" became "import lubricant," as it was bringing lubricant in from outside the system; "change part geometry" became "shape part" as the form of the object was changed; and "ensure part was cleaned properly" became "extract contaminant" as the outside contaminants were stripped away from the part.

This lead to the risk mitigation strategies being grouped into 42 categories by identifying common themes between strategies, such as the action they perform to mitigate the risk, such as "stabilizing" or "regulating" some aspect of the product, or what about the design they affect, such as a "part" or the "temperature."

The ultimate goal of this naming scheme is to produce a taxonomy that mirrors the form and functionality of the functional basis, where a consistent set of objects and verbs allows new functions to be created by combining functions and flows. In this same way, having a consistent set of definitions for the objects and verbs in the taxonomy would allow newfound strategies to be added to the taxonomy using a combination of existing verbs and objects. This will allow for data collected on mitigation strategies to be quantified and stored for future use, and used to evaluate different mitigation strategies.

3.3 The Risk Mitigation Strategy Taxonomy

Presented here are the terms identified in the risk mitigation strategy taxonomy. The verbs contained in these strategies were obtained from the functional basis (Tumer, Stone and Bell, 2003), and their definitions follow the forms outlined by the functional basis. The objects are a collection of terms that have been empirically determined after evaluating the collected mitigation strategies. These were then combined to form the 42 distinct mitigation strategies shown below.

3.3.1 Mitigation Strategy Taxonomy Definitions.

1. *Change Natural Frequency* – To adjust or alter the harmonic frequency of an object in a predetermined and fixed manner.
2. *Condition Material* – To render the substance that makes up the product or part appropriate for the desired use.
3. *Condition Part* – To render a component or portion of the overall product appropriate for the desired use.
4. *Convert Fuel* – To change from one chemical required for a combustion reaction to another.
5. *Convert Material* – To change from one substance that makes up the product or part to another.
6. *Convert Part* – To change from one component or portion of the overall product to another.
7. *Convert Process* – To change from one step or operation in the manufacture of a product to another.

8. *Couple Part* – To join or bring together components or portions of the overall product such that the members are still distinguishable from each other.

9. *Decrease Load* – To reduce the forces to which a product is subjected in response to a control signal.

10. *Decrease Motion* – To reduce a products ability to move freely in response to a control signal.

11. *Decrease Power Assistance* – To reduce additional force added to the system to assist with a given load in response to a control signal.

12. *Decrease Torque* – To reduce a turning or twisting force in response to a control signal.

13. *Decrement Noise* – To reduce an unwanted signal or disturbance in and electronic device or instrument in a predetermined and fixed manner.

14. *Decrement Voltage* – To reduce the electric potential in a predetermined and fixed manner.

15. *Extract Contaminant* – To draw, or forcibly pull out, foreign material whose presence can cause damage or deterioration of the product.

16. *Import Lubricant* – To bring in an agent added to a product to reduce the friction between two bodies from outside the system boundary.

17. *Import Material* – To bring in a substance that makes up the product or part from outside the system boundary.

18. *Import Part* – To bring in a component or portion of the overall product from outside the system boundary.

19. *Import Stress* – To bring in a force distributed through an area of a product from outside the system boundary.

20. *Increase Controls* – To enlarge a set of orders or rules that are followed to keep the product within proper specifications in response to a control signal.

21. *Increase Flow* – To enlarge the rate at which a fluid moves through a given area in response to a control signal.

22. *Increase Load* – To enlarge the forces to which a product is subjected in response to a control signal.

23. *Increase Temperature* – To enlarge the degree of hotness or coldness measured on a definite scale in response to a control signal.

24. *Increase Torque* – To enlarge a turning or twisting force in response to a control signal.

25. *Inhibit Contaminant* – To significantly restrain a foreign material whose presence can cause damage or deterioration of the product, though a portion of it continues to be transferred.

26. *Inhibit Moisture* – To significantly restrain water particles either suspended in the air or on the product, though a portion of it continues to be transferred.

27. *Inhibit Noise* – To significantly restrain an unwanted signal or disturbance in and electronic device or instrument, though a portion of it continues to be transferred.

28. *Inhibit Temperature* – To significantly restrain the degree of hotness or coldness measured on a definite scale, though a portion of it continues to be transferred.

29. *Position Part* – To place a component or portion of the overall product into a specific location or orientation.

30. *Process Material* – To submit the substance that makes up the product or part to a particular treatment or method having a set number of operations or steps.

31. *Regulate Flow* – To adjust the rate at which a fluid moves through a given area in response to a control signal, such as a characteristic of the flow.

32. *Remove Part* – To take away a component or portion of the overall product from its prefixed place.

33. *Secure Part* – To firmly fix a component's or portion of the overall product's path.

34. *Separate Contaminant* – To isolate a foreign material whose presence can cause damage or deterioration of the product into distinct components.

35. *Separate Part* – To isolate a component or portion of the overall product into distinct components.

36. *Shape Part* – To mold or form a component or portion of the overall product.

37. *Stabilize Flow* – To prevent the rate at which a fluid moves through a given area from changing course or location.

38. *Stabilize Process* – To prevent a step or operation in the manufacture of a product from changing course or location.

39. *Stabilize Temperature* – To prevent the degree of hotness or coldness measured on a definite scale from changing course or location.

40. *Stabilize Voltage* – To prevent the electric potential from changing course or location.

41. *Stop Process* – To cease, or prevent, the transfer of a step or operation in the manufacture of a product.

42. *Store Part* – To accumulate components or portions of the overall product.

This collection of 42 names and definitions can be used to describe mitigation strategies, allowing them to be catalogued and communicated in a consistent manner. Using the information contained in the taxonomy, risks in a new product can be mitigated efficiently, by quickly identifying risk mitigation strategies that can be applied.

4 HOW TO USE THE TAXONOMY TO IMPROVE RISK MITIGATION

The mitigation strategy taxonomy presented in the previous section can be used at any point during the products lifespan, from conceptual design to the retiring of the product. However, it is most useful to use the taxonomy to help eliminate failures during the conceptual design of the product, when changes can be made more simply and with less cost. In order to accomplish this, these mitigation strategies need to link to the failure modes that they aim to mitigate.

The mitigation strategies that exist in the taxonomy are linked to potential risks by failure modes. If a strategy was used to resolve a particular failure mode in the past, it makes sense that it could be applicable to the same failure mode in the future. Shown below, in Figure 1, is a step-by-step breakdown of the process, as outlined in this section.

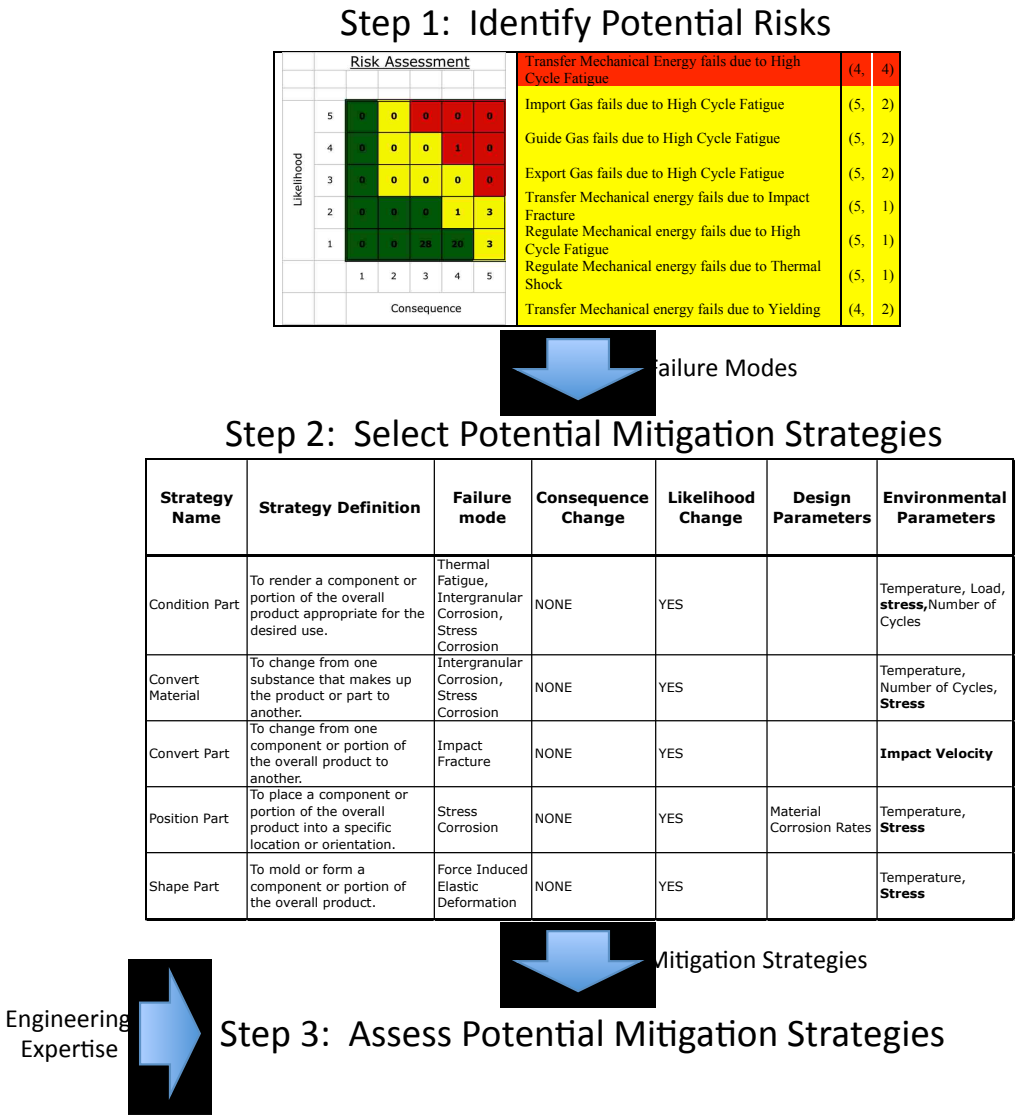


Figure 1. Breakdown of the Risk Mitigation Process Using the Mitigation Strategy Taxonomy

Step 1: Identify Potential Risks

The first step in the risk mitigation process is to identify the potential risks in the system. This task can be accomplished using any available risk analysis method or tool, such as FMEA, fault or event trees, or RED analysis. The failure modes corresponding to the risks will be used to identify potential mitigation strategies from the taxonomy.

Step 2: Select Potential Mitigation Strategies

The risk mitigation strategy taxonomy possesses data in the form of the design and environment parameters that mitigations strategies changed to prevent their failures. In this step, those parameters are matched up to the parameters found in the models of the failure modes from the risk analysis performed in Step 1. Failure mode models can be broken down into the design and environment parameters (Krus and Grantham, 2010), and they can be used to link failure modes with mitigation strategies. A search or sort of the mitigation strategy taxonomy would identify strategies that affected certain design parameters, creating a list of potential mitigation strategies that can be used on the product.

Step 3: Assess the Potential Mitigation Strategies

The mitigation strategies need to be analyzed to determine the applicable mitigation strategies for each specific case. Not every mitigation strategy is applicable in all situations. The list of strategies that have been generated needs to be evaluated, and the best potential strategy from the list selected based on the applicability of the strategy, available resources, and potential impacts, based on the information contained within the taxonomy and the engineer's experience.

The mitigation strategy taxonomy is a design tool that can be used to help mitigate the risk of failure any time in the product's life. It can be used alongside traditional risk mitigation methods to increase the design of safer and more failure free

products not just during conceptual design, but any time during the expected life of the product.

5 WIND TURBINE CASE STUDY

Presented here is an example of the above steps, applied to the design of a wind turbine during the conceptual stage of design. After the analysis has been performed, it will be compared to case studies not included in the taxonomy.

A wind turbine is an unmanned generator, powered by wind currents that are converted into mechanical energy by large fan blades. This in turn turns the turbine through the gearbox, and generates electrical energy that is stored in batteries before being sent to where it is needed. These large generators are important to analyze for risk, as it may be difficult to perform maintenance on them in the field (they are often used far from most towns and cities) and are under constant use.

The first step of this process is to determine the potential risks for the product. Since this analysis occurs during the conceptual design of the product, a functional model was created to employ the Risk in Early Design (RED) method for obtaining the product's risks. Shown in Figure 2 is the functional model of the wind turbine. The product takes in Gas (the wind), Kinetic Energy (the motion of the wind), and a status signal (what direction the wind is blowing), and output the Gas and Electrical energy.

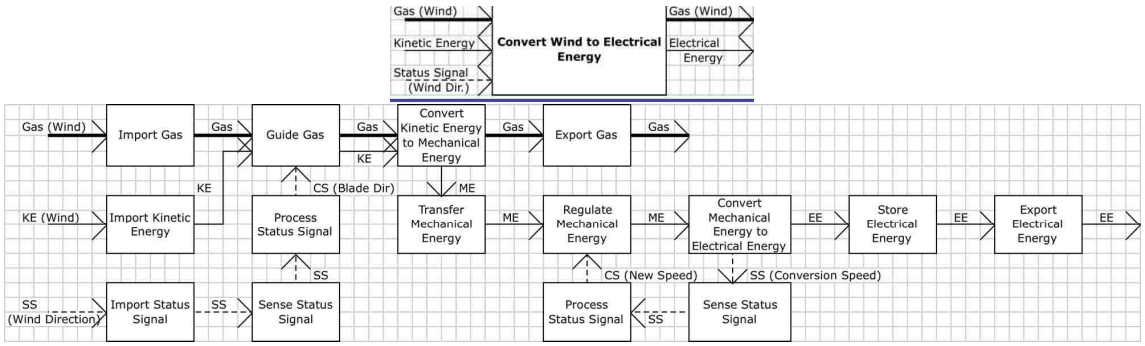
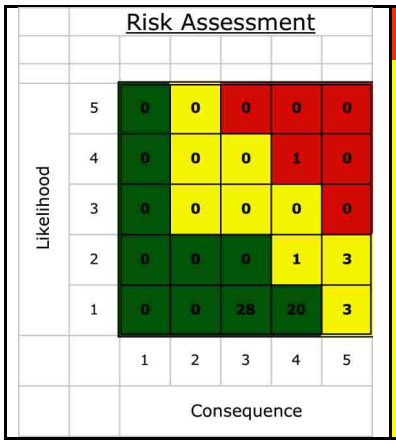


Figure 2. Wind Turbine Functional Model

This functional model is used as an input to the RED risk analysis. Using these fifteen functions, a RED analysis is performed. This analysis produced 1 high-risk element, 7 moderate risk elements, and 48 low risk elements, shown in Figure 3. Figure 3 also shows the 8 highest risk elements, including the function, failure mode, likelihood, and consequence of failure.



Transfer Mechanical Energy fails due to High Cycle Fatigue	(4, 4)
Import Gas fails due to High Cycle Fatigue	(5, 2)
Guide Gas fails due to High Cycle Fatigue	(5, 2)
Export Gas fails due to High Cycle Fatigue	(5, 2)
Transfer Mechanical energy fails due to Impact Fracture	(5, 1)
Regulate Mechanical energy fails due to High Cycle Fatigue	(5, 1)
Regulate Mechanical energy fails due to Thermal Shock	(5, 1)
Transfer Mechanical energy fails due to Yielding	(4, 2)

Figure 3. Wind Turbine RED Analysis Fever Chart

The second step is to determine the potential mitigation strategies for these risks. The risks shown in Figure 3 are caused by the failure modes “high cycle fatigue,”

"impact fracture," "thermal shock," and "yielding." The parameters for these failure modes, as shown in (Krus and Grantham, 2010), are shown below in Table 1. Data for thermal shock is not shown as there is currently no information on the design and environment parameters for that failure mode.

Table 1. Design and Environment Parameters for High Cycle Fatigue, Impact Fracture, and Yielding Failure Modes

Failure Mode	Design Parameters	Environment Parameters
High Cycle Fatigue	Fatigue Material Properties	Crack Growth
	Stress Intensity Factor	Number of Cycles
	Modulus of Elasticity	Strain
Impact Fracture	Density	Impact Velocity
		Stress
		Strain
Yielding	Yield Strength	Max Sheer Stress
	Compressive Strength	Principle Stresses
	Tensile Strength	

Using these design and environment parameters, the taxonomy is searched for mitigation strategies that have changed those parameters. Shown below in Table 2, are the results of those searches for "impact fracture." Tables C1 and C2 in Appendix C contain the results for "high cycle fatigue" and "yielding." In these tables, the strategies are shown with their definition, failure modes they have historically solved, whether the strategy lead to a change in the consequence of risk, likelihood of risk, or both, and the design and environment parameters involved in the case. As can be seen from these three tables, there are 5 strategies for "impact fracture," 7 for "yielding," and 10 for "high cycle fatigue."

Table 2. Mitigation Strategies for Impact Fracture

Strategy Name	Strategy Definition	Failure mode	Consequence Change	Likelihood Change	Design Parameters	Environmental Parameters
Condition Part	To render a component or portion of the overall product appropriate for the desired use.	Thermal Fatigue, Intergranular Corrosion, Stress Corrosion	NONE	YES		Stress
Convert Material	To change from one substance that makes up the product or part to another.	Intergranular Corrosion, Stress Corrosion	NONE	YES		Stress
Convert Part	To change from one component or portion of the overall product to another.	Impact Fracture	NONE	YES		Impact Velocity
Position Part	To place a component or portion of the overall product into a specific location or orientation.	Stress Corrosion	NONE	YES		Stress
Shape Part	To mold or form a component or portion of the overall product.	Force Induced Elastic Deformation	NONE	YES		Stress

The final step is assessing these potential mitigation strategies. For “impact fracture,” the five strategies present ways of altering environment parameters to control the risk. Conditioning the part involves treating the part to reduce the stress, and converting the material changes the material to reduce the stress as well. Converting the part switches the part to change the velocity of an impact. Finally, positioning and shaping the part alter the position of the part or its shape, to change the stress. Of these choices, converting the part is the most obvious strategy, as this would lower the velocity of the impact by switching out the part for a different one so it is struck with less velocity, or is out of the path of being struck (reducing the impact velocity to zero). The other strategies all indirectly try to decrease the stress due to the impact, making the impact less damaging.

For “high cycle fatigue” and “yielding” can be evaluated in similar fashions. For “high cycle fatigue,” securing the part and converting the material would be the ideal choices, as converting the material would change two potential parameters with a single

strategy, allowing for greater control of the failure, and securing the part would also reduce the consequence of failure as well as the likelihood. " Yielding" would be best handled by conditioning the material, the part, or increasing controls. Conditioning the material and part could be accomplished at the same time, and provide similar benefits to each other. Increasing the controls during manufacturing could increase the tensile strength of the part, giving it greater resistance to the failure mode. Further, condition the material and increasing the control would reduce the consequence as well, adding an additional benefit to selecting them.

These strategies were compared to a report by Manwell et al. (1999), which examined potential failures in a wind-turbine's gearbox, which can be represented as transfer mechanical energy in the above functional model. This report mentioned that impact fracture was one of the failures found in the gearbox. Three recommendations were made in the report, offering strategies of using improved 1st stage carriers with spherical bearings, improving the retention by using a tighter fit or locking mechanism, and adding a teeter damper to the design. These correspond to mitigation strategies of converting a part, positioning a part, or importing a part. As shown above, for impact fracture, the mitigation strategy taxonomy was able to determine two of the mitigation strategies suggested by the report. In a similar report on mitigations that have been performed on wind turbines (Moser, 2010), lubrication, tapered roller bearings, and refined material processing have removed similar failures. The refined material processing (condition material) is reported by both yielding and high cycle fatigue, and the bearings, as discussed above, are an application of convert part, which also covers yielding. As shown by these two examples, the mitigation strategy taxonomy can

correctly generate mitigation strategies that have been generated based on expertise, not using the taxonomy.

6 CONCLUSIONS

By using the mitigation strategy taxonomy presented here, engineers can add to their own experience and perform a more thorough mitigation of their products. The taxonomy assists with the mitigation of failure right from the beginning of the design process, allowing failure mitigation to become integral to the design of the product. Further, as the product becomes more developed, additional strategies can be selected for more specific aspects of the design, maintaining the focus on designing a failure free product. Finally, it categorizes mitigation strategies into a common language that can aid in the communication of risk and mitigation.

The taxonomy is also a growing project. Additional failure mitigation strategies will be added to the taxonomy, making it more complete and increasing the diversity of potential strategies. Like the failure mode taxonomy and component taxonomy, the risk mitigation strategies will grow as new mitigation strategies and failure modes that need mitigation strategies appear.

A means of rating potential strategies also needs to be created. Using the collected information in the taxonomy, rating using the likelihood change, consequence change, and a popularity rating based on the number of times a strategy has been encountered, a series of calculations could be made to help automate and speed the risk mitigation procedure. Further, the selection method presented in this paper could be

automated, allowing the transition from function-failure mode pairs to mitigation strategies to smoothly flow, and be implemented in the same program.

REFERENCES

"Analyst: Recall Costs Toyota $155M a Week As Fix for Gas Pedal Problem Underway, Japanese Auto Giant Braces for Public Backlash," 2010. Retrieved September 22, 2010, from http://www.cbsnews.com/stories/2010/02/02/business/main6165930.shtml

Akiyama, K., 1991. *Function Analysis: Systematic Improvement of Quality Performance*. Productivity Press.

Barsalou LW, 1992. *Cognitive Psychology: An overview for Cognitive Scientists*. Lawrence Erlbaum Associates, Inc.

"BP oil spill timeline," 2010. Retrieved November 3, 2011 from http://www.guardian.co.uk/environment/2010/jun/29/bp-oil-spill-timeline-deepwater-horizon.

Brody, S. D., S. Zahran, et al., 2009. "Policy Learning for Flood Mitigation: AA Longitudinal Assessment of the Community Rating System in Florida." Risk Analysis 29(6): 912-929.

Bryant, C., Stone, R., McAdams, D., 2006, "Automated concept generation from the functional basis of design," Accepted to Research in Engineering Design.

Chenhall, R. G., 1978, *Nomenclature for Museum Cataloging: A System for Classifying Man-Made Objects*, American Association for State and Local History, Nashville, TN.

Coit, D. W., 2000. "System Reliability Prediction Prioritization Strategy." Paper presented at the Annual Reliability and Maintainability Symposium.

Collins, J., Hagan, B., and Bratt, H., 1976, "The Failure-Experience Matrix - a Useful Design Tool," Transactions of the ASME, Series B, Journal of Engineering in Industry, 98:1074-1079.

Depatmnet of Defense, 1949. *Proceedures for performing failure mode, effects, and criticality analysis.*

Dillon, R. L., R. M. Liebe, et al., 2009. "Risk-Based Decision Making for Terrorism Applications." Risk Analysis 29(3): 321-335.

"Fukushima Accident 2011," 2011. Retrieved November 3, 2011 from www.world-nuclear.org/info/fukushima_accident_inf129.html.

Grantham Lough K*, et al.*, 2009. "Promoting risk communication in early design through linguistic analyses " *Research in Engineering Design,* vol. 20, pp. 29-40.

Grantham Lough, K., 2005. “Risk in Early Design.” Unpublished Dissertation, University of Missouri-Rolla, Rolla, MO.

Greer, J., Stock, M., Stone, R. and Wood, K., 2003, “Enumerating the Component Space: First Steps Toward a Design Naming Convention for Mechanical Parts,” Accepted to Proceedings of DETC2003, Chicago, IL.

Handbook of Case Histories in Failure, 1993. 2. Ed. Khlefa A. Esaklul. Ohio: Materials Park.

Hatamura, Y., 2009. *Learning from Design*. Springer.

Hirtz, J., Stone, R., McAdams, D., Szykman, S. and Wood, K., 2002, “A Functional Basis for Engineering Design: Reconciling and Evolving Previous Efforts,” Research in Engineering Design 13(2):65-82.

Hundal, M., 1990, “A Systematic Method for Developing Function Structures, Solutions and Concept Variants,” Mechanism and Machine Theory, 25(3):243-256.

J. F. Manwell, A. Rogers, U. Abdulwahid, A. Ellis and B. P. McNiff, 1999. "Wind Turbine Gearbox Evaluation," Proc. European Wind energy Conference, Nice, France.

Kirschman, C., Fadel, G., 1998. “Classifying Functions for Mechanical Design,” Journal of Mechanical Design, Transactions of the ASME, 120(3):475-482.

Koch, P., Peplinski, J., Allen, J. and Mistree, F., 1994, “A Method for Design Using Available Assets: Identifying a Feasible System Configuration,” Behavioral Science, 30:229-250.

Krus, D., and Grantham K., 2010. "A Step Toward Risk Mitigation During Conceptual Product Design: Component Selection for Risk Reduction," in *IDETC 2010*, Montreal, Qubec.

Krus, D., Grantham, K., 2011. “Towards failure free design: an analysis of risk mitigation communication.” In IDETC 2011, Washington DC, 2011.

Kurtoglu, T., Campbell, M.I., Bryant, C.R., Stone, R.B., McAdams, D.A., 2005, “Deriving a Component Basis for Computational Functional Synthesis,” Proceedings of International Conference on Engineering Design, ICED05, August 15-18, Melbourne, Australia.

Linnaei, C., 1937. *Determinationes In Hortum Siccum Joachimi Burseri: The Text of the Manuscript in the Linnaean Collections*, ed. Spencer Savage, London, England, Printed for the Linnaean Society by Taylor and Francis.

Little, A., Wood, K., and McAdams, D., 1997. “Functional Analysis: A Fundamental Empirical Study for Reverse Engineering, Benchmarking and Redesign,” Proceedings of the ASME Design Theory and Methodology Conference, Sacramento, California.

McAdams, D. and Wood, K., 1999. “Methods and Principles for Concurrent Functional Tolerance Design,” Proceedings of the 1999 ASME Design For Manufacturing Conference,” number 99-DETC/DFM49, Las Vegas, Nevada.

McAdams, D. and Wood, K., 2000. “Quantitative Measures for Design by Analogy,” Proceedings of the 2000 ASME Design Theory and Methodology Conference, number DETC2000/DTM-14562, Baltimore, Maryland, September.

McAdams, D., Stone, R., and Wood, K., 1999. “Functional Interdependence and Product Similarity Based on Customer Needs,'” The Journal of Research in Engineering Design, 11(1):1- 19.

Miles, L., 1972, *Techniques of Value Analysis Engineering*, McGraw-Hill.

Miller, Ryan, 2011. "Super Lightweight Tank Risk Management Case Study." NASA. Retrieved 22 June. 2011. <http://www.nasa.gov/externalflash/irkm-slwt/index.html>.

Moser, B., 2010. “Turbine Failure: Fine-tuning turbine gearbox performance,” Retrieved February 23, 2012, from http://social.windenergyupdate.com/om/turbine-failure-fine-tuning-turbine-gearbox-performance.

Ombete, Kenneth, 2009. “Preventing chemical product failure.” Unpublished Thesis, University of Missouri-Rolla, Rolla, MO.

Pahl, G. and Beitz, W., 1988. *Engineering Design: A Systematic Approach*, Springer-Verlag.

Patil, Rahul B., 2008. “Business risk in early design: an approach.” Unpublished Thesis, University of Missouri-Rolla, Rolla, MO.

Qiu, Y., Ge, P., & Yim, S. C., 2007. “Risk-Based Resource Allocation for Collaborative System Design in Distributed Environment.” Paper presented at the International Design Engineering Technical Conference, Las Vegas, NV, USA.

Roberts, R. A., Stone, R. B. and Tumer, I. Y., 2002. “Deriving Function-Failure Information for Failure-Free Rotorcraft Component Design,” Proceedings of the 2002 ASME Design Engineering Technical Conferences, Design for Manufacturing Conference, DETC2002/DFM-34166, Montreal, Canada.

Stock, M., Stone, R. and Tumer, I., 2003. "Going Back in Time to Improve Design: The Elemental Function-Failure Design Method," Proceedings of DETC2003, DETC2003/DTM-48638, Chicago, IL.

Stone, R., 1997. "Towards a Theory of Modular Design," Doctoral Thesis, The University of Texas at Austin.

Stone, R. and Wood, K., 1999. "Development of a Functional Basis for Design," Proceedings of DETC99, DETC99/DTM-8765, Las Vegas, NV.

Strawbridge, B., McAdams, D. and Stone, R., 2002. "A Computational Approach To Conceptual Design," Proceedings of DETC2002, DETC2002/DTM-34001, Montreal, Canada.

Tumer, I. Y., Stone, R. and Roberts, R. A., 2003. "Analysis of JPL's Problem and Failure Reporting Database," Submitted to Proceedings of the 2003 ASME Design Engineering Technical Conference, Design for Manufacturing Conference, Chicago, IL.

Tumer, I., Stone, R. and Bell, D., 2003. "Requirements for a Failure Mode Taxonomy for Use in Conceptual Design," Proceedings of the International Conference on Engineering Design, ICED 03, Paper 1612, Stockholm, Sweden.

Ullman, D. G., 2003. *The Mechanical Design Process*. 3rd Edition. McGraw Hill, Boston.

VAI (Value Analysis Incorporated), 1993. *Value Analysis, Value Engineering, and Value Management*, Clifton Park, New York.

Wang J. X. and Roush M. L., 2000. *What Every Engineer Should Know About Risk Engineering and Management*. New York, NY: Marcel Dekker, Inc.

Wilson R and Keil F, 1999. *The MIT Encyclopedia of the Cognitive Sciences*. Cambridge, Mass: The MIT Press.

PAPER IV

GENERATED RISK EVENT EFFECT NEUTRALIZATION: IDENTIFYING AND EVALUATING RISK MITIGATION STRATEGIES DURING CONCEPTUAL DESIGN

Daniel Krus

Department of Mechanical Engineering

Missouri University of Science and Technology

Katie Grantham, Ph.D.

Assistant Professor of Engineering Management and Systems Engineering

Missouri University of Science and Technology

ABSTRACT

In the design of new products and systems, the mitigation of potential failures is very important. The sooner potential mitigation strategies can be employed, the lower the cost of those changes will be. Still, there needs to be a means to generate and evaluate mitigation strategies to supplement the existing expertise of the designer. By combining a mitigation strategy taxonomy with various rating strategies, a means to quickly select strategies and demonstrate their effect on the risk of failure can be obtained. This paper explains the risk mitigation selection and evaluation methods, including the mapping calculations used to evaluate strategies and their use in a method to move from a functional model of a new product to a selection of mitigation strategies that can be compared, and select the best strategy for the product.

Keywords: Risk Mitigation, Risk Analysis, Conceptual Design

1 INTRODUCTION

1.1 Scope

During the design of a new product or system, the potential risk of failure is very important to consider. The damages caused by the lack of consideration of potential failures can be great. However, by taking an interest in these risks at the earliest stages of the design process, the largest impact can be made at the least cost.

There already exist several methods of determining potential failure modes in a product, such as Fault Tree Assessment, Event Tree Assessment, and the Risk in Early Design Method (RED) (Bedford and Cooke, 2001; W. E. Vesley, 1981; UNSRC, 1975; Grantham Lough, 2005). These methods, while providing what can go wrong with a product or system, do not address how that wrong can be avoided or made right. Currently, the creation and evaluation of risk mitigation strategies is an exercise left for the designer, and relying solely on their expertise and that of their team. There needs to be a way to bridge this gap between the locating of potential failures, and the creation of strategies to mitigate those failures.

Recently, there has been work on a mitigation strategy taxonomy, which collects strategies that were used to mitigate risks in products and systems (Krus and Grantham, 2012). While this taxonomy goes a long way towards allowing the risk mitigation process to be sped up and improved, it still lacks a means to evaluate individual strategies and select the best potential ones, still relying on the expertise of the designer to evaluate

the potential strategies.

This paper seeks to present that step, the Generated Risk Event Effect Neutralization (GREEN) method, and demonstrate how this method can used to move from a list of risks generated during the conceptual design to a group of mitigation strategies, from which the best can be selected.

1.2 Motivation and Applications

In engineering, unplanned failures can be catastrophic for both the end user of the product and the company that produced the product. These failures need not be complex for them to have large consequences. A simple design flaw in the accelerator of some of Toyota's vehicles caused the accelerator to seize in place and cause uncontrolled acceleration caused 52 deaths and 32 injuries. On top of this loss of life, the failures caused Toyota to recall 4.5 million vehicles and cost the company $900 million in repairs. The damage to the company's image also cost Toyota $155 million in lost business. All of this was caused when the design of the accelerator was changed from a mechanical accelerator (as had been used in all designs previous to this one) to an electrical accelerator. The new design did not offer the resistance the human operators expected, so a friction plate was added to provide the resistance. This new plate is what seized (Keane and Plungis, 2010; CBS.com, 2010).

Planning for failure can be instrumental in resolving potential failures. However, this planning has a greater effect when performed before the risk materializes. The cleanup from the Deepwater Horizon oilrig operated by British Petroleum developed many strategies for dealing with the oil spill after the failure occurred. From April 24

through September 21, 15 different mitigation strategies were attempted in an effort to close the well with limited degrees of success (Garudian.co.uk, 2010). By identifying this potential risk beforehand, these strategies could have been tested and evaluated in a controlled setting, and react to the failure with a proven strategy at a faster pace.

However, with proper planning, risks can be mitigated. The Fukushima nuclear reactors provide an example of successful risk mitigation in action. Like most nuclear reactors used today, the Fukushima reactors were designed with the principle of defense-in-depth; that is, by designing multiple, different, redundant strategies for greater than the worst possible scenario. Everything from the design of the reactor and fuel rods to the use of boric acid and sea water to cool the overheating reactor was a plan put in place from the beginning of design, and helped prevent a major disaster from turning into an even larger one (World Nuclear Association, 2011).

To follow this example, the GREEN method seeks to provide a means to determine potential mitigation strategies as early as possible in the design process, to allow these strategies to be worked into the design of the product, and allow for the maximum amount of testing before releasing the product to the public. Starting from the functional model of the product, GREEN uses generated failure modes provided by the RED method to suggest mitigation strategies from a collected taxonomy, and then rate those strategies based on historical data.

This will allow designers to focus on the risks inherent to a product from the very beginning of the design process, and making risk mitigation integral to the design. Further, it allows designers to supplement their already existing engineering expertise with the collected historical knowledge contained within the mitigation strategy

knowledgebase.

2 BACKGROUND

2.1 Risk Mitigation Theories and Methods

Risk mitigation is the process of generating strategies to remove risks from a system, limit remaining risks, and monitor and control the remaining risks (Wang and Roush, 2000). While the primary means of risk mitigation remains the use of expert knowledge, there are several different methods that are used to aid this process. These methods assist the process by helping to organize the created strategies or compare different strategies and determine the best potential one.

Failure Modes and Effects Analysis (FMEA) is a risk analysis tool that has risk mitigation as one of its steps. For a given product, all risks to be considered are listed out, the corresponding component identified, and then rated according to the occurrence, severity, and detection, which are then combined into a risk priority number. Each item on the list is also given a potential solution that can be used to mitigate the failure (Department of Defense, 1949). Recent advancements in FMEA make it better suited for use during conceptual design (Grantham Lough, 2007), however, this does not completely remove its subjectivity. Further, for the mitigation of the individual failure modes, there are no guidelines, relying only on the expertise of the on performing the analysis.

Cost-benefit analysis (CBA) is a means used to measure a strategy based on it perceived costs of execution and the benefits gained from implementing the strategy. Each strategy is evaluated based on the cost of putting it into action, usually converted to

a monetary amount. Then, the benefits, again converted to a monetary value, are evaluated. Then these values are compared across multiple strategies to determine which strategies give the best net gain. While this is the current method of comparing mitigation strategies, some costs and benefits, such as human life and health are difficult to quantify (Nas, 1996).

Some reliability prediction strategies, such as penalty functions, try to reduce risk by guiding the design toward the minimum risk. Using penalty functions alongside genetic algorithms, systems and products can be designed to maximize reliability and minimize cost, iterating designs until the most reliable products are designed (Coit and Smith, 1996). This method does not generate strategies as much as it tries to develop a design that minimizes the risk, limiting the choice of the designer.

Along the same line is the system reliability prioritization method, which uses the uncertainty of analysis methods to identify what portions of a design need additional analysis or refinement (Coit, 2000). This method focuses the mitigation on the components that are at the least understood or at the highest risk, driving the mitigation of the part to the parts that have the highest need. However, like the penalty functions, no actual strategies are generated, leaving the actual mitigation strategies developed and used to the designer.

More recently, the risk-based resource allocation methodology (R-DRAM) provides a means to allocate resources across a system to maximize risk reduction for a given budget. R-DRAM identifies the risk across all shareholders and then evaluates the probabilities for all of those risks consistently. Using these probabilities and the CBA of spending a given amount of resources on a given mitigation strategy, it evaluates the best

possible combination of strategies for dealing with a given risk (Qiu, Ge, and Yim, 2007). This method focuses on the most efficient expenditure of resources, not necessarily the highest risk items, and still relies on the designer to provide the mitigation strategies that will be used in the analysis.

The antiterrorism risk-based decision aid (ARDA) provides a means of risk mitigation tailored to the mitigation of potential terrorist attacks. This method collects the locations and facilities that may be at risk, and what the expected losses (costs) in terms of lives lost, values of facilities, and costs of repairs, and finally, the likelihood of an attack at that location. Using all of this data, various mitigation strategies are assessed and compared based on how much they reduce the cost of those terrorist incidents (Dillon Liebe, Bestafka, 2009). ARDA provides a solid means to evaluate strategies, but requires a fully developed system and a great deal of historical data in order to use properly. Further, like all of the above methods, it does not generate strategies, leaving it up to the designer to determine what strategies to evaluate.

Another way to handle potential risks during concept generation is the Theory of Inventive Problem Solving (TIPS). This design method was generated from studying millions of patents to determine trends in product design. From these trends, TIPS presents a set of generalized parameters for describing product metrics, and strategies for resolving conflicts between those parameters (Altshuller, 1984). When using TIPS, the engineer evaluates conflicts that exist in the product design, and then those conflicts stated as contradictions between two of the 39 parameters defined. That conflict then lists which of the 40 design principles are applicable to the conflict. These design principles can then be used to improve a design, and effectively resolve the conflict (Otto

and Wood, 2001).

A final method is one that uses not CBA to evaluate a mitigation strategy, but instead uses the system or product in production to test out mitigation strategies. Adaptive management generates policies to handle a given risk, and puts those policies into practice. If the policy works, then it can continue to be used to mitigate a particular risk. If it fails to address the risk, it can be adapted or replaced to meet with the changing requirements (Brody, et al., 2009). This system relies heavily on expert opinion and record keeping of the effects of past mitigation strategies. Further, it requires a developed system, making it unsuitable for conceptual design.

For risk mitigation during conceptual design, a method that generates mitigation strategies while only requiring a functional model of the product is quite advantageous, allowing for failure mitigation to be added to the system from the very beginning, before the physical design solution has been finalized. Further, the ability to rate those mitigation strategies based on their past performance would allow the designer to select the best possible mitigations for the given design. The GREEN method seeks to meet these requirements, filling gaps not covered by other methods, and supplementing the expert opinion normally called upon. However, before risk mitigation can move into using GREEN, the potential product risks need to be identified. For this purpose, the mitigation process in the conceptual design starts with the RED method.

2.2 The Risk in Early Design Method

The Risk in Early Design Method (RED) is a risk analysis tool designed to determine potential failure modes and their risk when given only a functional model

(Grantham Lough, 2005). RED has its basis in the Function Failure Design Method (Stock, Stone, Tumer, 2003), a means of connecting historical product failures to the functions those components performed. First, a collected knowledge base linking components to failure modes is made. This knowledge base is collected from historical failure reports, and compiled into a database listing the number of times a given component from the component taxonomy has failed by a given failure mode. This is the Component Failure Matrix (CF matrix).

A second matrix is also collected, using a collection of products and functional models to determine the connections between given functions and a component. This matrix simply lists if a component has ever solved a particular function. This is the Function-Component Matrix (EC matrix).

These two matrices are multiplied together (EC x CF = EF), to create the Function Failure Matrix. This new matrix provides the number of times a function has failed by a given failure mode. RED takes this basis from FFDM and adds the ability to calculate the likelihood and consequence of risk (Grantham Lough, 2005).

First, an additional matrix, the CF' matrix is created, where instead of the number of times a component has failed, the severity of the failure is recorded instead. This severity scale is a set of values, ranked from 1 to 5 based on a scale used by Wang and Rousch (2000), that determines the consequence of the risk for a given failure. This is combined with the EC matrix to determine the severity of failure for a given function and failure mode.

Second, a list of functions taken from a functional model is used to select the functions for the RED analysis. These functions are used to select the values from the EF

matrix and EC,CF' matrix to perform calculations on. These calculations are based on different mappings of the EF and EC,CF' matrices. The likelihood mappings L1 and L2 normalize the number of times a failure has occurred to an integer value between 0 and 5, based on either the functions in the product (L1) or the entire database (L2). L1 is useful for subsystem level analysis, comparing the likelihood only against other subsystems in the product; L2 is useful for system level analysis as it compares the likelihood against the entire database. Similarly, the consequence mappings C1 and C2 are appropriate for a human -centric (C1) and unmanned systems (C2). C1 take the worst case scenario for the given consequences, making it well suited when humans are involved. C2 averaged the values based on the function-failures that had recorded values, focusing on the low to mid range of values that deal with unmanned products (Grantham Lough, 2005).

Once the mappings are selected for the given analysis, those mappings are used to calculate the likelihood and consequence values for each combination of function and failure mode in the knowledge base. These results are then presented in two forms: a list of function failure mode pairs and their corresponding likelihood and consequence values, and a fever chart that lists the number of failures that occurred at a given combination of likelihood and consequence (Grantham Lough, 2005).

The RED method allows for risk analysis to be performed during conceptual design, and even by novice designers with minimal risk analysis experience. However, to move from this analysis to mitigation strategies, a historical knowledgebase of strategies, similar to RED's matrices, needs to exist. This is met by the mitigation strategy taxonomy.

2.3 The Risk Mitigation Strategy Taxonomy

The risk mitigation strategy taxonomy is a collection of 42 electromechanical risk mitigation strategies that was derived from 325 case studies from industry handbooks and corporate data (Krus and Grantham, 2012). The risk mitigation strategy taxonomy is a tool that defines mitigation strategies based on the changes they perform on the product, and what they make those changes to. These strategies are in verb-object form, with the object taken from the functional basis (Stone and Wood, 1999) and the object empirically determined from the analysis of the case studies.

The mitigation strategy taxonomy was based on the study of models used simulate different failure modes. These models were studied to determine the parameters that an engineer could directly modify and use to control risk due to those failure modes (Krus and Grantham, 2010). Expanding on the two categories of parameters and work on evaluating risk elements (Grantham et al., 2009), a linguistic means for evaluating mitigation strategies was developed, using six attributes to measure how well a mitigation strategy conveyed information (Krus and Grantham, 2011). These lead to the creation of the mitigation strategy taxonomy, using the attributes from the linguistic analysis to collect information on mitigation strategies and categorize them into 42 different strategies (Krus and Grantham, 2012).

The risk mitigation strategy taxonomy allows information on mitigation strategies to be collected and categorized. Because the mitigation strategy has consistently defined strategies, data from mitigation practices can be stored together, and used to generate strategies for new products (Krus and Grantham, 2012). Using risks determined by a risk analysis method, such as RED, the taxonomy can be used to generate mitigation

strategies based on the failure modes of those risks. These generated strategies can then be evaluated based on the product they are being generated for, using the engineer's experience to further select and refine the strategies (Krus and Grantham, 2012).

This process can be further enhanced. By having a standardized taxonomy of mitigation strategies, mappings can be performed on collected information on those strategies similar to the RED method, allowing the rating of how a mitigation strategy affects different risks. In the next section, the mitigation strategy taxonomy will be used to demonstrate how using failure mode data from a RED analysis, the information in the mitigation taxonomy can be used to select potential mitigation strategies and evaluate their effects on the failure modes.

3 THE GREEN METHOD

The Generated Risk Event Effect Neutralization (GREEN) method is a series of steps that lead from a risk analysis from RED to a set of risk mitigations that can be compared, to identify the best strategy for the given situation. The GREEN method can be broken down into linking the mitigation strategies with failure modes, comparing the strategies, and then selecting the best strategies. This process is illustrated in Figure 1. GREEN starts with a functional model, which is then used to perform a RED analysis. This provides the list of function-failure mode pairs that will be used to determine potential mitigation strategies. Next, the potential mitigation strategies are determined by using the GREEN matrices. These matrices contain information on potential failure modes and their parameters, parameters that have been changed by mitigation strategies, and the likelihood and consequence changes for a given mitigation strategy. Finally,

ratings are generated for the mitigation strategies based on the original likelihood and consequence of risk, the changes to the likelihood and consequence taken from the knowledge base, and the popularity from how frequently the strategy has been used. These ratings can then be evaluated, and the mitigation strategies that best fit the product selected based on those ratings.

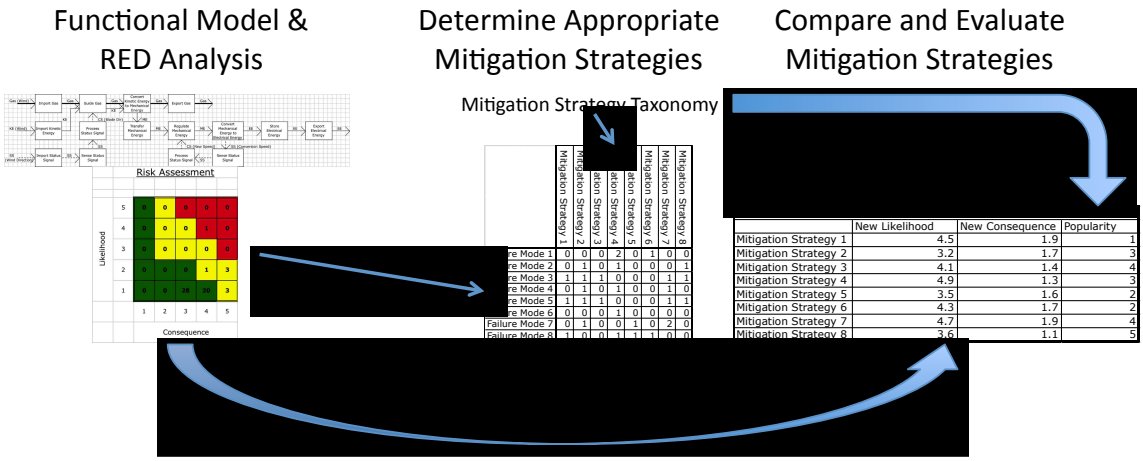


Figure 1. The GREEN Method

3.1 Linking Failure Modes to Mitigation Strategies

The GREEN method starts from a collection of function-failure mode pairs, as taken from a RED analysis. These pairs have a function, failure mode, likelihood of risk, and a consequence of risk. To start the method, the failure mode is used to find the appropriate links to mitigation strategies using the parameters the failure modes and mitigation strategies have in common. As proposed by Krus and Grantham (2010), the models for a failure mode are made up of parameters. By using those parameters, mitigation strategies that have corresponding design and environment parameters can be selected from the taxonomy.

To perform this linking, matrices linking the failure modes to parameters (**FP**) and the parameters to mitigation strategies (**PS**) need to be created. The **FP** matrix should be a *m* by *n* matrix, where *m* is the number failure modes and *n* is the number of mitigation strategies. Similarly, the **PS** matrix should be a *n* by *s* matrix, where s is the number of mitigation strategies. In the **FP** matrix's case, the entries are binary, recording which failure modes have corresponded to which parameters, with a 1 representing the failure mode is affected by that parameter, and 0 representing the parameter having no baring on the failure mode. The **PS** matrix, on the other hand, is incremented based on the number of times a mitigation strategy has altered a given parameter. Once these two matrices have been created, they can be multiplied together to create the Failure Mode-Mitigation strategy matrix (**FP** x **PS** = **FS**), which shows failure modes, which mitigation strategies are applicable, and how frequently the mitigation strategy have been used to answer a failure mode. An example of the **FP**, **PS**, and **FS** matrices is shown below in Figure 2.

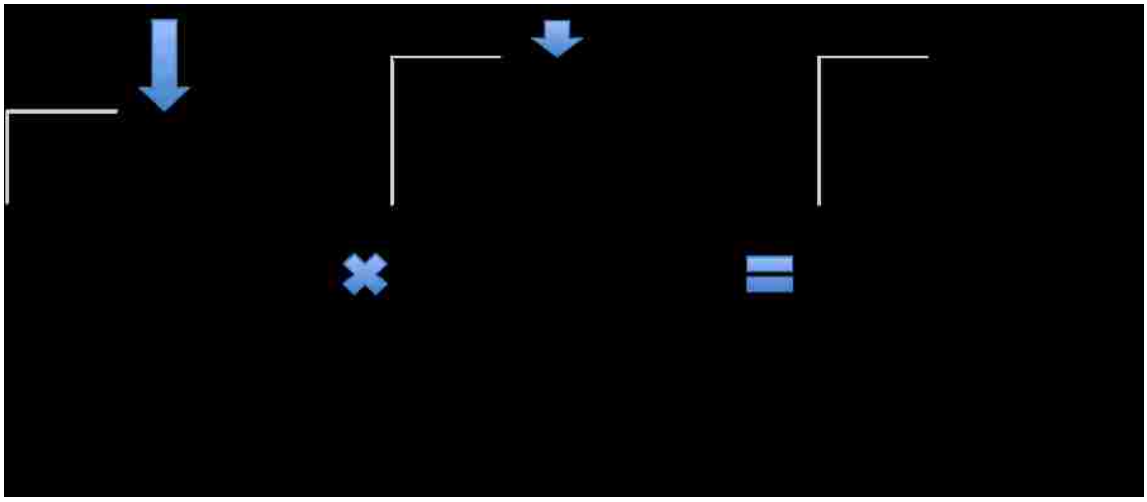


Figure 2. Linking the Mitigation Strategies to the Failure Modes (**FP**, **PS**, and **FS** Matrices)

A fourth matrix, the Mitigation Strategy Likelihood-Consequence (**SC**), collects the likelihood and consequence changes for each mitigation strategies. This matrix is a *s* by 2 matrix, with the likelihood and consequence recorded for each strategy.
These matrices can be created for any division of the mitigation strategy taxonomy or for the entire taxonomy, as needed. Again, this work focuses on electromechanical mitigation strategies. By selecting different types of strategies, a designer can focus the mitigation of a risk in a particular direction.

3.2 Comparing the Strategies

As shown in the previous section. each function-failure mode pair can be linked to several potential mitigation strategies from the mitigation strategy taxonomy. However, there is nothing differentiating these strategies from each other. In order to aid in evaluating the strategies, there needs to be a means to compare these strategies.

In order to evaluate these strategies, the only pieces of numerical data that can be used are the original likelihood and consequence of risk from the function-failure mode pair and the likelihood and consequence changes, and the number of times a strategy has been encountered. Using these five pieces of numerical data, ways to calculate the likelihood and consequence of the function-failure mode pair after the mitigation strategy has been applied, as well as the popularity of the mitigation strategy will be developed.

To design these equations, first, English sentences were made by stating exactly what each of the calculations was to be. Those sentences were then translated into mathematical terminology, using the available variables, such as the original likelihood and consequence and the likelihood and consequence changes from the risk mitigation strategy knowledge base. The following sections detail the derivation and use of the calculations for the new likelihood, new consequence, and the popularity of the mitigation strategy.

3.2.1 New Likelihood Calculation. The new likelihood calculation gives the new likelihood of failure for a function after employing the mitigation strategy to reduce the risk. This calculation takes the original risk due to likelihood, supplied from RED, and uses the likelihood change stored in the mitigation strategy taxonomy to calculate a new likelihood of failure. When developing the equation for this calculation, the sentence "The new likelihood is the original likelihood lowered by the change in likelihood." This sentence can be translated into the equation (1):

$$L_{new} = L_{original}(1 - L_{change}) \tag{1}$$

In this equation, $L_{original}$ is the original likelihood due to risk, L_{change} is the

likelihood change taken from the failure mitigation knowledge base, and L_{new} is the new likelihood of failure after the mitigation strategy. $L_{original}$, taken from the RED analysis is an integer value from 1 to 5, and L_{change} is a percent change between 0 and 1 taken from the **SC** matrix, which creates a L_{new} that is a decimal value between 0 and 5.

3.2.2 New Consequence Calculation. The new consequence calculation gives the new risk due to consequence after employing the mitigation strategy to reduce the risk. Similarly to the new likelihood calculation, it take the original consequence and uses the consequence change supplied by the strategy knowledge base to calculate the new consequence. The sentence, again, is almost identical to the one used by the new likelihood calculation: "The new consequence is the original consequence lowered by the change in consequence." This sentence gives equation (2).

$$C_{new} = C_{original}\left(1 - C_{change}\right) \tag{2}$$

In this equation, $C_{original}$ is the original likelihood due to risk, C_{change} is the consequence change taken from the failure mitigation knowledge base, and C_{new} is the new consequence of failure after the mitigation strategy. As above, $C_{original}$, taken from the RED analysis is an integer value from 1 to 5, and C_{change} is a percent change between 0 and 1 taken from the **SC** matrix, which creates a C_{new} that is a decimal value between 0 and 5.

3.2.3 Popularity. The popularity measure evaluated how frequently a given mitigation strategy has been encountered, and thus, how popular it is to use in industry. This is useful as the popularity of the mitigation strategy may contain information that the

likelihood and consequence reductions may not capture, such as a lower cost or easier implementation. To derive this equation, the sentence "The popularity of a mitigation strategy is the normalized ratio of the number of occurrences of this strategy to the greatest number of occurrences of all strategies in the knowledge base." This sentence, when translated, yields equation (3).

$$Pop_i = \text{int}\left\{5\frac{N_i}{\max\limits_{1<j<n}\left(N_j\right)}\right\} \tag{3}$$

In this equation, Ni is the number of occurrences for the i^{th} mitigation strategy, as found in the **FS** matrix. This equation gives a normalized integer from 1 to 5 based on how many occurrences a given strategy has had, compared to the number of occurrences the most seen strategy has. This rating is based purely on the number of times a given strategy has been encountered and recorded in the database.

3.3 Selecting the Mitigation Strategy

Once the mitigation strategies have been rated, they must be compared and the best mitigation strategy(s) must be selected. This can be accomplished in a number of ways. For a single function-failure mode pair, each of the individual applicable strategies can be looked at and compared based on their new likelihood and consequence ratings, as well as the popularity rating, and selecting the best strategy purely on straight comparison. Conversely, if the same mitigation strategy appears for several different function-failure mode pairs, it would rate higher than strategies that only appeared for a single function-failure mode pair but otherwise had the same ratings. At this point, the engineering expertise paired with the output from GREEN is used to select the best

mitigation strategies for the product.

4 AN EXAMPLE OF GREEN

Presented here is an example of the GREEN method applied to a design problem. In this example, the product being designed is a new wind turbine, based on case studies not included in the current GREEN knowledge base. This will be compared to the mitigation strategies recommended by the case study, to verify the GREEN method's results.

In order to perform a GREEN risk mitigation, first there needs to be a functional model of the product. Shown below in Figure 3 is a functional model of a wind turbine. This model contains 15 different functions, taking in gas (the wind), kinetic energy (the movement of the wind), and a status signal (the wind direction), and exporting the gas and electrical energy.

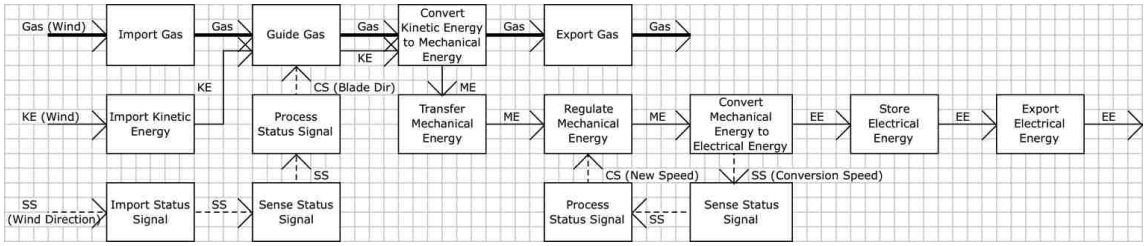


Figure 3. Wind Turbine Functional Model

Using this functional model, a RED analysis is performed on the functional model. For this particular example, the L1 C2 mapping will be used, as the failure of the individual subsystems was desired, and it will be operating far away from humans and is thus unmanned. Shown below in Figure 4 and Table 1 are the fever chart and the highest

risk (high and moderate risk) elements from the analysis. As can be seen from this analysis, there is 1 high-risk element, 7 moderate risk elements, and 48 low risk elements. For this assessment, the 8 highest risk elements will be focused on.

The 8 highest risk elements pertain to the failure modes "high cycle fatigue," "impact fracture," "thermal shock," and "yielding." Five of the 8 function-failure mode pairs are focused on high cycle fatigue, while 1 of each is focused on the three other failure modes. Of these, only thermal shock has no data currently in the knowledge base, and so will be excluded from this analysis.

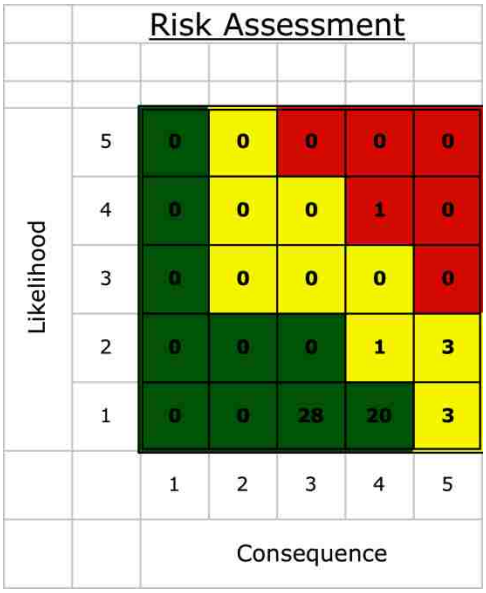


Figure 4. Wind Turbine RED Analysis Fever Chart

Table 1. Wind Turbine RED Analysis High Risk Results

Transfer Mechanical Energy fails due to High Cycle Fatigue	(4, 4)
Import Gas fails due to High Cycle Fatigue	(5, 2)
Guide Gas fails due to High Cycle Fatigue	(5, 2)
Export Gas fails due to High Cycle Fatigue	(5, 2)
Transfer Mechanical energy fails due to Impact Fracture	(5, 1)
Regulate Mechanical energy fails due to High Cycle Fatigue	(5, 1)
Regulate Mechanical energy fails due to Thermal Shock	(5, 1)
Transfer Mechanical energy fails due to Yielding	(4, 2)

The next step is to determine the potential mitigation strategies. Turning to the **FS** matrix made from the current set of failure mode models and mitigation strategy taxonomy, the potential mitigation strategies applicable to the mitigation of the above four failure modes can be found. Shown below in Tables 2, 3, and 4 are the collection of mitigation strategies provided by the **FS** matrix with the number of occurrences, as well as the likelihood and consequence changes provided from the **SC** matrix (YES and NO are shown where there is no numerical data, but it is known that the mitigation strategy had an effect). There were 20 mitigation strategies for high cycle fatigue, 14 for impact fracture, and 15 for yielding. While there is overlap between the three mitigation strategies, the number of occurrences changes for each failure mode, which will lead to different popularity ratings for the different failure modes.

Currently, due to lack of numerical data, only convert material and convert part have a numerical value for their likelihood and consequence change values. The

objective of this paper is to demonstrate the method, not to provide an exhaustive list of consequence and likelihood change values. In future work, this problem will be addressed.

Table 2. Mitigation Strategies for High Cycle Fatigue, with Number of Occurrences, Likelihood, and Consequence Change Values

Strategy	Number of occurrences	Consequence Change	Likelihood Change
Change Natural Frequency	1	NO	YES
Condition Material	4	NO	YES
Condition Part	3	NO	YES
Convert Material	8	4%	4%
Convert Part	4	NO	2%
Couple Part	1	NO	YES
Decrease Motion	1	NO	YES
Decrease Power Assist	1	NO	YES
Import Lubricant	1	NO	YES
Import Material	1	NO	YES
Import Part	1	NO	YES
Import Stress	1	NO	YES
Increase Controls	2	YES	YES
Increase Flow	1	NO	YES
Remove Part	1	YES	YES
Secure Part	4	YES	YES
Separate Contaminant	1	NO	YES
Shape Part	14	NO	YES
Stabilize Process	1	NO	YES
Stop Process	1	NO	YES

Table 3. Mitigation Strategies for Impact Fracture, with Number of Occurrences, Likelihood, and Consequence Change Values

Strategy	Number of occurrences	Consequence Change	Likelihood Change
Condition Material	4	NO	YES
Condition Part	5	NO	YES
Convert Material	5	4%	4%
Convert Part	4	NO	2%
Decrease Power Assist	1	NO	YES
Import Lubricant	1	NO	YES
Increase Controls	2	YES	YES
Increase Flow	1	NO	YES
Position Part	1	NO	YES
Remove Part	1	YES	YES
Separate Contaminant	1	NO	YES
Shape Part	8	NO	YES
Stabalize Flow	1	NO	YES
Stabilize Process	1	NO	YES

Table 4. Mitigation Strategies for Yielding, with Number of Occurrences, Likelihood, and Consequence Change Values

Strategy	Number of occurrences	Consequence Change	Likelihood Change
Condition Material	5	NO	YES
Condition Part	4	NO	YES
Convert Material	4	4%	4%
Convert Part	2	NO	2%
Couple Part	1	NO	YES
Decrease Load	1	NO	YES
Decrease Motion	1	NO	YES
Decrease Torque	1	NO	YES
Import Lubricant	4	NO	YES
Increase Controls	2	YES	YES
Increase Load	1	NO	YES
Increase Torque	1	NO	YES
Position Part	1	NO	YES
Secure Part	1	YES	YES
Shape Part	10	NO	YES

Using this data, the popularity, new likelihood, and new consequence values are

calculated, to use in comparing the strategies. For each of these strategies, the likelihood change and consequence change values are used to determine the new likelihood and consequence for each failure mode, and the number of occurrences are used to evaluate the popularity. As an example here, the strategies Convert Material and Convert Part and the function-failure mode pair "transfer mechanical energy fails due to high cycle fatigue" will be used to show the calculations for popularity as well as the new likelihood and consequence values, as their likelihood and consequence change data has been collected from real world data.

For the popularity, shown in equations (4) and (5), the number of occurrences for convert material is 8, and 4 for convert part. In both cases, the maximum number of occurrences belongs to shape part, with 14. Evaluating these values, the popularity for these two functions is X and Y, respectively.

$$Pop_{Convert\_Material} = \text{int}\left\{5\frac{8}{14}\right\} = 3 \tag{4}$$

$$Pop_{Convert\_Part} = \text{int}\left\{5\frac{4}{14}\right\} = 2 \tag{5}$$

For the first function-failure mode pair, transfer mechanical energy failing due to high cycle fatigue, the likelihood of risk is 4 and the consequence is 4. Shown in equations (6) and (7) are the calculations and results for the likelihood and consequence of applying the convert material strategy. Similarly, equation (8) shows the process for convert part. There is no calculation for the new consequence of convert part, as that strategy does not reduce the consequence. As shown in the equations below, the new likelihood and consequence values are very close to the original likelihood and consequence of risk. While this does show which has a higher reduction of the risk, the

values are not enough to change the integer value of the likelihood and consequence that RED uses.

$$L_{Convert\_Material} = 4 \bullet (1 - .04) = 3.84 \quad (6)$$

$$C_{Convert\_Material} = 4 \bullet (1 - .04) = 3.84 \quad (7)$$

$$L_{Convert\_Part} = 4 \bullet (1 - .02) = 3.92 \quad (8)$$

Following these examples, the process is repeated for each mitigation strategy and each function failure mode pair. Shown below in tables 5, 6, and 7, are the results for the function transfer mechanical energy failing due to high cycle fatigue, impact fracture, and yielding. Similar tables can be constructed for each of the other function-failure mode pairs.

Table 5. GREEN Results for "Transfer Mechanical Energy fails due to High Cycle Fatigue"

Strategy	Popularity	New Consequence	New Likelihood
Change Natural Frequency	1	4	<4
Condition Material	2	4	<4
Condition Part	2	4	<4
Convert Material	3	3.84	3.84
Convert Part	2	4	3.92
Couple Part	1	4	<4
Decrease Motion	1	4	<4
Decrease Power Assist	1	4	<4
Import Lubricant	1	4	<4
Import Material	1	4	<4
Import Part	1	4	<4
Import Stress	1	4	<4
Increase Controls	1	<4	<4
Increase Flow	1	4	<4
Remove Part	1	<4	<4
Secure Part	2	<4	<4
Separate Contaminant	1	4	<4
Shape Part	5	4	<4
Stabilize Process	1	4	<4
Stop Process	1	4	<4

Table 6. GREEN Results for "Transfer Mechanical Energy Fails due to Impact Fracture"

Strategy	Popularity	New Consequence	New Likelihood
Condition Material	3	5	<1
Condition Part	4	5	<1
Convert Material	4	4.8	0.96
Convert Part	3	5	0.98
Decrease Power Assist	1	5	<1
Import Lubricant	1	5	<1
Increase Controls	2	<5	<1
Increase Flow	1	5	<1
Position Part	1	5	<1
Remove Part	1	<5	<1
Separate Contaminant	1	5	<1
Shape Part	5	5	<1
Stabalize Flow	1	5	<1
Stabilize Process	1	5	<1

Table 7. GREEN Results for "Transfer Mechanical Energy fails due to Yielding"

Strategy	Popularity	New Consequence	New Likelihood
Condition Material	3	4	<2
Condition Part	2	4	<2
Convert Material	2	3.84	1.92
Convert Part	1	4	1.96
Couple Part	1	4	<2
Decrease Load	1	4	<2
Decrease Motion	1	4	<2
Decrease Torque	1	4	<2
Import Lubricant	2	4	<2
Increase Controls	1	<4	<2
Increase Load	1	4	<2
Increase Torque	1	4	<2
Position Part	1	4	<2
Secure Part	1	<4	<2
Shape Part	5	4	<2

The final step is determining which of these results is best for the chosen failure modes. For this example, popularity, new consequence, and new likelihood have been determined for the failure modes corresponding to transfer mechanical energy. For all

three failure modes, the most popular strategy is "shape part," where the geometry of the part is altered to better reduce the risk. However, another high popularity choice affects both the consequence and likelihood, "convert material." This strategy replaces the material with a different material better suited to resisting the failure. Finally, both of these strategies are applicable to all three failure modes, meaning that they can applied to handle all three potential risks. Thus, for this case, the best selection from GREEN is "convert material."

These results were compared to a pair of cases studies that reported recommended and successful mitigation strategies applied to currently operating wind turbines. Manwell, et al. (1999) examined potential failures in a wind turbines gearbox, which is a solution to transfer mechanical energy in the presented functional model. This report showed that the gearbox was susceptible to impact fracture, and recommended using improved 1st stage carriers with spherical bearings, improving the retention by using a tighter fit or a locking mechanism, and adding a teeter damper to the design. These strategies correspond to "convert part," "position part," and "import part" in the mitigation taxonomy. As shown in Table 6, GREEN was able to predict two of these strategies, "convert part" and "position part."

The second case study reported solutions used in the field as maintenance for turbines improve (Moser, 2010). This report mentioned failures in the gearbox have been mitigated by lubrication, tapered roller bearings, and refined material processing. These strategies are represented by "import lubricant," "convert part," and "condition material." All three of these strategies were generated by GREEN, with "condition material" being the second highest recommended strategy for yielding.

As shown by these examples, GREEN can generate useful mitigation strategies for a given function-failure mode pair, and can accurately produce strategies determined by engineering experience.

5 CONCLUSIONS

This paper demonstrated the GREEN method, and provided an example of how to perform this method from a design standpoint. The GREEN method allows a designer to approach the mitigation of risks during the earliest stages of the design process. By using the mitigation strategy taxonomy as a basis, it allows historical risk mitigation data to be used to generate mitigation strategies for a new design product. Also, due to its functional nature, it can be used across disciplines, as long as the design can be broken down into a functional model.

However, as shown in the calculations of the example, the current means of recording risk changes have small changes barely affect the risk as reported by RED. This needs to be rectified, and a means of capturing and evaluating likelihood and consequence change data needs to be defined to allow for more accurate measuring of the affect of a mitigation strategy on a risk.

5.1 Future Work

In the future, a means to evaluate the likelihood and consequence changes of the mitigation strategies needs to be developed, to allow for maximum use of the GREEN method. In addition, more strategies need to be added to the taxonomy, to increase the accuracy of the popularity data and the number of different strategies that are available.

Finally, a means to evaluate the consequence and likelihood reduction of a mitigation strategy needs to be determined.

ACKNOWLEDGEMENTS

The authors would like to thank the contributions of Delvrick Bozeman for his assistance with the mitigation strategy taxonomy.

REFERENCES

Analyst: Recall Costs Toyota $155M a Week As Fix for Gas Pedal Problem Underway, Japanese Auto Giant Braces for Public Backlash. (2010). Retrieved September 22, 2010, from http://www.cbsnews.com/stories/2010/02/02/business/main6165930.shtml

Bedford, T., & Cooke, R. (2001). Probabilistic Risk Analysis: Foundations and Methods. Cambridge: Cambridge University Press.

BP oil spill timeline. (2010). Retrieved November 3, 2011 from http://www.guardian.co.uk/environment/2010/jun/29/bp-oil-spill-timeline-deepwater-horizon

Brody, S. D., S. Zahran, et al. (2009). "Policy Learning for Flood Mitigation: AA Longitudinal Assessment of the Community Rating System in Florida." Risk Analysis 29(6): 912-929.

Coit, D. W. (2000). System Reliability Prediction Prioritization Strategy. Paper presented at the Annual Reliability and Maintainability Symopsium.

Coit, D. W., & Smith, A. (1996). Penalty Guided Genetic Search for Reliability Design Optimization. Computers and Industrial Engineering, 30.

Depatmnet of Defense. (1949). Proceedures for performing failure mode, effects, and criticality analysis.

Dillon, R. L., R. M. Liebe, et al. (2009). "Risk-Based Decision Making for Terrorism Applications." Risk Analysis 29(3): 321-335.

Fukushima Accident 2011. (2011). Retrieved November 3, 2011 from www.world-nuclear.org/info/fukushima_accident_inf129.html.

Grantham Lough, K. (2005). Risk in Early Design. Unpublished Dissertation, University of Missouri-Rolla, Rolla, MO.

Grantham Lough, K., (2007). Detailed Risk Analysis for Failure Prevention in Conceptual Design: RED (Risk in Early Design) Based Probablistic Risk Assessments. Paper presented at the International Design Engineering Technical Conference, Las Vegas, NV, USA.

Grantham Lough K, et al., (2009). "Promoting risk communication in early design through linguistic analyses " Research in Engineering Design, vol. 20, pp. 29-40.

Keane, A. G., & Plungis, J. (2010). Toyota Sudden Acceleration Tied to 43 Fatal Crashes. Retrieved Spetember 22, 2010, from http://www.businessweek.com/news/2010-03-02/toyota-sudden-acceleration-tied-to-43-fatal-crashes-u-s-says.html

Krus D. and Grantham K., (2010). "A Step Toward Risk Mitigation During Conceptual Product Design: Component Selection for Risk Reduction," in IDETC 2010, Montreal, Qubec.

Krus D. and Grantham K., (2011). "Towards failure free design: an analysis of risk mitigation communication." In IDETC 2011, Washington DC, 2011.

Krus D. and Grantham K., (2012). "The Mitigation Strategy Taxonomy: Organizing and Classifying Risk Mitigation Strategies." In ISERC 2012, Orlando, FL, 2012.

Manwell J. F., Rogers A., Abdulwahid U., Ellis A.and. McNiff B. P, (1999). "Wind Turbine Gearbox Evaluation," Proc. European Wind energy Conference, Nice, France.

Moser, B., (2010). "Turbine Failure: Fine-tuning turbine gearbox performance," Retrieved February 23, 2012, from http://social.windenergyupdate.com/om/turbine-failure-fine-tuning-turbine-gearbox-performance.

Nas, T. (1996). Cost-Benefit Analysis: Theory and Application. Thousand Oaks, CA, Sage Publications, Inc.

Stock, M., Stone, R., & Tumer, I. (2003). "Going Back in Time to Improve Design: The Elemental Function-Failure Design Method." In IDETC, Chicago, IL, USA, 2003.

Stone, R. and Wood, K., (1999). "Development of a Functional Basis for Design," Proceedings of DETC99, DETC99/DTM-8765, Las Vegas, NV.

Qiu, Y., Ge, P., & Yim, S. C. (2007). Risk-Based Resource Allocation for CollaborativeSystem Design in Distributed Environment. Paper presented at the Internation Design Engineering Technical Conference, Las Vegas, NV, USA.

Wang, J. X., & Roush, M. L. (2000). What Every Engineer Should Know About Risk Engineering and Management. New York, NY: Marcel Dekker, Inc.

W. E. Vesley, e. a. (1981). Fault Tree Handbook.

USNRC. (1975). Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, Appendix I: Accident Definition and Use of Event Trees.

PAPER V

FAILURE PREVENTION THROUGH THE CATALOGING OF SUCCESSFUL RISK MITIGATION STRATEGIES

Daniel Krus

Department of Mechanical Engineering

Missouri University of Science and Technology

Katie Grantham, Ph.D.

Assistant Professor of Engineering Management and Systems Engineering

Missouri University of Science and Technology

ABSTRACT

The objective of this paper is to introduce the method to add mitigation strategy data to the Generated Risk Event Effect Neutralization (GREEN) method knowledgebase, to improve its ability to effectively mitigate risks. Risk mitigation is the creation and selection of mitigation strategies to reduce, measure, or control risks in a system. Currently, the vast majority of risk mitigation strategies are created based on the engineering expertise of the engineers on a project. The Generated Risk Event Effect Neutralization (GREEN) method provides a means for an engineer to supplement their experience by generating risk mitigation strategies based on past successful risk mitigation strategies using the failure modes of the potential risks that the product faces. In order to better aid the engineer in selecting the best possible risk mitigation strategy for a particular risk, more information on mitigation strategies need to be catalogued in

the GREEN knowledgebase. This paper outlines and demonstrates the method for adding new data on mitigation strategies to the knowledgebase, and presents a case study of how this information is added and used to mitigate product risks.

Keywords Risk Mitigation, Failure Analysis, Risk Linguistics

1 INTRODUCTION

The objective of this paper is to introduce the method to add mitigation strategy data to the Generated Risk Event Effect Neutralization (GREEN) method knowledgebase, to improve its ability to effectively mitigate risks. The GREEN method is a tool that aids in performing risk mitigation by generating risk mitigation strategies and evaluating them based on collected historical risk mitigation data (Krus and Grantham, 2012a). As GREEN was designed for use during the earliest stages of the design process, it can aid the engineer in reducing or eliminating the unplanned failures a product might experience.

Unplanned failure is a problem in all fields of engineering, and if not addressed, can lead to disasters, loss of life, and loss of money. The recalls performed by Toyota are just one such case where these unplanned failures caused a great loss of life and resources. A design flaw in the accelerator pedal caused the vehicle to accelerate uncontrollably, and lead to the deaths of 52 individuals and injured 32 others. Approximately 4.5 million vehicles were recalled, and cost the company almost $900 million in repairs and $155 million in lost business (CBS.com, 2010).

Risk mitigation is the creation of strategies to limit risk, plan for potential

emergencies, and measuring and controlling any remaining risks in the system (Wang and Roush, 2000). These strategies reduce or remove risk from a system, either by reducing the likelihood or consequence of risk or transferring the risk to a different, less vital system. They can also be plans for when the product fails, as well as measuring the remaining risks that cannon be removed (Wang and Roush, 2000). These plans are primarily created using the experience and expertise of the engineers that generated the strategies.

The GREEN method is tool that can aid an engineer in performing risk mitigation, but for it to be more effective, additional information on successful mitigation strategies need to be added to it. By adding additional information to GREEN's knowledgebase, it will better reflect the practice of industry, and allow for more accurate calculations when used to evaluate the strategies.

2 BACKGROUND

2.1 Linguistic Terminology

Risk mitigation strategies are primarily developed by the engineers on a project, drawing from their own expertise and experience to generate potential solutions to risks. However, due to this, not all risk mitigation strategies are communicated the same way. This can create difficulty when attempting to store information on past mitigation strategies, as well as employing those strategies in new products.

The communication of these strategies, as well as storage of information related to them, is very important when attempting to mitigate risks in a product. Attempting to understand a mitigation strategy employed on an earlier product can be confusing if both

groups did not use a common vocabulary when defining and describing the strategies. To help resolve this issue, as well as improve storage of knowledge about mitigation strategies, the risk mitigation strategy taxonomy was created (Krus and Grantham, 2012b). This taxonomy has its roots in the functional basis, component taxonomy, and failure mode taxonomy.

2.1.1 Functional Basis and Other Taxonomies. The functional basis, formerly the functional taxonomy, is an attempt to create a standard language for discussing functions, the terms that are used to conceptualize, define, or understand a product in terms of function and purpose (Stone and Wood, 1999). There have been several attempts to formalize this list of definitions, dating back to the 1940s (Akiyama, 1991, Miles, 1972, VAI, 1993). Collins, et al. created a list of 105 functions that describe the mechanical functions of a helicopter, as well as store failure information (1976), which lead the way for later attempts. Later attempts tried to add structure and origination, by suggesting breaking the functions and flows into groups and classes based on a variety of methods, such as living systems theory or a departure from the verb-object format (Pahl and Beitz, 1988, Hundal, Koch et al., 1990, Kirschman and Fadel, 1998). The functional basis refined the categories of Pahl and Beitz, using the empirical study of over 100 products to add two more levels of detail (Kirschman and Fadel, 1998, Little, Wood, and McAdams, 1997). This basis has undergone additional revision since then, adding definitions for the flows (Stone, 1997), and being used for product similarity computations (McAdams, Stone, and Wood, 1999), design by analogy (McAdams and Wood, 2000), and functional tolerancing (McAdams and Wood, 1999).

The component taxonomy attempts to do for product components what the functional basis did for functions, and creates a naming convention for mechanical parts (Kurtoglu, et al., 2005). This was developed as a way to abstract a component down to a high level name to simplify information transfer, and help with concept generation during the conceptual phase of design. This taxonomy is based on the concept of a lexicon, which assumes that every artifact has a specific purpose to fulfill (Chenhall, 1978). The names were divided into four categories: Functional Form, where the name is based on the function the component performs; geometric shapes, where the name is based on the shape of the component; simple mechanics, where the names are based on the seven simple machines; and Nature, where the names are based on similar things found in nature. Using these four categories, 114 terms were collected from various literature and technical publications, as well as the expertise of the creators (Greer, et al., 2003). Using this taxonomy alongside such tools as the function-component matrix (Strawbridge, McAdams, and Stone, 2002), a concept generator can be formed, and used to rapidly generate many different designs from a single functional model (Bryant, Stone, and McAdams, 2006).

The failure mode taxonomy attempts to collect and define failure modes for electromechanical systems (Tumer, Stone, and Bell, 2003). Like the functional basis, it had its roots in the work of Collins, using the list of mechanical failures as its beginning (Collins, et al., 1976). Additional failure modes were added by empirical studying rotorcraft failure reports and accident reports from NASA's Jet Propulsion Lab (Tumer, Stone, and Roberts, 2003, Roberts, Stone, and Tumer, 2002). These were supplemented with the electrical failure modes required for the highly automated systems used by

NASA. Using this taxonomy with the functional basis and component basis allowed the creation of the Function Failure Design Method (FFDM), a means to link failure to component, and component to function, allowing the linking of function to failure, and allowing for failure analysis during the earliest stages of design (Stock, Stone, and Tumer, 2003). This was expanded into the Risk in Early Design (RED) Method, which allowed the function-failure mode pairs to be rated into low, moderate, and high risk based on the historically determined likelihood and consequence of the risk (Grantham Lough, 2005).

2.1.2 The Risk Mitigation Strategy Taxonomy. The risk mitigation strategy taxonomy is a collection of terms used to define risk mitigation strategies, based on how they mitigate a risk (Wang and Roush, 2000). The construction of the categories was based on a linguistic analysis of mitigation strategies. Krus and Grantham recommended an approach based on the pragmatics sub-field of linguistics (2011). This approach was based on similar work on risk elements performed by Grantham Lough et al. (2009). This pragmatics approach was chosen as communicating mitigation strategies is based on the context of the risk element they address, and pragmatics deals with how statements are used to communicate and how they relate to the context of a discussion (Barsalou, 1992, Wilson and Keil, 1999). This analysis used three theories of pragmatics, the Gricean Cooperation Principle (Barsalou, 1992), Functional Analysis (Green, 1996), and Relevance Theory (Wilson and Keil, 1999) to evaluate mitigation strategies.

This approach identified six attributes important to communicating a mitigation strategy. First was the failure mode the mitigation strategy tried to solve, followed by the

design parameters, aspects of the design the engineer has direct control over. The design and environment changes documented the changes made to the design or environment in an attempt to reduce, control, or monitor the risk. The likelihood and consequence changes recorded if the strategy had an effect on the likelihood or consequence of the risk (Krus and Grantham, 2011). Using these six attributes gave a common set of data to collect and use to record information about strategies.

Using these attributes, 325 strategies were collected and grouped into categories. The first grouping was based on similar actions, such as all strategies that changed the geometry of the part grouped together. These were then separated into three categories based on the different types of risk mitigation stated by Wang and Roush (2000). The strategies that performed a change to reduce or remove risks were then divided into design and environment changes. Design changes altered aspects of the design the engineer could controls, based on the design parameters of the product. Environment changes attempted an external control of the failure, by controlling an environment parameter of the failure. In addition to these categories, strategies were grouped based on the other purposes of risk mitigation: monitoring strategies implemented observation and inspection techniques to monitor a failure as it progresses and planning strategies set up plans for unavoidable failures (Wang and Roush, 2000).

Focusing on the 152 strategies that reduce or remove risks, the strategy names and definitions were further refined, using a verb-object form. The verbs were taken from the functional basis, using the function the mitigation strategy performed. The objects were empirically determined from the 325 case studies. These were combined to form 42 distinct mitigation strategies, which form the mitigation strategy taxonomy (Krus and

Grantham, 2012b).

This mitigation strategy taxonomy provides a consistent language that can be used to classify and quantify risk mitigation data, allowing it to be processed and used to evaluate strategies against each other.

2.2 Failure and Risk Mitigation Recording Matrix Techniques

Many successful failure prevention tools have used matrix techniques to store failure data and then link related concepts. Several methods of applying matrices to FMEA have been suggested, such as the Failure Experience matrix suggested by Collins et al (1976, 1993), which recorded information on the failure modes, mechanical functions, and corrective action on different axes of a three dimensional matrix, or the Automated Advanced Matrix FMEA (Goddard and Dussalt, 1984), which used the outputs of the assembly under analysis, test points under analysis, comments, remarks, and references in the columns and the inputs of the assembly being analyzed and their failure modes as the rows.

2.2.1 The Risk in Early Design Method.

The RED method is a risk analysis tool that uses historical data to predict potential failure modes for a product (Grantham Lough, 2005). In order to perform this analysis, a knowledgebase of historical data needs to be collected, containing the failure modes, components, functions, and severities of recorded failures, which are used to populate the Function-Component (**EC**), Component-Failure (**CF**), and Component-Failure Severity (**CF'**) matrices. These three matrices are used to populate the list of function-failure mode pairs, as well as calculate the likelihood and

consequence of each pair (Grantham Lough, et al., 2008a).

To populate these databases, individual case studies and failure reports are analyzed, and the important information is determined and added to the knowledgebase. The first step is to identify the component and failure mode. The report is analyzed to find the component that failed, translating it into a term from the component taxonomy. The failure mode is then identified in a similar fashion, using the failure mode taxonomy to identify the mode of the failure outlined in the report. These two elements together identify that this particular component failed by this failure mode, and is used to increment that pair in the **CF** matrix (Grantham Lough et al., 2008b).

After that, severity of the failure is determined, using an integer scale from 1 to 5, with specific definitions for each integer value. This is used with the component and failure mode to populate the **CF'** matrix with the given severity for the component-failure mode pair. The final step is determining the function of the component, using the functional basis. Once the function has been identified, the data for the function-component pair is entered as a 1 in the **EC** matrix, which is binary (Grantham Lough et al., 2008b).

The **EC** and **CF** matrices can then be multiplied together to determine the Function-Failure Mode (EF) matrix. This can be used with different mappings to determine failure modes for a given set of functions in a product, as well as their likelihood and consequence of risk. All of this is formatted so that it can be displayed on a fever chart, to allow for easier understanding of where the risk in a product lies (Grantham Lough, 2005).

2.2.2 The Generated Risk Event Effect Neutralization Method. Using the mitigation strategy taxonomy, along with the important attributes determined from the linguistic analysis, data on mitigation strategies can be collected into a knowledge base and used to help select and compare strategies based on how they change the likelihood and consequence of risk, as well as their popularity. This tool, the Generated Risk Event Effect Neutralization (GREEN) method, helps an engineer determine potential mitigation strategies for a risk by comparing the mitigation strategies in the taxonomy to what failure modes they have mitigated in the past, as well as helps the engineer compare the potential strategies based on the likelihood and consequence changes, as well as how often a strategy has been used (Krus and Grantham, 2012a).

Similar to RED, GREEN collects risk mitigation strategy data into matrices, and multiplies them together to form the links between failure modes and strategies. In order to effectively use GREEN, a well-developed knowledge base needs to exist. In order to populate the knowledgebase, risk mitigation strategies need to be cataloged into the knowledgebase in a form that can be used to perform calculations. This knowledgebase takes the form of two matrices, the Failure-Parameter (**FP**) matrix, which records the failure modes and the corresponding parameters they apply to, and the Parameter-Strategy (**PS**) matrix, which records which mitigation strategy, correspond to which parameters (Krus and Grantham, 2012a). A third matrix, the Mitigation Strategy Likelihood-consequence Change (**SC**) matrix, contains information on the likelihood and consequence changes caused by the mitigation strategy.

Using these matrices, failure modes can be linked to mitigation strategy based on the parameters they have in common. The **FP** and **PS** matrices are multiplied together

shown in equation (1), creating the Failure Mode-Mitigation Strategy (**FS)** matrix, which contains which mitigation strategies can mitigate which failure modes, and how frequently they've been encountered. Using the **FS** matrix, the popularity of a mitigation strategy can be calculated, as shown in equation (2), where N_i is the number of occurrences in the **FS** matrix for the given strategy. New likelihood and consequence values can be calculated using the **SC** matrix and the original likelihood and consequence of risk. Shown in equations (3) and (4) are the new consequence and likelihood calculations for a given mitigation strategy and failure mode. $L_{original}$ is the original likelihood of risk for a function-failure mode pair, and L_{change} is the likelihood change recorded in the **SC** matrix. Similarly, $C_{original}$ is the original consequence of risk for a function-failure mode pair, and C_{change} is the consequence change recorded in the **SC** matrix (Krus and Grantham, 2012a).

$$\mathbf{FP} \times \mathbf{PS} = \mathbf{FS} \tag{1}$$

$$Pop_i = \text{int}\left\{5\frac{N_i}{\max\limits_{1<j<n}\left(N_j\right)}\right\} \tag{2}$$

$$L_{new} = L_{original}\left(1 - L_{change}\right) \tag{3}$$

$$C_{new} = C_{original}\left(1 - C_{change}\right) \tag{4}$$

These calculations provide a set of ratings that can be used to evaluate potential mitigation strategies for a given risk. However, to provide the most accurate ratings possible, the GREEN knowledgebase should contain as much historical data as possible. Thus, new data needs to be added to the GREEN database so it can be used on a greater set of products.

3 KNOWLEDGEBASE CONSTRUCTION TO SUPPORT RISK MITIGATION THROUGH GREEN

The languages of the risk mitigation strategy taxonomy and failure mode taxonomy form the backbone of the construction of the GREEN knowledgebase. As stated previously, GREEN requires a knowledgebase of historical risk mitigation strategy information. In order to populate that knowledgebase, information from failure reports with mitigation information are needed. These reports can come from a number of different sources, such as consumer product failure reports, ASM handbooks, or corporate data.

The first portion of the knowledgebase construction is the population of the Failure-Parameter (**FP**) matrix, which contains the failure modes and the parameters that correspond to them. The second step is the recording the parameters that have correspond to a mitigation strategy in the Parameter-Strategy (**PS**) Matrix. Finally, the likelihood and consequence change information is collected for each strategy and recorded into the Likelihood-Consequence Change (**SC**) Matrix.

3.1 Population of the Failure-Parameter (FP) Matrix

The Failure-Parameter (**FP**) matrix is used in the computation of the Fail-Strategy (**FS**) matrix, which is used to link failure modes to risk mitigation strategies. The population of this matrix comes from failure mode reports, as well as existing failure mode parameter data, such as that collected in Krus and Grantham (2012a). This matrix is formed from failure modes, which make up the rows, and parameters, which make up the columns.

When populating this matrix, first the failure mode given in the report must be determined. If this is not explicitly stated, the context of the report can be used to deduce the failure mode. Next, the parameters that caused or are related to the failure mode are determined. These parameters can be the design and environment parameters used in the failure mode models, as presented Krus and Grantham (2010). This matrix is a binary matrix, only recording that a parameter was related to a failure mode, not how frequently it has occurred. Thus, in the **FP** matrix, a 1 should be entered for each combination of failure mode and parameter found, with 0 filling those with no relationship.

The excerpt below is from a failure investigation published in the *Handbook of Case Histories of Failure Analysis* (Esakul, 1993). This excerpt will be used throughout this section to demonstrate how to populate a GREEN knowledgebase.

> *A precipitation-hardened stainless steel poppet valve assembly used to shut off the flow of hydrazine fuel to an auxiliary power unit was found to leak. SEM and optical micrographs revealed that the final heat treatment designed for the AM-350 bellows material rendered the AM-355 Poppet susceptible to intergrannular corrosive attack (IGA) from a decontaminant containing hydroxyacetic acid. This attack provided pathways for which fluid could leak across the sealing surface in the closed condition. It was concluded that the current design is flight worthy if the poppet valve assembly passes a preflight helium pressure test. However, a future design should use the same material for the poppet and bellows so that the final heat treatment will produce an assembly not susceptible to IGA.*

Most probable cause: The optimal heat treat for the AM-350 bellows transforms the microstructure of the AM-355 poppet to a sensitized structure susceptible to IGA. Residual decontaminant solution attacks the sealing surface in an intergranular fashion, because the sensitized microstructure has a chromium depletion layer immediately adjacent to the grain boundary. This attack provides pathways by which fluid can leak across the sealing surface when the assembly is closed.

Remedial Action: The use of current poppet valve assemblies is acceptable if they pass the helium pressure test prior to each launch. Future efforts will focus on using the same material for the bellows and sealing surface. This material should not be susceptible to IGA. One recommendation is the use of AM-350 for the entire poppet valve assembly. This would allow optimum heat treatment of the assembly without sacrificing properties and would require less effort for requalification. Requalification is necessary for design/material changes of flight hardware (Esakul, 1993).

The process of identifying the failure mode and the corresponding parameters for this example is detailed next.

Identifying the Failure Mode: For this example, the "Most probable cause" section provided the specific detail that the failure was due to Intergranular Corrosion.

Identifying the Parameters: From the "Most probable cause" section, the case lists the heat treatment of the product as leading to the ultimate failure, as well as the material

properties of the assembly itself, giving the parameters of temperature of the poppet and the material corrosive rates.

Following this example, the intersections of "Intergrannular Corrosion" and "temperature" and "Intergrannular Corrosion" and "Material Corrosion Rate" should have a 1 entered, with the remaining entries filled with zeros.

3.2 Population of the Parameter-Strategy (PS) Matrix

The Parameter Strategy (**PS**) matrix is used to calculate the **FS** matrix. This part of the knowledgebase collects the strategies used, as well as the parameters that were affected by the strategy or that the strategy focuses on. This matrix is formed from parameters making up the rows, and mitigations strategies taken from the taxonomy making up the columns. This matrix is incremented for each time a mitigation strategy makes a change to a given parameter.

First, the mitigation strategy, chosen from the mitigation strategy taxonomy, needs to be identified. Once the mitigation strategy has been determined, the parameter that was changed by the strategy need to be identified. While, the parameters have already been determined while populating the **FS** matrix, when populating the **PS** matrix the particular parameter the strategy changed needs to be identified from that set. After the mitigation strategy and the parameter have been determined, the intersection of that strategy and parameter is incremented by 1 in the **PS** matrix.

The failure Report used in the section "Population of the Failure-Parameter (**FP**) Matrix" is used to provide and example of the mitigation strategy and affected parameters.

Identifying the Mitigation Strategy: For this example, the "Remedial Action" section provided a recommendation of "the use of AM-350 for the entire poppet valve assembly" as a means of solving the failure of this particular part. The changing of the material used in the part was identified as "Convert Material," as the recommendation was to replace an existing material with a different material.

Identifying the Affected Parameters: The "Remedial Action" recommends changing the material of the poppet assembly. This affects the corrosion rates identified in the "Population of the Failure-Parameter (**FP**) Matrix" section.

Using this information, the intersection of "Convert Material" and "Material Corrosion Rates" in the **PS** is incremented by 1.

3.3 Population of the Likelihood-Consequence Change (SC) Matrix

The Likelihood-Consequence Change Matrix (**SC**) collects the changes to the likelihood and consequence of risk that are caused by the strategy, and is used in calculating the new likelihood and consequence value for the risk. This matrix uses the mitigation strategies taken from the risk mitigation strategy taxonomy as the rows, and the likelihood and consequence changes as the columns. For this matrix, the change to the likelihood and consequence of risk are recorded for the mitigation strategy determined while populating the **PS** matrix. These values are percent changes, between 0 to 100% for each mitigation strategy.

The failure Report used in the section "Population of the Failure-Parameter (**FP**) Matrix" is used to provide and example of the likelihood and consequence changes.

Identify the Likelihood Change: The example does not list a change for the

likelihood of risk. However, by evaluating the change, the new material makes the product less susceptible to Intergrannular Corrosion. As such, the likelihood of the risk is lowered by the mitigation strategy.

Identify the Consequence Change: Similar to likelihood, no change is listed in the report itself. Evaluating the strategy, the change of the material does not change the severity of the failure, should it still occur. Thus, for this strategy, there is no consequence change.

Using this information, the likelihood and consequence change entries for "Convert Material" are recorded as "Yes" for the likelihood change (as there is a change, but the value is unknown), and a 0% for the consequence change.

3.4 Knowledgebase Construction Example

The section ''Population of the Failure Parameter (FP) matrix'' provided a sample failure report to demonstrate the population of each GREEN knowledgebase matrix as they were presented. In this section, another sample failure report is provided. The intent of this example is to demonstrate the complete process of determining the matrix entries from failure reports as well as show how the two sample failure reports come together to form the beginnings of a knowledgebase.

> *Catastrophic pitting corrosion occurred in type 304L stainless steel pipe flange assemblies in an industrial food processor. During regular service the pumped medium was pureed vegetables. In situ maintenance procedures included cleaning of the assemblies with a sodium hypochlorite solution. It was determined that the assemblies failed due to an austenite-martensite*

galvanic couple activated by a chlorine bearing electrolyte. The martensitic areas resulted from a transformation during cold-forming operations. Solution annealing after forming, revision of the design of the pipe flange assemblies to eliminate the forming operation, and removal of the source of chlorine were recommended.

Most probable cause: The most probably cause of the new stock pipe flange assembly failures was an austenite-martensite galvanic couple at the new stock pipe outer bends. The old stock pipe flange assemblies exhibited no austenite-martensite areas at the pipe outer bends; that is, the outer bends were fully austenitic. A strong contributing factor to the failure was chlorine contamination.

Remedial action: Several recommendations were offered. The pipe should be solution annealed after the forming operation. A solution anneal reverts any martensite back into austenite, eliminating the potential for an austenite-martensite galvanic couple. A fully austenitic condition usually ensures the highest possible degree of corrosion resistance. The pipe flange assembly design should be revised so that the pipe bend area material could be replaced with a molded inert plastic such as Teflon. The source of chlorine-bearing electrolyte should be removed by use of a chlorine-free cleaner that is aggressive to the pumped food product, but not the pipe. (Esakul, 1993)

Using the procedures presented in the sections ‘‘Population of the Failure Parameter (**FP**) Matrix,’’ ‘‘Population of the Parameter-Strategy Matrix,’’ ‘‘Population of the Likelihood-Consequence Change Matrix,’’ and ‘‘Knowledgebase Construction

Example,'' the knowledgebase entries are identified.

Identifying failure mode: Galvanic Corrosion. For this example, the report introduction and the "Most probable cause" section provided details that the failure was due to Galvanic Corrosion.

Identifying parameters: Given the identified failure mode, Galvanic Corrosion, and recommendations offered in the "Remedial action" section, the report does not explicitly identify any parameters, but it can be deduced from the proposed material revision that material corrosive rates can be considered the parameter that relate to the failure mode. Further, the attempt to clean the pipe shows that the environment corrosion rates are also important.

*Populating the **FP** Matrix*: In the **FP** matrix, the intersection of "Galvanic Corrosion" and "Material Corrosion Properties has a 1 entered, leaving the other entries as 0.

Identifying the mitigation strategy: For this example, the "Remedial action" section provided a few recommendations that can be translated into mitigation strategies. It states, "The pipe should be solution annealed after the forming operation." This recommends annealing of the part, which identified a strategy to be "Condition Part." This example also states "The pipe flange assembly design should be revised so that the pipe bend area material could be replaced with a molded inert plastic such as Teflon." This recommends solving the failure by "Convert Material," which indicates to change from one substance that makes up the part to another. Lastly, this section recommends, "The source of chlorine-bearing electrolyte should be removed by use of a chlorine-free cleaner that is aggressive to the pumped food product, but not the pipe," which translates

to “Extract Contaminant.” This strategy indicates to draw out foreign material whose presence can cause damage or deterioration of the product.

Identifying the affected parameters: For the three mitigation strategies, both “Condition Part” and “Convert Material” both affect the material corrosion rates. “Extract Contaminant,” on the other hand, affects the environment corrosion rates.

*Populating the **PS** matrix*: In the **PS** matrix, the intersections for “Condition Part” and “Material Corrosion Rate,” “Convert Material” and “Material Corrosion Rate,” and “Extract Contaminant” and “Environment Corrosion Rate” are each incremented by 1.

Identify the Likelihood Change: As the previous example, this example also does not list a change for the likelihood of risk. However, by evaluating the strategies, each of the strategies lower the likelihood of the risk. Again, exact values for this change are unknown; a “Yes” is recorded for each of these mitigation strategies in the **SC** matrix.

Identify the Consequence Change: Similar to likelihood, no change is listed in the report. Evaluating each strategy, the change of the material does not change the severity of the failure, should it still occur in the future. Thus, for each strategy, there is no consequence change. A 0% is recorded in the **SC** matrix for each strategy.

The results from the two presented failure cases thus far have been compiled into sample matrices to demonstrate the construction process of the knowledgebase. The **Tables 1-3** below demonstrate the sample Failure Mode-Parameter, Parameter-Mitigation Strategy, and Mitigation Strategy Likelihood-Consequence matrices, respectfully.

Table 1. Failure-Parameter Matrix From Sample ASM Failures

	Environment Corrosion Rate	Material Corrosion Rate	Temperature
Intergranular Corrosion	0	1	1
Galvanic Corrosion	1	1	0

Table 2. Parameter-Strategy Matrix From Sample ASM Failures

	Condition Part	Convert Material	Extract Contaminant
Environment Corrosion Rate	0	0	1
Material Corrosion Rate	1	1	0
Temperature	0	1	0

Table 3. Strategy Likelihood-Consequence Change Matrix From Sample ASM Failures

	Consequence Change	Likelihood Change
Condition Part	0	Yes
Convert Material	0	Yes
Extract Contaminant	0	Yes

4 KNOWLEDGEBASE DESIGN CASE STUDY APPLICATION

In an attempt to demonstrate how the GREEN method can be used to aid in risk mitigation, a GREEN analysis is performed on a wind turbine, a type of power plant that utilizes the wind currents to turn blades and power a generator. This case study will demonstrate GREEN's use in a design application, by demonstrating how mitigation strategies can be determined during conceptual design. The GREEN knowledgebase used in this example was populated from 325 mitigation strategies from different sources (Esakul, 1993, Hatamura, 2009, Miller, 2011), covering many different electromechanical failures and mitigation strategies that create changes to reduce or remove risks.

The first step in the process is a RED analysis of the wind turbine. The functional model of the wind turbine shown in Figure 1 had a RED analysis performed on it to determine the potential risks. The fever chart and the highest risks for this analysis are shown in Figure 2. As seen in the fever chart, there are 56 total risk elements, with 1 high-risk element, 7 moderate risk elements, and 48 low risk elements. The high and

moderate risks are “High Cycle Fatigue,” “Impact Fracture,” “Thermal Shock,” and “Yielding.”

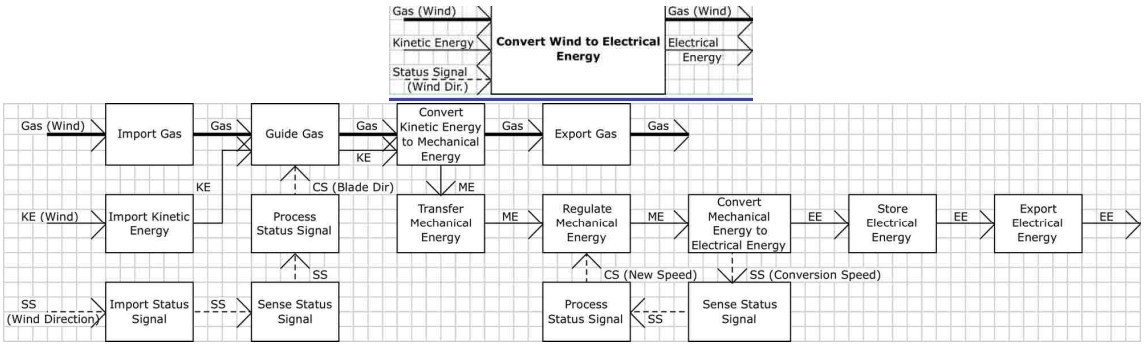
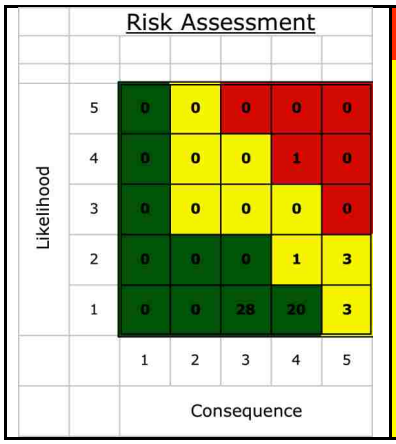


Figure 1. Wind Turbine Black Box and Functional Model



Transfer Mechanical Energy fails due to High Cycle Fatigue	(4,	4)
Import Gas fails due to High Cycle Fatigue	(5,	2)
Guide Gas fails due to High Cycle Fatigue	(5,	2)
Export Gas fails due to High Cycle Fatigue	(5,	2)
Transfer Mechanical energy fails due to Impact Fracture	(5,	1)
Regulate Mechanical energy fails due to High Cycle Fatigue	(5,	1)
Regulate Mechanical energy fails due to Thermal Shock	(5,	1)
Transfer Mechanical energy fails due to Yielding	(4,	2)

Figure 2. Wind Turbine RED Analysis Fever Chart and High and Moderate Risk Elements

Using the **FS** matrix, GREEN determined 20 mitigation strategies for High Cycle Fatigue, 14 for Impact Fracture, 0 for Thermal Shock, and 15 for Yielding. These strategies are evaluated based on their popularity, and likelihood and consequence changes, using the appropriate calculations. Shown below are the results of the analysis

for transfer mechanical energy failing due to high cycle fatigue, impact fracture, and yielding, all of which had strategies generated by GREEN. The collected results, and how they compare, are shown in Tables 4, 5, and 6. Using these strategies and ratings, along with engineering expertise, the best solutions for a given risk element can be selected.

Table 4. Mitigation Strategies for "Transfer Mechanical Energy Fails due to High Cycle Fatigue"

Strategy	**Popularity**	**New Consequence**	**New Likelihood**
Change Natural Frequency	1	4	<4
Condition Material	2	4	<4
Condition Part	2	4	<4
Convert Material	3	3.84	3.84
Convert Part	2	4	3.92
Couple Part	1	4	<4
Decrease Motion	1	4	<4
Decrease Power Assist	1	4	<4
Import Lubricant	1	4	<4
Import Material	1	4	<4
Import Part	1	4	<4
Import Stress	1	4	<4
Increase Controls	1	<4	<4
Increase Flow	1	4	<4
Remove Part	1	<4	<4
Secure Part	2	<4	<4
Separate Contaminant	1	4	<4
Shape Part	5	4	<4
Stabilize Process	1	4	<4
Stop Process	1	4	<4

Table 5. Mitigation Strategies for "Transfer Mechanical Energy Fails due to Impact Fracture"

Strategy	Popularity	New Consequence	New Likelihood
Condition Material	3	5	<1
Condition Part	4	5	<1
Convert Material	4	4.8	0.96
Convert Part	3	5	0.98
Decrease Power Assist	1	5	<1
Import Lubricant	1	5	<1
Increase Controls	2	<5	<1
Increase Flow	1	5	<1
Position Part	1	5	<1
Remove Part	1	<5	<1
Separate Contaminant	1	5	<1
Shape Part	5	5	<1
Stabilize Flow	1	5	<1
Stabilize Process	1	5	<1

Table 6. Mitigation Strategies for "Transfer Mechanical Energy Fails due to Yielding"

Strategy	Popularity	New Consequence	New Likelihood
Condition Material	3	4	<2
Condition Part	2	4	<2
Convert Material	2	3.84	1.92
Convert Part	1	4	1.96
Couple Part	1	4	<2
Decrease Load	1	4	<2
Decrease Motion	1	4	<2
Decrease Torque	1	4	<2
Import Lubricant	2	4	<2
Increase Controls	1	<4	<2
Increase Load	1	4	<2
Increase Torque	1	4	<2
Position Part	1	4	<2
Secure Part	1	<4	<2
Shape Part	5	4	<2

For each of these three function-failure mode pairs, "Shape Part" is the most popular strategy. However, this strategy only affects the likelihood of the risk. "Convert Material," on the other hand, is either the second or third highest popularity strategy, and affects both the consequence and likelihood of risk, making the failure less likely to happen and less critical when it does happen. Given the choices above, "Convert Material" would be the best option of these strategies.

To verify this analysis, it was compared to 2 case studies that were not included in

the GREEN knowledgebase. These two cases evaluate failures of the turbine's gearbox due to several failure modes, such as impact fracture, yielding, and high cycle fatigue. The gearbox accomplishes transfer mechanical energy in the functional model in Figure 1. The first case study dealt with impact fracture, and recommended strategies of using improved 1st stage carriers with spherical bearings, improving retention be using a tighter fit or a locking mechanism, and adding a teeter damper to the design (Manwell et al, 1999). Translating these strategies into the mitigation strategy taxonomy, they become "Convert Part," "Position Part," and "Import Part," respectively. Examining the results for impact fracture, two of those strategies, "Convert Part" and "Position Part" were generated by the GREEN analysis.

The second case study features solutions for the gear box that were generated as maintenance for gearboxes improve (Moser, 2010). This case study gave solutions of using lubrication, tapered roller bearings, and refined material processing. Converting into the mitigation strategy taxonomy, these become "Import Lubricant," "Convert Part," and "Condition Material." Examining the results for all three failure modes that transfer mechanical energy fails from, these three mitigation strategies are all generated by GREEN for all three failure modes.

As shown here, the GREEN method allows quick generation and evaluation of mitigation strategies for risk elements, including being able to generate mitigation strategies for systems that were not included in its knowledgebase. As it is independent of the experience of the engineer using the tool, even engineers with little training in risk mitigation can perform an analysis and determine potential mitigation strategies. Supplementing this with the engineer's own experience, more detailed plans can be

created from these strategies, expanding on this initial generation of strategies, allowing for better mitigation strategy generation.

5 CONCLUSIONS

The GREEN method provides an intuitive method for cataloging risk mitigation strategies so that these solutions to past failures can be used to prevent future risks. Current risk mitigation methods rely on the expertise of teams of engineers to generate the strategies to mitigate risks. This process can lead to subjective results that can overlook aspects of the risk, or not consider potential solutions for a risk. The GREEN method provides a means to use historical data to cover the potential gaps.

The GREEN method is not intended as a replacement for the expertise of engineering teams and other mitigation methods. It is intended to be used to perform risk mitigation early in the design process, allowing the mitigation of a failure to be taken into account throughout the design process. With a properly developed knowledgebase of mitigation strategy data, a team can generate mitigation strategies based on successful historical mitigation strategies, supplementing their experience with historical knowledge. GREEN provides a useful tool in the designer's toolbox for combating unexpected failures in a product. Therefore, GREEN promotes failure prevention through the cataloging of successful mitigation strategies.

6 FUTURE WORK

Future work on this project is a more complete knowledgebase of risk mitigation strategy data, as such a knowledgebase can always be improved. In addition to this, a

numerical scale for determining the likelihood and consequence changes will be determined, to allow mitigation strategies that lower the likelihood or consequence of risk but do not state how much to be measured.

REFERENCES

Akiyama, K., 1991. Function Analysis: Systematic Improvement of Quality Performance. Productivity Press.

Analyst: Recall Costs Toyota $155M a Week As Fix for Gas Pedal Problem Underway, Japanese Auto Giant Braces for Public Backlash. (2010). Retrieved September 22, 2010, from http://www.cbsnews.com/stories/2010/02/02/business/main6165930.shtml

Barsalou LW, 1992. Cognitive Psychology: An overview for Cognitive Scientists. Lawrence Erlbaum Associates, Inc.

Bryant, C., Stone, R., McAdams, D., 2006, "Automated concept generation from the functional basis of design," Accepted to Research in Engineering Design.

Chenhall, R. G., 1978, Nomenclature for Museum Cataloging: A System for Classifying Man-Made Objects, American Association for State and Local History, Nashville, TN.

Collins, J.A.: Mechanical Reliability and Design. Wiley (1993)

Collins, J., Hagan, B., and Bratt, H., 1976, "The Failure-Experience Matrix - a Useful Design Tool," Transactions of the ASME, Series B, Journal of Engineering in Industry, 98:1074-1079.

Goddard, P.L., Dussalt, H.B.: The automated matrix FMEA-A logistics engineering tool. In: Proceedings of the Society of Logistics Engineers' 19th Annual Symposium (1984).

Grantham Lough, K., 2005. "Risk in Early Design." Unpublished Dissertation, University of Missouri-Rolla, Rolla, MO.

Grantham Lough K, et al., 2009. "Promoting risk communication in early design through linguistic analyses " Research in Engineering Design, vol. 20, pp. 29-40.

Grantham Lough, K., Stone, R., and Tumer, I., 2008a, "Prescribing and Implementing the Risk in Early Design (RED) Method," Accepted to Journal of Industrial and Systems Engineering.

Grantham Lough, K., Stone, R., and Tumer, I., 2008b, "Failure Prevention through Effective Cataloguing and Utilization of Historical Failure Events," publication pending, Journal of Failure Analysis and Prevention.

Green DW, Cognitive Science: An Introduction: Blackwell Publishers Ltd, 1996.

Greer, J., Stock, M., Stone, R. and Wood, K., 2003, "Enumerating the Component Space: First Steps Toward a Design Naming Convention for Mechanical Parts," Accepted to Proceedings of DETC2003, Chicago, IL.

Handbook of Case Histories in Failure, 1993. 2. Ed. Khlefa A. Esaklul. Ohio: Materials Park.

Hatamura, Y., 2009. Learning from Design. Springer.

Hundal, M., 1990, "A Systematic Method for Developing Function Structures, Solutions and Concept Variants," Mechanism and Machine Theory, 25(3):243-256.

Kirschman, C., Fadel, G., 1998. "Classifying Functions for Mechanical Design," Journal of Mechanical Design, Transactions of the ASME, 120(3):475-482.

Krus, D. and Grantham, K. "Generated Risk Event Effect Neutralization: Identifying and Evaluating Risk Mitigation Strategies During Conceptual Design," in INCOSE 2012, Rome, Italy, 2012a.

Krus, D. and Grantham K., "A Step Toward Risk Mitigation During Conceptual Product Design: Component Selection for Risk Reduction," in IDETC 2010, Montreal, Qubec, 2010.

Krus, D. and Grantham, K., "Towards failure free design: an analysis of risk mitigation communication." In IDETC 2011, Washington DC, 2011.

Krus, D. and Grantham, K., "The Mitigation Strategy Taxonomy: Organizing and Classifying Risk Mitigation Strategies." In ISERC 2012, Orlando, FL, 2012b.

Kurtoglu, T., Campbell, M.I., Bryant, C.R., Stone, R.B., McAdams, D.A., 2005, "Deriving a Component Basis for Computational Functional Synthesis," Proceedings of International Conference on Engineering Design, ICED05, August 15-18, Melbourne, Australia.

Little, A., Wood, K., and McAdams, D., 1997. "Functional Analysis: A Fundamental Empirical Study for Reverse Engineering, Benchmarking and Redesign," Proceedings of the ASME Design Theory and Methodology Conference, Sacramento, California.

Manwell, J. F., Rogers, A., Abdulwahid, U., Ellis, A., and. McNiff, B. P., 1999. "Wind Turbine Gearbox Evaluation," Proc. European Wind energy Conference, Nice, France.

McAdams, D., Stone, R., and Wood, K., 1999, Functional Interdependence and Product Similarity Based on Customer Needs, Research in Engineering Design 11(1):1-19.

McAdams, D. and Wood, K., 1999. “Methods and Principles for Concurrent Functional Tolerance Design,” Proceedings of the 1999 ASME Design For Manufacturing Conference,” number 99-DETC/DFM49, Las Vegas, Nevada.

McAdams, D. and Wood, K., 2000. “Quantitative Measures for Design by Analogy,” Proceedings of the 2000 ASME Design Theory and Methodology Conference, number DETC2000/DTM-14562, Baltimore, Maryland, September.

Miles, L., 1972, Techniques of Value Analysis Engineering, McGraw-Hill.

Miller, Ryan, 2011. "Super Lightweight Tank Risk Management Case Study." NASA. Retrieved 22 June. 2011. <http://www.nasa.gov/externalflash/irkm-slwt/index.html>.

Moser, B., 2010. “Turbine Failure: Fine-tuning turbine gearbox performance,” Retrieved February 23, 2012, from http://social.windenergyupdate.com/om/turbine-failure-fine-tuning-turbine-gearbox-performance.

Pahl, G. and Beitz, W., 1988. Engineering Design: A Systematic Approach, Springer-Verlag.

Roberts, R. A., Stone, R. B. and Tumer, I. Y., 2002. “Deriving Function-Failure Information for Failure-Free Rotorcraft Component Design,” Proceedings of the 2002 ASME Design Engineering Technical Conferences, Design for Manufacturing Conference, DETC2002/DFM-34166, Montreal, Canada.

Stock, M., Stone, R. and Tumer, I., 2003. “Going Back in Time to Improve Design: The Elemental Function-Failure Design Method,” Proceedings of DETC2003, DETC2003/DTM-48638, Chicago, IL.

Stone, R., 1997. “Towards a Theory of Modular Design,” Doctoral Thesis, The University of Texas at Austin.

Stone, R. and Wood, K., 1999. “Development of a Functional Basis for Design,” Proceedings of DETC99, DETC99/DTM-8765, Las Vegas, NV.

Strawbridge, B., McAdams, D. and Stone, R., 2002. “A Computational Approach To Conceptual Design,” Proceedings of DETC2002, DETC2002/DTM-34001, Montreal, Canada.

Tumer, I., Stone, R. and Bell, D., 2003. “Requirements for a Failure Mode Taxonomy for Use in Conceptual Design,” Proceedings of the International Conference on Engineering Design, ICED 03, Paper 1612, Stockholm, Sweden.

Tumer, I. Y., Stone, R. and Roberts, R. A., 2003. “Analysis of JPL's Problem and Failure Reporting Database,” Submitted to Proceedings of the 2003 ASME Design Engineering Technical Conference, Design for Manufacturing Conference, Chicago, IL.

VAI (Value Analysis Incorporated), 1993. Value Analysis, Value Engineering, and Value Management, Clifton Park, New York.

Wang, J. X., & Roush, M. L. (2000). What Every Engineer Should Know About Risk Engineering and Management. New York, NY: Marcel Dekker, Inc.

Wilson R and Keil F, 1999. The MIT Encyclopedia of the Cognitive Sciences. Cambridge, Mass: The MIT Press.

2. CONCLUSIONS

This dissertation presented the risk mitigation strategy taxonomy and the GREEN method. The taxonomy is a useful tool that enables communication of mitigation strategies between groups, and allows for the collection of mitigation strategy data. Using this processed data allows for the generation of mitigation strategies, as shown by the GREEN method.

These two parts form the components and tools to helping construct a successful mitigation for a product. The risk mitigation strategy taxonomy provides the building blocks, identifying the potential plans that can be put into action. GREEN then evaluates which of those plans are applicable to the given situation, and how they compare to each other.

The risk mitigation strategy taxonomy and GREEN are not meant as replacements for currently used means of generating and evaluating mitigation strategies, but as tools to supplement and enhance it, using historical data to help cover gaps in an individual engineer's experience. By using these tools in conjunction with other tools and engineering experience, a better mitigation can be performed on a product, leading to a more failure free product.

APPENDIX A.
FAILURE MODE MODELS

Table A1. Failure Mode Models

Failure Mode	Equation	Description
Mechanical Failure Modes		
Buckling [34]	$P_{cr} = \frac{\pi^2 EI}{L_e^{\,2}}$	P_{cr} = max critical load (S) E = modulus of elasticity (D) I = moment of inertia (D) L_e = effective length of column (D)
Corrosion (Biological, Cavitation, Corrosion Fatigue, Crevice, Direct Chemical Attack, Erosion Corrosion, Galvanic, Hydrogen Damage, Intergranular, Pitting, Selective Leaching, Stress Corrosion) [35]	Corrosion rates exist for different materials and environments	-
Brinelling [36]	Brinnell Hardness Test/ Material Hardness	Harder materials are more resistant to Brinelling. (D)
Force Induced Elastic Deformation [34]	$\delta = \int_0^L \frac{Pdx}{AE}$	δ = deformation length (S) P = load (S) A = cross sectional area (D) E = modulus of elasticity (D) L = length of member (D)
Yielding [37]	Maximum Sheer Stress	τ_{max} = maximum sheer stress (S)

	$\tau_{\max} = \frac{\sigma_1 - \sigma_3}{2} \geq \frac{S_y}{2}$ Distortion-Energy $\left[\frac{(\sigma_1 - \sigma_2)^2 + (\sigma_2 - \sigma_3)^2 + (\sigma_3 - \sigma_1)^2}{2}\right]^{1/2} \geq S_y$ Coulomb-Mohr $\frac{\sigma_1}{S_t} - \frac{\sigma_3}{S_c} = 1$	$\sigma_1 > \sigma_2 > \sigma_3$ = principal stresses (S) S_y = yield strength (D) S_c = compressive strength (D) S_t = tensile strength (D)
Fatigue (High Cycle, Impact, Surface, Thermal) [26]	Stress Life Method $\frac{\partial a}{\partial N} = C(\Delta K)^m$	a = crack growth (S) C & m = material properties (D) K = Stress intensity factor (D) N = number of cycles (S)
Fatigue (High Cycle, Impact, Low Cycle, Surface, Thermal) [26]	Strain Life Method $\frac{\Delta\varepsilon}{2} = \frac{\sigma'_f}{E}(2N)^b + \varepsilon'_f (2N)^c$	ε = strain (S) σ_f, b, ε_f, c = material constants (D) E = modulus of elasticity (D) N = number of cycles (S)
Galling [27]	$V = Klw / p$	V = volume lost (S) K = wear coefficient (D) l = sliding distance (D) w = normal load (S) p = indentation hardness (D)
Seizure [28]	$P_m \geq \sigma_{YP}$ or $\frac{W}{A_a} \geq \sigma_{YP}$	P_m = nominal contact pressure (D) σ_{YP} = uniaxial yield point stress (D) W = load (S) A_a = apparent contact area (D)
Impact Deformation [28]	$V = \int_0^{\varepsilon_1} \sqrt{\frac{\frac{d\sigma}{d\varepsilon}}{\rho}} d\varepsilon$	V = impact velocity (S) σ = stress (S) ε = strain (S) ρ = density of material (D)

Impact Fracture [28]	$V_{\max} = \int_0^{\varepsilon_m} \sqrt{\frac{\frac{d\sigma}{d\varepsilon}}{\rho}} d\varepsilon$	V_{max} = critical impact velocity (S) σ = stress (S) ε = strain (S) ρ = density of material (D)
Brittle Fracture [37]	Maximum Normal Stress $\sigma_1 \geq S_{ut}$ or $\sigma_3 \leq -S_{uc}$ Brittle Coulomb-Mohr $\sigma_A = \frac{S_{ut}}{n}$ when $\sigma_A \geq \sigma_B \geq 0$ $\frac{\sigma_A}{S_{ut}} - \frac{\sigma_B}{S_{uc}} = \frac{1}{n}$ when $\sigma_A \geq 0 \geq \sigma_B$ $\sigma_B = -\frac{S_{uc}}{n}$ when $0 \geq \sigma_A \geq \sigma_B$ Modified I-Mohr $\sigma_A = \frac{S_{ut}}{n}$ when $\sigma_A \geq \sigma_B \geq 0$ $\sigma_A \geq 0 \geq \sigma_B$ and $\left\|\frac{\sigma_B}{\sigma_A}\right\| \leq 1$ $\frac{(S_{uc} - S_{ut})\sigma_A}{S_{uc}S_{ut}} - \frac{\sigma_B}{S_{uc}} = \frac{1}{n}$ when $\sigma_A \geq 0 \geq \sigma_B$ and $\left\|\frac{\sigma_B}{\sigma_A}\right\| > 1$ $\sigma_B = -\frac{S_{uc}}{n}$ when $0 \geq \sigma_A \geq \sigma_B$ Modified II-Mohr $\sigma_A = \frac{S_{ut}}{n}$ when $\sigma_A \geq \sigma_B \geq 0$ $\sigma_A \geq 0 \geq \sigma_B$ and $\left\|\frac{\sigma_B}{\sigma_A}\right\| \leq 1$ $\frac{n\sigma_A}{S_{ut}} - \left(\frac{n\sigma_B + S_{ut}}{S_{ut} - S_{uc}}\right)^2 = 1$ when $\sigma_A \geq 0 \geq \sigma_B$ and $\left\|\frac{\sigma_B}{\sigma_A}\right\| > 1$ $\sigma_B = -\frac{S_{uc}}{n}$ when $0 \geq \sigma_A \geq \sigma_B$	$\sigma_A > \sigma_B$ = plane stresses (S) S_{uc} = ultimate compressive strength (D) S_{ut} = ultimate tensile strength (D) n = factor of safety (D)
Ductile Rupture [38]	$K \geq K_{IC}$	K = stress intensity factor (S) K_{IC} = critical stress intensity factor (D)

Abrasive Wear [28]	$d_{abr} = \frac{\tan\theta_m}{3\pi\sigma_{YP}}\left(\frac{W}{A_a}\right)L_s$	d_{abr} = abrasive wear depth (S) $\tan\theta_m$ = weighted mean value of asperities (D) σ_{YP} = uniaxial yield point stress (D) W = load (S) A_a = apparent contact area (D) L_s = sliding distance (D)
Adhesive Wear [28]	$d_{adh} = \frac{k}{9\sigma_{YP}}\left(\frac{W}{A_a}\right)L_s$ and $\left(\frac{W}{A_a}\right) < \sigma_{YP}$	d_{adh} = adhesive wear depth (S) k = wear constant (D) σ_{YP} = uniaxial yield point stress (D) W = load (S) A_a = apparent contact area (D) L_s = sliding distance (D)
Impact Wear [39]	$W = \left(\frac{k\overline{P}Nx}{H} + KNe^n\right)\left(\frac{A_i}{A}\right)^j$	W = wear mass (S) K = sliding wear coefficient (D) $\overline{P}$ = average load (S) N = number of cycles (S) X= slip (D) H = hardness of softer material (D) K, j, n = impact wear coefficients (D) A_i = initial contact area (D) A = final contact area (S)
Surface Fatigue Wear [28]	$N = \left(\frac{C}{P}\right)^3$ for bearings	N = life in cycles (S) C = constant for a given bearing (D) P = bearing load (S)
Electrical Failure Modes		
Arc Discharge [40]	$V_{\max} = \frac{V}{D}$	V_{max} = dielectric strength of material

		(D) V = voltage between surfaces (S) D = distance between surfaces (D)
Electrostatic Discharge [40]	$V_{\max} = \frac{V}{D}$	V_{max} = dielectric strength of material (D) V = voltage between surfaces (S) D = distance between surfaces (D)
Time Dependant Dielectric Breakdown [41]	$Lifetime = A \cdot 10^{-\beta E_{ox}} e^{(Ea/kT)}$	A= scaling constant (S) β = electric acceleration factor (D) E_{ox} = applied stress electric field (D) Ea = Temperature acceleration factor (D) k = Blotzmann's constant (S) T = absolute temperature (S)
Electromigration [42]	Black's Equation $MTTF = AJ^{-n}e^{\frac{E_a}{kT}}$ for a wire	$MTTF$ = Mean time to Failure (S) A = constant based on area (D) J = current density (S) E_a = activation energy (D) k = Boltzmann's constant (S) n = scaling factor (S) T = temperature (S)
Galvanic Corrosion [35]	Corrosion rates exist for different materials and environments	- (D)
Thermal Fatigue [26]	Stress Life Method $\frac{\partial a}{\partial N} = C(\Delta K)^m$ Strain Life Method $\frac{\Delta\varepsilon}{2} = \frac{\sigma'_f}{E}(2N)^b + \varepsilon'_f(2N)^c$	a = crack growth (S) C & m = material properties (D) K = Stress intensity factor (D) N = number of

		cycles (S) ε = strain (S) σ_f , b, ε_f, c = material constants (D) E = modulus of elasticity (D)
Overcurrent [43]	$I_{\max}^2 rR = \theta_{\max} - \theta_A$	I_{max} = maximum current (S) r = resistance (D) R = thermal resistance (D) θ_{max} = maximum temperature (S) θ = ambient temperature (S)

APPENDIX B.
MITIGATION STRATEGIES

Table B1. Risk Mitigation Strategies, with Mitigation Attributes

Mitigation Strategy	Failure Mode	Design Change	Environment Change	Likelihood Change	Consequence Change	Design Parameters
Project Proposal for Redesign	NONE	Yes	NONE	2%	NONE	NONE
Integrated, multi-discipline, integrated product/process team formed	NONE	Yes	Yes	2%	NONE	NONE
Develop detailed project management aspects	NONE	Yes	NONE	2%	NONE	NONE
Develop detailed work statement	NONE	Yes	NONE	4%	NONE	NONE
Initial studies and cross functional research including economics	NONE	Yes	Yes	4%	NONE	NONE
Develop plan for concept design	NONE	Yes	NONE	2%	NONE	Product design, all design parameters
Early involvement with leadership and regulatory authority	Corrosion, Free Radical Formation	Yes	NONE	10%	10%	NONE
Identify applicable regulations and requirements	Corrosion, Free Radical Formation	NONE	Yes	6%	6%	Parameters tied to safety documents
define plan to meet regulatory and safety requirements	Corrosion, Free Radical Formation	Yes	NONE	6%	6%	Parameters tied to safety documents
Validate certification process	NONE	NONE	Yes	4%	NONE	NONE
Validate design process	NONE	Yes	NONE	6%	NONE	NONE
Design the product per he requirements	NONE	Yes	NONE	2%	NONE	Product design, all design parameters
Perform careful materials selection	Corrosion	Yes	NONE	4%	4%	Product material properties
Validate build process	NONE	Yes	NONE	4%	NONE	Product manufacturing parameters
Develop a prototype for testing	Corrosion, Free Radical Formation	Yes	NONE	2%	2%	Product design, all design parameters
Supplier management controls in place	NONE	NONE	Yes	6%	6%	NONE
Develop conformity and safety test plans	NONE	Yes	NONE	8%	NONE	Burning point, drag, etc...
Perform conformity and safety tests	Corrosion	Yes	Yes	4%	4%	Burning point, drag, etc...
Identify safety and certification issues & perform failure analysis	NONE	Yes	Yes	4%	NONE	Burning point, drag, etc...
Perform technical metrics and audit	NONE	Yes	Yes	4%	NONE	NONE
Conduct product readiness review	NONE	Yes	Yes	4%	NONE	NONE
Safe Life or Durability Method (Retire part after a calculated failure life)	Fatigue	Yes	Yes	Yes	NONE	Safety Factor, Durability analysis, Toughness, crack size
Fail Safe Method (Multiple redundant elements)	Fatigue	Yes	NONE	NONE	Yes	NONE
Fail Safe Method (Fail-safe Designs, crack stoppers)	Fatigue	Yes	Yes	Yes	NONE	Inspection interval, material toughness, crack size
Damage Tolerance method (Inspection of principal structural elements, replace if crack too large)	Fatigue, Fracture	NONE	Yes	NONE	Yes	Inspection interval, crack size, stress, stress intensity factor, material properties
Corrosion protection of Aluminum (coat with pure aluminum)	Surface corrosion, pitting corrosion	Yes	NONE	Yes	NONE	Material
Corrosion protection of Steel (High strength steels coated/plated with cadmium)	Corrosion	Yes	NONE	Yes	NONE	Material
Doubler redesign (Aircraft component)	Fracture	Yes	NONE	NONE	NONE	Stress, pitch (distance between rivets),geometry
Hole preparation (cold working by mandrel and split sleeve)	Fatigue	Yes	NONE	NONE	NONE	Stress intensity factor
Airborne data recorders to monitor average stresses during missions	Low-cycle fatigue	Yes	NONE	NONE	NONE	NONE
Reaming bolt holes and using interference-fit bushings	NONE	Yes	NONE	NONE	NONE	NONE
Removal of component at first visual signs of corrosion.	Pitting corrosion	NONE	NONE	NONE	NONE	Hardness (Rockwell C)
Heat treatment of component to softer condition	Pitting corrosion	NONE	NONE	NONE	NONE	Hardness (Rockwell C)
Perform crack inspection of bore surfaces before accepting parts into use	Low-cycle fatigue	NONE	NONE	NONE	NONE	Crack size
Barrier coating with an insulating material	Galvanic corrosion, pitting corrosion, fatigue	Yes	NONE	NONE	NONE	NONE

Mitigation Strategy	Failure Mode	Design Change	Environment Change	Likelihood Change	Consequence Change	Design Parameters
Better processing controls during etching and plating procedures to reduce potential pits chance of affecting material properties	Fatigue	NONE	Yes	NONE	NONE	Material properties, crack size
Use higher quality product to prevent defects in shaft	Fatigue	Yes	NONE	NONE	NONE	Material properties
Eliminate arc strike flaws in material by rewelding flaw or grinding out	Brittle fracture	Yes	NONE	NONE	NONE	NONE
Postweld heat treatment to lower residual stresses in material	Brittle fracture	Yes	NONE	NONE	NONE	Material properties, stress
Less steep weld toe to reduce stress at the toe	Brittle fracture	Yes	NONE	NONE	NONE	Stress concentration
Use tougher steel (A516 grade 70)	Brittle fracture	Yes	NONE	NONE	NONE	Toughness
Heat treat welding seams (600 to 640 C for 1h per inch for carbon manganese steel pipe.	Stress corrosion	Yes	NONE	NONE	NONE	NONE
Reduce moment stresses and change of material	Creep, intergranular corrosion	Yes	Yes	NONE	NONE	Stress, material properties
Preweld/postweld heat treatment	Creep, intergranular corrosion	Yes	NONE	NONE	NONE	Stress, material properties
Use of higher quality steel more resistant to the temperature changes (ASTM A213 Grade T22)	Stress rupture	Yes	NONE	NONE	NONE	Material properties
Mercury removal system to protect aluminum alloy piping system installed upstream	Direct chemical attack	Yes	NONE	NONE	NONE	NONE
Better manufacturing controls to remove any fluids after hydrostatic testing	Stress corrosion	NONE	Yes	NONE	NONE	NONE
Better care in assembly to prevent dents and stress concentrations	Stress corrosion	NONE	Yes	NONE	NONE	Stress concentration
Proper support of component to avoid cyclical loading while traveling by road	Fatigue	Yes	NONE	NONE	NONE	Load
Proper crack inspection to detect crack growth	Corrosion fatigue	NONE	Yes	NONE	NONE	Crack size

APPENDIX C.
MITIGATION STRATEGY OUTPUTS

Table C1: Mitigation Strategies for Yielding

Strategy Name	Strategy Definition	Failure mode	Consequence Change	Likelihood Change	Design Parameters	Environmental Parameters
Condition Material	To render the substance that makes up the product or part appropriate for the desired use.	Impact Fracture, Thermal Fatigue	YES	YES	Tensile Strength	
Condition Part	To render a component or portion of the overall product appropriate for the desired use.	Intergranular Corrosion, Stress Corrosion, Thermal Fatigue, High Cycle Fatigue	NONE	YES	Tensile Strength	Stress
Convert Material	To change from one substance that makes up the product or part to another.	Intergranular Corrosion, Stress Corrosion, Brittle Fracture, High Cycle Fatigue	NONE	YES	Tensile Strength	Stress
Convert Part	To change from one component or portion of the overall product to another.	Brittle Fracture	NONE	YES	Tensile Strength	
Increase Controls	To enlarge a set of orders or rules that are followed to keep the product within proper specifications in response to a control signal.	Surface Fatigue, Thermal Fatigue	YES	YES	Tensile strength	
Position Part	To place a component or portion of the overall product into a specific location or orientation.	Stress Corrosion	NONE	YES		Stress
Shape Part	To mold or form a component or portion of the overall product.	Force Induced Elastic Deformation, Yielding, Brittle Fracture, High Cycle Fatigue	NONE	YES	Yield Strength	Stress

Table C2: Mitigation Strategies for High Cycle Fatigue

Strategy Name	Strategy Definition	Failure mode	Consequence Change	Likelihood Change	Design Parameters	Environmental Parameters
Change Natural Frequency	To adjust or alter the harmonic frequency of an object in a predetermined and fixed manner.	High Cycle Fatigue	NONE	YES	Stress Intensity Factor	
Condition Material	To render the substance that makes up the product or part appropriate for the desired use.	Force Induced Elastic Deformation	NONE	YES	Modulus of Elasticity	
Convert Material	To change from one substance that makes up the product or part to another.	Thermal Fatigue, Corrosion Fatigue	NONE	YES	Stress Intensity Factor	
Convert Material	To change from one substance that makes up the product or part to another.	Force Induced Elastic Deformation	NONE	YES	Modulus of Elasticity	
Couple Part	To join or bring together components or portions of the overall product such that the members are still distinguishable from each other.	Yielding	NONE	YES	Modulus of Elasticity	
Import Material	To bring in a substance that makes up the product or part from outside the system boundary.	Surface Fatigue	NONE	YES	Stress Intensity Factor	
Import Part	To bring in a component or portion of the overall product from outside the system boundary.	Corrosion Fatigue	NONE	YES	Stress Intensity Factor	
Import Stress	To bring in a force distributed through an area of a product from outside the system boundary.	High Cycle Fatigue	NONE	YES	Stress Intensity Factor	
Secure Part	To firmly fix a component's or portion of the overall product's path.	Brittle Fracture, Ductile Rupture, High Cycle Fatigue, Impact Fatigue	YES	YES	Stress Intensity Factor	
Shape Part	To mold or form a component or portion of the overall product.	Brittle Fracture, Ductile Rupture, Impact Fatigue,	NONE	YES	Stress Intensity Factor	
Stop Process	To cease, or prevent, the transfer of a step or operation in the manufacture of a product.	Thermal Fatigue	NONE	YES		Crack Growth

VITA

Daniel Adam Krus was born on November 5, 1982 in St. Louis, Missouri. The son of Barbara and Gary was raised in St. Louis and Festus, Missouri and Graduated from Festus Public High School in 2001. Krus then enrolled at Jefferson Community College, earning his Associate of Science in May 2003. He then enrolled at the University of Missouri-Rolla, and completed his B.S. in Mechanical Engineering in December 2005. Continuing his education, he remained at the University of Missouri-Rolla, and received his M.S. in Mechanical Engineering in May, 2007. Finally, he received his Ph.D. in Mechanical Engineering from Missouri University of Science and Technology in May 2012.