Proceedings of ICAD2000
First International Conference on Axiomatic Design
Cambridge, MA – June 21-23, 2000
ICAD052

A TREATISE ON SYSTEM RELIABILITY AND DESIGN COMPLEXITY

Dr. Jayant Trewn
jtrewn@wayne.edu
Department of Industrial and Manufacturing Engineering
College of Engineering
Wayne State University
4815 Fourth Street
Detroit, MI 48202

Dr. Kai Yang
kyang@mie.eng.wayne.edu
Department of Industrial and Manufacturing Engineering
College of Engineering
Wayne State University
4815 Fourth Street
Detroit, MI 48202

ABSTRACT

The quality improvement process of reliability assessment and improvement is often a post design exercise that is traditionally practiced on the component level of products as a post design validation exercise. This article defines system reliability from a function delivery perspective that lays the foundation for reliability improvement in the concept design stage.

Design vulnerability is not intentionally designed into a design but it is the result of poor conceptual design processes that result in the selection of sub-optimal designs. By sub-optimal designs we mean designs that are not entirely capable of providing designed functions with certainty. The uncertainty of the provision of functions is a measure of the design vulnerability. Of interest to design science is a method for evaluating designs from a vulnerability point of view. This article clarifies the relationship between system reliability, cost of failures and design vulnerability.

The mathematical formulation of system design vulnerability from an Axiomatic Design Principles and a Multi-Level Hierarchical (MLH) perspective is stated in the form of a function failure cost model. The MLH cost model as a measure of design vulnerability is discussed. The MLH cost model adapts itself well to design evaluation because it captures the complexity of a design from a function reliability perspective with respect to the design independence and design uncertainty dimensions and also quantifies the impact of the uncertainty to deliver the design functions. A framework for applying the system design vulnerability criteria in the evaluation of reliability of alternative concepts is explained with an application. The MLH analytical system model is explained by applying the methodology to an overhead projector design.

Keywords: System Reliability, Function Reliability, Design Complexity, Cost of Failure, Multi-level Hierarchical Model

1 INTRODUCTION

Traditional reliability method focuses on the evaluation and assessment of reliability of systems/products. Most of reliability science is based on probability oriented analysis techniques. These techniques are used to analyze actual test data or field data in order to evaluate the performance of systems/products. This approach is characterized by the cycles of build-test-evaluate-fix. Clearly, these methods significantly increase the product development cycle time and product life cycle cost; thus it undermines a company's competitive edge. Also, testing, inherent in its definition, is after-the-fact, much in opposition to Deming's philosophy of bringing quality improvements upstream.

Traditional reliability theory is fundamentally driven by two assumptions. These are:

- Binary state assumption: the operational states of a system or component are simplified into binary states: success or failure
- Independence assumption: the components comprising the system work independently and their failures have no mutual interdependence [Bhattacharya, 1996]

In reality both assumptions do not hold true in most system designs. In traditional reliability assessment models, the binary state assumption is an oversimplified assumption. The binary state model may be appropriate for reliability goal setting, or reliability allocation, but it gives very little clues for intelligent engineering design improvement decisions regarding design parameters.

Also, the failure independence assumption does not hold true in most system designs. A recent study in the automotive industry [Paul Palady, 1995] showed that in some situations, component failures cause only 15% of system failures. The remaining 85% of the causes of system failure are due to sub-system interactions, poor sub-system interface, improper part installation, etc. These failures which are caused by the subsystem interdependence also contribute to the severity of the damage, add to the cost of repair and they make failures difficult to detect. The effectiveness of current reliability methodology is reduced by the fact that (1) it is not an early stage concept design aid but rather an after-the-fact evaluation and assessment methodology; (2) the binary state failure and failure independence assumptions are oversimplified.

2 EXTENDED DEFINITION OF RELIABILITY

Reliability definition is extended in FRD methodology in order for it to be more practical in engineering concept design practice, it is called functional reliability. Functional reliability is defined as the likelihood of successfully providing necessary functions that a system or a component is intended to deliver. The concept of failure is extended to include:

- hard failure (complete failure of function)
- soft failure (performance degradation in delivering functions)

Component failures are rated in varying degrees in terms of their impact on the overall system performance and the delivery of functional needs by the concept. Also, it is assumed that the performances of various components are not necessarily independent of each other. Dependent failure is defined as the failure of sub-systems due to either the hard failure of the sub-system itself or the performance degradation of other sub-systems. Since the dependent failure may involve failures of several sub-systems, its impact on overall system performance and the cost of repair may also be higher than the cost experienced due to single component failures.

In summary, besides the hard failures of components, the extended system reliability may also be affected by:

- Excessive complexity in component structures and interfaces;
- The effect of each components failure mode on system functions and the degree of damage that is caused by interdependency of failures.

3 UNDERLYING CONCEPTS

3.1 AXIOMATIC DESIGN PRINCIPLES

Motivated by the absence of scientific design principles, Suh [1990] proposed the use of axioms as the pursued scientific foundation for engineering design. Out of the twelve axioms first suggested, Suh introduced the following two basic axioms along with six corollaries as design principles that a design needs to satisfy:

Axiom 1: The Independence Axiom - maintain the independence of the functional requirement.

Axiom 2: The Information Axiom - minimize the information content in a design

In this approach, a design is defined as the creation of synthesized solutions in the form of products, processes or systems that satisfy perceived needs through the mapping of the functional requirements (*FRs*) in the functional domain to the design parameters (*DPs*) in the physical domain, and the proper selection of *DP's* that satisfy *FR's*. The Axiomatic design process is illustrated in Figure 1.

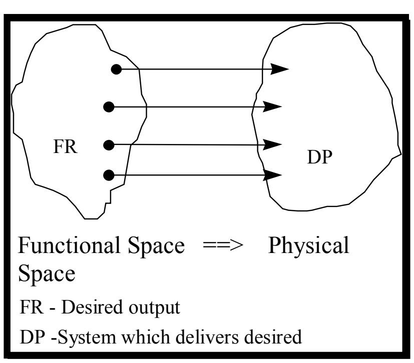

Figure 1: Axiomatic Design Process

3.2 MULTI LEVEL HIERARCHICAL (MLH) MODELLING

The conceptual design process is featured by the mapping of the functional domain (product functions) into the physical domain (actual physical entities) [Suh, 1990, Phal & Bietz, 1988, & Hubka and Eder, 1988]. As an independent development in the theory of engineering design, Hubka and Eder [1988] defined a technical system as a multi layer hierarchical (MLH) system at various levels of abstraction. The flow of customer requirements from the highest (most abstract, least concrete) level to the lowest (least abstract, most concrete) level as component structure is achieved in a conceptual design process. The layers of a MLH system are at various levels of abstraction and are shown in table 1.

Table 1: A Multi Layer Hierarchical (MLH) System

Design Layer	Abstraction	Level	Design structure
A	Highest	Functional Requirements	Functional Structure
B		Design Specifications	Organ Structure
C	Lowest	System model	Component Structure

Hubka and Eder's (1988) MLH model is a two step mapping process, which takes the design process from an abstract functional structure to a concrete component structure as illustrated in Figure 2.

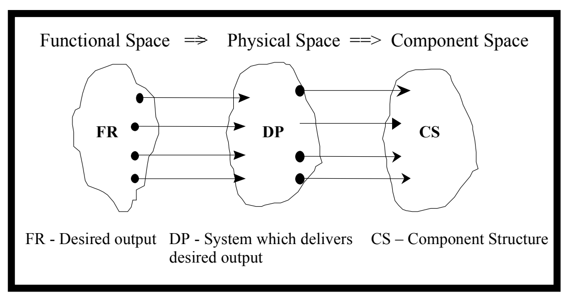

Figure 2. Mapping of Functional Requirements to component structure

3.3 ANALYTICAL MULTI LEVEL HIERARCHICAL MODELING

Trewn and Yang [1998] have developed a theoretical 2-step framework for establishing an MLH model to characterize the relationship between functional reliability and component reliability with the presence of failure dependence. This 2-step mapping provides added insights into the design process. There are many cases where several design parameters (DPs) can be encapsulated onto a single component. There are also cases where a single design parameter has to be delivered by using several components. Therefore, the structure of relationships among components is often different than that of design parameters. However, the subsystem/component structures are often the final form of an engineering design. From a reliability perspective, it is the subsystem/component structure that determines the reliability of the designed system. Hence mapping the component reliability to the function structure can help in determining function reliability of the system.

Design is defined as the mapping process between the functional requirement in the functional space to the design parameters in the design space and further to the components in the component space. Specifically, {**FR**} is the functional requirement vector. {**DP**} is the design parameter vector, and {**SS**} is the component space vector.

Let [**A**] be the design matrix that maps the design parameters to the functional requirements, so

$$\{FR\} = [A]\ \{DP\}\ \{\ aij = (0,1,)\} \tag{1}$$

Where a_{ij} is the element of the matrix [**A**] that maps the jth design parameter to the ith functional requirement. For reliability analysis purposes, the element a_{ij} is assumed to be binary, where 0 = no relationship and 1 = related. It defines the relationship between the ith functional requirement and the jth design parameter.

Further, component structure construction is defined as the mapping process between the design parameters in the design space to the component structure in the component space. Let the component space be characterized by a vector {**SS**} with k components and let [**B**] be the design matrix that maps the components to the design parameters, then

$$\{DP\} = [B]\ \{SS\}\{\ bjk= (0,1,)\} \tag{2}$$

Where bjk is the element of the matrix [B] that maps the kth component to the jth design parameter. The element bjk is binary, 0 = no relationship and 1 = related. It defines the relationship between the jth design parameter and the kth component. By combining the two mapping together, we get:

$$\{FR\} = [A]\ [B]\ \{SS\} \tag{3}$$

The Resultant matrix [D] = [A] o [B] is the relationship between the functional requirements and the components and it maps the relationship of each component of the system to the functional requirements that its existence satisfies. The operator (o) is a composite relational operator for binary matrices.

The composite relation A ° B ≡ the matrix [D] where [D] is defined as:

$$A \circ B = D = (dik)\ \text{where}\ \{\ dik = (0,1)\} \tag{4}$$

The mapping of functions to design parameters to components in an MLH mapping process is justified since in any structured design process, the functional requirements determine the design parameters that in turn determine the components that can deliver the desired system functions. The Multi Level Hierarchical (MLH) model for engineering design as theorized above, provides a much more detailed description about the relationship between system functions and component structure and lays a framework for establishing reliability models for function delivery. The layer of the design parameters is abstract to the reliability of the system; hence it is removed from the system reliability framework once it is captured in the MLH design mapping process. This results in the establishment of a relationship between the components and the functions they perform.

4 RELIABILITY BASED ANALYTICAL MULTI LEVEL HIERARCHICAL MODELING

Trewn and Yang [1998] have applied this two-step MLH model to develop the following functional reliability models that can be applied in concept design reliability evaluation:

4.1 FUNCTIONAL DELIVERY RELIABILITY AND SYSTEM RELIABILITY

From the definition of reliability, it is clear that the system functions only if it delivers all its functions. Therefore:

$$R_s = \prod_{i=1}^{m} P(FR_i) \tag{5}$$

Where $P(FR_i)$ is the probability that FR_i is successfully delivered and

$$P(FR_i) = \prod_{k=1}^{n} (1 - p_k)^{d_{ik}} \tag{6}$$

Where d_{ik} is the entry of **D** matrix in ith row and kth column and p_k is the failure probability of component k. Clearly, d_{ik} =1 indicates that kth component will affect the ith functional requirement and vice versa. Hence:

$$\therefore R_s = \prod_{i=1}^{m}\prod_{k=1}^{n} (1 - p_k)^{d_{ik}} = \prod_{k=1}^{n} (1 - p_k)^{\bigcup_{i=1}^{m} d_{ik}} \tag{7}$$

4.2 DEPENDENT FAILURE OF COMPONENTS

Dependent failure of components is defined as the failure of a component due to the failure of another component or a single failure mode may cause a number of components to fail simultaneously. In a system context, dependent failure can be defined as the overall effect on the system function performance due to dependent failure of components. For example, consider the design of a fluid pump seal and bearing assembly (figure 3).

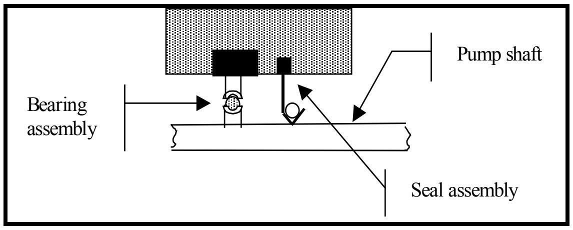

Figure 3: Fluid pump seal and bearing assembly

There is a coupling between the bearing and the seal in the context of functional reliability and the ability of the pump seal to perform its function to seal the liquid past the pump shaft. In MLH model terms, the performance of the seal is dependent on the performance of the bearing. The play in the bearing is a monotone-degrading characteristic with respect to time. As the bearing ages (in terms of operational cycles), the play between the inner and outer races increases due to wear of the ball bearing and the inner and outer races. At a certain point of time, the play may still be within the operating tolerance of the bearing, but it may cause the shaft to run out of true just enough to cause the seal to leak. In this case, the degradation in performance of the bearing causes the seal to leak. In other words, the seal is dependent on the bearing for its performance.

When a failure of one component will cause the failure of other components, it is said that the failure is a dependent failure. Dependent failures are not uncommon in engineering practice, Trewn and Yang [1998] have proposed that, the exact mathematical model which describes the effect of dependent failures with respect to functional reliability and failure costs is established based on this MLH model.

In a binary state failure model, dependent failure may be modeled by:

Let $p_{k|j}$ be the probability of failure of component k given the failure of component j, where k≠j and $p_{k|k} = 1$. Then:

$$P_k = \sum_{j=1}^{n} [p_{k|j} \times p_j] \tag{8}$$

Equation 8 may be represented in a system structure model as in figure 4.

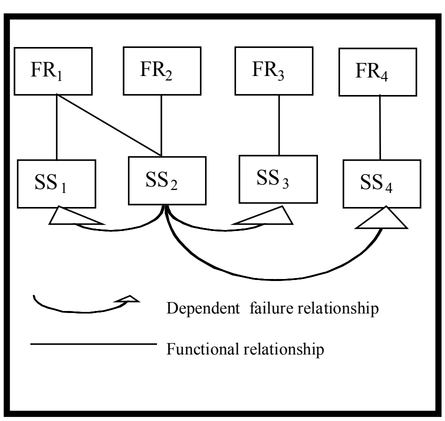

Figure 4: Dependent failure system structure

4.3 COST OF FAILURE

When failure occurs, the product may lose some or all of its functions. If the failure is due to the failure of the components, these components may have to be repaired or replaced. In the multi-level hierarchical model discussed earlier, each component will affect the product function in different ways. Some of the components may only affect some minor functions, whereas, some of key component may affect all the functions of the product. Also, different components have different repair/replacement cost. The following failure cost model analyzes the cost of component and function failures on system performance. let:

EC_{ss_k} = Expected cost of failure of component k

C_{ss_k} = Cost of replacement of component k

C_{FR_i} = Cost of loss of function i

$$E[C_{SS_k}] = \sum_{j=1}^{n} [p_{k|j} \times p_j]\left(C_{SS_k} + \sum_{i=1}^{m} d_{ik} C_{FR_i}\right) \tag{9}$$

Clearly, Equation (9) states that the expected cost of failure due to component k is proportional to the component replacement cost and the cost of losing relevant product functions affected by the failure of component k. There are several ways to reduce the expected cost of failure. First, it can be reduced by reducing p_k, the failure probability of that component. Secondly, failure costs can be reduced by improving the system design so that failure of components will disable fewer functions provided by the system.

4.4 DESIGN VULNERABILITY INDEX

The cost of failure model provides a good measure of the vulnerability of the design as determined by its inability to reliably provide the functions that it is designed to perform. Trewn [1999] has elaborated on the development of this index.

The design vulnerability index T is given by equation 10:

$$\mathbf{T} = (\mathbf{q}^T + \mathbf{r}^T \mathbf{D})\mathbf{P}\,\mathbf{p} \tag{10}$$

Where:

q is the component failure cost vector
r is the function failure cost vector
D is the MLH matrix
P is the component dependent failure probability matrix
p is the component independent failure probability vector

The design vulnerability model has the following benefits:

- It is dimensionless
- It incorporates the independence of the design
- It is insensitive to the level of abstraction of the design
- It has the same measurement unit for any design
- It removes the subjectivity of the designer in the evaluative process

This formulation of cost of failure model determines design vulnerability to failure of components. Design vulnerability provides the following analysis on the reliability of a system and its functions:

- A measure of the incapability of a design to deliver its intended functions
- A measure of the uncertainty of functional delivery
- Consequences of poor design practices
- A method for evaluating and comparing competing concept designs

The vulnerability index based on the cost of failure model is a true evaluation index since it is dimensionless, it incorporates the independence and complexity of the design and it is dimensionless. Further the index is insensitive to the level of design abstraction as the upper level sub-systems capture the cost of failure and probability of lower sub-systems. Last but not the least, the vulnerability index is insensitive to the subjectivity of the designer and decisions made by the model are entirely repeatable.

5 CASE STUDY (OVERHEAD PROJECTOR): DESIGN VULNERABILITY ANALYSIS

The MLH analytical system model is explained by applying the methodology to an overhead projector design. [Trewn, 1999]. The overhead projector is a product conceived by customers to project slides on a vertical screen so that page size documents may be magnified and projected for viewing by a large audience. The customer requirements refined through the life cycle of the product) requires the projected picture to be:

FR_1 Projected picture should have good intensity to be visible at a distance

FR_2 Projected picture should be able to be focused for picture clarity

FR_3 Projected picture should be able to be vertically positioned on the screen

FR_4 Cool projection equipment

FR_5 Supply electric power to operate fan and lamp

The two functions F_4 and F_5 are not design functional requirements, but are support functions. The MLH mapping of the overhead projector is shown in figure 5.

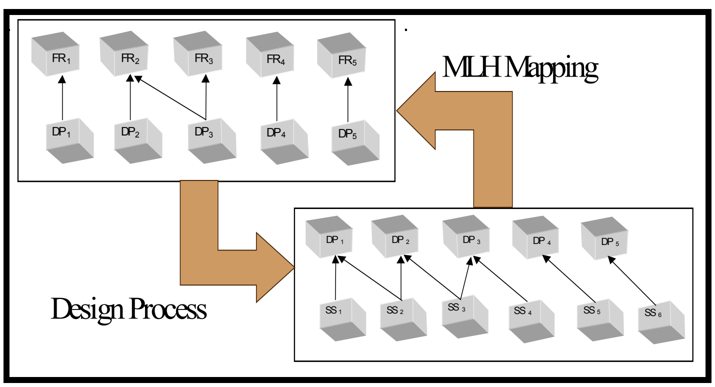

Figure 5: MLH mapping of the overhead projector

The MLH mapping determines the functional reliability mapping for the system. Figure 6 shows a schematic of the functional model.

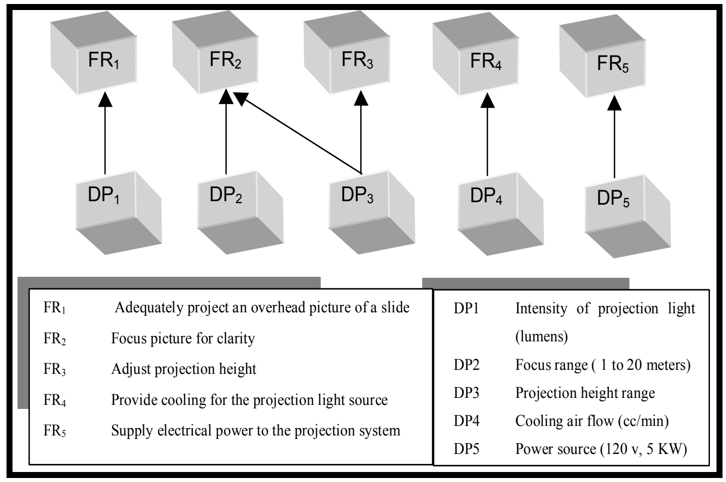

Figure 6: Functional mapping

The reliability of the functional requirements is determined by equation (7). Let R_{ss_1}=0.70, R_{ss_2}=0.99, R_{ss_3}=0.90, R_{ss_4}=0.90, R_{ss_5}=0.80, R_{ss_6}=0.85. Then from equation 6:

$$P(FR_i) = \prod_{k=1}^{n} (1 - p_k)^{d_{ik}},$$

hence

$$R_{FR_1} = (0.7)^1 \cap (0.99)^1 \cap (0.90)^0 \cap (0.90)^0 \cap (0.80)^0 \cap (0.85)^0$$
$$= 0.693$$

Similarly, R_{FR_2} = 0.802, R_{FR_3} = 0.810, R_{FR_4} = 0.80 and R_{FR_5} = 0.85

It is clear that the function with the worst reliability is the function of projecting an overhead picture of a slide (FR_1). This function's poor reliability is primarily due to the poor reliability of the projection lamp (SS_1). Hence the MLH model analysis of functional reliability of the design gives an insight into the reliability of each function and helps in determining the components that are responsible for delivering each function. This model can give insights to the reliability improvement process to help determine the most beneficial way to allocate limited reliability improvement budgets to get maximum gain in functional reliability improvement.

The corresponding cost of failure and failure probability parameters for the overhead projector case study is shown in Table 2.

Table 2: Overhead Projector case study design parameters

Functions	Failure probability p_{fri}	Failure cost r_i	$FR_i \backslash SS_k$	MLH matrix **D** SS_1	SS_2	SS_3	SS_4	SS_5	SS_6
Projection intensity	0.307	$ 50.00	FR_1	1	1	0	0	0	0
Focus range	0.109	$ 40.00	FR_2	0	1	1	0	0	0
Projection height	0.190	$ 30.00	FR_3	0	0	1	1	0	0
Cooling air flow	0.200	$ 10.00	FR_4	0	0	0	0	1	0
Electric power supply	0.150	$ 10.00	FR_5	0	0	0	0	0	1
Components	**Failure probability p_k**	**Failure cost q_k**	**$SS_k \backslash SS_j$**	**Failure dependence Matrix P SS_1**	**SS_2**	**SS_3**	**SS_4**	**SS_5**	**SS_6**
Projection lamp	0.30	$ 1.00	SS_1	1.00	0.00	0.00	0.00	0.75	0.00
Magnifying lens	0.01	$ 50.00	SS_2	0.00	1.00	0.00	0.00	0.00	0.00
Focus adjustment	0.10	$ 15.00	SS_3	0.00	0.00	1.00	0.00	0.00	0.00
Reflector	0.10	$ 10.00	SS_4	0.00	0.00	0.00	1.00	0.00	0.00
Cooling fan	0.20	$ 15.00	SS_5	0.00	0.00	0.00	0.00	1.00	1.00
Power regulator	0.15	$ 5.00	SS_6	0.00	0.00	0.00	0.00	0.00	1.00

This example is next extended to the cost of functional and component failure analysis. Figure 7 illustrates the cost of failure for the overhead projector model.

k	Component	Cost ($)	i	Function	Cost ($)
1	SS_1 Projection lamp	1.00	1	FR_1 Project an picture	50.00
2	SS_2 Magnifying lens	50.00	2	FR_2 Focus picture for clarity	40.00
3	SS_3 Focus adjustment	15.00	3	FR_3 Adjust projection height	30.00
4	SS_4 Reflector	10.00	4	FR_4 Provide cooling	10.00
5	SS_5 Cooling fan	15.00	5	FR_5 Supply electrical power	10.00
6	SS_6 Electrical power regulator	5.00			

$$E[C_{SS_k}] = p_k\left(C_{SS_k} + \sum_{i=1}^{m} d_{ik} C_{FR_i}\right)$$

Component Number	Failure Cost
$E[C_{SS1}]$	$ 15.30
$E[C_{SS2}]$	$ 1.40
$E[C_{SS3}]$	$ 8.50
$E[C_{SS4}]$	$ 8.00
$E[C_{SS5}]$	$ 5.00
$E[C_{SS6}]$	$ 2.25
Total	***$ 40.45***

Figure 7: Cost of failure model

From figure 7 it is clear that the expected cost of failure of component 1 is the highest as its failure not only results in its own replacement but it also causes the failure of function 1. Thus, the criticality of failure of components can be compared and this could lead to identification of critical components in the system. Even though component 1 is the cheapest component to replace, its failure could result in the most damage to the system as determined by its high expected cost of failure.

Next, the overhead projector example is extended to dependent failure analysis. Consider the scenario where the failure of component 6 (power source) would cause failure of the fan and the lamp. Also, the failure of the fan could cause the lamp to fail due to overheating. Figure 8 illustrates these dependent failures.

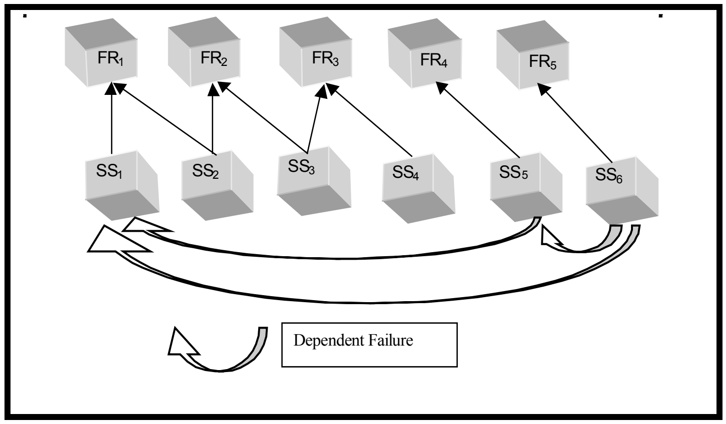

Figure 8: Dependent Failure

Since the failure of power supply will instantly disable the lamp and the fan, we have: P5|6 = 1.0 and P1|6 =1.0. Also, it is estimated that 3 out of 4 times the failure of the fan will cause the failure of the lamp, then: P1|5 = 0.75.

Lets apply the cost model from equation 9 to the overhead projector case study. The cost model is given by equation 9:

$$E\left[C_{SS_k}\right] = \sum_{j=1}^{n} [p_{k|j} \times p_j]\left(C_{SS_k} + \sum_{i=1}^{m} d_{ik} C_{FR_i}\right)$$

Thus cost of failure of component 5 is:

$$E\left[C_{SS_5}\right] = \sum_{j=1}^{6} [p_{5|j} \times p_j]\left(C_{SS_5} + \sum_{i=1}^{m} d_{i5} C_{FR_i}\right)$$

$E[C_{ss_5}]=[(p_{5|1} \times p_1)+(p_{5|2} \times p_2)+(p_{5|3} \times p_3)+(p_{5|4} \times p_4)+(p_{5|5} \times p_5)+(p_{5|6} * p_6)]\times[15.00 + (0+0+0+0+1\times(10.00+0\ )]$

$E[C_{ss_5}] = [(0 \times 0.30)+(0 \times 0.01)+(0 \times 0.10)+(0 \times 0.10)+(1.0 \times 0.20)+(1.0 \times 0.15)] \times [25] = 0.35 \times 25 = \$ 8.75$

It is clear that the introduction of dependent failure analysis gives a more complete picture about the damage caused by the failure of component 5. Assuming independence, the expected cost of failure of component 5 is $ 5.00. But, by the introduction of dependent failure, this cost escalates to $ 8.75 due to the dependence of component 5's performance on component 6's performance.

This example clarifies the applicability of the failure cost model and it also provides information that could be used for intelligent decision making in concept design evaluation and improvement processes.

6 CONCLUSION

The Functional Reliability Design process extends traditional reliability and enables the evaluation of competing concepts at the design stage. The output of this process is a design with minimized uncertainty to functional delivery. The Functional Reliability Design methodology provides the following benefits to reliability and concept design engineers:

- a systematic method to evaluate competing systems that satisfy the system functional requirements in the concept design stage;
- improved system designs with least complexity and improved function robustness leading to more reliable systems;

- reduced concept and prototype testing phase costs as the system will be optimized for reliability in the conceptual stage itself; and
- reduced dependent failures of sub-systems due to identification and analysis of these dependencies.

7 REFERENCES

[1] Bhattacharya, A., "Reliability Evaluation of Systems with Dependent Failures", *International Journal of Systems Science*, Vol. 27, No. 9, pp. 881-885, 1996.

[2] Hubka, V. and Eder, W.E., *Theory of Technical Systems*, Berlin, Springer-Verlag, 2nd Ed., 1988.

[3] Palady, P., *Failure Modes and Effects Analysis*, PT Publication Inc., 1995.

[4] Phal, G. and Beitz, W., *Engineering Design: A Systematic Approach*, Springer-Verlag, 1988.

[5] Suh, N.P., The *Principles of Design*, New York, Oxford University Press, 1990.

[6] Trewn, J. and Yang, K., "The relationship between system functions, reliability and dependent failures," The 1998 IEEE International Conference on Systems, man and Cybernetics, *IEEE-SMC '98*, San Diego, Sep., 1998.

[7] Trewn, J., "Systems approach to reliability design: Functional reliability design and evaluation methodology," *Doctoral Thesis*, Department of Industrial and Manufacturing Engineering, Wayne State University (WSU), Detroit, MI., USA, 1999.