INTERNATIONAL CONFERENCE ON ENGINEERING DESIGN, ICED'07
28 - 31 AUGUST 2007, CITÉ DES SCIENCES ET DE L'INDUSTRIE, PARIS, FRANCE

GRAYSCALE SYSTEM RELIABILITY: ASSESSMENT OF DEGRADATION, RELIABILITY, AND LIFETIME IN ENGINEERING DESIGN

Tomonori Honda and Erik K. Antonsson, Ph.D., P.E.
California Institute of Technology

ABSTRACT

Understanding of the risk and reliability of systems can be enhanced by modeling the grayscale degradation of the performance of components and determining the grayscale impact on the system performance. Rather than producing an estimate of the probability of the system being in either the working or the failed state, as more traditional risk and reliability modeling does, this approach produces estimates of the probability of the system being in any of a continuous range of states between fully working and completely failed.

The development of the approach is outlined and illustrated by an example.

Keywords: System Reliability, Component Degradation, Performance Degradation

OBJECTIVES

Every product has inherent failure modes and impacts of those failures. Products also typically have required or desired system reliability specifications. The most readily available reliability data is on component behavior (typically including statistical predictions of performance degradation). Therefore, it would be useful to be able to develop predictions of system degradation and failure based on component statistics. Currently, two distinct approaches are used for analyzing robustness and reliability of system performance by propagating the states of components: probabilistic risk assessment (PRA) and robust design techniques.

Probabilistic risk assessment was developed by the nuclear industry for analyzing system reliability when component failures consist of low probability but catastrophic events [1, 2]. The PRA method, and its variants such as binary decision diagrams [3, 4], dynamic fault trees [5], and stochastic petri nets [6] propagate the binary (working or failed) state of components into a binary state of system. To use these methods, the engineer must first convert a model of the dynamics of system into a simplified model that includes only two states.

In contrast, robust design techniques, such as Taguchi's method, were developed to analyze systems for performance loss caused by manufacturing and operational variations [7, 8]. In Taguchi's method, the Quality Loss function is continuous, and is modeled as a parabola. This method considers the performance of a system at a particular time (usually at beginning of the product life) and does not consider the time-evolution of the system performance.

These methods are sufficient for industry that is concerned with minimizing the probability of catastrophe (*e.g.*, the nuclear industry) or minimizing the performance variation caused by uncontrolled manufacturing variations (*e.g.*, the automotive industry). However, when analyzing aerospace missions, both the degree of system degradation and the time dependence of system degradation is important. This paper reviews the development of a new approach for computing and analyzing the continuous (or grayscale) changes to the performance of a system, given the expected degradation of its components over the time.

METHOD

The new approach presented here for analyzing the overall impact of component degradation on system performance consists of three steps: modeling the stochastic component degradations; obtaining the performance degradation caused by the degradation of the components, and combining the changes in each individual performance into an overall system impact (see Figure 1). Explicit component degradation models and performance models are input to this method and are assumed to be obtainable. Many researchers in reliability engineering focus on a Bayesian approach for obtaining binary component failure models, that could be extended to the grayscale component degradation models required in the method presented here. Currently, the performance model used in this method is a assumed to be the same model used for designing the nominal system. However, to increase computational efficiency, performance models could be approximated using methods such as response surface methods.

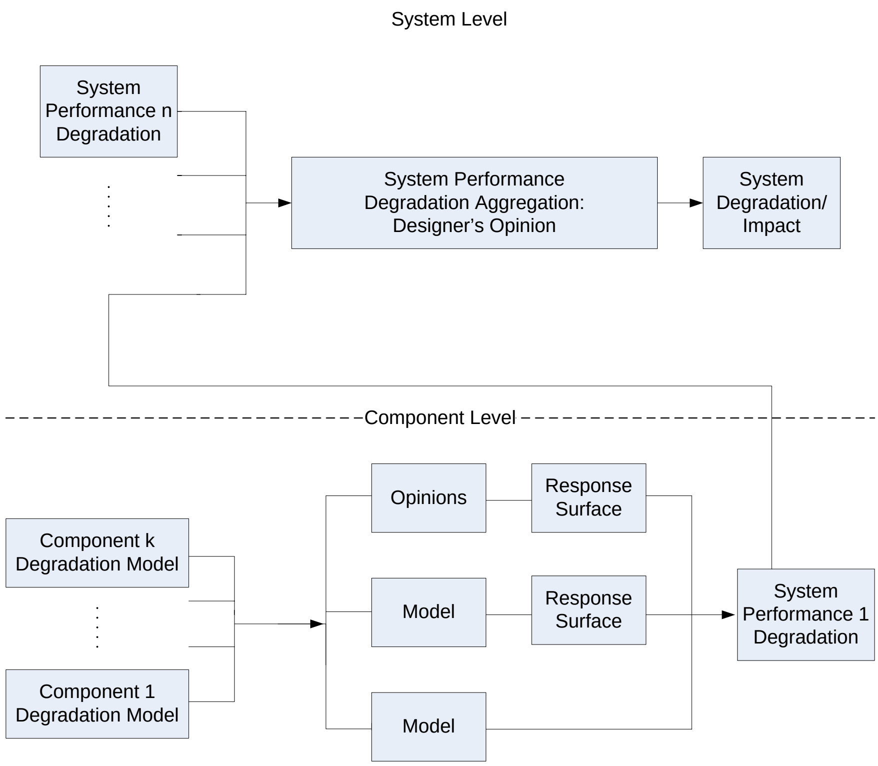


Figure 1: Propagation of Degradation from Components to System

To make the system impact into a grayscale (or continuous) quantity, the component degradation must also be non-binary (continuous). Thus, the first step is to define the degradation of the components as a continuous stochastic process of each design variable, rather than a probability distribution for catastrophic failure as a function of time. When designing the system, the state of components is defined by design variables over a design space, and therefore this is natural extension for representing the degrading state of components. These stochastic processes should include gradual change of each design variable over time as well as catastrophic failures. The most common stochastic process is a combination of Brownian motion with a drift that represents each degradation mode, and a catastrophic failure probability. The drift represents the average degradation path for a particular mode of degradation and it could be a function of time as well as path/history dependent. Brownian motion represent the stochastic nature of degradation. Rather than Brownian motion, the stochastic process could also have a skewed distribution that is time and space dependent, however, this complexity is not illustrated here. Also, a repairable system could have the performance of one or more components described by a jump process that allows the performance to jump from a failure state to a working state. These are illustrations of the possible richness of the representation of the degradation of components.

Given the component models of the first type described above, and using dynamic simulations of system behavior, a probability distribution for system performance(s) over time can be obtained for all required system attributes. These system performances over time can be converted into performance degradations as function of time ($X_i(t)$) by comparing them to requirements and incorporating designer and customer preferences. The resulting performance degradation function has the property that it is equal to 0 when it the system is performing perfectly, and it is equal to 1 when the performance does not meet the required specification, leading to system failure. This conforms to the convention for Fault Tree Analysis where 1 represents failure.

Finally, each individual performance degradation must be combined into a single system impact, which represents a measure of overall system performance degradation X_{sys}. Following the axioms of rationality described by Tribus [9], the system impact as a function of the performance degradation must have the following properties:

1. bounded between $[\max\{X_i\ \forall i\}, 1]$
2. monotonic with respect to all X_i
3. continuous with respect to all X_i
4. if $\exists i$ such that $X_i = 1$, $X_{sys} = 1$

These are similar to axioms of aggregation functions for preferences in the Method of Imprecision (M_oI) [10, 11]. Mathematically, the system impact and performance degradations act like complements of the preferences.

These criteria come from the observation that the aggregation of continuous (fuzzy) performance requirements forms a type of fuzzy OR gate. Because of possible coupling between the degradation of many individual performances, the catastrophic failure surface (which is defined as $\{(x_1, ..., x_n) : X_{sys}(x_1, ...x_N) = 1\}$) must be specified by the engineering designer. This catastrophic failure surface can be obtained using a technique similar to the elicitation of indifference points in the Method of Imprecision [12]. Given this failure surface, X_{sys} can be extended to the entire domain using non-intersecting contours of impact. Examples of possible aggregation schemes are illustrated in Figure 2.
The $\max$ represents the least conservative aggregation, implying that system degradation is the same as the worst performance degradation. The truncated sum represents the most conservative aggregation. The complement of the product of the complement is a probabilistic fuzzy OR function and has the property that it is similar to the $\max$ function when one performance degradation is near 1, and similar to the truncated sum when all of the performance degradations are small.

By propagating the degradation of components into an overall system performance degradation, the grayscale (continuous) system impact as a function of time can be obtained. This system impact uses the actual dynamics of the computational model used for designing the system, rather than a simplified fault diagram or tree, and allows nonlinear effects of coupling among degradations to be more easily captured. In some (rare) cases some of the degradation modes could even help improve system performance(s). Finally, the designer can compare grayscale system impact with a grayscale reliability requirement to determine when the system is likely to be in an excessively degraded state, and which components contribute most to the likelihood of each degraded state of the system.

RESULTS

As an illustrative example, the degradation of a mass-spring-damper system is analyzed. The governing equation for this system is given by:

$$F_{ext}(\tau) - k(t)x(\tau) - b(t)\dot{x}(\tau) = m\ddot{x}(\tau) \tag{1}$$

where F_{ext} is an external force, k is the spring constant, b is the damping constant, m is mass, and x is displacement. Both k and b degrade over the time, but at much longer time scale than the time dependence

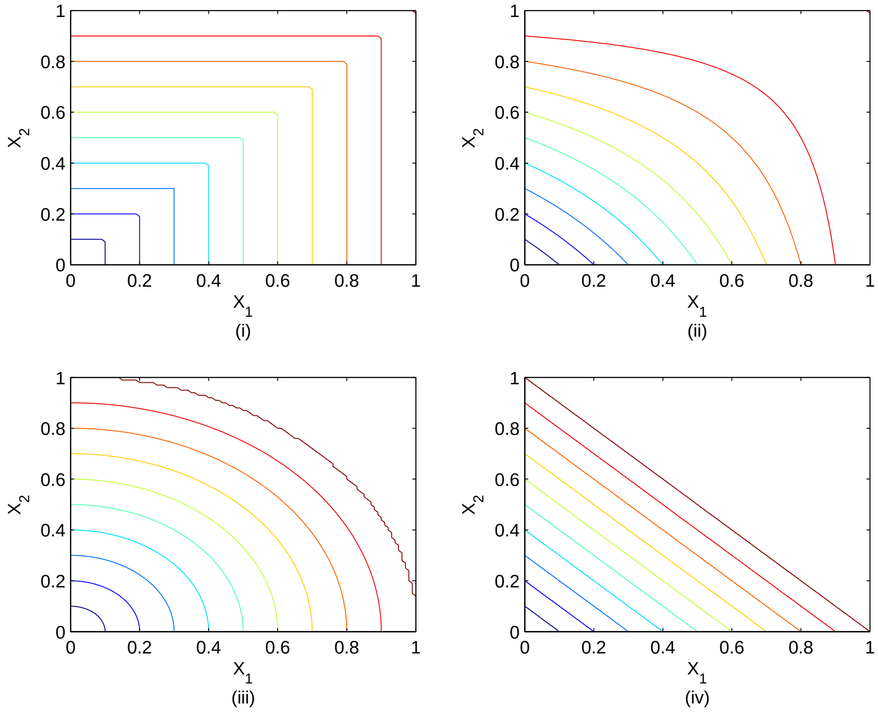


Figure 2: Iso-Impact Contour Examples: (i) $\max\{X_1, ..., X_n\}$, (ii) $1 - \prod_{i=1}^{n}(1 - X_i)$, (iii) $\min\left\{1, \sqrt{\sum_{i=1}^{n} X_i^2}\right\}$, (iv) $\min\{1, \sum_{i=1}^{n} X_i\}$

for x (i.e., t is a few orders of magnitude larger than τ). Thus, k and b are assumed to be constant for calculating the system performance at any given time t. The stiffness k of springs and the damping constant b of the dampers degrades as function of time as shown in Figure 3. Each distribution is a combination of a random walk with two drifts (one describing the case for becoming stiffer and other for becoming softer) and an exponential distribution for catastrophic failure. The probability of catastrophic failure is represented by the strip at $k = 0$ and $b = 0$, which increases over time, as expected. Even though this system is a simple system to model, the interaction of different modes of degradation for the springs and dampers gives some insight into the complex interactions between component degradations and system performance, and therefore why this method is important to providing a clear understanding of system reliability.

The next step is defining a performance degradation function, which is derived from the following performance specifications: the upper bound on the maximum amplification of the amplitude of oscillation of the mass, an upper bound on the maximum amplification frequency, and a lower bound on the damped natural frequency as shown in Figure 4. Having a continuous membership function represent the degree of performance degradation allows the definition of states where the performance of the system is marginally acceptable. For example, the bottom plot in Figure 4 shows that the designer needs the system to have a damped natural frequency higher than 1.5, but allows system to be between 1.3 and 1.5 with degraded performance, and system fails completely when the natural frequency is 1.3 or lower. For binary models of the system state, all performance degradations will be represented by step function.

Given the model of the degradation of components, the performance degradation definitions, and a particular performance degradation aggregation scheme, the probability distribution for the system impact over time can be obtained (see Figure 5). The volume above $(t, t + \Delta t)$ and $(X, X + \Delta X)$ represents the probability that the system will be in a degraded state between $(X, X + \Delta X)$ at time $(t, t + \Delta t)$. By comparing the catastrophic failure distribution for different aggregation schemes (Figure 6), the designer can determine if differences in the aggregation scheme are significant for managing a particular

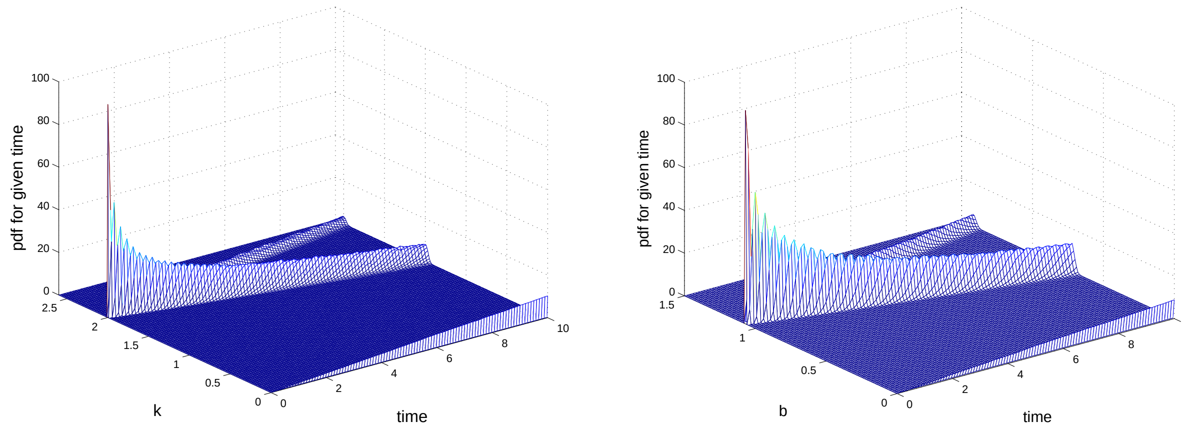


Figure 3: Spring and Damper Degradation over Time.

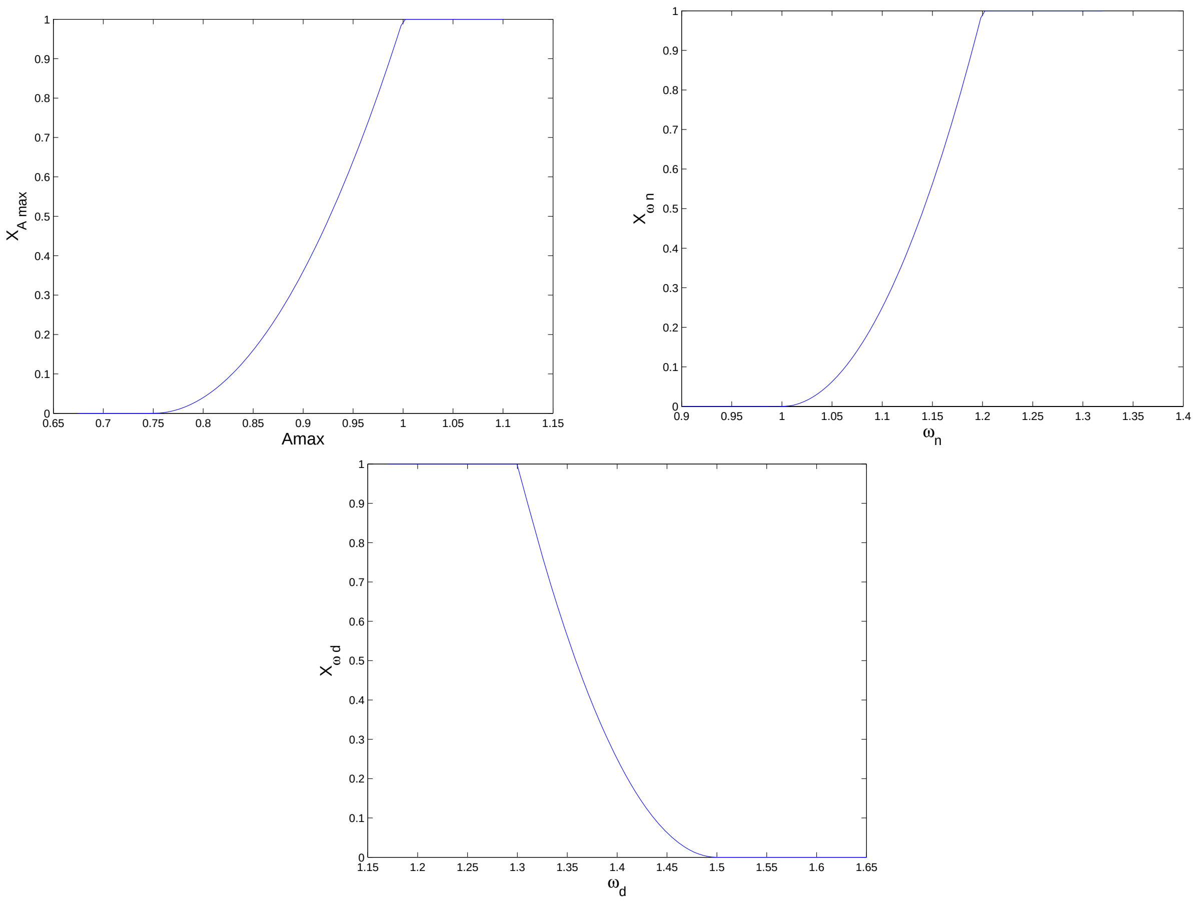
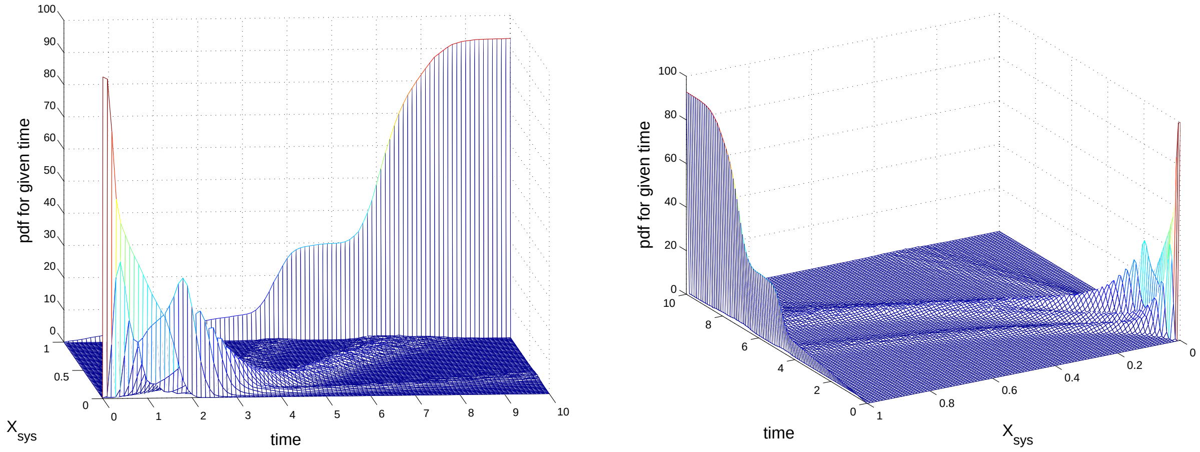
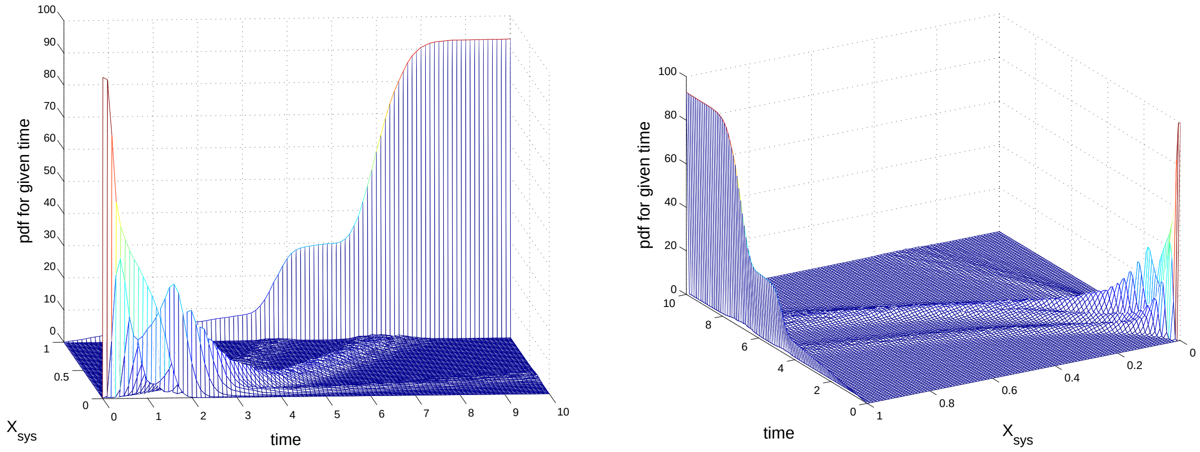


Figure 4: Amplitude, Maximum Frequency, and Damped Natural Frequency Specification

system reliability. The designer should also consider the difference between aggregation schemes and the accuracy of the component degradation model used. The figure contains important information necessary to make good design decisions. Taking a slice at a particular time gives the probability density function for X_{sys} at that time. If the design has an intended lifetime, the designer can obtain an expected system performance by obtaining the slice at the desired lifetime. Also, the cumulative distribution for complete system failure can be obtained by taking slice at $X_{sys} = 1$.



Max aggregation



Truncated Sum aggregation

Figure 5: Probability Distribution Function for System Impact over Time.

There is an additional representation for same data that may be useful. By accumulating the probability distribution into $P(X(t) >= X)$, the probability that the system will be at state worse than impact of X at time t can be found (see Figure 7). By examining this plot, the designer can determine how important the consideration of partial working states are. In this example, because there is a significant probability that the system is in a marginally working state, the designer will be missing information if she only considers the probability for complete failures to assess the reliability of the system.

Because the cumulative distribution, $P(X(t) >= X)$, is monotonically decreasing with respect to X, the designer can compute a reliability requirement surface, shown in Figure 8, that represents the upper bound on the probability that system impact must satisfy. Rationally, this requirement surface $S_{req}(X,t)$ should have the following general properties:

1. $S(0,t) = 1$
2. monotonically decreasing with respect to X
3. monotonically increasing with respect to t

The first property is simply a boundary condition stating that the system impact is always greater than or equal to 0. The monotonicity with respect to X comes from fact that $P(X(t) >= X)$ is a decreasing function of X and the monotonicity in time comes from fact that the cumulative probability for failure increases over time for non-repairable systems.

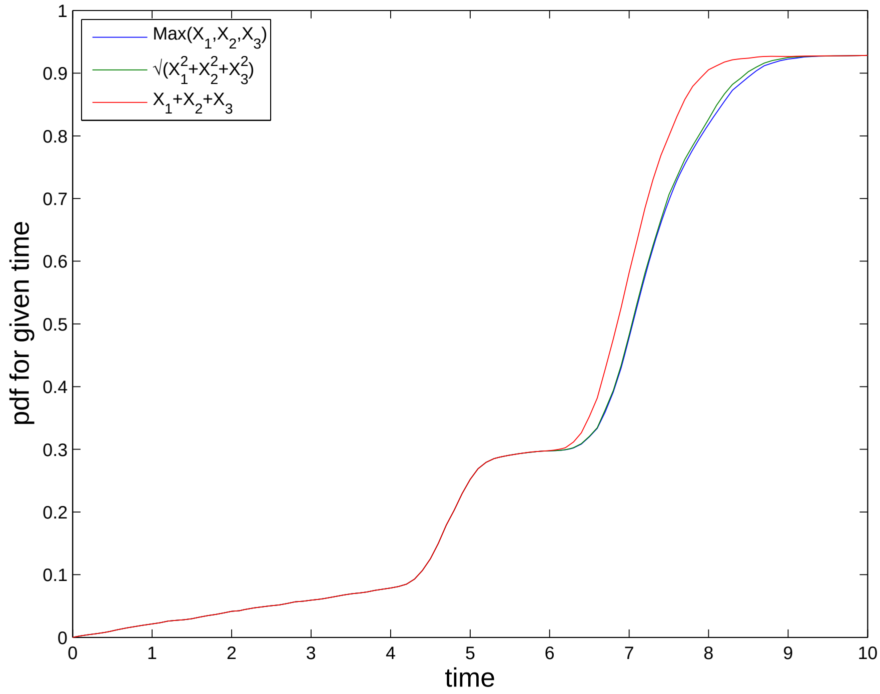
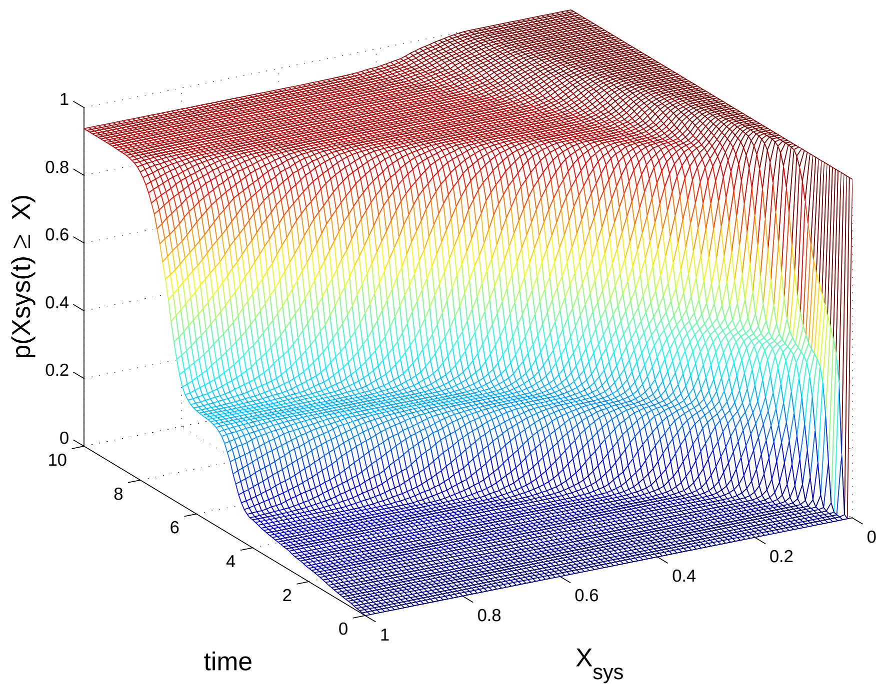


Figure 6: Comparison of Performance Degradation Aggregation Scheme



Truncated Sum Aggregation

Figure 7: Cumulative System Impact Distribution

By comparing two surfaces (see Figure 9), the likely time when the system first exceeds the reliability requirement can be determined. For this example, the reliability requirement is first broken at $time = 1.5$ along $X_{sys} = 0$. If the designer only considers catastrophic failure, then the system meets the requirement until $time = 7$. Thus, the traditional binary failure state analysis focuses only on $X = 1$, but Figure 9 shows that some of the partial failure states are important to consider as well.

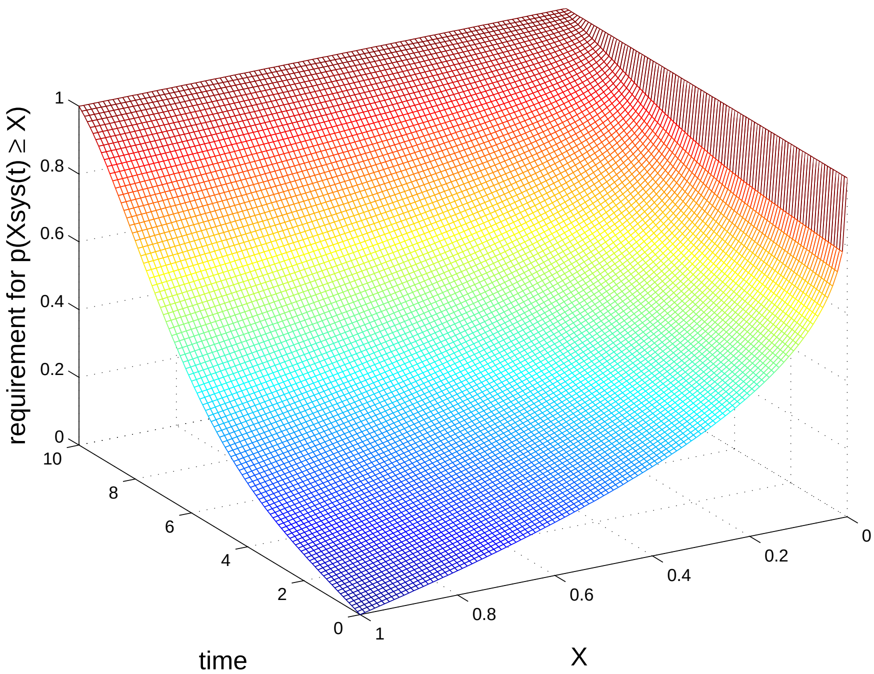


Figure 8: System Impact Requirement

By analyzing which degradation component (or mode) is causing early system failures, and the designer's criteria on acceptable reliability, the design could be improved accordingly. Subsequent research will explore the application of sensitivity analysis to this method, to allow the designer to determine cost efficient improvements. This method also provides a way to create time-dependent continuous reliability constraints that can be used for design optimization.

Reliability Based Design Optimization (RBDO) [13, 14] optimizes design objectives while satisfying probabilistic reliability constraints. The traditional RBDO lacks time domain considerations and uses a crisp failure boundary. The approach presented here illustrates a way for RBDO to use time-dependent fuzzy failure constraints that also constrains the probability for partial failures. Thus, the designer could optimize desired performances while satisfying new reliability constraints to obtain an highly reliable design. In addition, if the designer has various reliability requirement surfaces for different degree of reliabilities of the design, then the designer can trade-off reliability with other design attributes. Thus, the data for system impact could be used in different ways to help the designer make rational trade-offs between reliability and other attributes.

CONCLUSIONS

The new method presented here provides a way to predict the (continuous) state of a system based on data on the performance and degradation of components. This approach also provides a straight-forward way to compare the predicted performance and degradation of a system with a time-dependent performance requirement. The results provide more information on the probability of the state of a system than binary methods because the degradation of components and systems are represented on a continuous grayscale, and also because the degradation of the system performance is computed from the degradation of the individual components.

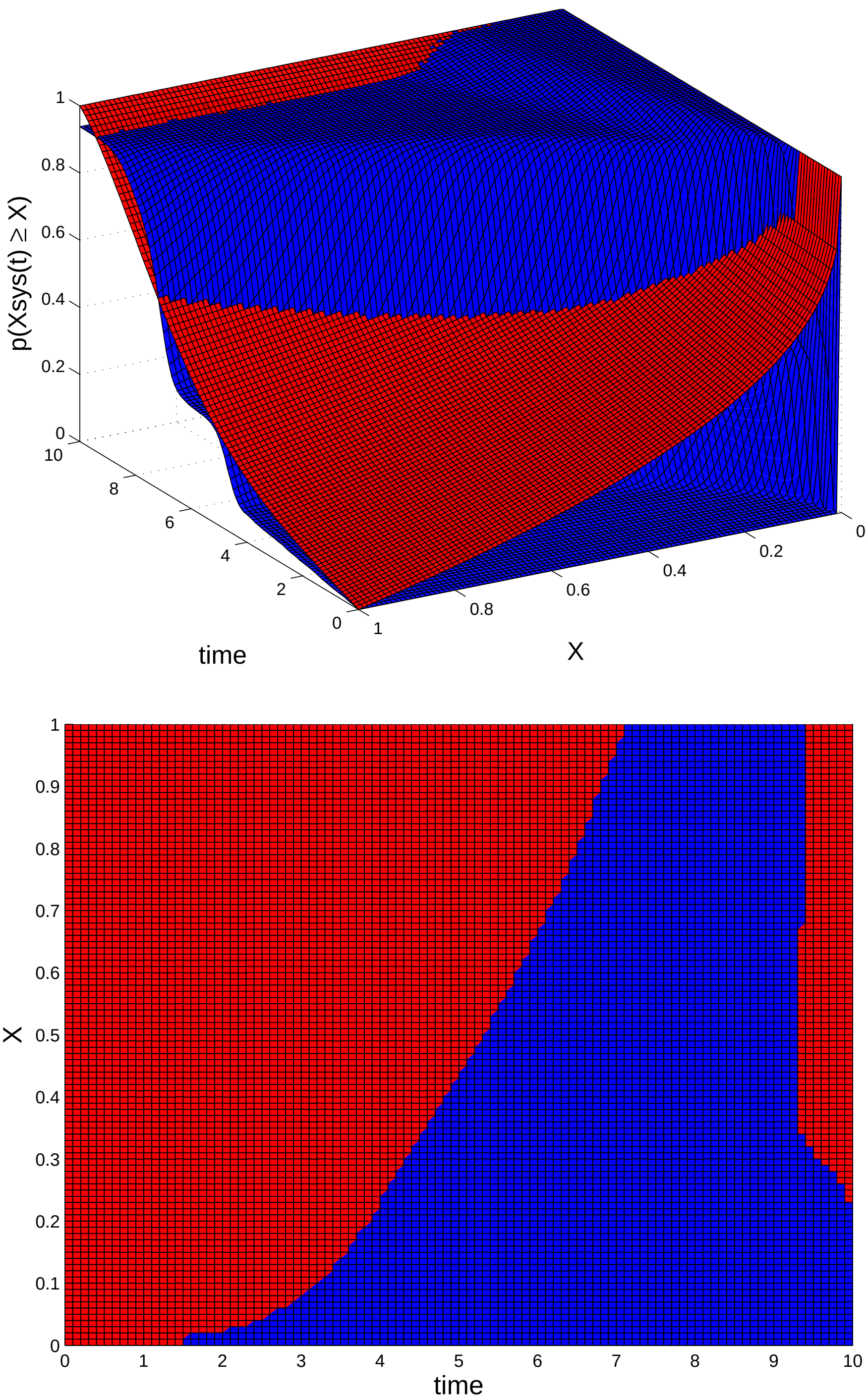


Figure 9: Comparison of System Impact with Requirement

REFERENCES

[1] Bedford, Tim and Cooke, Roger. *Probabilistic Risk Analysis Foundations and Methods*. 2001, Cambridge University Press, Cambridge UK.

[2] Lee, W. S., Grosh, D. L., Tillman, F. A., and Lie, C. H. Fault tree analysis, methods, and applications — a review. *IEEE Transactions on Reliability*, August, 1985, R-34(3), pp. 194–203.

[3] Sinnamon, Rosalyn and Andrews, John D. Fault tree analysis and binary decision diagrams. In

Proceedings of the Reliability and Maintainability Symposium, January, 1996, pp. 215–222.

[4] Akers, Sheldon B. Binary decision diagrams. *IEEE Transactions on Computers*, June 1978, c-27(6), pp. 509–516.

[5] Pullum, Laura L. and Dugan, Joanne Bechta. Dynamic fault tree analysis methodology examples. Technical report, Quality Research Associates, Inc., July, 1995.

[6] Murata, Tadao. Petri nets: Properties, analysis and applications. *Proceedings of the IEEE*, 1989, 77(4), pp. 541–580.

[7] Kackar, R. N. Off-line quality control, parameter design, and the Taguchi approach. *Journal of Quality Technology*, October 1985, 17(4).

[8] Byrne, D. M. and Taguchi, S. The Taguchi approach to parameter design. In *Quality Congress Transaction – Anaheim*. ASQC, May 1986, pp. 168–177.

[9] Tribus, Myron. *Rational Descriptions, Decisions, and Designs*. 1969, Pergamon Press, New York, NY.

[10] Otto, Kevin N. and Antonsson, Erik K. Trade-Off Strategies in Engineering Design. *Research in Engineering Design*, 1991, 3(2), pp. 87–104.

[11] Antonsson, Erik K. and Otto, Kevin N. Imprecision in Engineering Design. *ASME Journal of Mechanical Design*, June 1995, 117(B), pp. 25–32. Invited paper. Special Combined Issue of the Transactions of the ASME commemorating the 50th anniversary of the Design Engineering Division of the ASME.

[12] Scott, Michael J. and Antonsson, Erik K. Using Indifference Points in Engineering Decisions. In *11th International Conference on Design Theory and Methodology*. ASME, September 2000.

[13] Zhang, Thomas A., Hemsch, Micheal J., Hilburger, Mark W., Kenny, Sean P., Luckring, James M., Maghami, Peiman, Padula, Sharon L., and Stroud, W. Jefferson. Needs and Opportunities for Uncertainty-Based Multidisciplinary Design Methods for Aerospae Vechiles. Technical report, Langley Research Center, July 2002.

[14] Du, Xiaoping. Reliability-Based Design using Saddlepoint Approximation. In *32nd Design Automation Conference (DAC)*. ASME, September 2006. Paper Number: DETC2006-99077.

Acknowledgment

This material is based upon work supported, in part, by: a Moore Fellowship supported by the Gordon and Betty Moore Foundation. Any opinions, findings, conclusions or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of the sponsor(s). Special thanks are due for beneficial discussions with Leila Meshkat, Andrew Shapiro, Martin Feather, Steven Cornford and Stephen Prusha of NASA's Jet Propulsion Laboratory.

Contact: Prof. Erik K. Antonsson, Ph.D., P.E.
California Institute of Technology
Division of Engineering & Applied Science
1200 East California Blvd.
Pasadena, CA 91125-4400 U.S.A.
+1 626.583.4963 Fax
http://www.design.caltech.edu/