A Time-domain Modeling and Simulation Framework for Comparative Analysis of Prognostics, Reliability and Robustness in System Design

Nicholas A. Lambert[1], Kyle B. Ferrio[2], and Douglas L. Goodman[3]

[1, 2, 3]*Ridgetop Group, Inc., Tucson, AZ, 85741, USA*

nlambert@ridgetopgroup.com
kferrio@ridgetopgroup.com
dgoodman@ridgetopgroup.com

ABSTRACT

Redundancy is an effective, high-level solution to the requirement for reliable safety-critical systems, but it comes at the cost of Size, Weight and Power (SWaP) and reduced capability. A modeling and simulation framework was developed to address the need for robust design alternatives to redundancy. Robustness, in our application, is treated as the insensitivity of the performance with reference to specification. The necessity to characterize both reliability and robustness in the same framework has resulted in a time-domain simulation approach to modeling behaviors associated with unreliability and a lack of robustness. The incorporation of these features offers a novel insight into potential applications of prognostic technology. Further development of this approach has the potential to allow designers to choose how risks associated with failures are mitigated, by redundancy, robustness, or prognosis.

By modeling the life of parts, the factors that impact them and the resulting behaviors, the observability and predictability (even controllability in the case of optimized, fault-tolerant, closed-loop control) of faults and failures is identified. Designers can determine which parts of a system would benefit from prognostic health management (PHM) technologies, adaptive / tolerant features to yield robust design, or redundancy based approaches. The complex causality in the models requires a Monte Carlo approach analogous to the simulation of fleets of systems; this, combined with the ability to simulate systems made from new and old parts, can inform strategies for condition-based maintenance (CBM).

We present the mathematical modeling concept and the simulation framework which permits comparative assessment of reliability, robustness and prognostics. The multi-hierarchical, systems integration aspects inherent to the concept make this technique highly applicable to real-world dynamic systems. The framework also supports statistical, standards based and physics-of-failure descriptions of stress, aging, fault and failure behaviors in a unified way. There are challenges to be overcome in realizing the benefits of this approach to model-based system design. Issues of model validation, data availability and computational burden are recognized and discussed. As we show, these challenges can be overcome to produce new design tools providing better products and transparent project quality.

1. INTRODUCTION

1.1. The Requirement for a Unified Modeling Approach

Complexity is the arch-nemesis of the systems engineer. This has been addressed in a historical context in work by Zio (2009), where the need to develop methods for integrating dynamics and reliability analysis was highlighted. Reliability engineering methods employ methods that combat complexity by reducing a system to a list of its parts or by offering abstracted representations in the form of reliability block diagrams and fault trees. These typically have a much greater degree of abstraction than the detailed models which describe the dynamic behavior of the system, where causal relationships are the topic of interest.

Mathematical descriptions of system behaviors often take the form of differential and algebraic equations (DAEs), and comparable representations exist for discrete time, state, space, and event systems. Numerical integration methods and solvers are used to produce simulated solutions to the mathematical system representations. The simulations are used for testing of designs with reduced or no physical hardware representation of the system. They often represent the physical plant for development and testing of software.

Models of the system dynamics are computationally expensive to run and simulations of timescales associated with reliability are infeasible. As a result, reliability

considerations are omitted save for functionality for fault injection. In large projects and organizations, these starkly different modeling modalities are often implemented by separate teams, each with separate requirements and tools. Each team's input into the design decision making process occurs at different stages in the design of systems and this can miss opportunities for whole-system optimization, potentially producing sub-optimal solutions. The impacts to a high-level, abstracted reliability analysis of low-level design decisions made using the detailed dynamic models can be poorly communicated, understood or missed entirely given the organizational and methodological disparities that are inherent in the design of large, complicated systems. This issue has been identified and addressed by Siu (1994) and discrete event, explicit state-transition and extended reliability methods were reviewed; the methods described here approach the issue from a starting point of simulation of system dynamics.

1.2. A Novel Reliability Modeling Method

The primary focus of this work has been to assess robustness. Robustness is usually treated as a beneficial insensitivity of a design to variations in conditions or design parameters (for example, variation within manufacturing tolerance of component values), where the performance against the specification is used in assessing robustness. In this case, however, the question of robustness is with regard to a particular instance of a system. Is a given instance of the system design robust? In answering this, it was necessary to produce models of systems that lacked robustness. These models needed to exhibit features of variation, aging, degradation and failure in response to simulated usage. The measure of robustness used is also closely related to reliability, but rather than reporting the statistics of failure, the statistics of specification violations are used.

The incorporation of these aspects of system behavior makes it possible to include prognostic technologies. Through the mathematical modeling of fault and failure behavior that is accurate in its stochastic and deterministic properties, the attention of the designer can be focused on that which is predictable and where appropriate investments on prognostics can be made.

A number of challenges remain and are associated with computational feasibility (in this case of sequential and parallel Monte Carlo simulations) and verification and validation of modeling assumptions. This work presents the opportunity to unify system design practices by introducing time-domain simulation techniques that also serve as reliability predictions; the ability to assess robustness and prognostics as risk mitigating design features means that this topic will be applicable in safety and capability critical systems.

The following sections outline the techniques used for modeling and simulating unreliable systems and including behaviors from standards, statistical and physics of failure based approaches.

2. TIME DOMAIN MODELING OF UNRELIABLE SYSTEMS

Time-domain modeling serves as a useful tool for system integration. The behaviors of parts can be defined and their roles in the system interpreted, yielding the performance of the system as a whole. The methods presented here are intended to be used in the same way. There are models for aging, fault and failure behaviors associated with the usage of each part within a system. Changes that occur in parts are then represented in the system performance. For this method to offer some utility, it must be used as a system integration tool. In describing a part, there is little to be learned about the part; but by including that part in a system, we can learn something about the impact of the part behaviors on the system. We can also derive knowledge about system behaviors on individual parts. It is this causal loop that is the subject of investigations using this approach. There are two key questions to be answered:

1. Does the reliability and life performance of one part affect the reliability and life performance of other parts in the system?
2. Can knowledge of this be used as the basis for predictions about the behavior of individual parts and systems?

The first of these question aims to address challenges present in the design of ever more complex systems. The second question is regarding whether an enhanced understanding of system reliability behavior can be used to formulate effective prognostic solutions. A feature of the approach is that it allows for multiple and various representations of unreliable parts and systems to exist in the same modeling framework.

2.1. The Life State Approach

The key to modeling unreliable systems in a manner which fits with numerical integration based simulation techniques is to use a method involving a life state. This life state is a measure of the age of a part of a system which is analogous to a measure of time; however, the rate at which life elapses is linked to usage via a stress factor. For each part, the life state is the underlying variable upon which all age related behaviors are dependent. This is based on the fundamental reliability relationship found in MIL-HDBK-217:

$$\lambda_P = \lambda_b \pi \quad (1)$$

The predicted rate of failure is the product of the base rate of failure and the part stress factor. The part stress factor is unitless, but by considering the same equation expressed in terms of mean time to failure (MTTF), it can be deemed that

the unit of the part stress factor is hours per hour. It is the ratio of the predicted failure time to the base failure time. The part stress factor is the rate at which a part accumulates age; it is the rate (with respect to time) associated with the life state. This method yields a measure of physical age (referred to as "life") and chronological age as measured in elapsed time.

For complex parts, a vector approach can be taken such that a single part can have an n-dimensional life state with each state having its own stress factor function and accumulation properties. This feature permits multiple behaviors to be modeled.

Typical application of the part stress factors method requires estimation of nominal or maximal usage characteristics and operating temperatures. The life state approach allows for usage characteristics to be taken from time domain simulation results and integrated numerically with respect to time. Consider the Arrhenius relationship at the heart of the part stress approach:

$$\frac{dM}{dt} = Ae^{-\frac{E_a}{kT}} \tag{2}$$

M is the state of a chemical reaction process. If we consider the temperature, *T*, to be a function of time, *T(t)*, then numerical integration can be used to simulate the progression of the state, *M*.

One method for estimating the reliability of a part is to take a time averaged rate of life with respect to time and use a first-order prediction of when the life would reach the base mean time to failure. A more representative method is to re-estimate the part stress distribution in a system as the accumulation of stress into life results in changes of the physical properties of each of the parts. The physical properties will be referred to subsequently as *part parameters*.

2.2. Failure and Fault Onset Distributions

The use of predicted and base rates of failure is indicative of the single parameter exponential failure distribution; however, many distributions can be used in the analysis of reliability and these are supported by the life state approach.

Probability distributions are used to describe the random failure behavior of a population of systems, products, or test articles. The occurrence of failure events is typically described as a probability density function (PDF), cumulative distribution function (CDF), or hazard rate, expressed as functions of time. The life state approach sees these expressed as a function of the life state, rather than time.

The use of Bernoulli trials using uniformly distributed random numbers and the hazard rate for each distribution allows for the occurrence of fault onset and failure events in keeping with the distribution. This can be performed online, using numerical integration methods to derive the hazard rate, or offline where a set of events are pre-computed as crisp thresholds for comparison to a life state.

$$PDF = f(x) \tag{3}$$

$$CDF = F(x) = \int_0^\infty f(x)\,dx \tag{4}$$

$$h(x) = \frac{f(x)}{1 - F(x)} \tag{5}$$

Note that for exponentially distributed events, the hazard function is constant and the memoryless property is preserved in spite of the inclusion of the life state.

Where fault onsets and failure events are causally linked (i.e. the fault leads to the failure), the failure event can be associated only with life accumulated after the fault onset event.

Distributions can be continuous functions or discrete, and as usual, care must be afforded with numerical integration techniques in the case of Dirac and Kronecker deltas.

2.3. Part Parameters – Failure, Fault and Aging Effects

Parts exhibit a number of behaviors with respect to time including aging effects, faults, and failures. These effects are expressed in terms of the part parameters, which represent the role of the part within the system. For example, a capacitor can be modeled as having the parameters of capacitance, series resistance, and parallel conductance. Over the life of the capacitor, the capacitance can decrease dielectric degradation. These parameters affect the performance of a system with a capacitor. Failure effects, for example failing open or short, can be described in the part parameters or a new dynamic model without the capacitor can be used.

Part parameters vary in accordance with 4 effects:

1. Operating environment effects (temperature and pressure) – simulated with the system dynamics.
2. Aging effects – small effects as a result of the gradual accumulation of life.
3. Fault effects – accumulation of life becomes manifest in the part parameters in a more drastic manner.
4. Failure effects – catastrophic step change in part parameters.

Operating environment effects can be included in dynamic models based on deviations from a set of nominal parameters for states conditions.

Aging effects are usually the result of slow processes, long term usage and storage without incident. These can be

described as a function of a life state. Arrhenius approaches have been taken (Kuehl, 2010) in estimating variation of resistance and this is compatible with our approach. If the part parameter variations must be expressed purely as a function of time, then an element of the life state vector corresponding to a unity rate of life accumulation can be used; that is, the part representation has a built in clock. For example, for parts where there is no known correlation between failure and applied stress, but failures are distributed as a function of time, this behavior can be described with a stress factor equal to one.

The representation of faults is an extension of the method for representing the effects of aging. Faults are the manifestation of accumulated stress in the part parameters that occurs after a fault onset event. The occurrence of a fault onset event can be described using the same method as for describing failures through the use of distributions. For example, a part accumulates stress into a life state and demonstrates the effects of aging, after the occurrence of a fault onset event, the part parameters vary according to the fault behavior as a function of the still accumulating life state.

Failures are typically represented as the termination of aging and fault behaviors resulting in the part parameters taking a set of final values as determined by the failure mode. A part may have many failure modes, each corresponding to a particular set of part parameters.

2.4. Support for Physics of Failure Techniques

Modeling underlying parameters – the parameters used to represent the part in the dynamics are dependent on some underlying physical parameter. This is in keeping with the systems integration approach as it allows for definition of parts with internal behaviors – there is scope for self-similar, systems of systems model architectures. There is no fundamental limit to the level of detail that can be included in the mechanics of the through-life behaviors, although computational burden may establish practical bounds.

2.5. Stochastic Modeling with Random Walks

There is considerable literature content on the use of Markov chain and other random walk processes to model the progression of a part from full health through fault to failure. The accumulation of stress into a life state can be considered in similar terms. By use of stochastic integral techniques, random behavior can be modeled in continuous and discrete time and state.

The accumulation properties accumulation rate and accumulation severity have been defined. Accumulation rate is the probability that stress in any given time step will be accumulated into the life state. The accumulation severity is a gain factor that is applied to accumulated stress.

If the accumulation severity is the reciprocal of the accumulation rate, then in the limit as time tends to infinity, the average rate of stress accumulation is equal to the standards based definition. The accumulation of a life state is illustrated in Figure 1. It follows that the standard can still be applied, whilst permitting the expression of stochastic fault progressions. Taken in combination with the ability to describe physics of failure behaviors in the part parameters, the framework provides a strong basis for including models of different types in a single simulation environment.

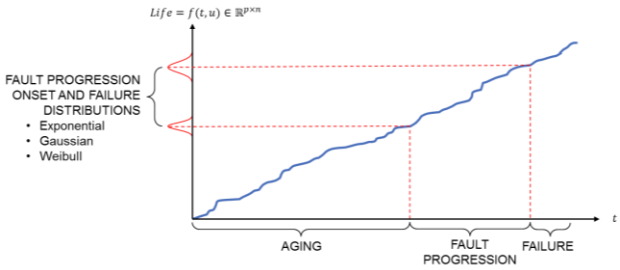

Figure 1. Accumulation of a "Life State"

2.6. System Representations

System representations must be extended to include the reliability and life data necessary to run simulations of models on product life timescales. In the framework, systems are described as a collection of parts. A system has the following attributes:

- A set of parts
- A dynamic model
- A set of specifications
- A set of use-cases

In typical time-domain simulations, a single part may only be represented by a single parameter (e.g. resistance). Part descriptions in this application are considerably more involved and should contain:

- A set of part parameters (observable and latent)
- A stress factor definition
- A set of life state accumulation properties
- Aging functions
- Fault onset distributions and fault effects
- Failure mode distributions and effects

2.7. Simulation Overview

The simulation uses parallel and sequential Monte Carlo approaches. The sequential part simulates a single instance of a system, and the variations that may occur over the life of that system. These variations can be internal variations in

part parameters or external factors like usage characteristics or operating environment. The parallel part of the Monte Carlo allows for variation in the initial conditions, which may be limited to the seed for random number generation or may include manufacturing tolerance or build configurations (which may include nominally identical systems that have differing part replacement histories). The steps in the simulation loop used in the sequential Monte Carlo are shown in Figure 2.

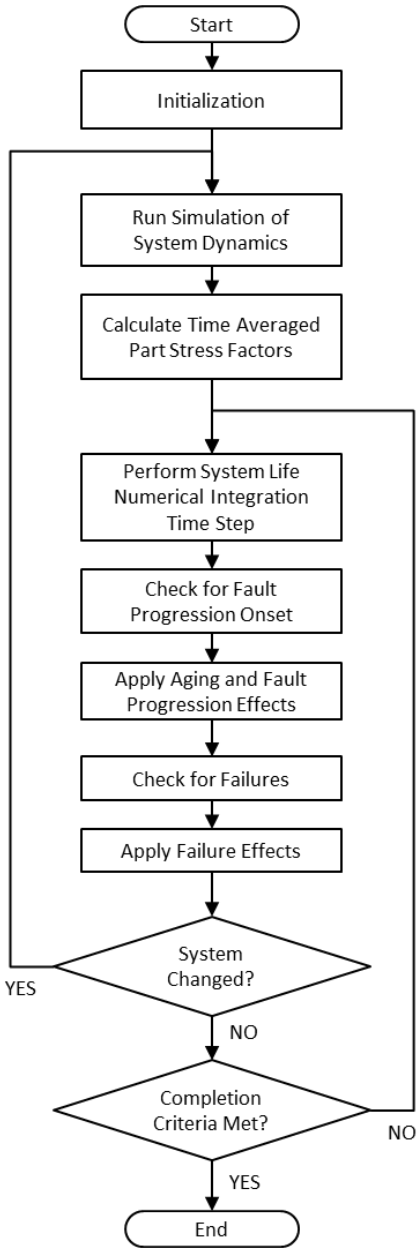

Figure 2. Simulation Steps

The numerical methods employed in running the simulation reuse and reinterpret the time series results from the simulation of the system dynamics in determining the amount of stress and life accumulated by the system. Only when the system is deemed to have changed sufficiently are the dynamic responses of the system re-simulated.

2.8. Specification Expression and Evaluation

In the assessment of robustness, aging and failures are simulated. The performance of the system is determined by measurement of some system properties against a set of rules. These properties can be time-domain simulation results, frequency domain transformations of simulation results or expressions formed from the set of available part parameters. A specification in the context of the framework is defined as:

<expression><operator><value><condition>

Where the expression contains the abovementioned system properties, the operator is a relational operator {=, ~=, >, >=, <, <=}, the value is a numeric or Boolean constant (but can also be another expression) and the condition is a constraint on the evaluation of the specification (evaluate subject to X being true, for example).

2.9. Use Cases

Use cases are the inputs to the dynamic model which indicate how the system is used. Each of these can be given a weighting, or in a more elaborate scheme, a usage sequence or schedule can be used over the life of the system. The set of use cases should describe in a complete sense the ways that the system will be used and the loads that the system will experience. Representations of the operating environment and ambient temperatures have been included.

2.10. Prognostics

By using techniques that take measurements of part parameters, either directly or by inference from system dynamic states or other parameters, prognostics aims to predict the time remaining before the system (or a part thereof) reaches the end of its life. Given the nature of the random behaviors incorporated into the simulation of system lives, and the nature of the inference algorithm, this prediction will have inaccuracies which can be classed as type I or type II errors:

- *Type I (False positive) error:* Prognostics falsely indicate imminent failure, system taken out of service to avoid failure effects resulting in a period when specifications are not met.
- *Type II (False negative) error:* Prognostics fail to indicate imminent failure, failure effects occur as they would have without prognostic.

2.11. Reliability, Robustness and Prognostics Assessment

A feature of the method is the comparative assessment of reliability, robustness and prognostic efficacy. Given the inclusion of fault and failure behavior, sets of system specifications and available prognostic techniques, the simulation results will indicate:

- the distribution of failures in time and their effects (a reliability analysis)
- the performance of the system with regard to the specifications over the range of part parameters (a robustness analysis)
- rates of false positive and false negative errors for the prognostic technique

3. AN RLC EXAMPLE

A resistor-inductor-capacitor (RLC) circuit serves to demonstrate clearly the essential features of the framework, without the distractions of a complex system. This example was chosen for its simplicity and for the fact that it calls out readily programmable sections of MIL-HDBK-217. The specifications and part parameters were selected arbitrarily, but such that simulation times were short. The inclusion of a thermal model was important for demonstrating coverage of a range of the stress factors. This example is not for the purpose of offering insight into the behavior of RLC circuits; the objective is to illustrate the incorporation of reliability behaviors in a time-domain robustness simulation. This example demonstrates the type of output data available and the reader is encouraged to envisage potential applications of the technique.

3.1. The System

The system was modeled using MATLAB/Simscape. Joule heating of each element was used in the thermal model. The thermal model was represented as a Cauer topology equivalent circuit. To enable calculation of the part stress factors, the model was required to output voltage, current and temperature time series. A schematic of the system is shown in Figure 3.

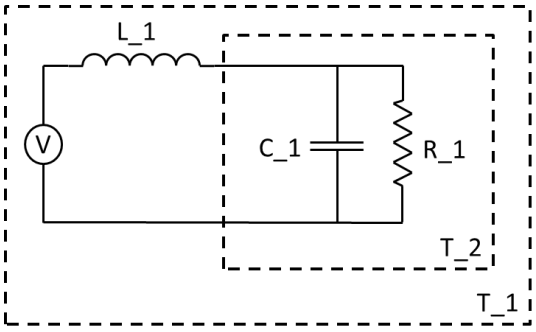

Figure 3. RLC circuit with thermal casings

3.2. Parts

Each part had a set of properties, parameters, aging functions and failure modes. Each part had exponentially distributed failure modes of *open* and *short*.

3.3. The Specifications

The specification applied to the circuit referred to the -3dB crossover frequency, which was calculated from the part parameters. The upper and lower limits for this frequency were defined as 2.340 and 2.436 radians per second, respectively.

3.4. System Usage

The use-cases for the model included sinusoidal and square wave input time series, and a range of ambient temperature and operating environment profiles.

3.5. Results

The results shown here are from a parallel Monte Carlo simulation where no variation was applied save for the random number generator seed. One hundred instances of the system were simulated with identical initial conditions and no through-life variation applied to the usage.

Figure 4 shows the variation in the characteristic frequency of the circuit as calculated from the part parameters. The vertical spikes are variations due to failure of a part - the distribution can be observed to be the result of constant hazard rate failures. The shaded regions correspond to the specification limits. There are breaches of the upper specification limit due to the aging of the parts.

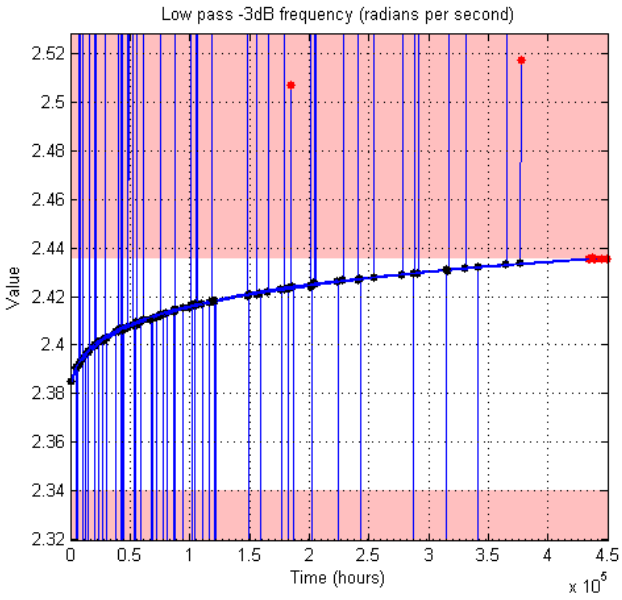

Figure 4. Through-life variation of frequency response characteristics

A selection of life states are shown in Figure 5. The randomized accumulation can be seen in the traces. The distributions of fault onset and failure are not representative as these life states were chosen for clarity of the graph.

The key aspect to these results is not the prediction regarding the reliability or robustness of the circuit, but that these data are the outputs of the same simulation.

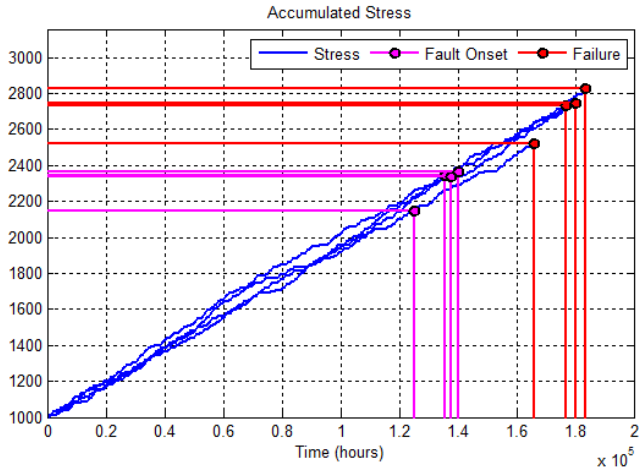

Figure 5. A subset of accumulated stress profiles

4. DISCUSSION

The results show the connection between simulation of the system dynamics, failures in the system and the adherence to the specifications for the system. The introductory example shows the type of outputs available using the framework; an enhanced demonstration would show the impact of variation of usage and operating environment on the reliability and robustness characteristics.

This following addresses advantages and disadvantages of the approach; it identifies key beneficial features and highlights areas which present new challenges in light of the novel techniques.

Advantages:

The incorporation of multiple types of part description into a model that captures causal relationships in a system yields an approach that can unify the analysis of a system design. This allows for trades between features of designs that were previously assessed by disparate means; reliability and robustness in particular. The unified analysis is well suited for complex systems. Application of variation in usage, operating environment and internal system states can yield variation in the reliability performance of the system and dominant system failure characteristics.

Models assessed against encoded specifications (and requirements) permits a closed loop design verification and validation methodology. Specification adherence in the face of applied variation forms the basis for an assessment of robustness. It can be argued that if the system design remains within the specification in the event of a failure, then the risk associated with the failure is mitigated by means of robustness. By the inclusion of the causal relationships of system parts, the impact of the long term presence of undetected degradations and failures to other elements of the system can be assessed. For example, if part A fails but the system remains in specification in the immediate term, is the long term performance of the system impacted due to increased stress on part B?

Further benefits are anticipated if this approach were coupled with executable specification modeling. This would permit early lifecycle design validation.

Other Considerations:

There is potentially a high computational expense of Monte Carlo simulations. Typical parallelization mitigations apply, but there are other mitigations that may yield substantially beneficial performance results:

- A database containing results for individual subsystems or units could allow for storage and reuse of costly simulation results.
- The consistent approach to modeling the many different types of behavior means that the execution of the simulation can be highly optimized.

It is recognized that the approach sets a high requirement for a large quantity of data about the parts of the candidate design. This may be offset with the development of libraries of standard parts, such that a design tool could make satisfaction of this requirement less challenging. Object oriented approach supports development of a library based design tool.

There is also a substantial outstanding burden to validate the approach against real world data, existing models and results from accelerated life testing. To that end, the use of the part stress approach is intended to be mathematically consistent with data in the standard, but the approach is not limited to standards based approaches. In the spirit of reliability standards, the methods demonstrated here are for the purpose of directing the attention of system designers at a stage where design decisions are critical.

Certain types of system may not be suitable for this approach and further work is required to determine the limits of applicability of the methods described here. Chaotic behavior, where the system state trajectories are highly sensitive to small deviations and variations from nominal can be simulated, however the computational burden may be well beyond reasonable limits.

5. CONCLUSION

An analytical framework to support systems-level decisions for robust performance has been presented. The "life state" method for time-domain simulation of unreliable systems has been explained. The methodology allows trade-space analysis on the appropriate use of prognostics to minimize the Size Weight and Power (SWaP) of redundant systems that otherwise would be needed. Significant potential benefits have been highlighted, yet further work is required to enhance demonstrations of the techniques described. It is anticipated that the development of these ideas will allow for better optimized designs, more unified analyses and a common approach to the design of reliable, robust and prognostic enabled systems.

ACKNOWLEDGEMENT

This work has been funded by the Air Force Research Laboratory (AFRL) through the Small Business Innovation Research (SBIR) program. Brett Jordan, AFRL technical point of contact, provided great support and encouragement during the course of this work.

NOMENCLATURE

CDF	cumulative distribution function
DAE	differential and algebraic equations
MTTF	mean time to failure
PDF	probability density function
RLC	resistor-inductor-capacitor

REFERENCES

Department of Defense (1995), Military Specification (MIL)-HDBK-217F NOTICE 2, *Reliability Prediction of Electronic Equipment*

Zio, E., (2009) Reliability Engineering: Old Problems and New Challenges, *Reliability Engineering and System Safety* **(94),** pp. 125-141.

Siu, N., (1994) Risk Assessment for Dynamic Systems: An Overview, *Reliability Engineering and System Safety* **(43),** pp. 43-73.

Kuehl, R. W., (2010) Using the Arrhenius Equation to Predict Drift in Thin Film Resistors, *CARTS Europe 2010 – 22nd Annual Passive Components Symposium*, (pp 121-133), November 10-11, International Congress Center, Munich, Germany.

BIOGRAPHIES

Nicholas A. Lambert, MEng, graduated from the University of Sheffield (UK) in 2006, with a first class honors degree in Mechanical Systems Engineering. He has keen interests in modeling, simulation & control as well as systems engineering. His experience includes modeling of physical systems, development for safety critical flight systems (BAE SYSTEMS – F-35 Fuel System IPT) and medical mechatronics design (with Imperial College London). Mr. Lambert's work has been centered on modeling fault progressions, failures, and prognostic algorithms, and has included development of design tools for assessment of reliability and robustness of dynamic systems with MATLAB/Simulink.

Kyle B. Ferrio earned the Ph.D. in Electrical Engineering and Computer Science from the University of Michigan at Ann Arbor. His research interests include topics in high-performance computing, algorithm development, and software modeling for complex and adaptive systems. His experience includes optimized design for optical fiber manufacturing, development of simulation codes for advanced optical systems and other computationally intense multi-physics modeling applications.

Douglas L. Goodman has an extensive background in electronic design, advanced diagnostics and prognostics, and test technologies. He has co-founded or managed other technology firms serving the industry, including Opmaxx (IC Test Software), Environmental Metrology Corporation (Process Metrology), and Analogy Inc. (Design Simulation). Doug received his BSEE from California Polytechnic State University, San Luis Obispo, and an MBA from the University of Portland and has held various managerial and engineering positions at firms including Tektronix and Honeywell.