CONF-970337--2 SAND96-2605C

Establishing Performance Requirements of Computer Based Systems Subject to Uncertainty

David Robinson

PO Box 5800 Mail Stop 0746
Sandia National Laboratories
Albuquerque, NM 87185-0746
drobin@sandia.gov

Abstract

An organized systems design approach is dictated by the increasing complexity of computer based systems. Computer based systems are unique in many respects but share many of the same problems that have plagued design engineers for decades. The design of complex systems is difficult at best, but as a design becomes intensively dependent on the computer processing of external and internal information, the design process quickly borders chaos. This situation is exacerbated with the requirement that these systems operate with a minimal quantity of information, generally corrupted by noise, regarding the current state of the system. Establishing performance requirements for such systems is particularly difficult. This paper briefly sketches a general systems design approach with emphasis on the design of computer based decision processing systems subject to parameter and environmental variation. The approach will be demonstrated with application to an on-board diagnostic (OBD) system for automotive emissions systems now mandated by the state of California and the Federal Clean Air Act. The emphasis is on an approach for establishing probabilistically based performance requirements for computer based systems.

Background

Establishing the performance requirements for a computer based system can be extremely difficult. The traditional approach is presented in Figure 1. In this case the requirements are established based vague system objectives, insufficient system modeling effort and on limited exposure to

This work was supported by the United States Department of Energy under Contract DE-AC04-94AL85000.

alternative implementation techniques. This approach results in requirements that may not be realistic or cost effective.

Figure 2 presents an alternative approach based on the well known precepts of systems engineering. In this case, all interested parties are involved with requirements definition (via the systems engineering modeling and analysis), a physical model is exercised to evaluated alternative solutions, and an optimum set of requirements are presented to the decision maker(s). While both approaches are iterative in nature, the first

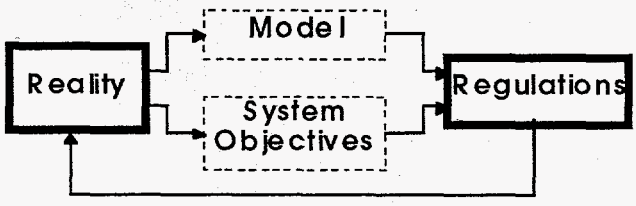

Figure 1. Typical Process for Regulation Development

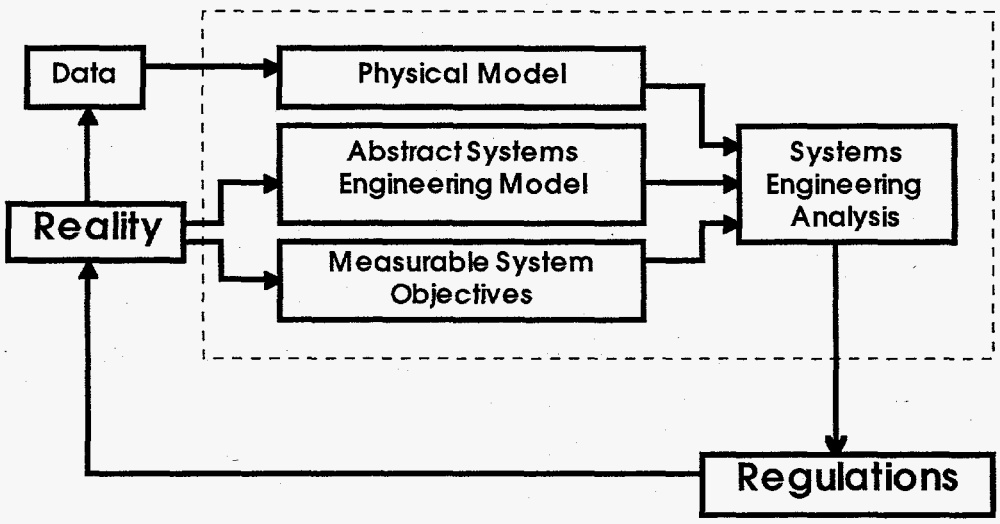

Figure 2. Systems Engineering Process for Regulation Development

approach is hindered by a lack of clear objectives and limited modeling. These deficiencies severely restrict communication of the regulatory impact on solving the problem (since the problem is never truly understood).

The design process for systems subject to uncertainty present some unique problems. The definition of requirements is complicated by the need to specify the performance of such systems in probabilistic terms. This difficulty arises primarily with the limited familiarity of most design engineers with the necessary probability and statistical analysis tools. The problem is further complicated by the need to simultaneously consider hardware and software performance as well as the performance of the decision algorithms embedded in the computer system software.

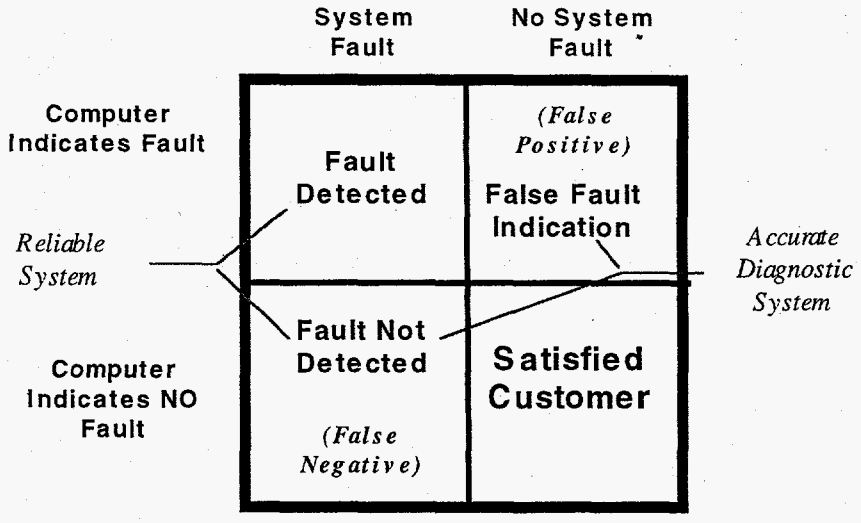

Figure 3. System Performance Decision Table

Figure 3 depicts the overall performance matrix of a typical decision process for a system subject to failure of system components combined with failure of the diagnostic algorithm. The upper left corner represents the situation where a system element has failed and the computer system correctly identifies the failure. The lower left corner represents the situation where the system has failed but the computer system fails to diagnose the failure either through failure of the computer hardware or a diagnostic error commonly referred to as a Type I error.

The upper right corner depicts the situation where no fault has occurred and the computer system falsely indicates a failure. This type of error is commonly referred to as a Type II diagnostic error. Finally, the lower right corner is the situation where not only has a system element not failed, but the computer does not indicate a failure: a very desirable state for the consumer.

For a time dependent system, it is necessary to maximize the time spent in the lower right corner or, similarly, minimize the time spent in the other three quadrants. Therefore, one design goal is to minimize the likelihood of being in the left hand column. This requires that the reliability of the hardware and software associated with the system, including the computer processor being used, be considered simultaneously with other performance objectives. In addition to the hardware reliability requirement, is the need to minimize the time the system spends in the upper right and lower left quadrant due to errors in the computer algorithm. Design of a robust diagnostic software system must be considered concurrently with reliable hardware design. The next section discusses an example where this approach to the design of computer based diagnostic system is sucessfully being applied.

Application

The California Air Resources Board has recently instituted the requirement that all passenger cars sold in California have the capability to diagnose emission system failure. These rules are known collectively as On-board Diagnostics II (OBD-II). While the primary function of the automotive OBD-II system is reduced automobile emissions, the diagnostic requirements affect several major vehicle systems including engine control, exhaust, evaporative purge and electronic transmission components. At the request of a colalition of Chrysler, Ford and General Motors, Sandia National Laboratories has been investigating alternative modeling and analyis schemes for the design of alternative OBD-II systems.

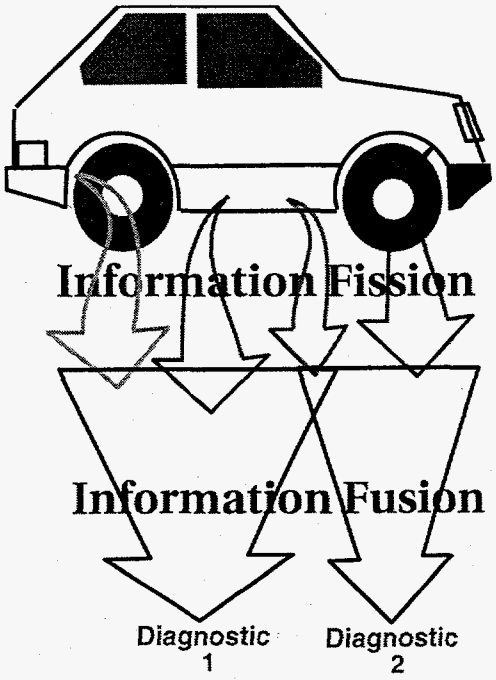

Figure 4. Diagnostic System

The overall objective of this design effort is the development of a robust OBD-II system with at least 150,000 mile expected lifetime. As depicted in Figure 4, information from approximately 32

different sensors is collected and processed through the on-board computer system. The current state of the sensor suite must be collected and decisions regarding the performance of the emission system made in real-time. Based on estimates of the current system state, a malfunction indicator light (MIL) is illuminated on the driver console. The consumer is then required to take the vehicle in for inspection and more detailed diagnosis by a repair technician. This technician must have the proper service equipment necessary to down load information from the computer system and interpret the associated diagnostic codes.

Establishing the performance requirements of such a system is difficult due to the competing nature of the system objectives. On the one hand, the regulatory agencies wish to assure that the public is protected from excess automotive emissions. The desire is for the MIL to be illuminated at the first indication of emission system failure. Alternatively, the automotive companies would prefer that the MIL be illuminated on a minimum number of occasions. Caught in the middle is the consumer.

Data collection and processing systems are inherently noisy and are compounded with variation in the manner and environment in which the consumer operates the vehicle. Temperature, humidity and even barometric pressure can all have a significant impact on the ability of a diagnostic system to evaluate the current state of an emission system. Vibration and corrosion are only two of the many factors which can significantly influence the failure characteristics of emission hardware. All of these factors must be considered when developing a general set of performance requirements for computer based automotive diagnostic systems.

Solution Approach

Working in conjunction with automotive design engineers from Chrysler, Ford and General Motors, analysts at Sandia National Laboratories are successfully applying a systems engineering approach to the design of the computer based diagnostic system. This specific approach involves

- the development of an evolutionary conceptual model,

- problem definition, including design constraints and alterables, and
- identification of the players involved (regulatory agencies, automotive companies, consumer, maintenance technicians, etc.).

The particular emphasis of this effort was the modeling and control of the uncertainty in the performance of the computer based diagnostic system (i.e. the OBD). Two simultaneous initiatives were undertaken: 1) modeling of hardware and software failure probabilities and 2) modeling of diagnostic error rates. As seen in Figure 3, these two efforts were necessarily inseperable in addressing the issues associated with the design of a robust computer based diagnostic system.

System Reliability

Two fundamental techniques were used for the reliability analysis of the system. The first involved the use of fault trees for modeling and analysis of the complex interaction of the system elements. However, the traditional fault tree approach was insufficient due to the limited information available regarding the failure characteristics of the various emission system components. For this reason, a Bayesian approach was incorporated into the fault tress analysis. This permitted the issues associated with data collection to be addressed objectively and quantitatively (How much failure information is needed? On what subsystems? What is the most cost effective scheme for collecting failure information?). Each

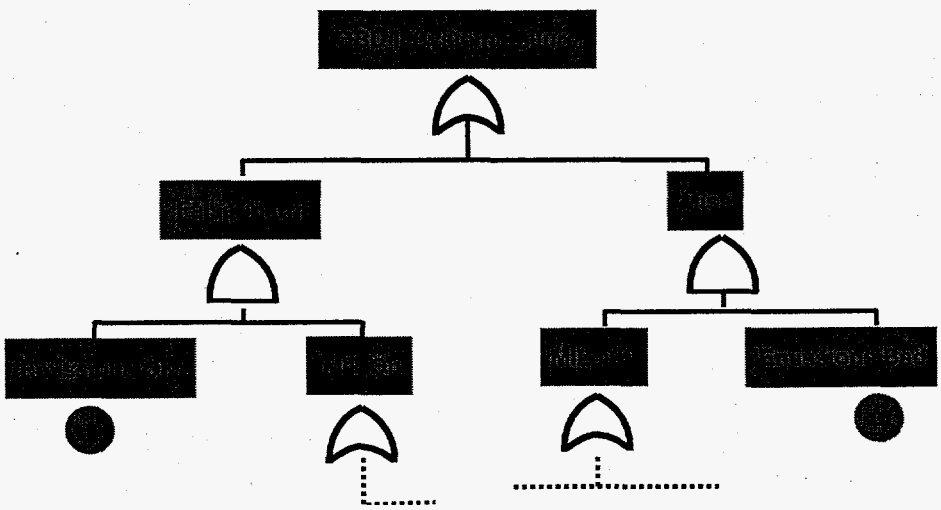

Figure 5. Typical Fault Tree

reliability characteristic therefore also had an associated uncertainty distribution. A generic fault tree approach was coupled with a Bayesian analysis scheme and incorporated into a reliability modeling software tool. Figure 5 depicts the very top level view of a typical fault tree.

Diagnostic Accuracy

A methodology based on the statistical concepts associated with power curves was used to develop a set of metrics for each of the system objectives. Power curves provide a simple, transportable means of evaluating the diagnostic performance of the OBD alternative. Power curves represent the likelihood of making a decision error assuming a true state of the system exists.

Figure 6 depicts a typical decision situation where two scenarios might exist: H_0 and H_1. The null hypothesis, H_0, represents the hypothesis that the vehicle is performing normally and the emission system performance characteristic is a random variable with mean μ_0 and variance σ_0^2. An alternative situation exists where, for some reason, the vehicle may not perform as expected and the performance characteristic increases such that it is now a random variable with mean μ_1 and variance σ_1^2. Periodically a decision must be made regarding the state of the vehicle: Is it operating correctly or has something happened to influence the performance characteristic?

A decision point must be established, whereby if the observed performance characteristic is above that value, it is decided that the vehicle is not operating correctly (point C in Figure 6). However, if the observed misfire rate is below the critical value, the vehicle is assumed to be operating correctly. Now, if the vehicle is operating satisfactorily, since the performance characteristic rate is assumed to be a random variable, there is a non-zero probability that the estimate of the

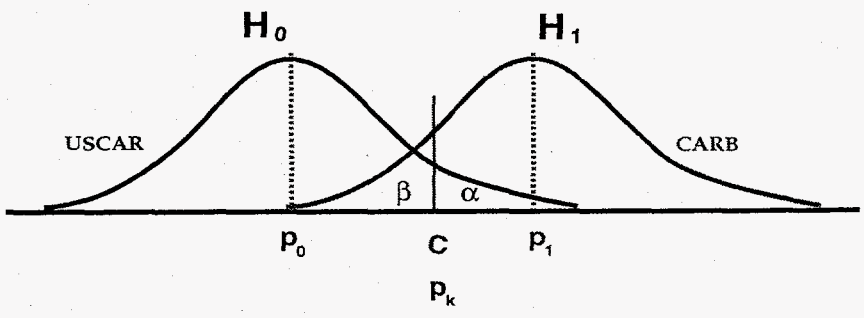

Figure 6. Uncertainty Characterization of System State

misfire rate will exceed the critical level. It is then decided that the vehicle is not operating correctly and a malfunction indicator light will be illuminated. The probability of making this incorrect decision is α and is generally referred to as a Type I error or the false alarm rate.

A similar situation can occur if the vehicle is not operating correctly and the decision statistic is less than the critical value. In this case, an error is made in assuming the vehicle is operating correctly when in reality a problem has developed. The probability of making this incorrect decision is β and is generally referred to as a Type II error or the miss rate.

The *power curve* combines these two errors into a convenient format. Define p_i as the misfire rate under hypothesis H_i. The power of a particular statistical test is defined to be:

$$\Pr\{\text{rejecting } H_i | H_i \text{ is true}\} = power$$

By fixing the critical test statistic, C, and varying the underlying misfire rate p_i, it is possible to generate a function which completely characterizes the errors associated with this particular hypothesis test. Figure 7 depicts a sample of such a curve. Statements regarding the Type I error (α) and Type II error (β) can then be made and an independent comparison of the robustness of various decision algorithms can be accomplished by simply comparing the associated power curves.

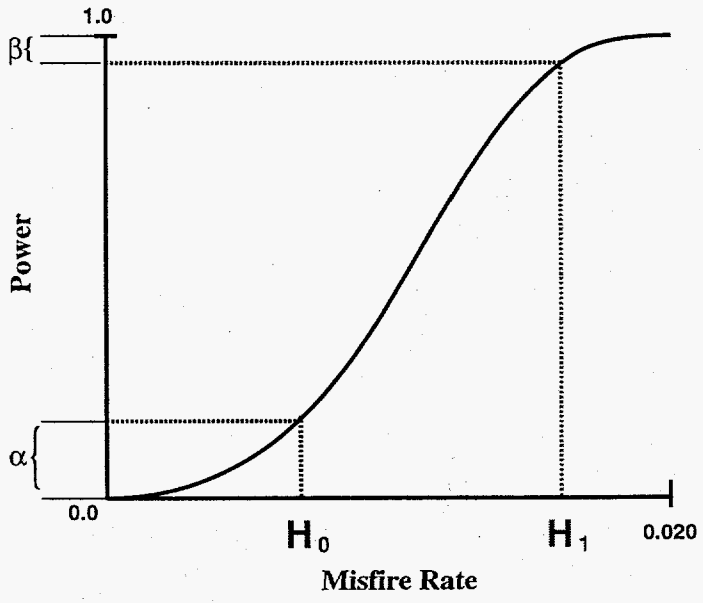

Figure 7. Power Curve with Type I and Type II Errors

Results

As a result of the application of a systems approach to the design of a robust computer based diagnostic system, a preliminary characterization of both the hardware and software reliability of the system was possible. Figure 8 depicts a typical output from a reliability analysis of one diagnostic. A sample of a comparison between different diagnostic strategies is depicted in Figure 9.

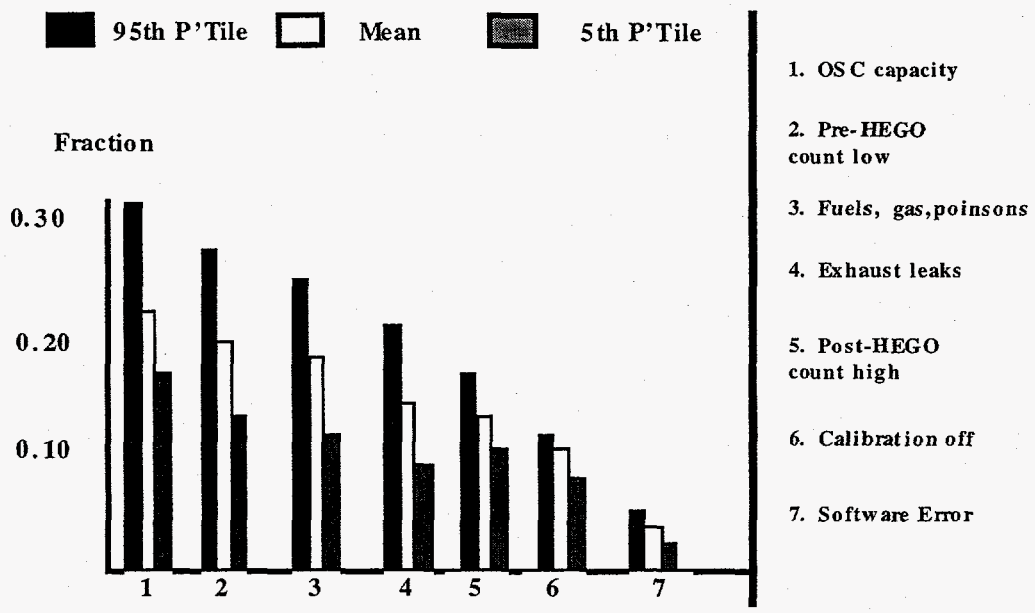

Figure 8. Pareto Analysis of Top Contributors to System Failure

Conclusion

As a result of the above effort, CARB is reviewing the current requirements for OBD-II to permit alternatives to the existing regulations. Efforts are continuing to refine the reliability analysis tools as well as the statistical tools necessary for evaluating diagnostic software algorithms. These tools are allowing the automotive manufacturers to accelerate the pace at which alternative diagnostic sensors and algorithms are identified and evaluated.

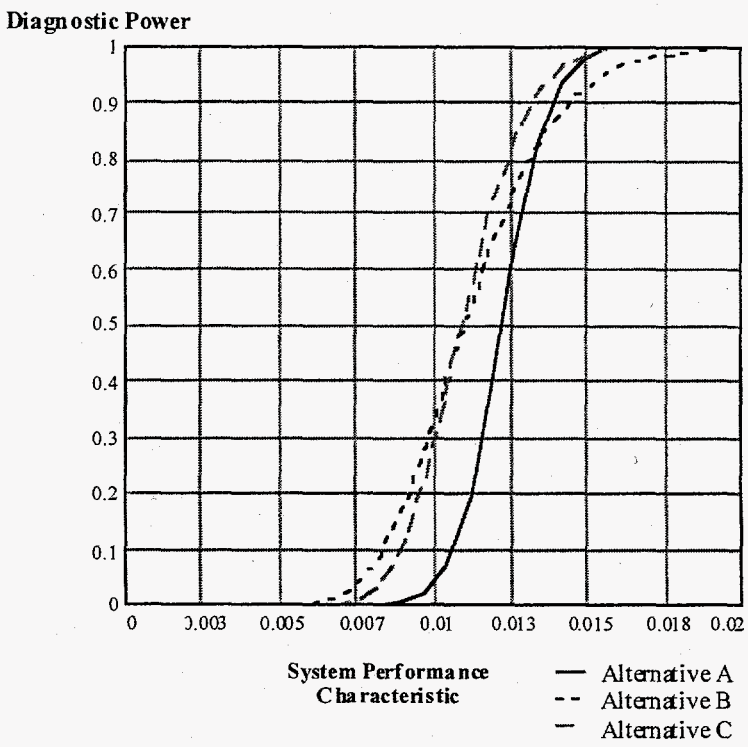

Figure 9. Typical Power Curve

It is clear that proper application of a systems engineering approach to the design of computer based systems can lead to shorter development time and more realistic, cost effective solutions. While foreign to most design engineers, the use of statistically based methods can provide a set of metrics that permits inclusion of uncertainty during the design process. This uncertainty is inherent in all real-world applications of computer based systems and without adequate consideration could lead to systems that are overly sensitive to variation in the operating environment. Inclusion of uncertainty also assists in the identification of critical factors within the design and permits these problems to be addressed in an objective fashion. Since most designs are evolutionary in nature, by addressing the problems identified by the uncertainty metrics, the data collection and feedback process can be focused during the redesign effort, resulting in much shorter development times.

The systems approach and the uncertainty analysis techniques are not in themselves particularly difficult, but require design engineers to have an open mind when dealing with new applications of computer based engineering systems. The result will be increased communication flow of critical

issues throughout the design process resulting in a product reaching the market sooner and robust to both anticipated as well as unanticipated operating conditions.

Acknowledgments

This work was supported by the United States Department of Energy under Contract DE-AC04-94AL85000.