IEEE 1995 Nuclear Science Symposium and Medical Imaging Conference, **San Francisco, CA, Nov. 1995.**

A Methodology and Tool for Measurement-Based Dependability Evaluation of Digital I&C Systems in Critical Applications

Dong Tang, Myron Hecht, and Herbert Hecht
SoHaR Incorporated, Beverly Hills, California

Abstract[1]

This paper presents an overview of a measurement-based dependability[2] evaluation *of digital safety systems and describes a software tool under development for it. The approach is based on measurements on operational systems and dependability models to provide quantitative assessments for system reliability and availability with stated confidence levels. A tool is being developed to automate the approach. Experience in use of the methodology are briefly discussed.*

1. Introduction

Both IEEE-Std-603-1991 [IEEE91] and IEEE-Std-7-4.3.2-1993 [IEEE93] include quantitative reliability criteria. The issue of the probability of failure on demand of a safety system is also a key factor in the regulatory process. However, methods and techniques for determining the dependability of digital systems which include software may not suitable for nuclear safety systems if very high reliability requirements are imposed. Such requirements may arise as a result of the allocation of system level quantitative safety and reliability requirements to digital safety systems.

Software reliability estimation techniques [Musa87] cannot be used in such cases because they require execution time that will produce at least five failures for the specified reliability under conditions equivalent to operational usage in order to have a reasonable estimate of mean time between failures (MTBF) at the 95% confidence level [Hogg83]. A totally test-based approach will also not suffice. For example, in order to show a probability of failure (PFD) of less than 10^{-6} with 95% confidence using system level testing, it would be necessary to run nearly 3 million independent test cases[3]. Use of only dependability models such as Markov chains [Sahner87] to analyze conditions that can lead to failure is equally unsuitable because there are no creditable data sources for transition probabilities from operational to non-operational states. The measurement-based approach builds on the complementary strengths of all these mentioned techniques and permits, at least under favorable conditions, creditable assessment of the reliability of safety systems. As such, the methodology represents a promising approach to addressing some of the design and licensing issues associated with digital safety systems.

Measurement-based analysis of computer system dependability has evolved into a mature process since the first work in that area more than 15 years ago [Iyer95]. However, these techniques have not yet been applied to safety grade systems in nuclear power plants. Issues of special concern in safety systems include an intermittent duty cycle for the application software and dealing with correlated and common cause failures.

This paper describes how these issues may be addressed in a combined measurement-based and modeling approach when it is applied to safety systems. Section 2 presents an overview of the methodology; section 3 provides background and discussion on using the methodology for safety systems; section 4 describes the design for a software tool currently under development; section 5 concludes the paper by briefly reviewing experience in using the methodology.

2. Methodology Description

The measurement-based methodology was developed based on previous work in computer hardware/software failure measurement and probabilistic analysis [Tang93, Iyer95]. The process consists of the following steps: Data collection, Data classification, Statistical analysis, and Dependability modeling. These steps are described in the following paragraphs.

[1] The opinions and viewpoints expressed herein are the authors' personal ones and do not necessarily reflect the criteria, requirements, and guidelines of the U.S. Nuclear Regulatory Commission (NRC).

[2] The concept "dependability" was proposed at the *15th International Symposium on Fault-Tolerant Computing in 1985* [Laprie85]. Dependability is defined as the "quality of the delivered service such that reliance can be justifiably placed on this service." The dependability impairments are faults, errors, and failures. The means to achieve dependability is through fault avoidance and fault tolerance. Two major measures of dependability are reliability and availability.

[3] This result is based on the use of the Binomial distribution and the assumption of independence between trials. The relation is $n= log(\alpha)/ log (1-p)$where α is the level of significance (1-α is the confidence level), p is the probability of failure on demand, and n is the number of trials [Tang95b].

Data collection. In this step, data on failures, the system configuration, operating time, test configuration, test procedures (if applicable), and other related data are collected. These data may be available in a variety of forms (automatically generated logs, manually generated event reports, test reports, test plans, vendor data, etc.). Ideally, the failure data should be from the operational environment and for all modes in which the system will be run, However, this is not always possible. For example, safety events causing challenges to the safety systems are rare. Thus a major consideration is to make the best use of available data from testing, operation, or from similar systems.

Data classification. In the classification step, the failure data are categorized and evaluated. The classification categories and evaluation criteria are unique to each system. However, one general consideration is to distinguish between failures whose causes can be addressed through developmental or administrative controls in accordance with the quality criteria of IEEE Std 7-4.3.2-1993 (controllable failures) and those which are not controllable. The general criteria for identifying such failures include (1) a known root cause, (2) failures occurring in a process under the control of the safety system developer or the installation and maintenance process of the user, and (3) a means of determining that the failure has been mitigated[4].

On the other hand, failures in the not controllable category are handled by statistical analysis and modeling. The basic assumption is that in a well tested system with a mature development process, failure and recovery are stochastic processes. That is, the predominant failure mechanisms are due to the interaction of randomly arriving inputs in a stable operational environment which interact with residual defects in the code or the hardware to cause failures. The extent to which this assumption is valid has to be verified by examining the causes identified in the failure data.

Statistical analysis. Once the appropriate failure data have been identified, statistical analysis methods identified in earlier work are used to provide point estimates and confidence intervals for failure rate (based on the chi-squared distribution), failure detection/ recovery probability (also called *coverage*) and probability of success upon demand (based on the binomial distribution), and to quantify probability of multiple correlated or common cause failures (correlation coefficients and conditional failure probabilities). The statistical analysis methods can also be used on the system level or for individual components to

- construct distributions for events such as challenges to safety systems,
- understand relationships between parameters and identify correlations, and
- determine trends such as reliability growth or degradation.

Dependability Modeling. In this step, system level dependability values are calculated based on the values of the parameters from the previous step. This step can be used for

- assessing current availability,
- identifying problem areas,
- predicting required test durations for achieving desired availability levels, and
- performing sensitivity analyses to determine the impacts of changing parameters.

Further details on the methodology are discussed in [Tang95a]. The following section provides additional background and discussion on how the methodology can be applied to a safety system.

3. Background and Discussion

Most previous work on measurement-based dependability assessment has been for highly available continuously operating systems. Such systems can be characterized by capacity or load profiles, failure rates, and availability. Because of their continuous operation, highly available systems permit systematic studies of failure mechanisms and occurrence rates that can be used to build and validate measurement-based software reliability models. The first subsection discusses significant differences between safety systems and other highly available systems which have been the subject of earlier research in this area; the second subsection introduces a model that can be used for a class of safety systems. The third and fourth subsections discuss approaches to estimating two important parameters: the success probability of the application software and the probability of multiple simultaneous failures due to a single common cause event.

3.1 Differences Between Safety Systems and Other Types of Highly Available Systems

Safety systems differ from the highly available continuously operating systems discussed above in the following ways:

1. *Both continuous and intermittent operating profiles.* Safety systems also constantly monitor a set of parameters, and thus, the work on continuously operating systems is applicable. However, an additional factor in safety systems is that the operational profile of the application software for the alarming or safety mitigation function will be intermittent.

[4] If the failure has been mitigated and all associated faults have been identified and removed, it may be reasonable to assume that the specific relevant category of failures will not occur.

2. *Importance of rare events such as common cause failures and correlated failures.* Unusual or rare events must be accounted for in the dependability predictions for critical systems. The incidence of common cause and correlated events can be measured and accounted for in the model. However, most such data will emerge from the testing environment, and determining whether the test or development environment is sufficiently similar to the operational environment is not always straightforward.

In order to demonstrate how the methodology accounts for these differences, the following subsection presents a model of a safety system. The subsequent subsections describe how the key parameters associated with the model can be estimated.

3.2 A Safety System Model

Figure 1 shows a Markov model for a safety system such as a reactor protection system. The modeled configuration has two major components: a plant and a digital safety system which protects the plant by responding to and processing challenges from plant instrumentation.

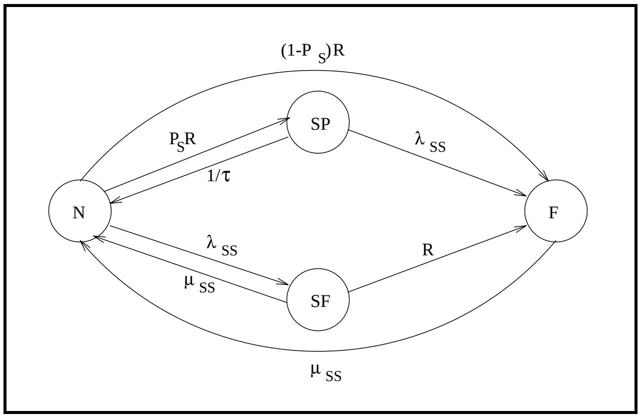

Figure 1 A Safety System Model

The notation used in the model is as follows:

N Normal state in which both safety and plant are functioning within technical specifications

SP Safety processing state in which the safety system is processing a challenge

SF Safety failure state in which the safety system is not available for responding a challenge while the plant is functioning with technical specifications

F System failure state in which the safety system has failed to process a challenge

P_S Probability of success upon demand, i.e., that the safety system will be successful in responding a challenge

R Arrival rate of challenges from the plant requiring a response of the safety system

τ Challenge processing time

λ_{SS} Failure rate of the safety system (including both correlated and uncorrelated failures of hardware and system software)[5]

μ_{SS} Recovery rate of the safety system after a failure

In the normal state, if a challenge arrives, the safety system will respond to it successfully with probability P_s and go to the safety processing state SP (modeled by the transition P_sR, from N to SP). During the safety processing, if the safety system fails due to its hardware or software problems, the system will fail (transition λ_{SS}, from SP to F). Otherwise, the safety system will go back to the normal state after the mean processing time τ (transition $1/\tau$, from SP to N). When a challenge arrives in the normal state, the safety system may respond to it unsuccessfully and go to the system failure state (transition $(1-P_s)R$, from N to F). Sometimes the safety system fails in the normal state and goes into the safety failure state SF (transition λ_{SS}, from N to SF). The safety system will go back to the normal state with rate μ_{SS} (transition μ_{SS} , from SF to N). But during the recovery period in the state SF, if a challenge arrives, the system will fail (transition R, from SF to F) because the safety system is not available for use in this state. Table 1 shows how the safety-related concerns identified in the opening paragraph are accounted for in this model.

Table 1. Key Issues Addressed by the Model

Issue	State or Transition in Figure 1	Remarks
Continuous and intermittent operation	Intermittent operation modeled by N to/from SP transitions	P_S is key parameter (see Section 3.3)
	Continuous operation modeled by N to/from SF transitions	λ_{SS} is key parameter and is evaluated from a separate submodel
Common cause or correlated multiple events causing safety system failure when needed	N to SF transition includes such failures	The coverage factor in the hot-standby submodel (Section 3.4.) accounts for common cause and multiple correlated failures
	SF to F transition models the joint event that the safety system is down and a challenge occurs	

3.3 Estimating P_s

One approach to estimating the probability of success upon demand, P_s, is by means of measuring the proportion of successful test runs from test data and using the binomial distribution to determine the confidence interval. Because safety systems typically have fairly simple and well defined functions, and because these functions must generally be unambiguously timely and effective, their success can be described as a simple Bernoulli trial.

[5] This value of failure rate is based on the result of a submodel which describes the extent and type of redundancy used in the safety system. A model for a hot-standby system is shown in Figure 3.

However, the validity of this approach is based on the assumption that the test environment was representative of the plant operational environment. This is not always possible to determine. In a safety system, it is unlikely that the system design or testing activity would not address conditions known to be likely to result in a catastrophic failure, i.e. those failures which may totally disable the safety system and are modeled as 1-P_s in Figure 1.

Thus, a major question is what measurement should be made to account for catastrophic system failures, even if they have not yet been observed. It may be possible to use the results of earlier work which has shown that catastrophic failures in well-tested systems (not only digital systems) usually result from the coincidence of a number of independent conditions that are individually tolerable or, at least, non-catastrophic [Hecht94]. Some examples are documented in NUREG/CR-6293 [Hecht95]. The rate of occurrence of non-catastrophic predecessor can be often estimated based on reported failures. An estimate of the probability of a catastrophic failure can then be determined by the combined probability of two or more of individual predecessor events. Whether the combined probability is a simple product of two individual probabilities or another function that incorporates both individual probabilities and correlation parameters can be determined by a correlation analysis.

3.4 Estimating λ_{SS}

The parameter λ_{SS} is the failure rate of the safety system hardware and software due to either multiple simultaneous random failures or due to a single common cause event. Estimation of this parameter is incorporated into a lower level model, or submodel. Figure 2 shows an example of such a submodel for a system consisting of two channels: a primary (or "hot") channel, and a standby channel.

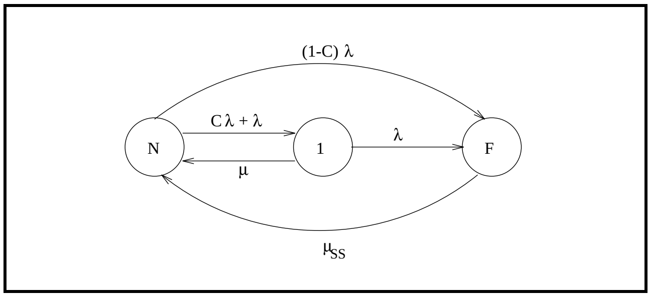

Figure 2 A Markov submodel for a hot-standby safety system with 2 Redundant Channels

The notation used in the model is as follows.

N Normal state in which both primary and standby channels are functioning

1 State in which one channel has failed and another channel is functioning

F Failure state in which both primary and standby channels have failed. This state is equivalent to SF in Figure 1; the total transition rate from N to F represents λ_{ss} in Figure 1.

λ Failure rate of a channel

μ Recovery rate of a channel

μ_{SS} Recovery rate of the safety system after a failure

C Probability that switchover to the standby will be successful when the primary channel fails. The complement of this quality, or 1-C, is the probability of a common cause or correlated failure at the system level which defeats both channels.

In the normal state, either the primary or the standby channel can fail. If the primary channel fails, the system will switchover to the standby successfully with a probability C (coverage). This is modeled by a transition from state N to state 1 with rate Cλ. If the standby channel fails, the system will also go to state 1, but with a transition rate λ. Thus, the aggregate rate of the transition from state N to state 1 is Cλ+λ. During the recovery of the failed channel (state 1), if another channel also fails, the system will fail, which is modeled by the transition from state 1 to state F. There is a possibility, 1-C, that the switchover to the standby will not be successful, which leads the system directly to the failure state F. This is modeled by the transition from state N to state F with rate (1-C)λ. After a system failure, the system will recover from the failure at a rate μ_{SS}, modeled by the transition from state F to state N marked by μ_{SS}.

Other models would be appropriate for different redundancy schemes. For example, in a four-channel reactor trip system, a 2-out-of-4 parallel reliability block diagram model could be used to handle multiple independent randomly occurring failures. Common cause and correlated failures could be modeled by Markov models similar to that in Figure 2. The output of these models could then be incorporated into the higher level Markov model shown in Figure 1.

4. The MEADEP Software Tool

A modeling tool called MEADEP (MEAsure DEPendability), is being developed to implement the data classification, analysis, and dependability modeling described in Section 2. The tools includes a data editing and processing module, a statistical analysis module, a model generation module, and a model solution module.

A library of model profiles will be an important part of MEADEP. A model profile defines the structure of a dependability model for a particular system, but does not contain the parameter values. To generate an evaluatable model, the required parameter values must be specified, either entered manually or obtained by the statistical module from failure data. Finally, the model solution module in MEADEP solves the model for results. The library frees users in nuclear utilities and other critical areas from the need to develop structured models. The library will be expandable to accommodate all likely dependability models of interest to customers.

All interactions between the user and the software modules discussed above are through a graphical user interface. The interface is menu-driven with extensive prompt and help information. Numerical results from statistical analysis and model solution modules can be converted to visual graphs (e.g., reliability or availability curves). Further details on the tool are discussed in [Tang95a].

5. Discussion and Conclusion

The methodology described in this paper consists of feasible and defensible methods in data collection and processing, statistical analysis, and dependability modeling. It assesses system dependability based on data with a reasonable size and allows evaluation of system dependability at a specified confidence level.

The methodology has been applied to three systems: an integrated control and safety system (ICS) under development, a plant protection system (Eagle 21) during early operation, and an air traffic control system (ATC) under development [Tang95a]. In ICS, data were gathered during the development and early test phases at a plant simulator. There was not sufficient operational time during which failure rate data could be gathered and assessed[6]. Thus, the primary focus of the data analysis was in the data filtering and classification step, i.e., to understand how to filter data and understand the qualitative aspects of the failure process.

In the plant protection system, data were collected during the first operational period of Westinghouse Eagle 21 systems at the Sequoyah Nuclear Plant [TVA90]. In contrast to the ICS case, the system was operational and therefore there was sufficient operating time to determine lower confidence limits on failure rates. Because operating time measurements were available, it was possible to estimate an upper bound for failure rates. However, the data which could be used to determine P_s were sparse because of the lack of safety events (challenges) in the operational environment. Thus, additional test data would be needed in order to provide a sufficiently large sample from which this parameter could be calculated.

Data from the ATC system undergoing stability tests were used successfully to estimate model parameters [Tang95b]. The key to this success was the existence of an automated data collection capability and an adequate amount of operational time (2000 processor hours). These characteristics permitted estimation of the coverage of the fault tolerance provisions and evaluation of system availability based on a model similar to that shown in Figure 2.

However, additional work on the methodology is necessary in order to develop approaches in dealing with non-deterministic failures introduced by controllable factors in the development process. Additional case studies are necessary in order to gain more experience and improve the library of models that will be included with the MEADEP tool.

Acknowledgment

This research was supported by the U.S. Nuclear Regulatory Commission (NRC) under Contract NRC-04-94-061.The authors wish to express their appreciation for the comments provided by Mr. Robert Brill, Project Manager.

References

[Hecht94] H. Hecht and P. Crane, “Rare Conditions and Their Effect on Software Failures,” *Proceedings of Annual Reliability and Maintainability Symposium*, Anaheim, CA, pp. 334-337, Jan. 1994.

[Hecht95] H. Hecht, M. Hecht, G. Dinsmore, *et. al.*, *Verification and Validation Guidelines for High Integrity Systems*, U.S. Nuclear Regulatory Commission and Electric Power Research Institute Report NUREG/CR-6293, March, 1995.

[Hogg83] R.V. Hogg and E.A. Tanis, *Probability and Statistical Inference*, 2nd Ed., Macmillan Publishing Co., New York, 1983.

[IEEE91] IEEE, *Standard Criteria for Safety Systems for Nuclear Power Generating Stations*, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855, USA.

[IEEE93] IEEE, *IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations*, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855, USA.

[Iyer95] R.K. Iyer and D. Tang, “Experimental Analysis of Computer System Dependability,” in *Fault Tolerant Computer System Design*, D.K. Pradhan (ed.), Prentice-Hall, 1995.

[Laprie85] J.C. Laprie, “Dependable Computing and Fault Tolerance: Concepts and Terminology,” *Proceedings of the 15th International Symposium on Fault-Tolerant Computing*, pp. 2-11, June 1985.

[Musa87] J. Musa, A. Iannino, and K. Okumoto, *Software Reliability: Measurement, Prediction, Application*, McGraw-Hill Book Co. 1987.

[Sahner87] R. A. Sahner and K. S. Trivedi, "Reliability Modeling Using SHARPE", *IEEE Transactions on Reliability*, vol 36, pp. 186-193, February 1987.

[Tang93] D. Tang and R. K. Iyer, “MEASURE+ — A Measurement-Based Dependability Analysis Package,” *Proceedings of the ACM SIGMETRICS Conference on Measurement and Modeling of Computer Systems*, Santa Clara, CA, pp. 110-121, May 1993.

[Tang95a] D. Tang, H. Hecht, Measurement-Based Dependability Analysis for Critical Digital Systems, SBIR NRC-04-94-061 Phase I Final Report, SoHaR Inc., May 1995.

[Tang95b] D. Tang and M. Hecht, “Evaluation of Software Dependability Based on Stability Test Data,” *Proceedings of the 25th International Symposium on Fault-Tolerant Computing*, Pasadena, CA, pp. 434-443, June 1995.

[TVA90] TVA Letter to NRC Dated May 10, 1990, *Sequoiyah Nuclear Plant (SQN) — Eagle 21 Functional Upgrade Commitments*, NRC Public Document Room, Accession #910715001.

[6] It should be noted that this system incorporated hardware and system software for which operational data are available and for which the lower limits of system level failure parameters could be estimated.