

## POWER2007-22119

### MARKOV MODELING APPLICATION TO A REDUNDANT SAFETY SYSTEM

George Adams and Fernando Ferrante  
Center for Nuclear Waste Regulatory Analyses  
Southwest Research Institute®  
6220 Culebra Road  
San Antonio, Texas 78238  
(210) 522-4957  
gadams@swri.org

#### ABSTRACT

Redundancy of components and subsystems is part of the design of reliable complex engineering systems used in several industrial applications, including power generation facilities. Such engineering systems may be in one or more intermediate operating states at various times. For example, these systems could continue operating during the repair of failed components and during maintenance intervals. For this reason, they do not lend themselves well to traditional reliability modeling techniques that do not account for a system's progression through various intermediate states. The use of traditional reliability modeling techniques may lead to significantly different estimates of the performance of a complex system required to exhibit high reliability.

This paper discusses the application of a Markov modeling approach for the development of reliability estimates of complex engineering systems. This approach is expected to have advantages for modeling reliability for such systems, since they are commonly comprised of redundant sets of components and require a strict set of maintenance operations to ensure their reliability.

#### NOMENCLATURE

The following nomenclature is used in this paper.

I	Identity Matrix
M	Fundamental Matrix
MTTF	Mean Time to Failure
Q	Truncated Stochastic Transition Probability Matrix
R	Failure Rate
$m_{ij}$	Element Corresponding to Row i and Column j of the Fundamental Matrix

#### INTRODUCTION

Maintenance intervals and the duration of maintenance become important when analyzing a system that is designed to operate continuously. Such a system may become vulnerable during maintenance operations. For example, maintenance may be conducted on one train of a two-train redundant system, and during this maintenance operation, a failure may occur in the running train, resulting in a system failure.

As an example of a system that requires continuous operation and can become significantly complex in large industrial applications, a hypothetical Heating, Ventilation, and Air Conditioning (HVAC) system was chosen for conceptualization and modeling in this paper. In applications where the HVAC system is expected to filter air that can be potentially contaminated with hazardous particles and may need to maintain negative differential pressure for containment of hazardous releases within a facility (such as in nuclear facilities), the estimated failure rate and its related uncertainty become crucial aspects of the design. The problem with applying traditional fault tree analysis is that it does not lend itself well to analyzing the reliability and availability of systems with the possibility of repair, since they consist of several components that can exhibit multiple states (e.g., normal, failed, standby). Markov techniques can be used to estimate failure rates for systems such as these, which may also have different modes of operation, as well as to assess the level of vulnerability of the system and the effect of a specific maintenance approach. In this paper we apply this approach to the HVAC system described above to illustrate the benefits of such methodology.

The failure rate for a hypothetical HVAC exhaust system may be estimated in a variety of ways. In this

paper, estimated failure rates for analyzing the system were generated using analytical and simulation-based Markov techniques and then compared to those obtained using fault tree analysis. Markov techniques can be applied to model these systems by breaking them down into a set of operating (or failed) states with an associated set of transitions among these states. Markov modeling is performed after a set of system states is defined. Generally, system states are characterized by (1) all components operating normally, (2) one or more components in a failed state or operating at reduced capacity while the system is still functional, or (3) one or more components in a failed state or reduced capacity while the system is no longer functional.

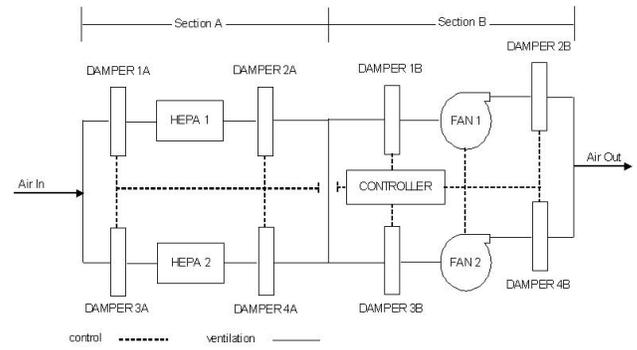
The analyses show the overall approach by identifying failure modes and system states, modeling of the system including maintenance considerations, consideration of uncertainty, and comparison of the results to those from other modeling techniques. The efficiency of the proposed Markov approach to reliability modeling is demonstrated by modeling a HVAC system.

The results support the use of the Markov model in such applications (i.e., complex engineering systems) while illustrating differences with the traditionally used fault tree analysis. In these analyses, the fault tree technique produced more conservative failure rates than those obtained through Markov techniques.

## MODEL DESCRIPTION

The hypothetical HVAC exhaust system in this paper is simplified from its actual complexity to illustrate the different failure rates that are estimated from the fault tree approach and analytical and simulation-based Markov techniques. While this simplification is performed to facilitate clear illustration of the techniques, more complexity can be added to the Markov model. Where systems become too large for full analysis, simplifications can be performed through the use of engineering judgment and system knowledge, as commonly done with other techniques such as fault tree analysis.

A schematic for the hypothetical HVAC exhaust system is shown in Fig. 1. Air flows through the system from left to right. In this figure, two sections are assumed (A and B), each with redundant trains. The air is filtered in Section A and then exhausted through Section B to the environment. The operating train in Section A includes Damper 1A, high-efficiency particulate air (HEPA) filter HEPA 1, and Damper 2A. The redundant train for Section A is composed of



**Figure 1. Schematic for a Hypothetical HVAC Exhaust System**

Damper 3A, HEPA 2, and Damper 4A. In Section B, the operating train includes Damper 1B, Fan 1, and Damper 2B; while the redundant train includes Damper 3B, Fan 2, and Damper 4B. In this system, for either section, one train is operating and the other one is in standby at any time. If a failure occurs in the operating train, then the controller automatically places the standby train online, if the standby train is available. Otherwise, a system failure occurs. Failure of the system is defined as the inoperability of both trains in either section. A train can become inoperable due to maintenance or component failure. Subsequent system failure occurs if a component fails in the running train. In addition, for this system, a single controller is used for which failure of the controller results in failure of the system regardless of the system state prior to the controller failure. Also, for simplicity, failure of the HEPA filters (i.e., HEPA1 and HEPA2) is not considered in this analysis; although they are included in Figure 1 to exemplify the arrangement of components commonly found in such systems. These could be added to the analysis, but for simplicity purposes, as mentioned above, they are not considered since it is not expected that this would enhance the illustration purposes of the approach further.

## MARKOV METHODOLOGY

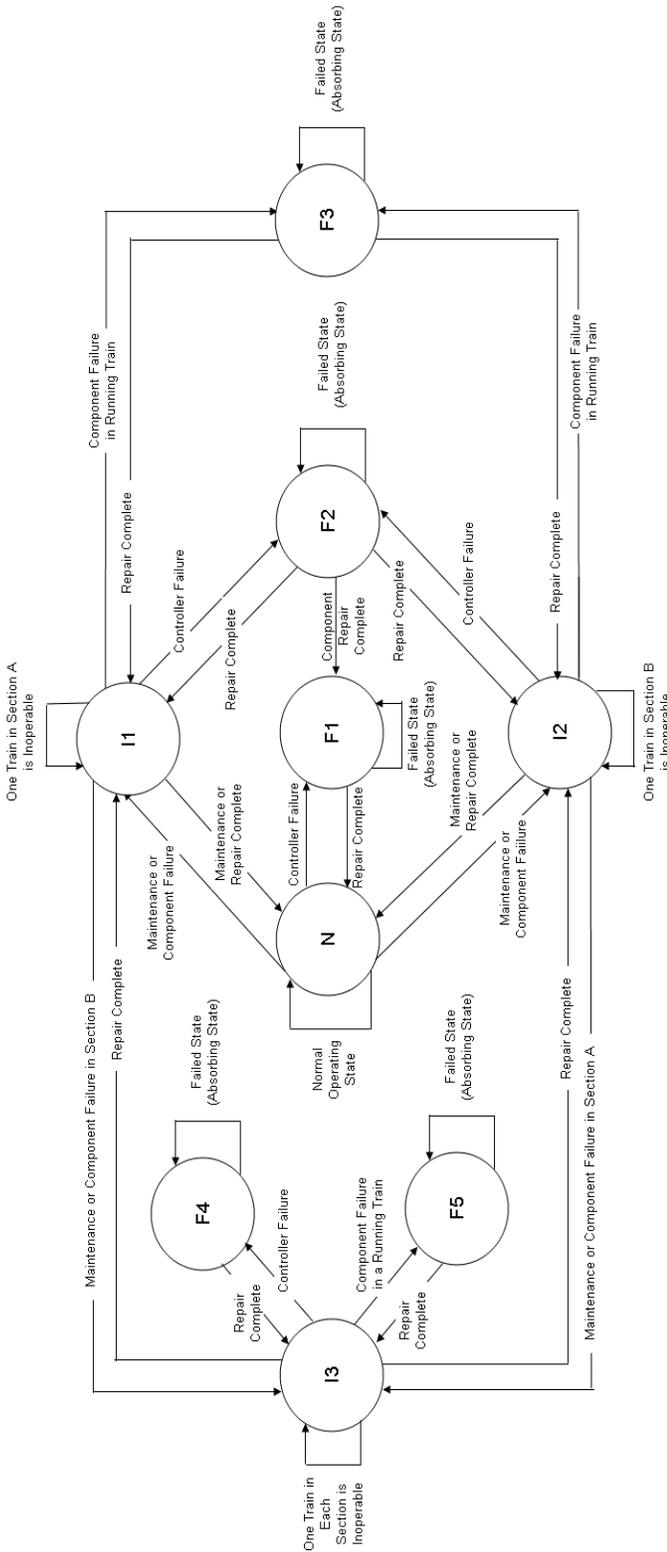
To develop the Markov model, a set of discrete system states is defined, and a set of transition rates from one state to another is determined [1]. The transition rates are developed from component failure rates and component repair/maintenance restore rates. Fig. 2 shows the system states identified in the Markov model for the hypothetical HVAC exhaust system. There is one normal operating state, identified as state “N,” three intermediate operating states in which one or more trains are inoperable (i.e., I1, I2, and I3), and five states in which system failure occurs (i.e., F1, F2, F3, F4, and F5).

Table 1 lists the component failure rates and repair/restore rates common to all the approaches considered here. Also shown in Table 1 is the assumption that mean time to repair a failed component or restore a train from a maintenance activity is arbitrarily varied from 4 hours to 48 hours. Failure rates were estimated over this range using fault tree and analytical and simulation-based Markov analyses.

Once the system states have been identified and the transition rates are estimated, a stochastic transition probability matrix is developed, which mathematically accounts for the transition rates from one state to the next. These system states are described in Table 2. To estimate the failure rate of the system, a truncated form of this matrix, Q, is used. This truncated matrix is formed by eliminating the rows and columns containing the absorbing states that result in the overall failure of the system. Absorbing states represent the cases where the system cannot recover once entered (i.e., unlike partial failures of the system due to one train being inoperable). The estimated failure rate for the system can then be developed by using the following equations [1]:

**Table 1. Failure Rates and Repair/Restore Rates**

Description	Value	Basis
Mean failure rate for a damper failing	$3 \times 10^{-6} \text{ hr}^{-1}$	Reference [2]
Mean failure rate for a fan failing to run	$3 \times 10^{-5} \text{ hr}^{-1}$	Reference [2]
Failure rate estimate for a controller	$2.1 \times 10^{-2} \text{ yr}^{-1}$	Reference [2]
Assumed frequency for a maintenance action	$5.3 \times 10^{-3} \text{ hr}^{-1}$	Reference [3]
Assumed mean time to repair a failed component or restore a train from a maintenance activity	4 hr, 8 hr, 12 hr, 24 hr, and 48 hr	Assumed



**Figure 2. System States Defined for Markov Model**

$$R = \frac{1}{MTTF} \quad (3)$$

State	Description
N	Normal operating state with one train operating in each section and one train in standby.
I1	One train in Section A is inoperable. The remaining train is operating normally.
I2	One train in Section B is inoperable. The remaining train is operating normally.
I3	One train in Section A is inoperable and one train in Section B is inoperable. The remaining train in each section is operating normally.
F1	The controller fails, resulting in system failure.
F2	One train in Section A or Section B is inoperable, and the controller fails, resulting in system failure.
F3	One train in Section A or Section B is inoperable, and a component failure occurs in a running train in the same section, resulting in system failure.
F4	One train in Section A is inoperable, one train in Section B is inoperable, and a controller failure occurs, resulting in system failure.
F5	One train in Section A is inoperable, one train in Section B is inoperable, and a component failure occurs in a running train, resulting in system failure.

**Table 2. System State Descriptions for Markov Model**

$$M = [I - Q]^{-1} \quad (1)$$

where

- M = fundamental matrix, M, with elements  $m_{ij}$  that indicate the average time spent in state j given that the system started in state i
- I = identity matrix
- Q = truncated stochastic transition probability matrix

$$MTTF = m_{i1} + m_{i2} + \dots + m_{ij} \quad (2)$$

where

- MTTF = mean time to failure (yr)
- $m_{ij}$  = elements of the fundamental matrix, M, that indicate the average time spent in state j given that the system started in state i

The failure rate, R, for the system is the inverse of the MTTF:

## MARKOV STOCHASTIC SIMULATION

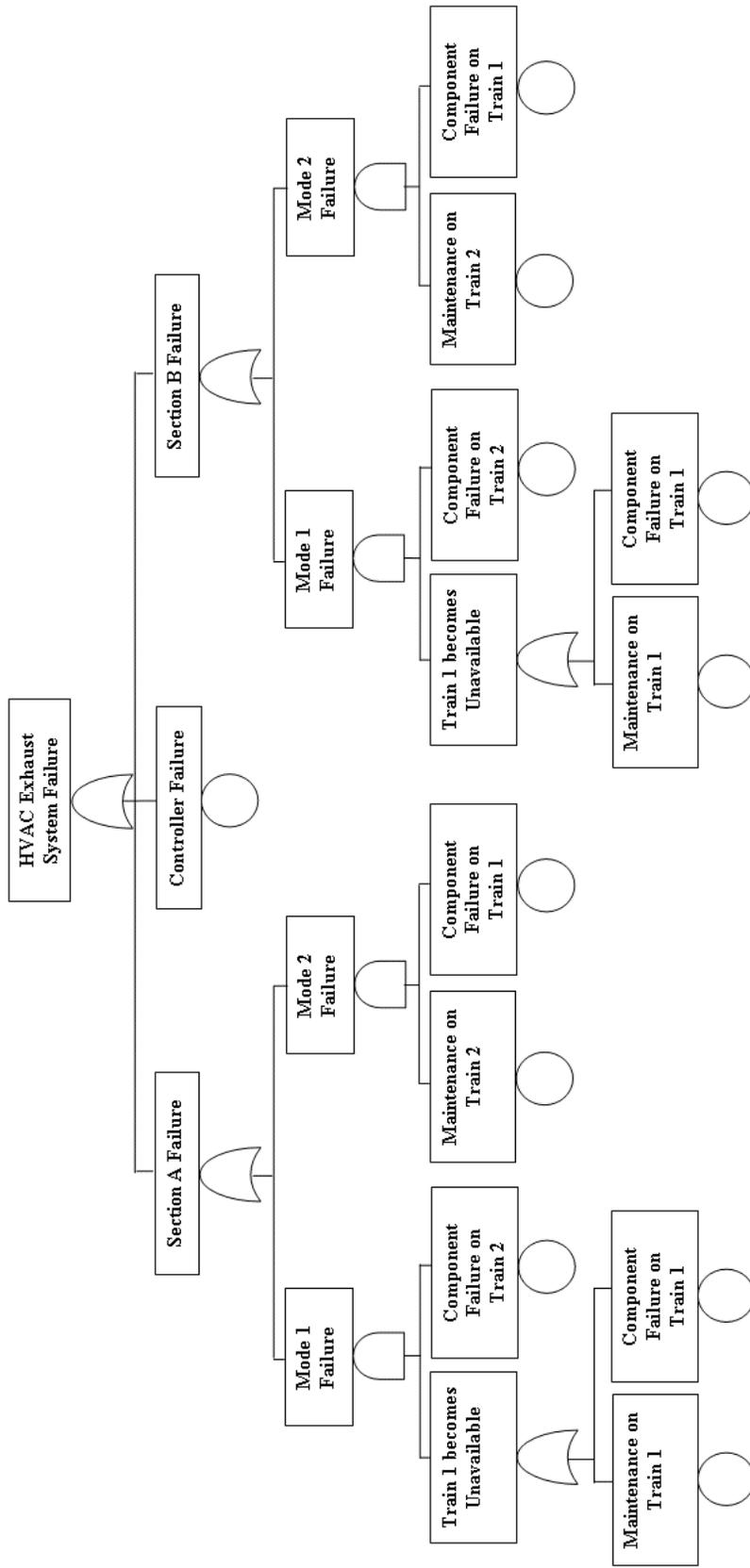
Markov stochastic simulation (i.e., a simulation-based Markov technique) was performed to verify the results obtained from the analytical Markov methodology. The stochastic simulation was performed in MATLAB<sup>®</sup> by conducting a series of test runs in which the mean time to repair a failed component or restore a train from a maintenance activity was varied from 4 hours to 48 hours. The time at which a failure or repair occurred was sampled from an exponential distribution for each of the component failure, component repair, or maintenance activities identified in Table 2 to simulate the system running over time. Each test run was conducted over 1,000 realizations and over a period of 50 years.

## FAULT TREE MODEL

The fault tree model for this system is shown in Fig. 3, where failure of the hypothetical HVAC exhaust system may occur due to controller failure or a failure in either Section A or Section B. The problem description is identical for the one used in the Markov Methodology, but the approach is described below to clearly identify the logic used in the construction of the fault tree model for the system presented in Figure 1 (also not considering the HEPA filters).

Each section has two modes of failure. In mode 1, the operating train (in this case, train 1) becomes inoperable due to maintenance or component failure. Operation is transferred to train 2, which experiences a component failure. In mode 2, the standby train (i.e., train 2) becomes inoperable due to maintenance, and afterwards a component failure occurs in train 1. In Section A, component failure would involve the failure of either damper in a train. In Section B, component failure would involve the failure of a fan or either of the two dampers in a train.

For the calculations in the fault tree model, an initiating event frequency (e.g., failure rate for a component in the operating train) was combined with a component reliability (e.g., reliability for a component in the other train) to develop the rate of failure for the minimal cut sets. These values were then combined to estimate the failure rate for the HVAC system. In this analysis, it was assumed that the probability the system will not switch to the standby train is zero. Therefore, this work focused on the failure of the redundant train to



Train 1 is operating initially  
 Train 2 is in standby

Figure 3. Fault Tree Model for Hypothetical HVAC Exhaust System

continue running while maintenance or repair is being performed on the other train.

## UNCERTAINTY ANALYSIS APPLIED TO ANALYTICAL MARKOV TECHNIQUE

Uncertainty in the component failure rates in published data can be an important aspect of reliability estimation. Furthermore, it can be used to enhance the performance prediction capabilities of the Markov model itself [4]. In this paper, an uncertainty analysis was performed on the analytical Markov technique.

To illustrate this approach, consider that the failure rates for the damper and fan listed in Table 1 have a recommended failure rate probability distribution [2]. The commonly used lognormal distribution is suggested for both components using the failure rates in Table 1 for the mean. The error factor (EF) is also provided as a measure of the spread of the distribution around its mean. Once the mean and EF are defined, the random numbers from a lognormal distribution can be sampled and provided as input to the truncated stochastic transition probability matrix,  $Q$ , described previously and shown in Eq. 1. The approach used was to sample directly from these distributions for each component to obtain a range of estimated failure rates versus mean time to repair/restore. For the fan and damper, the suggested EF values of 3 and 10, respectively, were used [2]; for the estimated controller failure rate obtained from Paula [3], an EF of 3 was assumed.

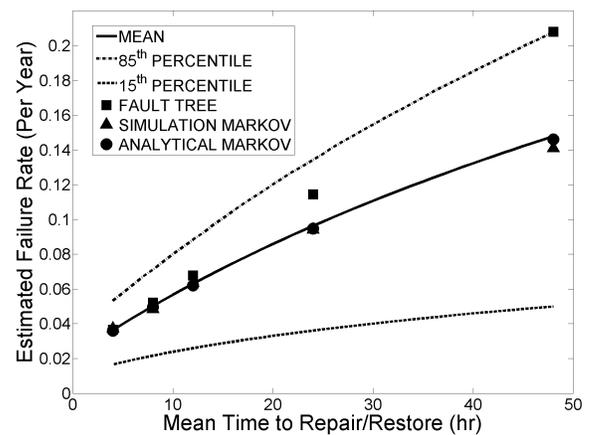
## RESULTS

The analytical and simulation-based Markov results were plotted along with results from the fault tree analysis and are shown in Fig. 4. An uncertainty analysis was performed for the analytical Markov technique, as described in the previous section. The uncertainty is represented by the mean value, the 15<sup>th</sup> percentile, and the 85<sup>th</sup> percentile of the estimated failure rate. Note that, while modeling the system using stochastic simulation is expected to confirm the analytical results as it does in this case, it also can provide a powerful alternative to cases where the failure and repair rates are not constant with time, and non-Markovian processes need to be considered instead.

As shown in Fig. 4, the failure rates for the hypothetical HVAC exhaust system compare well between the analytical Markov model and the stochastic simulation over all values for mean time to repair/restore, as expected. However, estimated failure rates calculated from the fault tree analysis diverge from the results obtained from the Markov approach as the mean times

to repair/restore increase, making the fault tree analysis more conservative at these higher times.

The primary reason for this divergence is that the analytical and simulation-based Markov methods account for the operation of the system as it transitions from the normal state to possibly intermediate states in which the system is still functional, whereas the fault tree model considers transitions from the normal operating state directly to one or more failed states. The fault tree technique generates an estimated failure rate of the hypothetical HVAC system that is essentially linear with mean time to repair/restore, while the Markov techniques generate an estimated failure rate that increases more slowly as mean time to repair/restore increases. These results show that consideration of these intermediate states plays a significant role when estimating the failure rate of a system subjected to maintenance or repair actions that may last for several hours. In this sense, the Markov techniques may generate a more realistic estimate for the failure rate of complex systems, and the fault tree model may result in more conservative estimates for these systems. Furthermore, the inclusion of an uncertainty analysis in the Markov approach also allows for the quantification of the confidence in the estimated results, similar to fault tree analysis, given that published component failure rates can exhibit variability. However, since the system state is modeled explicitly as a stochastic process, the uncertainty analysis benefits directly from the Markov modeling capabilities in handling standby redundancy.



**Figure 4. Failure Rates for Analytical and Simulation-Based Markov Analyses, Fault Tree Analysis, and Uncertainty Analysis (Mean, 85<sup>th</sup> Percentile, 15<sup>th</sup> Percentile) vs. Mean Time to Repair/Restore**

## **SUMMARY AND CONCLUSIONS**

The Markov methodology is effective in estimating the failure rates for a hypothetical HVAC exhaust system over a range of mean times to repair/restore. This methodology could be extended to more complex systems in which the traditional fault tree analysis technique may be more conservative as the mean times to repair/restore increase. This result indicates that fault tree techniques may not adequately capture the performance of complex engineering systems that can be in several intermediate operating states, whereas Markov techniques could be used for these systems.

The consideration of uncertainty is beneficial for quantifying the estimated failure rates to evaluate the confidence in the established maintenance and repair policy for a complex system. This can be particularly useful for cases where a high level of reliability is expected to fulfill specific requirements established by a client and/or regulations.

## **ACKNOWLEDGMENTS**

This paper was prepared to document work performed by the Center for Nuclear Waste Regulatory Analyses (CNWRA) for the U.S. Nuclear Regulatory Commission (NRC) under Contract No. NRC-02-02-012. The activities reported here were performed on behalf of the NRC Office of Nuclear Material Safety and Safeguards, Division of High-Level Waste Repository Safety. This paper is an independent product of CNWRA and does not necessarily reflect the views or regulatory position of NRC.

## **REFERENCES**

1. Billinton, R. and R. Allan. Reliability Evaluation of Engineering Systems, Concepts and Techniques, 2nd edition. New York City, New York: Plenum Press. 1992.
2. Roy, B.N. Savannah River Site Generic Data Base Development, WSRC-TR-93-262 Rev. 1. Aiken, South Carolina: Westinghouse Savannah River Company. 1998.
3. Paula, H.M. "Technical Note: Failure Rates for Programmable Logic Controllers." Reliability Engineering and System Safety. Vol 39. pp. 325-328. 1998.
4. McCormick, N.J. Reliability and Risk Analysis: Methods and Nuclear Power Applications, 1<sup>st</sup> edition. New York City, New York: Academic Press. 1981.