Proceedings of the 1988 Winter Simulation Conference
M. Abrams, P. Haigh, and J. Comfort (eds.)

Modeling viewpoints for assessing reliability

A. Alan B. Pritsker
Pritsker & Associates, Inc.
P.O. Box 2413
West Lafayette, IN 47906

ABSTRACT

This paper is the third in a series of papers dealing with model evolution and its importance in problem-solving when employing simulation as an analysis tool. In the paper, reliability assessment is used as a vehicle for presenting modeling viewpoints and constructs. As in the previous papers, the assessment of the worth of a model is not made. The paper describes modeling viewpoints and procedures in a reliability assessment context and describes the need for being able to build more detailed models from simpler models. The basic hypothesis of the paper is that model evolution is a way of life for the simulationist.

1. INTRODUCTION

This paper presents models for reliability assessment. Both mathematical and logical models are developed. The approach is to start with simple models and to add complexity. The simplest model assumes knowledge of the probability of failure of a set of subsystems and it is desired to compute a probability of system failure. Subsystem time-to-failure characteristics are then introduced in the model and reliability is assessed in terms of time-to-system failure. Next, models are developed which include both the probability of subsystem failure and a conditional time based on whether a subsystem succeeds or fails. Performance measures for such a system are the probability of success (failure) and the time at which success (failure) is achieved.

For systems which have alternate subsystems to perform a function, that is, parallel subsystems, the repair of a subsystem can extend the time until the system fails. Models that include subsystem repair are then developed. Lastly, a model is presented that estimates the time until first system failure for a system that includes spare and replacement subsystems.

In the paper, the assumptions required in order to build mathematical models are described. For the logic-oriented models, SLAM II®network constructs are used. Many authors have used network languages for analyzing reliability situations. A list of references to their work is included at the end of the paper. (Case, 1971, Gallagher, 1970, Hammesfahr, 1978, Polito, 1976, Pritsker, 1989, Whitehouse, 1970, 1973)

2. MODEL 1: STATIC RELIABILITY ASSESSMENT

For a system consisting of three subsystems in series, the probability of success of the system is the probability that all three subsystems succeed. If p_{f_i} is the probability of subsystem i failing, then the probability of success is given by

$$\text{P[SUCCESS]} = \prod_{i=1}^{3} (1-p_{f_i})$$

The probability of system failure, P[FAILURE], is then 1-P[SUCCESS]. This assumes that a subsystem either succeeds or fails and that the subsystems are independent. A network model for this situation is shown in Figure 1 for three subsystems. At each CREATE node, one entity is generated which is routed over one of two branches leaving the node in accordance with a probability. For the system to succeed, the three activities leading to the ACCUMULATE node SUCC must be taken. The fraction of runs on which this occurs is an estimate of P[SUCCESS]. One subsystem failure causes ACCUMULATE node FAIL to be released, and the fraction of runs on which this occurs is an estimate of P[FAILURE].

An alternate model, shown in Figure 2, employs one CREATE node to generate the three entities. ASSIGN node A1 sets a value for the component failure probability (computation not shown) for each subsystem. A single branch is used to model all subsystem successes and another branch represents all subsystem failures. This model is easy to modify to increase the number of subsystems by increasing the number of entities created at the CREATE node and changing the number of successes required at ACCUMULATE node SUCC.

SLAM II is a registered trademark of Pritsker & Associates, Inc.

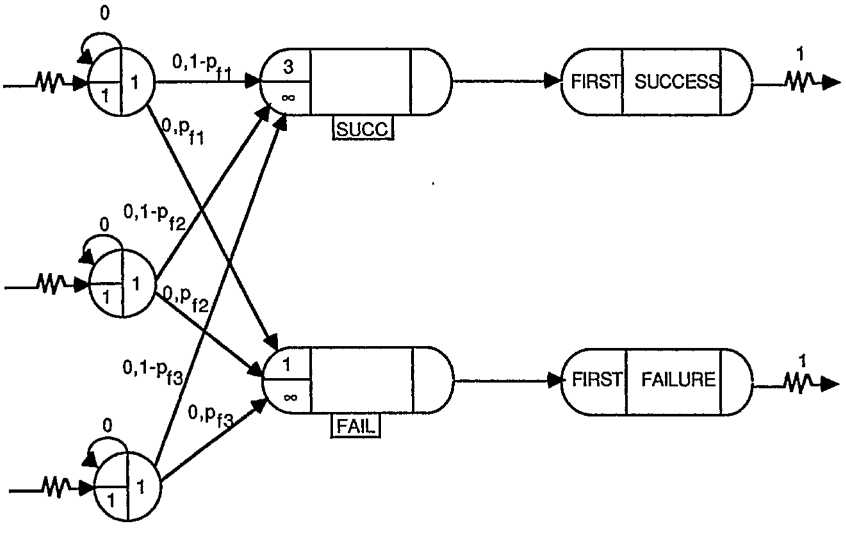


Figure 1. SLAM II network model of 3 subsystems in series.

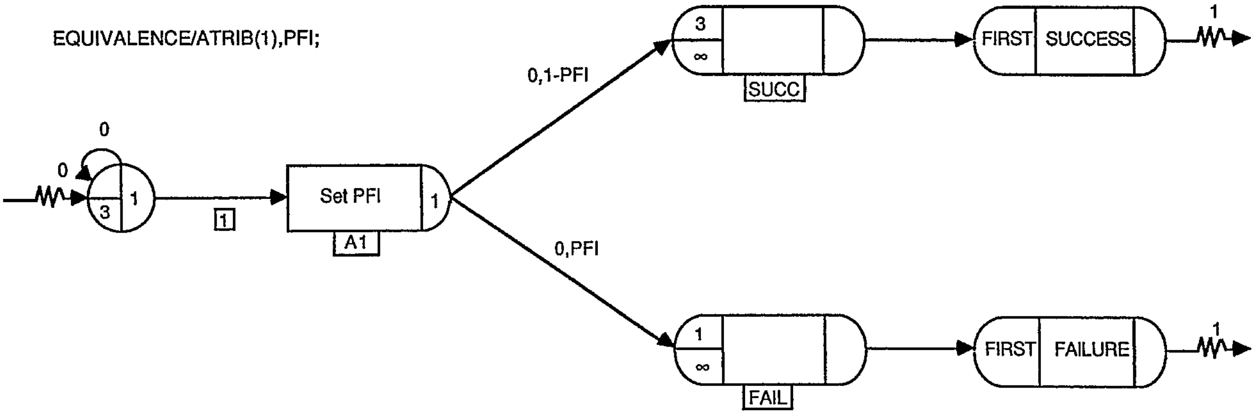


Figure 2. Alternate SLAM II network model of 3 subsystems in series.

For the system consisting of three subsystems in parallel, the probability of system failure is the probability of all three subsystems failing. Again, assuming independent subsystems, this probability is

$$\text{P[FAILURE]} = p_{f_1} * p_{f_2} * p_{f_3}$$

and

$$\text{P[SUCCESS]} = 1 - \text{P[FAILURE]}.$$

In a network model, the change required to go from a system involving subsystems operating in series to one in which the subsystems operate in parallel only requires changing the first release requirement of the ACCUMULATE nodes. Thus, in Figures 1 and 2, the first release requirement for ACCUMULATE node SUCC is changed from 3 to 1 indicating that if any of the subsystems succeeds the system succeeds. Correspondingly, the first release requirement for ACCUMULATE node FAIL is changed to 3 to indicate that all three subsystems must fail before a system failure occurs.

```
EQUIVALENCE/ATRIB(1),TFI;
```

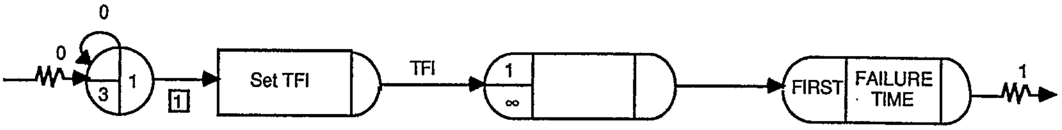


Figure 3. SLAM II network model to estimate the time-to-failure.

3. MODEL 2: TIME TO FAILURE ASSESSMENT

For three subsystems in series, the time-to-failure is the minimum of the subsystem times-to-failure, that is,

$$t_{FAIL} = \min [t_{f_1} ; t_{f_2} ; t_{f_3}].$$

The probability distribution of the time-to-failure can be obtained as shown below

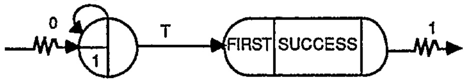
$$\begin{aligned} P[t_{FAIL} > t] &= P[\min [t_{f_1} ; t_{f_2} ; t_{f_3}] > t] \\ &= P[t_{f_1} > t; t_{f_2} > t; t_{f_3} > t] \\ &= P[t_{f_1} > t]\ P\ [t_{f_2} > t]\ P[t_{f_3} > t] \text{ if independent} \\ &= (P[t_f > t])^3 \text{ if identically distributed} \\ P[t_{FAIL} \le t] &= 1 - (P[t_f > t])^3. \end{aligned}$$

If each subsystem time-to-failure is exponentially distributed with a mean time of 1/m then $P[t_f]=1 - e^{-mt}$ and the distribution of the system time to failure is

$$\begin{aligned} P[t_{FAIL}] &= 1 - (e^{-mt})^3 \\ &= 1 - e^{-3mt} \end{aligned}$$

which is exponentially distributed with a mean of 1/3m.

A SLAM II network model to estimate the time-to-failure is shown in Figure 3. If a mission time, T, is prescribed, then a disjoint subnetwork is added to Figure 3 in order to compute a mission success probability as shown below:



The simulation involves a "race" in the two subnetworks and the one reaching its COLCT node first defines a failure or success on a run.

For subsystems in parallel, the time of system failure is the maximum of the times of each subsystem failure. The analysis for this situation is

$$\begin{aligned} t_{FAIL} &= \max [t_{f_1} ; t_{f_2} ; t_{f_3}] \\ P[t_{FAIL} \le t] &= P[\max[t_{f_1} ; t_{f_2} ; t_{f_3}] \le t] \\ &= P[t_{f_1} \le t; t_{f_2} \le t; t_{f_3} \le t] \\ &= (P[t_f \le t])^3 \text{ if } t_f \text{ are i.i.d.} \end{aligned}$$

If t_f is exponentially distributed with mean 1/m then

$$P[t_{FAIL} \le t] = (1 - e^{-mt})^3$$

which is not exponential.

As described in a previous paper (Pritsker, 1986), the continuous features of SLAM II can be used to estimate the mean, variance and higher moments of complex distributions. The SLAM II network model for subsystems in parallel is similar to the one in Figure 3 with the first release requirement for the ACCUMULATE node changed to 3, that is, the number of subsystems.

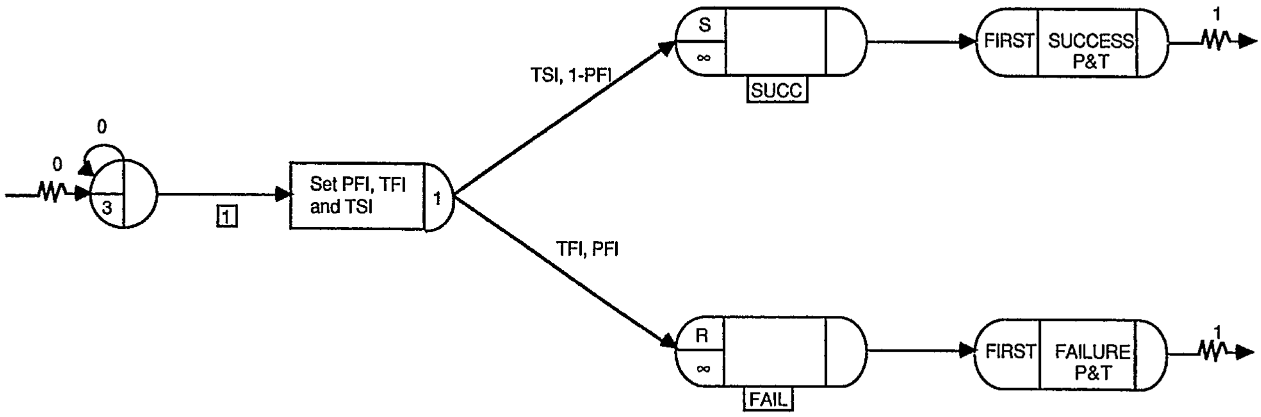
4. MODEL 3: COMBINED TIME AND PROBABILITY MODEL

When describing the characteristics of a subsystem, both the probability of a failure and the time of a failure are sometimes given, that is, the time is a conditional distribution given that a failure has occurred. Similarly, the time-to-success for a subsystem is described conditionally on the occurrence of successful operation. The mathematical analysis of this situation is performed in the same manner as presented for models 1 and 2. The SLAM II network models are combined and a single network is formed as shown Figure 4. In Figure 4, the number of first release requirements for nodes SUCC and FAIL are given as S and R where S equals 3 for in series subsystems and 1 for subsystems in parallel whereas R equals 1 for subsystems in series and 3 for subsystems in parallel.

The model presented in Figure 4 is a high level model. It assumes knowledge of the probabilities of failure and success and conditional times of failure and success for the subsystems. A detailed model which portrays the components of each subsystem can be developed in network form to estimate these values or detailed subnetworks can be substituted directly into Figure 4.

5. MODEL 4: ADDING REPAIR OPERATIONS

Consider the situation in which two subsystems operate in parallel but only one subsystem is required to maintain system operation. A repairman is available to fix a subsystem, and it is desired to know how long it takes for both subsystems to fail at the same time. A mathematical analysis to obtain the time until system failure involves an examination of the transitions from three states: 0 subsystems failed, 1 subsystem failed, and 2 subsystems failed (system failure). When the system starts up, the time to transition from state 0 to state 1 is the minimum of the failure times of the subsystems. The transition from state 1 to state 2 occurs if the repair time of the failed subsystem is greater than the remaining time-to-failure of the working system. If the repair time is smaller than the remaining time-to-failure of the working system, then we return to the state of both subsystems working. However, the time for the next failure is the minimum of the time-to-failure for the repaired subsystem and the remaining time-to-failure of the working system. The remaining time to failure is its original time-to-failure minus the failure time and the repair time of the other subsystem. If it is assumed that failure times and repair times are exponentially distributed, the remaining time following the occurrence of an event is also exponentially distributed. Thus, with exponentially distributed failure and repair times, a semi-Markov analysis of the system can be performed. (See GERTE analysis (Pritsker, 1979, Whitehouse, 1973) and Gallagher (1970) for generalizations of the statement.)



$S = \begin{cases} 3 \text{ for series subsystems} \\ 1 \text{ for parallel subsystems} \end{cases}$

$R = \begin{cases} 1 \text{ for series subsystems} \\ 3 \text{ for parallel subsystems} \end{cases}$

Figure 4. SLAM II network model combining probabilities and times to failures.

The logic described above can be put into a SLAM II network as shown in Figure 5. Since SLAM II networks allow actual realizations of the values to be placed on the network, conditions can be placed on the activities to direct the flow in accordance with a comparison of values. Following the creation of one entity, failure times for subsystems 1 and 2 are sampled as TF1 and TF2. Sample values for repair times are generated as TR1 and TR2. At GOON node G1, subsystem 1 fails first if TF1 is less than or equal to TF2 and the entity is routed to node G2. Otherwise, subsystem 2 fails first and the entity is routed to node G3. From node G2, subsystem 1 is repaired before the failure of subsystem 2 if the time-for-repair, TR1, is less than or equal to TF2 - TF1. If this occurs, TR1 time units are expended and the entity is routed to ASSIGN node A1. At node A1, the remaining time-to-failure for subsystem 2 is computed by subtracting from TF2, the values of TF1 and TR1. New values of TF1 and TR1 are then sampled and a return is made to node G1. If the repair time for subsystem 1 is greater than the remaining time-to-failure for subsystem 2 then a system failure occurs after TF2 - TF1 time units. This is shown on the activity from node G2 to COLCT node C1. A similar analysis is made if subsystem 2 fails before subsystem 1.

The model in Figure 5 follows the modeling logic used in developing a state transition diagram. In Figure 6, a different view is taken which is based on the events occurring in the network. An entity is used to represent a subsystem and the locations of the entities in the network determine when a system failure occurs. First, two entities are created, each representing a subsystem. In activity 1, the entity is in a working state. The time in activity 1 is the time for the subsystem to fail. Thus, there will be 0, 1 or 2 entities in activity 1. Whenever there are no entities in activity 1, both subsystems have failed, and the system has failed. This is recorded at node SFAIL. Activity 2 models the repair activity.

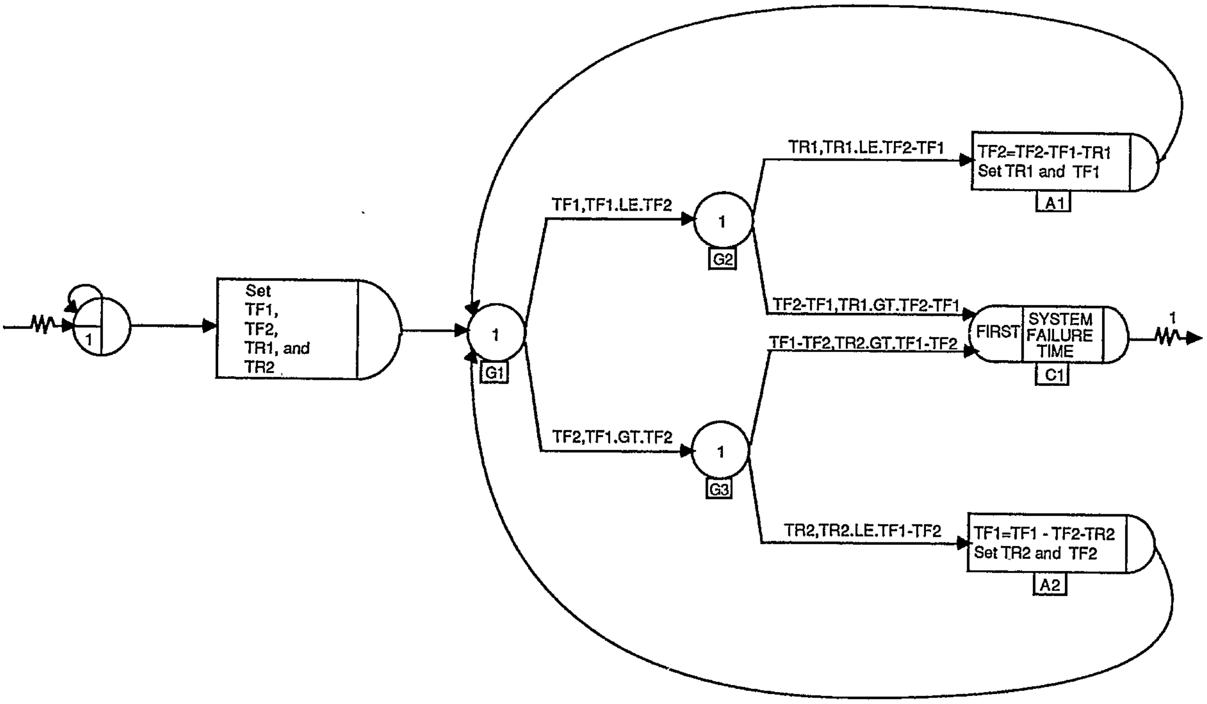


Figure 5. SLAM II network model of failure-repair operations.

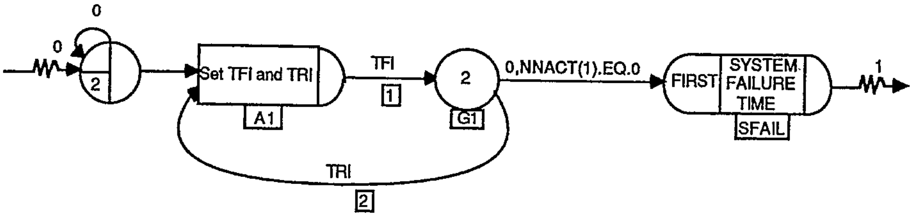
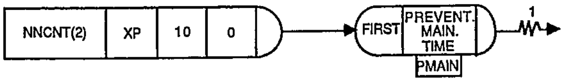


Figure 6. Different view of failure-repair model.

DETECT nodes can be used for assessing ending conditions for system operation. For example, if we shut down the system for preventative maintenance after there have been 10 repairs without 2 concurrent failures, then the following DETECT node can be used to detect the cumulative number of repairs crossing the value of 10



where NNCNT(2) is the number of completed repairs. The DETECT node creates an entity that is routed to COLCT node PMAIN when there are ten completions of the repair process, activity 2.

6. MODEL 5: SPARES AND OFF-LINE EQUIPMENT

A power station requires three generators to be on-line at all times. A spare generator and a replacement generator are available to replace any generator that fails. The spare generator has the same characteristics of the three generators but the replacement generator is not of the same quality and has a different failure time distribution associated with it. Company policy is to start repair work immediately on any generator that has failed and two repairmen are available for this task.

The model of this situation is shown in Figure 7 to obtain statistics on time-to-system failure due to the simultaneous failure of any three generators. The four regular generators are created at the CREATE node CR1. Three are placed in activity 1 and the spare generator waits in QUEUE node Q1. When a generator fails, the spare is put on-line. Time between failure statistics are collected at COLCT node C1. Up to two activities are started when a generator fails. Activity 2 represents the repair of the generator. If both repairmen are busy, then the failed generator causes a system failure. This is modeled by having the entity representing the failed generator balk from QUEUE node Q2 to COLCT node C2.

If less than three generators are operating, that is, NNACT(1).LT.3, an entity is routed to AWAIT node A1 to seize the replacement generator and put it on-line. The time-for-failure for the replacement generator, TRG, is prescribed for activity 3. The replacement generator is modeled as a resource to allow it to be preempted when a regular generator is repaired. If the replacement generator fails before a regular generator is repaired, the power station goes down and a system failure occurs as indicated by activity 3 leading to COLCT node C3.

Following the repair of a regular generator, the replacement generator is taken off-line if it is in activity 3 by preempting it at PREEMPT node P1. It is made available at FREE node F1. The regular generator is put back on-line by routing it to node A1 from GOON node G1. Statistics collected in this model are:

- The time between regular generator failures at node C1;
- The time of failure for the power station at node C2;
- Utilization of the repairmen on activity 2;
- Utilization of replacement generator from resource statistics; and
- Amount of time spent in inventory of a spare generator at node Q1.

Throughout the development of model 5, concepts from the previous models are employed. This evolution of models is a distinct and important feature of network models which are analyzed using simualtion techniques. It is an important feature of a simulation language.

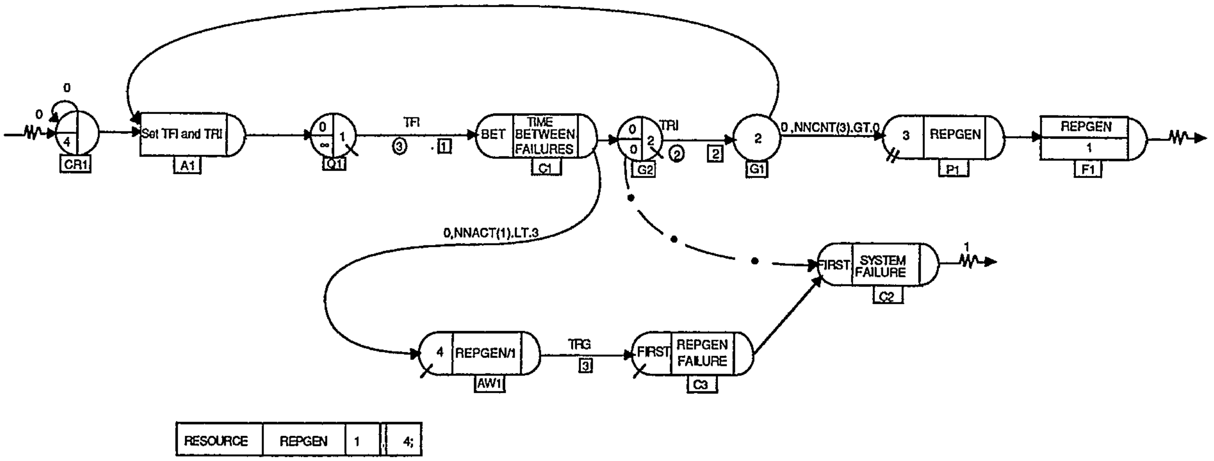


Figure 7. SLAM II network model of a power generator system.

7. DISCUSSION

In this paper, modeling viewpoints and approaches have been presented. The study of modeling is a much neglected subject.

The SLAM II network models presented in this paper have characteristics that assist in presentation and understanding. In some cases, there is a one-to-one correspondence between a subsystem and a SLAM II activity. In other instances, a SLAM II activity represents more than one subsystem. In the more advanced models, an entity is used to represent a subsystem. In the last illustration, a resource is used to represent a subsystem, the replacement generator. Clearly, there is not just one way to model a construct. Having alternative ways to model systems provides flexibility in the modeling process. Flexibility, however, adds complexity in a modeling language.

Another interesting aspect observed from this paper is that the thought processes used in developing mathematical or probabilistic models may not be a good first step in developing a model which is to be analyzed using simulation. For example, Markov assumptions could lead to a more complex simulation model. Another observation is that minimum and maximum operations are "races" and "assemblies" in a simulation model. There is also a twist in thought processes when modeling for reliability assessment. Service activities represent failure times, that is, time-to-failure is the service time in a reliability situation.

The evolution of models as presented in this paper provides insight into reliability assessment procedures. Reliability analysis and network analysis share a common approach. They both involve data collection at the component or subsystem level and the integration of the data in a model to develop system performance measures. They both require a purpose for modeling from which a level of detail can be determined. They both allow for the use of actual and hypothesized data.

8. REFERENCES

Case, K.E. and K.R. Morrison, "A Simulation of System Reliability Using GERTS III," *Virginia Academy of Science Meeting*, May 14, 1971.

Eisner, H., *Computer-Aided Systems Engineering*, Prentice-Hall, 1987.

Elmaghraby, S.E., *Network Models in Management Science*, Lecture Series on Operations Research, Springer-Verlag, 1970.

Gallagher, D.J., "A GERT Network Approach to the Study of Queueing Phenomena," Ph.D. Dissertation, Arizona State University, 1970.

Hammesfahr, R.D.J., T.R. Rakes and E.R. Clayton, "An Application of Q-GERT to the System Reliability Problem," *Proceedings, S.E. TIMS Conference*, October, 1978, pp.

Henley, E.J and K. Kumamotoh, *Reliabilty, Engineering and Risk Assessment*, Prentice-Hall,1981.

Phillips, D.T., and A. Garcia-Diaz, *Fundamentals of Network Analysis*, Prentice-Hall, 1981.

Polito, J., Jr. and C.C. Petersen, *User's Manual for GRASP*, Purdue Laboratory for Applied Industrial Control, Report Number 75, April, 1976.

Pritsker, A.A.B., C.E. Sigal, R.D.J. Hammesfahr, *SLAM II Network Models for Decision Support*, Prentice-Hall, to be published, January 1989.

Pritsker, A.A.B., "Model Evolution II: An FMS Design Problem," *Proceedings, 1987 Winter Simulation Conference*, 1987, pp. 567-574.

Pritsker, A.A.B., "Model Evolution: A Rotary Index Table Case History," *Proceedings, 1986 Winter Simulation Conference*, 1986, pp. 703-707.

Pritsker, A.A.B., *Introduction to Simulation and SLAM II*, Third Edition, John Wiley and Systems Publishing Corporation, 1986.

Pritsker, A.A.B. and C.E. Sigal, *Management Decision Making: A Network Simulation Approach*, Prentice-Hall, 1983.

Pritsker, A.A.B., *Modeling and Analysis Using Q-GERT Networks*, Second Edition, John Wiley, 1979.

Whitehouse, G.E., *Systems Analysis and Design Using Network Techniques*, Prentice-Hall, 1973.

Whitehouse, G.E., "GERT, A Useful Technique for Analyzing Reliability Problems," *Technometrics*, February 1970.

9. ACKNOWLEDGEMENT

This material is based on work supported by the National Science Foundation under Grant No. DMS-8717799. The government has certain rights in this material.

AUTHOR'S BIOGRAPHY

A. ALAN B. PRITSKER is Chairman of Pritsker & Associates, Inc. and FACTROL, Inc. He graduated from Columbia University with a BSEE and MSIE. He obtained a Ph.D. from The Ohio State University in 1961. From 1956 through 1962, Dr. Pritsker worked for Battelle Memorial Institute in Columbus, Ohio. From 1962 through 1981, he was Professor of Industrial Engineering at Arizona State University, Virginia Tech, and Purdue University. In 1973, he co-founded Pritsker & Associates.

Dr. Pritsker has published more than 100 technical papers and eight books. He is a Fellow of AIIE and recipient of AIIE's Distinguished Research Award and Innovative Achievement Award. He is also a member of the National Academy of Engineering. Dr. Pritsker served as a member of the Board of Directors of the Winter Simulation Conference from 1970 to 1974 and 1980 to 1987, and as Board Chairman in 1984 and 1985.

A. Alan B. Pritsker
Pritsker & Associates, Inc.
P.O. Box 2413
West Lafayette, IN 47906
(317) 463-5557