James Madison University

From the SelectedWorks of George H Baker

May, 2000

Time Domain Probabilistic Risk Assessment:

George H Baker, James Madison University
Charles T. C. Mo

Available at: https://works.bepress.com/george_h_baker/7/
Time Evolution Method Probabilistic Risk Assessment:  
A New Technique for Modeling the  
Functional Survivability of Complex Systems

George H. Baker, James Madison University, College of Integrated Science and 
Technology, Harrisonburg, VA 22807

Charles T.C. Mo, Logicon Advanced Technologies, 222 West Sixth Street, San Pedro, 
CA 90731

1.0 Introduction

For critical facilities and systems, survivability and reconstitution in stressful 
environments engendered by electromagnetic transients, cyber attacks, sabotage, terrorist 
activity, military conflict, or Murphy’s laws are issues of concern. Critical facilities and 
systems are likely to be functionally complex and their system-wide failure probabilities, 
modes, and consequences are often not obvious. To analyze and quantify survivability, 
eexisting probabilistic risk assessment tools provide a “snapshot” of failure modes at a 
single point of time for certain initiating conditions. Likewise, elaborate physics models 
developed to treat weapons effects on systems compute effects implicitly at a single point 
in time.

We have developed a tool that improves upon existing computational models by adding 
the time dimension to the evaluation of functional mission susceptibility to the failure of 
interdependent subsystems of complex facilities and systems. The tool computes the 
evolution of overall mission failure probability in time by evaluating initial failure 
probabilities, effects onset times and system repair/reconstitution times for single or 
combinations of critical facility subsystems. The tool allows the aggregation of scenario 
and facility functional tree (or diagram) inputs into an overall system effects evaluation. 
The model breaks new ground in quantifying and predicting not only initial probability of 
effects on system mission execution, but mission outage longevity. Computations invoke 
a component-up functional fault tree/diagram system analysis to synthesize and quantify 
overall facility mission survivability or operability. The model is unique in that the time 
evolution of the probability of effects on mission is built-in (effectively) as a stochastic 
finite difference equation with initial conditions, deterministic and stochastic, and uses as 
coded inputs:

1) the scenario dependent environmental stresses (insults)
2) The system fault analysis
3) The individual functional components’ damage threshold probability 
distributions, and
4) The time constants of effects onset and reconstitution/repair

The code provides output in the form of probability of effects vs. time.
The code is useful for determining the most critical failure points and the most cost-effective protection upgrades. It is a tool well-suited for predicting function impairment of complex facilities, systems, and networks due to electromagnetic over stress.

2.0 The Functional Survivability / Operability Problem

Complex facilities and systems may fail in many different ways due to many different causes, intentional and unintentional. Failures may propagate such that seemingly minor problems, in some cases, result in complete mission failure. Of particular concern is the presence of “single point failure” locations in many known facilities and systems. A question of concern is which failure points or point combinations would lead to the most serious and “most-to-be-avoided” consequences.

The Time Evolution Method Probabilistic Risk Assessment technique enables a comparative evaluation of potential functional debilitation modes using realistically available system information augmented by reasonable engineering assumptions. The code is designed to quantify both the probability of mission outage ($P_e$) and outage time. The code provides output to the user in a simple plot of $P_e$ vs time. A notional output plot is shown in figure 1.

![Figure 1](image)

3.0 Model Formulation

3.1 Basic Concept

The tool is based on probabilistic risk assessment techniques. Mission outage modeling is accomplished by building fault trees that link together the hierarchy of systems, subsystems, and components necessary for a facility or system to perform its mission.

In general, facility systems can be grouped into three categories according to their function as diagrammed in figure 2: (1) Operations Function, (2) Protection Function, and (3) Support Function. Operation systems perform mission specific functions such as communication, manufacturing, storage, or power generation. Protection systems function to provide physical security, information security, fire protection, emergency
services, etc. Support systems provide the environment control, electric power, or communications necessary for the operation of mission and protection systems.

Facility Composition

At first blush, the operational/mission systems appear to be most critical to system performance. However, support system outage has the most widespread effects on facility functionality. If a saboteur is familiar with subsystem fault trees and interdependencies, he may be able to bring down an entire facility by attacking one component of a support subsystem. Mission systems tend to have more protection/security making support systems the most accessible targets.

Because many subsystem and components are readily repaired or replaced, the model accounts for reconstitution times. Some subsystem/component failures may also result in cascading effects exhibiting latent time delays. For example, the failure of a facility’s environmental control system may cause room temperature to rise to a point in time where electronics begin to overheat. Thus, the code is designed to account for two time factors: (1) effects’ onset delays, and (2) damage repair/replacement times.

3.2 Mathematical Implementation

The code takes information in the form of subsystem fault and function diagrams, scenario stresses on critical components, component strengths (damage or disruption thresholds), effects onset times, and repair times. The code compares stresses to component strengths to determine the probability of effect at individual components. In cases where component and subsystem $P_e$’s are known, they can be input directly. These probabilities are combined using the functional diagram and onset/repair times to generate probability of system mission outage vs. time. A diagram of the basic process flow is shown in figure 3.

Consider a system consisting of a number of subsystems with each subsystem consisting of many components. Let the components be the basic units for which we compare an
environment-induced stress, \( S \), with the component’s physical damage threshold, \( T \). The stress occurs at the weapon onset time \((t=0)\). \( T \) can be either a scalar quantity or a \( K \)-dimensional vector. If component \( j \) sees \( S \geq T \), defined as \( \{ \min( S_{jk} - T_{jk} ) \geq 0, k=1...K \} \)

or as applicable, then it suffers a physical damage and will, at a latent time delay \( TL_{ij} \) after the stress onset, not perform its function. Component \( j \) is then defined as being in a state of “functional outage.” Notice that the overall component mission state at any given time is modeled as a binary functional or not-functional. Graduated mission function degradation is very difficult to model and beyond the capabilities of current fault-tree based models.

Let \( P_{oj} \) represent the probability that component \( j \) is physically damaged as a consequence of the stress \( S_j \) exceeding the component’s threshold \( T_j \) at \( t=0 \). In mathematical notation: \( P_{oj} = Pr \{ S_j \geq T_j \} \)

\( S \) and \( T \) are modeled as random variables, each with its own probability distribution determined on engineering and physical bases. These distributions, in practice, represent all estimated uncertainties and encountered variations. For different components, \( S_j \) may be statistically dependent due to physical proximity or other physical factors.

The model defines a functional outage status index variable, \( I_{dj} \). \( I_{dj} = 1 \) if and only if component \( j \) is in a state of functional outage and \( I_{dj} = 0 \) if and only if the component is functional. This binary function status is a simplification. The variable could be graduated into “shades of gray” on the interval \([0,1] \) quite straightforwardly if required. The model includes a latent time delay, \( TL_{ij} \) for component \( j \)’s physical damage to result in cessation of its functionality. The model allows for uncertainty in \( TL_{ij} \). This uncertainty is included by treating \( TL_{ij} \) as a random variable with a probability distribution \( f_{ij}(t) \) which may be scenario dependent. At the subsystem level, any one set of pre-specified combinations of non-functional components serves to prevent subsystem function. And, any one set of pre-specified combinations of subsystem outages
constitutes overall debilitation of the system’s mission.

In order to quantify the mission outage as a time varying probability, we define a state vector for each component $j$, $I_j = (I_{dj}, I_{cj})$ where $I_{dj}$ is the outage status index and $I_{dj}$ tracks the outage time condition such that for component $j$, $I_j = (0, 0)$ if there is no physical damage and $I_j = (0, TL)$ if it is damaged at effects onset time but will manifest a latent functional outage at a later time. At the functional outage onset time, $t_s$, $I_j = (1, t_s)$. Note that $t_s$ is itself a function of time because a component can be damaged and repaired and damaged again due to functional outage propagation path of other system components. If damaged, component $j$ may be repaired in time $TR_j$ where $TR_j$ is modeled as a random variable with a scenario-dependent probability distribution.

The repair start time may not commence immediately after subsystem/ component outage. The model accommodates situations where a repair sequence is needed i.e., certain components must be repaired before others can be fixed. The repair sequence is an explicit input and the model checks preceding components’ operational status and allows component $j$ to be repaired only if preceding components are functional.

It is also possible to model situations when, even if a component is not damaged directly at $t=0$, it can suffer a functional outage due to the accumulated outage of other “upstream” components. An example would be electronics overheating due to the failure of HVAC subsystems. Such outage propagation paths and times, $TP$ are accommodated by an additional layer of random variables with their uncertainty distributions as explicit inputs.

The probabilistic nature of system failure is implied by the input component stresses and thresholds which are described probabilistically. Likewise, the latent time delay, the propagated outage time, and the repair times are described using probability distributions. Such distributions bound both the uncertainties in the exact physical description of a specific single system of interest, and system-to-system variations if more than one system is involved. The time factors result in a time varying probability of effects.

The model maps each system state point $P(X)$, of the $2^N$ possible points in the component function space (where $N$ is the total number of components in the system), into a system function measure, 0 XOR 1. As time goes on, the state point, $P(X,t)$ traces a trajectory in the component function state space with its path influenced and controlled by all the physical constraints including damage, delay, propagation, and repair (see section 2). The time changes occur in discrete time steps. Thus, the system functional state is a piecewise step function of time with value $t=0$ or $1$. Because these physical constraints, including their initial values, are probabilistic, the code output indicates the probability that the system is in a state of mission outage up to time $t$ based on the specified effects scenario.

The equivalent mathematical problem of coupled finite difference equations with stochastic “forces” would be very difficult to solve analytically in closed form. The code
does it numerically, invoking a basic Monte Carlo simulation.

4.0 Practical Factors and Approximations

With perfect knowledge of a system, one could predict certain system outage or functionality deterministically as a function of time. Then there would be no need for a probabilistic formulation. Except in obvious, trivial cases it is practically infeasible to develop a rigorous, deterministic, analytical closed-form solution to quantify functional outage probabilities and their mathematical-statistical inference from data. This is particularly true if a classical frequency probability approach is used. At the other extreme, if too wide a range of weapon scenarios or facility variations is included in a probabilistic formulation, the quantification loses meaning. Purely subjective formulations lack consistency and credibility.

We have developed a balanced approach retaining the frequency interpretation as much as possible and use probability theory as a tool to treat and propagate the uncertainties. If necessary, the model will also to accept expert estimates, both explicitly and numerically. The actual implementation is complicated by the following factors:

- The mission function must be specified and the necessary and sufficient component subset disablement to achieve functional outage must be determined.
- Determining the level of detail, and basic components to include in functional diagrams is non-trivial.
- \( S \) and \( T \) are non-scalar in nature. Stresses at different components, and their uncertainties, are often not independent.
- There is often a latent time delay between component physical damage and the onset of functional outage.
- The propagation path and associated time delay from one component to another must be included.
- Component and subsystem repair times and inherent repair sequences must be specified. Also, the effect of human resource constraints and scenarios must be factored into the repair/reconstitution ability.
- The uncertainties associated with all input values and assumptions must be specified.

Our formulation accounts and allows for all the above complications. The difficulty of specifying the joint probability distribution of mutually dependent and time-dependent stresses, thresholds, internal damage propagation, and repairs makes an analytically explicit solution infeasible. Nevertheless, the model is set up such that defendable results can be obtained based on available system information and reasonable engineering approximations.

5.0 Model Validity and Limitations
Incomplete knowledge of the facility/system functional components, their interrelationships and outage mechanisms can limit the accuracy of the calculation in two ways:

1) If an in-parallel functional component, which contributes to system performance redundancy, is omitted from the model then the true effect is less than or equal to that assessed. In this case the assessed effect measure is defensive conservative.

2) If an in-series functional component exists, which contributes to system vulnerability, but is omitted from modeling due to lack of information, then the true effect measure is at least as assessed. That is, the assessed results are not defensive conservative.

Thus the completeness of the set of identified model components results in uncertainties in the output probability in both directions. Of course the tool can be used to gain insight into overall results sensitivity to model completeness by selectively omitting from and adding to a system’s component list.

A critical part of the modeling process is determining which components or combination of components must be nonfunctional to eliminate the system’s mission capability. The modeler must identify the minimum set of components whose disablement would be sufficient to cause functional debilitation of an entire facility or system. If all members of this set are nonfunctional, even if everything outside the set performs perfectly, the system ceases to function. This set is modeled as a “components-in-parallel” functional diagram. In some probabilistic risk assessment literature this is referred to as a “cut set” in that cutting off any one of its members, the set is invalidated as a sufficient cause of mission outage.

Another concept useful for ensuring model realism involves identifying the minimum sufficient set of components that ensures functional performance if all its members perform their respective functions. This is equivalent to an “all component in series” functional diagram and is sometimes referred to as a “path set” in PRA literature because a functional path through all of the set members constitutes a system function.

A theoretically trivial, but important and sometimes tricky consideration is the avoidance of double counting. This is a special case of correlated-cause component dependencies. In cases where one component’s operational status appears in different sets, the model must ensure that the component is modeled as one and the same.

Model validation can be performed using logical implication checks. This involves running self-consistency and special limiting-case checks. Because of the general inability to do multiple system copy pass-fail experiments, validation must be indirect and relative. This is a general problem for PRA models of complicated systems.
6.0 Summary and Conclusions

We have developed a new capability to model mission outage of complex facilities and systems due to any effect or attack mechanism where the an effect “stress” and subsystem/ component “strength” can be defined based empirical data or reasonable engineering approximations. Scenarios may include intentional physical or cyber attacks, RF Weapons, accidents, or Murphy. The model enables comparison of the effectiveness of alternative mitigation strategies techniques and enables location of most serious failure points from the standpoint of highest probability of effect and longest duration functional outage. Output in the form of probability of effects vs time output facilitates estimation of recovery times.

The model provides the following capabilities:

- Selection and identification of component subsystems at the desired level of detail
- Specification of minimum sufficient component sets to achieve mission outage
- Non-scalar subsystem stress / threshold comparisons at the component level
- Correlated cause dependencies of stresses and their attendant uncertainties
- Inclusion of propagation paths and times associated with component-to-component cascade effects (unique)
- Inclusion of latent time delay effects associated with onset of damage for real subsystems (unique)
- Inclusion of repair time and repair sequence for damaged components including effects scenario-dependent human and material resource constraints (unique)
- Accommodation of uncertainties in all input parameter values
- Output as a simple plot of probability of mission outage vs. time (unique)