D. Fritsch, M. Englich & M. Sester, eds, 'IAPRS', Vol. 32/4, ISPRS Commission IV Symposium on GIS - Between Visions and Applications, Stuttgart, Germany.

A STRATEGICAL MODEL FOR ANALYZING SURVIVABILITY OF ENVIRONMENTAL RESOURCE MANAGEMENT SYSTEM

Zhu Zesheng [a] and Sun Ling [b]

[b]JiangSu Academy Of Agricultural Sciences, Nanjing, JiangSu, 210014, P. R. China
[a]Nanjing Naval Institute of Electronic Engineering, Nanjing, JiangSu, 211800, P. R. China

ABSTRACT

The survivability analysis of system of environment resource management under complex networking environment is very important for effective management of environment resource. This analysis relates usually to integrity, survivability, failure evaluation, failure control of the system. This paper discusses several important issues and proposes a strategical model based on a probabilistic framework for the study of failure-based survivability of system of environmental resource management. The strategical model based on an unified framework is very important for investigation of the system survivability. Otherwise, this paper also reports two general survivability performance models. It is expected that these models have wide applicability in planning survivable system of environmental resource management under networking environment. Thus, the model provides an unified and practical approach to analyzing and designing highly survivable system of environmental resource management.

1 INTRODUCTION

Interest in reliable and robust system of environmental resource management has been increasing in recent years. Research and development of the system are very important for economical development of developing country. Especially, the system dependents more on its distributed computer network environment. Thus, it has increased dramatically in both size and complexity in the last few years. However, the new power brought with modern information processing technology creates greater vulnerability (Neumannm, 1992). Since faults are inevitable, their quick detection, identification and recovery are crucial to make the system more robust and operation more reliable.

As system of environmental resource management become more heterogeneous and more hardware and software from various vendors are used, the whole picture of the system specification becomes bewildering. This brings out the need for a unified approach or model to the area of survivability analysis of system of environmental resource management based on distributed network under failures and disasters.

On the other hand, traditional methods of designing the system aim at satisfying some specified performance objectives under normal conditions without explicit consideration of the system quality or survivability. Thus, the performance under failures or disasters can be unpredictable for the system based on these methods. But, a major benefit of setting survivability performance objectives will be to ensure that, under given failure or disaster scenarios, the system performance will not degrade below predetermined levels. Further, such a set of performance objectives should be used as the design and implementation goals of future system of environmental resource management.

Due to the lack of feasible method for analyzing survivability of a large complex and heterogeneous system of environmental resource management, some analysis method must be developed for the application need. This is particularly true in the area of survivability management of the system, which has been recognized as one of the main task of design of system of environmental resource management. The requirement of this method, usually, is a short development cycle and the fact that it can be easily applied to analyze the survivability of the system.

So far, the research result on survivability of system of environmental resource management is not still found. This research importance is not widely recognized. In fact, the research is more important than the system application itself. Especially, in networking environment, the system survivability determines whether the system can complete predefined design goals.

2 SURVIVABILITY ANALYSIS

Elements or components of system of environmental resource management can fail for any number of reasons, including architecture defects, design defects, and inadequate maintenance procedures. Intrusions can come from acts of earthquake, flood, hurricane, and other accidents related to environmental disaster.

The task of the survivability analysis is to keep track of failure and disaster status, which include both severity and extent, and trigger maintenance actions when necessary in order to recover the system operation. The analysis process can be divided into the monitoring process and maintenance process. The monitoring process involves collecting information about the short-term or long-term behavior of failure and disaster, and interpreting the semantics of the collected information. The maintenance process affects the status of failure and

D. Fritsch, M. Englich & M. Sester, eds, 'IAPRS', Vol. 32/4, ISPRS Commission IV Symposium on GIS - Between Visions and Applications, Stuttgart, Germany.

disaster according to the interpreted information to achieve a desired maintenance outcome.

2.1 Integrity

As a result, there is a growing need for ensuring that the system of environmental resource management maintains service despite failures or disasters. This desired service or quality is called survivability performance or survivability of the system. On the other hand, the system quality can be also evaluated by its integrity. The integrity problem of optical communication system was discussed in (Wu, 1992), which provides a number of valuable experiences for the similar study of other system. In general, the integrity is a higher measure and includes three major aspects as the followings.

(1)The availability deals with the fraction of time that the system is in service. For example, a metric is purposed to measure loss of environmental resource due to the system failure in units of US dollars/year in order to evaluate the system quality.
(2)After-failure survivability assumes that some failure has occurred in the system. Usually, the worst-case single or more failures are considered for computing the system quality.
(3)Failure-based survivability considers what happens in the wake of a failure in the system. The occurrence of a failure event is used as a given assumption. For example, in the case of a large-scale failure, failures of several components in the system could happen simultaneously. In general, the system may fail totally, partially, or not at all. Thus, the analysis result can be used for computing the system quality.

2.2 Survivability

Survivability discussion of system of environmental resource management involves analyzing availability of the system, computing quality of the system and evaluating failure-based survivability under various disasters or failures.

On the other hand, any traditional method of designing the system aims at satisfying some specified performance objectives under normal conditions without explicit consideration of the system survivability. However, the performance under failures can be unpredictable for the system designed with the method. In contrast, a major benefit of setting survivability objectives will be to ensure that, under given failure scenarios, the system performance will not degrade below predetermined levels. Further, such a set of performance objectives should be used to implement design and management goals of the system.

For example, these quantities related to the system survivability include the expected survivability, the worst-case survivability, the r-percentile survivability, and the probability of zero survivability. Particularly, one survivability function can be derived in closed form for analyzing plainly the system survivability under the system components or elements influenced by failures. The disasters or failures can be represented by undesirable events. Some typical examples are sever thunderstorm, tornado, hurricane, earthquake, fire, flood, tsunami, weather disasters, building destruction, the system fail, and other environmental disasters that affect the normal operation of system of environmental resource management. Some different types of failures may occur with different frequencies and may have different effect on the system, so that survivability of the system under different failure or disaster types must be studied separately.

2.3 Differences

Integrity of system of environmental resource management should not be confused with reliability (the probability of performing a function for a period of time), quality (customer satisfaction), or availability (ratio of up time to total time). Integrity is a higher level measurement of performance of the system that indicates ability of the system to operate in the presence of any failure or disaster. Architects and designers can use redundancy to build integrity into system of environmental resource management. They have recognized the critical role that the system plays in society and the consequences of failure in system of environmental resource management.

2.4 Analysis

There are two methods to survivability analysis related to system of environmental resource management. The method of probability models (Barlow and Proschan, 1975; Larson and Shubert, 1979) can be used. The first method uses probability of failures of system of environmental resource management and, possibly, rates of repair and restoration to calculate various probabilistic measures of availability or unavailability of the system. The second is a conditional method, defining measures of the system after given failure event have occurred. This method may either use probabilistic weighting of the resulting states of the system and resulting restoration and repair of the system after the failure or use deterministic analysis of these states. The methods can be used to evaluate different restoration, repair, or preventive policies.

3 FAILURE EVALUATION

3.1 Outage Concept

An outage about environmental failures or disasters in system of environmental resource management can be further represented by the following three key features: Unavailability, Duration, Geographic area, and Weight.

Unavailability (U). It is defined in terms of an usage component. In system of environmental resource management, the most common function is its ability to manage environment resource within the limits of predefined objectives. The usage component of the system is a work to provide management functions. In this instance, unavailability is the percentage of components that fail due to failure or disaster.

Duration(D). It defines the time during which the unavailability condition exists in system of environmental resource management. It is measured by determining the beginning and ending points of a failure in the system, based on the unavailability being above a given threshold.

D. Fritsch, M. Englich & M. Sester, eds, 'IAPRS', Vol. 32/4, ISPRS Commission IV Symposium on GIS - Between Visions and Applications, Stuttgart, Germany.

Weight(W). It includes the influences of failure and disaster patterns and other factors, in which the unavailability exceeds a given threshold.

Geographic area(G). It includes the influences of geographic area, in which the unavailability exceeds a given threshold.

3.2 Outage Types

The four parameters can be used as the basis of measuring and quantifying failures of system of environmental resource management and their impact on services and users. Depending on the values of U, D, G and W, outages of system of environmental resource management may be classified as large, middle and small failures as the followings.

(1)Large: A failure of system of environmental resource management with a combination of U, D, G and W that is more severe than a middle failure.
(2)Middle: A failure of system of environmental resource management with a combination of U, D, G and W that is less than large failure.
(3)Small: A failure of system of environmental resource management with a combination of U, D, G and W that is neither large nor small failure.

3.3 Failure Types

The failures of system of environmental resource management can be categorized by different sets of values for which the (U, D, G, W) triple qualifies for the particular category of outage. For example, a given category of failure could be defined by simple thresholds, $U \leq U0$, $D \leq D0$, $G \leq G0$, $W \leq W0$ for a given category of thresholds (U0, D0, G0, W0). However, more complex qualifying formulas may be appropriate for given systems, services, and users. Further, outages of system of environmental resource management may be classified as different levels such as large, middle or small, depending on whether the values of the (U, D, G, W) triple fall in the appropriate qualifying regions. These regions can be determined by past observations, data and experiences.

4 STRATEGICAL MODEL

This following discussion includes several important issues and proposes a probabilistic model for the study of failure-based survivability. This is because an unified model is very important for survivability investigation of system of environmental resource management. This general model can be used for characterizing survivability of the system. Based on this model, survivability of system of environmental resource management is computed by a survivability function, and various quantities of interest can be derived from the function.

In order to implement the survivability evaluation of system of environmental resource management in networking environment, it is necessary to build an effective model for this evaluation. The objectives related to the evaluation are typically set out in the form of general policies of evaluation into a number of more specific policies of evaluation to form a policy hierarchy in which each policy represents its procedures to meet its objectives.

The discussion focuses on development and implementation of a survivability analysis model for large-scale integrated system of environmental resource management. The objective is to improve the survivability of the system in handing various types of environmental disasters and failures. The efficacy of the model has been demonstrated on a testbed of system of environmental resource management.

4.1 Concepts

Users of system of environmental resource management have unique requirements and expectations for guaranteed service performance, depending on the user type, service value, and cost. To meet these user expectations, service providers may make use of various means, including specific configurations of the system, management policy of the system, restoration techniques or procedures, the system hardening, prevention of disasters and failures, and other emerging technologies.

In national and international emergencies, the government expects system of environmental resource management to be capable of providing survivable services for national decision makers, executing crisis management control, offering control of environment resource, and reconstituting of the system.

There are many ways to describe survivability of system of environmental resource management and define survivability measurements. Using the measurements, relevant quality can be defined.

In the model, it is assumed that failure has already occurred and the system reaction for restoration starts after failure. This is the way that survivability is simply measured. The general procedure for evaluating the survivability measures is as the followings.

(1)Define a survivability measurement."
(2)Choose a failure scenario".
(3)Obtain a list of all combinations of events.
(4)Calculate the survivability measures of system of environmental resource management.

4.2 Model

Survivability of system of environmental resource management, s, can be defined as the fraction of x that remains after an instance of the failure or disaster under consideration has happened. Here, x is a selected feature of the system, which can be quantified and represents the ability of the system to manage environmental resource in normal status. This feature describes also integrity of system of environmental resource management.

In general, s is a random variable rather than a fixed quantity, and survivability of system of environmental resource management can be described by a survivability function rather than a single-value survivability measure (Papoulis, 1965). For example, in a large-size system of environmental resource management, the number of remaining system components in the system can be

D. Fritsch, M. Englich & M. Sester, eds, 'IAPRS', Vol. 32/4, ISPRS Commission IV Symposium on GIS - Between Visions and Applications, Stuttgart, Germany.

determined under a serve failure or disaster. Some of the components may be destroyed by it. Depending on which components are destroyed, the value of s may be different.

Suppose that the set of inoperative components can be described probabilistically; a sample space E={e} consisting of all subsets of components can be built, each is assigned by a probability measure that represents the likelihood that the subset of components are destroyed. Thus, for each sample point e , a probability Pe and a survivability Se can be obtained, where Se is the fraction of components of normal operation. From this analysis, the related survivability function P[S=s]= ∑Pe can be found, which is the probability that a fraction s of components are in normal operation. Where e: Se=s, a fraction s of the components are operative. From survivability function, some usual parameters to describe survivability of system of environmental resource management can be given as the followings.

(1)Expected survivability for all s: E[S]= ΣsP[S=s];
(2)Worst-case survivability for all P[S=s]>0:s*=min s;
(3)r-percentile survivability for all P[S≤s]≤r/100: s_r=max s; and
(4)Probability of zero survivability P_0=P[S=0].

Obviously, larger value of E[S],s*, s_r, and (1-P_0) corresponds to system of environmental resource management that is more survivability. Each parameter captures a different aspect of survivability of the system.

For more general system of environmental resource management, a procedure for finding survivability function is as the followings.

(1)Specify failure or disaster type to be studied by outage analysis;
(2)Define Normal operation" of system of environmental resource management by outage analysis;
(3)List all combinations of events that may happen under the considered failure or disaster type as the sample points {e};
(4)Determine the survivability Se;
(5)Determine or assign probability of each event e; and
(6)calculate survivability function P[S=s].

4.3 Management

One of application of the above mode is survivability management. The role of survivability management is to manipulate the adjustable system parameters so that system of environmental resource management can adapt itself to a dynamic disaster or failure environment. The survivability management is divided into the followings.

(1) Survivability evaluation to find how changes in disaster or failure parameters affect the survivability measure of system of environmental resource management; and
(2) Decision making on how to adjust the system design parameters to increase the system survivability.

The first task is essentially equivalent to finding a relationship between the system performance and the disaster or failure parameters, which may be required to estimate the survivability performance of the system. The second task is to decide the direction and magnitude of parameter adjustment of the system design when considering occurrence of disasters and failures.

5 FAILURE MANAGEMENT

From the policy hierarchy, the major components of failure management related to system of environmental resource management include failure management, distribution management, and influence management. As its name implies, fault management is responsible for detection, isolation, and recovery from component failures and inflicted damages related to failure or disaster. Distribution management is related to determination of failure influence and accommodation of failure distribution changes, including services requested by failure management and influence management. Influence management is responsible for reducing the failure influence by adjusting the failure control decisions, and critical for efficient control of large-scale failure that occurs in a dynamic environment.

5.1 Method

Modeling management information of the failure or disaster is to map disaster distribution, characteristics, and events to objects, which is an effective method for the failure management. An inheritance hierarchy can be used to represent a simple classification of failure object classes, where the elements class has three subclasses: distributions, characteristics, and events. Physical entities class has two subclasses: affected entities and geographic positions.

5.2 Failure Data

Failure management data in the policy hierarchy of the failure management can be broadly classified into the followings.

(1)Measurement data. The measurement data of failure is the raw information that is received from the failure monitoring processes, and includes various variables related to the failure. The data provides the primary input for failure management. It represents the current status of the failure. Measurement data can be divided into two groups according to the general characteristics of management policy of the failure: persistent and perishable. The persistent data consists of measurement data, whose use is long-term, and therefore needs to be maintained permanently in database. On the other hand, perishable measurement data is of limited time use, so that its current value is valid only until the failure characteristic is being monitored.
(2)Structural data. In contrast to measurement data, structural data is composed of static failure information. Unlike measurement data, structural data is valid even when the failure does not occurs. Most of structural data is stored at initiation time of failure management system.
(3)Control data. Control data captures the current selection of control decision for failure. The process for changing an existing set of control decisions is usually completed by the failure managers of the policy hierarchy. Alternatively, the changes may be

D. Fritsch, M. Englich & M. Sester, eds, 'IAPRS', Vol. 32/4, ISPRS Commission IV Symposium on GIS - Between Visions and Applications, Stuttgart, Germany.

automatically triggered as a function of the information in the measurement data. In addition to the current settings of control decisions, the control database also stores a library of predefined control decision settings that reflect the appropriate settings for a variety of common failure patterns and distribution.

Thus, the failure management system based on policy hierarchy are responsible to monitor, interpret, and control the failure.

5.3 Influence Management

The role of influence management of any failure in system of environmental resource management is to manipulate the adjustable control decisions in real time so that the failure influence can be efficiently controlled in order to reduce the failure loss. Influence management from analysis for the policy hierarchy is divided into two task as the followings.

(1)Influence evaluation that finds how changes in control decisions reduce the influence of the failure; and
(2)Decision making on how to adjust the control decisions.

The first task is essentially equivalent to find a relationship between the failure influence and the control decisions, and may be required to estimate the failure influence. The second one is to decide what control decision is selected for controlling the failure influence.

5.4 Influence Evaluation

The analytical techniques, such as probability theory, can be used for the influence evaluation of the failure in system of environmental resource management. However, they require unrealistic assumptions and tend to be mathematically untractable as the structure of the influence measure becomes complex. On the other hand, discrete-event simulation is a viable alternative to analytical techniques. Its major advantage is that it can be modeled with much less stringent assumptions, and more complex performance measures can be handled with relative ease. However, discrete-event simulation usually suffers from significant computational burden because a single simulation run represents only one realization of a stochastic process. In order to obtain an accurate influence estimation under a given failure, several independent runs are needed, and these runs should be repeated.

5.5 Decision Making

In the policy hierarchy, this task requires control decision optimization, and can be accomplished by the learning and inference methods.

6 FAILURE CONTROL

The fundamental goal of failure management is to be able to control the influence of the failure. The failure control mechanisms can be classified along two dimensions: local versus global and automatic versus manual as the followings.

6.1 Local Control

Local control mechanisms rely on local data collection and local decision models related to the failure management. The local refers to specific components of the failure as opposed to the failure as a whole. The advantage of local controls is that they incur fewer decision overhead, since decisions are made locally with local data. Due to this locality of the operation, local control processes are unaffected by other local control decisions.

6.2 Global Control

Global control processes rely on all failure data and global decision models related to the failure management. Clearly, global control processes are capable of optimizing performance of total failure control decision. However, they are more vulnerable to the failure in system of environmental resource management and have greater information overhead since decisions require all failure data.

6.3 Automatic Control

Automatic controls monitor certain data of characteristics of the failure in system of environmental resource management. When specific conditions are met, control decisions are automatically changed without operator or manager intervention. Automatic controls can be either global or local.

6.4 Manual Control

Manual control processes either permit or require human intervention. The failure management alters control decisions using these processes. Clearly, the role of a management information base is to provide the failure manager with information that supports decision making regarding the failure. This supporting activity may be achieved passively by simply providing an interface between the failure manager and failure status information. Alternatively, it may be achieved through an alarm system that notifies the failure manager of failure conditions.

7 APPLICATION

It is expected that the strategical model has wide applicability in planning and managing survivable system of environmental resource management. Thus, the above framework and model provide an unified and practical approach to analyzing and designing highly the survivable system.

An example of system of environmental resource management can be discussed as the followings. Survivability of the system is defined as the fraction of the system components under normal operation when the disasters or failures occur.

7.1 Method

First, suppose that n components have been considered, and that a component failure is likely to be located anywhere within the system. The corresponding

survivability function P[S=s/n] can be derived as the followings.

Obviously, for n=0, no component will be destroyed. So, n>1 shall be assumed in the following. To the case that the number of components is very large, S becomes a continuous random variable. The survivability function P[S=s/n] is easily obtained.

When calculating the survivability function, one should first specify the type of failure and definition of the normal operation" of system of environmental resource management with the help of outage analysis. This is important since different failures may have different effects on system of environmental resource management. Thus, damage to the system and the probabilistic characterization will be different in different cases. This fact shows that different results can be obtained, depending on the feature of the system for which we are calculating survivability. For example, definitions for normal operation" may be the ability to provide management services for users.

The next step is to list all possible combinations of events that could happen under the failure type. These combinations may make relevant components of system of environmental resource management inoperative. Given a more general system of environmental resource management and a different definition for normal operation,", listing all the sample points may be difficult and can only be done effectively by a numeration method. Once the sample points have been listed, the next step is to calculate the survivability measure for each sample point. This calculation will depend on the definition of survivability related to outage analysis.

If the definition is the number of components under normal operation, then an efficient method can be used to determine the survivability. Otherwise, one may want to identify more efficient methods by exploiting the particular system of environmental resource management being considered.

To each sample point, a probability measure representing the likelihood of its occurrence can be assigned by outage analysis. The assignment of probabilities to sample points should be based on past observations, data or experience.

7.2 Graph Description

A system of environmental resource management may be represented as an undirected graph. Thus, graph theory is the proper framework for our considerations. A node in the graph represents a component of system of environmental resource management. A link or arc between nodes represents a control or management relationship between them. There is a central node in the graph for controlling or managing all other nodes through links or paths consisted of these links. The following notation can be used to describe system of environmental resource management.

N node set, with |N| nodes
L link set, with |L| links
(i,j) a link between nodes I & j
p, q link [reliability, unreliability] for all links; q+p ≡1
G(N, L, P) graph (N,L), including p
S(G) survivability of G
Xij selection status of (i,j):
Xi,j=1 if (i,j) is survivable, else Xi,j=0

7.3 Results

As a computing example, consider a system of environmental resource management which is represented as a ring structure with 10 nodes connecting a central node. Here Sa is the fraction of remaining nodes connected a central node. Under a failure, Cu nodes have been destroyed. Depending on which nodes are failed, the value of Sa may be different.

Cu is a random variable with values Cu=0,…, n. In this example, the number of failed nodes and the number of ways Cu=2 can occur. The set of nodes connected to the central node, Ca=0, …, (n-Cu). Using this information, the fraction of nodes connected can be easily obtained when given two failed nodes.

Assuming the two-node failed case, there are 45 ways of choosing the failed style. Thus, when two nodes are destroyed, there is a 41% probability that 72% of the nodes are connected to the central node, and there is about a 6% chance that no nodes are connected to the central node. These data describe clearly the survivability of system of environmental resource management and can be used to compute other important data about survivability of the system.

8 CONCLUSIONS

In summary, this paper discusses mainly basic principles, key techniques of a strategical model for analyzing survivability of environmental resource management system.

The above discussion shows that the usefulness of such method for analyzing survivability of system of environmental resource management and the ability to construct the relevant analysis model are limited not by computer technology but by knowledge of the model dynamics and the effect of various decision upon them. It is that a model dynamics may depend more on the manner in which its elements are described and linked than on the form of its equation and sub-systems.

Further, some major steps of application of the approach for developing the strategical model are as the followings: scooping of an application development project, in which the project area, requirement and relevant variables are defined by the plan objective, based on user requirements of system of environmental resource management and variable operation rules; collecting data relevant to variables in the application field, in which these data must be represented as variable; developing, evaluating and selecting all important logical relationships between the variables, in which the relationships are used to build basic framework of the model; integrating the relationships and the data relevant to variables, in which the final model is built; refining this model and improving its performance.

D. Fritsch, M. Englich & M. Sester, eds, 'IAPRS', Vol. 32/4, ISPRS Commission IV Symposium on GIS - Between Visions and Applications, Stuttgart, Germany.

The work to develop more efficient method to analyze the survivability of system of environmental resource management will become a future challenge in the domain. The survivability analysis related to failure or disaster will change from the current simple model into future more complex one. Many current mathematical tools will provide the powerful supports for the challenge or objective. However, the future major research works about the survivability analysis are to solve some key problems that include how to improve architecture of the model, how to construct the operation rules used in the architecture, and how to design and implement these rules. In summary, the above successful experiences have shown that our current work and outcomes provide a satisfactory ground and open a wider research domain for the development of future survivable system of environmental resource management.

9 ACKNOWLEDGMENT

The authors wish to acknowledge the valuable contributions from Mrs. Chen Gui-Zhen to the research. This work was supported by both the Project of China National Foundation of Natural Sciences (Project Number 39470415) and the Project of Navy Research.

10 REFERENCES

Barlow, R. E. and F. Proschan (1975). *Statistical Theory of Reliability and Life Testing: Probability Models*. Holt-Rinehart, Winston, New York.

Larson, H. J. and B. O. Shubert (1979). *Probabilistic Models in Engineering Sciences*. John Wiely & Sons, New York.

Neumannm, P. (1992). Risks to the public in computers and related systems. *ACM Software Eng. Notes*, **Vol. 17, no. 1**, pp. 3-32.

Moffet, J. D. and M. S. Sloman (1991). The representation of policies as system objects. SIGOIS Bulletin, **Vol. 12, no. 2 and 3**, pp.171-184.

Papoulis, A. (1965). *Probability, Random Variables, and Stochastic Processes*. McGraw-Hill, New York.

Wu, T. -H. (1992). *Fiber Network Service Survivability.* Artech House, New York.