# DISASTER TOLERANT SYSTEMS ENGINEERING FOR CRITICAL INFRASTRUCTURE PROTECTION

**Michael A. HARPER**
**Critical Infrastructure Protection Center, Department of the Navy**
**North Charleston, South Carolina 29419, U.S.A.**
**(843) 218- 4506**
**Michael.A.Harper@navy.mil**

**Mitchell A. THORNTON**
**Department of Computer Science and Engineering, Southern Methodist University**
**Dallas, Texas 75275, U.S.A.**
**(214) 768-1371**
**mitch@engr.smu.edu**

**Stephen A. SZYGENDA**
**Department of Computer Science and Engineering, Southern Methodist University**
**Dallas, Texas, 75275, U.S.A.**
**(214) 768-3959**
**szygenda@engr.smu.edu**

***Abstract - Quality of life in the United States relies, in large measure, on the continuous operations of a complex infrastructure. This infrastructure is comprised of physical and information-based facilities, networks, and assets, which, if disrupted would seriously impact health, safety and security of citizens or effective functioning of governments and industries. This infrastructure system includes telecommunications, energy, banking and financial, transportation, water, healthcare, government and emergency systems. All of these systems are linked through vast physical and cyber networks which have become completely interdependent. These networks present with a multitude of distributed heterogeneous components so tightly interconnected that a focal disaster can lead to widespread failure almost instantaneously. A disaster is an event that can cause system-wide malfunction as a result of one or more failures within a system. Disasters may occur as the result of single or multi-point failure and may occur either simultaneous or sequential. Disaster tolerance is a superset of fault tolerance in that a disaster may be caused by multiple points of failure in a system that occur very close together in time as well as a single point of failure that escalates into a wide catastrophic system failure. Adequate means to ensure continued system operation in the event of a disaster requires highly reliable and survivable system design of distributed and interdependent systems. This paper will evaluate specific methodologies for disaster tolerant systems engineering for improved command and control of critical infrastructure systems. The current state of disaster tolerant application systems is explored including an investigation into the reliability and survivability requirements necessary to achieve disaster tolerant system operation.***

**Keywords**: Disaster Tolerance Systems Engineering, Disaster Tolerant Computing, Survivability

## 1. INTRODUCTION

The survivability of critical infrastructure systems has become a major concern of the United States Government due to recent events directed both on the nation's homeland and American interests around the globe. These events have supported the growth of numerous government and industry initiatives in the area of homeland security and defense [4, 29]. The specific goal of these initiatives is to establish infrastructure systems that continue to provide acceptable levels of service to customers in the face of disturbances; natural, accidental or malicious.

The reliance of the nation's critical infrastructure systems on fragile information and communication systems puts these infrastructures at risk for catastrophic failure. Threats arise from reliance on commercial components of unquantified reliability, unsecured legacy software systems, and a lack of understanding of continuously evolving distributed complex networks. All of these variables are vulnerable to outside manipulation through networks and outsourcing of design.

Massive computerization of infrastructures has enabled major efficiency gains, but at the cost of tightened coupling. The financial cost of interruptions escalates more rapidly now than before computerization. There is a specific need for approaches to infrastructure design and evolution that simultaneously enable the efficiencies that computers make possible while ensuring that the costs of service stream interruptions remain acceptable in the face of disruption.

The vulnerability of critical infrastructure systems to disasters creates new challenges for systems engineering, as well as for research across related disciplines such as software engineering, computer science and security engineering. In systems engineering, design for disaster tolerance including survivability, reliability and fault tolerance, emerges as a research priority.

Infrastructure systems are large and distributed. Modeling for these complex systems requires interdependent sector analysis and the ability to handle potentially dissimilar fault models. In this respect, hierarchical modeling is investigated as a means to provide adequate systems analysis.

The following sections discuss the rationale for hierarchical analysis of infrastructure sectors and provide a background investigation into various methods applicable in this area. Further, the application of systems theory to critical infrastructures in the face of catastrophic events is discussed.

## 2. DISASTER TOLERANT SYSTEMS ENGINEERING

Fault tolerance of a system is essential to ensure continued operation and provide necessary system services despite the failure of components. The goal of a fault tolerant system can be defined as the specified degree of resiliency in a system, subject to minimizing overhead costs such as duplicate resources, communication, and time overheads [22]. Designing disaster tolerance into complex critical infrastructure systems is essential to ensure continued operation and provide necessary system services despite the failure of components.

When disrupted, an information system must be adjusted to assure continued provision of the information services on which the infrastructure depends. Adjustment will involve reconfiguration. To be reconfigured, an information system must be reconfigurable. System reconfigurability can occur at many levels, including operating parameters, module implementations, code location, replacement of physical devises, etc. An understanding of the failure rates inherent in these levels requires incorporating systems reliability.

Reliability theory is a critical component involved in this respect in order to model system behavior and ensure system operational success. Reliability is a function of probability which can be defined as a quantified measure of uncertainty about a particular type of event. Probability generally assumes that there exists certain information about a system such as the individual component reliability behavior. Generally, the completeness of this information relies on the satisfactory fulfillment of two conditions:

1. All probabilities or probability distributions are known or are perfectly determinable.
2. The system components are independent.

However, when attempting to model and analyze the reliability of large complex systems these assumptions may not hold. For example, when a system has a series-

parallel structure as represented in Figure 1, its time-to-failure (TTF) cumulative distribution function (CDF) can be obtained by multiplying together the failure-time CDFs of the parallel subsystems and subtracting from one the product of the reliability function of the series subsystems.

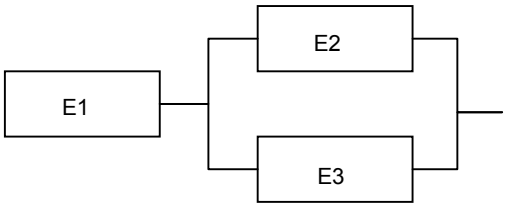


Figure 1. Series-Parallel Structure

This method works because the series-parallel nature of the system means that it can be broken down into substructures whose failure times are statistically independent of one another. When a system is modeled as a complex system and is not series parallel, such a breakdown is not possible and standard reliability modeling methodologies are not applicable.

Complex systems are typically structured in a hierarchical structure. Each layer of this system has a specific function. However, the reliability of each layer is dependent on inputs from other layers [20]. Hierarchy theory deals with the fundamental differences among one level of complexity and another. Its ultimate aim is to explain the relationships among different levels: what generates the levels, what separates them and what links them together [20]. Numerous approaches have adequately been proven for analytically predicting the reliability or availability of series-parallel fault tolerant systems where system components are assumed to be independent and the probability distribution of the components are known. These include combinatorial models, such as fault trees and reliability block diagrams, and the use of Markov models to analyze the system with linear time dependent algorithms [9] [12] [21]. However, when attempting to model the reliability of complex systems comprised of non-series-parallel structures these methods are not feasible. They are computationally expensive, or suffer from the state-space explosion problem [12] [23]. This section evaluates the use of several hierarchical reliability methodologies to model complex systems and provides potential means to design adequate system reliability into critical infrastructure. In addition a methodology is investigated on how performance is affected by combining dissimilar fault-tolerance schemes at adjoining levels.

Hierarchical models represent a large class of models that use hierarchical structures to avoid very large state spaces when modeling complex systems [12]. It is important to investigate methodologies for dealing with the state-space problem because reliability analysis of systems with very large state spaces requires the use of complex numerical methods for solving large systems of algebraic equations or the application of ordinary differential equations [23]. In addition, hierarchical models are necessary since most practical problems do not satisfy the assumptions of independence and series-parallel structures.

Sahner et al 1986, discuss the use of a hierarchical modeling technique called the Symbolic Hierarchical Automated Reliability and Performance Evaluator (SHARPE) to specifically avoid the state-space explosion problem. SHARPE allows the ability to use mixtures of reliability models at different levels while providing freedom in the number of levels in the hierarchy. The different types of reliability models can be combined hierarchically by using all or part of the solution to one model as part of the specification of another model. The authors' technique makes available mean and variance of each cumulative distribution function (CDF) produced in the analysis [21].

A second method is presented by Sharma et al 1991, and introduces a hierarchical approach for computing the terminal reliability between any given source-destination pair in large, complex networks. The method proposed allows the development of an approximate reliability expression for any large network of any size by modeling the network in a hierarchical form with specified 'clusters' of network nodes. An overall reliability value is approximated by computing various

parameters for individual clusters of network nodes and combining them to determine an approximate analysis [24]. Figure 2 illustrates this methodology of breaking down the problem into sub problems for a reduction in algorithm complexity.

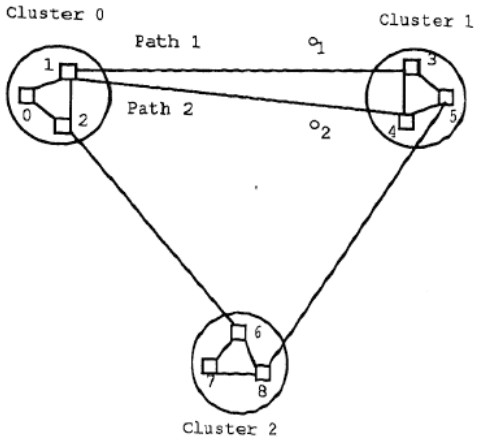


Figure 2. Example of a hierarchical network [24].

This model represents a 2-level hierarchical network where level one of the network is grouped as a cluster and level two of the network serves to interconnect clusters of level one nodes. In this fashion, each cluster is modeled as a node. The inter-cluster links create the network graph model. Each cluster may then be modeled individually as a graph which forms the set of cluster models, as seen in Figure 2 [23].

This type of model can be used to model the failure and recovery behavior of each node cluster type and predict the expected cluster availability. The availability of a path is the product of the availabilities of the node clusters in the path. The model is developed based on the notion of node clusters and origin-destination pairs. Reliability terms corresponding to the paths within a cluster are made disjoint with respect to each other. The advantage of this methodology is realized when attempting to evaluate the reliability of large systems. This algorithm breaks down a large problem of terminal reliability in large distributed systems into sub problems which drastically reduces the complexity of the evaluation. This process allows for an exact reliability expression to be obtained by multiplying the terms corresponding to each sub path [23].

Several researchers have identified the importance of understanding the effect on system performance and how information exchange may be affected when combining dissimilar fault-tolerant models between different levels of the hierarchy [21] [22] [23]. In particular, Shieh et al 1990 surveyed analytical models to evaluate the coordination of various levels of the hierarchy including the integration of various fault tolerant schemes required for complex hierarchical systems. They propose the use of Stochastic Petri Nets (SPN) for reliable process communication throughout a distributed hierarchical system through the use of *checkpointing with rollback recovery* as the method for fault tolerance [23]. They specifically focus on the probability of failures when processes from other 'hierarchical layers' synchronize in distributed systems. If a failure occurs at this integration, uncontrolled rollback of the system to its initial state may occur and result in a total system failure. The authors' combine SPN models with probabilistic analysis of uncontrolled rollback recovery to model what they define as the domino effect.

The rollback of one process due to failure may cause another non failed process to also rollback. This is due to the communication among the process between the times at which the communicating processes took their checkpoints. A rollback of non failed processes in this manner can lead to an uncontrolled rollback of all the communicating set of processes and as a worst case, bring the system back to an initial state, which is unacceptable for any real-time system [23].

To prevent the domino effect from occurring in these systems, the authors' propose the use of a planned checkpoint strategy where the processes mutually agree to perform a checkpoint function whenever any two processes communicate. This scheme would ensure that there is no domino effect. In the worst case, the processes would rollback to the most recent transition checkpoint before the synchronization and the place just before the next

synchronization. The main problem is the integration of the fault tolerant schemes at different levels and its effect on the choice of checkpoint strategy at different levels [26].

The final method evaluated uses a Bayesian hierarchical modeling technique to assess the reliability of a complex system comprised of multiple components by combining reliability information from various levels of a system which has been previously discussed as being problematic [12]. The goal of this technique is to improve model consistency at different levels of the reliability diagram by re-expressing non-terminal node probabilities in terms of probabilities using deterministic relations derived from the system reliability diagram [10]. Four sources of data are identified to accurately model the system using this methodology. The first source is data collected from actual component or subsystem tests and may generally take the form of binomial observations. The second type of data is expert opinion regarding the probability that a specific component or subsystem fails. A third, generally less precise source of information is expert opinion stating that a group of components in a given system or in related systems have similar failure probabilities. The authors stress the potential importance expert opinion can play in assessing the reliability of the system, particularly in large complex systems for which data collected on individual components may be sparse. However, as this type of data may be available from several experts where the quality of information from each expert may vary, the model assumes that this data take the form of a beta density function where prior information obtained from expert *m* concerning the lifetime distribution of certain component $C_i$ contributes a factor of

$$f_i(t_{im} \mid \Theta^i)^{N_m}$$

to the joint posterior density function. This expression represents the weight assigned to information collected from expert *m* including the number of observations assessed over the components lifetime distribution. For a non-redundant subset of system components, the information could then be defined to contribute a factor of

$$f_i(t_{im} \mid \Theta^i)^{N_m} = \left[ \sum_{j \in A_i} f_j(t) \prod_{\substack{k \neq j \\ k \in C_i}} (1 - F_k(t)) \right]^{N_m}$$

to the prior density of $\Theta$. This assumption allows the net contribution of expert opinion to take the form of a binomial likelihood function so that the aggregation of multiple opinions can be analytically handled as 'data' in a suitable format [10]. The final sources of data critical to model are the terminal node probabilities (components with no subcomponents). The combination of these sources of data leads to a joint posterior distribution which may be analyzed to determine an overall system reliability function [10]. It has been argued that the use of Bayesian hierarchical models may be unrealistic in problems where only partial information is available about the system behavior [23].

## 3. SYSTEMS THEORY AND CRITICAL INFRASTRUCTURE

A central tenet of systems theory is communication and control. Regulatory, or control action, is the imposition of constraints upon the activity at one level of a hierarchy which defines the "laws of behavior" at that level yielding activity meaningful at a higher level [21]. Hierarchies are characterized by control processes operating at the interfaces between levels. Control in open systems (those that have inputs and outputs from their environment) implies the need for communication. Closed systems, where unchanging components settle into a state of equilibrium can be distinguished from open systems which can be thrown out of equilibrium by exchanges with their environment. In systems theory, open systems are viewed as interrelated components that are kept in a state of dynamic equilibrium by feedback loops of

information and control [11]. Infrastructure systems, when viewed in this manner, can be treated as a dynamic process that are continually adapting to achieve its ends and to react to changes in itself and its environment.

Critical infrastructure networks can be described as complex systems spread across vast distances which are nonlinear and highly interactive. Each are composed of numerous cyber, physical, and organizational infrastructures subsystems, interconnected, and interdependent. The interrelation with other sectors constitutes a complex large-scale system of systems [7]. The relationships among these systems are dynamic, nonlinear and spatially distributed.

These systems of systems are complex in nature defined by the fact that no single centralized entity can evaluate, monitor, and manage all the interactions [2]. The relationships and interdependencies require complex mathematical theories and control methods often not representative of conventional methods. In reliability analysis of such complex systems, combinatorial models may be computationally efficient, but have limited expressive power. State-based models are expressive but computationally complex where the complexity increases exponentially with the size of the model [12]. It is in this regard that hierarchical reliability modeling may provide the ability to adequately design disaster tolerant infrastructure systems to provide better command and control capabilities including vulnerability assessment to protect against malicious attacks or forces of nature.

## 4. CONCLUSION

In studying large-scale systems with technological, societal, and environmental aspects, the efforts in the modeling as well as in the design and optimization are magnified and often overwhelm the analysis. This is due to the very large number of variables and complexity of the design models. Models must be built to address this complexity, but no single model can ever capture and represent all the essence of large-scale systems.

Hierarchical reliability for the design of disaster tolerant complex systems offers the ability to include diverse sources of information at different levels of the system and an ability to determine overall system reliability. In addition, traditional systems engineering techniques support the development of a coherent framework for incorporating multiple sources of non-terminal node probabilities using the structure of the system reliability block diagram and terminal node failure time distributions. Hierarchical reliability evaluation decomposes the overall model into a set of sub models where construction and generation of a large model is avoided and a solution can be obtained through interactions analysis among the sub models.

There is a strategic need to understand the societal consequences of infrastructure failure risks along with benefits of various tiers of increased reliability. From an infrastructure interdependency perspective, power, telecommunications, banking and finance, transportation and distribution, and other infrastructures' are becoming more and more congested and are increasingly vulnerable to failures cascading through and among them. A key concern is the avoidance of widespread failure due to these cascading and interactive effects. Moreover, interdependence is only one of several characteristics that challenge the control and reliable operation of these systems.

Dealing with system wide disruptions that may potentially result in infrastructure disasters sometimes requires diagnostic and corrective actions. In almost all cases, minimizing the loss of aggregate value to users and ensuring that it remains within a range required to safeguard the public interest is achieved only by taking a system-wide view coupled with disaster tolerance techniques and technologies.

## 5. ACKNOWLEDGEMENTS

The authors gratefully acknowledge the support from the Critical Infrastructure Protection Center (CIPC), SPAWAR Charleston for the research performed in this paper. Specifically, the authors would

like to acknowledge with thanks the assistance of John Linden, Becky Balon, and Richard P. Harper. The views and conclusions contained are those of the author and should not be interpreted as necessarily representing; either expressed or implied those of CIPC, SPAWAR Charleston, or the U.S. Government.

## 6. REFERENCES

[1] M. Amin. "Toward Self-Healing Energy Infrastructure Systems" IEEE Computer Applications in Power, January 2001, pgs 20-28.

[2] M. Amin, "National Infrastructures as Complex Interactive Networks", *Electric Power Research Institute. Automation, Control, and Complexity: An Integrated Approach*, Samad & Weyrauch (Eds.), John Wiley and Sons, pp. 263-286, 2000

[3] Billinton, R.; Satish, J.; Goel, L."Hierarchical Reliability Evaluation In An Electric Power System." Athens Power Tech, 1993. APT 93. Proceedings. Joint International Power Conference

[4] Executive Order *13010—Critical Infrastructure Protection*. Federal Register, July 17, 1996. Vol. 61, No. 138.

[5] F. Chang, M. Ji, S.T Leung, J. MackCormick, S. Perl, L. Zhang, "Myriad: Cost-effective Disaster Tolerance," Proceedings of the FAST 2002 Conference on File and Storage Technologies. USENIX Association. Monterey, California. January 28-30, 2002.

[6] Haimes, Yacov Y., Kyosti Tarvainen, Takashi Shima, and Jacob Thadathil, *Hierarchical Multiobjective Analysis of Large-Scale Systems.* New York: Hemisphere Publishing Corporation, 1990.

[7] Haimes Yacov Y. "Roadmap for Modeling Risks of Terrorism to the Homeland." Journal of Infrastructure Systems, June 2002.

[8] Hein Axel, Dal Cin Mario. "Performance and dependability evaluation of scalable massively parallel computer systems with conjoint simulation." ACM Transactions on Modeling and Computer Simulation. VOL. 8 Issue 4. ACM Press. October 1998.

[9] "Improving system availability with storage area networks," Barocade Communications Systems, Incorporated, 2001.

[10] Kubiatowicz John. "Extracting Guarantees from Chaos." Commutations of the ACM. February 2003 Vol. 46. No2. pg 33-38.

[11] Lanus Mark, Yin Liang, Trivedi Kishor S. "Hierarchical Composition and Aggregation of State-Based Availability and Performability Models." IEEE Transactions on Reliability, VOL. 52, NO.1, March 2003

[12] Ledlie Jonathan, Taylor Jacob M., Serban Laura, Seltzer. "Self-Organization in Peer-to-Peer Systems" Margo Division of Engineering and Applied Science. Harvard University SIGOPS 2002.

[13] H. F. Lipson and D. A. Fisher, "Survivability-A New Technical and Business Perspective on Security," *Proceedings of the New Security Paradigms Workshop*, September 21-24, Association for Computing Machinery, 1999.

[14] K. Parris, "Disaster Tolerant Cluster Technology and Implementation", HP World 2003 Solutions and Technology Conference and Expo, 2003.

[15] "Integrating Availability and Disaster Tolerance" 1999; Strategic Research Corporation.

[16] Longstaff, Thomas A, Clyde Chittister, Rich Pethia, and Yacov Y. Haimes. "Risk and complexity of information-based interconnected telecommunications infrastructure." *Software,* IEEE, 2000.

[17] Nitin H. Vaidya, "A Case for Two-Level Recovery Schemes," *IEEE Transactions on Computers*, vol. 47, no. 6, pp. 656-666, Jun., 1998.

[18] Reese C. Shane, Johnson Valen E., Hamada Michael, Wilson Alyson. "A Hierarchical Model for the Reliability of an Anti-aircraft Missile System." University of Texas, MD Anderson Cancer Center UT MD Anderson Cancer Center Department of Biostatistics and Applied Mathematics Working Paper Series, 2005.

[19] Rykov Vladimir, Dimitrov Boyan, Green David, Jr., Stanchev Peter. "Reliability of Complex Hierarchical Systems with Fault Tolerance Units" (accepted for publication in *Proceedings MMR-2004.* Santa Fe (U.S.A.) June, 2004.)

[20] Sahner Robin A., Trivedi Kishor S. "A Hierarchical, Combinatorial-Markov Method of Solving Complex Reliability Models." Proceedings of 1986 ACM Fall Joint Computer Conference. IEEE Computer Society Pres. November 1986.

[21] Sharma Nita, Agrawal Dharma P. "Hierarchical Reliability Evaluation of Large Networks." Parallel and Distributed Processing, 1991. Proceedings of the Third IEEE Symposium on pgs 444-451

[22] Sheldon Frederick, Potok Tom, Loebl Andy **"**Managing Secure Survivable Critical Infrastructures to Avoid Vulnerabilities" *Applied Software Engineering Researc*

[23] Shieh, Y.-B. Ghosal, D. Chintamaneni, P.R. Tripathi, S.K. "Modeling of Hierarchical Distributed Systems with Fault-Tolerance" IEEE Transactions on Software Engineering. April 1990 Vol 16, Issue: 4. pg 444-457.