December 2003

Holistic Evaluation of Real-Time Safety-Critical Large-Scale Networks

Tuncay Bayrak
Western New England College

Martha Grabowski
Rensselaer Polytechnic Institute/LeMoyne College

HOLISTIC EVALUATION OF REAL-TIME SAFETY-CRITICAL LARGE-SCALE NETWORKS

Tuncay Bayrak
Western New England College
tbayrak@wnec.edu

Martha Grabowski
Rensselaer Polytechnic Institute/
LeMoyne College
grabowsk@mail.lemoyne.edu

Abstract

The growing importance of real-time computing in numerous applications poses problems for network architectures. This research proposes a model for evaluating safety-critical real-time Wide Area Networks (WANs), using assessment and performance requirements for highly reliably and dependable real-time networks, incorporating both human and technical performance criteria.

Keywords: Computer networks, safety-critical systems, service systems, wide area networks

Research Objectives

Designing, building and evaluating large-scale networks that are always available is a complex, multidimensional problem. In this context, WANs pose significant performance analysis challenges. First, the execution environment of geographically distributed wide are networks is far less deterministic than those of locally distributed small-scale networks. Second, large-scale networks, which contain hundreds of nodes, are highly complex [Shaffer, et al., 1999].

There has been a considerable amount of research in the area of network performance evaluation. However, although much network evaluation research has been undertaken [Banerjee, et al., 1997], [Niehaus et al., 1997], [DaSilva, et al., 1997], [Higginbottom, 1998], [Havercort, 1998] little of the research focused on the evaluation of real-time safety-critical WANs. Examples of such safety-critical wide area networks include intelligent transportation systems (Andrisano et al., 2000), distributed health care networks (Yamamoto et al., 2000), global oil and gas exploration and research networks (MacIntyre, 1999), and aviation traffic monitoring systems (Cheng et al., 2000).

Most large-scale networks depend on hardware, software, and human operators to function correctly. Failure of any of the network elements can bring the entire network down and in safety-critical settings, the consequences can be disastrous. A well-known example of such failure is the 1990 nationwide AT&T network failure (Kuhn, 1997). This example is not an isolated one: according to the Federal Communication Commission (FCC), network failures in the United States with impact on more than 30,000 customers happen on the order of one every two days and the mean time to repair them is on the order of five to 10 hours (Demeester, et al., 1999).

A combination of quantitative assessments of a network and qualitative measurements of operators' performance with a network is important for understanding relationships between operators and networks and the impact of both on organizational performance; such an approach is presented by this research.

Performance Evaluation of Real-Time Safety-Critical WANs

Wide Are Networks are complex large-scale systems. Wang & Pham (1997) argue that usually there are four main difficulties in evaluating complex large-scale system reliability, availability and Mean Time Between Failure (MTBF): the system structure

may be very complex, subsystems may follow various failure distributions, the failure data of subsystems are not sufficient, and finally, subsystems may follow arbitrary failure and repair distributions for repairable systems.

In addition to the well-defined metrics such as response time, throughput, and latency that are used to evaluate networks, Kirner (1997) focuses on six essential quality requirements for real-time safety-critical systems, which are timing, reliability, safety, security, usability, and maintainability.

Timing requirements are essential for real-time safety-critical systems because failure to meet timing constraints in such applications can lead to intolerable system degradation and, in some cases, result in catastrophic loss of life, environment, and property [Kirner and Davis, 1996a]. Real-time safety-critical systems are subject to unexpected and unpredictable conditions and circumstances that negatively interfere with their behavior, leading to failure, faults, hazards, and accidents [Kirner and Davis, 1996b]. Failure is a deviation in the expected system behavior. A fault is a causative agent for failure. A hazard is a condition resulting from failure, and an accident is a hazard that results in unacceptable loss or damage of life, environment, or property [Kirner and Davis, 1996b].

In order to achieve high integrity levels in complex, real-time, safety-critical systems, it is necessary to detect failures and take appropriate fault recovery action, to maintain safe system operation or fail to a safe state [Johnson, 1996a]. Safety-critical systems tend to have reliability requirements ranging from 10^{-5} to 10^{-9} over a given time period [Leveson, 1994]. Achievement of this requires the use of redundancy, the detection of failures with very low probabilities of occurrence, and often immediate response to the detection of a failure [Johnson, 1996a]. One of the most important considerations associated with designing safety-critical networks is redundancy. All safety–critical systems rely on some form of redundancy, be it time, data, algorithmic, or structural (hardware or software) [Profeta III, et al, 1996].

Safety is defined as freedom from those conditions that can cause death, injury, occupational illness, or damage to or loss of equipment or property [Leveson, 1994]. Safety is a system property, not a component property [Leveson et al, 1997]. While reliability engineering concentrates on component failure accidents, system safety deals with a broader class of accidents including both component failure and system accidents [Leveson, 2000], which may arise in the interactions among components rather than the failure of individual components [Perrow, 1984]. Safety is often confused with reliability. Leveson (1994) discusses the interrelationship between safety and reliability. In general, reliability requirements are concerned with a system failure free, whereas safety requirements are concerned with making it mishap free. Kirner (1997) argues that a system can be reliable but not safe, a system can be both safe and reliable, and a system can be both unsafe and unreliable.

A system is secure if it has the ability to detect, protect itself, and recover from possible inappropriate access involving one or more of its components, including physical facilities, hardware, software, interfaces, and data [Sennet, 1991]. Varadharajana and Katsavosa (1997) argue that the fundamental questions that we need to consider when addressing security in high speed WANs are: a) What are the security threats in the network environment? b) What are the required services and mechanisms? c) Where should these services and mechanisms be provided in the protocol stack? and d) How are they to be managed? They outline different types of security threats, including unauthorized disclosure of information, unauthorized modification of information, masquerading attack, unauthorized access to network resources and services, unauthorized denial of service, and repudiation.
A system is usable if it has appropriate user interface [Day and Boyce, 1993]. Usability is important for real-time safety-critical systems because poorly designed human computer interfaces may cause system failures. Mayhew (1999) lists the benefits of usability to users, including increased productivity, decreased user training time and cost, decreased user errors, increased accuracy of data input and data interpretation, and decreased need for ongoing technical support.

Maintainability is defined as a measure of the ease and rapidity with which a system or equipment can be restored to operational status following a failure **[http://www.hq.nasa.gov/office/codeq/mtecpage/pm1.pdf]**[10/05/2000].

The metric Mean Time To Repair (MTTR), defined as the average time necessary to troubleshoot, remove, repair, and replace a failed system component, is often utilized in maintainability measurement. [www.hq.nasa.gov/office/codeq/mtecpage/at2.pdf] [10/05/2000].

Theoretical Model

In safety-critical settings, where network failures can have catastrophic effects and networks provide an important social and technical infrastructure, utilizing performance criteria that reflect the differing requirements that such networks must meet is

important [So and Durfee 1996]. For instance, real-time safety-critical WAN's must meet stringent response, availability, reliability and accuracy; thus, use of technical performance criteria can provide some measure of the network's ability to meet those requirements. Similarly, real-time WAN's in safety-critical settings must also meet critical communication, decision-making, problem-solving and organizational effectiveness requirements; as a result, social, psychological and organizational network performance criteria can also be used to measure the social and organizational effectiveness of the network infrastructure. Finally, in many cases, real-time WAN's in safety-critical settings must also satisfy demanding commercial and economic requirements, as befitting their industrial hosts. Thus, commercial and economic performance criteria can provide measures of the network's ability to satisfy its economic and resource requirements. These requirements suggest important performance criteria for use in evaluating real-time WAN's in safety-critical settings. In such evaluations, technical, social, organizational, psychological, commercial and economic evaluation criteria provide a means of measuring the performance of the network, and of addressing the social, technical and economic challenges faced by real-time WAN's.

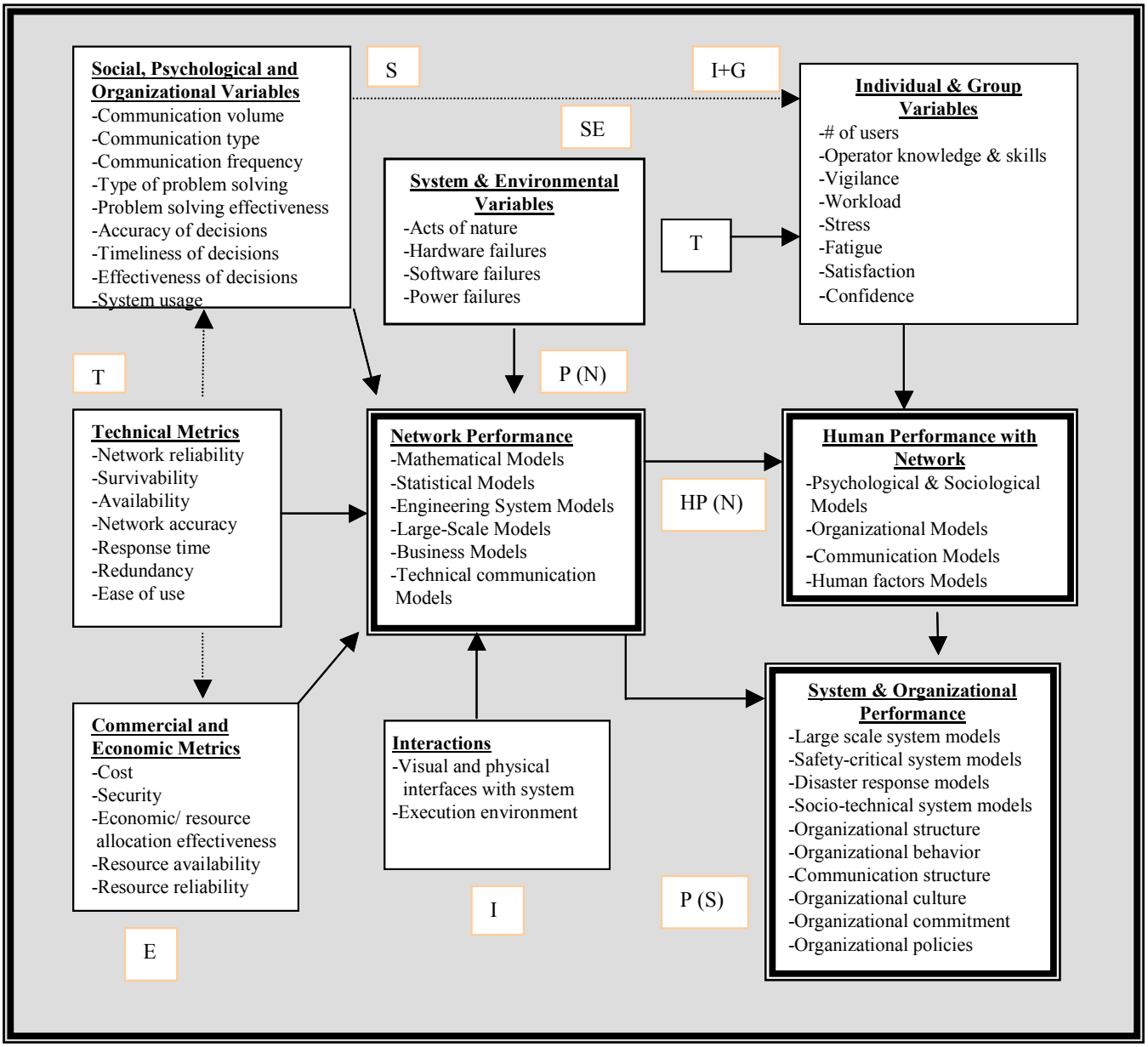

Figure 1. Real-Time Safety-Critical WAN Evaluation Model

Figure 1 illustrates the proposed evaluation approach. Three types of performance are of interest in evaluating WANs in real-time safety-critical settings: the performance of the network P (N); the human performance of those using the network HP (N); and the performance of the system and organization P (S), as seen in Figure (1).

As discussed earlier, real-time networks interact with humans, the environment, and other technologies, and interactions between these different elements may contribute to network failures. Hence, in addition to traditional technical performance considerations, the proposed model of WAN evaluation deems human factor and environmental considerations crucial in evaluation studies. This is because human error and acts of nature are among the major sources of failures in networks (Kuhn 1997).

Technical variables (T), such as network reliability, response time and utilization, certainly impact network performance P (N), as do social, psychological and organizational variables (S), commercial and economic variables (E), or system and environmental variables (SE) such as hardware failures and software failures, and interactions (I_N) between the network and its working environment (Figure 1). Note that in Figure 1, technical variables (T) also influence commercial and economic variables such as cost and social, psychological and organizational variables (S), such as accuracy, communication and system usage. These are indirect effects on network performance P (N), and the impact vectors in Figure 1 for these variables are shown as dotted lines.

In turn, network performance P (N) influences human performance with the network HP (N) as well as the performance of the system that the network serves P (S). Individual (I_H) and group (G) variables such as vigilance and workload, also influence human performance with the network HP (N), as seen in Figure 1.

Finally, overall system performance for the systems that host real-time WANs is influenced by the performance of a network P(N) as well as by human performance with the network HP(N).

The model posed also fits with Checkland's (2002) well-established systemic framework, which proposes 5E's that stands for: efficiency, efficacy, effectiveness, ethics and aEsthetic.

Research Methodology

Research Setting and Subjects

To evaluate the Figure 1 model, an empirical evaluation of the proposed model was undertaken. The research setting was a 24 x 7 network operations center where several real-time safety-critical wide area networks are monitored and maintained. The real-time WAN under study is the Continuous Operational Real-Time Monitoring System (CORMS), which was designed and built by the U.S. National Oceanic and Atmospheric Administration (NOAA). CORMS's purpose is to provide a 24 hour/day monitoring and quality control of water level and meteorological data from around the US to ensure the availability and accuracy of tide and water current observations that are used for navigation and safety of life and property decisions. CORMS is monitored in 24 hour/7 day mode by 6 watchstanding operators who monitor CORMS and determine what actions are necessary if the accuracy of any of the measured parameters is deemed to be questionable (NOAA, 1999).

Since there are three types of performance evaluations proposed by the model, there are three sets of subjects for this research: the CORMS wide area network for the network performance evaluation, the operators who monitor and utilize the network for the human performance evaluation, and the host organization (NOAA) for the system performance evaluation.

Procedure

The network, operator and system performance hypotheses tested in this research are listed in Table 1. The hypotheses, variables, their operationalizations and measurements are listed in Table 2. Network, operator and system performance were evaluated by utilizing well-defined and well-known metrics. The appropriate statistical tests and mathematical analyses were run on collected data, and the results of the mathematical analyses and statistical tests were used to evaluate the hypotheses.

Table 1. Hypotheses

Hypothesis	Description
Network Performance Hypotheses	
H1	Increased use of a real-time WAN will be associated with decreased network reliability, decreased network accuracy, and increased network response time.
H2	Increased network redundancy will be associated with increased network workload, increased cost, increased usage, and increased network reliability.
Operator Performance Hypotheses	
H3	Decreased network reliability will be associated with decreased operator satisfaction, decreased operator confidence, and increased operator workload.
H4	Increased network usage will be associated with decreased operator vigilance.
H5	An increased number of tasks processed in a real-time network will be associated with decreased operator accuracy, decreased operator reliability, and decreased operator communication.
H6	Decreases in operator performance will be associated with decreases in network reliability.
System Performance Hypothesis	
H7	Changes in user perceptions of a network's contribution to organizational success will be associated with changes in network reliability.

Table 2. Hypotheses, Dependent Variables, Operationalizations, and Metrics

Hypothesis	Dependent Variable	Variable Operationalization	Measurement
a. Network Performance Hypotheses			
1a: Increased use of a real-time WAN will be associated with decreased network reliability.	Network reliability	1) Type, and time of breakdowns	1) MTBF, MTTR, Availability (%).
1b: Increased use of a real-time WAN will be associated with decreased network accuracy.	Network accuracy	2) Correctness of data	2) Probability of detecting error.
1c: Increased use of real-time WAN will be associated with increased network response time.	Network response time	3) Time taken to obtain response	3) Mean response time.
2a: Increased network redundancy will be associated with increased network workload.	Network workload	1) How much traffic is flowing from a given source to a given destination network	1) Flow volume in bytes.
2b: Increased network redundancy will be associated with increased network usage.	Network usage	2) Level of system use	2) Frequency of network use by an operator.
2c: Increased network redundancy will be associated with increased network reliability.	Network reliability	3) Type, and time of breakdowns	3) MTBF, MTTR, Availability (%).

Hypothesis	Dependent Variable	Variable Operationalization	Measurement
b. Operator Performance Hypotheses			
3a: Decreased network reliability will be associated with decreased operator satisfaction.	Operator satisfaction	1) Operator satisfaction with network performance.	1) User satisfaction survey questions
3b: Decreased network reliability will be associated with decreased operator confidence.	Operator confidence level	2) Operator confidence in network performance.	2) User confidence survey questions
3c: Decreased network reliability will be associated with increased operator workload.	Operator workload	3) Operator workload.	3) NASA Task Load Index (TLX)
4: Increased network usage will be associated with decreased operator vigilance.	Operator vigilance	1) Monitoring performance change over time	1) Stanford Sleepiness Scale (SSS)
5a: An increased number of tasks processed in a real-time network will be associated with decreased operator accuracy.	Operator accuracy	1) Operator assessment of accuracy, supervisor assessment of accuracy	1) The number of tasks executed successfully per unit time.
5b: An increased number of tasks processed in a real-time network will be associated with decreased operator reliability.	Operator reliability	2) Operator error rate	2) Expert review of # of errors committed.
5c: An increased number of tasks processed in a real-time network will be associated with decreased operator communication.	Operator communication	3) Operator-Supervisor communication.	3) Number, type, frequency of operator communications.
6: Decreases in operator performance will be associated with decreases in network reliability.	Operator performance	1) Operator error rate 2) Task completion time 3) Task volume completed	1) Number of errors made in one shift, Expert review 2) Time it takes an operator to complete a task. 3) Number of tasks completed per unit time.
c. System Performance Hypothesis			
7: Changes in user perceptions of a network's contribution to organizational success will be associated with changes in network reliability.	Organizational performance Organizational efficiency Organizational effectiveness	1) Achieved system objectives 2) Increasing work satisfaction 3) Impact on operational coordination	1) User Survey 2) Opinion scale

A Mapping Between the Hypotheses and the Six Kirner 1997 Metrics and the Checkland Five E Metrics

In addition to the types of metrics proposed by the Kirner (1997) and Checkland (2002) models, the model incorporates several other disciplines en route to a holistic evaluation model. Table 3 shows the interrelationships and a mapping between the hypotheses and the 6 Kirner (1997) metrics, and the Checkland 5 E metrics. Both models provide essential metrics to be heeded in evaluating complex large-scale information systems.

Because humans and technology cooperatively perform tasks in network-centered safety-critical large-scale systems in the real world, the proposed model encompasses both social and technical dimensions. This study provides an example of how those dimensions might be operationalized in metrics and measurements. Data was gathered from the research sponsor for this study based on the metrics and measurements listed in Table 2. The research thus provides an example of how the theoretical research model might be operationalized by LAN and WAN managers. A presentation of the results of the data analysis will be available at the conference.

Table 3. A Mapping between the Hypotheses and the Six Kirner 1997 Metrics and the Checkland Five E Metrics

Hypothesis #	Description	Kirner Metric	Checkland Metric
H1	Increased use of a real-time WAN will be associated with decreased network reliability, decreased network accuracy, and increased network response time.	Reliability, Security, Timing	Effectiveness
H2	Increased network redundancy will be associated with increased network workload, increased cost, increased usage, and increased network reliability.	Reliability, Maintainability	Effectiveness
H3	Decreased network reliability will be associated with decreased operator satisfaction, decreased operator confidence, and increased operator workload.	Usability	Efficiency, Effectiveness
H4	Increased network usage will be associated with decreased operator vigilance.	Usability	Efficiency, Effectiveness
H5	An increased number of tasks processed in a real-time network will be associated with decreased operator accuracy, decreased operator reliability, and decreased operator communication.	Usability	Efficiency, Effectiveness
H6	Decreases in operator performance will be associated with decreases in network reliability.	Usability, Reliability	Efficiency, Effectiveness
H7	Changes in user perceptions of a network's contribution to organizational success will be associated with changes in network reliability.	Reliability	Efficacy, aEsthetic

Current Status

The literature review is concluded, and the proposed model, hypotheses, dependent variables, and their operationalizations to evaluate subjects have been defined. Data analysis is complete and results will be available for conference presentation.

References

Andrisano, O., Verdone, R., and Nakagawa, M. Intelligent Transportation Systems: The Role of Third-Generation Mobile Radio Networks, *IEEE Communications Magazine,* (38:9), 2000, pp.144-151.

Banerjee, S., Tipper, D., Weiss, B.H.M., and Kahlil, A. Traffic Experiments on the vBNS Wide Area ATM Network, *IEEE Communications Magazine*, (35:8), 1997, pp.126-133.

Cheng, A. Y., Liu, R. Y., and Luxhoj, J. T. Monitoring Multivariate Aviation Safety Data by Data Depth: Control Charts and Threshold Systems. *IIE Transactions*, (32:9), 2000, pp.861-872.

DaSilva, L. A., Evans, J.B., Niehaus, D., Frost, V. S., Jonkman, R., Beng O. L., Lazarou, G.Y. ATM WAN Performance Tools, Experiments, and Results, *IEEE Communications Magazine*, (35:8), 1997, pp.118-124.

Day, C. M., and Boyce, J. S. "Human Factors in Human-Computer System Design," *Advances in Computers*, Vol.36, pp.333-

Demeester, P., Wu, T., and Yoshikai, N. Survivable Communication Networks, *IEEE Communications Magazine*, (37:8), 1999, pp.40-42.

Haverkort, B, R. *Performance of Communication Systems, A Model-Based Approach*, Wiley, Chichester, NY, 1998.

Higginbottom, G.N. *Performance Evaluation of Communication Networks*, Artech House, Boston., 1998.

Johnson, M. D. "A Review of Fault Management Techniques Used in Safety Critical Avionic Systems," *Progress in Aerospace Sciences*, Vol.32, 1996a, pp.415-431.

Kirner, G, T. "Quality Requirements for Real-Time Safety Critical Systems," *Control Engineering Practices*, (5:7), 1997, pp.965-973.

Kirner, G. T., and Davis, M. A. "Requirements Specification of Real-Time Systems: Temporal Parameters and Timing-Constraints," *Information and Software Technology*, Vol.38, 1996a, pp.735-741.

Kirner, G. T., and Davis, M. A. "Nonfuntional Requirements of Real Time Systems," *Advances in Computers*, Vol.42, 1996b, pp.1-37.

Leveson, N. G. *Safety, Encyclopedia of Software Engineering*, (J. Marciniak, Ed) Vol.2, Wiley & Sons, 1994, pp.1108-1133

Leveson, N.G. *System Safety in Computer-Controlled Automotive Systems*, SAE Congress, March, 2000.

Leveson, N., L. Alfaro, C. Alvarado, M. Brown, E.B. Hunt, M. Jaffe, S. Joslyn, D. Pinnel, J. Reese, J. Samarziya, S. Sandys, A. Shaw, Z. Zabinsky. Presented at the Software Engineering Laboratory Workshop, NASA Goddard, December 1997.

Kuhn, R. D. Sources of Failure in the Public Switched Telephone Network, *IEEE Computer*, (30:8), 1997, pp.31-36.

MacIntyre, H. Linking Up to the Behemoth." *Mobile Radio Technology*, (17:3), 1999, pp.37-9.

Mayhew, J. D., *The usability Engineering Lifecycle*, Morgan Kaufmann Publishers Inc, 1999.

National Oceanographic and Atmospheric Administration (NOAA). Center for Operational Oceanic Products and Services (CO-OPS), Silver Spring, Maryland, 1999.

Niehaus, D., Battou, A., McFarland, A., Decina, B., Dardy, H., Sirkay, V., and Edwards, B. Performance Benchmarking of Signaling in ATM Networks, *IEEE Communications Magazine*, (35:8), 1997, pp.134-142.

Perrow, C. *Normal Accidents: Living with High-Risk Technologies*, Basic Books, NY, 1984.

Profeta III, A. J., Andrianos, P. N., Yu, B., Johnson, W. B., DeLong, A. Todd., Guaspari, D., and Jamsek , D. "Safety-Critical Systems Built with COTS," *Computer*, (29:11), pp.54-60.

Sennet, T. C. *Computer Security, Software Engineer's Reference book* (edited by John A. McDermid), Butterworth-Heinemann, 1991

Shaffer, E., Reed, A.D., Whitmore, S., and Shaffer, B. "Virtue: Performance Visualization of Parallel and Distributed Applications, *Computer*, (66:12), 1999, pp.44-51.

Varadharajana, V., and Katsavosa. P. "High-Speed Network Security. I. SMDS and Frame Relay," *Computer Communications*, (20:10), 1997, pp. 832-847.

Wang, H., and Pham, H. "Survey of Reliability and Availability Evaluation of Complex Networks Using Monte Carlo Techniques," *Microelectronic Reliability*, (37:2), 1997, pp.187-209

Yamamoto, K., Takada, T., Nakai, K., and Nagaoka, H. Structuring WAN and LAN for EPR Use in Community Health Care, *International Journal of Medical Informatics*, (60:2), 2000, pp.219-226.