COMBAT INFORMATION TRANSPORT SYSTEM RELIABILITY AND AVAILABILITY PERFORMANCE

Mitchell J. Mondro

The MITRE Corporation
Reliability and Maintainability Center
Bedford, Massachusetts

ABSTRACT

This paper describes the network modeling techniques that were developed to assess the reliability and availability performance of the Combat Information Transport System (CITS). CITS is the backbone network that provides high-capacity transport of data, voice, and video for all active duty and reserve Air Force bases. The model includes the network topology, the configuration and interconnection of network hardware, reliability and maintainability design predictions for all network hardware, and the expected network operational maintenance and sparing policies. The model provides an estimate of the mean time between critical failure (MTBCF), mean time between corrective maintenance action (MTBCMA), and availability performance of the CITS network. In addition, this paper describes how this modeling effort impacted the network design process and provides a summary of lessons learned. Finally, this paper will address simulation-based modeling efforts that are being developed, and how these can be used to enhance reliability and availability performance for highly-fault tolerant networks such as CITS.

INTRODUCTION

There have been many studies of communication and computer network reliability and availability performance [1-5]. These studies present a number of different modeling techniques. One reason that there are many different approaches to network reliability and availability modeling is that a critical failure can be defined in a number of different ways. For example, a failure can be defined as the loss of a communication path between two nodes or users of the network. Another way to define a network failure is the loss of a communication path from one user to many other users. These models were studied to determine which might be used to evaluate the reliability and availability performance of the Combat Information Transport System (CITS). For CITS, a critical failure occurs when a certain percentage of all users of the network cannot communicate with the majority of other users of the network. Unfortunately, due to this definition of critical failure, none of the most common network modeling techniques were appropriate. This paper will provide the methodology that was developed to support the CITS program.

The CITS program will ensure that every active duty and reserve Air Force base has an information transport system that will link existing and future voice, data, and video via a high capacity transport media. CITS includes an information transport system (ITS), voice switching system, telecommunications management system, and network management system base information protection. The reliability and availability analysis focuses on the ITS only. The ITS consists of a base-wide integrated backbone transport network (switches, cable, and other transmission equipment), the links from the backbone to specific end buildings that contain network users (i.e., computers, workstations), interfaces to external and internal networks, and components required to integrate the various transport services. It is typically a partially-meshed network of ATM switches, Ethernet or ATM uplinks, with transport rates of OC-12 (622Mbps) or OC-3 (155Mbps) over single mode fiber optic cables. For simplicity, the ITS will be referred to as CITS throughout this paper.

An important outcome of the modeling process is the identification of potential weaknesses in the design that may hamper reliability and availability performance, or areas of costly "over-design" (e.g., excessive redundancy and increased total ownership cost). This paper will highlight how information gathered as a result of the modeling process was used to impact the network design and ensure that the reliability and availability requirements were achieved in a cost-effective manner. Also, it will summarize the most important lessons learned and how these lessons are being applied to enhance reliability and availability performance for highly-fault tolerant networks such as CITS. Finally, this paper will address simulation-based modeling efforts that are being developed, and how these can be used to improve future CITS modeling efforts.

DEFINITIONS AND REQUIREMENTS

The model measures three reliability and availability performance metrics: operational availability (A_o), mean time between critical failure (MTBCF), and mean time between corrective maintenance action (MTBCMA).

A_o is the probability that the network is up (i.e., does not meet the critical failure criteria) at any random point in time. It only includes downtime due to unscheduled maintenance. While not specifically required, the model was also designed to include downtime due to administrative and logistics delay time (ALDT).

MTBCF is the average time between unscheduled corrective maintenance actions that meet the criterion of a critical failure. A critical failure is any failure that causes the network to lose a predetermined level of capability.

MTBCMA is the average time between unscheduled corrective maintenance actions. It provides a measure of the amount of maintenance and spares that are needed to support the network.

The reliability and availability requirements for the CITS program are the following:

- The availability shall be greater than 0.9999. The network is considered unavailable when 20 percent of the users cannot communicate with the majority of the other users of the network.

- The mean time between critical failure (MTBCF) shall be greater than 50,000 hours. A critical failure occurs when 20 percent of the users cannot communicate with a majority of the other users of the network.

- There is no requirement for MTBCMA.

While the analysis evaluated each of these parameters, this paper will focus on the methodology developed to evaluate the CITS network availability performance. A similar technique was used to evaluate MTBCF. MTBCMA was estimated using a series reliability model.

Before describing the availability modeling technique, an example of a typical CITS network topology is provided (Figure 1).

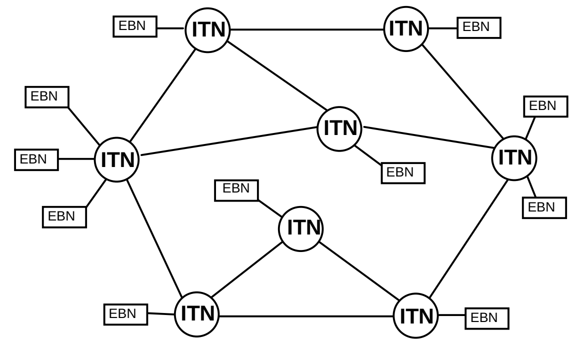

Figure 1. Notional CITS Network Topology

Each of the nodes of the network is called an information transport node (ITN). Each ITN may contain many different types of network equipment (e.g., routers, ATM-switches, Ethernet switches). While the quantity, types, and interconnection of equipment differ for each ITN, the functions performed within each ITN are similar (figure 2).

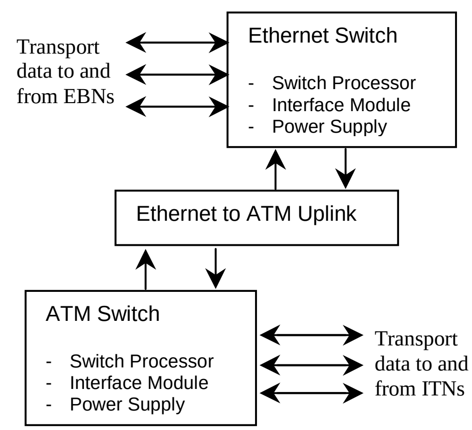

Figure 2. Typical Functions of an ITN

Each end building node (EBN) is connected to the CITS network through an ITN. The users, who reside within the EBNs, gain access to CITS through the LAN networking equipment within the EBN. However, the edge of the CITS network is defined as the equipment within the EBN that is needed to interface with CITS. Therefore, the model does not include the LAN networking equipment needed to link the users to the CITS interface or the user's equipment (e.g. workstation).

MODELING TECHNIQUE

For this analysis, there were several reliability modeling techniques that were considered; these included reliability block diagrams, Markov modeling, simulation, and common network reliability analysis techniques. None of these techniques were found to be appropriate due to the significant complexity of the network combined with the unique definition of a critical failure. Therefore, it was necessary to develop an ad hoc technique based upon common reliability and probability theory.

Assumptions were needed to bound the scope of the analysis. The following is a list of the major assumptions:

- The model is limited to equipment that is replaceable upon failure. The most common replaceable items are at the module-level within the ITN switch, but box-level items (i.e., multiple modules) are sometimes included as well. No components-level or piece parts will be replaced on CITS.
- All failures are catastrophic; that is, equipment cannot partially fail (i.e., interface modules lose only one port). This is reasonable since even if only one function failed, the subsequent repair would require the entire module to be taken offline.
- Every user of the network has equal importance. That is, no user is considered more critical than another user.
- Each repairable item in an ITN has an exponential time to failure distribution with a constant failure rate.
- Each repairable item in an ITN has an exponential time to repair distribution with a constant repair rate.
- There is perfect switching between redundant items upon failure - that is, the probability that a redundant item takes over for a failed item is 100 percent.
- Software reliability was not included.
- Sufficient personnel would be available to perform any unscheduled maintenance activity.
- Preventative maintenance (PM) is assumed to cause negligible downtime.

The modeling process consists of three primary steps:

1. Estimate the availability performance of each repairable item within the ITN.

2. Identify each possible operational state of the ITN and quantify the probability of being in each state at any random point in time. The operational state is the number of users attached to that ITN that lose connectivity to the network when an item or multiple items within the ITN fail.

3. Combine the data for each ITN to identify all operational states of the network and quantify the probability of being in each state at any random point in time.

Step 1. Item Availability Analysis

The modeling process begins by estimating the reliability (i.e., MTBCMA) of each item within the ITN equipment that are designated as replaceable upon failure per the maintenance policy. Next, the maintainability performance, or mean time to repair (MTTR), of each item is estimated. Then, the ALDT is estimated based upon the expected maintenance and sparing policy. The mean down time (MDT) for each item is calculated by adding the MTTR and ALDT. These MTBCMA and MDT data are applied to equation (1) to find the availability performance of each item in the network.

$$Availability_{item} = \frac{MTBCMA_{item}}{MTBCMA_{item} + MDT_{item}} \quad (1)$$

Sources of MTBCMA and MTTR data include the equipment vendors and experience with similar technology equipment. The ALDT is a function of the maintenance policy and is typically in the range of 0 to 72 hours.

Step 2. ITN Availability Analysis

At any random point in time, the operational state of each repairable item is either "up" (i.e., available) or "down" (i.e., failed or unavailable). The probability of an item being in the "up" state is equal to the $Availability_{item}$; the probability of that item being in the "down" state is one minus the $Availability_{item}$.

Assuming that the operational state of an item is independent of the other items in the ITN, the probability of any one combination of item states is the product of all item state probabilities (i.e., up or down), as shown by equation (2).

$$P_{ITN_i} = \prod_{item=1}^{n} P_{item_{state}} \qquad (2)$$

where,

P_{ITN_i} = The probability of being in the i^{th} combination of item operational states.

$P_{item_{state}}$ = The probability that an item is in a particular operational state (i.e., up or down).

For an ITN that contains n repairable items, there are 2^n combinations of all item operational states. Therefore, equation (2) is calculated 2^n times for each ITN. The result is a table of that identifies the operational state of the network and the probability that the network is in that state.

The number of users unable to connect to the network is a function of the ITN operational state. Two or more ITN operational states may have the same impact on the users. For example, lets assume that two ITN operational states have the same impact–k users lose connectivity to the network. Then, the probability that an ITN is in an operational state that loses k users at any random point in time is found by adding the probabilities for both ITN states that lose k users. This concept is shown by equation (3) in general form.

$$P_{ITN_k} = \sum P_{ITN_i} \qquad (3)$$

(for all ITN states that lose k users)

where,

P_{ITN_k} = The probability of being in an ITN operational states that cause k users to lose connectivity to the network.

This process is repeated for all possible combinations of users that lose connectivity to the network. Therefore, for each ITN there is an operational state defined as the number of users lost and the probability that the ITN is in that state. These calculations are made for each ITN.

Step 3. Network Availability Analysis

The network availability analysis is an extension of the concepts provided in the previous step. An operational state of the network is defined as m users losing connectivity to the network. The probability of any one combination of ITN states is the product of one ITN state probability from each ITN, as shown by equation (4).

$$P_{Network_j} = \prod_{i=1}^{r} P_{ITN_i} \qquad (4)$$

where,

$P_{Network_j}$ = The probability of being in the j^{th} combination of ITN operational states.

P_{ITN_i} = The probability that an ITN is in a particular operational state.

r = number of ITNs in the network

The number of users impacted for each network operational state is assigned by adding all of the users lost from each ITN operational state. Adjustments to this user count are made to account for dependencies between ITNs. Two or more network operational states may result in the loss of the same number of users. In this case, similar to step 2, these probabilities are added. The general form is shown in equation (5).

$$P_{Network_m} = \sum P_{Network_j} \qquad (5)$$

(for all states that lose m users)

where,

$P_{Network_m}$ = The probability of being in a network operational states that cause m users to lose connectivity to the network.

This process is repeated for all possible combinations of users that lose connectivity to the network. At the completion of this process, there is a network operational state defined as the number of users lost and the corresponding probability that the network is in that state at any random point in time.

Network availability, A_o, is the probability that the network is up (i.e., does not meet the critical failure criteria) at any random point in time. As long as the network is in an operational state where less than 20 percent of all network users lose connectivity to the network, the network is available or up. Therefore, A_o is the addition of all probabilities for operational states that are less than 20 percent of users down, as shown in equation (6).

$$A_o = \sum P_{Network_m} \qquad (6)$$

(as long as m is less than 20 percent of all users)

Due to the uncertainty inherent in any prediction of future performance, a sensitivity analysis was always performed using various levels of predicted item MTBCMA, MTTR, and ALDT. These results were considered when developing the final assessment of A_o.

PERFORMANCE

The methodology described in the previous section has been performed for seven bases. Table 1 provides a summary of the results for all final designs.

Base	A_o	MTBCF (hours)	MTBCMA (hours)
Requirement	0.99990	50,000	N/A
A	0.99999	>1,000,000	340
B	0.99991	60,000	820
C	0.99996	750,000	450
D	0.99998	75,000	850
E	0.99995	255,000	1,300
F	0.99999	>1,000,000	460
G	0.99999	>1,000,000	478

Table 1. CITS Reliability and Availability Performance

Not all of the bases met the requirements after the initial design and implementation phase. For example, the initial design of base D did not meet the A_o and MTBCF requirements. Figure 3 shows the network topology for base D. At first glance, the network appears to be a highly fault tolerant, reliable design. However, while the network has sufficient physical diversity, a large percentage of the network's users are concentrated in ITN 4. Within this ITN, there are several single points of failure that can cause a loss of more than 20 percent of the network users. When redundancy is added to eliminate these single points of failure, the network meets its requirements.

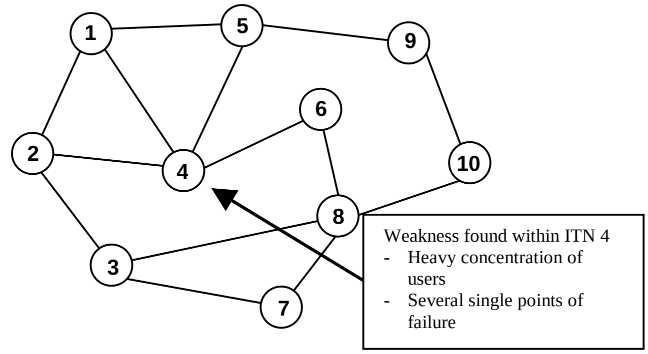

Figure 3. Base D Network Topology

This problem (heavy concentration of users in a small number of ITNs) is inevitable for bases that have three or less ITNs. Clearly, the biggest challenges for CITS meeting its reliability and availability requirements will be for small bases.

LESSON LEARNED

The development and execution of this methodology for the CITS program has provided an opportunity to gain insight into the strengths and weaknesses of network reliability and availability analysis. This section highlights these lessons learned that are applicable to all network analyses.

First, it is very important that unambiguous and precise definitions of availability and reliability objectives are developed, including a detailed definition of a critical failure. There are many ways to define critical failure of a network and that definition will dictate the type and complexity of analysis that needs to be performed. It may be appropriate to have multiple availability and reliability objectives for a network.

The primary solution to any weaknesses in a network's reliability design is to add redundancy. While generally effective, it can be costly. If this approach is implemented without a clear understanding of the potential weaknesses of the network, costly "overdesign" may occur. This analytical process was found to provide the guidance for incorporating redundant configurations only where needed which helped optimize the impact of limited budget resources.

While the goal is to have as accurate a prediction as possible, it is unlikely that field reliability or availability performance will precisely match the prediction. This is because this prediction (like any prediction) requires assumptions about future performance that introduce uncertainty and error. Since error is inevitable, steps should be taken to understand the sources of error and limit their impact on the analysis. This was accomplished through sensitivity analyses that investigate alternative assumptions. These analyses provide a measure of confidence in the results of the analysis.

Analytical network reliability and availability modeling techniques have limitations. For example, it will not model degradation failures such as bottlenecks due to failures in the network. To enhance the network analysis capabilities of the CITS program, a simulation-based network reliability analysis tool is being developed. This tool will randomly fail items within the network, broadcast data packets throughout the network, and document a number of availability and reliability metrics. This will help reduce the number of assumptions that must be made to make the analysis tractable and also provide additional measures of performance (e.g., the availability of each user).

SUMMARY

The modeling methodology described in this paper has proven to be an important part of ensuring highly reliable, cost-effective networks for CITS. It has been very effective at identifying weaknesses that can prevent a network from meeting its reliability and availability requirements. In addition, this analytical process was found to help reduce the cost of some networks by identifying and eliminating the redundant configurations that do not significantly impact the reliability design of the network. This effort has proven valuable to network integrators who have begun incorporating lessons learned from previous analyses into their current network designs, eliminating many of the weaknesses from past designs.

REFERENCES

1. S. Rai and D.P. Agrawal, *Distributed Computing Network Reliability*, IEEE Computer Society Press, Los Alamitos, CA, 1990.
2. G. S. Fishman, "A Monte Carlo Sampling Plan for Estimating Network Reliability," *Operational Research*, Vol. 34, 1986, pp. 581-594.
3. Y. F. Lam and V. O. K. Li, "Reliability Modeling and Analysis of Communication Networks with Dependent Failures," *IEEE Transactions on Communications*, COM-34, No. 1, 1986, pp. 82-84.
4. S. Nojo and H. Wantanabe, "Incorporating Reliability Specifications in the Design of Telecommunications Networks," *IEEE Communication Magazine*, June 1993, pp. 40-43.
5. D.L. Deeter and A.E. Smith, "Hueristic Optimization of Network Design Considering All-terminal Reliability," *Proceedings of the Reliability and Maintainability Symposium*, 1997, pp. 194-199.