Proc. 9th Int. Conf. on Fault-Tolerant Systems and Diagnosis FTSD–9,
Brno., Czechoslovakia, June 1986.

Modeling and Evaluation of Fault-Tolerant Bus Structures for Local Area Networks

Juan A. Carrasco, Engineer **Juan Figueras, Ph.D., Professor**

Departament d'Enginyeria Electrònica, E.T.S.E.I.B.
Universitat Politècnica de Catalunya
Barcelona, SPAIN

Abstract

A combinatorial model for bus LAN structures with backup buses is derived. The model assumes immediate detection of faulty standby elements and same failure rates for both active and standby elements. The model is used to analyze the improvement attained by the addition of backup buses and the effect of catastrophic failures induced by faulty stations. A more general Markov model is used for the double-bus structure. The model accounts for lower failure rates in and limited test of standby elements. An overview of the model is given and the methodology followed for its specification is explained. Results show that for typical dormancy factors preventive test may be no necessary and then design can be simplified.

1 Introduction

Recent advances in communication technology have motivated a widespread success of distributed systems structured as Local Area Networks. The distribution and multiplicity of resources in these systems offer good opportunities for the implementation of both fault-tolerant and gracefully degradable operation. In order to attain these goals the communication subsystem has to be reliable enough. Two aspects affecting the reliability of the communication subsystem have to be considered. First, communication protocols are to be recoverable /1/. Second, permanent faults in the structural elements have to produce gracefull degradation. In this paper only the structural (last) aspect will be considered.

The increasing demand for LANs has motivated work leading to standardization. The IEEE 802 Standard /2/ will propose several methods and two of them (CSMA/CD-bus and token-bus) use a bus structure for the communication subsytem. The structure proposed is primarily a non-redundant one: a single bus interconnecting all stations in the LAN. The addition of backup buses is a simple approach to improve the reliability, and feasible if short interruptions in the communication functions (during backup activation) are allowed. Reliability attributes of bus structures for LANs have been often qualitatively discussed (see, e.g., /3/). Quantitative results /4//5/ are limited and lack generality. It is our purpose to develop a simple but comprehensive combinatorial model taking into account the most significant parameters and also to study the effect of latent faults in and limited preventive test for the standby elements.

2 Structures and measure

The communication subsystem is made up of stations and buses. Stations offer attachment points to the LAN and release hosts from doing most communication functions. Stations are interconnected by m global buses but only one of them is active. Backup buses are used when necessary to maintain

LAN operation. Buses include cable, coupling units and end-line impedance adapters. Each station comprises a communication processor (CP) and a transmitter/receiver unit (TR) for each bus.

In order to evaluate the structures it has been chosen as a measure the *communicability*, previously used by Juanole /6/ and Ihara and Mori /7/. The communicability is defined as the mathematical expectation of the number of pairs of stations through communication is possible, divided by the total number of pairs of stations in the LAN. Denoting by a_{ij} the availability of the communication through stations i and j, and by $C(n,m)$ the combinatorial numbers, the communicability is evaluated as:

$$C = \frac{1}{C(n,2)} \sum_{i=1}^{n} \sum_{j=i+1}^{n} a_{ij} \tag{1}$$

3 Combinatorial Model

In this section a combinatorial model is derived. The model accounts for two mechanisms by which the stations may produce buses be unusable. In the first one, a faulty TR introduces an anomalous physical condition on the bus; in the second one, a faulty CP transmits continuously and prevent other stations from using any bus. Note that for the last mechanism it has been made the pessimistic assumption that the faulty station will try to activate the same standby bus than the others, making the recovery of the LAN impossible.

3.1 Hypotheses and derivation

1) Communication processors, transmitter/receiver units and buses fail with, respectively, rates λ_{CP}, λ_{TR} and γ.

2) Stations and buses in faulty state are independently repaired with maintenance rate μ.

3) The failure of a communication processor corrupts all buses with probability $1 - r_{CP}$. The failure of a TR unit corrupts the bus it is connected to with probability $1 - r_{TR}$. In the last case, the non-confinement condition is supposed to persist while the station is being repaired.

4) standby buses are succesfully activated with probability 1.

These hypotheses establish independence among the states of the elements in the LAN (stations, buses) and simplify the analysis. Let $E_1, E_2, \ldots, E_n$ be the n stations and $B_1, B_2, \ldots, B_m$ the m buses in the LAN. According to the model, buses can be in only two states: 1) operational, and 2) faulty. For the stations, besides the operational state, there are, for $m > 1$, $m + 2$ faulty states: 1) confined fault, 2) non-confined fault corrupting one bus B_i ($i = 1, \ldots, m$), and 3) non-confined fault corrupting all buses. For $m = 1$, the distinction among the non-confined faulty states disappears and the number of faulty states reduces to 2.

Due to the symmetry of the structures all communication availabilities a_{ij} in (1) are equal and C turns out to be their common value. Let us consider, for instance, stations E_1 and E_2. For the communication through them to be possible it is necessary that both stations be in operational state and at least one bus can be used. Let a_e be the station availability and A_k, $k = 1, \ldots, m$ the events *bus B_k is in operational state and stations $E_3, \ldots, E_n$ are not corrupting B_k*. The communicability can be expressed as:

$$C = a_e^2 \Pr\{\sum_{k=1}^{m} A_k\} = a_e^2 [S_1 - S_2 + \cdots + (-1)^{m-1} S_m] \tag{2}$$

$$S_k = \sum_{1 \le i_1 < i_2 < \cdots < i_k \le m} \Pr\{A_{i_1} A_{i_2} \cdots A_{i_k}\}$$

Let a_b be the bus availability and $a'_e(k)$ the probability that a station is in operational state or in faulty state without corrupting a given set of k buses. By symmetry terms in summation S_k are equal and considering the definition of the events A_k it can be written:

$$S_k = C(m,k)a_b^k[a'_e(k)]^{n-2} \tag{3}$$

Finally, combining (2) and (3) it is obtained:

$$C = a_e^2 \sum_{k=1}^{m} (-1)^{k-1} C(m,k) a_b^k [a'_e(k)]^{n-2} \tag{4}$$

Assummed hypotheses allow to model buses and stations with continuous-time Markov processes and the following results are easily found.

$$a_e = \frac{\mu}{\mu + \lambda_{CP} + m\lambda_{TR}} \tag{5}$$

$$a'_e(k) = a_e + \frac{r_{CP}\lambda_{CP} + (m - k + kr_{TR})\lambda_{TR}}{\lambda_{CP} + m\lambda_{TR}}(1 - a_e) \tag{6}$$

$$a_b = \frac{\mu}{\gamma + \mu} \tag{7}$$

The combinatorial model is defined by (4), (5), (6) and (7).

3.2 Application and analysis

Some numerical results obtained using the combinatorial model are presented. In all of them dependency on the number of stations is considered, and for λ_{CP}, λ_{TR} and μ typical relative values have been used ($\lambda_{CP} = 0.95$, $\lambda_{TR} = 0.05$, $\mu = 1000$). In addition, bus failure rate has been supposed to be proportional to the number of stations ($\gamma = n\gamma_u$) and for γ_u two values have been considered: 0.01 (reliable bus case) and 0.1 (unreliable bus case).

Communicability has values closed to 1 and for representatioon purposes it has been used the incommunicability $IC = 1 - C$. A lower bound for IC can be obtained considering that stations must be in operational states for communication through them to be possible. Therefore:

$$IC \geq 1 - a_e^2$$

Following Powell /4/ we will call *ideal* (denoted by IC_{id}), to the lower bound incommunicability for the non-redundant structure. With the adopted values for the parameters $IC \approx$ [illegible]$.10^{-}$[illegible]. The goodness of the structures may be estimated by the proximity of IC/IC_{id} to 1.

The benefit gained by the addition of backup buses has been explored in Figure 1 for the most sensitive case ($\gamma_u = 0.1$, $r_{CP} = r_{TR} = 1$). The most significative improvement is provided by the first backup bus, and the addition of a second one may be advantageous only when the number of stations is very high. For low number of stations the complexity added to the station by the third bus increases the total station failure rate and produces negative results.

Figure 2 compares the single and double-bus structures for the reliable bus case and analyzes the effect of the confinement factor r_{CP}. A similar analysis for r_{TR} showed that a value for this parameter of 0.9 leads to results quite similar to those corresponding to the optimal case ($r_{TR} = 1$). The double-bus structure with perfect confinement of communication processor failures ($r_{CP} = 1$) gives an almost ideal communicability for all number of stations and improves significally the non-redundant structure when n is large, but the improvement is seriouslly limited by even relatively small unconfinement probabilities. Therefore, a main issue in the design of the stations is to minimize this factor as much as possible.

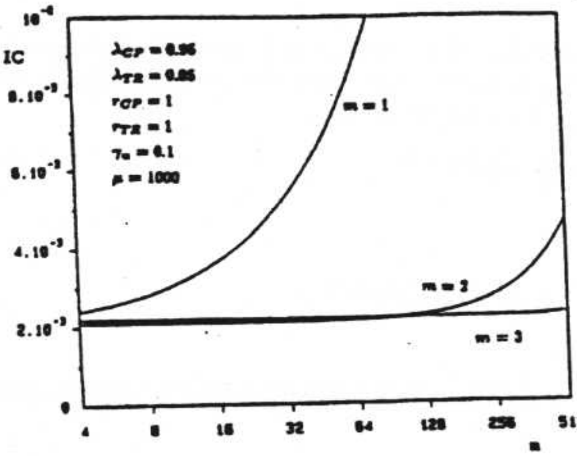

Figure 1: Improvement produced by the addition of backup buses (unreliable bus case)

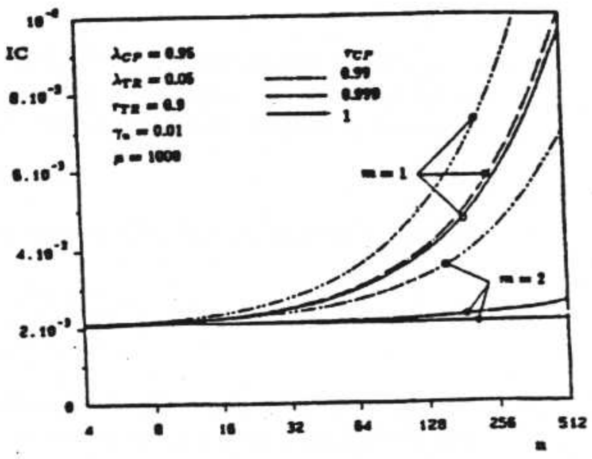

Figure 2: Influence of the confinement factor r_{CP} in single and double-bus structures

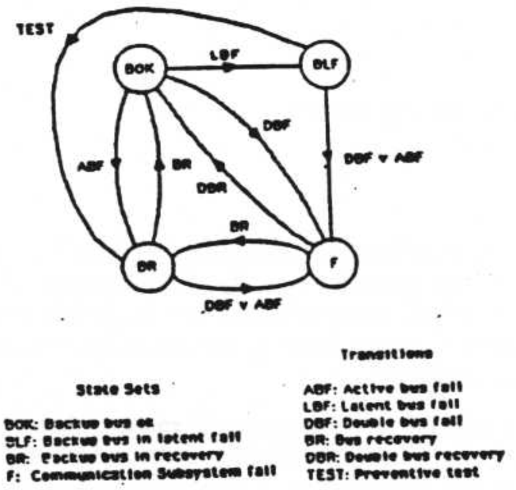

Figure 3: Aggregated transition digraph of the Markov process modeling the double-bus structure

MNEF	n	m
1	18	63
2	41	192
3	74	414
4	119	751
5	178	1226
6	253	1862
7	346	2682

Table 1: Sizes (*n*: number of states, *m*: number of transitions) of transition digraphs obtained for several values of MNEF

4 Stochastic Model for the double-bus structure

The analysis carried out in the last section showed that the double-bus structure achieves an almost ideal communicability in many cases. In this section a more refined model using continuous-time Markov processes will be described and used. The refinements include lower failure rates for and limited test rate of standby elements. We introduce now *dormancy* factors (ratio between failure rates in standby and active states) for standby buses and TR units: K_B and K_{TR}, and a constant preventive test rate ψ.

4.1 Model and Methodology

Figure 3 presents a concise description of the model using state sets. Single bus *falls* can be produced either by bus failures or non-confined TR failures, whereas double bus falls are produced by non-confined CP failures. Single-bus and double-bus recoveries involve the repair of all faulty elements corrupting the bus/es. In set BLF, the bad condition of the backup bus is unknown and no recovery action is taken.

To reduce the number of states the following hypotheses were assumed:

1) A bus being recovered does not fail (the bus has not to be necessarily in non-faulty state)

2) No element fails in the states in set F

3) At subsystem reactivation from F all stations in confined faulty state have been repaired

Specification of the model and automatic generation of the Markov processes were done using a software tool called METFAC (for "Computer Aided Modelling and Evaluation of Fault-Tolerance"). Using METFAC the specification is done symbolically. A set of *production rules* with several responses allow to model the elementary processes determining the state level behaviour of the system. *Action rate* functions associated to production rules specify the rates at which processes are produced. Similarly, *response probability* functions determine the probabilities with which the responses associated to a produçtion rule are issued. An *index* function allows to associate weight factors to states for performance (see, e.g., /8/) or cost /9/ related measures evaluation. Automatic construction of the Markov process is done in two steps. In the first one, a rotulated transition digraph is obtained by applying the production rules to an initial state and those successivelly obtained. In this digraph nodes are rotulated with values of state variables and transitions with pairs action/response. In the second step, this information is used to assign values to transition rates and state indexes. As it was pointed out, the specification is symbollic. Production rules and functions are specified using a set of state variables and sets of structural and functional parameters, being structural parameters those the topology of the transition digraph depends on. Another feature of METFAC is the use of low numerical complexity algorithms, making feasible the processing of large size models. More details about the methodology and the tool can be found in /10/.

A *generative specification* for modeling the double-bus structure was constructed. A structural parameter MNEF (maximum number of faulty stations) was introduced to limit the number of states while attaining the desired accuracy on the results. Functional parameters included: n (number of stations), λ_{CP}, τ_{CP}, λ_{TR}, τ_{TR}, K_{TR}, γ_u, K_B, μ and ψ ; 11 state variabies and 16 production rules were used. A index function giving the uncommunicability in the states was defined. The generative specification can be found in /10/. Table 1 shows the sizes of the transition digraphs for several values of MNEF used in the computations.

4.2 Application and analysis

The model was validated in relation to the simplifying hipotheses (cfr. Sec. 4.1) by comparing their results for $K_{TR} = K_B = 1$ to those given by the combinatorial model. For typical values of the parameters, the error in IC was found to be smaller than 0.7%.

Figure 4 shows results obtained for the extremal cases: no preventive test ($\psi = 0$) and continuous test ($\psi = \infty$), with several values of the dormancy factor K_B . The influence of K_{TR} is smaller and is not presented. Also, the results for the non-redundant structure have been plotted for comparison purposes. Several conclusions can be drawn. First, the combinatorial model ($K_B = 1$) is a fairly good approximation for the continuous test case. Second, though the absence of preventive test degrades communicability, if the dormancy factor for the bus is low, significant improvement over the non-redundant structure can be still obtained without test. Accepting an incommunicability 50% higher than the ideal, the non-redundant structure can interconnect only 9 stations, but, for $K_B = 0.2$ the redundant structure without test acomplish specifications for $n \leq 101$.

The dependency on ψ is illustrated in Figure 5 for a particular case and several values of K_B . Almost all the influence of is concentrated in an interval of about two orders of magnitude.

5 Conclusions

Qualitative conclusions based on the numerical results have been drawn in the previous sections. At the methodological level, the use of continuous-time Markov processes has been shown useful

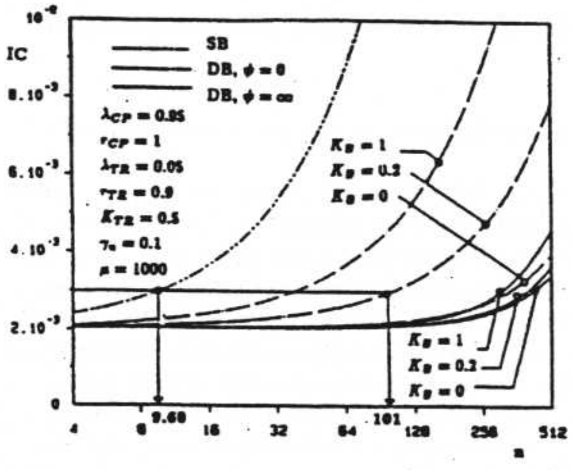

Figure 4: Comparison of no preventive test ($\psi = 0$) and continuous test ($\psi = \infty$) strategies for the double-bus structure

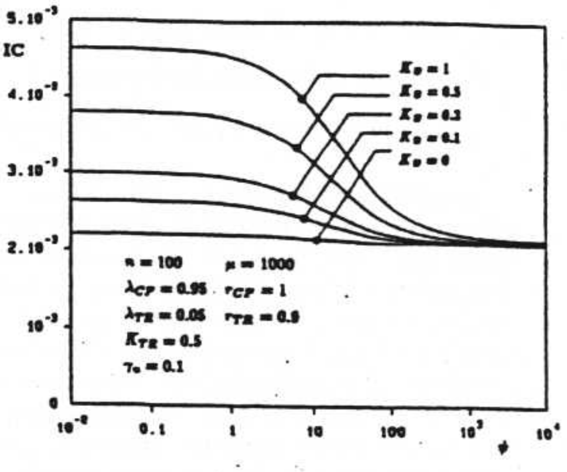

Figure 5: Effect of preventive test rate for the double-bus structure for several values of K_B

to model latent faults. Problems arising in this methodology are related with the large size of the models. Simplifying hypotheses have to be introduced that by taking away asymetries in the model allow to group states and at the same token do not introduce significant errors. Intuition plays here an important role. Finally, flexible model specification methodologies and ability to process large size models, as found in METFAC, are crucial when dealing with the modeling of complex fault-tolerant systems.

Acknowledgments

We would like to express our gratitude to the "Comisión Asesora de Investigación Científica y Tecnológica" (CAICYT) and the "Comisiò Interdepartamental per la Recerca e Innovació Tecnològica" (CIRIT) for their financial support.

References

/1/ P.M. Merlin, D.J. Farber, *Recoverability of Communication Protocols–Implications of a Theoretical Study*, IEEE Trans. on Communications, vol. COM-24, no. 9, September 1976, pp. 1036-1042.

/2/ IEEE-802 Standardization Project, draft D.

/3/ J.M. Ayache, J.P. Courtiat, M. Diaz, *REBUS, A Fault-Tolerant Distributed System for Industrial Real-Time Control*, IEEE Trans. on Computers, vol. C-31, no. 7, July 1982, pp. 637-647.

/4/ D. Powell, *Réseaux Locaux de Commande-Contrôle sürs de fonctionnement*, Thèse de Docteur d'Etat, Institut National Polytechnique de Toulouse, October 1981.

/5/ J.P. Blanquart, J.L. Boussin, K. Kanoun, J.C. Laprie, *Rebecca: a Dependable Communication Support System for the Protection System of Extra-High Voltage Substations*, EUROCON'82, Copenhague, 13-18 June 1982, pp. 825-829.

/6/ G. Juanole, *Prévision de la sûreté de fonctionnement des communications entre calculateurs. Application aux systèmes de traitement geògraphicament distribués*, Thèse de Doctorate d'Etat, Université Paul Sabatier, Toulouse, 20 June, 1978.

/7/ H. Ihara, K. Mori, *Highly Reliable Loop Computer Network System based on Autonomous Decentralization Concept*, FTCS-12, Santa Monica, California, USA, 22-24 June 1982, pp. 187-194.

/8/ J. Arlat, J.C. Laprie, *Performance-related Dependability Evaluation of Supercomputer Systems*, FTCS-13, Milano, Italy, 28-30 June 1983, pp. 276-283.

/9/ J. Moreira de Souza, *A Unified Method for the Benefit Analysis of Fault-Tolerance*, FTCS-10, Kyoto, Japan, 1-3 October 1980, pp. 201-203.

/10/ J.A. Carrasco, *Modelación y Evaluación de la Tolerancia a Fallos de Sistemas Distribuidos con Capacidad de Reconfiguración*, Doctoral Thesis, in spanish, in edition.