ON FAILURE PROCESSES IN COMPUTER SYSTEMS

99

Mátyás Arató

Research Institute for Applied Computer Sciences
Budapest I., Csalogány u.32.

1. Introduction

The purpose of this paper is to study the performance of a computer system under the effect of various system failures. A modern computer system with its operating system, large data bases, user programs, transactions via terminals and at last the hardware is a large scale system. Here by a failure we can mean a deficiency in the hardware or software, parametric or functional one, but we mean also the intentional or unintentional introduction or erroneous information which breaches the integrity of the information stored in the system. It is well known that the failure symptoms of hard failures remain unchanged if most parameters are varied. The failure symptoms of software can come and go by varying the parameters. Failure analysis process means not only the identification of failure rate and mean time between failures but quantifying all important reliability parameters and factors. Further there is making a great deal of effort in the area of fault-tolerant computing which means that the system has achieved high reliability and aviability via automatic fault diagnosis and repair.

Here we are not interested in hardware failure analysis. We remark that some interesting mathematical models of transaction oriented systems under intermittent failures were proposed in [4] - [8] . The systems were assumed to operate with check-pointing and roll-back recovery methods.

In this paper we go further and try to describe the functioning of a computer system with some errors or uncertainties and various types of noise in it.

2. Errors and their sources

Errors occuring in operational systems are investigated as the most characteristic example for troubles of the program systems. The producing companies give, as a rule, error lists and error corrections on the errors found in the operation of an operational system functioning since several years. The reason of such an error is that the program does not work in the same way as it is described or the working process of the program is not described in every detail in the reference manual. These error correcting systems usually consist of several volumes. In general, after the knowledge of the errors, accumulated during a longer period, a new program system or an operation system, a so-called new "release" is introduced concerning the facilities. Error correction has, however, a great deficiency as the application program systems that functioned in a faulty system till then, may get out of order in the new "release". This "arrangement" may happen to ruin functioning systems, for this reason introduction of a new "release", though it has better and greater possibilities, may cause important economic damages. What are the causes of this confusion? As a rule, the programmers notice before the new "release" that the operational system does not do what the description contains. To avoid this, they use the real functioning system when writing their programs and thus the programs are functioning well as regards application. The modified operational system corrects the original, truly faulty solution and makes the system adequate to the description, but at the same time, it ruins the earlier developped application systems. This time we don't enumerate the errors occuring in the error lists of the operational systems. Errors in the operation system may be the sources of failures in information retreavel systems and a new release increase the rate of failures.

In the sequel we investigate some kind of errors in large data base systems, which we managed by an application program system.

It is an"interesting"error phenomenon, in connection with functioning systems often processing data bases that in the case of changing only a few data or inserting into the data basis, causes deviations in the program which cannot be observed even "with human eyes". The observation of a faulty operation of the program system takes place only after some months of system processing /may be 1-2 years later/ when the sum of faulty data exceeds a determined level. The reason of the disturbance is, in general, a branch of the program system being utilized that only once in ten or hundred thousand cases gives a faulty result.

During the conversion of a large data basis a methodical error created in the data causes an important disturbance if it is impossible to recreate the original data, e.g. conversion of a data group into another data group which may be generated in a different manner,too. Generation of the faulty record is unequivocal, but its resetting is impossible. The original state may be reset only using the original data and their correct reconversion. If such an error is detected only after a few months, after carrying out the systematical processing on data, a critical situation may occur. Elimination of the error might signify the repetition of the whole evaluating process, an almost unrealizable fact. The filtering of the fault may be realized also by building a correcting system of great security based on logical or possibly language tests with different level.

Introduction of dictionaries is an often used accelerating procedure in processing large data systems. With their help the procedure of searching and retrieval may be accelerated and so the processing much shortened. Introduction of dictionaries has, however, the great disadvantage that errors or inaccuracies occuring in them mean errors of the good data of the data system. The dictionaries may consist of family names, street names or names of various tools employed in production. Insertions or descriptions too, may be entered into the dictionaries that are not suited to the demands of the Hungarian grammar. Effect of these errors is fundamental in data processing.

The following type of error causes an important problem in processing large data systems. In many cases the program system postulates the processing of controlled data in the second step of a multi-step processing. A data error occuring by chance after the first step ruins the processing program system of the second step.
The reliability of large data systems, the level of processing depends on the human qualities of the computer personnel. The subjective elements and their statistical investigation have to be dealt with in the same manner as it is done in everyday life, e.g. in production. Though not very much is known about the influence of human error on the risk of a system, several authors tried to include human error in fault-tree calculations using rather rough estimates of the error rates. Some authors mentioned a probability p of human error $10^{-3} \le p \le 10^{-2}$ per response under usual conditions. The uncertainty in estimates of human error rates and the lack of insight on how human errors occur provide good reasons for a systematic research

on this subject in computer systems and mostly in managing large data bases.

As regards data circulation, we may distinguish between three systems in Hungary nowadays.

- The large systems, which means that the number of records has the order $10^7 - 10^8$. The behaviour of such data bases is statical enough and they can be treated on large computers. The questions in the retreaval system about the records and their files generally have to be stable enough, and the system of questions may be easily developped.

- The middle-size data systems have number of records in order $10^4 - 10^5$. These data bases are submitted to a relatively fast changing and, concerning its composition, they have intricate inquiring system.

- The third type of data collection is connected with measuring in process control or systems known in telecommunication. In this case we describe the data collection by $\underline{X}_1, \underline{X}_2, \dots, \underline{X}_n, \dots$ where $\underline{X}_n$ means a random vector. In this case, however, the vectors $\underline{X}_n$ are not very large dimensioned. Investigations of such systems stay in the centre of scientific applications. Such systems deserve more attention concerning computer processing mostly in the field of multivariate analysis and statistical inference of time series /stochastic processes/.

The first two types of data bases have been investigated empirically till now, and it seems that further progress demands systematical study and modelling. For this reason the following fact has to be considered: the entry of the data into the computer is connected with human work what affects on the quality of the data and the automatization of their control. The processing time is very long and the control of data is lengthy. In most cases the data are received from documents and formats and the entry into the computer is not automatical. One of the most important tasks is to accelerate the processing of the controlled data. Reduction of the previous half manual control and maintenance procedure from 1-2 weeks, or even 1-2 months, to 1-2 hours may essentially change the efficiency of application systems in operation. This is necessary commercial and manufacturing applications where the problem of data entry in key to board systems is unsolved.

3. Mathematical models

3.1 Many valuable results have already been obtained and mathematical models developped concerning integrity of data and data systems, e.g. we recall the names Gelenbe [8], [9] and Chandy [7], but Hungarian researchers are also linked with successful investigations, [4], [5]. In this section we consider the following example when the state of the data basis will be assumed to operate in the so-called "check point rollback recovery mode". A random time passes between arrivals of the transaction, also the time necessary for execution of it is generally random. It is assumed that the service times of transactions are independent, identically distributed random variables, mostly with exponential distribution. This sequence of random variables is independent of all other processes.

It is assumed that request for transactions is a Poisson process with rate $\lambda(t)$ and the failure process is an independent Poisson process with rate $\gamma(t)$. Let b_i denote the ith transaction time and c_j the jth failure time $(b_0 = c_0 = 0)$. At specific instants of time $\{a_i\}$, a checkpoint is instaured /dump/; that is a secure and valid copy of all the information contained in the system is stored into a memory unit. The creation of the ith checkpoint immobilizes the system during M_i time, which is a failureless run time necessary for a dump. N_i means the run time necessary for a load, regenerating a control point after a failure.

Supposing that a failure occurs at some time t between $a_i + M_i$ (or $a_i + N_i$) and a_{i+1} then the recovery depends on $t-(a_i+M_i)$ /or on the number of transactions in this interval/ $h(t-a_i-M_i)$. Further we may assume at control points a_i the failure may be identified only with probabiliy p /it is natural that $p \sim 1$ /

In this model the system has the following 5 states:

1. normal processing
2. generating a checkpoint /dump/
3. regenerating a checkpoint after a failure /load/
4. recovery of the tasks processed since the nearest checkpoint to a failure
5. failure is missed

Chandy [7] discussed the case when $M_i = N_i = k$ /constant/ and $\lambda(t) = \lambda$ $\gamma(t) = \gamma$. Gelenbe [8], [9] assumed that $\lambda(t) = \lambda$, $\gamma(t) = \gamma$

REFERENCES

[1] M.Arató — Statistical problems connected with queuing models for operating systems. Colloquium on Point Processes and Queuing Theory, Keszthely, 1978

[2] M.Arató — On computational and mathematical problems of informatics /in Hungarian/, Alkalmazott Matematikai Lapok 1977 No.3-4, 245-255

[3] M.Arató — On the mathematical tools of computer science /in Hungarian/ Információ-Elektronika 1978 No.2, 89-92

[4] A.Benczúr — Integrity of data base management systems /in Hungarian/ Ph.D. thesis - 1977 - Budapest

[5] A.Benczúr-A.Krámli — A note on data base integrity, Acta Cybernetica 3 1977 No.3. 181-185

[6] A.Benczúr-A.Krámli — An example for an adaptive control method providing data base integrity. Performance of Computer Systems eds.M.Arató; A.Butrimenko, E.Gelenbe-North Holland 1979 263-276

[7] K.Chandy-I.Browne-C.Dissly-W.Uhring — Analytical models for roll back and recovery strategies in data base systems, IEEE Transactions on Software Engineering 1/1975/ loo-llo.

[8] E.Gelenbe — On the optimum checkpoint interval, 2nd Hungarian Computer Science Conference, Budapest, 1977 /also in Alkalmazott Matematikai Lapok 5/1979/ 141-156.

[9] E.Gelenbe-D.Derochette — Maximum load and service delays in a data-base system with recovery from failures, Modelling and Performance Evaluation of Computer Systems, eds. H.Beilner, E.Gelenbe, North Holland, 1976

[1o] C.Shannon-E.Moore — Reliable circuits using less reliable relays.7. Franklin Inst. 262 /1956/ 191-2o8, 281-297

[11] A.Shiryaev — Statistical sequential analysis, Nauka /1969/Moscow /in Russian/