Woman C.P.A.

Volume 41 | Issue 4 Article 9

10-1979

Electronic Data Processing: Systems Reliability and Recovery Procedures

Elise J. Jancura

Electronic Data Processing

Systems Reliability and Recovery Procedures

Editor:

Elise G. Jancura, CPA, Ph.D.
The Cleveland State University
Cleveland, Ohio

In the most efficient and the most carefully controlled data processing environment, errors and malfunctions occur. In some instances, the results of these occurences impact a relatively small part of the operation and can be readily reversed if adequate provision is made for error recovery and data reconstruction. At other times, a major installation breakdown occurs requiring extensive recovery procedures. In all cases, however, a common element is the reconstruction of the data files.

Reconstruction of Data Files

The basic criteria that determines how long information should be retained in a machine-readable format is the usefulness of that information to the installation. Machine records are saved as long as they are needed for production of reports, for use in an up-dating process, or for use in a reconstruction process. Reconstruction in computerized activities occurs when, for one reason or another, original data in its machine-readable format is destroyed and has to be recreated. If proper thought is given to forms for saving data in its machine-readable form, this reconstruction procedure can be greatly facilitated. If, however, when machine-readable data is destroyed, the installation has to go back to original non-machine-readable forms to reconstruct that information, the process can be time consuming.

Generally transaction records that affect a given version of the master file are saved until such time as that master file has been used as the input to another up-dating cycle in which a subsequent generation of the master file is produced. The procedure involves retention of several generations of the master file as well as retention of all of the intervening transaction files.

When a new generation has been created through an up-dating procedure, it becomes the input for the next processing cycle. Basically up-dating can be accomplished by one of two techniques. First, up-dating can be done nondestructively. In a non-destructive up-dating environment the old master file is kept intact. This is done by mounting the old file on a device physically separate from the device that will record the new file. This is the technique that is employed in magnetic tape processing. It allows for the retention of several generations of a file and, of course, it facilitates reconstruction in those instances where it is necessary. It is in non-destructive up-dating that it is possible to implement the grandfather-father-son cycling technique.

In non-destructive up-dating, the old generation is retained until completion of the next processing cycle to provide backup in case the current generation is damaged. After two processing cycles there will be three generations of the master file. The most recent is often referred to as the son; the file generation used as input to the second processing cycle (and output to the first cycle) is referred to as the father; and the generation used as in-put to the first processing cycle is referred to as the grandfather. Once the son generation has been successfully created, the installation no longer needs to retain the grandfather generation or the transactions processed against it for reconstruction purposes. Of course any reports or printed record of the data represented by these files will still be available.

Destructive up-dating occurs in those instances where the new version or the new generation of information is written on the same physical space as that previously occupied by the old version or old generation of the master record. This type of up-dating is frequently employed in direct access devices. Because the previous generation of data is destroyed in the process of up-dating, additional precautions must be taken in this approach to file up-dating. All possible checking of the transaction information should be performed before the data is used to ensure its accuracy, and additional procedures should be performed during the up-dating procedure to ensure the transactions are in fact being matched against the proper master transaction.

Because destructive up-dating does not automatically produce a reconstruction trail or temporary audit trail, some additional procedure must be executed to accomplish this function. The usual approach is to make periodic copies of the master file, a process referred to as dumping the file. All transactions used in up-dating the master records since the last dump should be retained for reconstruction purposes until the next dump is made. Should any erroneous up-dating or other damage to the master file occur, it is then possible to reconstruct the proper data by going back to the previous version as it exists in the file dump and up-dating that with all intervening transactions.

An alternative to periodic dumping of the entire file is the technique of logging changes to the master file as up-dating is being performed by writing the contents of the transaction and the master record before and after the up-date on a logging device (usually a reel

of tape). Up-dating logs or periodic dumps can be made to another recording device similar to that containing the master file, they can be made to magnetic tape, or they can be printed out. The closer the form of the dump to that occupied by the master file, the faster the reconstruction procedure.

Reconstruction of a Data Base

A data base or an integrated file system provides greater processing efficiency by eliminating duplicate items currently existing in separate, non-integrated files. A transaction that would have affected several different sets of records through several separate processing runs in non-integrated files can up-date the single integrated file or data base in one processing pass. This approach, while providing greater efficiency, does introduce a greater risk of damage to an organization's total information system. When each set of files is up-dated separately, an error in processing affects only one set of master files. The organization can continue to operate with all the rest of its data while reconstructing the particular file in error. In an integrated data base system an error in the system can have more far reaching effect on the operational viability of the organization.

Despite the best planning, situations will occur that can have destructive effects on the data base. Interruption of processing in the middle of an update operation can introduce errors into the record currently being processed. Other error conditions, such as malfunction within the input/output device containing the data base can effectively destroy the data stored there. Any recovery procedure must provide for verification of the accuracy of the data base and for reconstruction of any file information adversely affected by a systems failure.

A critical requirement of an effective recovery system for a data base is the necessity to keep track of the consequences of every up-dating transaction. This is particularly important in the integrated file systems, where one transaction affects several logically related records. It is not enough to know just which transaction is being processed at the time of the failure but the full impact that that transaction has had to the point of failure on the master record must also be determined. A technique must be developed to notify the user initiating a transaction (usually at a remote terminal) what the results of that transaction are so that in the case of a systems failure, the user can be aware of whether that transaction has been processed or not and therefore, if whether it must be retransmitted or not.

One approach to reconstruction of the data base is to maintain a dual recording of the file. Up-dating transactions are used simultaneously to update both files. Error conditions caused by an input/output device (for example a disk file) can be handled by this method, for the second device is unlikely to have a similar malfunction at the same time. Under these circumstances the recovery procedure would be simply to use the remaining good copy to duplicate the correct data file. This approach has a weakness, however, for error conditions within other components of the system, such as failure of a central processing unit, an environmental failure, or an unexplained error in the application program, will produce the same erroneous condition in both copies of the data file.

Another approach, and the one most commonly used, is periodically to dump the data file onto another storage device, on a regularly scheduled basis. The most frequent technique is to dump the file contained on a disk to a tape file. This approach requires that all of the transactions that have occurred since the last dumping operation also be saved. In the event of a failure, all of these transactions must be reprocessed. To minimize the reconstruction time the dumping can be done on a more frequent basis, so that the intervening processing period for which transactions must be saved can be kept to a minimum. This approach to reconstruction has the disadvantage that the dumping operation itself requires time and, of course, that the reconstruction operation can be time consuming, since it requires a re-execution of all of the transactions occurring since the preceding dump.

Where possible, it is desirable when using the dumping technique to incorporate in the dump operation additional processing activities. Thus, while dumping records, an edit routine can be executed to perform edit and reasonableness checks on the logical fields within each record in order to determine, where possible, consistency within the records. In addition, inactive or logically deleted records can be reorganized, so that file rearrangement and compaction can be obtained as a by-product of the normal dumping procedure.

The third approach, which can be used to good advantage in those systems where a systems failure destroys only a few records rather than the entire data base, is an approach that can be referred to as an audit trail approach or a logging approach. Basically this technique keeps a record of all transactions that occur as well as the contents of each master record both before and after up-dating via specific transaction. The log can be recorded on any medium although the most efficient is some machine-readable medium that can be accesible to the recovery routine. By copying the contents of the data base record before up-dating, the full text of the transaction, and then the contents of the data base record after up-dating, the reconstruction log makes it possible for the recovery routine to determine all transactions that were in the process of up-dating when a failure occurred. The records containing information regarding the contents of the data base records allow restoration of any of those records involved in the failure. Serious failures, in which the full file is destroyed, are still best handled by the latest file dump. Then the reconstruction log can be used to merge in the after copy of those master records that have been up-dated by transactions since the last dump.

Recovery Procedures in Real-Time Systems

System re-start in a real-time environment can rarely be accomplished merely by re-loading the program, remounting the data files, and re-starting the system at the beginning. It usually requires instead the execution of specially prepared programming routines that are designed to search out the data files to determine the exact status of the processing previous to the error and to reposition all of the various elements of the system. Sometimes the most difficult part of a restart procedure is determining exactly which part of the system has failed and the status of all of the concurrent activities occurring within the system. The approach taken to recover from an error condition will vary depending upon the cause of the error. Thus, for a large real-time system with many remotely located terminals and communication lines, the procedure for an error in one of the terminals varies from the procedures for errors within the central processing unit.

For some systems, reliability means continuous performance with no failures at all. This need for continuous performance requires the maintenance of fairly complete back-up facilities, even though these back-up facilities are themselves expensive and may not otherwise be fully utilized. For other users, reliability means no prolonged periods of unavailability. For these users, breakdowns, while not desirable, are not of major concern so long as provision is made for a fast recovery and resumption of service. For a third group, protection of the data base and prevention of any loss of data is of primary concern. For many, a combination of these concerns applies.

In those systems where continuous performance without interruption or where high speed recovery from an error condition are of critical importance, the usual procedure is to provide a complex of equipment and program procedures with various stand-by units, switch over devices, and a highly organized set of pre-defined emergency techniques and procedures. A basic approach to handling system failure is to provide for switching to stand-by systems. This approach requires a complete back-up of all of the equipment, the power supply, and the programming systems. It is extremely expensive and thus is used only in those instances where immediate continuation or lack of interruption is essential.

One approach is a duplexed system. In this approach the back-up system is not used by the normal processing unless there is a failure in the primary system. Switching to the back-up system can be accomplished through either manual or programmed techniques. Because the secondary system is not actively engaged in the normal processing, it is available for other uses while the primary system is operational and thus can somewhat subsidize the cost of reliability insurance. Switch over to the secondary system is, of course, not so simple as it may seem, for it becomes necessary upon detection of an error condition within the primary system to ensure that the back-up files are current or to take steps to maintain them in that condition. It is also necessary to provide for loading all of the active programs that had been processing on the primary system into the back-up system.

A second approach to duplicating hardware for immediate continuation of processing is that which exists in a dual computer system. In this approach both systems operate in parallel so that either one can continue operating if the other fails. Duplication in a dual computer system is slightly more expensive than that in a duplex system, but it provides the insurance of more immediate switch-over if techniques are properly designed.

Another approach that is similar in concept to providing duplicate systems is one in which only critical elements are duplicated rather than the whole system. Where an error condition occurs, the system can be reduced (either manually or by programming techniques) to a sub-system consisting only of those critical components necessary to maintain a minimum processing environment. This approach has some disadvantages, for failure in any of the unduplicated components can shut the system down, but it has the advantage of lower cost.

A variation on the approach of duplication of a sub-system is a technique in which alternate forms of data acquisition and processing are established (although not necessarily duplicated). For example, systems that contain several modes of output may switch from a high speed device such as a tape drive to a lower speed but still operating device such as a card punch. Or, in those instances where the computer can segregate memory modules, execution may be limited to just those memory modules still operating, avoiding the module that is experiencing error conditions. The result of this technique is to force the system into a less efficient mode of operation, since by reducing the number of memory modules usable the amount of programming that can be held in core at one time is reduced. This approach does, however, allow the system to continue operating for essential applications. It is successful only in those instances where the system error occurs in components that can be by-passed.

Under some circumstances the only viable approach to error recovery is to bring the system or that part of the system causing the error to a halt. If the error conditions can be identified with the particular application or a particular group of terminals, it is possible to halt that segment of the processing until the cause of the error can be identified and a correction affected. In other cases, such as failure in the central processing unit itself or environment conditions (power or air-conditioning failures), it may be necessary to stop the system until the situation can be corrected. It is important to implement the halt in a planned orderly sequence that allows for completion of transactions in process and identification of the status of all of the major master files.

Contingency Plans for Major Installation Breakdowns

The need for protection from major breakdowns is becoming increasingly important as the information flow of organizations becomes increasingly computerized. Companies with large computerized data files representing a substantial proportion of their accounting records or companies engaged in real-time processing applications that directly affect their normal operations must consciously provide for procedures that allow recovery of data and re-institution os service in the case of a major installation breakdown. For real-time systems actually affecting the physical operations of a company, a major breakdown can mean an interruption of service and the need to provide facilities to prevent or minimize that interruption of service.

Major breakdowns can occur from such natural catastrophes as fire, wind, flood, or earth-quakes, but they can also be precipitated by carelessness or by deliberate sabatoge either by outsiders or employees within the installation. Provision for adequate physical security helps minimize the probability of a major breakdown. However, it is prohibitively expensive, if not impossible, to guard against all potential accidents or equipment failures, hence a contingency plan should be developed to handle unexpected disruptions of service. An essential first step in developing a useful contingency plan for installation breakdowns is a thorough investigation of the data processing applications installed and a decision as to which applications have a vital impact on the continued operation of the company. Once these vital areas are identified, the procedures and data files that must be protected can be identified, and realistic planning for the development of recovery techniques can take place.

Responsible management personnel from both the data processing area and the user department must cooperate jointly in determining which information procedures and computer systems

are important to the health and vitality of the company. Once the recovery plan is developed and responsibility is assigned for maintenance of the recovery procedures, it is important that the necessary raw material for such a procedure—the data files, the programs, the supporting hardware, and the operating instructions—be documented and stored in an off-sight location physically removed from the installation itself. An off-sight location provides safety from natural disasters that might engulf the installation proper and also provides some protection from the actions of disgruntled employees at the home location. Access to the off-sight location must be controlled, and all material kept at the off-sight location must be carefully maintained so that it is current and ready for use at all times.

Provision for Duplicate Hardware—There are several major areas of concern in the development and maintenance of a good recovery or contingency plan. First, arrangements must be made to make available, when needed, particular hardware-software configurations. Duplicate programs and operating instructions are useless unless the company can provide the same computer configurations (including software support systems) for which these programs and instructions were designed. Since the stresses produced by an emergency situation are not conducive to very effective performance in changing operating procedures, and even programs to fit different computer configurations, arrangements for alternative computers should be made well in advance, with frequent review of both the home and the alternative computers.

Periodic review is important, for the value of the back-up plan could be severely limited should the back-up computer be changed without notification and without corresponding revisions to the back-up plan. Not only must the back-up computer be frequently reviewed as to its physical configuration, but the arrangements providing for the use of the computers should also be periodically reviewed. There are environmental circumstances in addition to the physical configuration of the alternate computer that are important. Unavailability of time on the alternate computer can have the same negative impact as a change in its physical configuration. Thus if arrangements have been made to use a particular system, based on the assumption that it will have shifts free during the day, and if the load in that installation has changed so that that computer now has only a few hours free a day, it is important that contingency plans be reorganized to recognize that limitation.

Provision for Duplicate Software—Second, the operating instructions for the recovery procedures must be carefully documented and stored in a safe area away from the primary installation sight. These should include not only the actual computer procedures, but documentation on all the manual procedures such as data preparation and balancing that are a critical part of a successful operation. As important as the documentation is the training of those individuals who will be involved in the recovery operations. Vital time can be lost and expensive errors made when personnel are expected to handle unfamiliar activities during a period of stress. Third, the programs themselves must be copied and stored where they can be properly secured and made readily available when needed. Proper maintenance of the back-up program library is as important as its original creation. At a minimum, current copies of the object programs and their related constant or table data should be stored. Additional documentation such as source programs and diagrams are also highly desirable, once the immediate restart has been accomplished and the secondary recovery activity such as re-establishing normal documentation in the main installation are begun.

Data files that are essential to continued company operation must be copied and stored in the off-sight location. This task more than any other represents an on-going, continuing effort. Each time one of these critical files is up-dated, the off-sight back-up file must also be up-dated. Further, provision must be made for keeping back-up records of the transactions that will affect the latest generation on file (or procedures for recapturing the content of those transactions) as well as emergency alternative procedures for collecting data from currently occurring transactions until the main installation is again functioning.

Audit and Review of Contingency Plans—Because of the importance of the contingency plan to the installation, and because one missing data file could cause an entire system and all of the preliminary planning to be nullified, it is essential that the contingency plan be current and executable at all times. For this reason a periodic review and audit of the proposed procedures is highly desirable. The plan of action and the facilities provided for the recovery procedure should be examined regularly. Responsibility for maintenance of the reconstruction plan should be assigned definitely to a responsible staff within the installation or within the internal audit group. Surprise audits of the off-sight location should be conducted, and any discrepancy between the data files actually stored in the off-sight location and those that should be stored as indicated by the off-sight list of the contingency plan must be resolved, and immediate corrective steps taken to correct current differences and prevent future repetitions of such discrepancies.

It is frequently helpful to have third parties to read the contingency plan and determine if the information needed is clearly presented. This plan will most likely be called into action in a time of crisis, and items such as the correct file to use and the correct generation of the file should be readily ascertainable. The panic like atmosphere in a time of crisis does not encourage clear thinking and systems development. Frequently a simulated emergency in which the auditor actually follows the instructions of the contingency plan, checking the clarity of operating instructions and the availability of necessary programs and files, is a good test of the adequacy of the plan. A systematic review and evaluation of the contingency plan is as important as the original development of that plan. Often the plan originally designed was sound but has deteriorated over a period of time when laxity can develop in the day to day administration of the plan.

The programs and documentation of an installation are important assets of a company. Replacing them is costly, particularly in a time of emergency. Keeping duplicates of programs on magnetic tape and instructions on micro-film in another location is comparatively inexpensive. Carefully planned file storage and predetermined emergency procedures in many instances actually make continued operation possible. Continued vigilance to safe-guard the validity and usefulness of such a contingency plan is a small price to pay for prompt re-start of vital information service.■