An Overview of Reliable Business Systems in Japan

YUKIO MIZUNO*

Introduction

Utilization of computers in Japan began on a full scale around 1961, and from that time on has quickly spread keeping pace with the high-pitched economic growth. In spite of the recent economy recession, the number of computers installed reached 41,929, valued $10,682 million at the end of June 1977. This figure is second to the United States in the worldwide computer utilization.

The application of computers has contiguously spread over various fields, become highly complexed and sophisticated.

Reliability of computer systems has been important today, since it is impossible to talk about all the social activities as well as politics and economy in disregard of influence of computers.

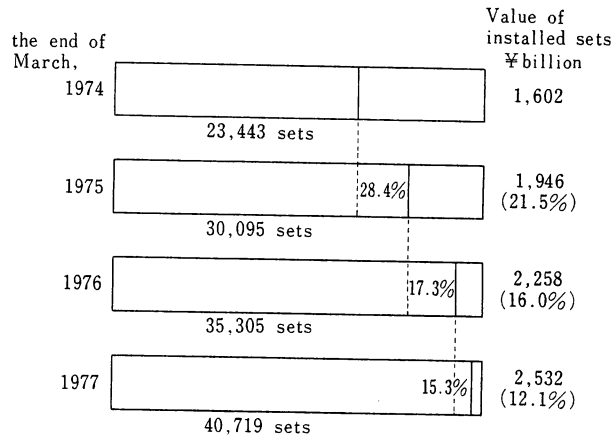
So far, in Japan, the reliability of computers had been discussed mainly in terms of physical damages caused by flood, fire, earthquake and others as well as system failures such as equipment failure and software malfunction, etc. Recently, however, our concern increases toward the operational aspects of the issue, such as invalid or malicious usages of systems/information, computer robbery, privacy violation and so forth.

In this, I report the current status of computer reliability problems, their Japanese peculiarities and how we are going to prepare for them today. I also touch briefly upon the state of arts reliability features seen in Japanese computer systems.

1. Overview of Computer Installation in Japan

In fiscal 1976, a total of 7,533 general-purpose computer systems, valued at ¥731.5 billion, were delivered and installed in Japan. As a result, the number of computer systems in operation totaled 40,719, valued at ¥2,532 billion, at the end of March 1977. These figures represented a 15 percent increase in systems and a 12 percent gain in value over a year before. In comparison with the last year's ratio, a 17 percent increase in systems and a 16 percent gain in value, which were the lowest ever for Japanese computers installation history, we can see the severeness of the impact of the recession caused by Yen revaluation. Though this was partly due to a sort of saturation in the computer market and changes in the market structure, still no one can deny the fact that the computer industry is one of the industries which have high growth potential.

Type-wise, small computer systems comprised the largest single group of all types of computer systems in operation, numbering more than half the total. However, in terms of value, large-scale computer systems in operation accounted for about 60 percent of the total. In the year under review, small computer systems marked the highest growth rate of 4 percent in value. Large-scale computer systems grew 3.6 percent in value, and parti-



Source : Ministry of International Trade and Industry

Fig. 1 No. of installed sets (Growth rate against Previous year).

Table 1 Installation of general-purpose computer systems.

	Japanese-Built	Foreign-Built	Total
Large A	513	552	1,065
More than $1,670	1,556.6	2,065.8	3,622.4
Large B	788	379	1,167
$830–$1,670	915.5	525.2	1,440.7
Large (Sub-total)	1,301	931	2,232
	2,472.1	2,591.0	5,063.1
Medium A	1,827	611	2,438
$330–$830	948.4	398.9	1,347.3
Medium B	2,973	863	3,836
$130–$330	640.6	221.6	862.2
Medium (Sub-total)	4,800	1,474	6,274
	1,589.0	620.5	2,209.5
Small	8,721	2,897	11,618
$33–$130	547.5	198.3	745.8
Very small	11,858	8,737	20,595
Less than $33	247.2	176.3	423.5
Total	26,680	14,039	40,719
	4,855.8	3,586.1	8,441.9

Source: Japan Electronic Computer Company.

*Senior Vice President, NEC-Toshiba Information Systems Inc.

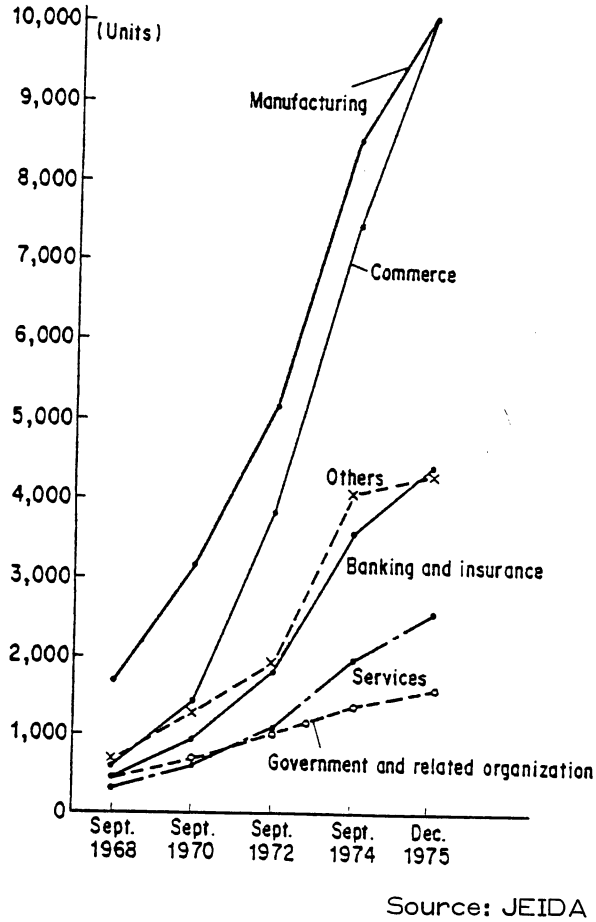


Fig. 2 Trends in the number of computers in operation by industry.

cularly large-scale A or super-large systems recorded a higher growth rate of 4.4 percent. Medium-scale systems hovered on a low growth rate of 3.3 percent. It appears that demand for large-scale and small-scale specialized computer systems is in contiguous growing pace.

The installation of general-purpose computer systems at the end of March 1977 is shown in detail in the Table 1. The number of systems installed passed the 40,000 systems mark. (The top line figures for each kind of computer systems show numbers of sets, and the bottom line figures, values in millions of US dollars (at ¥300/dollar)).

Fig. 2 shows trends in the numbers of computer installations classified by industry. In comparison with trends in U.S.A., it is remarkable in Japan that computers are used much more in the private industries than in the public sector including the Government and Governmental Agencies. It is expected that the utilization of computers in the latter will be expanded by leaps and bounds.

2. Recent Application Trend

Several events or moves which influence the application trends.

(1) Nippon Telephone Telegraph (NTT) recently starts Digital Data Exchange (DDX) Service. This opens another era of computer and communication utilization. This event especially stimulates the minds of both manufacturers and their customers toward the realization of distributed processing.

(2) A series of national projects are under practice, primarily promoted also by NTT, heavily oriented data communications, aiming to solve urban problems and increased social welfare. They are, for example, "pollution information systems", "emergency medical care information systems" and "traffic control systems" etc.

(3) Popularization of Micro-Computers

Nippon Electric Company initiated to sell do-it-yourself type micro-computer kit, TK-80, three years ago. This hit the burst boom along with its consultation service shop systems, Bit Inn. After this, other micro-computer manufacturers followed. Now we found, such micro-computer kits are very convenient hand-on computer education tools. As the result, less Japanese people think that a computer is a magic box any more. Rather, they start thinking of application of micro-computers enthusiastically.

(4) International time sharing services using satellite communication.

Dentsu/GE-Mark III service first broke the national isolation concept of Japanese. There are some such services available today like CDC and so forth. Not few Japanese industries appreciate these services as a new type international data exchange method which also performs data processing.

(5) Shared use of computer resources among industries. Not only through service bureaus but by private industries themselves, computers are used in shared fashion. Recent economy recession eased industries to take such accommodation in terms of available computational resources as well as financial resources. It is also to be mentioned that improvement of security features in modern operating system made this possible.

All of these events, mentioned above, contribute to enriching sophistication and complexity of the computer systems. Especially among large-scale computer systems, few are independent from commonly used data-bases and on-line access to them. Durability and security of computer systems increased its importance day by day under such circumstances.

3. Security and Privacy Issues

According to Japan Electronic Computer Company (JECC) publication on accident prevention and security for information processing, 1977, the total of reported losses reached $6.45 million (43 cases) in the period from February 1968 through September 1976. The causes of these losses include flood, fire, earthquake, hardware/facility malfunctions and operational errors. Along with these external or unintended damages, we experienced several exposed cases of computer crimes and bombing targeted industry data centers. The first commonly known case was reported in 1971. A part-time operator at a

magazine publisher copied the subscriber information tape and released it to external hands for some money. Several million dollar embezzlement cases by accounting clerks were reported where the existences of computerized data processing were used for concealing their crimes from supervisory eyes.

On-line cash dispensers are very popular in Japanese banking systems. Crimes utilizing them were increasingly publicized. Theft using CD cards and credit cards are normally not reported since the bankers are very conscious to protect their safe saving image. A peculiar case happened in 1974, such that a ransom for a kidnapped child was asked to deposit to a bank account opened with false name and address, and was withdrawn through cash dispensers which were some of numerous installed over cities.

It is told that Japan is one of the most secure countries in the world. This is true and mainly because the geographical isolation granted us "everybody-know-each-other" community structure. Therefore people's concern to the computer security might sound low-tone in comparison with that of the United States. However it is no doubt that importance of security issue will increased as computer dependencies of social and business activities increase.

4. Computer Reliability Precautions

According to the survey conducted in 1976 by the Department of Governmental Administration,

(1) users precautions are paid mainly for the reliability or integrity of processing rather than security,

(2) consciousness to system reliability is higher in Finance, Insurance and Government users,

(3) more or less investments were in practice for the peculiar domestic natural disasters (e.g. typhoon flood and earthquake) and

(4) few precautions were paid for software security. Here I think it useful to introduce the survey results a little more in detail.

4.1 Reliability Precaution on Central Hardwares

Precautions for central hardware failure were paid on; Backup Control, Recovery Procedures, Operational States Logging, Test and Diagnosis, Auditing and other management controls.

(1) Backup Control

52% users are using some kind of backup computer systems. Among them, 47% are duplex systems, 9% are dual systems and 4% are multiprocessor systems. Some users are employing cluster configuration system as an enhancement of duplex system. Other users use mono-processor systems with duplicate peripherals and communication facilities. Fail soft configurations are also used for system contingency in some systems.

(2) Recovery Procedures for Hardware Failure

83% users have pre-defined operational procedures for recovery. Among them, 37% specify fully detailed recovery procedures and 63% set only basic rules. Remaining systems only depend on the vendor offered facilities such as system error messages upon which a call is made to field service engineers.

(3) Automatic Operational Event Logging

90% users are using automatic logging features of operational status. These are normally used postmortem analysis.

(4) Test and Diagnosis

80% users are incorporating automatic test and diagnostic facilities within their systems.

(5) Operation Time Recording and Checking

94% users are recording actual system operation time and among them 54% are conducting the checking of time difference between schedule time and actual time.

(6) Management of Operation

50% users are strictly defining operational rules and disciplines and monitoring operators to avoid illegal operations. Examples of such practices are as follows;

- Publish written instructions of operations
- Clear separation of personnel roles such as console operation, peripheral unit operation, tape mounting, printer operation, terminal operation, job control macro preparation, job execution, job reception, operation administration.
- Assign a few operators to one operation function and check and monitor mutually.
- Implement automatic job scheduling by computer
- Simplify and standardize computer operation
- Auditing computer operation with logged data

4.2 Reliability Consideration in Software

Almost all roots of software faults caused in application programs or data files, were found in the development phase of the systems. Therefore, variety of practices had been done to improve software quality at the system design, implementation and debugging stages.

(1) Design and Implementation

The most commonly used implementation language is Assemblers followed by COBOL, PL/I and RPG. The first three languages occupy 81% of the usage. Nearly 71% users use some kind of Software Engineering methods such as Structured Programming and/or Top-down design method to insure the software quality.

(2) Program Testing

40% of users experienced some kind of difficulties in program debugging and testing. Some are using vendor supplied debugging tools, such as dump list or Tracer, and others use their self-developed debugging or testing methods. Test data used for testing were prepared in various fashions. Some established internal standards for test data generation for developers and other asked their end users to provide them. Several users reported that they developed an automatic test data generation program, but they could not totally depend on them because of their poort practical efficiency. An acceptance test is performed for such programs developed by the third party. Over 85% users are performing such ac-

ceptance test by themselves and others depend upon the third party specialized for such works.

(3) Program Maintenance

When a part of application program was modified and if other end user uses this application not knowing the modification, the results will be disastrous. Hence some rules for program modification must be established. 46% users are using methods that the administrator of EDP division authorizes the program modification. 36% users are merely keeping record of modification on papers.

4.3 Reliability Considerations for Communication Lines

Communication line failures result from the degradation of line quality or the line shutdowns. The security and the integrity of messages on the communication circuits are to be protected.

(1) Message Checking

58% users employ the request-repeat system (ACK-NAK) and 12% use automatic redundant resending method. In a few high reliable systems, the echo checking or concurrent multi-route checking is employed. Line quality is checked mainly by cross parity checking (53%). Other use only vertical or horizontal parity checking or the mark counting system.

(2) Communication Line Backup

20% of users prepare duplicated active lines for backup, 16% escape to alternative telecommunication methods such as facsimile or telex. In other cases, messages are to be routed to public telephone lines, to dedicated standby lines which are normally manually switched, or to paper tape output equipments.

(3) Protection of Messages

Terminal ID and user password are generally used for terminal access protection. The encription/description features to protect wire-tapping for abuse, are not yet used. 93% users are using validity checking feature of message header by software.

4.4 Reliability Considerations for Terminal Failure

Features implemented for terminal reliability are; backup terminals, off-line terminal operation, systematic test/diagnostic functions and accommodated restart/recovery features. Frequently keyboard arrangements are designed to avoid misoperation. Terminal security feature and input validity checking are also incorporated.

(1) Terminal Backups

53% users are employing one or more of the following backups;

- Same type of terminals are grouped and installed in one location so that any of them could be the alternative of others.
- Only the key portions are duplicated, such as terminal controllers or key application terminals.
- Standby terminals are pooled off-line for replacement.
- Message delivery to an alternative location site.
- Message delivery to the center computer.
- Full time attendance of field service engineers.

(2) Off-line Terminal Operation

42% users are preparing off-line terminal operation procedure for line failure. This setup is not applicable for such users who depend on centralized data and processing capabilities.

(3) Self Test/Diagnostic Function of Terminals

43% users are using terminals equipped with self test/diagnostic features.

(4) Recovery from Terminal Misoperation

84% users depend on the warning messages sent by the center computer when misoperation was detected. Corrections are made through the same terminal, special dedicated terminal for recovery, or the center console.

(5) Keyboard Arrangement

50% users are making some consideration for keyboard arrangement to prevent misoperation. These are;

- Color coded key tops by functions.
- Arrange keys according to usage frequency.
- Rearrange character keys for non professional operator convenience (Japanese phonetic alphabet sequence, etc.).
- Arrange keys to minimize upper/lower case shifting. Lock unused key by applications.
- Keymat designation by applications.
- Use abbreviation keys where applicable.
- Use special terminals tailored for a specific application.

Some user is implementing terminal software which designates the next key to be operated.

(6) Terminal Security

44% users are employing mechanical protection features such as use of mechanical key and lock. 63% are using protection by software. Among them, 66% are using personalized password checking and 34% use magnetic key equipments which generate application dependent code messages. Other protection features such as password/answer back code, double key, key/operator code and terminal ID are also used.

(7) Input Validity Check

94% users are using software validity checking feature for input data. 64% users are also performing validity check on major operation codes.

4.5 Avoiding Natural and Physical Disasters

Precautions for natural and physical disasters such as fire, flood, wind storm, explosion and earthquake must be preparec in computer installation room, software and terminals.

(1) Computer Room

Some special precautions must be considered against natural and physical disasters for computer rooms. These includes computer installation methods and air conditioning. 73% users are equipping some kind of facilities against such disaster. Among them, 70% users are using fire prevention facilities and electric power regulator systems. Precautions for flood and earthquake are also considered.

As for fire prevention and detection, they use a combination of thermal detectors, ionization detectors, alarms, carbon dioxide flooding systems, halogenated extinguishing systems, use of fire-resistant materials and so on.

To prevent dust and salt hazard, fixed window and double window are installed.

Computer room must also be protected against burglary and riots. For such disasters, 62% users are equipping some kind of facilities such as single entrance with ID card, human security guard system and so forth.

17% users are performing regular precautions activities for mice and insects.

(2) Software

86% users are maintaining copies of master files in specifically designed safe storages, others keep them in an off-site location. Recovery procedures are prepared to reconstruct master files from old masters.

(3) Terminals

Precautions for terminals depend on the environment where terminals are installed. 21% users furnish some equipment for power voltage turbulence, 20% for temperature, 16% for humidity. Precautions for lightening and salt hazard are also considered.

(4) Electrical Power Facilities

58% users are preparing some facilities for electric power outage. Among them, 41% are equipped with two separate feeding facility or in-house diesel auxiliary generators. 10% users are using storage batteries which provide power for more than half an hour, other using less powerful batteries.

5. Earthquake Precaution

Five fifteen in the afternoon, on June 12, this year, an ultra-scale earthquake, magnitude 7.5, erupted in North–East part of Japan.

In Sendai City, the largest city in North East district, population close to a million, many houses and properties were destroyed. Electric power and other utilities were going out almost immediately. Fortunately there was no fire loss which normally makes up a large portion of damage in such catastrophe.

Since Sendai is the center for governmental and business activities in North–East district, there were numerous computer systems under operation. However, no big computer related loss was reported except one.

This one exception happened on a NEC ACOS computer installed on the eleventh floor of a twelve story building.

I should state that this is neither because our ACOS System was fragile nor because our installation engineering was poor, but because the building structure resonated with the vibration of the earthquake.

As the result of the resonance, the equipments received 2 to 3 times larger gravity than that expected. The damage and its recovery are summarized in Table 2.

We evaluated that this is a very special exception because this is the only case out of 166 NEC computers installed in the area under the same degree of influence of the quake.

Table 2 Summary of accident.

Strength of earthquake power received	
	0.3G–0.6G (11th Floor)
	0.07G–0.2G (1st Floor)
Detail description of damage	
Equipment broken:	None
Equipment fell down:	Magnetic tape units: 9
	System console: 1
	Optical mark reader: 1
	Peripheral console: 1
	Tape cabinets: 4
Equipment moved:	Central processors: 2
	Main memory units: 4
	Magnetic tape units: 3
	Magnetic disk units: 9
	Unit record devices: 8
	Other peripheral units: 11
	Air conditioning units: 2
Other computer room damage:	Cables cut: 6
	Broken window glasses & sashes by collision: 4
	Data media destroyed: 12
Recovery	
Working hours spent for hardware recovery & tests: 9 hours	
〃 for software recovery & tests: 31 hours	
Operation resumed three (3) days after the happening	
Total cost for recovery (estimated):	¥44,000,000 ($220,000)

Even though, we studied this case very carefully, since Tokyo and vicinity, where one third of Japanese population are concentrated, are under scare of bigger earthquake, magnitude 8 or more in the very near future.

With our customers, we developed degree of safe installation techniques. One of them, developed by Ohbayashi-gumi Company, is employing floating floors suspended by spring shock absorbers. According this technique, equipments will not receive any earthquake power of less than 1G magnitude. The cost of this, however, is reasonable enough to make DP managers hesitate. It costs $300–400 per square meter, versus $50 per equipment unit for simple slippage stopper method.

However, in the case which I just mentioned, the floating floor is the economical choice, since the cost required for the installation will be ¥11,250,000 or $56,000, which is one half of the domage cost.

6. Reliability Features Implemented in Computer Systems

Here I'd like to introduce briefly the state of arts reliability features found in current operational computer systems in Japan.

6.1 Runtime Error Confinement

Most systems employ MASTER/SLAVE privilege control and page key protection as seen in IBM 360/370

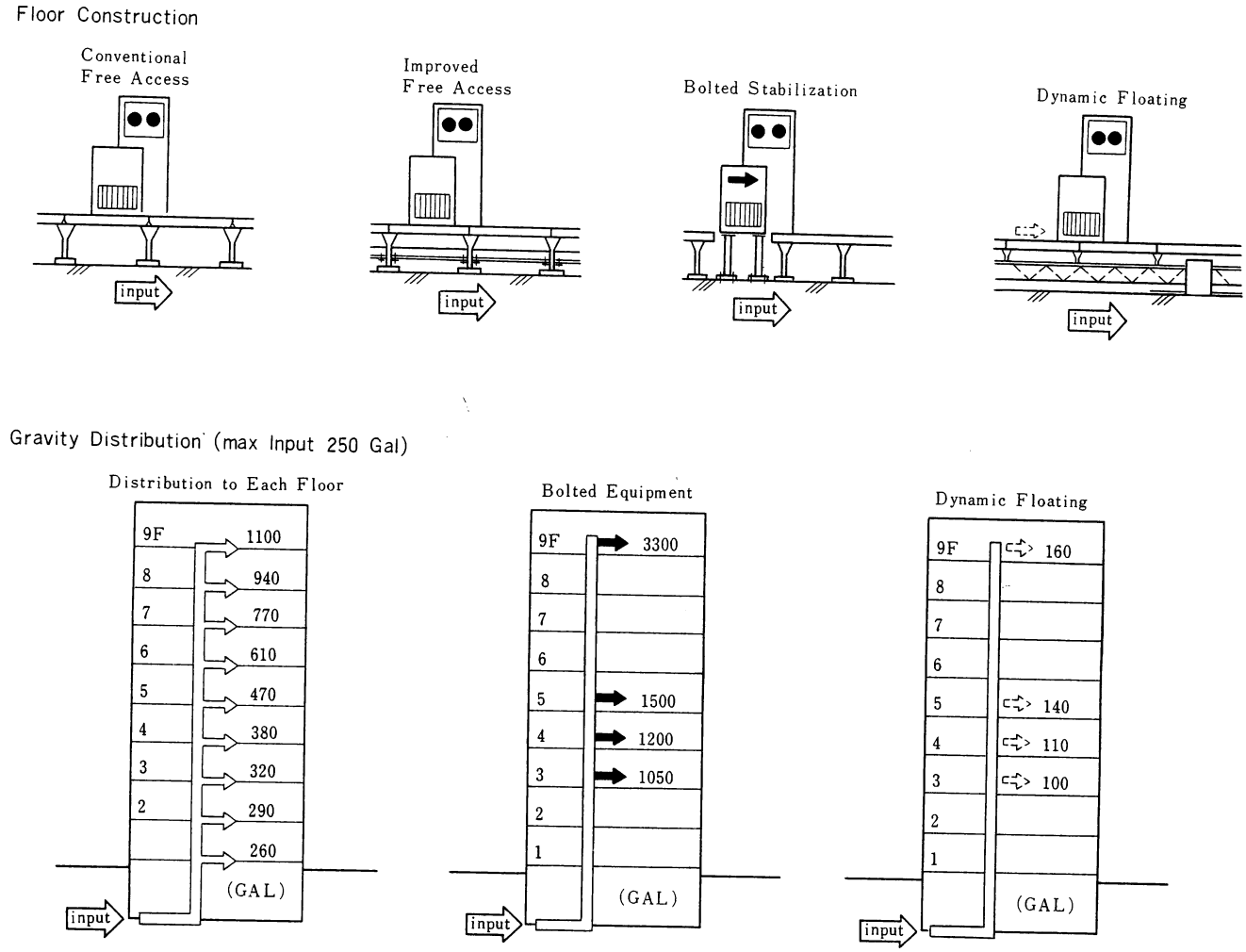


Fig. 3 Tumble free computer flooring (developed by Ohbayashi-gumi).

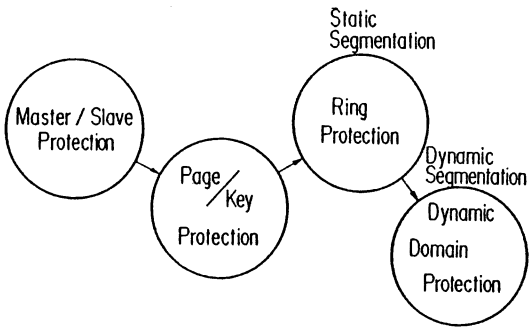


Fig. 4 Runtime error confinement.

architecture. However, Hitachi Series 8000/EDOS and NEC ACOS Systems are furnished with ring protection mechanism a la MULTICS. ACOS Systems incorporate most of advanced runtime confinement features. Capability list feature of ACOS, which controls a process accessible domain dynamically, is one of the most advanced runtime confinement mechanisms. This feature is a must for large computer systems where a number of shared procedures and data are accessed concurrently by application processes. This mechanism is also effective to avoid the gift/foreign program problems or Trojan Horse syndrome.

6.2 Access Control by Authentication

Most computer systems are furnished with some kind of access control by authentication.

Password or key/lock mechanisms in system access level, file access level and record access level are among them. These access control mechanisms are incorporated with other system features such as catalog or directly system for data files and data bases.

6.3 System Recovery Restart

Advanced DB/DC packages, such as Fujitsu AIMS and NEC TDS, provide the full journalizing capability for automated system/data file recovery. Checkpoint and Restart features are common in most computer systems available in Japan.

6.4 System Degradation

NEC ACOS has nearly complete system degradation features. Its main memory could be isolated in 4KB piece automatically if failure occurs there. Addressing mechanism restructures the rest of memory and the processing resumes in seconds. If alternative equipment is available in the configuration, any of erroneous units, e.g. peripherals, controllers, paths or even central

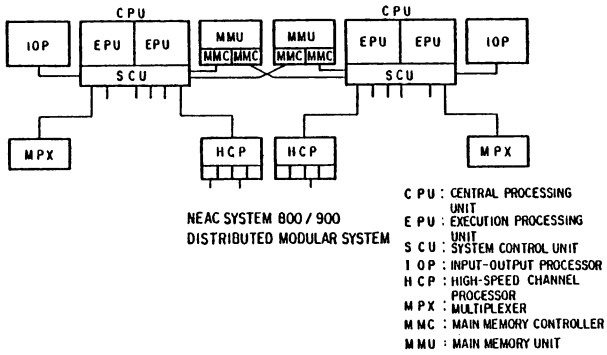


Fig. 5 An example of degradable system.

- On-line Diagnostic to Other Components
- Prepare Maintenance Information
- Failure Isolation
- Dynamic Reconfiguration / Degradation
  incl. CPU, Main Memory, Channels...
- Demand Operator Actions

Fig. 6 System T+D of 10P.

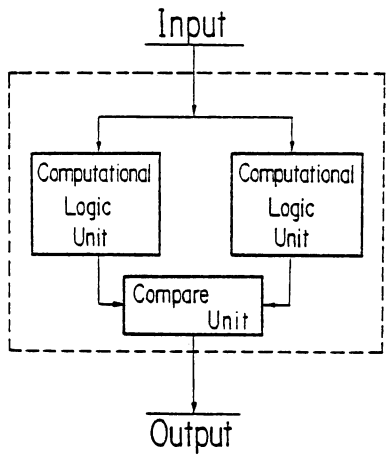


Fig. 7 LSI'd dual logic.

processors could be isolated without operator intervention except some rare cases.

6.5 Error Detection and Diagnosis

Almost all computer systems are employing ECC features in main memory, control memory, tape system and disk system. Instruction retries and I/O channel command retries are also implemented.

Every errors are logged by a service processor in modern systems and these errors are analized by diagnostic programs concurrently with normal processing.

6.6 Reliability Improvement by LSI Technology

LSI (Large Scale Integration) and its associated packaging technology is extensively used in Japanese large scale computers such as NEC ACOS, Fujitsu/Hitachi M Series. Thus increases net hardware reliability.

In addition, in case of ACOS, arithmetic unit of centra processor and I/O processor itself are completel duplicated by taking full advantage of LSI and th processing results from duplicated units are compared i real-time fashion. This feature seems to be employe only in ACOS system as commercial computer in th world, although it appeared in non-commercial digit systems like Bell's ESS.

7. Conclusion

No reliable system is realized unless an experience system engineering is practiced for careful analysis an arrangement of environments, facilities, compute communication hardware and software, human bein and their behavior, information to be processed and n to be processed. I have not mentioned much abo system engineering, which I know that other speake who represent Japanese computer system application can give you good examples of excellent system enginee ing for reliable systems. I confined the issue to economic aspects of reliability precaution and conclude this speec

As you may see, the majority of Japanese comput users have employed more or less reliability precautio However, it is hard to judge whether such precautio are enough adequate or not. Since any system trouble disaster can not be predicted when it happens in natu the adequacy of the precaution is proven only after t preventive worked out successfully on an occurrence such events.

To determine the adequacy of computer reliabili investment for one type of trouble, we have to consid trade-offs among Probability of occurrence P(t), es mated Losses L(v) and the Cost for the preventive C.

$$\mathrm{Min}\left\{\int_0^T P(t)\cdot L(v)\,dt + C\right\}$$

Probability P(t) is mainly dependent upon time. F practical evaluation, a time span is normally fixed. T is reasonable because the social environment conditio system value, available preventive technologies and th costs will vary in a long time. It also depends upon wl to be protected. For example, to protect data files wh are cyclically generated, double or triple of the cycle ti may be good enough for the purpose. Cost, C is a fixed when a preventive is selected for evaluation.

Loss, L(v) is a function of value of the involved co puter systems. Here the value, v should include value system hardwares, developed or purchased prograr data in files as well as effects of its services.

You may realize that L(v) estimation is the difficult one. Our recommendation to our customers for this issue, is as follows:

Since if we do not have the preventive in question, we have to perform a series of recovery efforts on the occurrence of the disaster. The cost of such recovery efforts is the adequate value of the losses.

I believe this is a very practical way to determine L(v)'s.

We see there is no grobal resolution for these trade-offs. Rather, we have to work on each individual case. Sometimes we are forced to give up even the minimal requirement for its cost.

Technology evolution could break this situation either by offering a totally new scheme or by improving the cost of old one. Moreover, such technology improvements sometimes cut the cost of an expensive scheme drastically so that everybody can appreciate it. A good example of such technological breakthrough is the duplicated LSI logic employed in NECACOS mentioned before. Through this, customers are now secured by the redundant duplicated configuration at an average cost.

Your trial on risk isolation and preventive cost analysis is very important since it may trigger such technology evolution in the near future.

References

1. Computer white paper, JECC, 1978.
2. JECC Computer Note, JECC, 1977.
3. EDP in Japan, JECC, 1978.
4. Standards for Electronical Computer Systems Security, MITI, June, 1977.
5. Security Precaution for Information Processing-Domaye Summary Report of Miyagi off Shore Earthquake, JECC, August, 1978.
6. Computer Security, Y. Mizuno, at Kanto NEAC User Association, August, 1978.
7. Security Sub Committee Report, Kanto NEAC User Association, March, 1978.
8. EDP System Security-Management Information System Development Course Report, Japan Productivity Center, February, 1977.
9. Special Features on "ACOS System 800/900", NEC Technical Journal No. 123, March, 1978.
10. Dynamic Floor System, Ohbayashi-Gumi Company, Ltd., 1977-9-10-373-NTS, 1977.