Dependable IT System Building Technologies

HIGASHI Kenji, UWAKUBO Shin'ichi, YASUBA Hiroki

Abstract

With the increasing utilization of IT systems, due to the availability of broadband services and popularization of mobile phones, the influences of malfunctions are becoming greater as well. The concept of high availability is essential for building IT systems that make it possible to use the desired services whenever they are wanted and at the expected service levels, which are dependable IT systems. The causes of failures are diverse, ranging from the deterioration of hardware with age to malfunctions of complex and varied software, such as operating systems and middleware. Appropriate building technologies are necessary to realize IT systems that will not interrupt services when either scheduled or unexpected shut downs take place, while minimizing service down time. IT system building technologies with the assumption of failsafe systems are summarized in this paper.

Keywords

OMCS, SI technology, high availability, failsafe, VALUMO-ware

1. Introduction

Access to the Internet has been increasing in recent years due to the availability of broadband services and popularization of mobile phones. According to the information and communication white paper of fiscal 2005, the number of Internet users has reached 80 million[1]. However, the survey conducted on consumers by the Ministry of Public Management, Home Affairs, Posts and Telecommunications, revealed that about 70% of the respondents indicated that their opinion demanded the "realization of a safe and secure living environment"[2].

With such a rapidly changing environment, the services provided by businesses and public institutions through IT systems that were "convenient if available" have transformed into "inconvenient if unavailable" services.

Services by banks intended for individual persons, for example, are used by many people and also are rapidly expanding and becoming more popular in recent years, due to the convenience in terms of time and location increased through the installation of ATMs at convenience stores and expanded business hours at branch offices. Furthermore, mobile phones are being used by many people due to the increasing modes of use, which are not limited to voice communications but are also used for e-mails, browsing web sites and for using mobile EC services, etc.

IT systems providing such services that are used by so many people require to make available to users "desired services whenever they are wanted and at the expected service levels," which means such systems need to be "dependable."

The building of dependable IT system technologies is introduced in this paper. Furthermore, readers are directed to refer to the paper[3] published in Vol. 58, No. 5 of the NEC GIHO (in Japanese) for details regarding dependable network building technologies.

2. Issues of IT Systems, and then OMCS

Large-scale general-purpose systems (mainframes) and fault tolerant systems were the principal dependable IT systems of the past. These days, however, there has been an increase in the number of open products adopted for such systems. Open products, for which external specifications are disclosed and in common, are on one hand able to offer a superior cost to performance ratio using advanced technologies, but on the other hand they are offered in a diverse range of product groups, while numerous combinations exist between the versions, resulting in more than just a few prominent unexpected failures (pitfalls).

NEC started building large-scale backbone systems (Open Mission Critical Systems and Solutions: OMCS) using open products since 1995. The following SI technologies have been established through the process using open products (known also as "best-of-breed" products):

Item	Cause of system failure	Advance strategy	Post strategy
Unanticipated interruption	Hardware deterioration from aging Hardware failure	Detecting early indications relating to failing sections, health checks, as well as continuation of services through redundant or duplicate configurations.	Isolating or degenerating tasks to separate a failed section in order for the system to provide services.
	Software bug	Code reviews and advance evaluations.	Same as above.
	Package design error	Review of architecture and methodology design.	Same as above.
	Operational error	Thorough implementation of operating procedures, training and raised degree of familiarity through rehearsals.	Immediately establish an emergency strategy office to consider and implement top-down countermeasures and restart services.
	Spike traffic and attack	None.	Prevent the total downing of systems by controlling traffic, regulating networks and suppressing the maximum number of sessions and threads.
	Force majeure (natural disaster or terrorist attack)	None.	Continue services by switching systems over to backup centers.
Scheduled interruption	Periodical replacement of hardware	Prevention of confusion by thoroughly informing stakeholders in advance regarding scope and degree of impact. Interruption of services are classified into no service interruption, temporary service interruption and complete service interruption according to work implemented to standardize procedures in order to shorten maintenance time.	
	Emergency replacement of hardware		
	Addition of new service		
	Application of emergency patch		
	Modification of facility system		

Table Categorization of causes for system failure.

• Large-scale super parallel batch systems that realize the management at multiple centers and operations of uninterruptible unmanned centers, which are operational around the clock 365 days a year, as disaster response strategies.

• Uninterruptible online systems that make it possible to expand systems without interrupting operations.

• Fully open accounting systems using a multiple layer architecture through hubs and a high-speed server switching technology.

• Interoperability using multiple platforms and daily settlement systems that support real-time management.

• Super parallel thread control middleware that processes several tens of thousands of transactions per second and mobile internet gateway systems, which make it possible to perform the centralized management of hundreds of devices.

NEC established the OMCS-SI technology by sorting out, organizing and systematizing SI technologies, such as those mentioned above, accumulated through system building. The three mainstays that support the OMCS-SI technology are the project management technology, application development technology and platform building technology [4].

3. Viewpoint and Perspective for Design of Dependable IT Systems

Defining the requirements in the upstream design stage of IT systems is considered critical. Requirements are often categorized into functional requirements and non-functional requirements. The perspective often tends to emphasize a focus on the functional requirements which is directly linked to service content. With the OMCS platform building technology non-functional requirements are treated as system requirements and are categorized into the following six characteristics (MC characteristics*). A design evaluation index is defined and sorted out for each of these.

1. High availability: Service is not interrupted.
2. High performance: Guarantee of service level.
3. High operability: Monitoring of service.
4. Highly collaborative: Interconnection of services and protocols.
5. High confidentiality: Service security.
6. High expandability: Phased expandability through optimized investments.

One of the most important features that must be incorporated into dependable IT systems, providing the desired services whenever they are wanted and at the expected service levels, is "high availability." This is realized by incorporating a mechanism for preventing the interruption of services during prede-

* Mission critical characteristics: General term used for features that need to be incorporated into computer systems, other than those essential functions that must be provided.

termined service provision time periods or minimizing service interruption time.

In order to "prevent the interruption of services" of IT systems, failure countermeasures based on a failsafe concept becomes essential. The cause of system failure is classified based on the assumption that "failure will certainly occur," to sort out the strategies to ensure that incidents occur in a manner where they will fall on the safer side of the system. These are categorized into strategies against the causes of failure that need to be implemented in advance (advance strategies) and those that are implemented after a system failure occurs (post strategies) (**Table**).

Technical responsive strategies can be sorted based on such categorizations determined by the causes of failure. System failures, arising from software bugs, can occur due to downed processes from referencing to unauthorized addresses or process stalling from deadlocks. For downed process failures can be localized through early detection using process monitoring mechanisms and service monitoring mechanisms, before automatically executing process reboots or the confinement of relevant tasks.

4. Case Examples of Packaging Technology for Dependable IT Systems

The basic design policy for high availability in the OMCS platform building technology is "when in doubt, switch[**]". This is based on the failsafe concept. It monitors the anticipated fail sections, and once it detects a failure and determines that the interruption of services will cause irreparable conditions such as a breakdown in the consistency of data or partial or total interruption of services, if processes are allowed to continue, it degenerates the system by isolating the target section or switches to the stand-by mode with which the entire system falls to the safer side.

An example for realizing this concept is summarized using an online transaction processing system (OLTP system).

The structure and operation of typical OLTP systems that use an open system are shown in **Fig. 1**. Request messages transmitted by client systems, such as bank ATMs, for example, are received by an application node and processed by the business application (Application A to Application X), which is controlled by the transaction monitor. The business application exchanges data with the database node as required. For example, response messages, such as responses to balance inquiries, are returned to client systems.

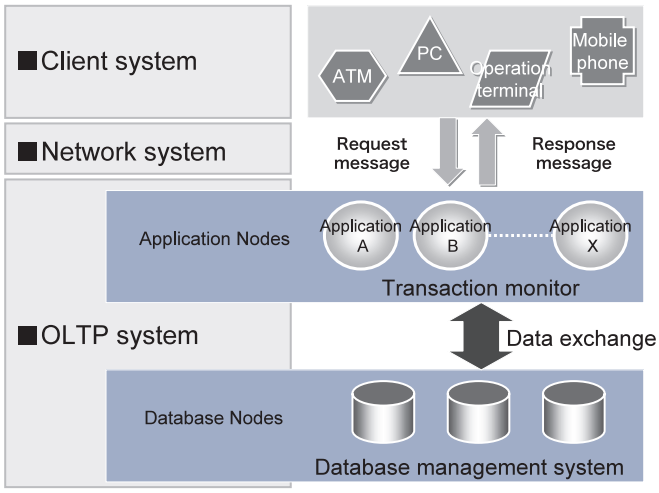

Fig.1 OLTP system structure and operation.

If requests from business applications cannot be received by the database node for some reason, the service of the OLTP system is interrupted and a system failure results. Various types of malfunctions that trigger such a failure can be considered, such as the downing of database software, stall of an operating system, downing of an operating system (PANIC), CPU failure, corrupt memory, defective disk or LAN failure. With regards to all failures that can potentially occur, it is necessary to design and package mechanisms for detecting early indications relating to failures, mechanisms for detecting failures that have occurred, mechanisms for notifying persons or systems that need to be notified about the detected incidents, implementations on sections in which failures have occurred, as well as implementations to be performed once failures have been resolved. For example, active or inactive, as well as the stall monitoring of tasks and processes must be performed with a critical processes monitoring mechanism, while automatic rebooting must be in place when processes are down. A function that forcibly shuts down a node and switches over to a standby node, if a process at that node is not resumed after attempting rebooting a number of times (three times, for example) during a prescribed period of time (five minutes, for example), is also available as an advanced function.

Similar monitoring is also conducted on hardware as well. For example, redundant LAN cards (network interface cards; NIC) must be installed with one for current and another for standby network devices, with the standby system sending health check packets to the current system. When a network failure occurs and operation of the current system is interrupt-

[**] More accurately, this is about switching from the current system to a standby system, as well as the comprehensive cutoff and degeneration of all current systems.

ed, the health packet transmitted by the standby system will break off. In such circumstances the NIC of the current system will be deactivated and the IP address assigned to the current system will be assigned to the standby system, while the NIC of the standby system becomes activated (**Fig. 2**, IP failover). An IP failover is usually completed within a few seconds and therefore, failures in the network, such as NIC, will be concealed from communicating parties.

It is possible to shorten the service down time by implementing clusters at multiple nodes. Nodes that configure clusters detect failures by mutually performing health checks. When a node is down (PANIC), an operating system stalled or when a critical process is down the health check process becomes discontinued and the server is separated from the cluster in which the failure occurred (Fig. 2, cluster reconfiguration). It usually takes tens of seconds to a few minutes to reconfigure a cluster. Since rebooting and the recovery of applications takes place after a cluster is reconfigured, a few minutes to tens of minutes of time will be required for services to resume (Fig. 2, node failover). For this reason any failure that involves reconfiguration of a cluster may result in service interruptions that are visible to clients.

The extent to which such service down time can be minimized is a critical issue for the high availability design of dependable IT systems. For example, although the time required to resume services from the time the downing of an operating system (PANIC) occurs at a database node that configures an OLTP system is ordinarily a few minutes to ten minutes, the tolerance value for the service down time can be 60 seconds or less for some systems. Since it is difficult to realize the swi-

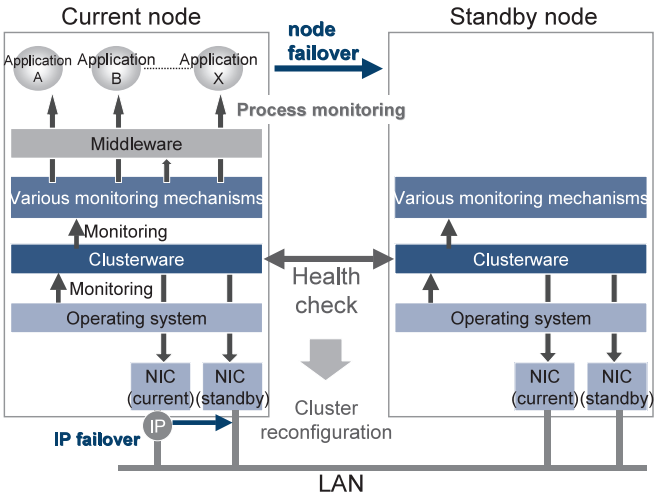

Fig. 2 Cluster structure.

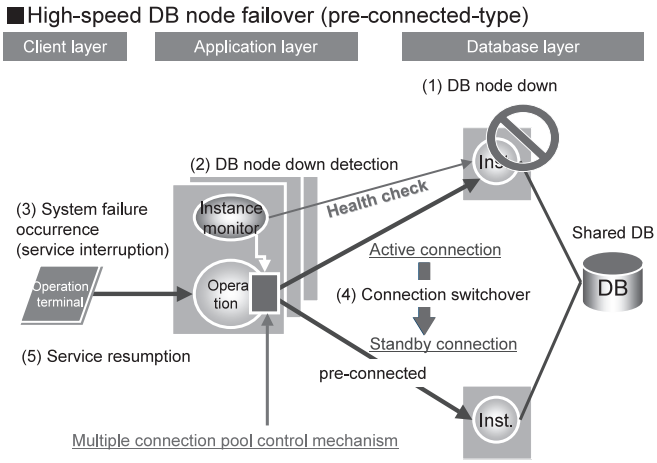

Fig. 3 High-speed database switchover technology using common-type database.

tchover from the current to a standby system using a database node switching technology to meet such requirements, it will be necessary to employ a hot standby technology in such circumstances.

Furthermore, it is also possible to adopt a technology that enables multiple servers to share a single database and then simulate the very same database as both current and standby databases from the application (**Fig. 3**).

There are, however, a number of issues that must be considered for the design of such a package, including:

- Criteria for determining that the current server is down.
- Means to trigger switchovers to standby connections.
- Methods for releasing records (forcibly disengaging remaining locks) that are locked in transactions being processed at the time an application server goes down.

NEC completed the aforementioned high-speed database switchover technology in 2000, which has subsequently been adopted in a number of actual systems. While some products provide a failure detection mechanism in the database layer, the point to keep in mind here is the perspective on whether or not the "database is available for use from the application." On an even further macro level it is possible to monitor the database layer from simulated application programs. However, on one hand the scope of service downs that can be detected becomes broader but on the other hand, the service down time will becomes longer in such circumstances. In order to minimize the service down time as well as to localize the downed service, it is necessary to detect failures on each level of the configuration components, subsystems and overall system, as well as have coordination between the individual detection mechanisms.

Realizing systems with such advanced dependability is difficult using best-of-breed products alone and it would, therefore, be necessary to complement shortages by using middleware (known as "complementing middleware"). NEC has been sequentially commercializing VALUMO-ware products with complementing functions that offer a high degree of versatility incorporated into systems during system building in the field thus far.

In this way, NEC has built large scale IT systems equipped with high reliability safely, surely, and speedily.

VALUMO-ware, related to high availability clusters in particular, have been adopted for the IT systems of customers requiring a high degree of reliability, as illustrated with the SI case example described in Section 2.

5. Conclusion

Even more diversified business models will be created and realized as IT network systems in the ubiquitous society of the future. With such evolution the fusion of IT technologies as well as network technologies will progress and we recognize that dependability more than ever before will be required for critical infrastructures.

Descriptions provided in this paper were primarily based on the concept of dependability for IT systems, as well as relevant building technologies. NEC intends to continue refining the SI technologies, with an emphasis on OMCS, NGN and IT-NW integration solutions in order to promote service businesses that support the ubiquitous society.

References

1) Ministry of Public Management, Home Affairs, Posts and Telecommunications: Information and Communication White Paper http://www.johotsusintokei.soumu.go.jp/whitepaper/ja/cover/index.htm
2) Ministry of Public Management, Home Affairs, Posts and Telecommunications: "YUBIKITASU NETTO SYAKAI NO JITSUGEN NI MUKETA SEISAKU KONDANKAI (Final Report on "Round Table Conference on Policy for Realizing Ubiquitous Society")" http://www.soumu.go.jp/s-news/2004/041217_7.html
3) Arutaki, et al., "DIPENDABURU NETTOWAKU KURITIKARU SISUTEMU KOUCHIKU GIJUTSU (Construction of Dependable Network as Social Infrastructure)," NEC GIHO, Vol. 58, No. 5, pp. 79-85, September 2005. http://www.nec.co.jp/techrep/ja/journal/g05/n05/g050528.html
4) Tomiyama, et al., "Open Mission Critical System Integration Technology," NEC GIHO, Vol. 56, No. 7, pp. 47-50, August 2003. http://www.nec.co.jp/techrep/ja/journal/g03/n07/g030712.html

Authors' Profiles

HIGASHI Kenji
Chief Systems Architect,
Government Community Financial and Career Solutions Planning Division,
NEC Corporation

UWAKUBO Shin'ichi
Senior Manager,
Communications Solutions Division,
Carrier and Media Solutions Operations Unit,
NEC Corporation

YASUBA Hiroki
Staff,
Government Community Financial and Career Solutions Planning Division,
NEC Corporation

●The details about this paper can be seen at the following.
Related URL: http://www.sw.nec.co.jp/solution/omcs/