New Evaluation Techniques for Achieving High Reliability and Availability of ETERNUS Storage System

● Mamoru Komatsu ● Masashi Sakita

(Manuscript received July 10, 2007)

Fujitsu provides storage system products that protect the important data of customers and continue operation, even if any part of the storage system should fail. In developing these products, we have verified the error recovery function by repeating various pseudo-error generation tests in the configurations of customer systems. Through these tests, we can improve product reliability, availability, and the validity of error recovery procedures to be used during operation. Before 2002, all pseudo errors for these tests had been manually generated, resulting in limited coverage. In 2002, however, we developed new evaluation techniques that significantly expanded coverage. This paper describes our work in developing some new evaluation techniques for the ETERNUS series in 2002. These techniques use a test robot called "BBC," error-generating disk drives, and error repetition tests for achieving high reliability and availability.

1. Introduction

Fujitsu has targeted the development of storage system products that protect the important data of customers and continue operation to ensure data integrity, even if any part of the storage system should fail. In developing such products, we have repeatedly conducted various pseudo-error generation tests during the development process. Through these tests, we have verified the error recovery function of the systems including the servers by checking data assurance, continuity of operation, and the validity of error recovery procedures to be used during operation.

Before 2002, all pseudo errors for these tests had been generated manually. This limited the coverage of recovery verification, resulting in the error generation timing and error points not being set for a sufficiently wide range. To address these problems, we proactively developed new evaluation techniques in 2002 that significantly expanded coverage.

This paper describes the new evaluation techniques that we introduced in 2002 for the storage products of the ETERNUS series. These techniques use a test robot called "BBC" (hereinafter referred as BBC test robot), error-generating disk drives, and error repetition tests for achieving high reliability and availability.

2. Importance of verification of error recovery

This section describes the storage system configuration and importance of the verification of error recovery.

2.1 Storage system configuration

The storage system consists of controller modules (CMs: main control printed circuit boards [PCBs] on which the CPU is mounted), disk drives, power supply units (PSUs), and

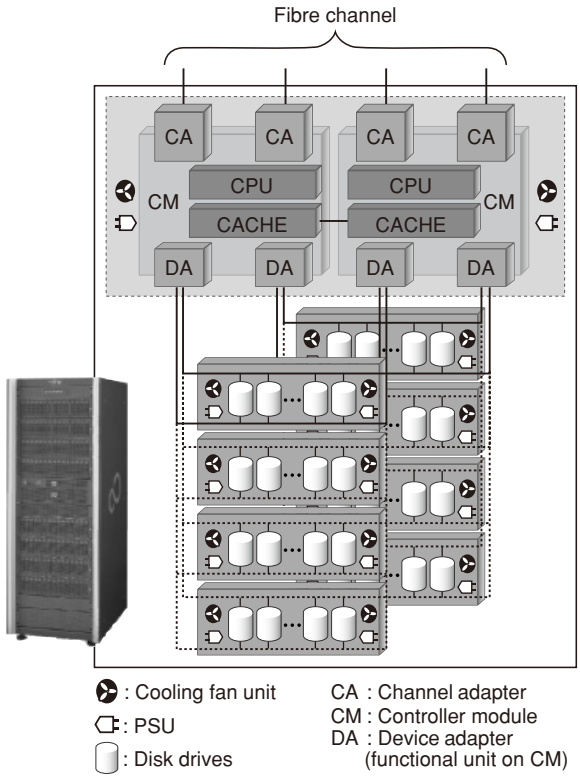


Figure 1
Block diagram of storage system.

cooling fan units. **Figure 1** shows that these components are fully multiplexed to have a redundant configuration. Therefore, even if a channel adapter connected to a server should fail, operation can be continued and the original redundant configuration recovered by replacing the faulty part with a normal part without having to stop operation.

2.2 Preliminary detection of firmware trouble in error recovery

The error recovery function serves an important role should any part of the system break. Firmware for the storage system controls this function. The firmware analyzes the contents of a detected error, identifies the faulty position, and then retries operation or isolates the faulty part from the storage system in order to continue service.

The firmware is designed to ensure recovery from errors in all possible cases of combining the error mode (temporary or permanent hardware error mode) with the timing of error occurrence.

However, a part in an actual storage system may fail in an unexpected error mode or at an unexpected timing, potentially causing firmware trouble.

Such firmware trouble at error recovery for a part failure must be predicted beforehand in the verification process for assuring high quality. For this purpose, the coverage of part error modes and error occurrence timing must be made as wide as possible.

3. Conventional evaluation techniques and related problems

This section describes the limitations of manual evaluation techniques and related problems.

3.1 Manual generation of pseudo part errors

Pseudo errors on each PCB of the CM and other units in the storage system are generated by a technique of inactivating electric signals in the pattern wiring on the PCB.[note)] Such electric-signal inactivation is difficult when the PCB is already mounted in the system. To make such signal inactivation possible, lead wires must be connected to the pattern wiring on the PCB beforehand, and then the PCB must be mounted in the system so that the ends of lead wires are pulled outside the storage system. The electric signals on the lead wires can be inactivated to generate pseudo errors. However, the maximum number of lead wires is limited depending on the workspace, and too many lead wires could cause other circuit errors. To prevent this from occurring, pseudo-error generation points had to be limited to the representative points of each

note) Technique to generate pseudo hardware errors by inactivating electric signals in the pattern wiring

signal. Since pseudo error generation degrades the PCB being tested, the PCB had to be remounted to recover configuration redundancy.

3.2 Manual generation of pseudo disk errors

In addition to the pseudo disk errors generated as previously described, we generated medium errors to a specific block of the disk by using a special command prepared for the disk drive. However, it was difficult to generate pseudo hardware errors, interface errors, and other errors requiring internal disk operation because the disk drives were purchased from vendors.

3.3 Limitations of coverage

Before 2002, we verified the error recovery function by using the manual pseudo-error generation techniques described above in processes ranging from development to evaluation. However, new problems occurred in the part error recovery function during shipment tests conducted at our factory after completing evaluation or during actual service following delivery to customers. In some cases, recovery from pseudo errors was possible in evaluation tests. However, this was not possible in case of actual failure since the error mode was the same, but the timing of error generation was different.

Solving such new problems entailed much additional work time, adversely affected the next development work, and reduced product reliability. Under normal circumstances, such problems should be detected beforehand in the evaluation process. Since pseudo errors had to be manually generated in the past environment, however, widening the test coverage and increasing the repetition count proved difficult because it took too much time.

In view of such background, we needed new, automatic evaluation techniques to provide sufficient coverage efficiently in a short time.

4. New evaluation techniques

To solve the problems described above, we introduced three new techniques involving error repetition tests, the BBC test robot, and error-generating disk drives (**Figure 2**). The following describes these techniques.

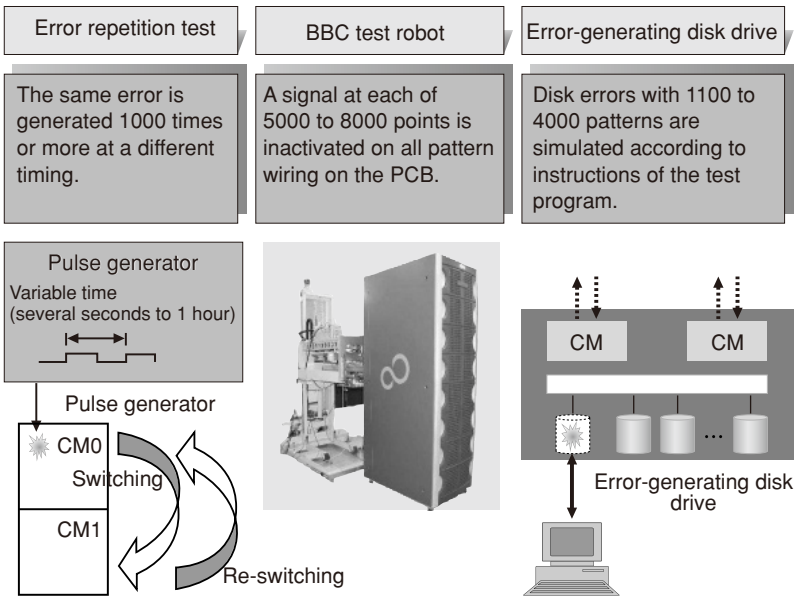


Figure 2
New evaluation techniques.

4.1 Error repetition tests

We developed a pulse generator that could set the electric-signal inactivation time and interval. With this pulse generator, pseudo errors can be generated repeatedly at the same point. Generating a pseudo error in a CM degrades the CM and disconnects all paths from the server to the CM. In such case, the firmware automatically reboots and reconnects the CM, and thus restores the system status held before the error occurred.

This new technique enables a series of error recovery procedures whereby the pulse generator generates pseudo errors during access from the server, the CM is disconnected (degrading the path, but allowing access to continue using another path), then automatically rebooted and reconnected, and the path recovered. This test technique shortened the time period for executing the test 1000 times at one pseudo-error occurrence point to about one-tenth of the previous time period.

4.2 BBC test robot

We developed a tester that could generate a pseudo hardware error by inactivating a signal at each point on all pattern wiring on each PCB mounted in the storage system. This tester is called a BBC test robot. This robot receives the pattern wiring data of each PCB as input data, and then automatically generates pseudo errors in all pattern wiring. This robot can also inactivate signals continuously while changing the error generation time and interval. When this robot is used together with the error repetition test technique (for automatic CM rebooting and reconnecting the server access path) described above, pseudo-error verification can be done automatically for all pattern wiring without having to stop 24-hour verification after the occurrence of one pseudo error.

The technique employing the BBC test robot remarkably improved error occurrence coverage, and largely reduced the test time as compared with the conventional, manual lead wire connection technique.

4.3 Error-generating disk drives

The firmware controls the writing and reading of data to and from a disk drive. If a disk error occurs, the error is posted to the firmware. The firmware then analyzes the error and executes various types of error recovery, such as retrying the command or degrading the disk drive. To execute such error recovery verification, various types of pseudo errors must be generated.

Generating pseudo disk errors by inactivating signals proved difficult, however, since the disk drives were purchased from vendors. To address this problem, we developed a test tool that could simulate the actual disk function and operation. This test tool is called an error-generating disk drive.

The error-generating disk drive consists of a PC and a special adapter. The PC runs a program that simulates disk operation. The special adapter is mounted in the disk slot of the storage system, and operates on the same disk interface. This simulation program can post a medium error, hardware error, or other error in response to execution of a disk write/read command when necessary. In addition, linking the server-side test program with the PC-side simulation program enables control of the disk-error generation timing.

The technique described above enables automatic, continuous disk-error recovery verification in response to all commands issued to the disk drive by linking the error-generating disk drive with the server-side test program.

5. Results of activities to introduce new techniques

These new evaluation techniques were introduced in 2002 for ETERNUS series evaluation.

The verification period was consequently reduced from six to three months, while the number of verification items was increased as

Table 1
Comparison of number of verification items.

Manual evaluation in 2000	
Verification name	No. of verification items
Signal inactivation test	2030
Disk test	200
Total	2230 (1)

ETERNUS evaluation in 2002	
Verification name	No. of verification items
Error repetition test	32000
Automatic pseudo-error test by BBC test robot	5100
Disk test	4000
Total (rate for items in 2000)	41100 (18)

many as 18 times. Both evaluation efficiency and coverage were significantly improved at the same time (**Table 1**).

The ETERNUS series completely passed these verifications, and shipment began in 2002. Compared with previous models, the number of serious cases of trouble in the ETERNUS series at customer sites was dramatically reduced, and these activities for data assurance and high availability yielded impressive results.

We also applied these new evaluation techniques to the previous models. This resulted in a reduced number of serious cases of trouble at customer sites, and largely improved the reliability of those previous models.

6. Further quality improvements

This section describes our activities geared toward making further quality improvements from 2002.

6.1 Introduction from development stage

In ETERNUS series verification from 2002, the BBC test robot and error-generating disk drives were introduced for design verification from the development stage, so as to detect and handle problems in the error recovery function at an early stage. Consequently, the percentage of completed products was already high at the start of evaluation, and necessary processes were strictly retained to ensure high quality.

6.2 Enhancement of error-generating disk drives

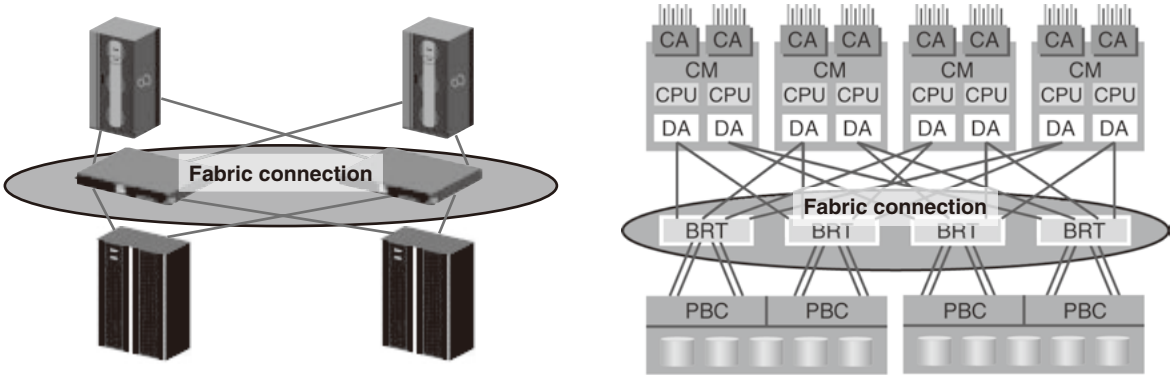
We have verified the disk-error recovery function through firmware by introducing error-generating disk drives and generating various types of errors such as medium errors. However, when a firmware retry command was executed to handle a medium error in disk operation during actual service, an inappropriate error message was sometimes reported or no response made to an error message within the specified time (time-out event).

To address these problems, we added new functions to the error-generating disk drives. Up until that time, an appropriate error message was issued in response to a disk-error recovery command, as well as to an ordinary error-handling command. The new functions allow us to change the time at which to report errors. As a result, the coverage of disk error recovery was expanded.

6.3 Support of new technologies

New technologies have been positively introduced to storage systems for improving performance and functions. Therefore, the evaluation techniques must be able to accommodate these new technologies.

The configuration of a fibre channel interface used for server connection, for example, reflects a recent trend toward connection via a fabric switch, which has been widely introduced. We also used fabric switches for connecting CMs



(a) Connection of servers to storage system

(b) Connection of CMs to disk drives in ETERNUS8000

Figure 3
Fabric connection.

to disk drives for the ETERNUS series developed in 2006 (**Figure 3**). Compared with the conventional loop connection, the fabric connection enables a greater number of connectable lines and a higher transfer rate. The fabric connection also offers the advantage of limiting the range affected by an error. Conversely, the fabric connection poses a problem. Since the interface standard for fabric connection is already defined, a standard for log-in and other processing tasks is not clearly defined. Therefore, log-in operation may fail in some cases because the switches or disk drives are incorrectly connected to CMs.

To detect and solve such problems beforehand, we introduced a pseudo fabric tester that simulated fabric interfaces. We will improve the coverage of error handling, such as the handling of time-outs at log-in.

7. Conclusion

We introduced new evaluation techniques in 2002 for use as standard process techniques for design verification and evaluation. These techniques are now well known to all persons involved in stages ranging from storage product development to shipment.

In the future, the persons involved with the ETERNUS series will carefully consider quality, always detect and handle new problems on an ongoing basis, and proactively continue improvement activities to provide storage products that customers can easily use.

Mamoru Komatsu, *Fujitsu Ltd.*
Mr. Komatsu graduated from Nagano Technical College, Nagano, Japan in 1975. He joined Fujitsu Ltd., Kawasaki, Japan in 1975, where he has been engaged in the quality assurance of global server systems. Since 1987, he has also been engaged in the quality assurance of storage systems.

Masashi Sakita, *Fujitsu Ltd.*
Mr. Sakita received the B.S. degree in Electronics Engineering from Doshisha University, Kyoto, Japan in 1983. He joined PFU Ltd., Ishikawa, Japan in 1983, where he had been engaged in development of firmware for server and storage systems. In 2002, he joined Fujitsu Ltd. in Numazu, Japan, where he has been engaged in the quality assurance of storage systems.