C-019

On-line Divided Diagnosis for High-availability Systems

Yuzuru Maya†

Abstract

The decrease in availability in mission critical systems has become a serious problem due to open source software and commoditization of hardware. Serious failures such as system-down occur during fault recover processing even in the high-availability systems. To solve this problem, I propose an on-line divided diagnosis. This scheme divides high-availability functions into several sub-functions and diagnoses each sub-function in on-line processing. It acquires the system status at the diagnosis of the sub-function. I show that availability can be improved because the proposed scheme suppresses fault occurrence during fault recovery processing.

Keywords high-availability; on-line diagnosis; hot-standby scheme;

1. Introduction

Due to open source software and the commoditization of hardware, the decrease in availability in mission critical systems has recently become a widespread and serious problem. There are increasing examples of high-availability (HA) functions not working normally when a fault occurs.

Thus, in this paper, I propose an on-line divided diagnosis and the data integrated scheme in order to avoid the system-down and improve availability.

2. Proposed scheme

2.1 System configuration and HA functions

HA systems include the dual-system, hot-standby system, and triple modular redundant system. These HA systems make hardware redundant. The software performs fault detection of the hardware, fault recovery, and a re-synchronizing processing for hardware redundancy. These software functions are called HA functions.

2.2 System configuration and HA functions

In general HA systems, the HA function include fault detection, hardware reset, recovery processing, and re-synchronization processing. These functions are classified in hardware processing and software processing.

Therefore, the divided diagnosis scheme divides HA functions into sub-functions (from Sub F-1 to Sub F-n) and diagnoses each sub-function on-line in order not to affect the on-line process even if a fault occurs. Each sub-function uses on-line data or dummy data and is checked to see whether it operates normally, as shown in Fig. 1.

（1） Diagnosis for hardware

The backup unit uses the dummy data in the divided diagnosis scheme. This is the reason that the on-line unit really resets hardware (Ex. CPU and IO) if the backup unit uses the on-line data.

（2） Diagnosis for software

The backup unit uses the on-line data, not the dummy data, in order to acquire the exact system status such as checkpoint data and running AP.

2.3 Data integrated scheme

The data integrated scheme acquires on-line hardware data and software data at the diagnosis of the sub-function. In this way, it can diagnose its own results from widespread operating conditions.

（1） Hardware data and Software data

The hardware data is usage data for CPU, memory, network, and disk. Because of increased load, faults occur easily. The software data is operating data for an operating system (OS), middleware, and AP.

（2） Integrated scheme of hardware and software data

This scheme can diagnoses its own results in more operating conditions by using the on-line data. It can collect operating conditions from the sub-functions and unify them. Therefore, this scheme can improve availability, particularly in critical timing cases.

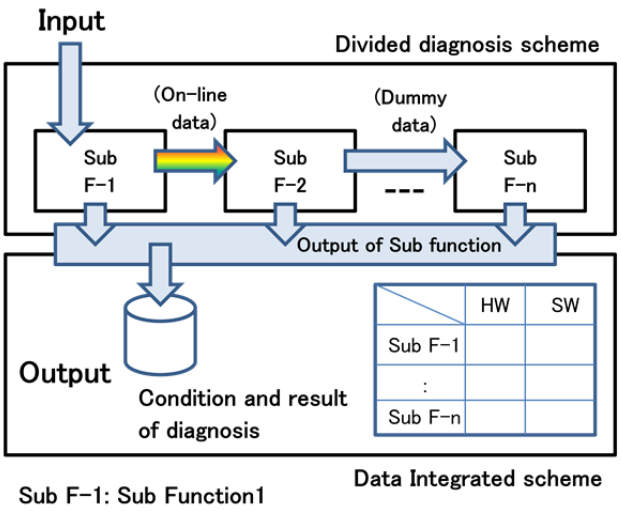

Fig. 1. On-line divided diagnosis scheme.

† Hitachi, Ltd., Research & Development Group, Center for Technology Innovation - Systems Engineering

3． Adaptation to hot-standby system

In this chapter, I adapt the proposed schemes to hot-standby systems in Fig. 2. The hot-standby system consists of the on-line unit, backup unit, and shared disk. I describe a case in which the backup unit diagnoses the on-line unit when a temporary fault occurs in the on-line unit.

3.1 Sub-function and divided diagnosis scheme

The hot-standby function consists of the following sub-functions. This proposed scheme diagnoses each sub-function using the dummy data and the on-line data properly in order not to affect the on-line processing.

（1） Acquisition of checkpoint data (Sub F-1)

The on-line unit sends the checkpoint data to the backup data every few seconds. The backup unit uses the on-line data in the diagnosis.

（2） Temporary fault detection (Sub F-2)

The on-line unit sends "I am alive" dummy messages to the backup data every few seconds. The backup unit receives them and detects temporary faults of the on-line unit.

（3） Reset of fault unit (Sub F-3)

The backup unit sends a dummy reset message to the on-line unit. The on-line unit receives it and checks the reset processing but does not reset the CPU or IO of the on-line unit.

（4） Shared device Switching (Sub F-4)

By using the hot-standby scheme, shared devices of the on-line unit and the backup unit include a shared disk and local area network (LAN). The shared disk and LAN need to be switched at take-over processing temporarily (the back-up unit becomes an on-line state temporarily) and virtually (the back-up unit connects another disk and LAN). However, it runs the processing by using dummy data so as not to affect on-line processing.

（5） Checkpoint re-start (Sub F-5)

The backup unit restarts from the latest checkpoint. It reads write-IO from the IO journal file and updates the state of the file in the state of the latest checkpoint. This scheme diagnoses whether the backup unit can restart in hot-standby systems.

3.2 Consideration

I compare proposed schemes with conventional schemes for initial diagnosis and on-line diagnosis and consider their availability. Table 1 evaluates the proposed and conventional schemes. The proposed on-line divided diagnosis scheme can diagnose the hot-standby function from various conditions by using the operation data on-line. Therefore, even if a fault occurs in the on-line unit, it can avoid a fault in the system switching processing.

On the other hand, the conventional schemes can diagnose HA functions from a part of the state of hardware and software in only the initial test. However, it does not have a function that diagnoses the HA function on-line. It also has a problem with the system shutting down if a fault occurs during the takeover.

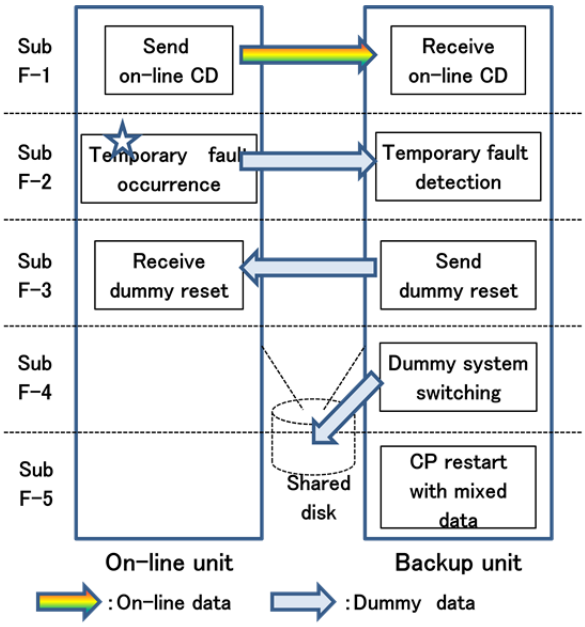

Fig.2. Adaptation to hot-standby systems.

Table 1. Evaluation.

Scheme	Conventional schemes	Proposed schemes
Initial diagnosis	A part of preconditions for diagnosis.	Same as on the left.
On-line diagnosis	Impossible.	Possible.
	(Resets CPU and IO really.)	(No hardware reset due to divided diagnosis)
Availability	Not so high.	High.
	(Only initial diagnosis.)	(Increase diagnosis patterns and extend operation preconditions by on-line divided diagnosis.)

4. Conclusion

High-availability (HA) functions must be diagnosed on-line using online data in consideration of such faults as timing errors. However, the HA function is complicated and its operation depends on the usage of CPU and IO.

Thus, I proposed a scheme to divide the HA function into sub-functions and diagnose each sub-function on-line so that the HA function always works. It acquired detailed hardware and software statuses at the diagnosis of the sub-function. In hot-standby systems, it avoids system-down, allowing the take-over processing to work normally. Furthermore, this proposed scheme is applicable to other HA systems.

References

[1] Algirdas Avizienis, "Bacic Concepts and Taxonomy of Dependable and Secure Computing", IEEE Transaction on Dependable and Secure Computing, vol.1, no.1, pp.11-33, 2004.