Efforts Toward Automation Using TRIOLE

● Kazuo Hajikano ● Toshihiko Hirabayashi

(Manuscript received December 10, 2003)

In today's wildly changing business environment, IT systems must be quickly developed, reliable, stable, and less costly to operate and maintain. Fujitsu's TRIOLE IT infrastructure answers these needs. The core technology for automation of TRIOLE is an autonomous control system. This paper first describes the goals of TRIOLE. Next, it describes the control mechanism for automation, the process loop for autonomous control, and the autonomous sequences of TRIOLE's autonomous control system. Finally, this paper describes future migrations for realizing automation.

1. Introduction

The inevitable move toward enormous, highly complex IT systems for enterprise business requires a huge amount of work for installation, expansion, and dynamic reconfiguration. This leads to the equally enormous problems of rising operating and management costs and longer periods during which business cannot be conducted. These problems not only increase customers' working costs but also increase system suppliers' operating hours.

In order to provide safe and stable operation in mission-critical and social-infrastructure systems, it is essential that systems continue to operate stably when failures and rapid increases in access and data volumes occur.

We propose an autonomous control system that is a key for meeting these requirements. The proposed system does the following:

1) Automatically configures or reconfigures IT systems that comprise servers, storages, and network devices when installing resources (hardware and software), adding resources, and changing the configuration of resources.
2) Provides stable system operation by monitoring and measuring the operating status and utilization of resources and the performance of services during operation.
3) Manages and analyzes the results of monitoring and measurement to identify failures and insufficiencies in resources and then designs and verifies an optimized resource allocation.
4) Automatically adjusts the resource allocation based on the design and verification results with minimal human intervention.

This paper first describes the goals of Fujitsu's IT infrastructure "TRIOLE,"[1] which include making changes to the business environment and IT systems. Then, it describes three key technologies of our proposed autonomous control system: the control mechanism for automation, the process loop for autonomous control, and the autonomous sequences. Finally, this paper looks at the evolutionary steps of autonomous control systems and future migrations of IT systems based on our autonomous control system.

2. TRIOLE in enterprises and an overview of IT systems

2.1 TRIOLE in enterprises

The rate of enterprise integration and diversification and the global re-organization of business are accelerating. Also, to create new business value across a broad range of enterprises, there is a notable move toward business integration and mutual service interaction through mergers, acquisitions, and business alliances. Particularly, with the advance of open systems, the number and scale of distributed systems are increasing to meet the needs of different departments and business applications. This is causing business IT systems to become more complex. Also, because these IT systems are linked via networks, they are growing into enormous enterprise systems. As a result, it is becoming difficult to guarantee the quality of IT systems containing multiple products and isolate problems attributable to those products.

The Internet, with its use of Web services, plays an important role in helping customers expand their businesses, and we have even seen the introduction of an infrastructure for electronic commerce. Also, mission-critical and social infrastructure systems are now required to operate continuously, 24 hours a day, 365 days a year, so that the quality and stability of services are guaranteed.

TRIOLE is a Fujitsu IT infrastructure that meets the following important requirements in business and social activities: business agility; rapid development and deployment of business applications; and stable, reliable systems and reduced Total Cost of Ownership (TCO).

1) Realizing business agility

TRIOLE helps businesses make the best use of their resources. It links systems and develops a complete, optimized IT system that meets the customers' needs for business agility. Also, TRIOLE can be used to expand business and increase convenience by cooperating with Web services and ubiquitous networks.

2) Realizing rapid development and deployment of business applications

TRIOLE applies an application-development framework to mission-critical systems, thereby shortening the construction time of a business system. In TRIOLE, conventional control-logic components that are individually developed as part of a business system are used as standardized common parts in a framework. This approach speeds up application development and system construction and increases reliability during this work. Applications can also be re-used.

3) Realizing stable and reliable systems and reduced TCO

TRIOLE applies autonomous control not only to products themselves but also to the entire system. Its goal is high reliability, from the product level to the system level. Furthermore, with Fujitsu's abundant experience, TRIOLE guarantees the compatibility and quality of the entire system, including Independent Software Vendor (ISV) and Independent Hardware Vendor (IHV) products. This provides a stable and highly productive IT system. Moreover, Fujitsu's Remote Customer Support System (REMCS) helps prevent system trouble by performing prediction monitoring and quickly taking the required action when a problem is identified.

The third requirement is met through TRIOLE's autonomous control system.

2.2 Realizing IT systems with TRIOLE

IT systems are changing at an accelerating rate along with the changes in business environments. Particularly, as the Internet becomes more diffused in society and various means of communication, for example, cellular telephones, PDAs, and PCs, also become more diffused, there will inevitably be a greater realization of ubiquitous networks. A ubiquitous network can be freely accessed anywhere and at anytime to obtain information and use services.

Enterprises consign the operation of their systems to Internet data centers (IDCs), thereby

increasing the need to execute their business through outsourcing. IDCs must provide a variety of services that have a variety of usage and demand conditions. It is important for outsourcing businesses to provide these services at the quality demanded by each business. Utility computing,[2] which is a new technology for IDCs that fulfills these demands, is gaining much attention. In December 2003, Fujitsu started its OnDemand Outsourcing Services, which enables customer to use IT resources, as and when they are required, and then charges them according to the amount of resources they use.[3]

Recently, the technology known as grid computing[4] is being used to realize large-scale processing capabilities through the virtualization and sharing of computer resources dispersed over wide regions. Today, the Open Grid Service Architecture (OGSA) is being discussed in the Global Grid Forum (GGF),[5] which is a standardization organization for grids. The OGSA is being discussed as an architecture that fuses grid computing and Web service technologies such as eXtensible Markup Language (XML), Simple Object Access Protocol (SOAP), and Web Services Description Language (WSDL). In the future, Fujitsu will use the grid as the core technology of TRIOLE and promote grid applications in business.

Of course, it is also necessary to introduce the most advanced technologies to effectively use existing IT assets in IT systems. Particularly, because of the ever-increasing size and complexity of IT systems, reduced TCO and stable system operation are important issues. To solve these issues, an autonomous control system should monitor and measure the operating status of a system's resources and autonomously optimize those resources by analyzing the measurement results with minimal operator intervention. Specifically, an autonomous control system autonomously performs the following.

1) Configures and re-configures a system when installing resources, adding resources, and changing resource configurations
2) Recovers a system from failures and predicts failures
3) Optimizes resources for load variation and predicts performance degradation
4) Constructs and operates IT system environments with advanced security functions

3. TRIOLE autonomous control system

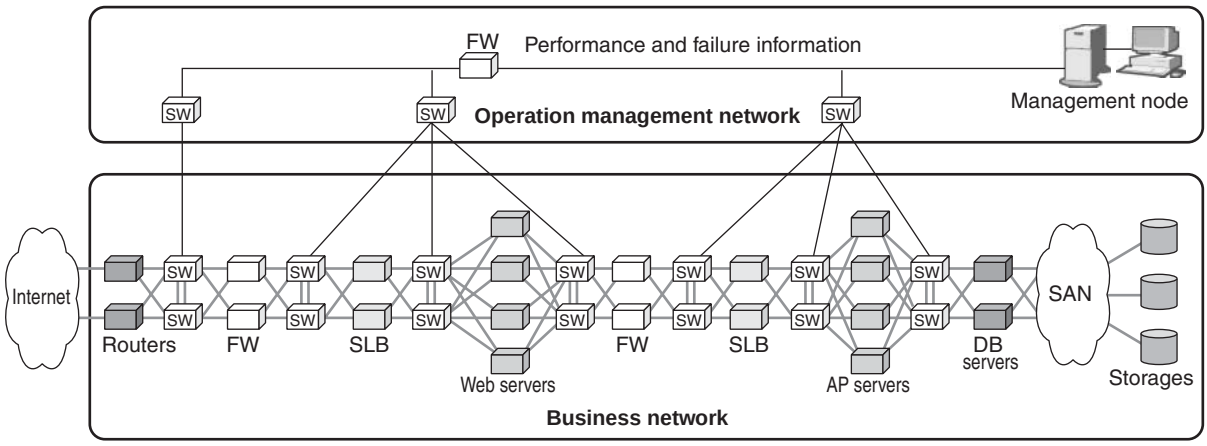
Embedded control mechanisms for automation, a process loop for realizing those control mechanisms, and autonomous control sequences based on the process loop are important elements in an autonomous control system. Sections 3.1 to 3.4 describe our architecture for these three elements. Section 3.5 describes the migration of the autonomous control process loop, and Section 3.6 describes key products for realizing an autonomous control system.

3.1 Application system model

The application system model is applied to systems in enterprise centers and systems in a branch of an IDC that handles IT services. The application system model shown in **Figure 1** consists of a business network with autonomous control-targeted hardware resources and an operation management network for operating and managing them. The business network comprises a three-tiered model for a Web server, application server, and database server. It also includes an Internet system front tier comprising a router and firewall. Note that, for security, the network for the business and the network for operation and management are physically separated or logically separated using VLANs.

3.2 Control mechanism for automation

The autonomous control system is an IT system that ensures continuous and safe operation of a system according to the service level agreement (SLA) so that businesses are not affected by system failures, load variations, and attempts at



FW: Firewall, SLB: Server load balancer, SW: Ethernet switch
SAN: Storage Area Network

Figure 1
Application system model.

illegal access. It does this by monitoring the status of resources and services over the entire system. Fujitsu has defined the following four control mechanisms as the configuring elements for automation: configuration control, failure recovery control, resource optimization control, and protection control (**Figure 2**). Failure recovery control and resource optimization control act based on the configuration control. Protection control must be installed in each control mechanism and can be found in all locations of the system.

3.2.1 Configuration control mechanism

This mechanism recognizes the status of the system resource configuration and sets resources as necessary. This enables dynamic handling of changes in the system configuration. The functions of this mechanism are outlined below.

1) Integrated management of system configuration

This mechanism manages the configuration of the entire system, including shared resources, and displays it as required by an operator. The distributed type control method is used to manage resources at the node level for each server, storage, and network device. With management nodes, it is possible to manage resources over the

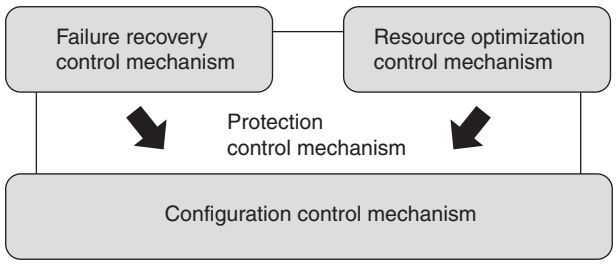


Figure 2
Autonomous control mechanism.

entire system, manage the relationships between nodes and between resource types, and understand the management of relationships between services managed on the system and resources. With this mechanism, a system can be optimally configured for the services it delivers.

2) Pooling of resources

This mechanism manages the spare resources of servers, storages, and network devices as resource pools. By allocating resources from the pools when resources are needed and returning excess or unneeded resources back to the pools, this mechanism ensures that spare resources are used efficiently in the system or center.

3) Automation of installation and re-organization by automatic recognition

This mechanism automatically recognizes the system configuration when installing

resources, adding resources, and changing their configuration. Also, it autonomously re-organizes resources that satisfy the capacity and performance required based an operating policy. For example, when adding server nodes from a pool, the management node analyzes information relating to the settings and operation of the server node targeted for application. After obtaining nodes from the server pool, it verifies the configuration of the corresponding server, storage, and network devices. If no problem is found in the verification of each configuration, this mechanism determines the optimal resource allocation for the entire system (including the added nodes), sends the configuration information to the peripheral nodes, and changes the settings of the resources.

4) Dynamic changes of the control program

This mechanism has two sets of the control programs (e.g., the OS and firmware). When a new version of a control program is installed in the standby side, this mechanism can instantly switch from the working side to the standby side; thereby making it possible to upgrade control programs without affecting services.

5) GUI settings

This mechanism enables remote acquisition and setting of system configurations.

3.2.2 Failure recovery control

This mechanism monitors the resource failure status and operating status. When a failure is detected or predicted, it substitutes the affected resources with alternative resources to recover the system or prevent trouble. Also, if there are no usable substitute resources, it isolates the failed resources and degenerates to continue system operation. This makes it possible to minimize the amount of system damage that occurs. The functions of this mechanism are outlined below.

1) Identification and visualization of locations of failures and range of effects

Based on the failure information, this function identifies failed resources in the system configuration and determines the range of effects (the affected area in the physical configuration and the affected range at the business level).

2) Dynamic degeneration of failed resources and automatic switching to alternative resources

When a failure is detected, if there is a redundant configuration, this function switches to alternative resources. However, if there are no alternative resources, this function acquires corresponding resources from the resource pool and switches over to them after making the necessary settings. Also, this function isolates failed resources from the system.

3) Failure prediction monitoring control

This mechanism isolates from the system the resources that are predicted to fail as a result of comparative analysis of error information and thresholds from each resource and switches to alternative resources.

3.2.3 Resource optimization control

This mechanism monitors changes in the utilization of resources, adjusts resource allocations, and dispatches resources from shared resources. It improves the utilization of the system. The functions of this mechanism are outlined below.

1) Adjustment control based on resource usage rates

This mechanism constantly monitors the resource utilization, resource allocation status, and performance of the system. It improves the load balancing and efficiency in the entire system to stabilize the system by adjusting the current resources, allocating resources from the resource pool, and returning resources to the resource pool.

2) Knowledge of resource utilization

By analyzing the record of resource utilization, the autonomous system forecasts load transitions and suggests the most appropriate measures to take before system performance is degraded.

3) Load prediction monitoring control

This mechanism continuously monitors the use status of the resources and the allocation

status. It also prevents system trouble by optimizing the arrangement of resources when it is predicted they will fall below the minimum performance level described in the SLA.

3.2.4 Protection control

This mechanism prevents improper operations and protects against illegal processes from both inside and outside of the system. It ensures that the system operates stably. The functions of this mechanism are outlined below.

1) Prevents operating and setting mistakes

This mechanism cumulatively manages the logs of operating and setting mistakes, checks compatibility when operations and settings are made, and compares logs. If this mechanism detects that the operator has issued an instruction to execute an incorrect operation or setting, it prevents its execution and warns the operator.

2) Notification and protection against illegal processes from inside and outside the system

This mechanism detects and analyzes illegal processes from inside and outside the system (e.g., access, usage, viruses, and attacks). It determines how to handle these processes based on operating policies from the results of the analysis and automatically changes the security settings. This mechanism autonomously improves the protective power of the system. Particularly, with regard to providing an autonomous control system, this mechanism initializes resources to prevent leakage of information when returning resources to the shared pool. Also, by physical separation or VLAN-based logical separation between the operation management network and the business network, this mechanism guarantees security of shared resources. Also, this mechanism requires operator authorization to prevent illegal access. Moreover, integrated operation management such as unified management of security events and application status management of security patches are provided.

3.3 Process loop for autonomous control

It is important to apply autonomous control not only for products, but also for the entire system to optimize resources from the product level to the system level; that is, from partial optimization to total optimization. An autonomous control must be considered not only as a process loop for each node of the servers, storages, and network devices, but also as a process loop that autonomously controls resources and operation management across multiple nodes over the entire system. Through these process loops, an autonomous system realizes the configuration control, failure recovery control, resource optimization control, and protection control described above.

An autonomous control process loop is composed of four basic phases: monitoring and measurement, analysis, design and verification, and operation (**Figure 3**). As can be understood from the figure, in the execution of the process loop, all four of these phases can be executed sequentially or just the two phases of monitoring and measurement and operation can be executed sequentially. For example, analysis and design and verification are necessary to optimize resources by allocating them from the pool and cover the four phases. However, on redundant devices, when there is a demand for high-speed restora-

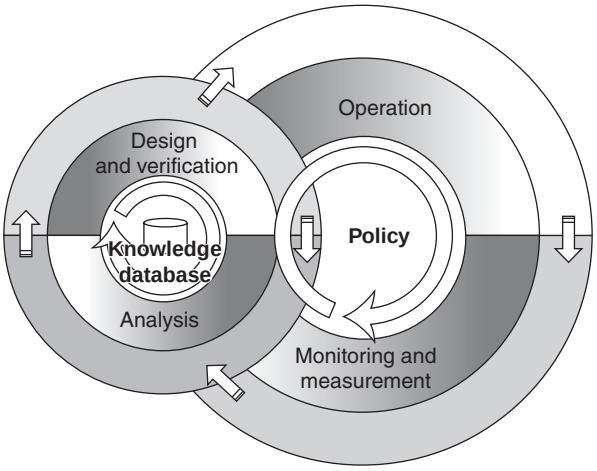


Figure 3
Autonomous control process loop.

tion such as for hot-standby switching, only the two phases of monitoring and measurement and operation are executed. Note that this process loop uses a policy as its base and references and updates the knowledge database in the analysis and design and verification phases. The following describes each phase.

The monitoring and measuring phase mainly monitors the resource configuration and failures and measures the performance of the resources. This phase monitors the configuration and performance of servers, storage devices, networks, middleware, and services and makes them visible. Also, this phase displays failure locations when a system failure occurs and performance measurement results when the performance falls below a specified level.

The analysis phase mainly estimates resource amounts to maintain the service level using the above monitoring and measurement results. When a failure occurs, this phase locates it and analyzes its cause according to the failure information and identifies the range of its effects. When the performance is degraded, this phase identifies the bottleneck and its effects on other locations according to the performance information. Also, based on the monitoring and measuring results, this phase predicts failures and traffic loads. Based on the results of these predictions, this phase determines the required amounts of resources according to policies. It also displays the results of the analyses of failure and load predictions.

The design and verification phase mainly adjust resources according to the aforementioned analysis results and policy. First, it displays improvement proposals for resource reallocation and simultaneously verifies the system configuration according to those proposals. Then, if the verification results are acceptable, it determines the new resources available for services and makes new designs that include changes to the settings of peripheral resources related to the resources that have been added.

The operation phase mainly configures or re-configures the system by 1) distributing, installing, or upgrading firmware, OSs, middleware, and applications for each device and 2) distributing or applying patch files when installing resources, adding resources, and changing the configuration of resources based on the design and verification results.

The following section describes how the four process phases are executed in each autonomous sequence. These sequences include not only installation, addition, and resource configuration change, but also failure recovery and optimum resource allocation.

3.4 Autonomous control sequences

The autonomous control system consists of an automatic configuration block and an autonomous control block. **Figure 4** shows the relationship between the automatic configuration block and the autonomous control block from the viewpoint of the process loop phase and its usage pattern. The automatic configuration block automatically configures or re-configures the system when installing resources, adding resources, and changing the resource configuration. It also automatically changes the system configuration by using resources pooled according to the load variation and failures in order to perform dynamic provisioning. The autonomous control block monitors and measures the operating status and predicts failures and performance degradations through analysis based on the operating status information. Then, it prevents failures and performance trouble by instructing the automatic configuration block to make configuration changes based on the verification of the system layout.

Figures 5 to **7** and **Table 1** show the general concepts of the sequences used to install resources, add resources, change resource configurations, optimally allocate resources, and recover from failures. For example, in the installation, addition, and change configurations sequence, automatic generation from the logical

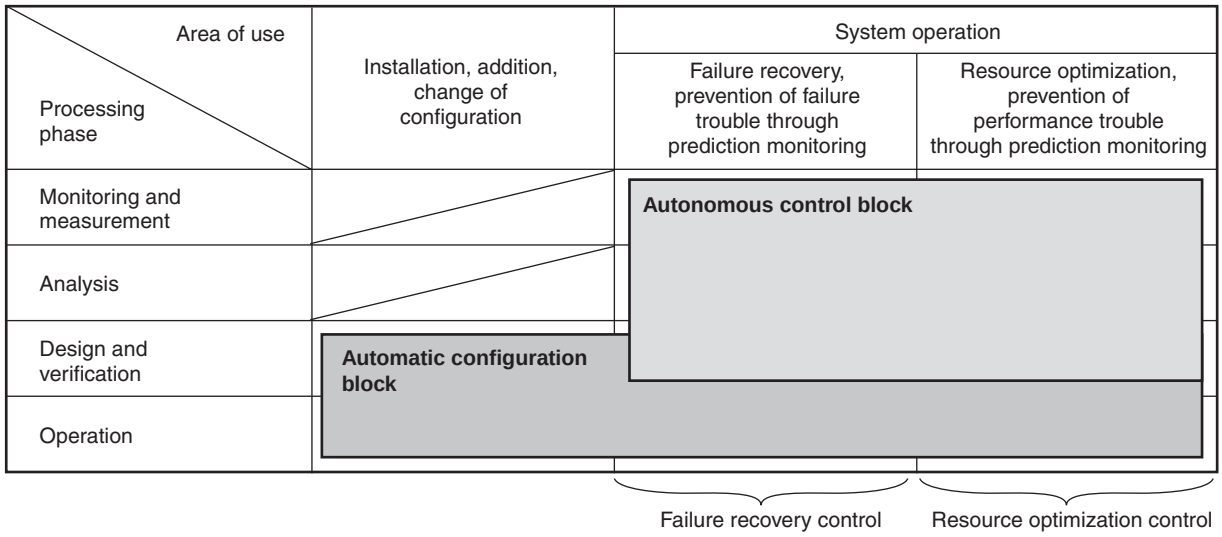


Figure 4
Autonomous control system.

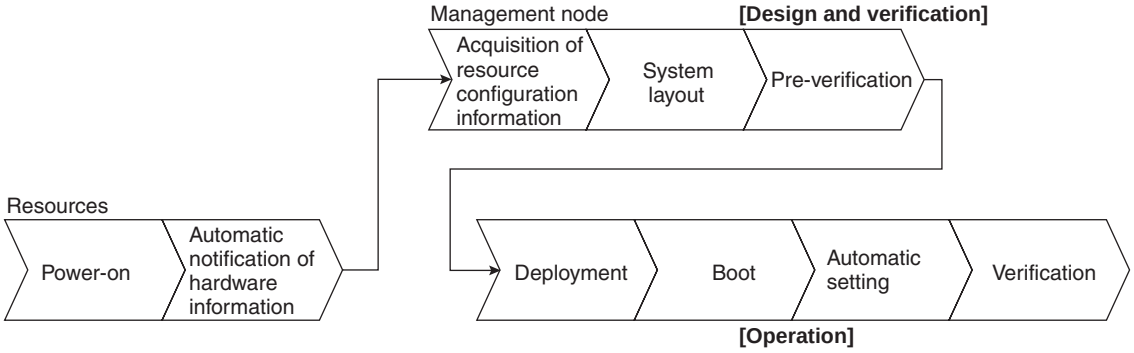


Figure 5
General concept of installation, addition, and configuration change sequence.

system to the physical system (system layout) and pre-verification of the system layout using a simulation (connectivity verification) are performed in the design and verification phase. In the subsequent operation phase, the OS and firmware are booted, the application and settings information is automatically set, and the system layout is verified before starting in-service operations using test data (network topology discovery).

This section describes the operating concept of the system layout, connectivity verification, and network topology discovery.

3.4.1 System layout

The system layout allocates the physical devices and sets the routes between the devices according to the logical system, which is the design format of the platform that describes the requirements for the system to be configured to automatically generate the physical system. The allocation and setting of physical devices (hardware) in the IT system and the arrangement and setting of software in each physical device are described in the physical system. When configuring the physical system, it is important to consider how to meet the requirements of the logical system using the available physical devices and their interconnection relationships. The system layout identifies these requirements, starting with the one that is hardest to achieve. If multiple candidate layouts satisfy a logical system condition, the system layout searches a data table that describes

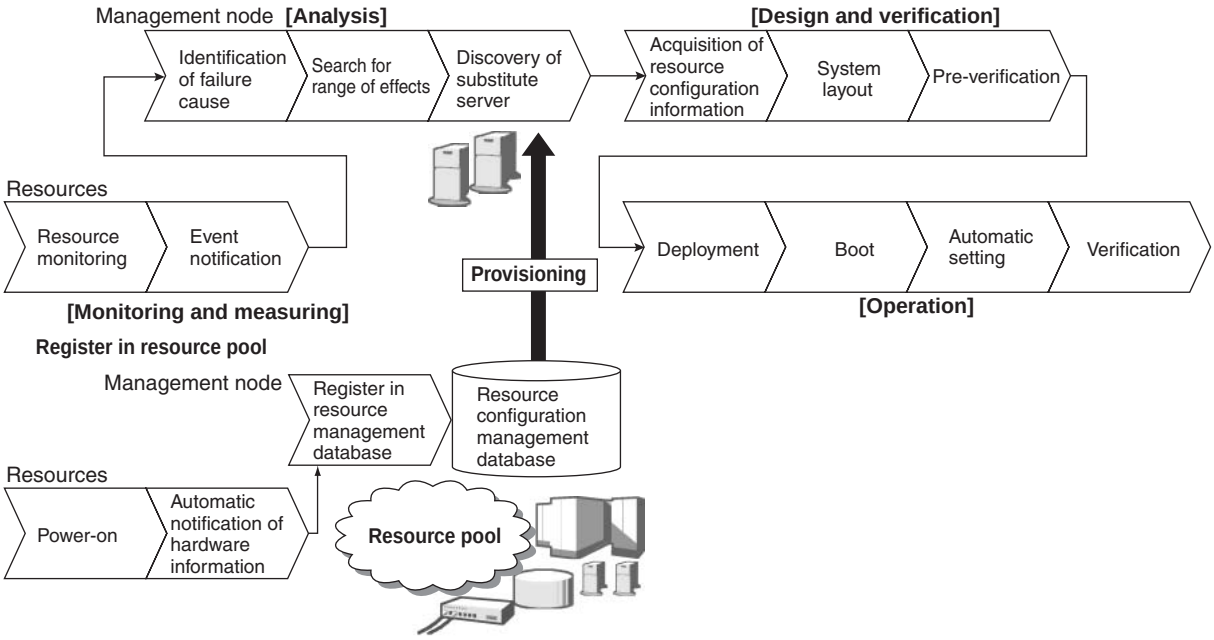


Figure 6
General concept of failure recovery control sequence.

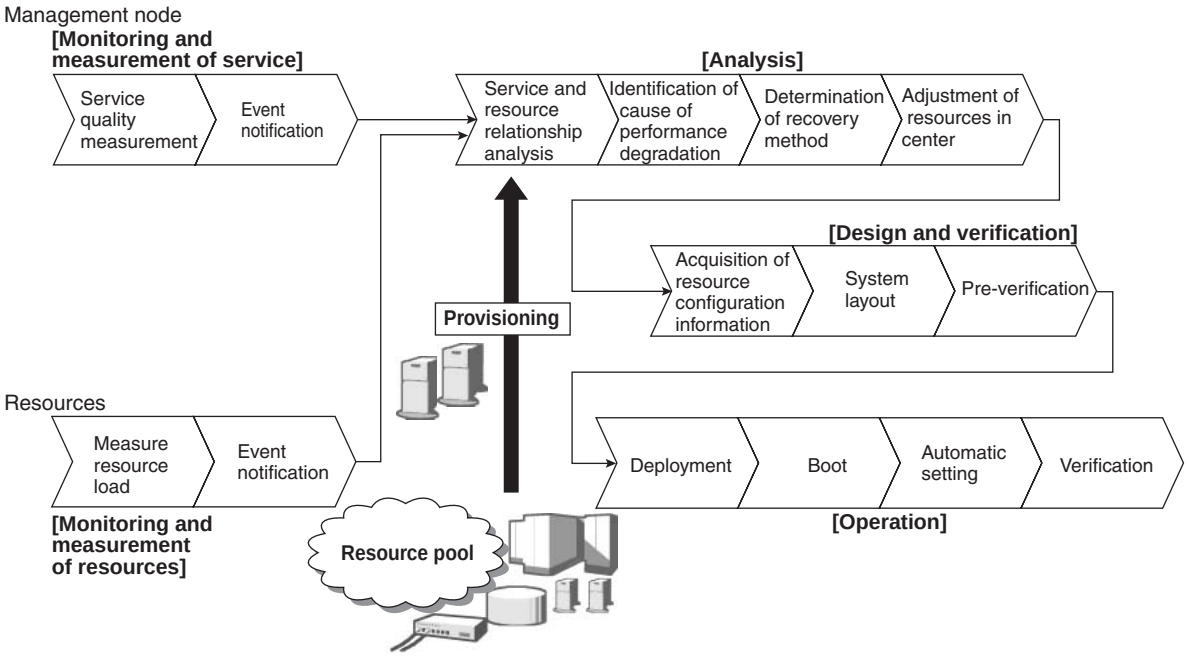


Figure 7
General concept of resource optimization control sequence.

Table 1
Summary of each sequence.

	Installation/addition/reconfiguration	Failure recovery	Resource optimization
Monitoring and measurement		• Monitoring and measurements necessary to identify locations of failures and ranges of effects. • Monitoring and measurements necessary to identify possibility of failures.	• Measurements necessary for optimizing resources. • Measurements necessary for identifying possible trouble due to load variations.
Analysis		• Analyze and specify whether there are breakdowns or failures in resources based on reported failure information. • Compare to analyze error information of each resource and thresholds to predict breakdowns and failures (analysis of failure prediction).	• Analyze performance bottlenecks from the results of measurements of resource use status and service performance status, and determine necessary resource amounts. • Predict trends in loads and performance from accumulated measurement results, and determine necessary resource amounts (analysis of load prediction).
Design and verification	• Acquire resource configuration information. • Automatic generation of physical system from logical system (system layout). • Preverify system layout by simulation.	• Design and verify according to the following based on analysis results: - Switch to substitute resources. - Cut failed resource if there are no substitute resources, and degenerate. • Design and verification procedures are the same as described at left. • Specify configuration change based on results of design and verification.	• Design and verify according to the following based on analysis results: - Adjust resource distribution. - Allocate resources from resource pool. - Return resources to resource pool. • Design and verification procedures are the same as described at left. • Specify configuration change based on results of design and verification.
Operation	• Distribute firmware, OS, and applications; configure; and set information. • Boot OS and firmware, automatic setting of applications and setting information. • Verify system layout before operating using test data.	• Operate resources according to configuration change directions. • Operating procedures are the same as described at left.	• Operate resources according to configuration change directions. • Operating procedures are the same as described at left.

the evaluating points of each candidate and selects the one with the most evaluation points.

3.4.2 Connectivity verification

Connectivity verification is done when the topology must be reconfigured due to failures or load variations. Before a reconfiguration is implemented, the proprieties of a system layout are verified by modeling the topology of an actual system composed of network devices and interconnecting links and simulating changes in the paths on each layer from the physical level to the service level. We are currently studying three stages using simulations. Operations on an actual system can be guaranteed by performing these simulations in advance. The three stages are:

1) Simulation of path cut-off

This stage models the path control protocols of layers 2 and 3 and simulates changes in paths caused by cut cables and node failures.

2) Simulation of redundant switching

This stage models switching operations for redundant devices and simulates path changes after the devices have been switched.

3) Simulation of additional devices

This stage models application protocols and simulates path changes of service levels when devices such as load balancers and network address translators (NATs) are added to an IT system.

3.4.3 Network topology discovery

Network topology discovery automatically creates the system topology, including the network configuration and paths, by 1) flowing test data for searches in a network at installation or before operation and 2) collecting the necessary information from each network device. The conformity of the system layout can be verified by comparing the created system topology with the physical system topology. With conventional means, it is only possible to create logical connection relationships of the IP levels (layer 3). However, with this topology search, the physical connection relationships and the service levels can be searched by collecting information using the following two methods:

1) Topology discovery of the physical level (layers 1 and 2)

This method acquires data tables directly from network devices and acquires the physical connection relationships between devices by sending search packets.

2) Topology discovery of the service level (layers 4 to 7)

This method identifies the configuration of the service level by extracting the routes of each application protocol by acquiring and analyzing the management information base (MIB) and policy tables in the devices.

How to implement the autonomous function in the four process phases of the autonomous control system is an important issue. The following outlines our scenario for migration to autonomous functions.

3.5 Migrations of automation

Fujitsu will realize the evolution (stages of development) of an autonomous control system through three steps (**Figure 8**).

The first step supports manual operations. It involves monitoring and measuring the operating status, visualizing the results, and executing operations based on the operator's indications in the autonomous control system. The operator analyzes the operating status based on the results of the monitoring and measuring. Then, the operator designs and verifies a system re-configuration and instructs the system operations to eliminate problems.

In the second step, an automatic operation function and an operation suggestion function are embedded in the autonomous control system. The automatic operation function operates according to an operating policy based on the results of

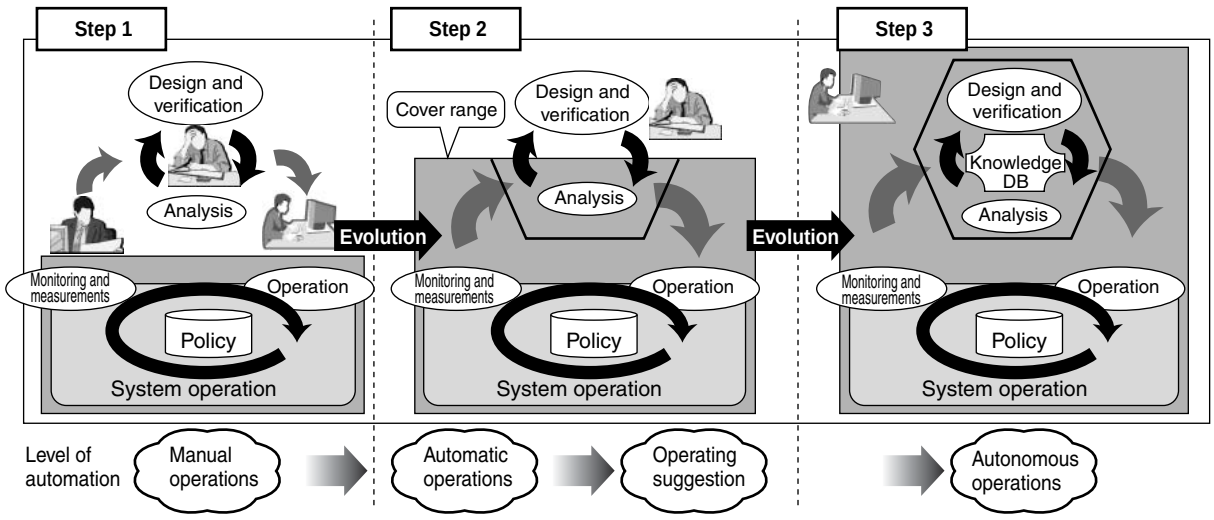


Figure 8
Migrations of automation.

monitoring and measuring. The operation suggestion function provides suggestions about the possible causes of failures and performance degradations by analyzing the results of monitoring and measuring. In the automatic operation phase, the operator defines conditions such as threshold values that are set for the monitoring and measurement and the operations to be executed when the conditions are met. In the operating suggestion phase, the operator designs and verifies a system re-configuration based on these suggestions to eliminate problems.

In the third and final step, the autonomous control system uses a function for autonomously analyzing, designing, and verifying based on the results of the monitoring and measurement and the contents of the knowledge database. Normally, with this autonomous function, the operator only needs to monitor the operating status.

As describe above, of the four phases in the process loop of autonomous control, the monitoring and measuring phase and the operation phase will be implemented first, because they are the basic phases that support automation. On the other hand, functions for establishing analysis technologies based on knowledge and know-how, installing devices and business application configuration databases, and completing databases containing accumulated field know-how are essential in the analysis, design, and verification phases. Fujitsu will add these functions to the autonomous control system step by step.

3.6 Products for realizing an autonomous control system

To realize an autonomous control system, it is necessary to optimize mechanisms from the viewpoint of the overall system. We apply the autonomous control mechanism not only to IT hardware resources such as servers, storages, and network nodes, but also to middleware. We can realize integrative management of resources and service quality and control them automatically by applying the mechanism to middleware. The core products for realizing automation of an IT infrastructure in this mechanism include the Resource Coordinator and the Service Quality Coordinator (**Figure 9**). The main functions of these two

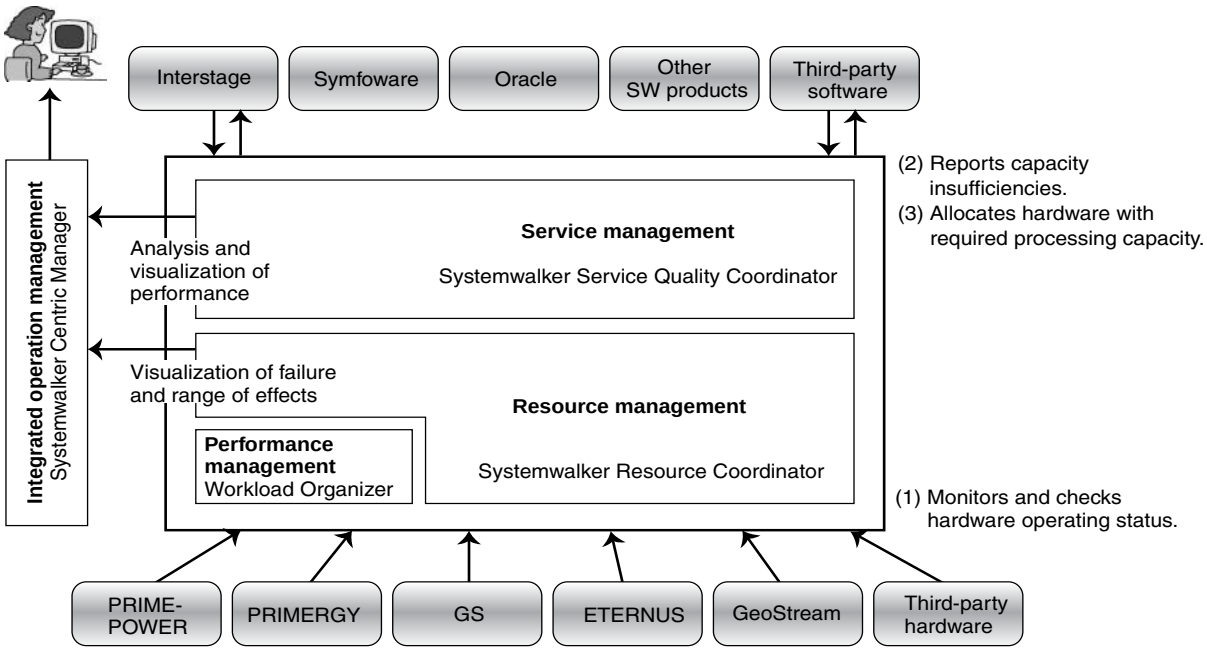


Figure 9
Products composing the autonomous control system.

products are as follows:

1) Resource management: Systemwalker Resource Coordinator[6)]
- Visualization of component failures and range of effects in the IT infrastructure
- Autonomous recovery by event delivery function between AP and DB servers
- Efficiency of installation and development and speedy reconfiguration by configuration management and automation of setting work

2) Service management: Systemwalker Service Quality Coordinator[7)]
- Autonomous notification of whether the IT infrastructure configuring a service is operating as expected
- Speedy analysis of causes in service quality degradations
- Support of optimized resource control according to service level analyses

4. Future migrations to IT infrastructures

We will now describe a migration of the TRIOLE IT infrastructure that is performed when applying an autonomous control system equipped with the automated functions provided in the steps outlined in Section 3.5.

In the first step, the autonomous control system monitors the logical relationships between resources and services or business applications by viewing the resource configuration and the locations of failures. This step enables an operator to grasp the range of effects on services caused by failures in the IT infrastructure.

In the next step, the autonomous control system provides efficiency and stability in services and business applications by applying a dynamic provisioning that optimizes the resources according to the failures and load transitions occurring in the IT infrastructure. The autonomous control system also prevents trouble by predicting failures and performance degradations with minimal operations.

Finally, in the third step, we aim to provide high-performance and quality in services and business applications in the IT infrastructure by introducing autonomous functions based on SLAs and policies without operator interventions. We are also working toward the realization of next-generation IT systems such as utility computing systems and grid computing systems by optimizing the resources across an entire network of enterprise systems or IDCs.

5. Conclusion

This paper described the aim of Fujitsu's IT infrastructure "TRIOLE," the architecture (control mechanisms for automation, process loops for autonomous control, and autonomous sequences) of the TRIOLE autonomous control system, and future expansions of automation. The autonomous control system automatically configures or re-configures an IT system when installing resources, adding resources, or changing the resource configuration. Furthermore, the operating status and performance of resources are monitored and measured during operation. The results are managed and analyzed to identify failures and resource insufficiencies and then design or verify an optimized system arrangement. Finally, the autonomous system can automatically adjust IT resources based on these results with minimal human intervention. The application of an autonomous control system reduces operating management costs and realizes stable operation of an IT system.

References

1) TRIOLE White Paper. *http://www.fujitsu.com/services/solutions/triole/whitepaper/index.html*
2) M. Adachi and H. Orikasa: Utility Computing Technology for IDC Operation. *FUJITSU Sci. Tech. J.*, **39**, 2, p.175-181 (2003).
3) OnDemand Outsourcing Services. *http://fenics.fujitsu.com/service/os/ondemand*
4) Grid Computing. *http://triole.fujitsu.com/jp/grid/index.html*
5) GGF. *http://www.gridforum.org/*
6) T. Hirao and T. Abe: Resource Management. *FUJITSU Sci. Tech. J.*, **40**, 1, p.123-132 (2004).

7) K. Ishibashi and M. Tsykin: Management of Enterprise Quality of Service. *FUJITSU Sci. Tech. J.*, **40**, 1, p.133-140 (2004).

Kazuo Hajikano received the B.E. and M.E. degrees in Electronics Engineering from Waseda University, Tokyo, Japan in 1978 and 1980, respectively. He joined Fujitsu Laboratories Ltd., Kawasaki, Japan in 1980, where he has been engaged in research and development of broadband switching systems. Since 1992, he has been with Fujitsu Ltd., also in Kawasaki. He is currently a director of the TRIOLE Business Development Division and is responsible for the business strategy of TRIOLE in the global market.

Toshihiko Hirabayashi received the B.E. degree in Information Engineering from Keio University, Yokohama, Japan in 1983. He joined Fujitsu Ltd., Kawasaki, Japan in 1983, where he has been engaged in development of network software. Since 2003, he has been engaged in planning and development of the TRIOLE autonomous system in Fujitsu Ltd.