computing@tanet.edu.te.ua
www.tanet.edu.te.ua/computing

ISSN 1727-6209
International Scientific
Journal of Computing

AUTONOMOUS DECENTRALIZED DATA CONSISTENCY FOR HIGH-ASSURANCE EMBEDDED SYSTEM

Akio Shiibashi [1], Kinji Mori [2]

[1] East Japan Railway Company, 2-2-2 Yoyogi, Shibuya-ku, Tokyo 151-8578 Japan, shiibashi@jreast.co.jp
[2] Tokyo Institute of Technology, 2-12-1 O-okayama, Meguro-ku, Tokyo 152-8252 Japan, mori@cs.titech.ac.jp

Abstract: *Advancement in computer and communication technologies have resulted in an explosive growth in embedded systems. The market and users requirements have been rapidly changing and diversified. Under these evolving situations, the assurance to keep the continuous system operation of embedded systems is becoming more and more important. The Autonomous Decentralized System (ADS) has been proposed for resolving the on-line property to achieve the step-by-step expansion, maintenance and fault-propagation prevention for high assurance. This architecture is effective to improve the reliability and reduce the development cost and product cycle time to market by data-driven mechanism. The technologies have been applied in the IC card system for train fare collection and its effectiveness has been proven.*

Keywords: – *embedded system, ADS (Autonomous Decentralized System), assurance, fault-tolerance, expansion, maintenance*

1. INTRODUCTION

Distributed embedded systems with multiple processing elements are becoming common in various application areas ranging from multimedia to robotics, industrial control, and automotive electronics. Heterogeneous distributed architecture is required for such systems, where several processors, application-specific integrated circuits (ASIC), and field-programmable gate arrays (FPGA) are interconnected by various types of communication links, and multiple tasks are concurrently run on the system. Each task can be executed on a variety of software and hardware platforms with different costs [1][2]. In addition, the markets have been expanding rapidly and user's requirements have been diversified and varied. However, the conventional architecture is either overdesigned or fails to meet the specified constraints. Therefore, it is important to find an effective architecture to meet the heterogeneous requirements of hardware and software under this dynamic changing. As the breakthrough over the conventional systems, Autonomous Decentralized System (ADS) has been proposed in 1977 [3]. An autonomous decentralized system is defined as such a living thing, which is composed of largely autonomous and decentralized components (subsystems). Their technologies have been developed in the various fields of transportation, factory automation, utility management, satellite on-board control, newspaper printing factory, information services, e-commerce, community service, and so on.

In this paper, the ADS concept and technologies are discussed and their applications to "Suica," the IC card system for train fare collection, are shown to be effectively operated.

2. BACKGROUND AND REQUIREMENTS

In the following years, the information technology will be strongly marked by the presence of embedded systems. Such systems are typically application specific systems containing software, hardware and communications channels tailored for a particular task. Nowadays, embedded systems are presented in almost all electronic devices even they are hardly noticeable. There exists a large variety of applications and functionality in which they are applied. In control systems, Program Logic Controllers (PLC) have been used for controlling processes such as temperature, mixture, position, and velocity in critical industrial systems. In consumer products, many further enhancements and numerous new home control, kitchen appliances and white-good products have been designed based on sensor/actuator signal processing by embedded systems. Mobile phones depend heavily on the use

of standards implemented in embedded systems. In other professional areas like traffic control, car navigation, train control, plant control, etc., embedded systems can realize the functionality that cannot be provided by human beings (Fig.1) [4][5].

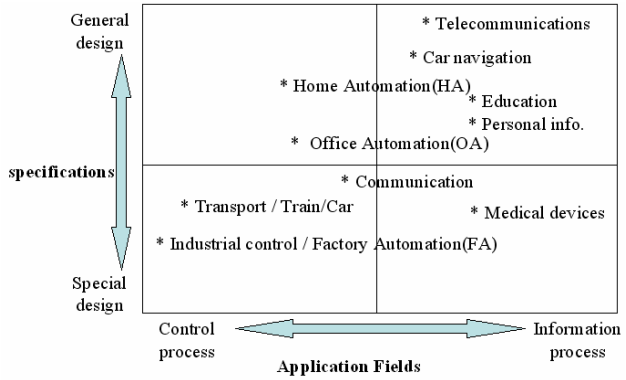


Fig.1 – Applications of Embedded System

In a beginning, embedded systems had been designed for satisfying a specific task or functionality in a single device. However, with the constant advance in the IT and the solution they provide while meeting a lot of constraints, the pervasion of embedded systems was derived. The possibility to share an embedded systems platform over many different applications in a domain makes them very attractive. For example, in home automation, a large extent specific hardware and/or software components, even for high-volume consumer-electronics applications, are connected in a network system in order to provide the functionality for living that each person is demanding. In this sense, gradually our society is becoming dependent on the proper functioning of embedded systems [6].

The embedded systems are characterized by the four properties: Heterogeneous, Complex, Flexible, and Communicative. Heterogeneous (software, hardware, mechanical components, optics, etc.) Embedded systems of various technological areas are designed under different hardware and software (Linux, Windows, Tron, etc.) platforms. Complex (real-time requirements, low power, low cost, reliable, etc.) Embedded systems are mostly reactive systems, that is, they react continuously to their environment at a speed imposed by the environments which lead often real-time capabilities. Low power and low cost are an inherent requirements for embedded systems. Reliability, robustness and safety constraints derive from situations where service continuation is impossible. Flexible (time-to-market, personalized, online maintenance, online testing, etc.) The time for the design and commercialization of an embedded system have to be done considering that the users requirements that derive from general trends in society related to aspects like individualization, globalization, mobility, fashion, etc., are always changing. Increasing individualization leads to more diversity in products and services, and therefore to the need for more flexibility in design. Growing needs for continuous service utilization and provision leads to online maintenance and testing. Moreover, exponential size increase continues in the embedded systems. Communicative (networked, connected, sensors and actuators, etc.) Most of the current embedded systems are connected through a network and it is expected that in the future Internet plays also an important role. Sensors and actuators are also inherent components of embedded systems.

The increasing heterogeneity in software and hardware will require shifting to open standards. For example, Linux, an open-source operating system is garnering acceptance in the embedded world, multipurpose microprocessors are more likely to be used, etc.

In contrast with interactive systems that respond to external stimuli when they are ready with calculating their response at their own pace, embedded systems reactivity imposes often real-time capabilities. This results in special requirements for the hardware and software architecture of the platform to be used in which more decentralized control is required. Reliability, robustness and safety constraints derive from situations where service continuation is impossible and a certain degree of adaptive behavior, self-configuring and self-restoring should be possible.

The time-to-market is one of the major requirements that embedding systems have to override by shortening it. Current hardware/software design and integration technologies must be developed in order to cope with such challenges. The individualization in the users preferences will force that the new embedded systems must be designed under the metrics of collaborative adaptive systems. The non-stop service utilization and provision will impose constraints on the design and implementation of embedded systems for supporting online maintenance and testing. Moreover, due to the gigantic size of the future systems, the design and implementation will be done on step-by-step development considerations.

Since devices will become more and more connected in some kind of network, information management in the network will become a serious issue. Closely related to networking devices, they need to access information available in the network to do their job. While embedded systems nowadays access local data, in the future this data might be retrieved from elsewhere. Therefore, some technology that can envision Web-connectivity is required. Distributed and networked sensors and

actuators will start to behave as intelligent agents. The complexity of these systems will increase and they will require increasing bandwidth for audio, video and wireless communication. Novel communication architectures and technologies are also required and they are achieved by Autonomous Decentralized System (ADS). We describe it in the next chapter.

3. AUTONOMOUS DECENTRALIZED SYSTEM

ADS has been proposed to resolve the on-line property of on-line expansion, on-line maintenance and fault tolerance in a system, which means that the system can continue operation during partial expansion, maintenance and at the time of a partial fault [7]. The ADS is defined as the characteristics that each subsystem can control itself and coordinate with all of the other operating subsystems. Therefore the following two properties must be satisfied by each subsystem: Autonomous Controllability and Autonomous Coordinability (Fig.2).

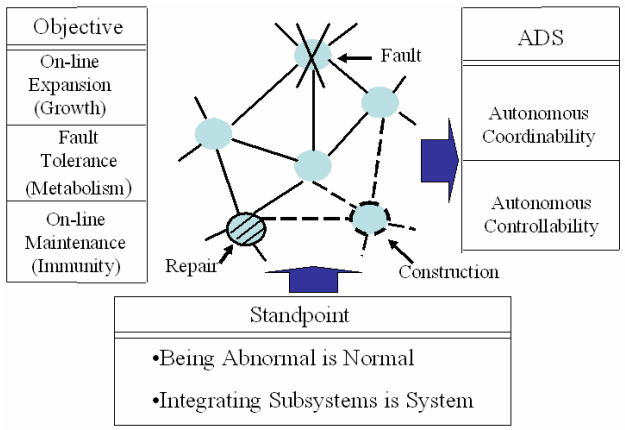


Fig.2 – Autonomous Decentralized System Concept

Each subsystem has its own management system, the Autonomous Control Processor (ACP) to manage itself and coordinate with the others. The subsystem including its application software modules and ACP is an autonomous unit called "Atom." The self-contained subsystems including their respective ACPs are integrated into a system. In the ADS, all of the subsystems are connected only through the Data Field (DF); all data is broadcasted into the DF and the data itself logically circulates in the DF (Fig.3). The data moves around the application modules in the Atom and the DF in the Atom is called the Atom Data Field (ADF). In the DF, each data is attached with its "content code" which is uniquely defined with respect to the content of the data. To protect the operation of the subsystems from variation in the system, each subsystem broadcasts a message containing the content code instead of the receivers address. The application module is specified only by input and output content codes, and it is executed by the ACP only when all of the necessary data with the proper input content codes is received from the DF (Data-Driven Mechanism). The necessary content codes for the Atom are determined dependently on the application functions within it (Fig.4).

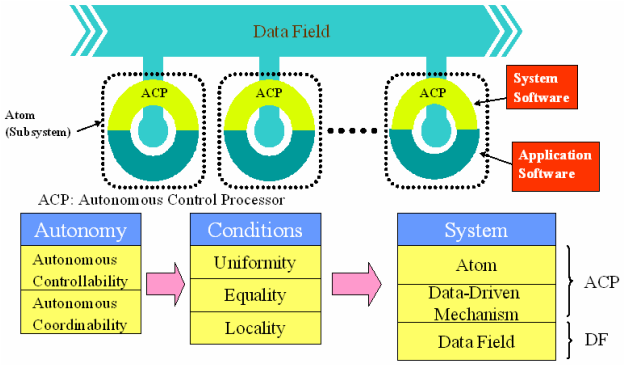
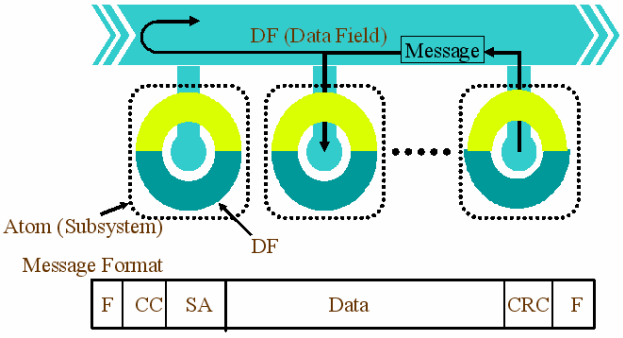


Fig.3 – ADS Architecture



F: Flag
CC: Content Code
CRC: Cyclic Redundancy Check

Fig.4 – Data Field

4. APPLICATION TO "Suica"

An embedded system, which has successfully been developed and implemented, utilizing ADS concept and architecture is "Suica," the system for train fare collection introduced by East Japan Railway Company in November 2001. This system is an integrated combination of wired and wireless systems; contact-less IC cards communicate wirelessly with automatic fare collection (AFC) terminal devices such as AFC gates while the terminals communicate via LAN with servers. The current number of card holders is over 13 million and the number of daily transactions is in the order of 8 million (Fig.5). The transactions are expected to grow up to 30 million in a close future. The terminals and servers are configured in autonomous decentralized architecture, so trouble does not expand to the whole system even if it occurs. It is

necessary for AFC terminal devices to provide high-speed processing and high reliability because of the nature of railway transportation service: safety and accuracy. For these reasons, technologies and applications that can meet these requirements have been introduced.

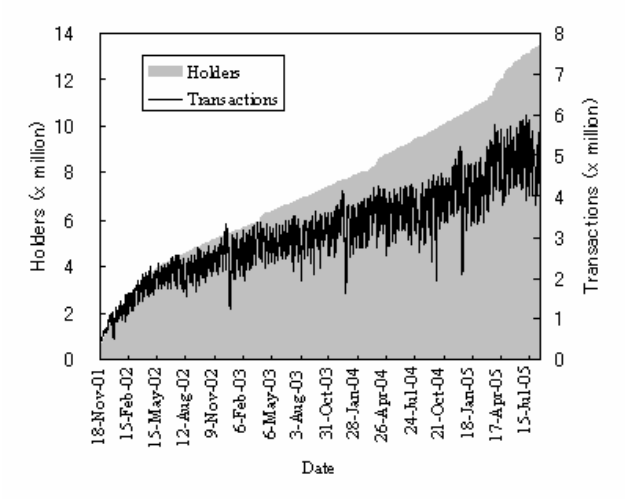


Fig.5 – Holders and Transactions of IC card System

IC card tickets can be purchased from automatic ticket vending machines. Stored fare (SF) values can be added to the card at the ticket vending machines and fare-adjustment machines. AFC gates can process both IC card tickets and conventional magnetized cards and tickets, however, simplified AFC machines, installed at smaller stations without AFC gates, accept IC card tickets only. A unique ID number is assigned to each Suica card and all the records of usage are finally compiled into a center server with the ID number. Information about all IC card tickets is consolidated into one information source, which is used for reliable and unified control of the IC card usage and for monitoring unauthorized use of the IC cards.

5. "Suica" SYSTEM STRUCTURE

The IC card ticket system consists of "IC cards," "terminals" (e.g. AFC gates), "stations servers," and a "center server." Minimum operation must be guaranteed in case of failures, which can lead to terrible confusion at stations. This is why "autonomous decentralized architecture" is used. The basic functions of the IC card ticket system are checking cards, calculating fares, and voiding cards of suspicious use.

Fig.6 is the overview of the system. This system is unique with three different data fields (DFs) with various time ranges. In DF1, wireless communications are done within a second while the data flow hourly in DF2 and the data transmission in DF3 has 2 cycles: daily and hourly. These time ranges of communications for consistency are varied according to the needs and aim at both high performance (high-speed processing) and high reliability.

Fig.7 is the detail around DF1. AFC terminals use wireless communications with IC card tickets. IC card tickets broadcast the data with content codes to DF1 and AFC gates as terminals select the data to collect and to process.

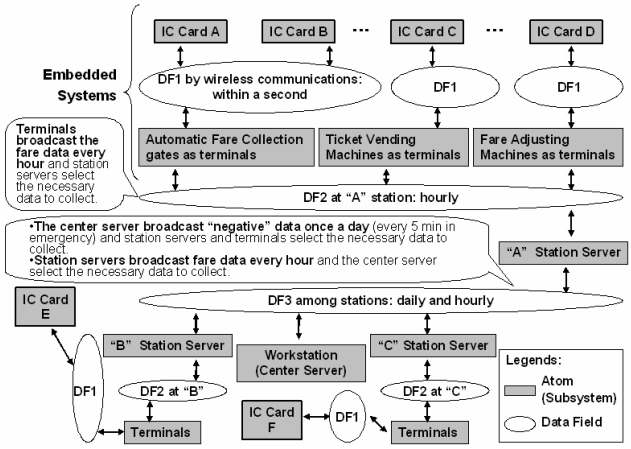


Fig.6 – Autonomous decentralized IC card system

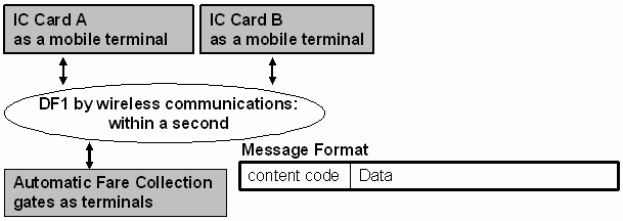


Fig.7 – Data field between IC card and terminal in autonomous decentralized IC card system

Each terminal and a station server are linked to station LAN and work on autonomous decentralized process through DF2. At stations a station server broadcast the data to DF2 and terminals such as AFC gates and ticket vending machines select the data to receive. Then the terminals check cards, calculate fare, and so on. Each terminal operates autonomously and failures at some terminals do not influence on the others. When a station server fails, some functions are suspended because the data from the center server do not flow, however, operations at the station can be kept normal with the stored data in each terminal. Station servers are connected to a center server through DF3 and thus, passengers can use all the functions, derived from DF3 among stations, when they move to another station with a normal station server [8][9][10][11].

The transaction between an IC card ticket and a terminal always depends on manual operations. At terminals each AFC device can execute autonomous high-speed processing, communicating with IC

cards in about 200ms. The data processed by terminals can be stored for a specific period, being connected in autonomous distribution architecture with center systems. Besides, the center systems process the data autonomously to deal with the data from terminals that have been accumulated for a certain period of time. Moreover, the operation data for the terminals are received by the center server, so that any necessary measures can be taken on the center side. To enhance the reliability of the networked system as a whole, a style of accumulating a certain amount of data processed by terminals at each level was adopted. Finally, in order to secure the system expendability, the devices are configured in autonomous architecture so that it is easy to add different types of terminals and to connect with each other.

6. AUTONOMOUS DECENTRALIZED ALGORITHM

When using IC card tickets, it is necessary to keep the security of their unique data, maintaining high speed processing. IC card tickets are provided with respective keys for respective files and IC card reader/writers (R/Ws) are provided with keys that enable simultaneous access to multiple files. This chapter explains the outline of the technology to process data at high-speed at the AFC gate for railway fare calculation.

The IC card ticket system has two types of IC cards: SF cards and commuter passes. SF cards are simply rechargeable prepaid cards while commuter passes include not only SF values but free rides within periods and areas declared in advance. Passengers have only to touch their own IC cards to the R/Ws when they go through AFC gates. Appropriate fares are automatically collected from the stored values if they have SF cards or commuter passes out of the declared areas and periods. Calculation becomes more complicated when a passenger with a commuter pass travels station A to B via the valid commuter-pass area because the regulations require AFC gates to collect the minimum fare upon entrance and to adjust the balance upon exit; the valid commuter-pass area, of course, should be taken into account (Fig.8).

It takes a long time if whole the calculation is thoroughly processed at station B. To solve this problem, "autonomous decentralized algorithm on fare calculation" is devised. In this algorithm, fares are autonomously calculated upon entrance into station A (pre-boarding process) and upon exit from station B (post-boarding process) and then, the results are compared and cooperated.

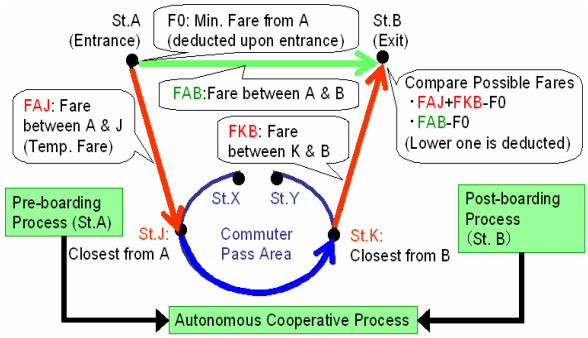


Fig.8 – Temporary memory method for fast fare adjustment

As for the case described in Fig.8, a passenger has a commuter pass valid between stations X and Y and enters from station A, outside of the valid commuter pass area. The AFC gate at station A judges that the pass is not valid there, deducting the minimum fare (F0) from the IC card. Then it selects the station J, closest to the station A within the commuter pass area, and writes the data of the station name and the fare between A and J stations (FAJ) in the IC card. When the passenger gets off at station B, also outside of the valid commuter pass area, the AFC gate at station B judges that the pass is not valid there. Then, it selects the station K, closest to the station B within the commuter pass area, and calculates fare between K and B stations (FKB). Finally it compares (1) the direct fare between A and B (FAB) minus F0 and (2) the sum of FAJ and FKB minus F0 and the less expensive fare is selected and processed in the IC card (autonomous cooperative process).

7. AUTONOMOUS DECENTRALIZED DATA CONSISTENCY TECHNOLOGY

Fig.9 shows how the IC card ticket system detects the end of process; a R/W updates its data when it receives a "data-process completed" signal from an IC card. This last signal is transmitted near the boarder of communications area, so that the process is not always completed successfully due to the ways of passengers' waving, which is demerit of contact-less method. In this case, the data through the R/W (and to Center server) are not updated though the ones in the card are updated. This is a serious problem called "data lack."

To prevent this "data lack," we have proposed "autonomous decentralized data consistency technology." This technology recovers the data from "data lack," using different DFs mentioned in Chapter 5. The details of this technology are as follows.

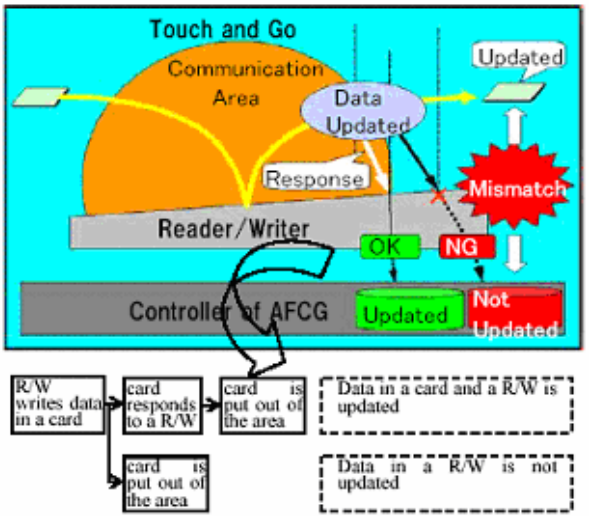
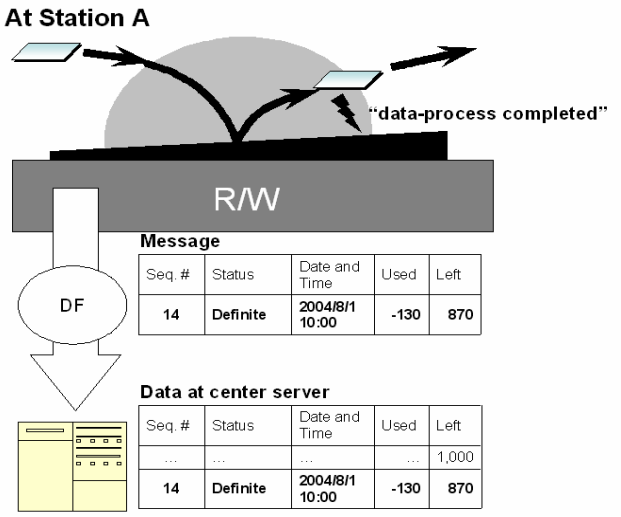


Fig.9 – High-speed communication and data reliability between IC card and terminal

According to this technology, the data in the R/W are saved as "temporary data" in the center server even when the R/W cannot catch the "data-process completed" signal. If the next processes are completed normally, the consistency of normal data sent to the center server and the previously-saved data is checked and the "temporary data" is revised as "definite data" [12].

Fig.10 to 12 explain an example. A passenger has a SF card with the SF value of 1,000 yen and travels from station A to B. Minimum fare of 130 yen is deducted at an AFC gate in station A. The AFC gate broadcasts the data to DF as "definite" with sequential number (#14 in this sample) when the process is successfully completed and the R/W receives "data-process completed" signal (Fig.10). Suppose that a R/W at station B fails to catch the "data-process completed" signal though the process is completely finished at the card. The data in the card are actually updated but the R/W and the servers cannot detect it because no response from the card is received. On the other hand, the R/W knows it has commanded that the card should update the data. In this case, the AFC gate broadcasts the unconfirmed data to DF as "temporary" (sequential number 15) (Fig.11). If the passenger uses the same card upon entrance at station C and the process finished completely, the data numbered 16 is "definite." The center server checks those sequences and changes its status from "temporary" to "definite" if the "temporary" record is surrounded by "definite" data and no inconsistency exists through the sequences (Fig.12).

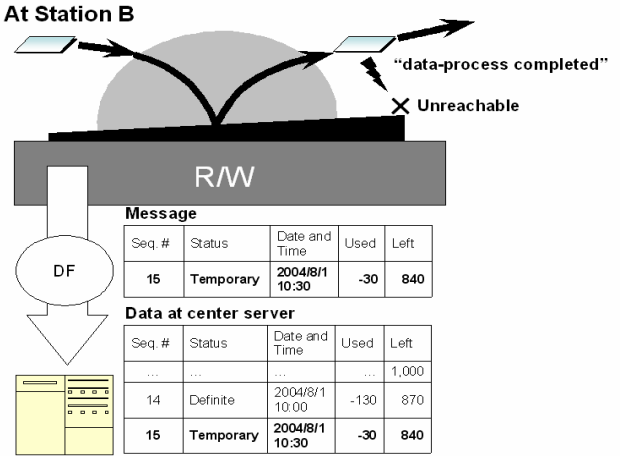
With this method, IC cards can escape from being voided as the data recover before blacklisted even if passengers have caused "data lack." That is, this technology assures the reliability of data with integration of autonomous processes at terminals and one at the center server.



Seq. #	Status	Date and Time	Used	Left
14	Definite	2004/8/1 10:00	-130	870

Seq. #	Status	Date and Time	Used	Left
…	…	…	…	1,000
14	Definite	2004/8/1 10:00	-130	870

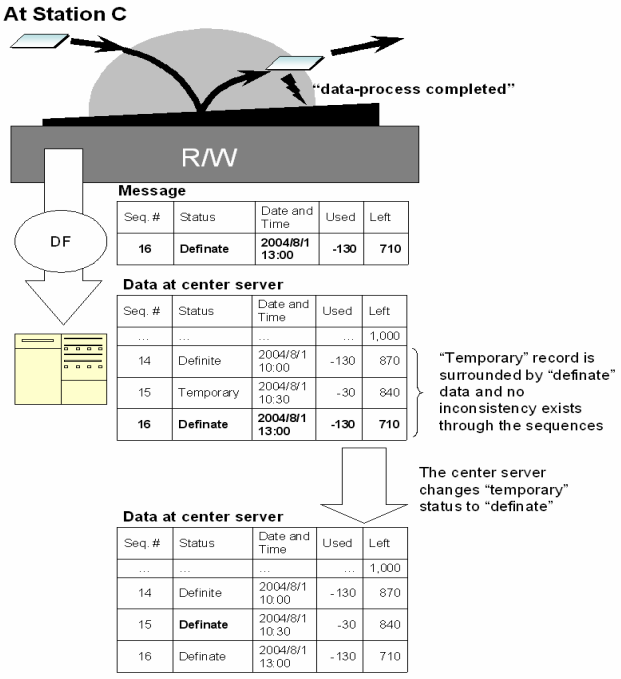
Fig.10 – Data consistency technology (1): normal process at reader/writer



Seq. #	Status	Date and Time	Used	Left
15	Temporary	2004/8/1 10:30	-30	840

Seq. #	Status	Date and Time	Used	Left
…	…	…	…	1,000
14	Definite	2004/8/1 10:00	-130	870
15	Temporary	2004/8/1 10:30	-30	840

Fig.11 – Data consistency technology (2): unconfirmed process at reader/writer



Seq. #	Status	Date and Time	Used	Left
16	Definate	2004/8/1 13:00	-130	710

Seq. #	Status	Date and Time	Used	Left
…	…	…	…	1,000
14	Definite	2004/8/1 10:00	-130	870
15	Temporary	2004/8/1 10:30	-30	840
16	Definate	2004/8/1 13:00	-130	710

Seq. #	Status	Date and Time	Used	Left
…	…	…	…	1,000
14	Definite	2004/8/1 10:00	-130	870
15	Definate	2004/8/1 10:30	-30	840
16	Definate	2004/8/1 13:00	-130	710

Fig.12 – Data consistency technology (3): another normal process at reader/writer and data recovery

8. CONCLUSION

Under the recent severe economic situation, the business in the various fields has been changing to produce new products and to supply new services. Moreover, the life cycles of these products and services have been getting short. As the technological trends, the openness and the down-sizing phenomena have been in progress, and the system is constructed by the multi-vender's machines.

The ADS concept is explained under the backgrounds not for the resource utilization, but for the easy-to-use and the easy-to-construct of the computing and controlling systems. This architecture shows that there exists no master and no direction among subsystems, and then the software productivity is much improved by building block manner of autonomous software modules. Moreover the applications in the distributed embedded systems of the ADS are described and its validity has been verified.

As a successful sample in practical use of the ADS-embedded system, this paper has introduced "Suica," the IC card ticket system. This system requires the correspondence of both high-speed processing (high performance) and high reliability (data consistency). Also, it needs to change itself as the circumstances change (e.g. Suica card holders have grown to 13 million in 4 years). Therefore, we have used the ADS technology to construct the system. In addition, we have proposed two technological methods: "autonomous decentralized algorithm on fare calculation" for high-speed processing and "autonomous decentralized data consistency technology" for high reliability. Thus, high assurance has been achieved. Also, there is not an especially big trouble and the effectiveness of this technology has been proven [13].

8. REFERENCES

[1] B.P. Dave, G. Lakshminarayana, N.K. Jha: COSYN: Hardware-software co-synthesis of heterogeneous distributed embedded systems, *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol.7, no.1, (1999), 92-104.

[2] J. Liu, P.H. Chou: Distributed Embedded Systems for Low Power: a case study, *IEEE Proc. of Parallel and Distributed Processing Symposium*, April 2004.

[3] K. Mori and et al: Proposition of Autonomous Decentralized Concept, *Trans. IEE of Japan* vol.104C, no.12, (1984), 303-340.

[4] L.D.J Eggermont and et al: Embedded Systems, *Vision on technology for the future PROGRESS*, Ludwig D.J. Eggermont edit., 2002.

[5] M. Hirayama. Current State of Embedded Software Development. *Information Processing Society of Japan (IPSJ)*. VOL.45. No.7, 677-681,2004.

[6] N. Subramanian and L. Chung: Architecture-Driven Embedded Systems Adaptation for Supporting Vocabulary Evolution, *IEEE Proc. of Principles of Software Evolution*, November 2000, 144-153.

[7] K. Mori: Autonomous Decentralized Systems: Concept, Data Field Architecture and Future Trends, *Proc. of ISADS'93*, Kawasaki, Japan, 1993.

[8] K. Mori, "Autonomous Decentralized System Concept, Data Field Architecture and Future Trends"ISADS1993, Kawasaki, Japan, pp23-34, Apr.1993

[9] K. Mori, et. al "Autonomous Decentralized System Software Structure and It's Application", IEEE Fall Joint Computer Conference, pp.1056-1063, Nov.1986

[10] K. Mori, "Autonomous Decentralized System [I–VI]", IEICE, No.6-10, Vol.84,2001

[11] K. Mori," Technology that flaps in the world -Autonomous Decentralized System(1) (2)", The Institute of Electrical Engineers of JapanNo.2-3, Vol.121,2001

[12] A. Shiibashi: Autonomous decentralized high-speed processing technology and the application in an integrated IC card fixed-line and wireless system, *Proc. ISADS'05*, Chengdu, China, April 2005.

[13] M. Matsumoto, K. Mori, "Assurance evaluation technology for an autonomous decentralized ATC system", Electronics and Communications in Japan, Vol. J86-D-I-No.1, pp.14-22, 2003

Akio Shiibashi *graduated from Mechanical Engineering Department, Faculty of Engineering, Saitama University in 1976, and joined Japan National Railways (JNR). In 1987, JNR changed its name into East Japan Railway Company. He started to engage in the R&D of IC card based automatic fare collection gate system in 1994. He has been in charge of the "Suica system promotion project" since 1998. He is a member of JSME and IEICE, Japan.*

Kinji Mori *received the B.S., M.S. and Ph.D. degrees in the Electrical Engineering from Waseda University, Japan in 1969,1971 and 1974, respectively. From 1974 to 1997 he was in System Development Lab., Hitachi, Ltd. In 1997 he joined*

Tokyo Institute of Technology, Tokyo, Japan as a professor. His research interests include the distributed computing, the fault tolerant computing and the mobile agent. He proposed Autonomous Decentralized Systems (ADS) in 1977 and since then he has been involved in the research and development of ADS. He is one of founders of the International Symposium on ADS (ISADS), was the general chair of the fourth ISADS, and now is the steering committee chair of ISADS. He served many international academic activities as the general chair, the program committee chair and the editorial board of IEEE Transaction on Computing, and as the IEEE Technical Board Committee of Computer Communication. He is a Fellow of IEEE and a member of IEICE, IPSJ and SICE, Japan.