Paper accepted for presentation at 2009 IEEE Bucharest Power Tech Conference, June 28th - July 2nd, Bucharest, Romania



# A SCADA System Using Mobile Agents for A Next-Generation Distribution System

Tetsuo Otani, *Member, IEEE* and Hiromu Kobayashi

***Abstract*—We are studying a future distribution system that solves the problems caused by connection of numerous distributed generators. A SCADA (Supervisory Control and Data Acquisition) system for this distribution system should be economical, flexible and reliable as well as executing a real–time process. In this paper, we propose a SCADA system using mobile agents in order to make it flexible. In addition, we show two types of communication protocols that make agent migration more fault-tolerant. We have carried out experiments in which the SCADA system executes ground fault protection within the required time. These results indicate that the SCADA system based on our proposed technologies, should be able to fulfill the requirement for real–time processing.**

***Index Terms*—SCADA systems, Power system communication, Power distribution control**

## I. Introduction

Photovoltaic and wind generators will be installed in large numbers to prevent global warming and conserve energy. Their mass will be connected to a distribution system, which is likely to involve problems concerning voltage control and protection. We are studying a future distribution system, named ADAPS (Autonomous Demand Area Power System), which solves these problems and affords facilities to distribution system operators and customers[1]. ADAPS adds two types of equipment to the existing distribution system. The first is a power electronics device that controls a loop distribution system with no increase in the short circuit current[2], named an LPC (Loop Power flow Controller). The second is a piece of apparatus that monitors and controls a distributed generator and/or load device[3]. We call it the DSIF (Demand–Supply Interface).

In terms of the operation and management of ADAPS, we should consider several aspects that differ from those for existing transmission or distribution systems. It is difficult to estimate the number of distributed generators and their connecting points, because the generator owner might differ from the system operator. In addition, a connecting point could be a power supply point at one stage, and a power demand point at another. Of course, such operation and maintenance should be performed economically.

We have identified the following three requirements for a SCADA (Supervisory Control And Data Acquisition) system for ADAPS, based on the background we mentioned:

- Economic efficiency by integrating various applications, adopting a low cost apparatus, and saving on the maintenance of SCADA itself
- Flexibility in terms of a change in the system configuration or functions
- Operation in real–time and reliability for protection

These requirements would not be satisfied by the current technologies of communication and the SCADA system[4]. A control-communication framework proposed by Mazumder et. al.[5] has demonstrated an optimal compromise between the performance of a control system and the resource utilization of a communication network. However, it seems to lack the viewpoint of flexibility. Advanced Metering Infrastructure (AMI)[6] is one of the state of the art communication technologies related to a distribution system. AMI is usually used for real–time pricing, demand side management or demand response and/or outage management. Although these functionalities cover some part of ADAPS, they do not consider protection a distribution line.

In this paper, we propose a SCADA system using mobile agents and wide–area Ethernet. A mobile agent is a software component capable of migrating to, and performing on a remote host. This characteristic could render a system flexible, and allow applications to be integrated into the same using low cost apparatus[7]. On the other hand, a wide–area Ethernet provides economical broadband communications, allowing it to transmit data dispatched by various applications. Therefore, this paper focuses on how to ensure this SCADA system operates reliably and in real–time. Specifically, we show how this SCADA system is capable of protecting a ground fault on a distribution line, even though communication failure has an adverse effect on communication in this SCADA system. The protection of ground faults is subject to the most stringent requirements in the performance of this SCADA system, with completion within 1 second required based on regulations in Japan.

This paper is organized as follows. Section II illustrates the SCADA system we propose, while Section III shows experiments and their results in order to evaluate our SCADA system. We consider the feasibility of our SCADA system in Section IV, then finally state our conclusions in Section V.

## II. SCADA system for ADAPS

Our SCADA system for ADAPS comprises three elements, namely, control devices as hardware, mobile agents as software, and a wide–area Ethernet as a communication network.

Tetsuo Otani is with Central Research Institute of Electric Power Industry, 2-11-1, Iwodo Kita, Komae-shi, Tokyo 201-8511 JAPAN (e-mail: ohtani@criepi.denken.or.jp)

Hiromu Kobayashi is with Central Research Institute of Electric Power Industry, 2-11-1, Iwodo Kita, Komae-shi, Tokyo 201-8511 JAPAN (e-mail: hiromuk@criepi.denken.or.jp)

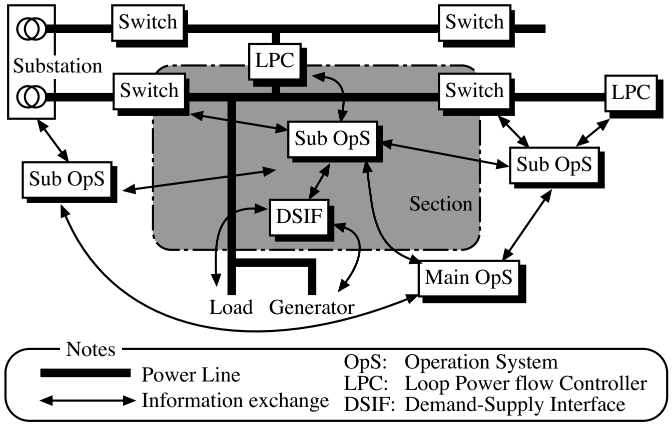


Fig. 1. An overview of ADAPS

## A. Control Devices

The SCADA system is configured as a distributed system to render it scalable. Fig. 1 illustrates part of the SCADA system from the viewpoint of a Section bound by section switches and LPC. Each control device has sufficient computing power for mobile agents to work and migrate. There are five types of control devices in the SCADA system.

- The Main Operation System (Main OpS) operates the entire ADAPS and determines the settings of LPC and a tap position in the power transformer.
- The Sub Operation System (Sub OpS) monitors and controls a specific section. It also interacts with control devices in its section, Main OpS, and other Sub OpSs.
- The Control Unit in the Section Switch measures the current and voltage at the section switch to which it is installed as well as opening and closing the section switch.
- The Control Unit in the LPC operates the LPC in which it is installed. In cases where this unit receives a fault notification, it changes the LPC operation mode in order to continue supplying power to a sound section.
- The DSIF monitors and controls a distributed generator and/or load device. In case where it receives a fault notification from the Sub OpS, it disconnects all of the generators of which it has control.

## B. Mobile Agents

We have designed a QoS (Quality of communication Service) control method in order to ensure real–time operation in cases where many applications are integrated into this SCADA system[8]. In addition, we have also designed a fault-tolerant protocol for agent migration to make this system more reliable. Fig. 2 illustrates the mobile agents with these two mechanisms.

*1) QoS Control Method:* This QoS control method specifies three priorities of mobile agents used for scheduling migrations and tasks. As illustrated in Fig. 2, an emergency agent has a high priority, a rapid agent medium priority, and the best effort agent low priority. Tasks of agents with higher priority interrupt all the working tasks of those with lower priority. If multiple agents with equivalent priority work, processing time is shared evenly. An emergency agent migrates to a remote host in which emergency agents are pooled for quick migration. In addition, a best effort agent migrates after some seconds have elapsed since the departure of the previous best effort agent. This interval helps avoid congestion in the communication network.

An agent base receives and invokes a migrating agent, while an invoked agent starts working autonomously. This QoS control method provides two types of agent base. One operates with a receiving entity of high priority for an emergency agent. The other is for other types of agents, with a receiving entity of medium priority. Their behavior is the same as the agents in terms of priority, in other words, an agent base for emergency interrupts all the working tasks of medium or low priority, which enables an emergency agent to arrive at a remote host in which some agents have already been working.

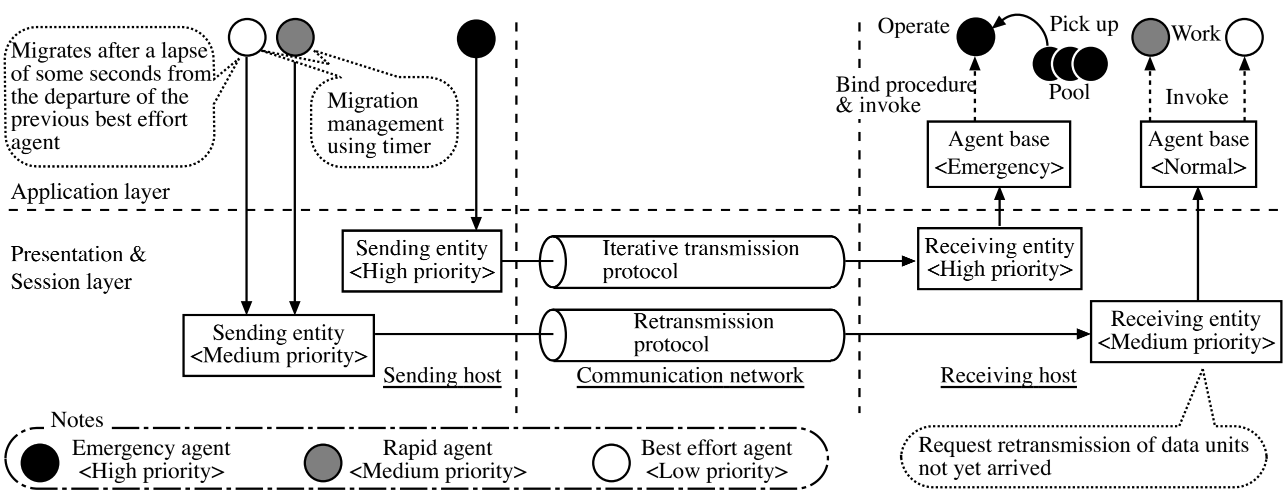


Fig. 2. Mobile agents used in SCADA system for ADAPS

TABLE I
MAIN FEATURES OF FAULT-TOLERANT PROTOCOL FOR AGENT MIGRATION

| | Iterative Transmission Protocol | Retransmission Protocol |
|---|---|---|
| Lower Layer Protocol | UDP (Multicast) | UDP (Unicast) |
| Topology | 1:N | 1:1 |
| Fault-tolerant Method | Iterative transmission from sender | Request of retransmission from receiver |
| Parameters to be set | – Iteration count (integer more than 1)<br>– Interval between iteration<br>(on a millisecond time scale)<br>– Payload size (in terms of bytes) | – Period to emit a request of retransmission<br>(on a millisecond time scale)<br>– Payload size (in terms of bytes) |
| Acknowledgment of Migration | Sent by a receiving entity | |
| Application | Emergency Agent | Rapid & Best Effort Agents |

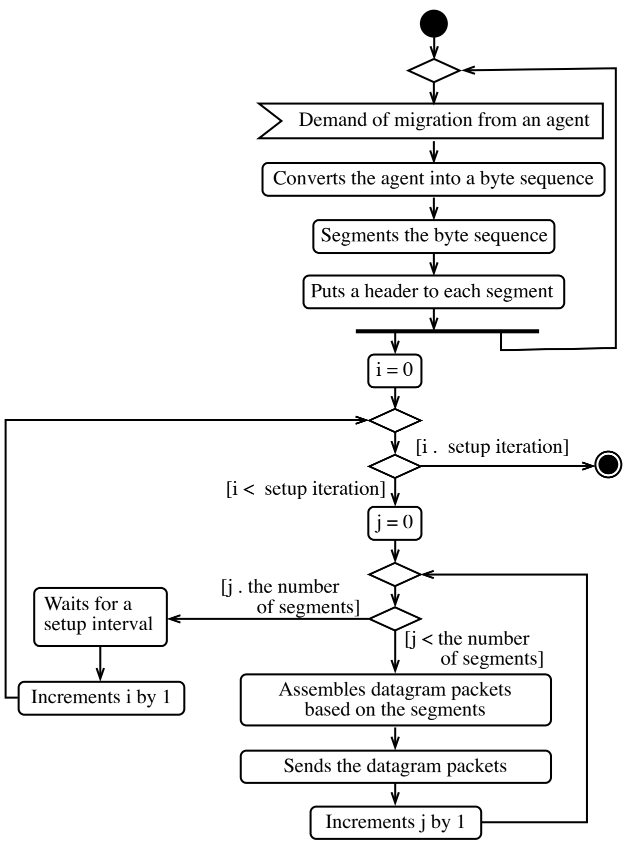


Fig. 3. Procedure sending an agent according to the iterative transmission protocol

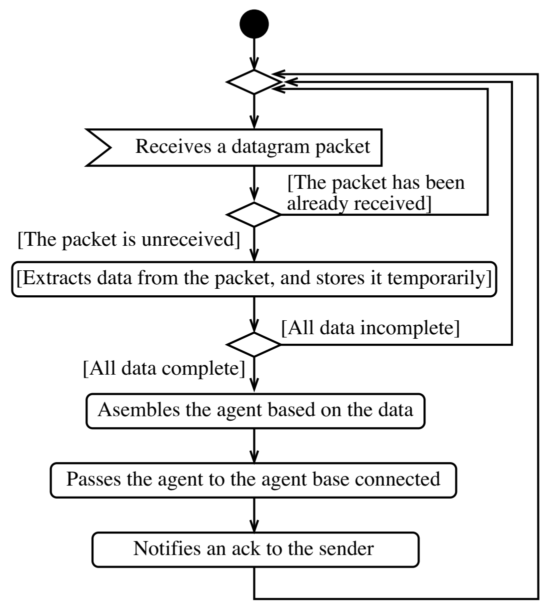


Fig. 4. Procedure receiving an agent accoding to the iterative transmission protocol

*2) Fault-tolerant Protocol for Agent Migration:* Two types of protocols are used for agent migration in this system, which differ in terms of transmission, while both have the same functionalities for encoding / decoding an agent and dividing / combining an encoded agent. Table I shows main features of the protocols. It is also common for them to utilize the UDP (User Datagram Protocol)[9] as a transport protocol, because they can use their own functionalities for reliability as well as avoiding the slow start mechanism[10] and using the retransmission timer of the TCP (Transmission Control Protocol)[11]. If TCP is used for an agent migration, the restart of communication is too late to protect a distribution line within the required time[12].

The first one, named the iterative transmission protocol, is used for the migration of an emergency agent. Fig. 3 illustrates the procedure for data transmission according to the notation of the activity diagram in UML[13]. It sends an encoded agent iteratively at intervals of some milliseconds, regardless of the success in migration. An administrator can set the iteration count and the interval between iterations. This mechanism enables an agent to migrate to its destination host in case of communication failure if Ethernet establishes an alternative route within the time calculated by the formula 1.

$$\text{Interval} \times (\text{Iteration count} - 1) \tag{1}$$

A receiving entity of this protocol works according to the procedure illustrated in Fig. 4. It abandons the fragment of an encoded agent already received. When all data comprising an agent are received, the entity assembles an agent and passes it to the agent base it connects. The agent will be activated by the agent base. Eventually, this entity sends back an

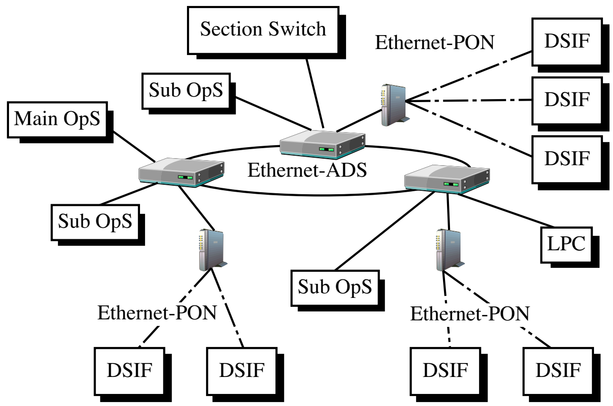


Fig. 5. A Configuration of wide–area Ethernet Following Our Design Policy

acknowledgement that indicates completion of the migration.

The second one, named a retransmission protocol, is used for the migration of rapid and best effort agents. The sending entity sends an encoded agent once, while the receiving entity requires the sending entity to retransmit a fragment of the encoded agent if it does not reach the destination within the required time. An administrator can set this required time in one millisecond.

### *C. Configuration Policy of Wide–area Ethernet*

This policy employs an Ethernet ADS (Active Double Star) and an Ethernet PON (Passive Optical Network). Fig. 5 depicts a configuration of the Ethernet following our design policy. The Ethernet ADS establishes a logical network using the rapid spanning tree protocol (RSTP) [14] on a loop physical topology. If a communication failure occurs, a logical network in Ethernet ADS is reconfigured in order to resume communication within a second and thus hooks up with a Sub OpS, section switch and LPC that have important roles in protecting ADAPS. On the other hand, the Ethernet PON has the merit of enabling the economical connection of many devices, despite being unable to set up an alternative route. A number of DSIF will be installed in ADAPS so that they are connected using an Ethernet PON connected to Ethernet ADS.

## III. Experiments for protection of ground fault

To evaluate the real–time performance and reliability of the SCADA system, we carried out experiments in which it protected a ground fault on a distribution line. The protection of ground faults is the function with the shortest time period provided in the SCADA system, because a short circuit will be protected only by local sensing data. It must also be completed within 1 second due to regulations in Japan. In addition, we measured the processing time of the SCADA system in cases where a communication failure also occurred at the same time.

We mention these experiments from three aspects, namely, system configuration, procedure of protection and their results in the following sections:

### *A. Experimental System Configuration*

The experimental system was composed of a distribution line, three distributed generators and the SCADA system. The specifications of elements in the experimental system were equivalent to those for commercial use. Fig. 6 illustrates its configuration. Please note that this system does not supply power to real customers because we need to cause a ground fault arbitrarily.

*1) Structure of Power Equipment:* This distribution line was approximately 3 km in length and 6.6 kV in voltage, divided into three sections via two Section switches, which had built-in sensors for the current and voltage.

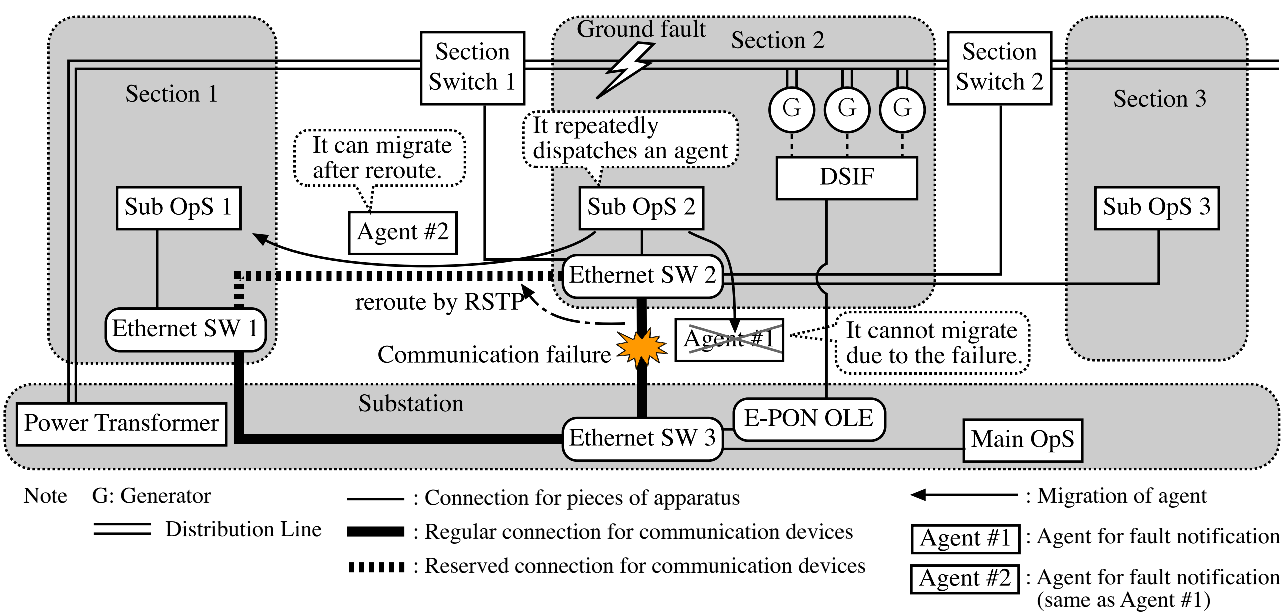


Fig. 6. Experimental system configuration

TABLE II
COMPUTER SPECIFICATIONS USED IN THE EXPERIMENTAL SYSTEM

| Apparatus | CPU | OS |
|---|---|---|
| Main OpS | Pentium® 3 GHz | MS Windows® XP |
| Sub OpS | Celeron® 2 GHz | Solaris™ 10 |
| DSIF | Celeron® 2 GHz | MS Windows® XP |

Three generators were connected to the center section named Section 2. Two of them were inverter-type generators whose power was 20 kW each, and the rest is a synchronous generator whose power was 150 kW. Section 2 also connected a load system capable of varying its load capacity.

A ground fault occurred on the distribution line in Section 2. This fault was monitored by a measuring system that was installed in addition to the SCADA system in this experimental system. This measuring system also monitored events on the Section switches and generators.

*2) Configuration of the SCADA System:* The SCADA system in the experimental system was composed of a Sub OpS in each section, DSIF in Section 2, and a Main OpS in the substation. Table II shows the specifications of the computers for each piece of apparatus in the SCADA system. The mobile agents in the SCADA system were implemented using Java™ SE 5.0, and run on these computers. The Section switches housed sensors and a processing unit, the latter of which did not support java, hence communication between the Section switch and the Sub OpS was done via a TCP connection.

The parameters of the iterative transmission protocol were set as follows:

- The iteration count was 50.
- The interval between iterations was 20 milliseconds.
- The payload size was 1,448 bytes.

The reason for the interval setup came from the results of preliminary tests indicating that processing was not congested in cases where the interval was 20 milliseconds. In addition, the shorter the interval, the quicker the recovery from a communication failure. The reason for the iteration count setup came from the requirements for ground fault protection. In other words, the migration of the mobile agent was not needed after 1 second had elapsed from a ground fault. In cases where the interval count was 50, this protocol sent datagram packets for 1 second. The reason for the payload size setup was calculated based on the difference between the MTU (Maximum Transmission Unit) of Ethernet and headers of IP, UDP, and the iterative transmission protocol.

In terms of the retransmission protocol, the emission period for retransmission was set to 1 second, which came from application requirements supported by a rapid agent. The payload size was the same as the for the iterative transmission protocol.

The communication network in the SCADA system was composed of Ethernet–ADS with RSTP and Ethernet-PON. The bandwidth between the Ethernet switches was 1 Gbps, and that between an Ethernet switch and an apparatus was 100 Mbps. The network based on Ethernet–ADS had a physical loop, and the link between Ethernet switches 1 and 2 was blocked. The communication path under a normal condition traversed the Ethernet switches 1, 3 and 2. A communication failure occurred in the link between the Ethernet switches 2 and 3, which was caused in conjunction with a ground fault on the distribution line. RSTP activated the link between the Ethernet switches 1 and 2 in the event of the communication failure, so that every piece of apparatus could communicate with all others. The average rerouting time was 884 milliseconds according to our preliminary tests. We set a time lag between the communication failure and ground fault, hence we varied the rerouting time.

### B. Procedure of Protection

Fig. 7 illustrates the procedure of ground fault protection we used in the experiments.

The Section switch judged that a fault occurred on the distribution line in cases where the following two conditions were met. The first condition was the zero-phase-sequence voltage exceeding 10 V during 50 milliseconds. The second condition was that the product of the zero-phase-sequence current and zero-phase-sequence voltage also exceeded 5 VA during 50 milliseconds. The Section switches notified the Sub OpS in Section 2 that they had detected a fault, when one was detected.

The Sub OpS judged whether the fault occurred in Section 2 or outside. If the fault occurred in Section 2, mobile agents migrated to the Sub OpSs in the neighboring sections in order to change their operational mode and continue power supply. The Sub OpSs in the neighboring sections called for mode change of LPC. This processing was done by a mobile agent that simulated migration to an LPC. The agents migrated back to the Sub OpS in Section 2 after the LPC changed its mode.

In experiments with a communication failure, the fault interrupted the agent migration from the Sub OpS in Section 2 to that in Section 1. We measured two types of time for the protection. One was the time from a ground fault to Section switch open status, while the other was to generator disconnection.

After the neighboring sections got ready to continually supply power, the Sub OpS directed that the Section switches be opened and the generators disconnected. All processing and communications other than those between the Sub OpS and the Section switches were carried out by the mobile agents.

The protection was completed when the Section switches were opened and the generators disconnected. Finally, a mobile agent migrated to the Main OpS to inform of the completion of protection.

During the experiments, best effort agents operated within the SCADA system to gather data from the generators and distribution lines. When a best effort agent started its migration, it confirmed that 2 seconds or more had elapsed since its previous best effort agent had left the apparatus.

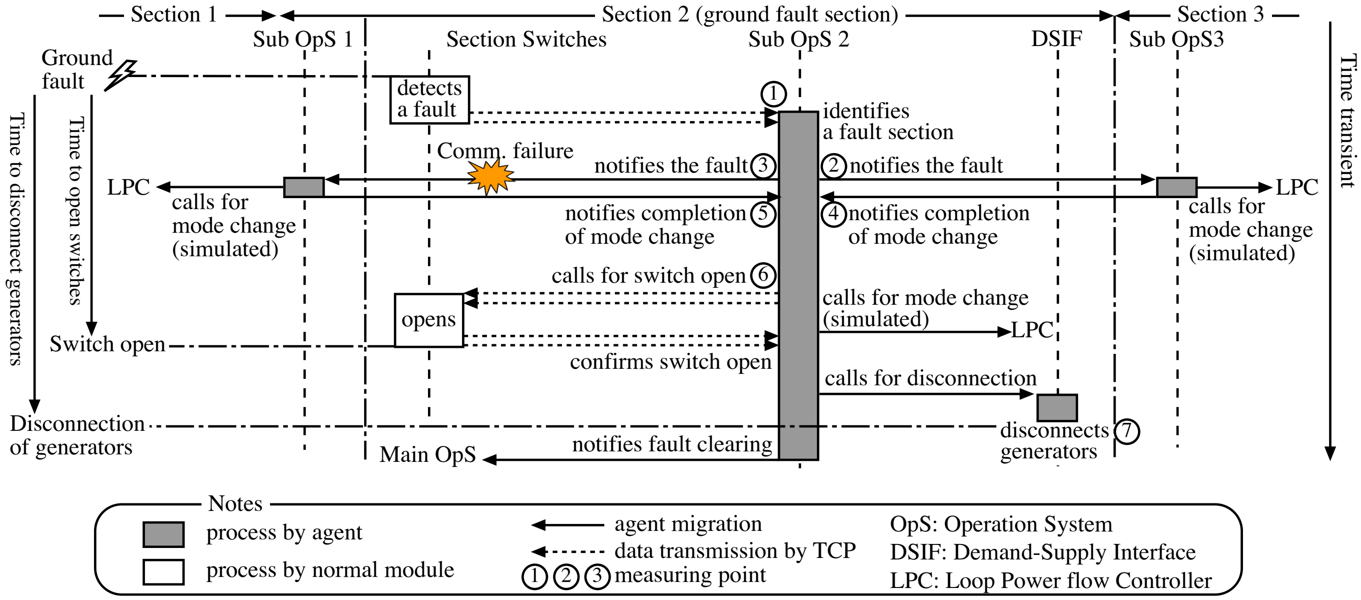


Fig. 7. Procedure used in the experiments of protection

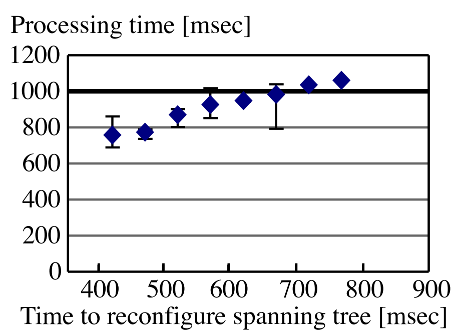


Fig. 8. Elapsed time to open the swtiches

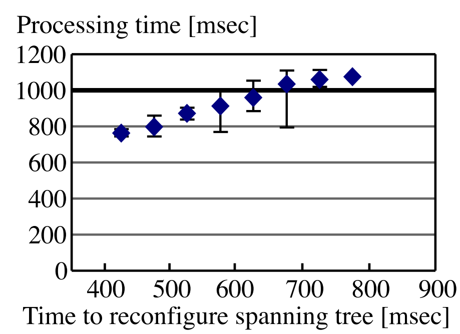


Fig. 9. Elapsed time to disconnect the generators

### *C. Experimental Results*

We will mention two types of experiment results. One is under normal conditions, in which the protection procedure was implemented without communications failure. The other is in cases where a communications failure affected the protection procedure.

*1) Results under the normal condition:* Ground fault protection without communication failure in these experiments was implemented within about 450 milliseconds. These results indicate that the SCADA system we propose could satisfy the regulatory requirements.

*2) Results in case of communication failure:* We show the results in graphs that show the elapsed time from the point when the zero-phase-sequence current flowed. The abscissa axis of each graph is a time scale from the ground fault to setting of an alternative route in Ethernet–ADS.

Fig. 8 shows the elapsed time to the point when both the Section switches opened. In terms of the Section switch 1, the point when the value of the zero-phase-sequence current became zero was regarded as that when the Section switch opened. This is because power flow was supplied from the substation to the ground fault location until the fault was cleared. On the other hand, we regarded it as the Section switch 2 opening when the value of the exciting current in the potential transformer in Section 3 became zero. This is because no power was supplied from Section 3, meaning we were unable to detect the zero-phase-sequence current on Section switch 2.

Fig. 9 shows the elapsed time up to the point when all of the generators were disconnected. We judged that a generator was disconnected when the current it supplied became zero.

These results mean that a ground fault could be resolved within the required time if Ethernet ADS sets up an alternative route within 550 milliseconds within this SCADA system.

*3) Results of each processing step:* We also measured the processing time of each step that was not influenced by a communication failure. Table III shows the average and maximum times of each step in the procedure. The column

TABLE III
PROCESSING TIME OF EACH STEP

| Step | Meas. Pt. | Ave. time | Max. time |
|---|---|---|---|
| Fault notification | ① ∼ ③ | 16 msec | 79 msec |
| Switch open command | ⑤ ∼ ⑥ | 61 msec | 110 msec |
| Opening section switches | ⑥ ∼ fin. | 171 msec | 305 msec |
| Disconnection command | ⑥ ∼ ⑦ | 42 msec | 185 msec |
| Disconnecting a generator | ⑦ ∼ fin. | 118 msec | 130 msec |

fin.: section switch opened / generator disconnected

named Meas. Pt. (measurement point) shows the beginning and end measurement points, while the circled numbers in this column correspond to those in the Fig. 7 illustrating the protection procedure. Therefore, the step "Fault notification" included agent migrations to the neighboring Sub OpSs, while the step "Disconnection command" also included agent migration from Sub OpS 2 to LPC and DSIF.

## IV. CONSIDERATION

We consider the feasibility of the protection and the SCADA system we have proposed. Our considerations are viewed from two perspectives. One includes the possibility of satisfying requirements for ground fault protection. The other concerns the scalability of this SCADA system itself, in terms of the increase in piece of apparatus such as DSIF.

### *A. Requirement Satisfaction about Ground Fault Protection*

We consider the potential to satisfy the requirements for ground fault protection based on the results mentioned in Section III-C. Fig. 10 depicts the time available for interactions with neighboring sections based on the average time of each step mentioned in Section III-C3. Similarly, Fig. 11 depicts the time based on the maximum time. We assign 200 milliseconds for sensor and fault identification, which is used in a typical distribution automation system in Japan, while also assigning an additional 50 milliseconds "just in case".

A mobile agent could spend 502 milliseconds for its migration and execution on a Sub OpS in neighboring Section under average time condition. Ethernet–ADS should establish an alternative route within 402 milliseconds, if a mobile agent spends 80 milliseconds and the interval between iteration is set to 20 milliseconds.

Current products of Ethernet switches should be capable of establishing an alternative route using RSTP within 402 milliseconds. Catalogs about such latest products mention that the time of rerouting using RSTP would be about 200 or 300 milliseconds. If we use a proprietary technology (VSRP from Foundary, Super Ring from Korenix, etc.), we can shorten it further in order to set up an alternative route. VPLS (virtual private LAN service)[15] proposed as IETF RFC is also promised. These technologies enable an alternative route to be established within 50 milliseconds.

In cases where the maximum time of each step is considered, a mobile agent could spend 246 milliseconds, while establishing an alternative route could result in 146 milliseconds being expended on the above calculation. This means that RSTP should not satisfy the requirement, but VPLS or other technologies could.

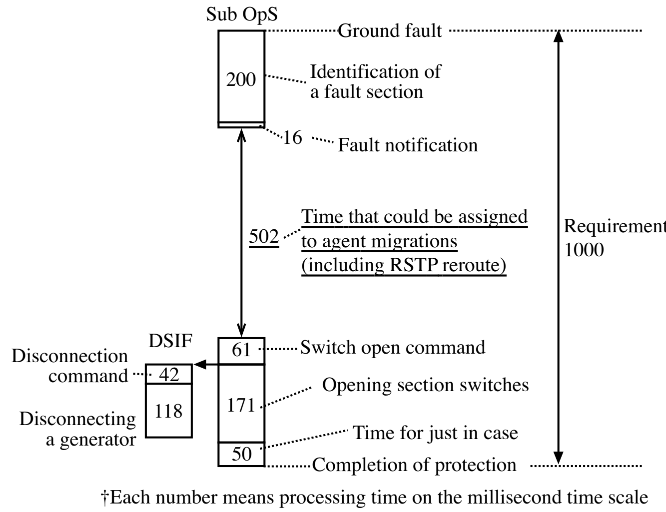


Fig. 10. Temporal structuring of protection processing based on the average processing time of each step

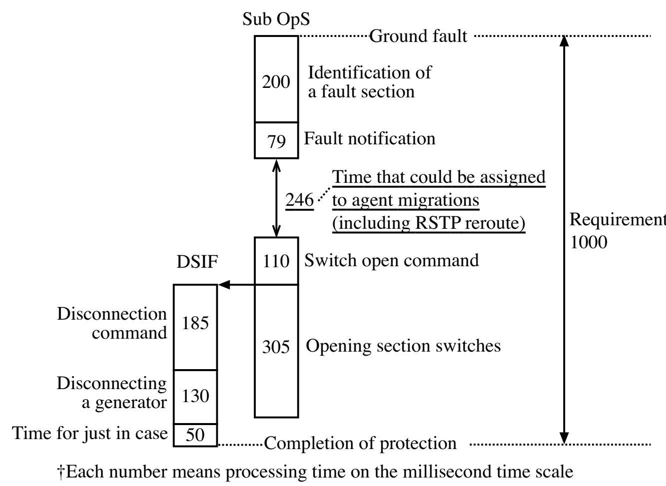


Fig. 11. Temporal structuring of protection processing based on the maximum processing time of each step

We can assign a longer time to rerouting in Ethernet–ADS if we make the maximum time of each step closer to the average. One of the methods should involve the use of real–time specifications for Java[16]. The Java virtual machines used in the experiments did not conform to the specifications, hence the interruption handling would be unsuitable for this SCADA system. The real–time specifications for Java[17] would, however, have positive effects on the steps "Migration to a neighboring Sub OpS", "Switch open command" and "Disconnection command."

According to the results of experiments and the above considerations, the SCADA system we have proposed could satisfy the requirements for ground fault protection in case where it is applied to fields.

### B. Scalability of SCADA system

The experimental system we used was small as it included only two Sub OpSs in neighboring sections and only one DSIF in Section 2. A power distribution system for real service is considerably larger than is the actual format. Its typical Section usually includes from three to eight neighboring sections. In addition, it is predicted that several hundred DSIF will be installed in its section. Therefore, the SCADA system we have proposed should be expandable in terms of the number of piece of apparatus.

An emergency agent is able to migrate to multiple pieces of apparatus such as Sub OpS or DSIF. This is because the iterative transmission protocol uses UDP multicast. In other words, it could prevent the load for agent migration from getting heavier according to the number of pieces of apparatus. Of course, all of the pieces of apparatus to which an emergency agent migrates at one time should be connected to join a multicast group. DSIF, in great volume, will be connected using Ethernet-PON based on our design policy, so that all of the pieces of apparatus in an ADAPS could be in the same domain. Therefore, the ground fault protection performance would remain intact in cases where many Sub OpS and DSIF are installed in a SCADA system.

A rapid or best effort agent can go the round of the pieces of apparatus in sequence. This is because an agent incorporates a processing procedure in its objects to facilitate the processing load being shared by pieces of apparatus. In addition, an agent can duplicate the same, so that the route for a round can be shortened according to the number of nodes it contains.

Therefore, we could mention that these characteristics should make the SCADA we have proposed expandable.

## V. Conclusion

We have proposed a SCADA system for ADAPS using mobile agents and wide-area Ethernet. It could be economical and flexible due to the characteristics of these two technologies. In addition, the agents have QoS control methods, via which processing is scheduled according to three priorities and communication congestion would be avoided. Two types of protocols for agent migration are provided in the SCADA system, one of which iteratively sends a datagram packet to a destination in order to contribute to real-time and reliable processing in this system. On the other hand, the wide-area Ethernet is composed of ADS (Active Double Star) and PON (Passive Optical Network). Ethernet-ADS provides RSTP that is capable of establishing an alternative route in case of communication failure. On the other hand, Ethernet-PON connects DSIF in significant volume in an economical way.

We carried out experiments in order to evaluate the real-time performance and reliability of the SCADA we have proposed. The system completed ground fault protection within the required time (1 second) in case where an alternative communication route was established within 550 milliseconds by RSTP in Ethernet-ADS.

We considered the feasibility of the SCADA system based on the results of experiments and the state of the art communication technologies. In terms of real-time performance with fault-tolerance, the current RSTP performance should be rapid enough to complete ground fault protection within the required time. It also contributes to the feasibility of the SCADA system to use the real-time specification for Java in the implementation of mobile agents. The scalability of the SCADA system should be ensured by multicast used in the protocol for agent migration and a round trip of mobile agents.

According to these results and considerations, we conclude that the SCADA system we have proposed should satisfy the requirements.


## Acknowledgments

The authors would like to thank Masayuki Ito for his support of the experiments. Our gratitude also goes to Hiroyuki Koda in the Tohoku Electric Power Company. He contributed to designing the configuration of the wide-area network when we worked for our institute.


## References


[1] H. Kobayashi and M. Takasaki, *Demonstration Study of Autonomous Demand Area Power System*, Proc. of Transmission and Distribution Conference and Exposition, 2005/2006 IEEE PES, pp.548–555, Aug., 2006.

[2] N. Okada, *Development of Loop Power Flow Controller*, Proc. of ICEMS 2006, IEEJ, Nov. 2006.

[3] M. Asari, *Ancillary Service for Low Voltage Distribution Network with Demand Supply Interface*, CRIEPI Report R04021, 2005 (written in Japanese)

[4] C. H. Hauser, D. E. Bakken and A. Bose, *A Failure to Communicate*, IEEE Power and Energy Magazine, Vol.3, Issue 2, pp.47–55, Mar/Apr 2005.

[5] Sudip K. Mazumber, K. Acharya and M. Tahir *Towards Realization of a Control–Communication Framework for Interactive Power Networks*

[6] A. Vojdani, *Smart Integration*, IEEE Power and Energy Magazine, Vol.6, Issue 6, pp.71–79, 2008

[7] D. Lange and M. Oshima, *Seven Good Reasons for Mobile Agents*, Comm. of ACM, Vol.42, No.3, pp.88–89, 1999.

[8] T. Otani, *System Configuration and QoS Control of Mobile Agents for a Next-Generation of Distribution System*, IEEJ Trans. on Electronics, Information and Systems, Vol.124–C, No.3, pp.921–928, 2004.

[9] J. Postel, *User Datagram Protocol*, IETF STD0006, 1980.

[10] M. Allman, V. Paxson and W. Stevens, *TCP Congestion Control*, IETF RFC2581, 1999.

[11] V. Paxson and M. Allman, *Computing TCP's Retransmission Timer*, IETF RFC2988, 2000.

[12] T. Otani, H. Kobayashi and Y. Koda, *Performance Evaluation of SCADA System Isolating Fault Section in a Demand Area Power System*, IEEJ Trans. on Power and Energy, Vol.126–B, No.10, pp. 985–993, 2006.

[13] Object Management Group, *OMG Unified Modeling Language$^{TM}$(OMG UML®) Superstructure, V 2.1.2*, 2007.

[14] IEEE, *Standard for Local and metropolitan area networks – Part 3: Media Access Control (MAC) Bridges: Rapid Configuration*, IEEE 802.1W–2001, 2001.

[15] V. Kompella and M. Lasserre (edition), *Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling*, IETF RFC4762, 2007.

[16] Java Community Process, *JSR 1: Real–time Specification for Java*, http://www.jcp.org/en/jsr/detail?id=1.

[17] Sun Microsystems Inc., *Sun Java Real–Time System*, http://java.sun.com/javase/technologies/realtime/.