# An Adaptive Multi-Agent System Application for Power Systems

Juhwan Jung Jong-Woong Choe
LG Industrial Systems, Co., Ltd
Seoul, Korea

Chen-Ching Liu
Electrical Engineering Department
University of Washington, WA, U. S. A.

***Abstract*--When a power system is under stress due to a fault(s) or a disturbance(s), the sources of vulnerability such as human errors, natural calamities, communication system's failures, and hidden failures of protective devices can lead the whole power system to a catastrophic failure. This paper presents a defense system that is able to analyze / minimize the impact of faults or disturbances accompanying with the sources of vulnerability. This paper also proposes a multi-agent system application of the defense system that is designed to provide preventive and corrective self-healing strategies to avoid a catastrophic failure of a power system. Several multi-agent system technologies to build such a defense system are discussed in this paper. This paper is focused on the multi-agent system technologies and the adaptive application to defense a power system from the sources of vulnerability.**

***Index Terms*—Vulnerability, Multi-Agent System, Adaptation, Defense System.**

## I. INTRODUCTION

WHILE power systems are designed to withstand disturbances, there have been several crucial outages that eventually perturb the balance between supply and demand when the disturbances are accompanying with the sources of vulnerability such as human errors, protection and control system failures, gaming in the electricity market, missing or uncertain information in decision making, or a failure of communication systems for critical control signals [1]. In other words, power systems can become vulnerable if the designed protection or control system fails to maintain a high level of reliability in unanticipated and complicated situations. Therefore the fundamental design concept of the control systems should change from 'protection' to 'defense' that is able to reduce the threats from the sources of vulnerability as well as isolate or eliminate the impact of a local event.

There have been numerous efforts on development of defense plans that are regarded to be a part of a complete defense plan against different identified extreme contingencies [2-7]. In [2], the authors define that the primary purpose of defense plans is to detect abnormal system conditions and to take predetermined, corrective actions to preserve system integrity and provide acceptable system performance. Generally the defense plans consist of special protection schemes (SPSs) such as load shedding, generation, or system reconfiguration to maintain system stability, acceptable voltages, or power flows [3]. These defense plans or SPSs can vary from a country to another due to power system characteristics and other considerations. For example, due to the great distance between generation and load, the Hydro-Québec power system deployed a defense plan to preserve the integrity of the whole power grids and to provide the most extensive possible coverage against all possible extreme contingencies [2]. However, these defense plans are not designed systematically so maintenance of detailed control actions in the defense plans is the most common and critical problem. For instance, the SPSs of Bonneville Power Administration (BPA) have to be updated as often as once every three months [7]. Therefore a defense system, which can coordinate / modify various control actions and decision parameters in autonomous, adaptive, and systematic manners, is required.

Generally, human operators perform control actions with the support of decision-making software modules in a centralized control center such as Energy Management Systems (EMS). Thus, most of the information that represents the current power system status has to be transmitted to the control center. However, the time between identification of a potential failure and its occurrence may be too short for effective intervention through centralized control. Since services provided with electric power systems are becoming more complicated, centralized scheduling, operation, and control of power systems may not be feasible or desirable anymore [8]. Therefore, an intelligent, distributed control system is a promising tool to achieve real-time, adaptive, and dynamic control in a large-scale power system [9]. Recent research in distributed artificial intelligence has focused on multi-agent system (MAS) that is a distributed and coupled network of intelligent problem-solving (or decision-making) agents. Multi-agent system technologies have been applied to the defense system in order to tackle the problems of the centralized control system in this paper.

The performance of multi-agent systems can be decided by the interactions among various agents based on the autonomous capability of each agent. In other words, agents should exchange their resources, knowledge, and decisions with each other to determine who does what, when, by what means, with whom, and in what way to solve various sub-problems [10]. One way to achieve these goals is to endow a communication capability to each agent not just to transmit data/information but also to induce coordinated decisions with other agents. KQML (Knowledge Query and Manipulation Language) and FIPA (Foundation for Intelligent Physical Agents) are popular agent communication languages [11-12]. These two agent communication languages are designed based on human speech acts to interchange 'knowledge-level' information.

Due to the uncertainty and complexity of a power system or some large-scale industrial applications, most of the decision-making software modules perform tasks in a dynamic and incompletely known environment. Thus the decision-making software modules of the defense system should be able to adapt and learn in an autonomous manner [13].

The rest of this paper presents a multi-agent system framework, which performs self-healing strategies to defense power systems from the sources of vulnerability, and a prototype application. The proposed system will be refereed to as the Strategic Power Infrastructure Defense (SPID) system that is being developed by the Advanced Power Technologies (APT) consortium, consisting of University of Washington, Arizona State University, Iowa State University, and Virginia Tech.

## II. Design Structure of the SPID System

The ownerships and/or services of generation, transmission, and distribution systems are being unbundled, which creates an environment appropriate for distributed decision-making. Moreover all components (i.e., protective devices, transformers, generators, and so on) in power systems are decentralized and their local goals are different from each other. Even if each component in power systems is designed to perform its local goal(s), power systems should be controlled and monitored from a system-wide perspective as mentioned earlier. However it might be impractical for a centralized control system to manage the whole power grids. Since the decision-making processes of the software/hardware modules in power systems are asynchronous, a scheme, which can coordinate their decisions and can solve possible conflicts among the decisions made by the software/hardware modules, should be considered [13]. Based on the requirements and problems described above, this section presents an architectural analysis of a multi-agent system for the SPID system purposes.

The MAS for the SPID system (hereafter, SPIDMAS) consists of two types of agents. One is a cognitive agent and the other is a reactive agent. A cognitive agent is an intelligent agent that has a knowledge base, comprises all the data and know-how to carry out its task(s), and has a capability to handle interactions with other agents and its environment. The reactive agents in the SPIDMAS work in a stimulus-response manner so each reactive agent does not have to be individually intelligent but the system itself can be an intelligent system to solve complex problems by a designed coordination scheme. The fundamental design concept of having two different types of agent is to consider response-time requirements for power systems. Generally, local controls (e.g., relay tripping signals) should be made in a short time of period while global controls require some computation time. Since the functions and characteristics of the two types of agents are different, a coordination scheme should be deployed. The subsumption architecture is proposed by Brooks [14]. The architecture originally is designed for a robot control system whose control system consists of several layers performing different tasks. The subsumption architecture uses inhibition signals so that the agents in the higher layer can inhibit the decisions / control actions of the agents in the lower layer if needed. Even though only reactive agents are considered for a short-term reasoning process in the Brook's subsumption architecture, basic philosophy has been applied to the SPIDMAS. In other words, the cognitive agents, which can monitor and control the whole power grid, can inhibit the decisions/control actions from reactive agents that perform only local monitoring and control.

The architecture of SPIDMAS has three layers as illustrated in Fig. 1. The lowest layer, the reactive layer, is located in every local subsystem and performs pre-designed self-healing actions that require an immediate response. The agents in the deliberative layer, the highest layer, can analyze the whole system from a global point of view. For instance, the hidden failure of the phase-unbalance relays (i.e., reactive agents) at the McNary power plant tripped all 13 generators in two minutes, which led the power grids (i.e., WSCC system consisting of several western states in U. S. A) to a catastrophic failure in August, 1996 [15]. If there was a control strategy that could analyze the impact of the hidden failure from a system-wide point of view and inhibit the tripping signals, then the August 1996 outage could have been avoidable or the impact could have been reduced. The decisions to inhibit the relays' tripping signals can be made by the deliberative layer as illustrated in Fig. 1. The coordination layer, the middle layer, plays several roles as follows:

- Examine the importance of events/alarms: If a triggering event exceeds a threshold value, the agents in the coordination layer will allow the event to go to the deliberative layer.
- Consistency checking: Since the agents in the deliberative layer do not always respond to the current state, there might be inconsistency between the plans / decisions provided by the deliberative layer and the current state of the power system. If the plans are not consistent

with the real-world model, the coordination layer triggers the deliberative layer to modify the plans. The coordination layer continuously updates the current model of the power system for this purpose.

- Decomposition of plans into actual control signals: Plans received from the deliberative layer may be too condensed. The coordination layer analyzes the plans based on the current model of the power system and decomposes the plans into actual control signals.

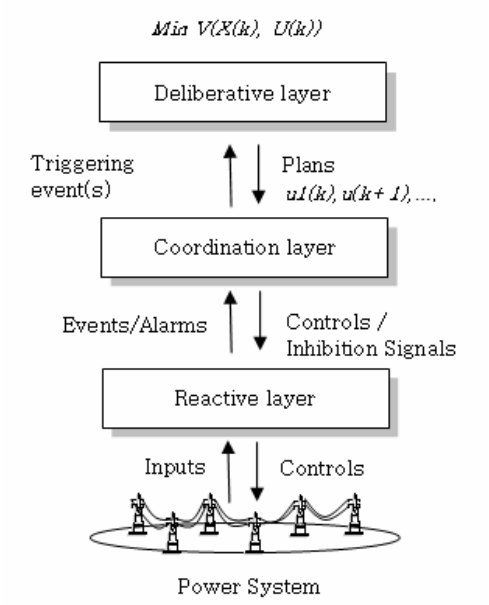


Fig. 1. Hybrid Multi-Agent System Architecture for SPIDMAS

As illustrated in Fig. 1, each agent in the deliberative layer tries to find an optimal control action based on the following optimization problem:

$$\min V(X(k), U(k)), \qquad (1)$$

where,

$$X(k) = \{x_1(k+1/k) \ldots \ldots x_{m-1}(k+1/k) \ldots . x_m(k+N/k)\},$$
$$U(k) = \{u(k+1/k) \ldots u(k+N/k)\},$$

s.t.

$$x_j(k+i+1/k)=F(x_j(k+i/k), u(k+i/k))$$

$x_j(k)$ is the state of the system measured by the $j^{th}$ agent in the reactive layer, $u(k)$ is the control plans made by the agents in the deliberative layer at discrete time instant $k$, $N$ represents the number of control actions or states, and $m$ is the number of reactive agents that send the state information to the agents in the deliberative layer. As represented in the mathematical formulation above, the agents in the deliberative layer decides sequential control actions based on the state information received from the agents in the reactive layer. At $k^{th}$ time instant, the next state is decided by the function of the current state $x(k)$ and the control action $u(k)$ made by agents in the deliberative layer. Let us suppose that $V$ be the vulnerability index that represents how vulnerable the current power system is. Then as represented in (1), the overall objective of the deliberative layer is to find a sequence of control actions, $U(k)$ that is able to minimize the power system vulnerability index, $V$.

## III. The Software Agent in SPIDMAS

Software agents in SPIDMAS and their structure are illustrated in Fig. 2. Based on the design concept as shown in Fig. 1, each agent's functions and information interchange flows are also illustrated in Fig. 2. As mentioned in the previous section, the deliberative capability of the hybrid SPIDMAS is used for vulnerability assessment and development of self-healing strategies.

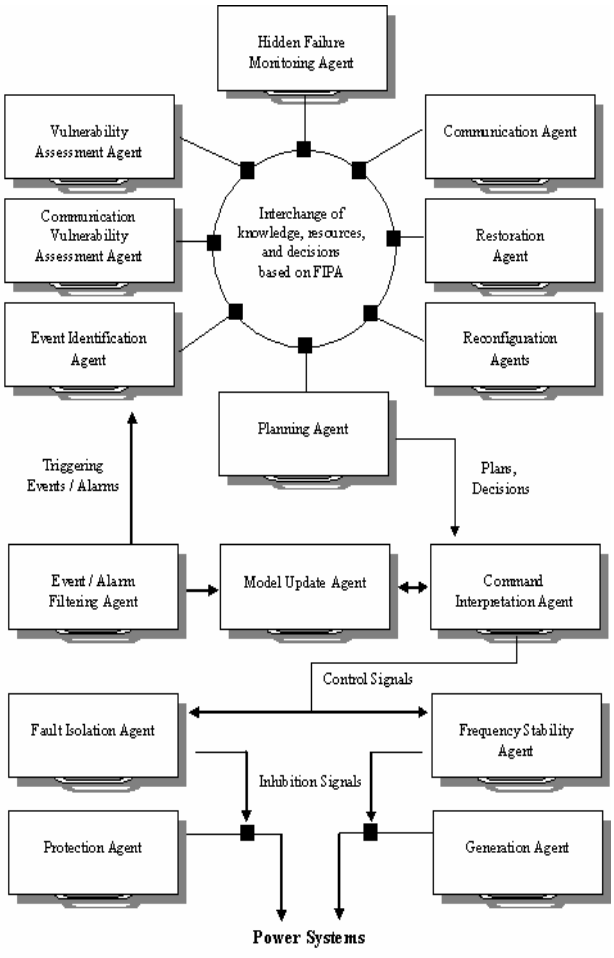


Fig. 2. Software Agents in the SPIDMAS

The lowest layer quickly reacts to system perturbations while the highest layer analyzes the whole system from a wide-area point of view. As discussed earlier, the subsumption architecture is applied for the coordination between these two layers. Each agent in the SPIDMAS is independent of other agents and tries to achieve its individual goals. Based on the context of cooperative interactions, however, the whole system can achieve the

global goal that the whole system pursuits. More detailed definitions and roles of each software agents can be found in [1] so only brief description about the software agents is provided in this section. Based on the design structure shown in Fig. 1 and the definitions of the software agents described in this section, several software agents have been implemented to evaluate the performance of SPIDMAS.

- Protection agent: Each agent represents a computer protective relay modeled by relaying logic and operating condition.
- Generation agent: Each agent represents a generating unit modeled by MW and MVAR capabilities.
- Fault Isolation agent: This agent identifies a fault / disturbance event by protection logics and schemes.
- Frequency Stability agent: Each agent determines frequency control actions by inhibiting actions of Generation / Protection agents.
- Event / Alarm Filtering agent: To avoid excessive events / alarms, this agent evaluates the importance of the events that trigger the deliberative layer.

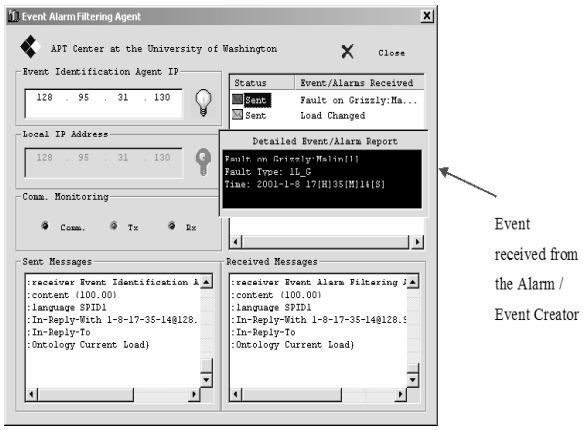


Fig. 3. Event/Alarm Filtering Agent

- Model Update agent: This agent continuously updates the current model of the power system to validate the decisions from the deliberative layer.
- Event Identification agent: The current model of a power system is generated by this agent. The model is shared by all of the agents in the deliberative layer through the agents' communication channel.
- Command Interpretation agent: This agent decomposes the plans received from the deliberative layer into actual control signals based on the current model of the system.
- Vulnerability Assessment agent: This agent assesses power system vulnerability based on the sources of vulnerability and the current model generated by the Event Identification agent.
- Hidden Failure Monitoring agent: This agent investigates hidden failures of protective devices and provides the region of vulnerability.

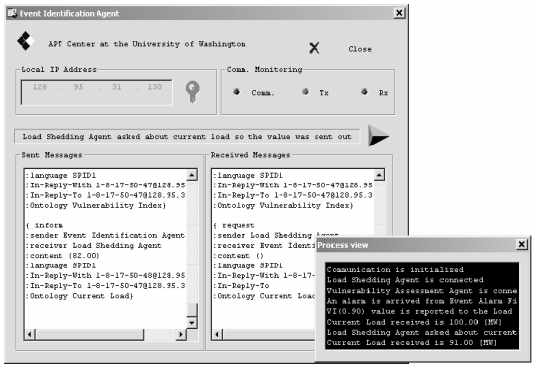


Fig. 4. Event Identification Agent

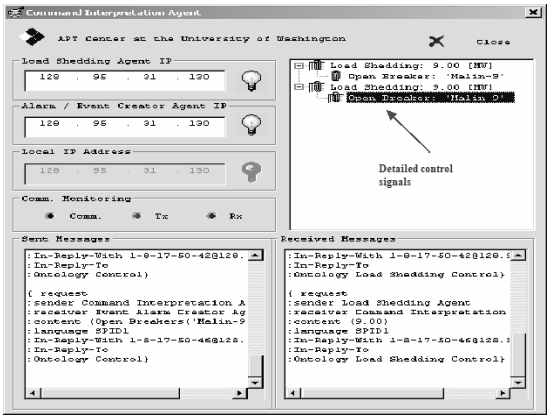


Fig. 5. Command Interpretation Agent

- Planning agent: Based on the self-healing plans provided by the Reconfiguration agents, this agent determines the optimal sequences of the plans.

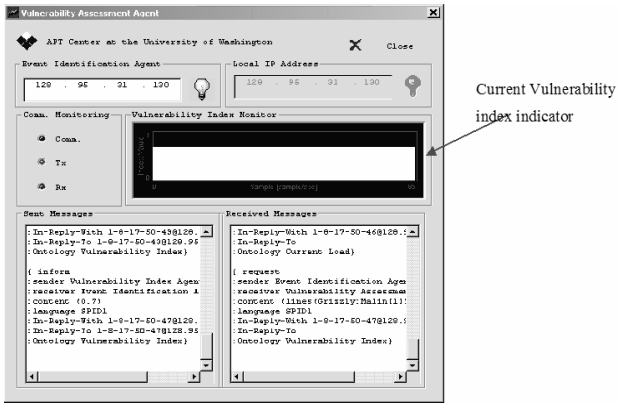


Fig. 6. Vulnerability Assessment Agent

- Communication agent: This agent assesses communication system's vulnerability and provides a fast / safe network path for a critical control signal(s).
- Reconfiguration agents: Each agent provides corrective / preventive self healing control actions (e.g., load shedding) based on the vulnerability assessment. There may be

several agents that provide self-healing strategies but only load shedding agent is implemented as shown in Fig. 7.

- Alarm / Event Creator agent: This agent shown in Fig. 8 is not included in the original SPIDMAS design but this agent is implemented to simulate the protection agents in the reactive layer and a load bus. This agent communicates with the Event / Alarm Filtering and Command Interpretation agents.

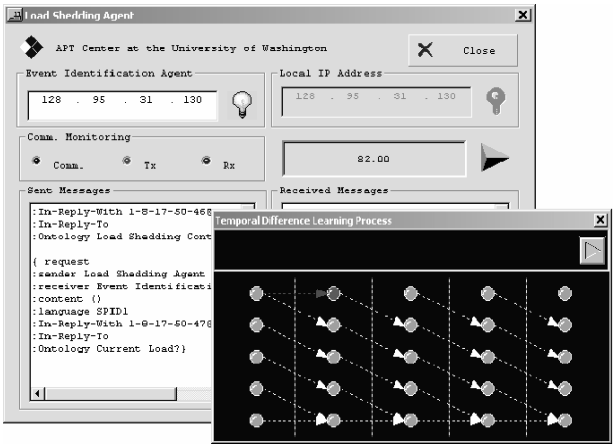


Fig. 7. Load Shedding Agent

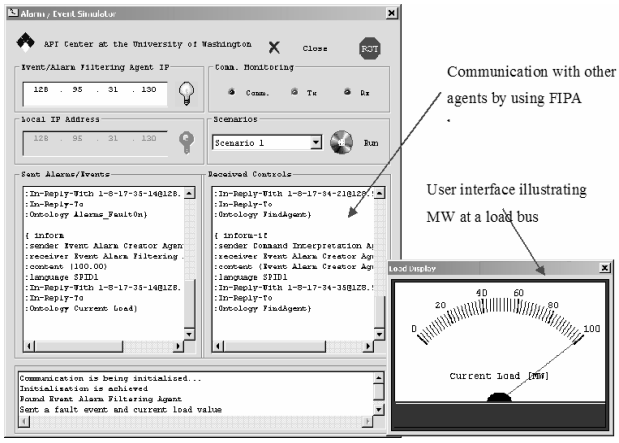


Fig. 8. Alarm/Event Creator Agent

FIPA has been used to implement agents' communication. In order to evaluate the whole system's performance, a 179 bus system that is a variation of the WSCC system model has been tested with the EPRI Extended Transient and Midterm Stability Program (ETMSP). Since the ETMSP is an off-line simulation tool, it is difficult to evaluate the proposed multi-agent system's performance in terms of the system's response time requirement. This issue still might be a challenging when this system is applied to the real field.

The agents perform tasks in a dynamic and incompletely known environment. Thus it is required for the agents to be able to adapt and learn. An important class of methods for such purposes is the supervised learning in which training data is provided to an agent by a supervisor within limited training time. However, it is often difficult for the supervisor to generate representative scenarios. Especially for power systems, constructing an exact model of a real environment is impractical [13]. Therefore, 'reinforcement learning' that does not require the complete dynamics of an environment has been applied to the agents in the SPID system. The temporal difference (TD) learning method has been applied for the reinforcement problem to check the feasibility of an agent's adaptive learning capability with load shedding control schemes. One of the difficulties in TD method is to find an optimal 'learning factor' which decides the convergence of the TD method. In [16], the author provides a proof of the convergence of the TD method. However, the proof is not directly applicable for the agents in the SPID system. In reference [17], the proof is revised to find the optimal learning factor for the agents in SPIDMAS.

## IV. Conclusion

Due to the existence of various sources of vulnerability, a power system can be in a vulnerable situation that may eventually lead to a catastrophic failure. The SPID system, which can assess power system vulnerability and perform self-healing control actions, is proposed in this paper. The proposed defense system is designed with multi-agent system technologies in order to provide greater flexibility and intelligence. The major functions that the SPID system can provide are:

- Ability to identify hidden failure modes and identify the region of vulnerability,
- Ability to perform system-wide vulnerability assessment,
- Ability for the power system to take self-healing control actions through reconfiguration,
- Ability to monitor and control the power grid with a multi-agent system designed to reduce the power system's vulnerability.

The openness and flexibility of the conventional EMS control center are limited when the size and structure of the interconnected power systems are rapidly changing. The multi-agent system technologies applied to SPIDMAS are expected to tackle these problems. This paper presents the prototype of the SPIDMAS in order to check the feasibility of the FIPA agent communication language and the TD method for agent's adaptive learning capability. More detailed descriptions about the efficiency of deploying FIPA and TD method can be found in [17].

The time requirement for a decision making process in the proposed multi-agent system framework depends on complexity of the goals that agents try to achieve. From the power system's control perspective, the agents in the reactive layer should provide control actions in a few

hundred milliseconds while the time requirement for a decision making process of the deliberative layer can vary from a few seconds to minutes. More detailed specifications of the time requirement can be decided in the development stage.

Another challenging issue may be the precise and robust coordination of agents' activities because knowledge, information, and control strategies in a multi-agent system are distributed. A systematical method that can evaluate the overall quality of the agents' team work should be studied.

## V. ACKNOWLEDGEMENT

This research is sponsored by U. S. Department of Defense and Electric Power Research Institute through the Complex Interactive Networks/Systems Initiative, WO 8333-01. We would like to thank Drs. Massoud Amin, Ram Adapa, EPRI, and Robert Launer, DoD, for their leadership and guidance.

## VI. REFERENCES

[1] C. C. Liu, J. Jung, G. T. Heydt, V. Vittan, and A. Phadke, "Conceptual Design of the Strategic Power Infrastructure Defense (SPID) System," *IEEE Control System Magazine*, August 2000.

[2] G. Trudel, S. Bernard, and G. Scott, "Hydro-Québec's Defense Plan Against Extreme Contingencies," *IEEE Trans. Power Systems*, August 1999, pp. 958-966.

[3] B. K. Lereverend, Cigré G05 of Study Committee 39, *Industry Experience with Special Protection Schemes*, Elcetra No. 155, August 1994.

[4] NERC Planning Standard September 1997, North American Electric Reliability Council. Available in NERC web site: www.nerc.com.

[5] C. Counan, M. Trignon, E. Corradi, G. Bortoni, M. Stubbe, and J. Deuse, "Major Incidents on the French Electric System: Potentiality and Curative Measure Studies," *IEEE Summer Meeting*, August 1993, pp. 879-886.

[6] O. Faucon and L. Dousset, "Coordinated Defense Plan Protects Against Transient Instabilities," *IEEE Computer Applications in Power*, July 1997, pp. 22-26.

[7] M. E. Coultes, D. L. Gold, J. R. Taylor, and P. J. Traynor, "An Operations View of Special Protection Systems," *IEEE Trans. Power Systems*, August 1988, pp. 1078-1083.

[8] G. P. Azevedo, B. Feijo, and M. Costa, "Control Centers Evolve with Agent Technology," *IEEE Computer Applications in Power*, July 2000, pp. 48-53.

[9] S. Talukdar, V. C. Ramesh, R. Quadrel, and R. Christie, "Multiagent Organizations for Real-Time Operations," *IEEE Proceedings*, May 1992, pp. 765-778.

[10] M. Wooldridge, "Agent-based Software Engineering," *IEEE Proceedings of Software Engineering*, February 1997, pp. 26-37.

[11] Y. Labrou and T. Finin, *A Proposal for a new KQML Specification*, Computer Science and Electrical Engineering Depratment, University of Maryland. Available in web site: www.cs.umbc.edu/kqml.

[12] L. Chiariglione, *FIPA 98 Specification*, Foundation for Intelligent Physical Agents. Available in web site: www.celt.it/fipa/spec/fipa98/fipa98.htm.

[13] R. S. Sutton, A. G. Barto, and R. J. Williams, "Reinforcement Learning is Direct Adaptive Optimal Control," *IEEE Control System Magazine*, April 1992, pp. 19-22.

[14] R. A. Brooks, "Intelligence Without Reason," *Artificial Intelligence Journal* (47), 1991, pp. 139-159.

[15] Western Systems Coordinating Council, *Disturbance Report for the Power System Outage that Occurred on the Western Interconnection*, August 10, 1996. Approved by the WSCC Operations committee on October 18, 1996.

[16] R. Sutton, "Learning to Predict by the Method of Temporal Differences," *Machine Learning*, vol. 3, pp. 9-44.

[17] J. Jung, C. C. Liu, S. L. Tanimoto, and V. Vittal, "Adaptation in Load Shedding Under Vulnerable Operation Condition," Accepted by *IEEE Trans. on Power Systems*, 2002.

## VII. BIOGRAPHIES

**Juhwan Jung** He received Ph. D. degree from the University of Washington, Seattle, WA, in 2002. Dr. Jung's are of interest includes power systems, AI system applications, and Information Technology. He is currently with LG Industrial Systems, Korea.

**Jong-Woong Choe** He received Ph. D. degree from ChungNam National University, Korea. He is currently a vice president of LG Industrial Systems, Korea. Dr. Choe's interests are power system control, Information Technology, and signal processing.

**Chen-Ching Liu** He is currently Professor of EE and Associate Dean of Engineering at the University of Washington. Dr. Liu serves as Director of the Advanced Power Technologies (APT) Consortium and Electric Energy Industrial Consortium (EEIC) at the University of Washington. He is a Fellow of the IEEE.