SANDIA REPORT
SAND2000-1004
Unlimited Release
Printed March 2001

Operating Environment and Functional Requirements for Intelligent Distributed Control in the Electric Power Grid

Douglas C. Smathers and Abbas A. Akhil

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of
Energy under Contract DE-AC04-94AL85000.

Approved for public release; further dissemination unlimited.

Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Printed in the United States of America. This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865)576-8401
Facsimile: (865)576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.doe.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd
Springfield, VA 22161

Telephone: (800)553-6847
Facsimile: (703)605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/ordering.htm

SAND2000-1004
Unlimited Release
Printed March 2001

Operating Environment and Functional Requirements for Intelligent Distributed Control in the Electric Power Grid

Douglas C. Smathers
Secure Networks and Information Systems Department

Abbas A. Akhil
Electric Surety Department

Sandia National Laboratories
P. O. Box 5800
Albuquerque, New Mexico 87185-0455

ABSTRACT

The restructuring of the U.S. power industry will surely lead to a greater dependence on computers and communications to allow appropriate information sharing for management and control of the power grid. This report describes the operating environment for system operations that control the bulk power system as it exists today including the role NERC plays in this process. Some high-level functional requirements for new approaches to control of the grid are listed followed by a description of the next research steps that are needed to identify specific information management functions.

Prepared for the
Transmission Reliability Program
Office of Power Technologies
Assistant Secretary for Energy Efficiency and Renewable Energy
U.S. Department of Energy

The work described in this report was funded by the Assistant Secretary of Energy Efficiency and Renewable Energy, Office of Power Technologies of the U. S. Department of Energy.

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under contract DE-AC04-94AL85000.

CONTENTS

1. Introduction

The U.S. electric power industry is undergoing a major restructuring. The U.S. Federal Energy Regulatory Commission (FERC) is well along in its efforts to create competitive wholesale power markets, to separate management of generation from transmission, and to assure nondiscriminatory access to all users of the power grid. The substantial changes in the character of participants in the bulk power markets and significant increases in the number and complexity of transactions associated with greater competition has affected bulk power reliability. A number of findings from the Department of Energy Power Outage Study Team (POST) are related to the transition to competitive energy service markets [1]. These changes will surely lead to a greater dependence on computers and communications to allow appropriate information sharing for management and control of the power grid. This report describes the operating environment for system operations that control the bulk power system, as it exists today including the role NERC plays in this process. Some high-level functional requirements for new approaches to control of the grid are listed followed by a description of the next research steps that are needed to identify specific information management functions. The focus of the discussion is to show how evolving intelligent agent technologies can facilitate and improve the reliability of control of the power grid. This project seeks to develop and demonstrate a practical role for multi-agent systems in real-time operation of the bulk power system. Multi-agent systems are proving successful for other information management applications in other industries and promise to revolutionize the way information is shared for control of the power grid. Intelligent agents, which learn from past events and change their behavior to adapt to new conditions, may be particularly valuable in this environment [2].

The North American Electric Reliability Council (NERC) is a voluntary organization of power industry members that has specified operating procedures to assure reliability in the delivery of power since interconnected operations became widespread in the 1960's. The key concept for reliable operation of the power grid has been the Control Area. Recently, NERC established the Control Area Criteria Task Force to reconsider how reliability functions should be allocated among the participants in the new competitive power industry. The results of their deliberations will surely result in significant changes in the operating environment in which control functions are performed.

The initial focus of this research is investigating requirements for and developing intelligent agents to mediate and coordinate information sharing between Control Areas and Security Coordinators. The industry must develop a way to balance the conflicting goals of open markets with free access to information for all and security from information system intrusions which would introduce bogus data or shut down computers due to data overload or malicious software viruses. The next steps are to research information flows in detail and to identify necessary information management functions at each node in the control network.

Managing the reliability of the North American electric power grid is a very complex task performed by many individuals located throughout the continent. An essential requirement for this control system to operate effectively is the acquisition and exchange of information among the participants in a timely, reliable, and secure manner.

It is convenient to consider the electric power system in three parts. Generation refers to the power plants that produce electric energy for the Bulk Power System. Transmission refers to the high-voltage transmission lines that carry power from generation the distribution systems. Distribution refers to the network that carries power from the transmission system to individual power users. The Bulk Power System included generation and transmission. This report only addresses the evolving control need of the Bulk Power System.

Power industry equipment vendors have started to address distribution system automation with distributed intelligent agents. While these early products [3] are not very intelligent, private industry research and development appears to be adequately addressing this need.

Reliability in the power industry consists of two requirements: adequacy and security. To achieve adequacy of supply, a power system must have available at all times, i.e., dispatch, sufficient generation resources to meet the projected demand or load plus some reserves and sufficient transmission capabilities to carry the power to distribution systems for delivery to users. A unique characteristic of a power system is that electricity must be generated at the same instant that it is used. To minimize power disturbances to users, the power system is operated so that it can continue to supply all users even when a major component fails. This is called first contingency operation. Security of the power system is achieved when it can withstand a set of credible contingencies.

A complex information system is required to support the control functions for reliable operation of a power system. Reliability of a distributed information system has a different set of requirements. Communication links are needed to transmit information between control center locations. Usually redundant communication links using different physical routes and, if possible, different technologies are needed. Compatibility of information format must exist between the two ends of a communication channel. The Secretary of Energy Advisory Board (SEAB) Task Force on Electric Reliability highlighted the importance of this issue. In a recent report, the Task Force recommended that an appropriate, non-proprietary standard for communications among control centers be adopted and an appropriate, non-proprietary database access standard for control centers be adopted [4]. In addition, the Task Force recommended that the Self-Regulating Reliability Organization (SSRO) specify information management protocols that will ensure the complete interoperability of system operations records in compliance with the Federal Energy Regulatory Commission (FERC) Orders 888 and 889. The last requirement for a reliable information system is resistance to cyber attacks. The Task Force recognized the trend toward increasing utilization of computer networks for information management and the growing vulnerability to cyber threats. They recommended that the DOE examine information assurance issues for the interconnected electric system and establish appropriate cooperative programs to address these issues as warranted [5].

Recent congressional testimony to the Joint Economic Committee from a leading U.S. cyberwar expert voiced his concern for the threat of cyber attacks. "The very same means that the cybervandals used a few weeks ago could also be used on a much more massive scale at the nation-state level to generate truly damaging interruptions to the national economy and infrastructure." Another expert testified that hackers do not have the sophistication to successfully attack the U.S. power grid, but Russian military and intelligence services do [6].

2. Operating Environment for Control of the Bulk Power System

The electric system of the United States, Canada, and a part of Baja California Norte, Mexico comprise three interconnects: the Eastern Interconnection, the Western Interconnection, and the ERCOT Interconnection. Each interconnection operates synchronously at 60 Hertz but not synchronously with the other interconnections. Power can be transmitted from one interconnection to another through direct-current connections. For each of the interconnections to operate safely, reliably, and provide dependable service to its customers, it must be continuously monitored and controlled. A key concept for reliable operation of the power grid is the Control Area. This monitoring and control function is distributed among the Control Areas that comprise the Interconnection.

A Control Area is an electrical system bounded by interconnections or interties to adjacent Control Areas. All parties benefit from operating in an interconnected grid. All power flowing across the interties must be scheduled ahead of time. It is the Control Area's responsibility to directly control its generation to continuously balance the actual interchange with the scheduled interchange. In addition, a Control Area must help the entire interconnection regulate and stabilize its AC frequency. A Control Area only deals with bulk power generation and transmission. Distribution of power to customers is monitored and controlled by a separate control center.

3. Role and Activities of the North American Electric Reliability Council

The North American Electric Reliability Council (NERC) is a voluntary industry group that sets the operating policies for all entities using the interconnected power grid. Its mission is to promote the reliability of the electricity supply for North America. It does this by reviewing the past for lessons learned, monitoring the present for compliance with Policies and Standards, and assessing the future reliability of the bulk electric system. To ensure cooperation among the Control Areas, NERC has established rules for reliable electric system operation and monitors performance to tell if the rules are applied in a fair and nondiscriminatory manner for all participants in the electric power market. NERC is a not-for-profit corporation whose "owners" are the Regional Councils. Ten Regional Councils promulgate additional rules for operation of a Control Area in their regions. An electric utility or some other entity is certified to operate a Control Area. Often a Control Area contains several utilities and other entities. For example, most of New Mexico is contained in one Control Area operated by Public Service Company of New Mexico (PNM). The PNM Control Area has interties with seven adjacent Control Areas. PNM is in the Western Interconnection but has one direct-current connection with a Control Area in the Eastern Interconnection. The Western Interconnection has 33 Control Areas extending from Alberta and British Columbia in the north to Baja California Norte, Mexico, Arizona, New Mexico and a piece of Texas near El Paso to the south. All of the Western

Interconnection is in a single regional reliability council, the Western Systems Coordinating Council (WSCC).

The NERC Board of Trustees established the security coordinator function in May 1996 to establish requirements for the sharing of data and information about the "health" of the Interconnection, to establish an Interregional Security Network for each Interconnection, and to establish a network of Security Coordinators. The functions of the Security Coordinators are to provide security assessments and emergency coordination for the Control Areas within the Region and across Regional boundaries [7].

Recently, the North American Electric Reliability Council (NERC) established the Control Area Criteria Task Force to reconsider how reliability functions should be allocated among the participants in the new competitive power industry [8]. It is important to define the functions and responsibilities that must exist to ensure the reliability and information security of the interconnections. The Task Force is charged with:

1. Define the functions and responsibilities for ensuring real-time operating reliability of the Interconnection.
2. Define the roles of entities that may provide all or part of the functions or responsibilities for security.
3. Define the relationships of entities with each other for ensuring operating reliability.
4. Identify the incentives and obligations for being a Control Area and remove the economic advantages of performing the reliability functions.
5. Several other questions related to Control Areas.

The Task Force will report its recommendations to the NERC Security Committee in anticipation of new procedures or Operating Policy changes as appropriate. The results of Task Force deliberations will surely result in significant changes in the operating environment in which control functions are performed. Smathers from Sandia participates on the Task Force.

Current thinking of the Task Force envisions a three-level reliability hierarchy as shown in Figure 1. The lowest level entities have the most market interest while the upper-level entities are mostly concerned with grid reliability. The Task Force has identified several dozen reliability functions. Some functions will be the exclusive responsibility of one entity while others may be shared among several entities. The organizations that currently perform the reliability functions have evolved over time so there are different structures for different Control Areas. The reliability functional entities are allocated functions but this does not mean to imply that each entity will be a separate and independent organization. It is anticipated that different Control Areas may have different structures in the future.

3rd LEVEL (Interconnection)

ISN (Interregional Security Network)

Among Security Coordinators within each respective Interconnection
(Data exchanged across Interconnection boundaries as needed)

2nd LEVEL (Subdivision of Interconnection)

Security Authority

For Defined Area
One or more covering 100% of Interconnection

LOWEST LEVEL (ENTITY)

Generator
- •Single plant/single unit
- •Single plant/multiple units
- •IPP
- •Self Serve
- •Fleet of plants/units - common control
- •Generation Aggregator (Every source of Generation connected to the Grid)

Transmission Provider
- •Each operator of segments of an overall grid
- •Transmission Aggregator under common control (Includes every segment of the grid within a defined

Load Serving Entity
- •Wholesale
- •Retail (Each load served within a defined area
- •Reserves

Figure 1. NERC Reliability Hierarchy

Major changes to NERC Operating Policies require considerable time for deliberation, review, and consensus building. Once a policy change is proposed, NERC employs "due process" to solicit industry and public comment before a policy change will be approved and implemented. The earliest that major policy changes are likely to occur is 2002. NERC itself is in the middle of a transition from a voluntary industry group to a Self-regulating Reliability Organization (SRO). If legislation currently in Congress is passed, a SRO will assume NERC's responsibility for power grid reliability but will also have enforcement authority. With all these changes in the works, it is no wonder that the software vendors to the power industry have not shown much interest in this area. But it is the right time for new approaches and new information technologies to be considered for research.

4. Functional Requirements for Control of the Power Grid

Operating the electric power grid requires the successful execution and smooth coordination of a large set of complicated functions by the participants in the electric power market. This report only deals with those functions directly related to information management at a Control Area. Intelligent agents could benefit a range of other functions such as system planning, maintenance planning, power marketing, transaction scheduling, outage restoration, accounting and billing, and operations compliance reporting but these will not be considered here.

A System Operator has the responsibility to maintain reliable power delivery to bulk power users. A Control Area control center often has several System Operators on duty each shift in order to perform all the required functions in a timely manner. The System Operator is provided with system planning studies, maintenance schedules, load forecasts, transmission system models, generation unit operating capabilities, generation unit economic analysis, interchange schedules, contingency analysis studies, and real-time metering data from throughout the Control Area.

The System Operator employs a number of software tools to help him review and respond to all the information that continuously arrives at the control center. A modern control center typically has a number of computer workstations connected to a set of servers communicating over a local area network. As new data arrives at the control center, it is placed in a database so that all software tools have immediate access to information about current grid operating conditions. The suite of software applications that support the System Operator is called an Energy Management System (EMS). The exact software tools installed at a control center vary slightly from Control Area to Control Area due to the historical evolution of the control center and which control software vendor provided the EMS. Some Control Areas need to accommodate additional operating agreements among its participants so the real-time control functions are even more complex. The following functions are typical software tools in an EMS, but do not reflect what is installed at any particular control center.

Supervisory Control and Data Acquisition (SCADA)

The SCADA function collects real-time status data about current conditions of the power grid and allows the System Operator to actuate circuit breakers and other remotely controlled equipment. The SCADA function is controlled by a software application at the control center. The SCADA communicates with Remote Terminal Units (RTU) located at substations and generating stations throughout the Control Area. Data are updated every 2-4 seconds.

The type of data collected by the SCADA system are real and reactive power flows (MW and MVAR), voltages on substation buses, circuit breaker position, motor-operated disconnect (MOD) switch position, and generator unit MW output. In addition, energy flows (MWH) at metering points around the gird are collected from pulse accumulators at the end of each hour. The hourly data are used for both energy accounting and billing and for control performance monitoring. The supervisory control portion of SCADA allows the System Operator to operate a circuit breaker or MOD switch in order to energize or de-energize a transmission line, a shunt capacitor bank, a shunt reactor on a transmission line, or to change the tap on Tap Changing Under Load (TCUL) transformers.

State Estimation

The state estimation function is a software application at the control center that uses available real-time metered data to estimate the voltage and phase angle at every bus on the grid. This is necessary since not all buses are measurement points for the SCADA system. The estimates are based on the real-time SCADA data, grid model data such as transmission line impedance, and current grid configuration data. The state estimator can identity inconsistencies that indicate bad metering data.

Alarm Processing

The alarm processing function checks to see if any circuit breaker has changed state or if any power flow voltage level is outside pre-established operating limits. If an alarm condition is detected, it produces an alarm message for the System Operator to warn that operator action is required.

Automatic Generation Control (AGC)

The AGC function is responsible for monitoring Area Control Error (ACE) and requesting changes in Control Area generation in order to bring ACE to an acceptably low level. ACE is the difference between Control Area load (native load) and Control Area generation plus net interchange with other Control Areas plus a frequency bias term to account for a Control Area's contribution to regulating the frequency of the Interconnection. A more detailed definition of ACE is in Appendix 1A of the NERC Operating Manual [9].

A generator unit can be set to one of three AGC control modes:

- Base Mode - unit used for ACE control.
- Ramp Mode - AGC uses System Operator entered values for scheduled unit commitment to ramp to a new value of generation output. Unit does not respond to ACE control.
- Off - Unit is not on AGC control. Generation System Operator controls generation output.

NERC policies require that a portion of generation units be operated in Base Mode. ACE calculations are performed on a 2-4 second cycle.

Economic Dispatch

When a Control Area controls a number of generation units, it is possible to satisfy ACE requirements in a number of different ways. The economic dispatch software analyzes current conditions and tries to adjust the generation allocation of each unit to minimize the total cost of generation. In addition to raw cost of generation, there are a number of other restrictions and limitations that must be considered. This analysis is performed on a 5-10 minute cycle. Adjustments recommended by the economic dispatch application are passed to the AGC application for implementation.

Generation Reserve Monitoring

A Control Area operator must arrange to supply adequate power to meet all loads this instant but must also provide operating reserves to meet all loads as demand changes over the next minutes and hours. There are formal policies specifying how much operating reserve is required, how quickly it must be available, and how to credit diverse types of generation resources toward the operating reserve requirements. Operating reserves are accounted for using two classes. Regulating reserves, responsive to AGC, provide for normal deviations in ACE, primarily due to errors in load forecasting. The second class is contingency reserves. A contingency is the unscheduled loss of a generation unit, transmission line, transformer, or other major system component. The contingency reserves must be adequate to continue power delivery when the utility's largest resource hazard fails. Resources for contingency reserves must be able to be ramped up within 10 minutes. A portion of contingency reserves can be loads that have agreed to be interrupted when a contingency occurs. Utilities typically reduce their contingency reserve obligations by joining a reserve-sharing group with neighboring utilities. In this way, each member only has to provide a portion of the contingency reserves needed by the whole group. The generation reserve monitoring application calculates the actual operating reserves that are available minute to minute, compares the result with the operating reserve requirements, and alarms the System Operator when operator intervention is required.

Dispatcher Power Flow

This power flow analysis application uses the real-time data collected by the SCADA system and results from the state estimation application to calculate the power flow on the entire transmission system. Conditions where pre-established operating limits are exceeded can be identified and corrected. If detailed bus-load forecasts are prepared, then the dispatcher power flow application can be used to investigate potential problems with particular future system loading conditions of interest.

Contingency Analysis

This application automatically configures the data sets to analyze a specific set of transmission line outage contingencies. The analysis is performed by the dispatcher power flow application. Any problems identified by this analysis are displayed to the System Operator so he can take preventative action.

Block Load Shedding

This application allows the System Operator to trip, and later restore, predetermined large blocks of customer load during an emergency when immediate action is required to prevent a cascading outage.

Inter Control Center Communications

Recently, more information exchange is required among Control Areas and between Control Areas and a security coordinator. Digital communication protocols have been developed to manage this information interchange. Usually, dedicated, redundant communication circuits are used for real-time data exchange.

5. Data Flow Requirements

The data flows required to perform real-time control at a Control Area are shown in Figure 2. This section lists the types of data exchanged between locations. Details of how the data are stored in the Control Area vary from Control Area to Control Area but portions of the data must be made available to the functions listed above. Figure 3 shows the data flows associated with planning and marketing functions that support real-time control but are not modeled in detail. They provide the reference information necessary to understand the configuration of the system and the power transaction schedules that are to be followed by the System Operator. The power marketing entity in Figure 3 is also known as a Purchasing-Selling Entity (PSE).

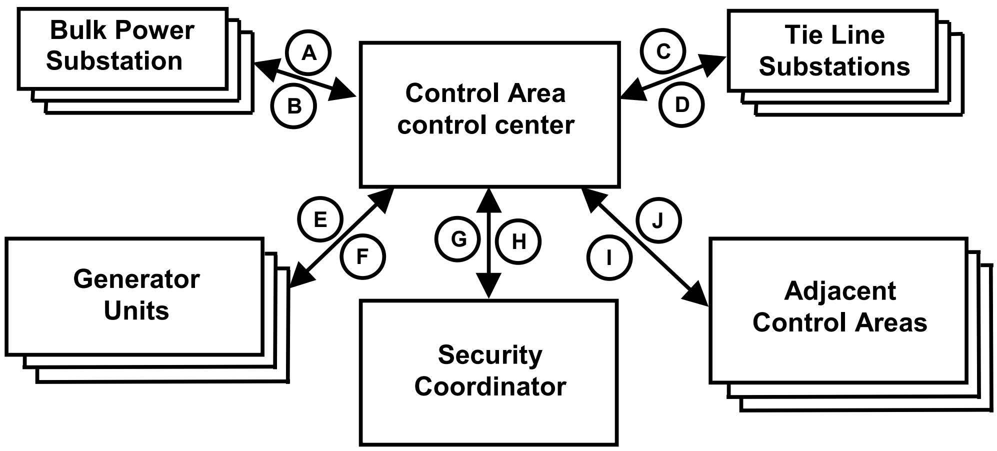

Figure 2. Data flows for real-time operations at a Control Area

A) Bulk power substations to Control Area control center
- Voltage level at substation buses (KV).
- Power flow for each transmission line at substations (MV and MVAR).
- Circuit breaker positions at substations (Open/Closed).
- Substation and communication system alarms (Various).

B) Control Area control center to bulk power substation
- Commands to open or close a circuit breaker or switch (Open/Close).
- Commands to change a transformer tap position (Go to position N).
- Commands to activate or de-activate line reclosers (Activate/De-activate).

C) Tie line substations to the Control Area control center
- Same data flows as A) with the following addition:
- Line flow at each tie line metered with pulse accumulator (MWH).

D) Control Area control center to tie line substations
- Same data flows as B)

E) Generator units to Control Area control center
- Generator unit output (MW and MVAR).
- Generator unit auxiliary loads (MW).
- Generator unit AGC mode status (Base/Ramp/Off).
- Generator unit maximum/minimum operating limit under AGC (WM and MVAR).
- Generator unit generation schedule for units not on AGC (MW and MVAR).

- Substation and communication system alarms (Various).
- Report generator unit ramping schedule (MW/min, Start and Stop time).
- Report generator unit capability status (MW and MVAR).
- Generator unit startup and shutdown schedule (Startup/Shutdown/Date/Time).
- Notification of problems affecting unit capability (MW, MVAR, Date/Time).
- Notification of requirement to do unscheduled shutdown of unit (Date/Time).
- Estimate for returning generator unit to service (Date/Time).

F) Control Area control center to generator units
- Commands to change AGC mode (Base/Ramp/Off).
- Command generator unit schedule for units not on AGC (MW and MVAR).
- Command generator unit ramping schedule (MW/min, Start and Stop time).
- Commands to change generator unit set point value for units on AGC (MW and MVAR).

G) Security Coordinator to Control Area command center
- Notify Control Area of transaction curtailment to relieve constrained facilities (Transaction ID).
- Notify Control Area of generation unit redispatch per transmission load relief (TLR) procedure (Generation unit, MW and MVAR).
- Notify Control Area of transmission reconfiguration according to TLR procedures (Transmission ID, configuration changes).
- Notify Control Area of required load curtailment (Location, MW).

H) Control Area command center to Security Coordinator
- Proposed interchange transaction schedules (MW and MVAR, Start time, Stop time).
- Bus voltages for major substations (KV).
- Power flows for major transmission lines (MW and MVAR).
- Actual or potential generation deficiencies in the Control Area (Location, MW and MVAR).
- Emergency or planned equipment outages (Equipment ID, Date/Time).

I) Adjacent Control Areas to Control Area command center
- Hourly contingency reserve quota from Reserve Sharing Group manager (MW).

J) Control Area command center to adjacent Control Areas
- Hourly projections for next day firm load and largest contingency hazard to Reserve Sharing Group manager (MW).
- Actual contingency reserves to Reserve Sharing Group manager (MW).
- Emergency assistance requests to Reserve Sharing Group (MW).
- Verify Net Interchange Schedule (MW, Time).
- Establish short-notice revised schedules (MW, Time).

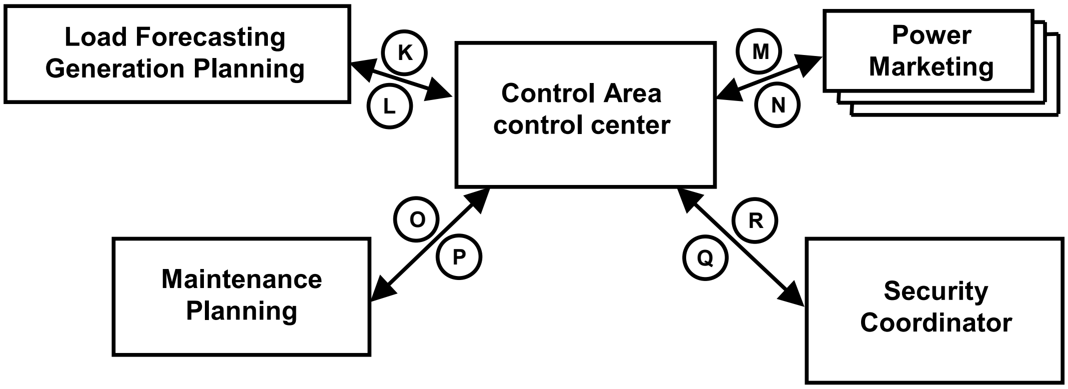

Figure 3. Data flows for planning and scheduling at a control center

K) Load forecasting and generation planning to Control Area control center
- Hourly native load (load within the Control Area) forecast for the next day (MW tabulated by hour and location).
- Hourly generation unit dispatch for next day (Unit, MW and MVAR).

L) Control Area control center to load forecasting and generation planning
- Requests for adjustments to generation unit dispatch as needed for projected operating limit violations (Unit, MW and MVAR).

M) Power marketing to Control Area control center
- Hourly schedules for native loads within the Control Area (Location, MW).
- Schedules for approved interchange transactions (MW, Date/Time).
- Requests for approval of interchange transactions sourced in Control Area (MW, Date/Time).
- Requests for approval of interchange transactions that sink in the Control Area (MW, Date/Time, ancillary services, transmission path).

N) Control Area control center to power marketing
- Approval of schedules for native loads within the Control Area (Location, MW).
- Approvals of interchange transactions that sink in the Control Area (Approve/ Deny/Pending).
- Approval of interchange transactions sourced in the Control Area (Approve/Deny/Pending).

O) Maintenance planning to Control Area control center
- Scheduled maintenance outage plans for generation resources (Unit, MW, Date/Time).
- Scheduled maintenance outage plans for transmission facilities (Line, Date/Time).

P) Control Area control center to maintenance planning
- Requests for adjustments to generation outage schedule (Unit, MW, Date/Time).
- Requests for adjustments to transmission outage schedule (Line, Date/Time).

Q) Security Coordinator to Control Area control center

- Approvals of interchange transactions, which sink in Control Area (Approve/Deny/Pending).

R) Control Area control center to Security Coordinator

- Request for approval of interchange transaction, which sinks in Control Area (MW, Date/Time, ancillary services, transmission path).

6. Grid Model for Detailed Data Flow Analysis

The IEEE Reliability Test System (RTS) [10] will be the basis of a grid model used to develop a network of intelligent software agents. The RTS defines a 24-bus system with 32 generation units located at 10 of the buses. The buses are connected with 38 transmission lines. Extensive operating conditions are defined for the RTS including weekly peak load, daily peak load, and hourly peak load conditions; transmission line impedance and rating data; forced outage rates and duration; and generation unit operating parameters. An expansion of the RTS was presented at an IEEE Power Engineering Society conference in 1996 but has not been published. It expands the test system by linking three copies of the RTS. Some additional modifications and extensions, such as defining Control Areas, will need to be made to provide a realistic model to demonstrate the operation of an intelligent agent system.

7. Potential Benefits of Intelligent Agents to Information Management

The initial application of intelligent agents for real-time control of the power grid focuses on Control Area functions related to interchange schedule management, reserve monitoring, and Area Control Error. A multi-agent system is a group of intelligent agents that communicate with each other and work cooperatively to achieve common goals. Although agents have been used for a wide range of applications, they are not a universal solution to complex problems [11]. A number of agent applications have been deployed even though agent technology is relatively immature. It is important to have a clear and detailed understanding of the problem to be solved and then to identify clear benefits of an agent approach before beginning development of an agent application. Up to this point, we have concentrated on understanding the operating environment and potential functions that agents could perform. Subsequent work will make a detailed information flow model and define a software requirements specification. Since no standard engineering practices have emerged for developing multi-agent systems, it is important to build a prototype system to demonstrate that the system performs as desired and that undesired behaviors would not occur.

A number of research organizations are working on multi-agent systems for a number of important applications. The use of deliberative, autonomous agents in high-consequence applications, such as control of the power grid, will require a commensurate level of protection and confidence in the predictability of system-level behavior. The required level of assurance has not yet been thoroughly discussed, much less attained. We use the term "surety" to mean an appropriate balance between safety, security and reliability. Much of the focus in intelligent agent and multi-agent systems has centered on fundamental issues of architecture and attaining basic performance. While all the tools required to design and build multi-agent systems are not in place at this time, significant progress is being made. The Federation for Intelligent Physical Agents (FIPA) has been established to share research results and develop useful standards for multi-agent systems. In a sense, real-time control of the power grid is currently a distributed control system since each Control Area operates independently. The Energy Management System (EMS) applications require frequent and detailed system operator interactions. Intelligent agent systems promise a new approach to managing information.

Sandia National Laboratories has developed many of the elements of a comprehensive development environment that humans can readily use to organize and dispatch multi-agent systems to perform demanding, high-consequence tasks with enhanced security, stability, and robustness. This environment could be used to organize and initialize multi-agent systems for command and control or other collaborative activities. In addition to providing a development environment needed for use in Sandia's national security missions, the environment appears to be very appropriate for developing multi-agent systems for national infrastructure protection, i.e., improving the reliability of the power grid, managing the exchange of information among participants in a competitive power industry, and protecting from cyber attacks.

The agents we are targeting are complex yet realizable software programs that are situated in and interact with their environments, have sophisticated deliberative and learning mechanisms, and can be viewed as autonomous entities. Malfunctions in individual agents must neither destroy the multi-agent system nor keep it from its objectives. Building such objects and organizing them into systems that achieve high-consequence results requires (1) formal scientific and theoretical framework that accounts for large numbers of agents with complex interaction dynamics; (2) pervasive surety foundation; and (3) the requisite engineering implementation tools.

We have made significant progress towards this formally motivated engineering environment. Our research is expanding the issues of agent autonomy, mobility, communications, security and rationality toward a theory of realization. If multi-agent systems are to be successfully deployed and verified for high-consequence applications, we must be able to engineer and enforce non-functional as well as functional properties. Ideally, one wants to have a high level of confidence that a multi-agent system will perform as designed and that the behavior of the system is bounded -- specifically, that unacceptably bad behaviors will not occur.

8. Conclusions and Recommendations

Real time control of the power grid, at the bulk power level, is in transition as the industry undergoes restructuring. The amount of information, primarily in the form of interchange transactions, is expected to grow dramatically as additional participants enter the power markets. The growth of distributed generation will also add to the amount of information that a Control Area must deal with to perform its real time control functions. Current practices, which involve significant operator interactions, will not be able to handle and respond to all the additional information. The reliability Policies formulated by NERC are also in a significant state of revision.

We recommend the first functions to be performed by an agent-based system will be to mediate communications between Control Areas and Security Coordinators. In addition to relieving the operators from routine information management functions, the agents will have advanced cyber-security capabilities and will employ secure multiparty cryptography to ensure robust operations immune to external cyber attacks and certain attacks from malicious insiders.

The agent-based systems will initially appear to be a new layer of complexity over legacy Energy Management Systems but as agent's behaviors become understood, additional functions can be incorporated into the agents.

To test the agent-based control system, a ten-agent prototype will be built and tested.

References

[1] "Findings and Recommendations to Enhance Reliability From the Summer of 1999", Final Report, Power Outage Study Team, U. S. Department of Energy, March 2000, p S-2

[2] For additional details about major thrusts in restructuring, refer to the CERTS White Paper on "Real-Time Security Monitoring and Control of Power Systems" by G. Gross, A. Bose, C. DeMarco, M. Pai, J. Thorp, and P. Varaiya, Office of Power Technology, U. S. Department of Energy, August 30, 1999, pp 33-35

[3] IntelliTEAM ® Overview of Operations, " EnergyLine Systems, Alameda, CA. www.energyline.com

[4] "Maintaining Reliability in a Competitive U. S. Electricity Industry: Final Report of the Task Force on Electric Systems Reliability," U. S. Secretary of Energy Advisory Board (SEAB), U. S. Department of Energy, September 29, 1998, pp. 96-97

[5] IBID. p. 98

[6] Vernon Loeb, "Cyberwar's Economic Threat", *Washington Post*, February 24, 2000, p. A19

[7] "Policy 9 - Security Coordinator Procedures", North American Electric Reliability Council, *Operating Manual*, pp. P9-1 through P9-5, September 15, 1998. Available from www.nerc.com/~oc/operman1/html

[8] Charter and current activities of the Control Area Criteria Task Force are available at www.ner.com/~oc/cactf.html

[9] The Area Control Error (ACE) Equation, Appendix 1A, Operating Manual, North American Electric Reliability Council, Princeton, NJ: Dec. 3, 1996, pp. A1A-1 through A1A-4. Available from www.nerc.com/~oc/operman1html

[10] "IEEE Reliability Test System", *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-98, no. 6, pp. 2047-2054, Nov./Dec. 1979

[11] M. J. Wooldridge and N. R. Jennings, "Pitfalls of Agent-Oriented Development, "*Proceedings of the 2nd International Conference on Autonomous Agents*, Minneapolis, USA, 1998, pp. 305-391.

Distribution

3 US Department of Energy, EE-15
Office of Power Technologies
1000 Independence Avenue, SW
Washington, DC 20585-0121
Attn: Philip Overholt

3 Lawrence Berkeley National Laboratory
1 Cyclotron Road
Berkeley, CA 94720
Attn: Joseph Eto, MS 90-4000

1 Southern California Edison
2131 Walnut Grove Ave.
Rosemead, CA 91770
Attn: Carlos Martinez

2 Pacific Northwest National Laboratory
P.O. Box 999
Richland, WA 99352
Attn: Jeff Dagle, MS-K5-20
Carl Imhoff

2 Washington State University (2)
School of Electrical Engineering and Computer Science
P.O. Box 642714
Pullman, WA 99164-2714
Attn: Anjan Bose
David Bakken

1 Electric Power Group
201 South Lake Avenue, Suite 400
Pasadena, CA 91101
Attn: Vikram Budhraja

1 Cornell University
428 Phillips Hall
Ithaca, NY 14853
Attn: Robert Thomas

1 Oak Ridge National Laboratory
P. O. Box 2008, MS 6186
Oak Ridge TN 37831-6186

Attn: Marilyn Brown

1	MS 0449	Jason Stamp	6516
1	MS 0451	Ronald Trellue	6501
1	MS 0451	Jennifer Nelson	6515
1	MS 0455	Reynold Tamashiro	6517
2	MS 0455	Steven Goldsmith	6517
1	MS 0455	Laurence Phillips	6517
2	MS 0455	Douglas Smathers	6517
1	MS 0741	Marjorie Tatro	6200
2	MS 0741	Abbas Akhil	6201
1	MS 1140	Samuel Varnado	6500
1	MS 9011	Barry Hess	8910
1	MS 9018	Central Technical File	8945-1
2	MS 0899	Technical Library	9619
1	MS 0612	Review & approval Desk For DOE/OSTI	9612