MEĐUNARODNO REGIONALNO SAVETOVANJE O ELEKTRODISTRIBUTIVNIM MREŽAMA

REGIONAL CONFERENCE AND EXHIBITION ON ELECTRICITY DISTRIBUTION

Crna Gora, Herceg Novi, 5 - 8. oktobar 2004. / ***Montenegro, Herceg Novi, October 5 - 8, 2004***

* *

APPLICATION OF SCADA SYSTEMS IN DEREGULATED POWER SYSTEMS

J. Car[1], Pupin Institute, Belgrade, Serbia and Montenegro

G. Jakupović, Pupin Institute, Belgrade, Serbia and Montenegro

J. Trhulj, Pupin Institute, Belgrade, Serbia and Montenegro

INTRODUCTION

Modern power control systems emerged as a consequence of technical and technological progress and complex control demands, and were developed as decentralized architectures, consisting of hardware and software modules. By using the information technology at all levels of control, power companies may offer better quality of service and lower electricity prices. Supervisory Control and Data Acquisition Systems (SCADA) developed in order to fulfill control needs of Power Utility of Serbia both at transmission and distribution level has almost all features which satisfy the needs of a modern power system. In the circumstances of establishing a deregulated power market, the advantages of the use of one such supervisory and control system become increasingly significant, Trhulj (10). Today's society is dependent on computer networks that are used to control the infrastructure that makes everyday life possible. The use of embedded systems in the control systems of increasingly complex technological society also makes the question of its security more sensitive.

DEVELOPMENT OF SCADA/EMS SYSTEMS

In the mid-twenties of the last century measuring devices were developed which enabled telemetering of the basic features of a power system: frequency and power. Subsequently the control methods were developed and the first rules of energy dispatch were laid down. Although the importance of the load frequency control (LFC) has been realized, the methods of precise measuring of frequency and the power interchange were still not established. Along with the spread of interconnective systems and the breakthroughs in the control, telemetry also experienced significant development. The application of radio transmission became widespread, allowing collection and display of data from distant locations. However, even until the 1960s, primarily the analog computers were used. The application of digital computers in control systems led to the replacement of analog calculations for regulation methods. Development of computer programming sped up the progress of methods for the defining of the system reliability, Cohn (1).

---

[1] *Jelena Car, Pupin Institute, Volgina 15,Belgrade, Serbia and Montenegro*
jelena.car@automatika.imp.bg.ac.yu

In November 1965, US power system experienced a massive blackout which consequently led to the formulation of new demands on the power supervision and supply, Wollenberg (2). Prior to this event, US utility companies used two independent real-time control systems. The first system consisted of analog computers connected to measurement transducers and generating plants, performed Load Frequency Control, and Economic Dispatch (ED) calculations. The other system, called a Supervisory Control System, was realized using relay logic in order to allow remote control of substations. Using circuit breakers, the transmission lines and substation transformers were turned on and off. When digital computers were introduced, the acquisition of measurements from substations was also made possible, and this system was renamed SCADA (Supervisory Control and Data Acquisition). However, what was lacking was a reliable procedure for testing the ability of a system to withstand disturbances occurring in its parts. Thus, special teams used to make daily schedules of the operation of the power system based on the archival information gathered from previous years, and possible worst-case scenarios. This made system operators totally blind for any events that were not included in the daily schedule. Although the use of digital computers and their ability to be reprogrammed greatly influenced the development of control systems, the computers of that time were not capable of "guiding" the operators in the case of a disturbance. As a result of the investigation of the causes of 1965 blackout, there emerged an idea to equip control systems with powerful computers that would operate online, and be able to perform the analysis of a power disturbance at regular intervals. Those applications and the other that followed them formed the base of what is now known as Energy Management Systems (EMS) at production and transmission level and Distribution Management System (DMS) at distribution level.

The role of real-time communication protocol in the increase of EMS reliability

After the major blackout of US power system in August 2003, numerous studies were made analyzing the causes of power failure and a possibility for preventing this from occurring in the future, Babb (3). Two concepts were presented to increase the reliability of the system: improvement and regular maintenance of the transmission system, and the addition of new functions to a SCADA/EMS system. In deregulated power market the maintenance of transmission structure is more demanding than making improvements to the SCADA systems, since it requires large investments for repair and continuous maintaining of the equipment quality. Besides, by improving the SCADA systems a much efficient functioning is achieved of the entire power transmission and distribution system. Independent power suppliers in the United States use different types of SCADA systems, which are usually not connected Although each supplier is obliged to protect the neighboring systems from failures at the local level, the real-time communication between different SCADA systems would enable supervision of the grid at a regional level. By rapid identification and localization of a failure in a part of the system, protective measures can be taken to prevent the failure from bring down the entire power grid. Next generation of intelligent measuring devices will be able to synchronize their measurements using the Global Positioning System (GPS), thus providing better and more precise monitoring of the state of power system. According to the theory of optimal control, the observability of power system increases our ability to control it. If we were able to detect instabilities in a certain part of a power grid, it would take only a fraction of a second to return the system to its stable state by taking the appropriate control action, Adamiak i Premerlani (4).

Workstations and personal computer networks, which replaced old main-frame computers, made possible a decentralization of the control systems. Communication between various networked computers became standardized. Today, the real-time data exchange between intelligent electronic devices and other parts of the control system is governed by the international standard (IEC60870-6 TASE.2), in the form ICCP-TASE.2 (Intercontrol Center Communications Protocol). The protocol defines the principles of communication between the control centers, substations, power plants, EMS, SCADA systems and metering equipment in the electric and gas utility suppliers. TASE.2 protocol also defines ways of real-time connectivity of deregulated power systems. Figure 1. shows the position of the TASE.2 protocol in relay of SCADA data to a local grid and beyond, to other parts of an power system. It is precisely the absence of real-time communication between SCADA systems of different power utilities in the US that was singled out as a possible cause of the August 2003 blackout.

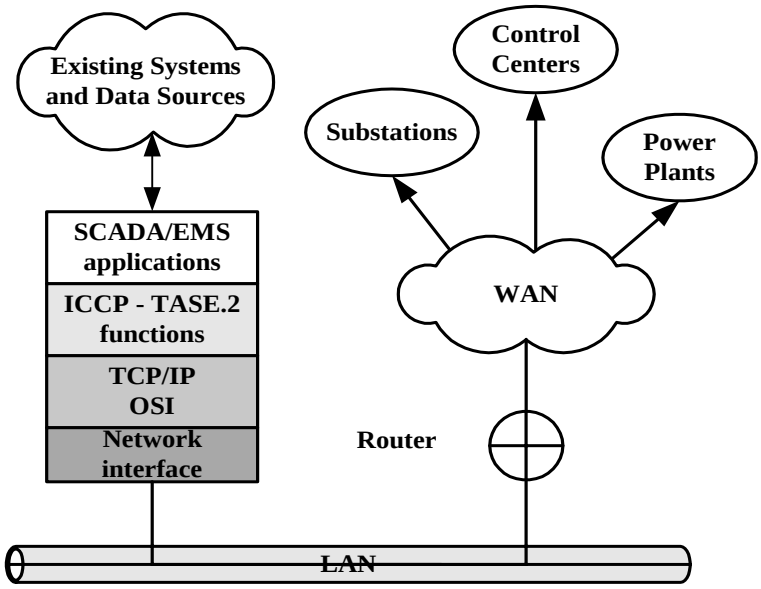

Figure 1 - ICCP-TASE.2 Protocol in SCADA/EMS

DECENTRALIZATION OF CONTROL SYSTEMS

Decentralization of control systems, followed by the advances in the communications, directed the development of software architectures in control centers towards open architectures, Azevedo i Oliveira (5). Open architecture requires a system to have the following properties:

- portability
- interoperability
- expandability
- modularity and
- scalability

Portability presents the ability to run the software independent of hardware/software platform used, thus enabling the use of appropriate hardware. The choice of the most appropriate equipment suitable for a specific action can thus be made based on the price and performance, so is no longer limited by the selection of a specific vendor, or whether the vendor will stay in business. Full portability has not yet been achieved as it depends on standards applied (POSIX – Portable Operating System Interface, etc …), and on the operating systems (UNIX and Linux operating systems can be implemented in almost all hardware). Also, the emergence of the Java programming language, which can be applied on practically all hardware platforms, enables larger degree of portability, Locke i Dibble (6). Portability of graphical interfaces can be achieved by using web browsers, thus replacing X-Windows or Motif (*NETVIEW* system, web based application for dynamic monitoring in power system). Portability becomes fully important if at the same time the system achieves interoperability, that is, if it is possible to run identical or different software modules within the same network using various hardware, or various operating systems. Transformations and restructuring of electric power companies placed demands on SCADA systems for much wider forms of communication than those used so far limited to local/power company networks. Standardization of data models for the power control systems is defined by a standard that describes a Common Information Model (CIM). The control center should be able to support the expansion of the power system and the inclusion of new software functions and features while maintaining an adequate level of performance. This constitutes the expandability and has to be allowed for when SCADA software is designed. By a careful design of system architecture at a macro level, and by using object-oriented software techniques, system can also incorporate modularity. Modularity enables exchange of the parts of software, software modules, their removal or integration into the system without affecting the operation of the other parts of the system.

Modularity makes the exchange of modules in a SCADA system a routine operation, and simplifies the adjustments of the system required to suit an individual user, or changes in the existing system, thus extending the exploitation lifetime of the system. A step further in the universality of the modular concept can be achieved by transforming software modules into autonomous units which communicate and exchange data in a universal communication language, using architectures such as Common Object Request Broker Architecture (CORBA). In this way limitations by non-standard database models can be overcome. Modular structure of SCADA systems enables another important feature of an open architecture – scalability. Scalability, within the context of SCADA/EMS/DMS systems, is the ability of software to operate in control centers of various sizes and structures, by selecting the appropriate application modules.

VIEW2 SCADA SYSTEM

Modern SCADA systems (such as VIEW2 SCADA system developed at the Mihajlo Pupin Institute, Belgrade, and installed in regional grids, Figure 2.), are being designed as distributed supervisory-control systems with client-server architecture. The system consists of one or more computer components located in the center, to which remote terminal units (RTU) are installed.

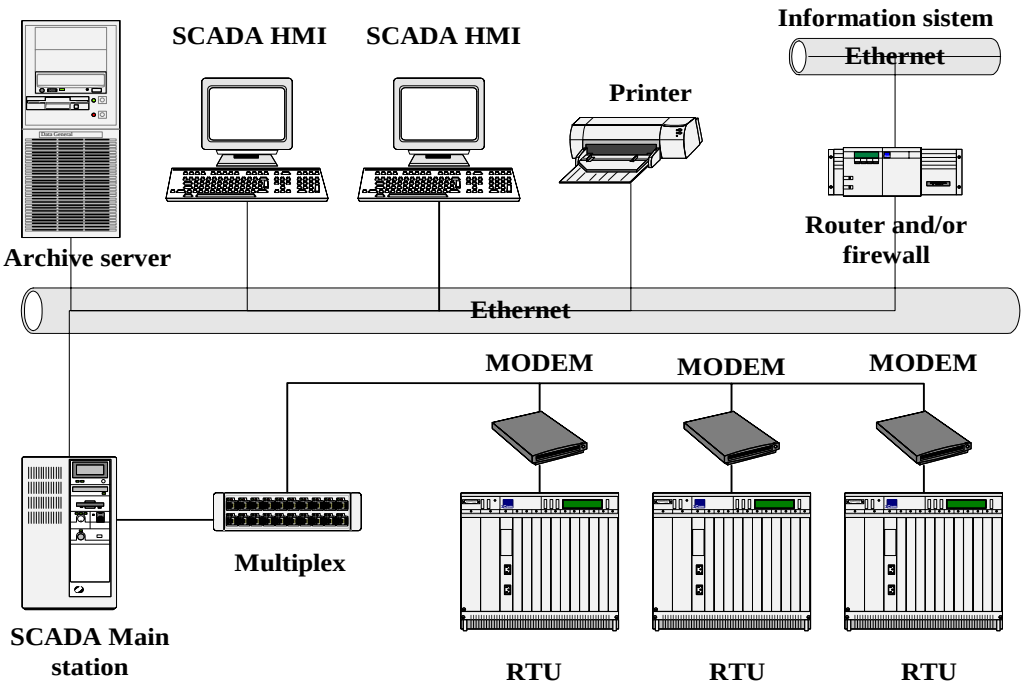

Figure 2 - SCADA/EMS System

Characteristics of the system are:

- Standard hardware and software technologies;
- Fulfill OPEN technology demands to achieve full interconnectivity of hardware/software products made by different vendors;
- Full portability;
- As distributed supervisory-control system, VIEW2 enables full scalability and expandability;
- Structured and vector graphics HMI with zoom/pan layers;
- Capable to connect to other SCADA applications over TCP/IP layer by ICCP TASE.2 protocol;

- RTU connectible by different protocols: IMP Protocols (ATLAS SST, ATLAS MAX, Micro ATLAS), other protocols (Rade Koncar protocols 801T, 803T, IEC standard protocols 60870-5-101, 60870-5-103, 60870-5-104, DNP 3.0);
- System can be tailored by customer demands because it is developed with standard software technologies: UNIX (POSIX), TCP/IP LAN and WAN network, X windows systems and Motif based user interface, RDBM server with ODBC connectivity.

If we would to compare basic features of VIEW2 SCADA system with features that define modern distributed supervisory-control systems having an open architecture, we would conclude that VIEW2 SCADA system fulfills all the criteria that define such systems. SCADA/EMS/DMS system for transmission and distribution allows a simple configuration of a system into a SCADA/EMS or SCADA/DMS system, thus achieving a wide applicability of the platform in dispatch control centers, both at the level of generation and transmission and at the level of distribution systems.

SECURITY OF THE CONTROL SYSTEMS

Massive blackout of the part of the EMS in the United Sates in 2003 was not a result of a catastrophic breakdown, but rather of a cascading process that followed a minor failure. If the reliability of a system is defined by its capability to maintain the functioning over some period of time and under certain conditions, we can say that the reliability is a measure of the system quality. Also, we can define the survivability of a system as a combination of reliability, availability, security and safety. Every component of the system contains these four factors which ensure successful operation of the entire system. Many internal factors (malfunctioning components, complexity of a system that causes faults in normal operation) and external factors (working environment, various forms of attacks) operate on each component, thus compromising system survivability. The use of structured models allows system reliability to be derived from determined reliabilities of its components. The probability that a complex system can survive depends explicitly on each of the constituent components and their interrelationships. Modern society has become dependent on computer networks that control infrastructures (including energy grids, oil and water pipelines, transportation systems, etc.) that sustain everyday life. Information technologies that are imbedded in the infrastructure make the society more complex and efficient, but also more vulnerable in terms of security. With the computerization of industries that use and develop infrastructure, the risk of disruption of operation from a range of enemies has increased, whether it comes from hackers who see this as an entertainment, or from terrorists who seek to cause major disturbances, or from failures due to natural disasters or the complexity of systems. Electric infrastructure should have a priority when allocating funds for maintaining security, since the functioning of the entire society (telecommunications, transportation, industry, banking, various services, and the basic living conditions in urban areas) depends on the stable and reliable operation of this resource. It has become quite clear that it is essential to make EMS optimized in order to increase its reliability in everyday operations in which massive breakdowns can occur due to a cascading effect of a minor fault occurring in one of its part. Basic demand concerning the survivability of a system is that it maintains basic control functions when parts of it fail. The implementation of protective mechanisms is to a large extent made difficult due to a geographic distribution of electric power systems and due to a presence in the system of a large number of devices with numerous input nodes that are vulnerable to hacker attacks. The additional difficulty is posed by the fact that the system is not interoperable, so that the different protocols that protective intelligent electronic devices use to communicate with PLCs, RTUs, PCs, and other SCADA systems limit the attempts to protect the communication between the center and substations. Besides the diversity of the devices used in the system, different communication media are often used between system parts (commercial and leased phone lines, wireless communication, optical fibers), thus posing additional demands when protective model of a system is defined, Sheldon i Potok (7).

Protection of EMS is being developed in these different areas:

- securing network and telecommunication assets
- modeling and analysis of robust and fault-tolerant systems
- developing architectures with a higher level of survivability

Infrastructure protection starts at the level of individual components, by installing protective mechanisms and methods that mitigate causes of failure, thus increasing component survivability. In the next phase, protective mechanisms are being installed in hierarchical system models and serve to protect against failures due to the complexity of engaging unanticipated component interactions. During the addition of optimization techniques with a goal of increasing the security of the specific parts of the system we can monitor the effects of the applied protection on the system operation and the consumption of the available resources. We differentiate between the protection from accidental faults and from intentional faults or intrusions. By combining these protective techniques we can achieve greater robustness and survivability, but on the other hand we risk depleting resources necessary for proper system operation. An ideal system would be self-managing and resistant to changes in its environment. It should contain the following capabilities:

- Self-configuration – Automated configuration of components according to high-level policies. Rest of the system adjusts automatically
- Self-optimization – Components in the system continually check opportunities for improving their own characteristics
- Self-healing – System automatically detects, diagnoses, and repairs software and hardware problems
- Self-protection –System automatically defends against cascading failures or outside attacks, by using early warning to prevent system-wide failures.

Also, these systems should be able to understand, learn from, and respond intelligently to events which they encounter for the first time, and therefore provide a secure protection against unforeseen intrusions, Sheldon i Potok (8).

Validity of metering information in a control system

Validity and protection of metering information from unauthorized use or misuse is particularly important in deregulated power systems in which the production, transmission and distribution of power is performed by various companies. Metering information, in this case the amount of produced and transmitted power, should be verified by an independent entity and be kept in a database that can be accesses by all parties involved in a contract. Thus, regardless of the way the power is being traded, whether it is sold to the end user or there is a power exchange, it is necessary to have one independent entity which performs metering according to duties defined in a contract. This entity needs to own metering devices and to perform metering at various locations, and that metering information needs to be valid and be managed based on contracts and agreements. The independence of this entity ensures the validity of information for all participants in trade or exchange. There are several questions that emerge when considering the integrity and the independence of metering information:

- Who should own, maintain and read meters at different locations?
- Who should own the metering data, and thus have the right to have them at their disposal, or make them available to third parties?
- Who should have a license to access data obtained from meters at different locations of the system?
- Based on what principles should licenses to access data be given to third parties (for making load forecasts, statistical analyses, etc.)?

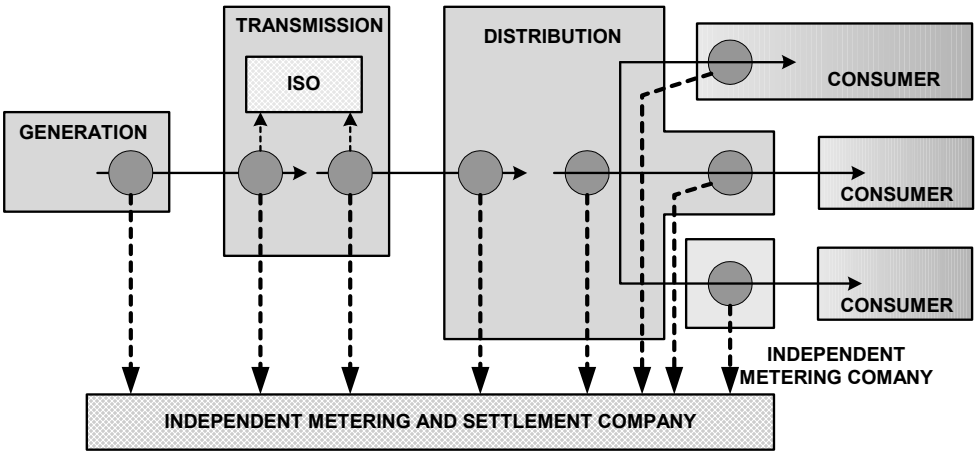

Figure 3 - Metering places in Power System

Answers to the above questions allow definition of the rules of the trade, that would prevent certain parties to dominate in a monopolistic way in the process of production, exchange or trade of power. Figure 3. shows the necessary metering locations for gathering data on power flow, as well as metering information based on which contract responsibilities are fulfilled. Producers of electric power meter the produced and delivered amount of power, transmission utilities continually control the power flow in their part of the grid, and the distribution utilities meter power delivered to consumers, while individual consumers can operate their own metering devices or use metering systems of other companies. All metering locations send data to the independent entity (agency or a committee), which does not perform metering but ensures the validity of the data, and issues licenses for data access according to contracts, Hreinsson (9).

CONCLUSION

In this paper we present the evolutionary path of the control systems used in electric power production, transmission and distribution. We discussed the events that led to the definition of rules for supervision and control, and which led to the realization of the importance of specific methods for increasing the reliability of power production and distribution systems. Technological progress, development of software, and the emergence of information technologies brought a new concept in the organization of power control systems. Information technologies that are imbedded in the infrastructure make the society more complex and efficient, but also more vulnerable in terms of security. Control systems based on the application of modern information technology become increasingly important in deregulated power market, which is subject to frequent and profound changes.

REFERENCES

1. Cohn N., 1984., "Recollections of the Evolution of Realtime Control Applications to Power Systems", Automatica, Vol. 20, No. 2, pp. 145-162
2. Wollenberg B. F., 1996., "An Engineer's Perspective on the 1965 Blackout", Power Generation Operation and Control, Wiley Europe, March
3. Babb M., 2003, "Were control systems responsible for the U.S. blackout?", Control Engineering Europe, October
4. Adamiak M., Premerlani W., 1999., "Data Communications in a Deregulated Environment", IEEE Computer Applications in Power, Vol. 12, No. 3, July, pp 36-39
5. Azevedo G. P., Oliveira F. A. L., 2001., "Control Centers with Open Architectures", IEEE Computer Applications in Power, Vol. 14, No. 4, October , pp 27-32
6. Locke D. C., Dibble P. C., 2003., "Java Technology Comes to Real-Time Applications", Proceedings of the IEEE, Vol. 91, No. 7, July pp. 1105-1113
7. Sheldon F. , Potok T. et all, "Energy Infrastructure Survivability, Inherent Limitations, Obstacles and Mitigation Strategies", www.csm.ornl.gov/~sheldon/public/ SheldonPwrCon03-434-801.pdf

8. Sheldon F. , Potok T., Loebl A., et all, "Autonomic Approach to Survivable Cyber-Secure Infrastructures", www.csm.ornl.gov/~sheldon/public.pdf
9. Hreinsson E.B., September 2-2002, "Requirements For An Electricity Trading Infrastructure In A Small Deregulated Hydro-System", Technology Impact European Electricity Markets (TELMARK) Discussion Forum, 4, Kingston University, London, UK
10. J.Trhulj, G.Jakupović, N. Čukalevski, M. Stojić, 2002, "Komparativna analiza postojećih nadzorno-upravljačkih sistema prenosnih i distributivnih EES", Odeljenje za upravljanje EES, IMP