SMART POWER GRID SECURITY SERVICES: RISK MANAGEMENT APPROACH CONSIDERING BOTH OT AND IT DOMAINS CASE STUDY: SHIRAZ POWER DISTRIBUTION COMPANY

Mina Sajjadi
Shiraz Power Distribution Company
mina_sajjadi@yahoo.com

Babak Niknia
Next Generation Solutions Company
babak.niknia@gmail.com

ABSTRACT

Now a day, many progresses in both Information Technology and Power System Operation domains lead to outspread their applications in power distribution systems. Convergence of utility business information technology (IT) and power system operation technology (OT) are bringing new protocols, analysis and performance challenges for interoperable end to end security risk management systems. Unified risk management approaches are critically needed to effectively guide resource allocations, identify best practices on the basis of practical and meaningful benchmarks and demonstrate various regulatory and business compliances for both the control systems and business domains. Implement an appropriate security system on the network has the advantage that at any time, depending on the alert, network will go to a secure position in terms of both topology and information system. This paper presents essential characteristics and properties for security risk management approaches in the context of the smart power grid. The work is typically illustrated using the network architecture of Shiraz Power Distribution System.

INTRODUCTION

The power distribution companies have been utilizing advances in operation systems as well as communication and information technology over the years in order to improve efficiency, reliability, security and quality of services.

The Smart Grid (SG) is envisioned to be an automated, digitalized, widely distributed energy delivery network. It will be characterized by mutual flow of electricity and information, enabling the monitoring of a wide range of components within the grid in real. [1]

The tendency to Smart Power Grid is to take the advantage of all modern technologies in intelligent power grid to facilitate: [2, 3, 4, 5]

- Better situational awareness and operator assistance.
- Autonomous control actions to enhance reliability by increasing resiliency against component failures and natural disasters, and by eliminating or minimizing frequency and magnitude of power outages subject to regulatory policies, operating requirements, equipment limitations and customer preferences. Such control actions can be more responsive than human operator actions.
- Efficiency enhancement by maximizing asset utilization
- Resiliency against malicious attacks by virtue of better physical and IT security protocols.
- Integration of renewable resources including solar, wind, and various types of energy storage. Such integration may occur at any location in the grid ranging from the retail consumer premises to centralized plants. This will help in addressing environmental concerns and offer a genuine path toward global sustainability by adopting "green" technologies including electric transportation.
- Real-time communication between the consumer and utility so that end-users can actively participate and tailor their energy consumption based on individual preferences (price, environmental concerns, etc.).
- Improved market efficiency through innovative solutions for product types (energy, ancillary services, risks, etc.) available to market participants of all types and sizes.
- Higher quality of service – free of voltage sags and spikes as well as other disturbances and interruptions – to power an increasingly digital economy.

Among these trends and facilities, system reliability is the main priority for design and operation of modern grids.

As a result of Smart Grid, the power grid operational system is developing from an isolated network of computers running stand alone applications on a proprietary platform to highly interconnected system in a large information and communication systems. Obviously, vulnerabilities and risks in such system are very different in size, scope, probability and frequency of occurrence than ones in traditional system. [6] Convergence of Information Technology (IT) and power system Operation Technologies (OT) are bringing new protocols, analysis and performance challenges for practical security risk management systems.[7, 8, 9]

This paper discusses a different approach for security risk management in a Smart Power Grid. These services are functionally pervasive, topologically distributive but flexible in supporting traditional and smart grid characteristics. Such systems need to balance the challenges of different security conditions that the OT system warrants and the availability and data integrity that IT system warrants. Such solutions should be aware of the differing of safety and cascading impacts that external attacks, malicious inside breaches, or erroneous operations could have on the power grid or the information systems.

There are three Main contributions to the work. At first, all parts of a smart power grid and operation information system will be considered and it will be illustrated that these activities require secure automated information exchange, analysis intelligent decision making throughout the grid. Secondly, a unified smart grid cyber security service is presented and it's response to changes in the power and/or information system is considered due to security, reliability and stability events. Third, a

methodology has been employed to evaluate security risks and finally it is concluded that according to different data collection devices and various analysis software to correlate them with other power system and customer data and control elements in a smart power grid, it is essential to develop a distributive but sensitive security risk analysis and control systems.

CONVERGENCE OF OT AND IT IN SMART GRID

The Smart Grid consists of many operation information systems such as Energy Management System (EMS), Distribution Management System (DMS), Supervisory Control and Data Acquisition (SCADA), Advanced Metering Infrastructure (AMI), Customer Information System (CIS) and Outage Management System (OMS). The interconnection between mentioned systems allows the companies, customers and other service providers not only to monitor energy exchange and grid status with high accuracy but also to analyze resources and storage options, pricing prediction according to consumption patterns and to balance power generation capacity and demand in real time.

Having these capabilities require secure automated information exchange, analysis and intelligent decision making distributed throughout the grid. As it is shown in Figure 1, various power generation, transmission, distribution, customer energy management and business functionalities interact in such a system with increasing interdependence (sensing, measuring, consuming, processing, controlling), diversity in interconnections (e.g., remote monitoring and testing, synchrophasors, field devices and equipments, asset management, corporate analysis and decision systems) and adaptivity (in the ways control decisions dynamically interact and influence the entire sense-process-decide-control loop) – transforming the power system from a very complicated machine to a complex system.

In distribution power grid, security means the degree of protection in system against deliberate attacks, equipment failures, operator accidental errors or natural disasters. This include both power and cyber system technologies.

Today, power operation systems are increasingly using IT hardware and software platforms and network protocols. But these are very different in priority of the security objectives. In view of the integration of IT and OT domains, unified security solutions are essential to warrant communication and information security among multiple systems of different topologies in Smart Grid. This security system should balance the challenges of various security postures which are in OT and IT domains and be aware of safety and impacts an attack or incorrect operation could have on the power grid or the information systems.

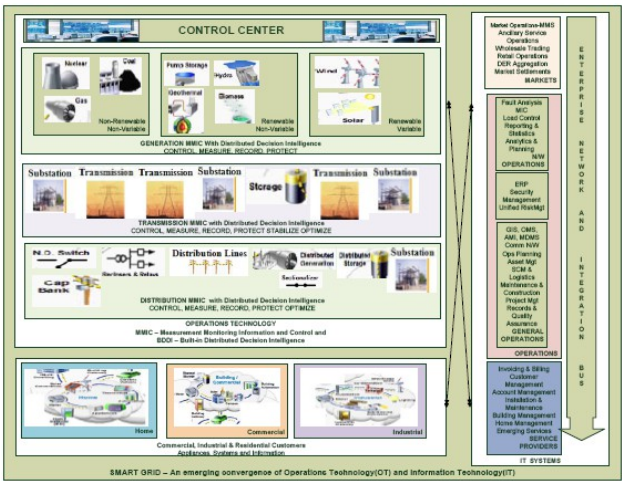

Fig. 1: SMART GRID: convergence of Operations Technology (OT) and Information Technology (IT)

UNIFIED SMART GRID CYBER SECURITY SERVICE

A schematic diagram of Shiraz Power Distribution computer network is shown in Figure 2. As the diagram represents, the network consists of seven clusters of computers connected via communication network. Servers in each cluster are designed for a main function and named as "Application Server", "Database Server", Data Acquisition Server", "Web Server" and "Message Server". The communication network can be Intranet, LAN or WAN with special protocols to exchange needed data between source and destination computers. There is an Enterprise Service Bus (ESB) in each cluster for computer's communication within the cluster. The messages which exchange can be as large as the largest file or as small as just a command code to open/close a breaker.

Figure 3 is a schematic diagram showing the self-similarity of the solution domain over various hierarchical levels of the network. The surrounding circle depicts an enterprise wide computer network to be protected. It also consists of smaller circles which are subsystems. Each subsystem itself surrounds other smaller circles representing lower level subsystems and individual computers and so on. This hierarchical representation can be carried down to as many levels as necessary to include all MCEs and the underlying business processes. Figure 4 shows the necessary security with the monitored and controlled elements (MCE) of the enterprise-wide network.

This MCE monitors and analyzes the collection of all information exchanges through an Enterprise Service Bus (ESB) and also messages from external computer networks (e.g. partners, customers, markets, etc). The term SE in each individual computers, applications, and local networks is a Security Engine which monitors and analyzes all data exchanges through the various parts of computers including inputs and outputs.

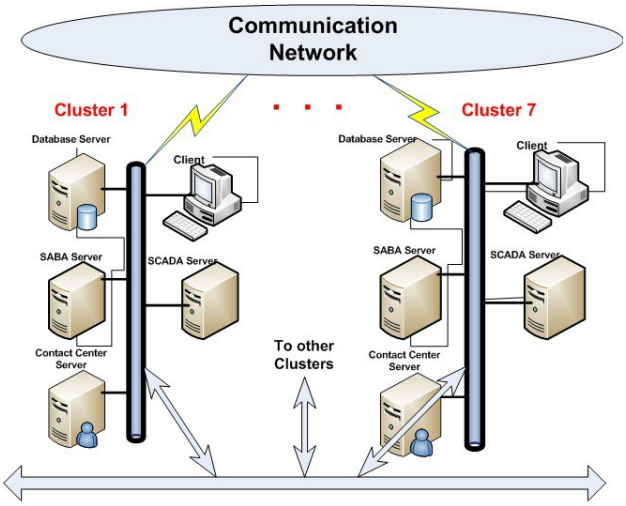

Fig2. Schematic diagram of Shiraz Power Distribution computer network

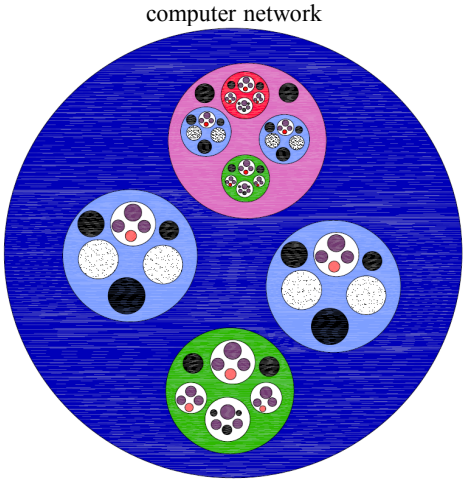

Fig3. The Pervasive Architecture

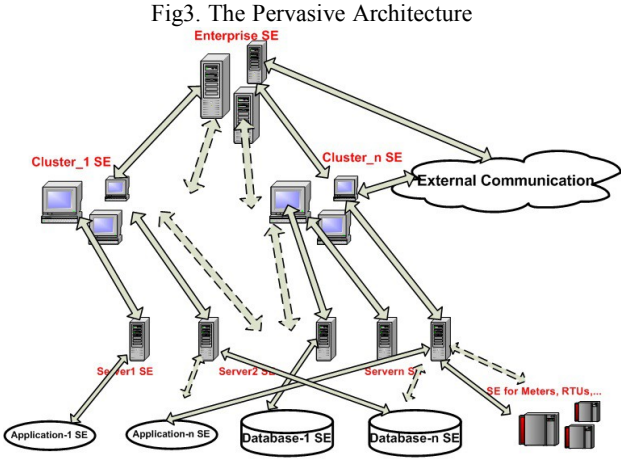

Fig 4: System Security Monitoring & Controlled Hierarchy

To provide the security for the system, each of the monitored and controlled elements (MCE) at the lower levels of applications, databases should have their own security engines (SE) for monitoring and analyzing all related information. A real time adaptive security system designed for Shiraz Smart Grid is illustrated in Figure 5. This adaptive security system shows how the security control attitude changes in about real time (maybe till hours) in response to changes in the power and/or information system due to security, reliability and stability events. The System consists of two major parts:

- OT Response Agent
- Risk analysis Expert System

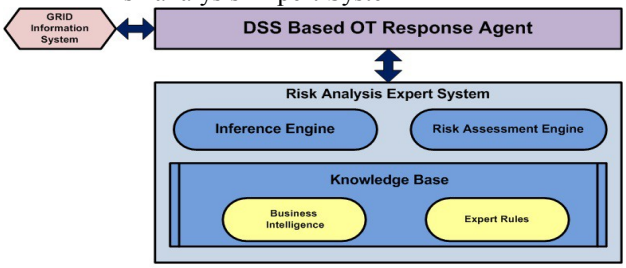

Fig 5.Real time adaptive security system

The first part represents a full automated agent that receives real-time information about power grid status and sends this information in special classification to expert system. Main task of this part is receiving network special situation status and handling proper information to the expert system and get recommended actions list. The expert system sends its recommendation based on historical experiences and related rules stored in its knowledge base. Expert rules consist of some operational best practices and calculation of numerical factors of the network. These recommendations will be analyzed by risk assessment engine prior to past experiences and documented recommendations so the result will be a sorted list of actions based on associated risk. Proper action could be selected automatically or by the help of a supervisor. Risk assessment tasks are based on grid control devices availability, required network reliability, technical team availability, grid load balancing factors and results of past actions. Historical information (knowledge) has very important role on action recommendation and risk assessment task. So system accuracy will be increased during the operation of the system. Automatic selection of the best action for current state of the network depends on various factors including training period of the system. So the system is learning from experts and its own recommendations regarding to final result and impacts on the grid network. The automation of decision making in such a complex environment could increase operational risks and decrease grid reliability especially at the beginning of expert system training. So the system should work as a decision support system and help network supervisors for awhile till learn from them during time. Using such an adaption has the advantage of right sizing security by balancing costs against benefits.

RISK EVALUATION AND SECURITY METRICS

Another important and necessary objectivity in risk management in a smart power grid is to find a methodology to evaluate security (or other) risks in a large enterprise. The proposed methodology consists of the following steps:

- Identifying all assets and investments that are important for the company

- Estimate vulnerabilities of each assets
- Analyze all potential threats that can lead to identified vulnerabilities
- Determine optimum security condition for each assets

In this methodology some metrics are defined to model assets & services, vulnerabilities, threat, security control and security conditions in a unified consideration of OT and IT domains.

Assets and Services:

Metrics to model assets and services must represent impact on the profits and costs to the company, customers and other stakeholders. It can be considered in two categories:

Power Systems

Power system equipment which is essential to keep the stability of the grid should be given high degree of importance. For power system services, in general, facilities that relate to life support system like Hospitals, Traffic light and some of political residences, should be treated as the highest level of importance. Social safety facilities are ranked based on their situation.

Information Systems

Each IT system component should be assigned its importance degree depend on the impact of its failure on the system.

Vulnerabilities:

Vulnerabilities are the nature to either individual equipment or groups of equipment. Both physical and informational valnerabilities have to be assessed. Examples of power system vulnerabilities that treat security include:

- Weather (probability of lighning or fire along a feeder)
- Loading levels (higher feeder loading levels make the system go to unstable situation)
- Risks to energy supplies.

Examples of valnerabilities in IT system are:

- Interfered data in control signals or operational data.
- Risk damage in data center or communication link.

Threat Models:

Threats are those of vulnerabilities which could be exploited. Both intentional or unintentional attacks should be considered. Attacks on the power system equipments or distribution feeders or energy supply routes, like switching devices at distribution networks. This may include an interfering with switching devices at distribution networks or errors in meter reading and other measurements data, pricing and operating data.

Security Controls:

Security controls are mechanisms to prevent threats and it may be more than one to block one threat or conversely a single security control for several threats. Since there is no solution which can guarantee security definitely, metrics to model them are time based like time to detect attacks and time to respond.

Security Conditions:

Security conditions can be physical or informational. Examples of physical ones are security guards, fences, gates, physical locks, remote cameras, etc.
Informational security conditions include improved encryption levels, virus recognition by processing messages.

CONCLUSIONS

According to different data collection devices and their various analysis softwares to correlate them with other power system and customer data and control elements in a smart power grid, it is essential to develop a distributive but sensitive security risk analysis and control systems.
Unified risk management approaches are critically needed to effectively guide resource allocations, identify best practices on the basis of practical and meaningful benchmarks and demonstrate various regulatory and business compliances for both the control systems and business domains.
This paper presented essential characteristics and properties for security risk management approaches in the context of the smart power grid. The strength of this work is introducing an adaptive security system designed for Shiraz Distribution Network which consists of two main parts of OT response agent and risk analysis expert system. The automation level of decision making will increase by implementation the system for long period of time. Having such a system ensures power Distribution Company to offer their customers a sustainable system for integrated security and risk reduction solution.

REFERENCES

[1] U.S. Department of Energy, “The smart grid: an introduction.”

[2] “Smart Grid Policy”, [Docket No. PL09-4-000], 2009, Federal Energy Regulatory Commission, USA.

[3] “Title XIII - Smart Grid, Sec. 1301, Statement of Policy on Modernization of Electricity Grid”, Energy Independence and Security Act of 2007 (EISA), USA.

[4] “Smart Grid Systems”, SB1438, California, USA.

[5] American Recovery and Reinvestment Act of 2009, P.L. 111-5, USA.

[6] P.D. Ray, R. Harnoor, M. Hentea, 2010, "Smart Power Grid Security: A Unified Risk Management Approach", *Proceedings for the 44th IEEE International Carnahan Conference on Security Technology (ICCST)*,San Jose, CA, October 5th – 8th,

[7] P. D. Ray,2011, “The Smart Grid’s Singular Security Challenge”, *POWERGRID INTERNATIONAL*, vol.16, 58-60.

[8] J. Katz, “Smart Grid Security and Architectural thinking”, http://www.ibm.com/smarterplanet/global/files/smartgridsecurity_and_architecturalthinking_katz.pdf

[9] W. Jansen, 2009, “Directions in Security Metrics Research”, NISTIR 7564.

[10] K. Moslehi, R. Kumar, 2010, “A Reliability Perspective of the Smart Grid”, *IEEE Transactions on Smart Grid*, Vol1, Issue 1, pp.57-64.