Cyberwarfare on the Electricity Infrastructure

Executive Summary

Electric utilities are increasingly integrating innovative information technologies in the face of significant changes in the electric power industry fueled by deregulation and other marketplace forces. Such networking and automation aimed at increasing the quality and efficiency of operation makes the power grid all the more vulnerable to cyberattacks. Few utilities have information security functions for their operational systems due to lack of prior experience with information attacks. However, the information security community has started to recognize the potentially devastating impact of coordinated information attack on the power grid. In this report, we analyze the possibility and consequences of cyberwarfare on the electricity infrastructure. We present a framework for achieving risk-based selection of security tools through modeling and simulation of power system information system components, potential threats and protective measures. We therefore offer a framework for infrastructure protection.

To begin with, we discuss the modeling aspects for a generic utility power system in the context of cyberwarfare. Along with the conventional generation, transmission and dustribution elements, the system also includes the information system components that monitor and control the field equipment and connect with the other external interfaces for administration and operational interactions. Then, we identify specific threats facing a utility information system and model these threats as isolated objects that can be imposed on the system model developed previously. As a next step, we identify suitable information security tools for protection of the information system associated with the power grid. Subsequently, we investigate modeling aspects for these tools such that these tool models can be deployed on the system model developed earlier. Finally, we integrate the different models into the overall framework. We describe the required simulation studies and formulate an optimization problem that can provide the final selection of security tools.

We found that the security awareness and preparedness of electric power control networks and information systems varies widely from utility to utility. An information security function should be established in each of the utilities to perform systematic risk-based analysis of the security situation and to determine a selection of commercially available security tools for deployment in the network. The new structure of the industry enabling generating, transmission, distribution and service provider companies operating individually but interconnecting functionally to satisfy the consumer's needs, opens up new avenues of electronic threats and necessitates establishment of security architecture. Further research can be devoted to designing and developing such an architecture that incorporates security tools and services to handle secure interactions among the power system elements.

DOE Patent Clearance Granted
11/17/00
Daniel D. Park
Date
(630) 252-2308
E-mail: daniel.park@ch.doe.gov
Office of Intellectual Property Law
DOE Chicago Operations Office

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, make any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

RECEIVED
NOV 22 2000
OSTI

1 Identification and Significance of the Problem

Security, continuity and availability of national infrastructures are critical to the nation's defense, economic prosperity and quality of life. The rapid proliferation and integration of telecommunications and computer systems have enhanced the efficiency of operation and maintenance of these infrastructures, as well as have connected them into a complex network of interdependence. Such connectivity and automation have also opened up new avenues for malicious electronic attacks by adversaries.

The electric power grid is the backbone of many other infrastructures such as telecommunications, finance and banking. Despite the proven stability and reliability of the U.S. electricity infrastructure, there are significant challenges to sustaining this robustness and resilience, especially in today's deregulated industry and the onset of the information age. A cyber attack aimed at crippling the electric power grid can, in turn, result in a cascading failure of almost all other infrastructures. Hence, it is important to ensure that the electricity infrastructure is adequately protected against cyberwarfare.

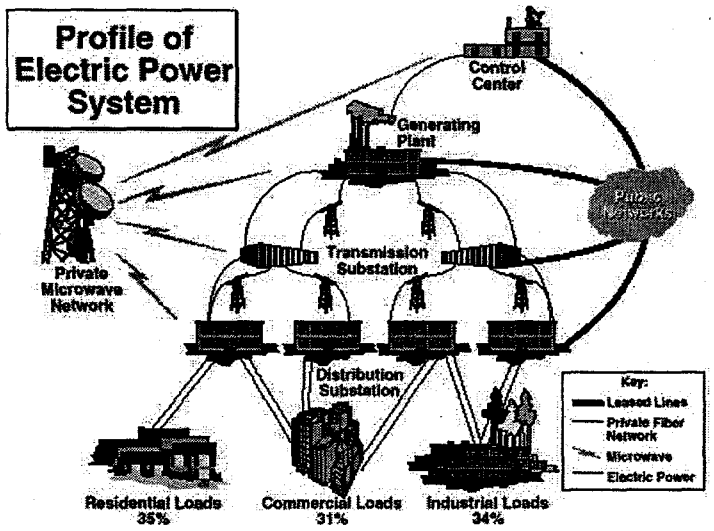

Figure 1: Power flows and information flows (from the PCCIP report mentioned below)

The electric power grid is a highly interconnected and dynamic system of over 3000 private and investor-owned public utilities, government owned systems, cooperatives and manufacturing industries that also produce power, as mentioned in the report "Electric Power Risk Assessment" released by the Information Assurance Task Force (IATF) of the National Security Telecommunications Advisory Committee (NSTAC). With the advent of deregulation, the industry is undergoing significant changes, with new players entering the generation and delivery market and existing utilities being required to compete and transact with them using state-of-the-art information systems. According to the NSTAC report, nearly 80 percent of the nation's power generation comes from the approximately 270 investor-owned public utilities. Significant damages can be inflicted

on the nation's power grid by disrupting the power network of a major utility. Moreoever, for risk management purposes, the other entities can also be considered as scaled-down version of a major utility in terms of the resources, threats and vulnerabilities. Hence, we focus our attention on the management of risk resulting from cyber attacks against utility power and information systems.

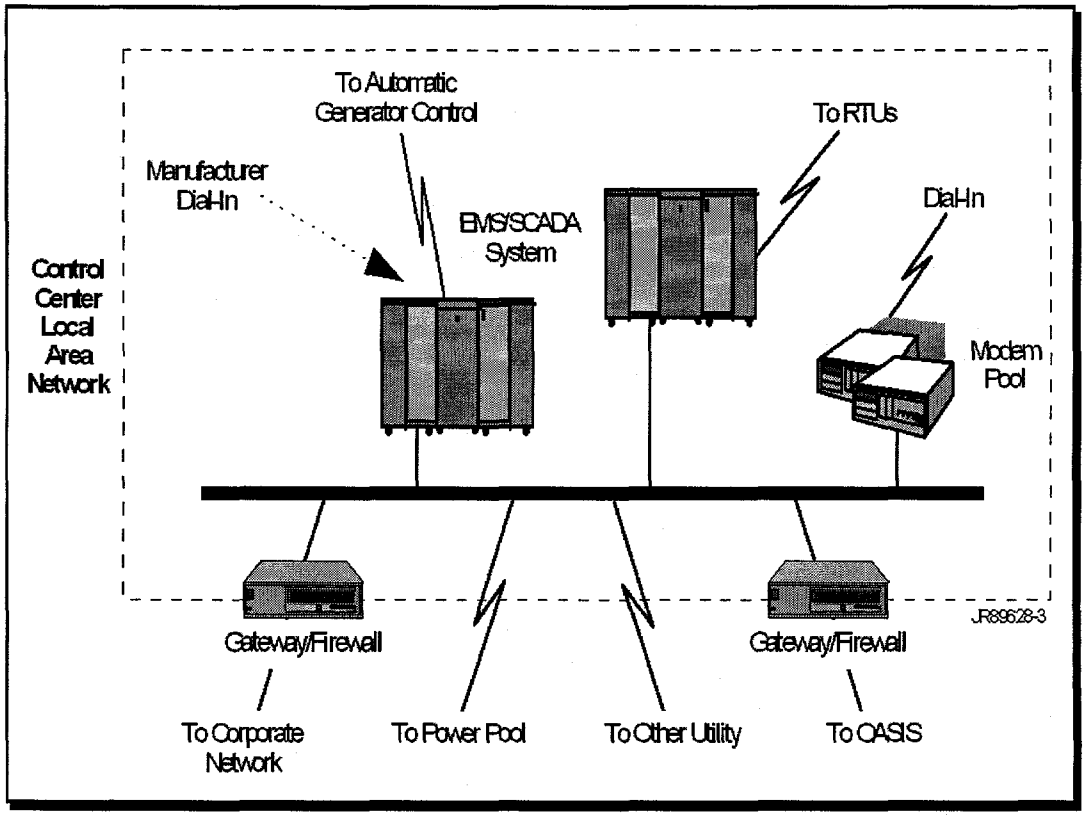

Figure 2: Control center information system interfaces (from the NSTAC report)

The profile of information and power flows in a conventional electric utility power system is depicted in figure 1, adopted from the document "Critical Foundations: Protecting America's Infrastructures; Report of the President's Commission on Critical Infrastructure Protection (PCCIP); October 1997". Additional links for information exchange are shown in figure 2, adopted from the NSTAC report. As these figures indicate, there are two kinds of information flows: one that pertains to information transfers required for the control and operation of the power grid and another that pertains to information exchange for interaction with external entities. The information flow presented in figure 1, belongs to the first category. The control center is the heart of the information network where the components of the Energy Management System (EMS) are used to monitor and control the operation of the power system. Intelligent electronic devices (IED) directly involved with the generation, transmission and distribution systems for intelligent control and data collection are deployed in the substations. Private channels based on microwave, fiber optics and other technologies are used for

communications between the control center and the field equipment. Hence, security loopholes in the EMS system as well the communication media can be used by offenders to intrude and disrupt the normal operation of the power system. Utilities use a variety of security measures to protect the electric power grid from disruption, including contingency analysis, redundant control centers, dial-back modems, and firewalls. However, few utilities have an information security function for their operational systems, and the lack of convincing evidence of a threat has led to minimization of information security investments. Further, many of the new players in the electricity marketplace are small independent power producers and power marketers who are often ill-equipped to deal with information security issues.

The second category encompasses all other interfaces such as links to the corporate information system, the Open Access Same-time Information Systems (OASIS) that is used for Internet-based electric transmission reservation, links to other utilities or power pools, links to supporting vendors, remote maintenance and administration ports and customer service. On the customer service side, deregulation has resulted in a whole new set of demands such as real-time pricing, automated metering and remote control of appliances such as air conditioners. Many of these services will eventually be provided through the Internet. All these interfaces to the control center, as depicted in figure 2, are potential channels for electronic intrusions.

In order to protect the electricity infrastructure from cyber attacks (threats), the decision makers (at the utilities as well as at national security organizations such as the FBI) need a framework (and associated tools) for performing "what-if" analysis. To begin with, vulnerabilities specific to the electricity infrastructure need to be identified and characterized. The potential damage to the electricity infrastructure posed by these threats needs to be quantified. Given the complex and nonlinear nature of the physics of electricity flows and given the myriad of players in the electricity marketplace, modeling and simulation tools are required to do damage assessment. In addition to such risk assessment, the framework should also provide risk management tools which encompass both preventive and corrective actions. Such a decision support framework will allow policymakers and other stakeholders to determine the appropriate mix of protective measures that are most effective in reducing potential damage to the electricity infrastructure. The report "Research and Development Priorities for Communications and Information Infrastructure Assurance" (http://www-itg.lbl.gov/security/PCCIP/C+I_Report.html) highlights modeling & simulation and risk management as important R&D needs in information assurance in general. Thus, it would also be desirable to design the framework such that it can be easily extended to other infrastructures.

2 Technical Approach

The overall technical approach of our research is to take a strategic system-wide perspective of the electricity infrastructure protection problem. The goal is to enable reasonably accurate risk assessment and risk management through the use of realistic modeling and simulation tools. Given the geographically dispersed nature of the electric power grid and the increasing use of the Internet in information flows pertaining to the power grid, it would be reasonable to require the use of a distributed computing model for the simulation. We need to simulate both the physical power flows and the information flows since the two are closely coupled. Hence, the (computationally intensive) simulation tools employed by the power industry such as the SCADA system and some of the EMS applications such as load flow need to be a part of the simulation toolkit. Further, since the risk analysis problem is inherently probabilistic, we would need to perform a large number of simulations corresponding to various scenarios of threats and countermeasures. Thus, the approach entails the use of high-performance distributed computing over a wide-area high bandwidth network.

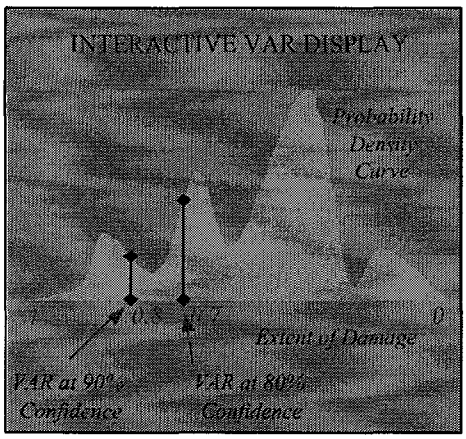

Figure 3: VAR figures corresponding to two different positions of the sliding bar

Value-at-Risk (VAR) is a powerful measure of risk employed extensively on Wall Street for handing the uncertainty and risk inherent in the capital markets. We selected VAR to summarize the system security situation and obtain a strategic perspective on system vulnerabilities and countermeasures. VAR is defined in the financial world as the amount of money such that the portfolio (of stocks, bonds etc.) will lose less than that amount over a specified period with a specified probability. In the current context, we define VAR as the maximum degree of disruption in the power grid exposed to risk over a specified period with a specified probability. The degree of damage is taken as a fractional number between 0 and 1. In the Interactive VAR Display (IVD) in figure 3, VAR at 90% confidence interval is 0.8 implies the probability of the power grid suffering a disruption of degree less than 0.8 is 90% or 0.9. Corresponding to this position of the sliding bar, the area under the probability density curve to the right of the sliding bar is 0.9 whereas the area on its left is 0.1. The probability of occurrence corresponding to a different value of the maximum degree of damage can easily be found just by positioning

the sliding bar at the desired location on the horizontal axis and computing the area under the curve to its right. On the other hand, the maximum degree of damage corresponding to a desired probability of occurrence can also be found from the same figure by adjusting the position of the sliding bar such that the area under the curve to its right is equal to the desired value, and noting the corresponding value on the horizontal axis. Hence, first fixing up the value for one of the two variables viz. the degree of damage and the probability of occurrence, and then by using the sliding bar, the value for the other variable can be found interactively.

We have developed a decision support framework for electricity infrastructure protection from a utility's perspective. The framework is based on the profile of a utility power system depicted in figure 1. We recognize the fact that the system is most vulnerable at the point where the connectivity is the greatest and the access control is the weakest. The field equipment comprising of specialized instruments and the private communication networks connecting the control center and the field equipment are not directly accessible from the outside world. Therefore, our initial assumption is that the options to consider for attacking the electric power grid electronically are: the control center, the substations, the corporate information interface, the remote administration and maintenance interface, links to the other utilities and power pools, links to supporting vendors and the external communications infrastructure. Our other assumption is that since the locations of attack are the computer and communications systems that are directly connected to the Internet or otherwise accessible to the external world, the nature of these attacks are quite similar to the ones commonly observed in the telecommunications and other information networks. Therefore, our framework can use the statistical information regarding the probabilities of occurrence of these attacks.

The methodology commences with a sequence of modeling and simulation exercises to prepare for the actual risk management analysis. The first task is the modeling of the utility power system such that the operations and controls can be simulated using popular tools such as MATLAB. The model incorporates the control center EMS applications that include Supervisory Control And Data Acquisition (SCADA) system, Automatic Generation Control (AGC) system, and the analysis applications such as optimal power flow, unit commitment, economic dispatch, contingency analysis etc. The model also includes external interfacing with the other information systems such as remote administration, OASIS etc. Consequently, the entire system can be simulated to confirm and verify the system state comprising of the power flows, the voltage magnitude and angles etc. such that the real system is properly represented in the simulation environment. The next exercise is the identification of threats in the form of well-known information attacks that are oriented towards exploiting the vulnerabilities in the locations mentioned. A set of threats are isolated and categorized that can be included in the simulation environment prepared earlier. The attacks are modeled and implemented as isolated modules that can be readily imposed on the simulated system. The third task is identification of the protection measures such as firewalls, intrusion detectors, vulnerability scanners etc. that can also be included in the simulation environment. These measures are also appropriately modeled and implemented as objects that can be deployed on the simulated system as desired.

Once the components are suitably modeled and implemented, the final simulation should be performed in three stages with monitoring of system stability parameters and performing contingency analysis. The initial simulation in the context of a preset time horizon such as the 16 hours of weekday peak load should display the normal secure operating conditions with system parameters maintaining their values within their limits. The next simulation is the representation of the situation where the system is under electronic attacks. For each identified threat (such as a virus or a denial of service attack), the attacks need to be imposed and impacts measured in terms of deterioration of the system conditions at critical locations such as heavily loaded transmission lines, voltages at the critical distribution substations etc. Large number of simulations should performed to reflect the existence of large number of information attack methods encountered so far. The impacts would be consolidated stochastically using the probabilities associated with the occurrence of the attacks to output a probability distribution depicting the probabilities of various levels of damage ranging from no disruption to a complete blackout.

The third simulation is for designing countermeasures and for evaluating their relative merits in mitigating security risks. The protection measures are deployed using the simulation objects developed earlier. These tools include intrusion detection systems, network analyzers, antivirus software and spam filters. The effect of each such tool is measured through large-scale simulations and the output is displayed as the change in the probability distribution (histogram) of the impact of (damage caused by) each threat. The modification in the histogram caused by this protection measures provides an immediate visual feedback to the decision maker on the effectiveness of the particular tool.

2.1 System modeling and implementation

Modeling of a system is very specific to the context of application of the model. In the

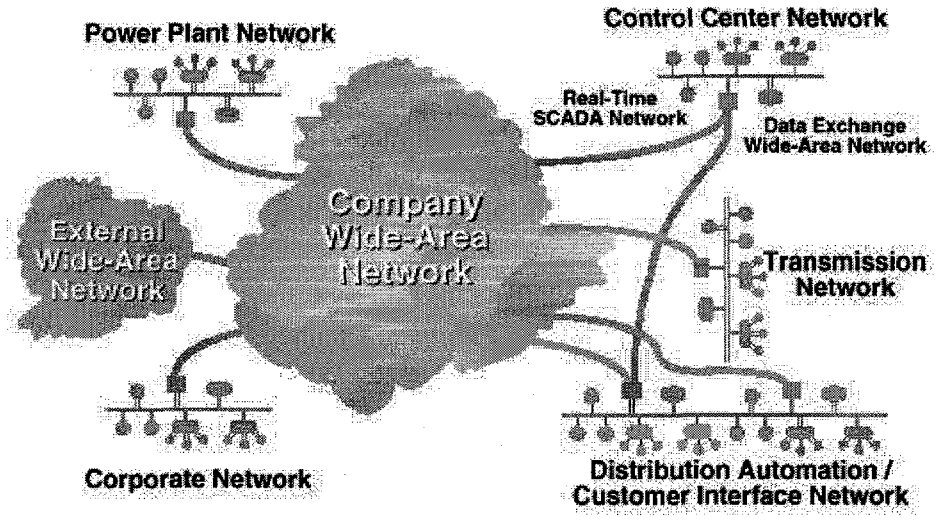

Figure 4: Utility Information Systems (from the PCCIP report)

present context, the typical operations of a utility power system need to be modeled such that the essential functions are adequately incorporated and represented. The objective is to understand and analyze the effects of electronic intrusions on the normal operations of the system. Hence, the main emphasis should be on representing the information system that is susceptible to such attacks and the dynamics of other components can be ignored. The model should accept the inputs in the form of the wide range of anticipated electronic attacks and the outputs should provide indications of effects of these attacks on the normal operations of the system.

A power system operates through supply of electrical energy to meet the demands of consumers. In today's deregulated environment, generation, transmission and distribution functions are treated individually as isolated entities. Market forces decide the interconnection among these entities. Additional functions have evolved such as transmission reservations using OASIS, ancillary services etc. So far as the end users are concerned, their energy requirements can be met by a number of energy supplier and related service providers operating in collaboration. Therefore, the utilities are being required to change their operations, procedures and management functions from the traditional vertically integrated organization to a collection of independent entities responsible for their individual functionality.

The new environment does not exclude the possibility of a utility owning and operating all three components providing a unified service to the end user. In fact, recent mergers and acquisitions among the major utilities owning transmission and distribution facilities, independent power producers, energy service providers and power marketers reflect the operational and economic benefits of such a unified entity. Hence, without loss of generality a typical utility information system can be considered for our analysis of information security as depicted in figure 4, adopted from the PCCIP report.

The power grid can be modeled in one of the popular simulation environments such as MATLAB Simulink. These simulation tools are already equipped with facilities to develop operational models of a power system. The components should be modeled as driven by the standard inputs as well as the control information such that the performance can be monitored with respect to changes in the control settings. For example, the generation plant is controlled by AGC systems and erroneous control signals from the AGC systems caused by information attacks can adversely affect the performance of the plant. On the other hand, a corrupted transmission reservation database can cause allocation of power flow beyond the limits of a transmission line resulting in overload of the lines and inefficient operation of the system.

The information system components can be modeled with varying degree of details depending on the analysis requirement. A simple model would be a functional block for each component system essentially serving to generate necessary control inputs for the power grid. These models can be easily connected to the power grid model. The models can be improved depending on the requirements by the simulation for representing additional capabilities.

2.2 Threat modeling and implementation

The objective of threat modeling is to identify and characterize vulnerabilities and associated threats specific to the electricity infrastructure. To begin with, an extensive list of threats that are commonly encountered in cyberspace are considered. These include various forms of viruses, Trojan horses, denial of service attacks (flooding, spamming etc.), password sniffing, malicious code embedded in applications, logic bombs, remote purging of data and/or software, hacking, electromagnetic interference, and jamming of signals. While all of these can be used against the electricity infrastructure, some have more devastating effects than others. Given the fact that it is prohibitively expensive and technically difficult to protect against all of these threats, we prioritize the threats in terms of the potential damage they could cause to the electricity infrastructure. Knowledge of the specific information flows in the electric power industry is needed to perform such prioritization. For example, SCADA systems are vulnerable to electromagnetic interference since they gather data from far-flung sensors located in remote generating plants and switch yards. On the other hand, OASIS nodes are by and large Web servers which are most vulnerable to denial of service attacks like spamming. Further, infiltration of SCADA systems will result in far greater damage to the electric power grid than infiltration of OASIS nodes.

As mentioned before, we expect that the isolated field equipment and private communication channels are quite unreachable for electronic intrusions. However, the control center is connected to the outside world through vulnerable interfaces. These interfaces are links to corporate information system, links to other utilities or power pools, links to supporting vendors and remote maintenance and administration ports. Systems such as OASIS are located on the Internet for real-time access by transmission customers and hence, are easy targets for information attackers. Utilities are responsible to install automated procedures to establish communication channels between the control center and the OASIS such that the transmission capacity availabilities are updated as frequently as required. Lack of adequate security measures at OASIS will allow the intruders to gain privileged access to the utility control center through these channels. Similarly, the other interfaces should be explored to identify the potential attack channels.

The next step is to investigate the disruptions that can be inflicted by the adversary with various levels of access to the system. An external intruder with access to internal resources can be essentially considered an insider with identical privileges. Once in the control system network, a sophisticated offender could corrupt the databases and disrupt the billing operations causing significant economic damage to the utility. A knowledgeable attacker can issue erroneous commands to the system – opening and closing circuit breakers shutting down lines affecting generation and power flow. An extremely knowledgeable attacker could manipulate the flow of data to the control center, causing the control center operators to respond to spurious indications. Fortunately, the technical skills and specific knowledge of an individual utility's applications and procedures limit this kind of attack to a very small number of potential attackers. Furthermore, most utilities can revert to manual coordination if all control center functions are lost; however, this is a costly measure for the utility.

Once all these factors are explored, the specific threats and disruptions identified, characterized and standardized, a suitable threat model can be designed and implemented to interface with the simulated system model.

2.3 Protection modeling and implementation

Security tools will be required to protect against the threats identified in the previous task. These tools include firewalls, vulnerability assessment tools, intrusion detection systems, antivirus software, anti-jammers and spam filters and are deployed at the host, network or routers in the information network. The effectiveness of each of these kinds of protect tools will vary depending on the portion of the electricity infrastructure that is being attacked and on the threat. For example, intrusion detection systems are of value to OASIS nodes but not against viruses or malicious codes. Similarly, anti-jammers are useful for protection of SCADA systems but only for electromagnetic interference and jamming. Each of these tools is expensive both in terms of acquisition cost and in terms of installation and maintenance. Further, these tools do impose a performance penalty on the concerned information systems. Therefore, for each threat, it is necessary to choose a minimal set of protect tools that provide the maximum coverage in terms of protection.

The protect tools need to be modeled such that they can be plugged in to the simulated system model developed earlier. As mentioned before, the threat models should also have the same capability. The idea is to simulate the system with chosen attacks and protect tools deployed at appropriate locations. The simplest method is to model the system improvements in terms of reduced chances of intrusion events and reduced impacts of disruptions caused by the attacks. For example, installation of a gateway firewall in the corporate information system will reduce the probability of electronic intrusions into the control center from the corporate system interface. Similary, deployment of intrusion detection systems will enable fast detection of invasion attempts and suitable remedial actions can be taken to confine the attack before any significant damages occur.

After the threats are identified, and the protection measures are characterized, models for the protection tools should be developed that represent these characteristics and interact with the simulated system model appropriately.

2.4 Final Analysis

The final analysis would consist of a sequence of simulation studies. First, the operational system should be simulated including the control center and other information system elements that interface the power grid. The state of the system would be analyzed using optimal power flow and contingency analysis tools to identify the critical elements of the system. The state parameters such as power injections, voltage magnitude and angles etc. should be monitored for various supply and demand conditions to determine the stability range of these parameters. For example, a 20% overload on a transmission line can result in tripping of a relay such that the line is shut off causing disruption of supply to the load at the end of the line. Therefore, this amount of overload can be considered to cause the

maximum impact and normalized to "unit" impact as in figure 3. Similarly, the range of impact of the other critical parameters should be determined.

Next, the effects of various threats on the normal operation of the system should be simulated. The threat models developed earlier were designed to produce disturbances in the control inputs to the operational equipment. Therefore, these models can be plugged in to the simulated system and the effects can be observed through the deterioration in the critical system parameters. Large numbers of simulations are performed against varying threat conditions and the probabilities of occurrence of the attacks are used to stochastically combine the normalized impacts to produce probability density curves. VAR is calculated from each curve based on a preset confidence level (probability) to summarize the situation in terms of the maximum disruption with selected confidence against the chosen time horizon.

The results from the preliminary simulations represent the existing security situation in the face of information attacks and also indicate the necessity of installing protection measures to improve the situation. The final series of simulations includes the protect tools at various critical locations such that the combined effect of the threats and the security tools can be obtained. Appropriate pairing of threat conditions and protection measures should generate large number of cases. Corresponding simulations should be performed to generate the probability density curves and determine the associated VAR values, as before.

We approach the problem of tool selection in two steps. First, using the VAR figures from the third series of simulations, a threat-tool matrix should be composed that reflects the effectiveness of each tool against the cost of deployment of the protection measure for each threat on every major component of the electricity infrastructure. Then, this matrix should be utilized to formulate an optimization problem whose solution will yield the desired tool mix. Figure 5 depicts a typical threat-tool matrix.

Threats / Tools	← OASIS NODES →				← SCADA SYSTEMS →		
	Virus	*Hacking*	*Jamming*	*Flooding*	*Virus*	*Spamming*	*Jamming*
Anti-Virus	High	N/A	N/A	Low	High	N/A	N/A
Intrusion detection	Low	High	N/A	Low	Low	Low	N/A
Anti-Jammer	N/A	N/A	High	N/A	N/A	N/A	High

Figure 5. Threat-Tool Matrix for the Electricity Infrastructure

In Figure 5, "N/A" implies that the protect tool is ineffective against that threat for that component of the electricity infrastructure. Similarly, "high" and "low" indicate the degree of effectiveness of the tool. Note that these qualitative indicators of effectiveness

should be replaced by the VAR values that are derived from the simulations as quantitative measures of effectiveness (extent of damage).

Given the above matrix, the following optimization problem can be formulated:

Determine the tools to be used and the amount to be invested in each tool

so as to Minimize the extent of damage AND Minimize cost

subject to

constraints based on policy guidelines

constraints imposed by minimum performance requirements

constraints pertaining to the allocated budget

The objectives and the constraints are derived from the threat-tool matrix. Also note that this is a multi-objective optimization problem with two conflicting objectives. In general, this problem could be a nonlinear programming problem (NLP). The solution obtained would provide a risk-based strategic selection of security tools that should be deployed in the electricity infrastructure to minimize the impact of electronic information attacks.

3 Conclusion

The greatest risk facing the electric power infrastructure of the United States remains physical damage and destruction. Compared to the threat posed by natural disasters and physical attacks on electric power infrastructure elements, electronic intrusion represents an emerging, but still relatively minor, threat. However, changes within the electric power industry and in technology are increasing the risk posed by electronic intrusion. The security of electric power control networks and information systems varies widely from utility to utility. We developed a framework for risk-based selection of security tools for enhancing the security of a generic utility owning and operating the essential elements of a power system and facing electronic attacks on the information network integral to the system. Several commercial tools are available to develop the components in the framework and we expect that the resultant tool will serve as a decision aid for the information security manager of a utility.

The new structure of the industry enabling generating, transmission, distribution and service provider companies operating individually but interconnecting functionally to satisfy the consumer's needs, opens up new avenues of electronic threats and necessitates establishment of security architecture. Further research can be devoted to designing and developing such an architecture that incorporates security tools and services to handle secure interactions among the power system elements.