UNIVERSITY OF FLORIDA

Secure Energy Systems - Vision and Architecture for Analysis and Design

PI: Pramod Khargonekar
Student: Tejaswini Akunuri

Description: The goal of this project is to investigate the concept of secure energy systems and formulate a concrete vision of a broad-based, comprehensive research program. An additional project goal is to develop architecture for modeling, analysis, and design of secure energy systems. An energy system consists of a collection of interconnected subsystems representing energy generation devices, energy consumption devices, transmission, distribution, and storage devices, and communications and computing devices. Such systems are dynamic and its operation is influenced by external perturbations. Definition of the system and it environment depends on the problem of interest. This project is motivated by strong interest among key decision makers in understanding and assuring security of energy systems in the face of various natural and man-made threats. Increasing penetration of renewable energy sources and capabilities offered by smart grid have the potential to enhance or degrade security of energy systems. Thus, these new developments present additional motivation for understanding of secure energy systems. Whereas there is an intuitive understanding of security and assurance, much work remains to be done in formulating precise definitions that cover problems of interest and devising an overall architecture that may facilitate a system level analysis and design of such secure energy systems. Taking into account rapid changes in the energy issues in a wide variety of private and public sectors, this project is a proactive effort to develop a vision and architecture for analysis and design of secure energy systems. It is expected that the results of this project will lead to future development and integration of specific analysis and design algorithms and software that will assist system designers in assessing and ensuring an appropriate level of system security.

The term security can take on different meanings depending upon the context. There are risks associated with intentional disruption of the system (sabotage) and operational risks of the system (whether from physical failure of the plant, human error, or market-based instability). Both can pose short- and long-term national security risks for the electric energy system which consists of the basic elements: generation, transmission, distribution, the load (users); and the control system. These elements are the choke points and can cause great harm by causing outages and moderate-term disabling of important elements in the energy system. We present the security issue by considering the various elements of the energy system one-by-one. At the generation end, we consider the security of the power plant. The attacks on the power plant are mainly physical i.e. the attack on the pipelines which carry the gas or oil (input to the turbine), attacks on the manual valves (which can be opened/closed physically), physical security of a nuclear power plant is in itself a topic which has been extensively researched. Thus we start with the generation system and move onto the transmission system (transmission towers and lines), the distribution system (local transmission lines and substations), and finally the control system which connects all these elements. Network security at the plant level (the connection of the control system and SCADA to the physical components) has also been considered.

Progress Summary

We have focused much of our efforts in two related directions: electric grid and a graphical user interface that can help visualize potential security analysis tools. In electric grid, we have worked on the new issues that arise in the smart grid from the cyber-security perspective. These issues are already central to the future of the electric grid. We have also investigated integration of intermittent renewable energy into the electric grid. This

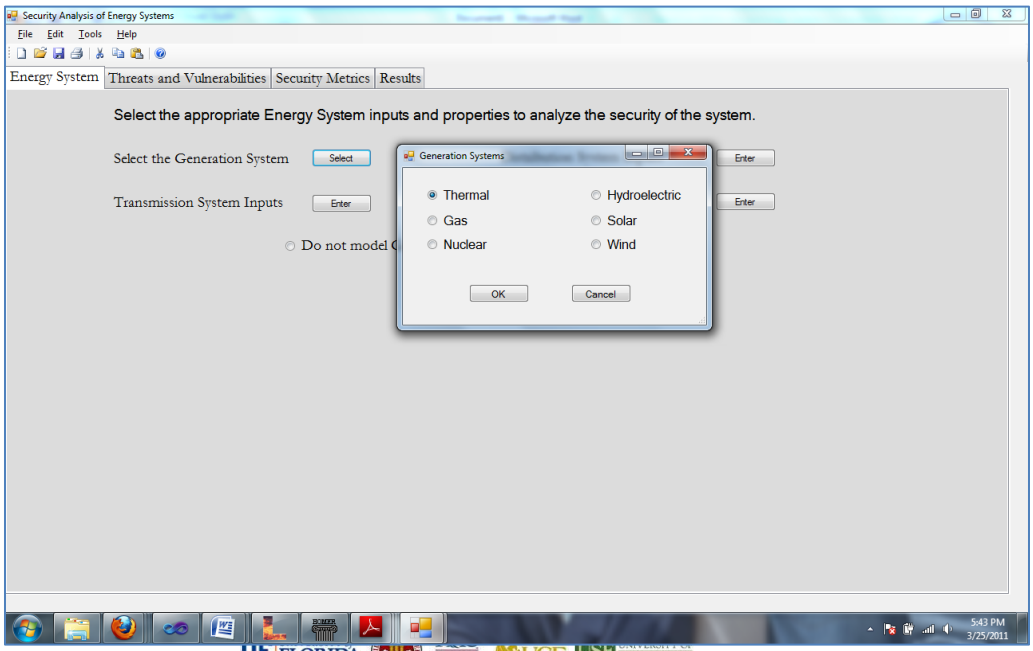
is one of the major goals for the smart grid. With distributed renewable generation and smart grid enabling components, the electric grid becomes much more open to cyber-attacks. Here we are investigating attacks on the SCADA based state estimation by cyber-attacks on the measurement system. We are working on optimal deployment of the new synchrophasors (which will be integrated using the new NASPInet framework) for thwarting attacks on the SCADA system. A paper based on this work is under preparation. This work is being done in collaboration with colleagues at the University of California at Berkeley and Idaho National Labs.

We next describe the outline of a graphical user interface which will form the external interface for the analysis system. This will serve as a framework for a tool which will be able to analyze the security situation of the energy system. The graphical user interface will consist of the various threats faced by the energy systems and the analysis of the situation in case of an attack. In the work conducted so far, we have found that there is no document or analysis present which takes a complete look at the energy system as a whole. We are hoping to develop a comprehensive view and research agenda for analysis and design of secure energy systems.

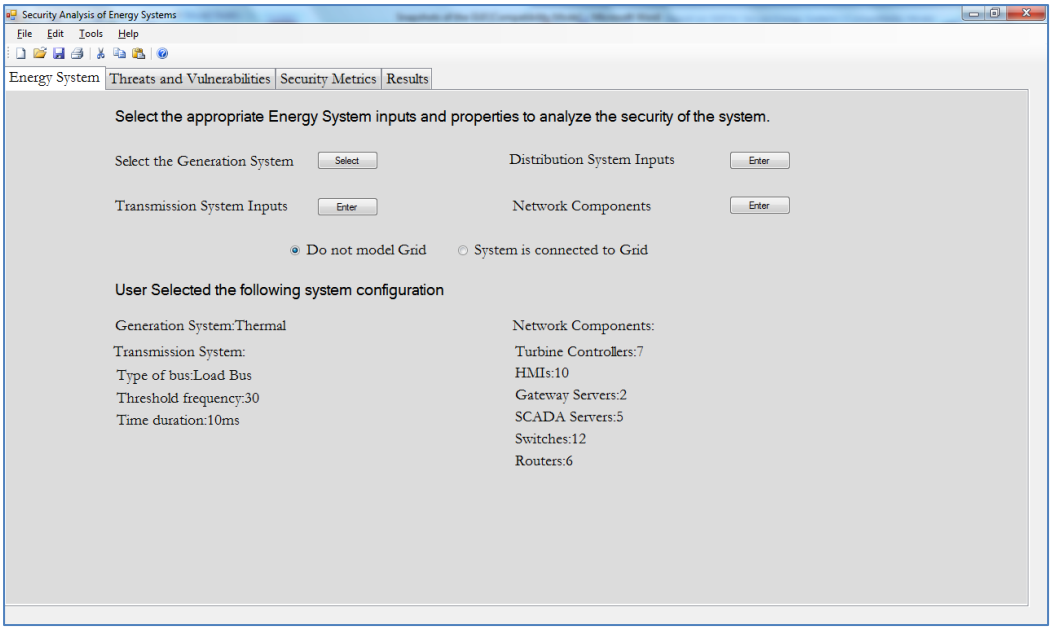
The initial framework for the Security Analysis GUI has been created. The salient features of the GUI include the user's inputs specifying the kind of generation system, transmission and generation system and the network architecture i.e., specifying the control system applications and network switches. The GUI has been created used C# language in Visual Studio 2010 tool. The concept of this framework has been based on the following elements:

- Degree of loss and damage due to the impact of the hazard.
- Degree of exposure to the hazard i.e., the likelihood of being exposed to the hazards of as certain degree and the susceptibility of an element at risk to suffer loss and damages.
- Degree of capacity of resilience i.e., the ability of a system to anticipate, cope with/absorb, resist and recover from the impact of a hazard or disaster. For example, the vulnerability of the electric power system might be assessed in terms of the frequency of major blackouts and the associated severity. A number of approaches can be undertaken for the vulnerability assessment depending on the type of system, the objective of the analysis and the available information.

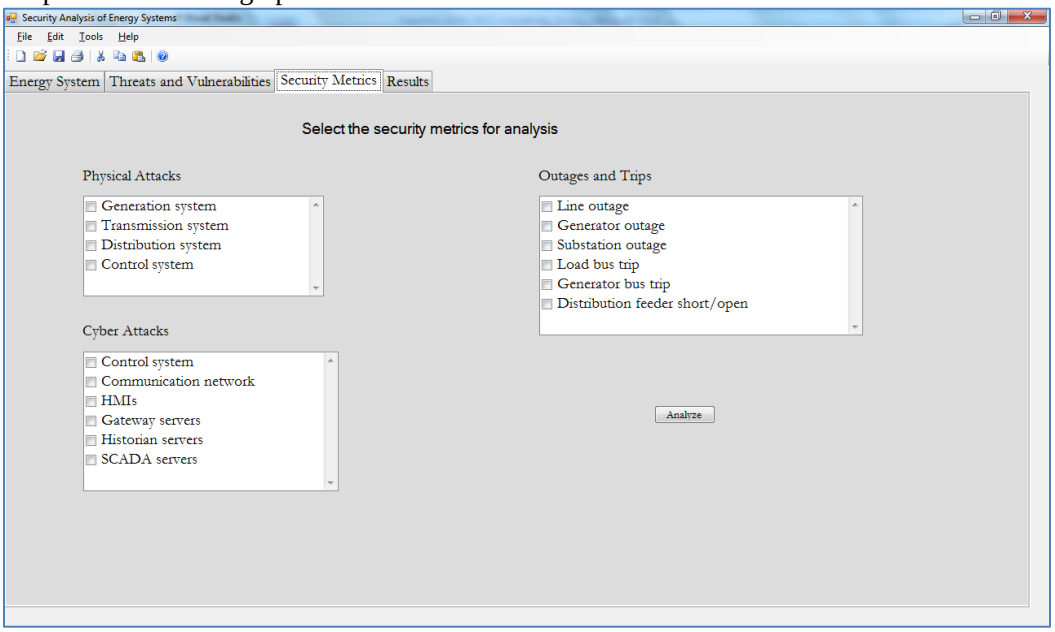
The GUI developed has the functionalities for analyzing the energy system as a complete system, including the generation, transmission, distribution and the control system; the snapshots of the GUI are as follows:

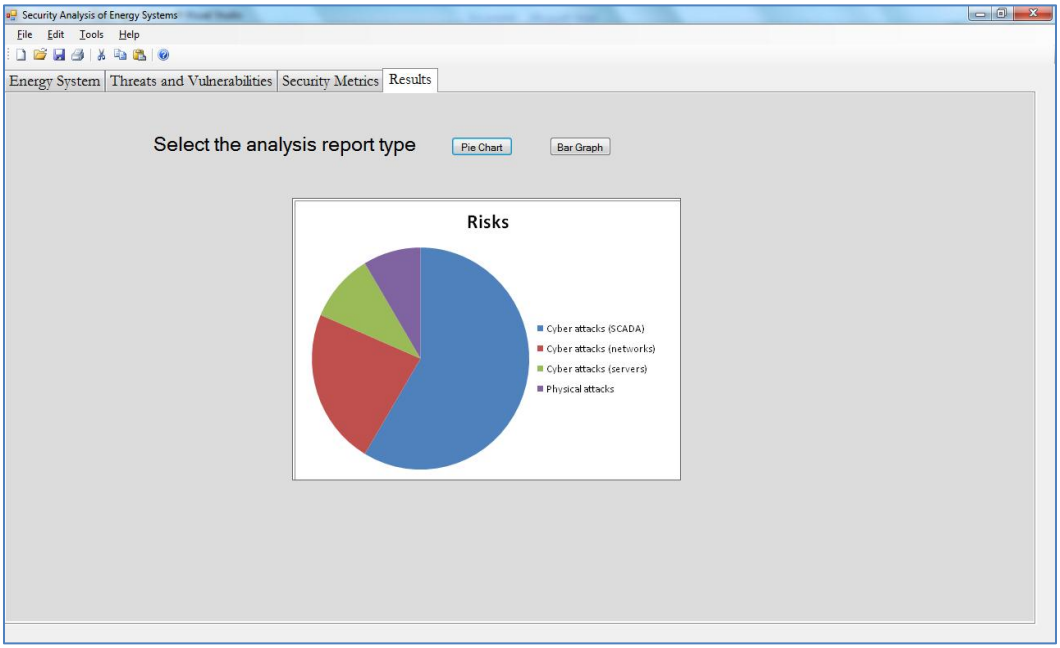


By clicking the Select button, the user can select the type of generation system. This would give the user the ability to analyze the selected energy system. The database at the back-end would contain the elements which are contained in the generation system. Similarly, the user can select the transmission, distribution and control system elements. The inputs are reflected back for the user to review and make changes if needed.



The threats and security metrics for the analysis are then selected and the analysis yields results which can be viewed as a pie chart or a bar graph.





Next Steps:

The research on the security of energy systems has made a clear point that the threats and attacks on the energy system are very dangerous and can cause serious damages to the systems and people globally as well as in the country. The security measures for physical, cyber and the various other kinds of attacks mentioned above need to be in place for the impact of the attacks to be minimal. This needs to be done effectively and efficiently so as to avoid major damages. The next steps would be to complete the GUI with additional functionalities as needed and make it a complete tool for the analysis of security of energy systems.

New collaborations		
Partner name	**Title or short description of the collaboration**	**Funding, if applicable**
Poolla, Varaiya UC Berkeley	Smart Grid	None