THE CAPS-SNL POWER SYSTEM SECURITY TESTBED

J. Tang (*), R.Hovsapian (*), M. Sloderbeck(*), J. Langston(*), R. Meeker(*),P.G. M[c]Laren (*), D. Becker (+), B. Richardson (+), M. Baca (+), J. Trent (+), Z. Hartley (+), R. Parks (+), S. Smith (+)

(*) Center for Advanced Power Systems, Florida State University, Tallahassee, FL, USA
(+) Sandia National Laboratory, Albuquerque, New Mexico, USA

Introduction

Securing cyberspace is a vital element of critical infrastructure protection efforts currently underway in the United States and other industrialized nations. As pointed out in U.S. Department of Homeland Security Testimony to Congress, interdependency of cyber and physical infrastructure is particularly "acute" in the case of control systems [1]. The automation and communication networks being used today to control electrical power systems are a particular concern, and, until now, methods to explore the effects on the physical power system due to control system compromise have been very limited. "Successful" hackers could gain access to vital control and protection settings and commands and cause significant problems for the operators and the system. In order to understand the consequences of hacker attacks and to find ways to harden the system against such attacks, Sandia National Laboratories (SNL) and the Center for Advanced Power Systems (CAPS) at FSU have combined forces to create a "virtual" electrical grid system linked to an actual control, communication and protection system.

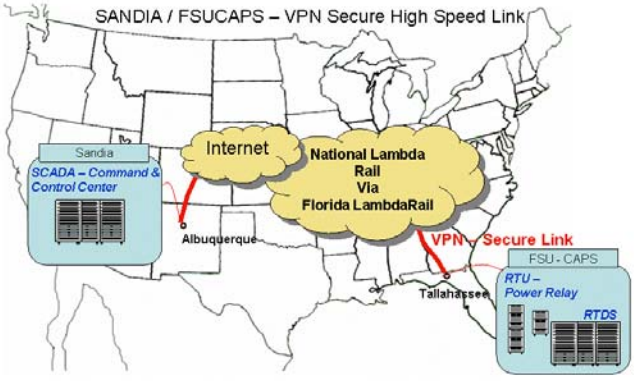

Figure 1. CAPS-SNL test bed and VPN Link.

The virtual testbed utilizes the established facilities in each organization as shown in Figure 1. At SNL, a commercial electric utility SCADA (Supervisory Control and Data Acquisition) system has been installed; VPN (Virtual Private Network) link terminals are available. At CAPS, there is a real time power system simulator (RTDS^{TM}), a real time protection and control system and two SCADA communication protocol interfaces. Facilities at the two locations are connected by the VPN link. Over the link, the SNL control center can control the "virtual" electrical grid system modelled in the RTDS; the SNL engineers can access control and protection settings. This testbed provides a realistic platform on which "virtual" hackers (computer experts at SNL) can exercise their skills in showing how and with what consequences the system can be breached. The hacker attacks will be carried out in a secure facility, SNL, and the consequences of hacker attacks will be seen in the other facility, CAPS. This combination shields the critical hacker attack information from the public domain in CAPS.

This paper describes the setup of this testbed and some of the recent hacker scenarios being tested. These hacker scenarios range from a casual hacker who has no power system knowledge to a hacker who has read the publicly available relay manuals and is familiar with the power system operation. These experiments reveal weaknesses in the cyber security set-up of the networks and in the security safeguards built into the operating software of control and protection equipment.

SCADA Automation

Figure 2. shows a typical contemporary substation with its various links to control stations including SCADA and protection engineering control centers. The various control stations may all be in the same location or in different locations to better suit the application in question. At the Bay level there are relays, meters, recorders and other IED's that communicate with a central processor at the substation level for distribution to the various control stations. Typical communication protocols are shown on the links. A substation control center may include the following functions:

- Remote Data Collection
- Displays
- Remote Control
- Event Alarm

The control center polls data from local meters, recorders, relays and IED's on a typical refresh interval of 2-3 seconds. Typical analog values are RMS currents (I), RMS voltages (V), Active Power (P), Reactive Power (Q), Frequency (Freq). Digital data may include various switchgear states.

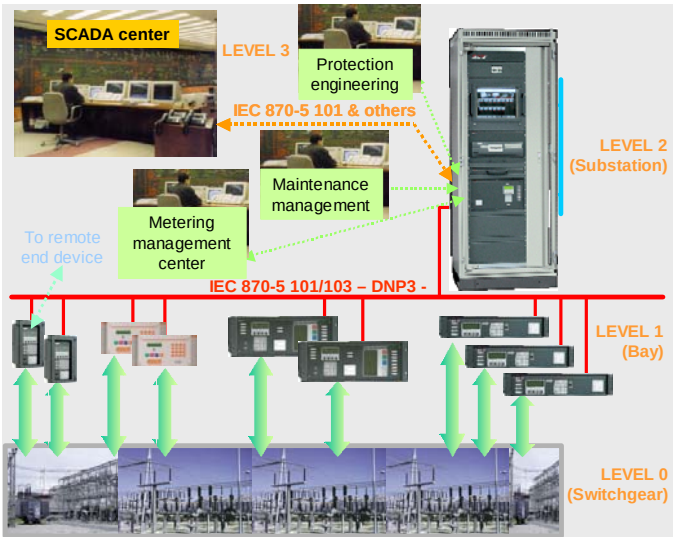

Figure 2. Typical modern substation showing apparatus and communication links

Those data will be displayed in the control center in view of the operators. The control center will have a display showing a singe line diagram network layout with 'real time' switch position, states and power flow values on various lines. The operators will monitor those values to gain information on the actual system. The control center can reconfigure the system by remotely operating the circuit breakers. This is the control center remote control function. It will become necessary when a fault and the subsequent protective actions give rise to a region where customers lose power. A separate protection engineering center will provide access to the relays, RTU's etc. when there is a need to download a recording after a system fault to analyze the cause, or when a relay setting needs to be changed after the system reconfiguration.

Control center functions have been implemented within commercial SCADA software. A typical commercial software is used in this study for the control center functions.

RTDS

The real time digital power system simulator (RTDS) is a massively parallel computer custom-built to solve the power system network differential equations in real time with a typical time step of 50μs. Unlike a standard supercomputer it also has a large number of I/O ports to allow access to particular nodes or line ends to measure current or voltage either in digital or analog format. These analog outputs are scaled to ±10V and must be taken through conditioning amplifiers before being connected to an actual measuring or control device. Outputs from the latter devices, e.g. a trip signal from a relay, can be taken back into the simulator to trip the corresponding breaker while the simulation runs on with the breaker in its new state. The RTDS and control/protective devices form a hardware-in-the-loop closed system, with the hardware devices seeing signals similar to those they would see from a real system. Figure 3. shows the set up at the CAPS end with 5 relays and a communication processor interfaced to the RTDS.

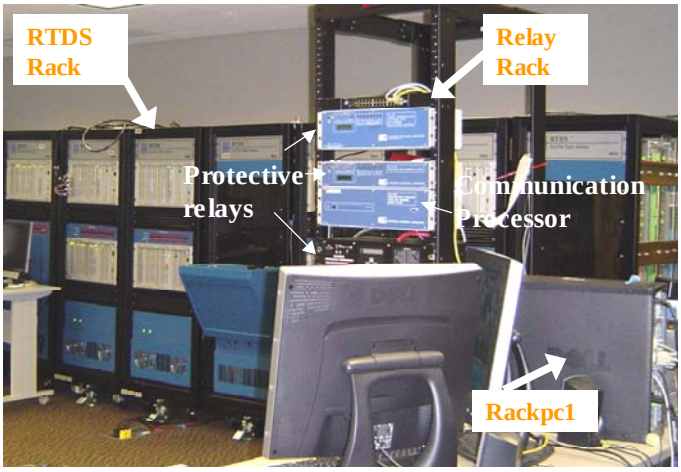

Figure 3. The CAPS real time digital simulator system

(Relays in the figure are typical types of modern digital relays used in the field.)

Where:

RTDS Rack: representing a real time electrical power grid

Relay Rack: representing a real time protection system

Rackpc1: representing a real time control system

The simulator is configured and controlled through a graphical user interface that contains sliders and push buttons, which can be used to alter set points and initiate events during a simulation run. The operator can also choose to take snapshots of a particular variable and to display measured variables on a "screen" meter.

Setup

Communication

Network Media

A Wide Area Network (WAN) was needed to enable a secure Virtual Private Network (VPN), for site-to-site secure communications and connection for the FSU-CAPS Real Time Digital-Power Simulator to Sandia's **S**upervisory **C**ontrol **A**nd **D**ata **A**cquisition (SCADA) – Network and control system simulator. A VPN solution was selected which would lower the capital outlay and ongoing operating cost of a traditional point-to-point secure network. The traditional point-to-point network solution had been evaluated and deemed to be too expensive. The VPN network solution leverages the existing Florida State University's Florida Lambda rail infrastructure, which is also a part of the National Lambda Rail network. It also leverages the Internet where the Lambda rail is not available as shown in Figure 1. The selected solution meets the security level needed and has the flexibility and scalability to meet the project future growth. This solution also supports the commercial standards and allowed the geographically distributed research team, CAPS located in Tallahassee Florida, and Sandia in Albuquerque New Mexico, to benefit from each others installations and expertise. The team was able to cooperate while developing the simulated power grid infrastructure on the RTDS at CAPS

as well as when the control center system for the simulated power grid was developed at Sandia.

Protocol Interfaces

Communication protocols that are typically used in the SCADA automation system are:

- Modbus
- DNP V3.0 (predominantly popular in North America)
- IEC 870-5-101 (The European partner to DNP V3.0)
- UCA

Some SCADA software may have additional protocols such as BETAC, Harris, PERT, TRW, etc. Those protocols were developed in the past to interface with some particular vendor's products. They are not commonly used. The CAPS-SNL Testbed has installed two SCADA protocol interfaces, Modbus/Ethernet and DNP V3.0/ Ethernet. The Modbus/Ethernet links the RTDS to the SNL control center and the DNP V3.0/Ethernet links the local protective devices through the communications processor to the SNL control center.

Security

The team adopts the recommendations from the Sandia security experts and applies the 'Virtual Private Network (VPN)' method and the password protection method in constructing the CAPS-SNL secure testbed. At each end of the facility (CAPs or SNL), there is a private network dedicated for use by the CAPS-SNL testbed project. Devices and computers in the network are protected by passwords. At the endpoints of the two private networks, information packages are encrypted before transport across the public WAN. Many things have to happen in order to successfully establish a security relationship between the two endpoints capable of building an encrypted tunnel across the WAN. SNL supports all this work. Once the work is completed, the encrypted tunnel 'virtually' connects the two endpoints as if they were on the same LAN and creates a virtual private network.

Latency

The network performance, i.e. latency, speed and reliability, is tested. A type of network data traffic capture software is installed at each end of VPNs. It captures the data information emanating from the SNL end and finally arriving at the CAPS end and vice versa. Those data packages are analyzed in the SNL facility to determine the status of the network, i.e. how good it is and how good it could be.

CAPS-SNL Power System Security Testbed

Figure 4. is the diagrammatic representation of the CAPS-SNL hook up. The control center test bed at SNL is connected by a VPN link to the real time power system simulator at CAPS. The latter runs a model of an electrical power network. CAPS also has a control center data display connected to the RTDS on which correct data and switch positions are shown whereas the control center display at SNL may be corrupted by the hacker. Data transport over the network includes RMS voltages, RMS currents, Reactive Power, Active Power and Switchgear states. Sandia has also access to switches and set points on the RTDS using a Modbus protocol and to the actual relays using the DNP3 protocol.

The hacker attacks take place at the Sandia end (Figure 5.) by the SNL "Red Team" who gain access to the network and intercept the flow of data between the control center and the RTDS. This allows them to change the data in such a way to operate a switch, display incorrect metering data or change a relay setting

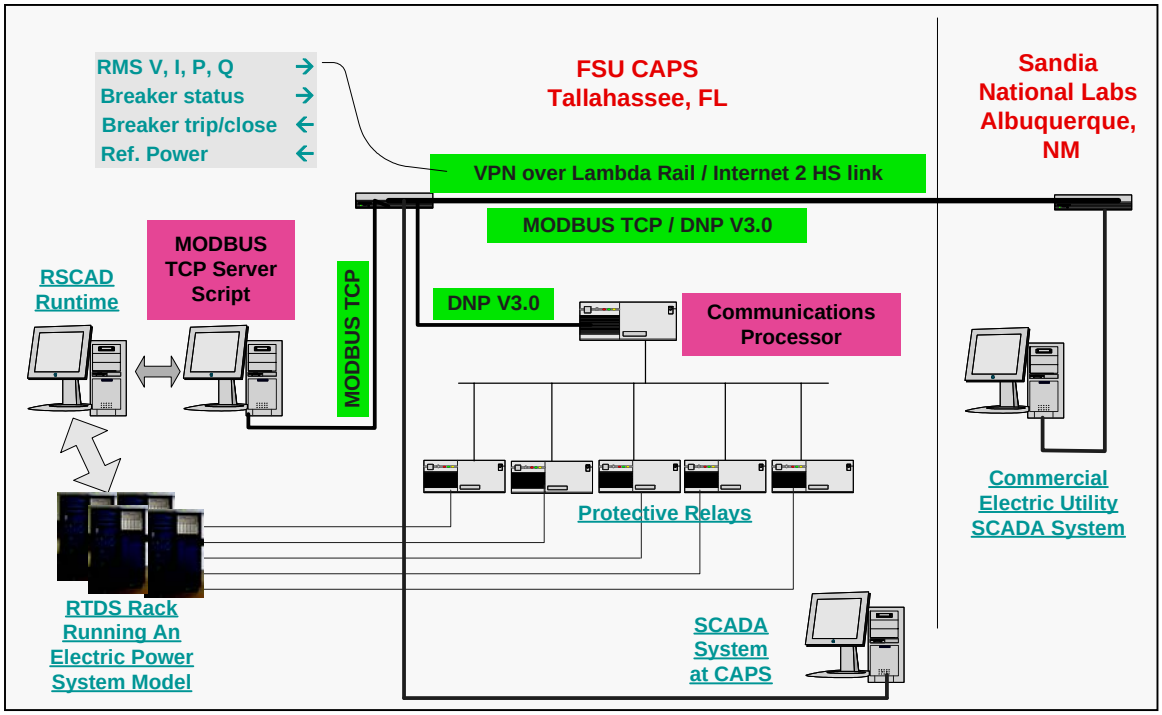

Figure 4. Diagrammatic Representation of CAPS-SNL Power System Security Testbed

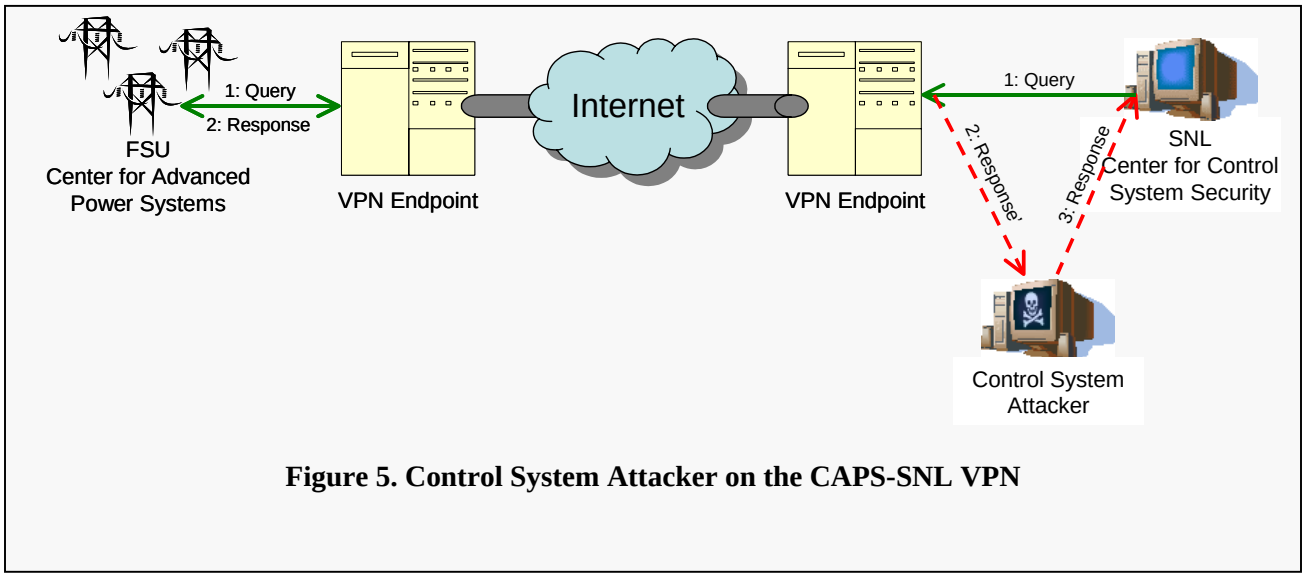

Figure 5. Control System Attacker on the CAPS-SNL VPN

Attacks

Test System

A small portion of a power grid was chosen for the purposes of demonstrating the operation of the test set up. (A larger more complex system will be arranged for the next stage test). A one-line diagram of this demo system is given in Figure 6 and Figure 7. The system consists of a remote hydro station on the right hand side feeding a large equivalent system on the left hand side through some 230kV overhead transmission lines. The hydro station is represented by a full generator model including prime mover, governor, AVR and PSS. The transmission lines are distributed parameter models and the large equivalent system is an ideal source in series with an impedance. The hydro generator set will swing against the ideal source when the system is disturbed. There is a generator relay, a transformer relay, a distance relay and a couple of busbar protection relays interfaced to the appropriate location in the RTDS and some additional relays are simulated as necessary in the RTDS.

Cyber Attack Scenarios

Two types of hacker are considered in the examples given.

1) The first type is a "benign" computer buff who gains access to the network and randomly changes data streams going from the control center to the power system on the RTDS.

2) The second type is a 'malicious' hacker with power system knowledge who has read the publicly available documentation on relaying devices and control devices. He/She could gain access to the network, get past the device password (often a default password), and then change the setting/states to cause maximum damage to the power system.

Attack Scenario 1

The SNL 'Red team' (representing the "benign" hacker) gains access to the CAPS-SNL VPN. By randomly altering bits in the data stream flowing from the SNL control center to the CAPS RTDS power system they succeed in opening all breakers within a relatively short time. The generator G1 in Figure 6 was separated from the network and any loads on the intermediate busbars were dropped.

Attack Scenario 2

The SNL 'Red team' (this time representing the "malicious" hacker) gains access to the engineering network through the CAPS-SNL VPN. The hacker decides to alter a relay setting to achieve a breaker trip when the system is heavily loaded. Once the hacker finds the IP address for the relay he then has to get around the password in order to change the relay setting. He tries the manufacturer's default password and to his surprise it works. A careless relay engineer has not changed the relay default password, which gives the hacker full access to the relay. He changes the setting on one of the over-current elements of a relay to just below full load current and saves the setting to let the new current setting take effect. When the load current reaches this value during a peak load period the relay trips, removing line 2 from the network. In this case the network remains stable with only a small power swing.

Attack Scenario 3

The malicious hacker plans to cause severe damage to the power system. He wants to set a scenario in which a relay trips when the system is running at maximum power and this event results in a power swing which causes the system to separate. This kind of trip will have maximum effect on the remaining system because of the heavy loading and will possibly lead to cascading events. The hacker is familiar with the daily operation of the power system. He knows that in the late afternoon, around 4:00PM, to meet the maximum load demand, the control center will raise power generation at the G1 station to 90% of its maximum station capacity. The only exception is when there is a line out of service in which case the power output is restricted to 70%. The distance relays on

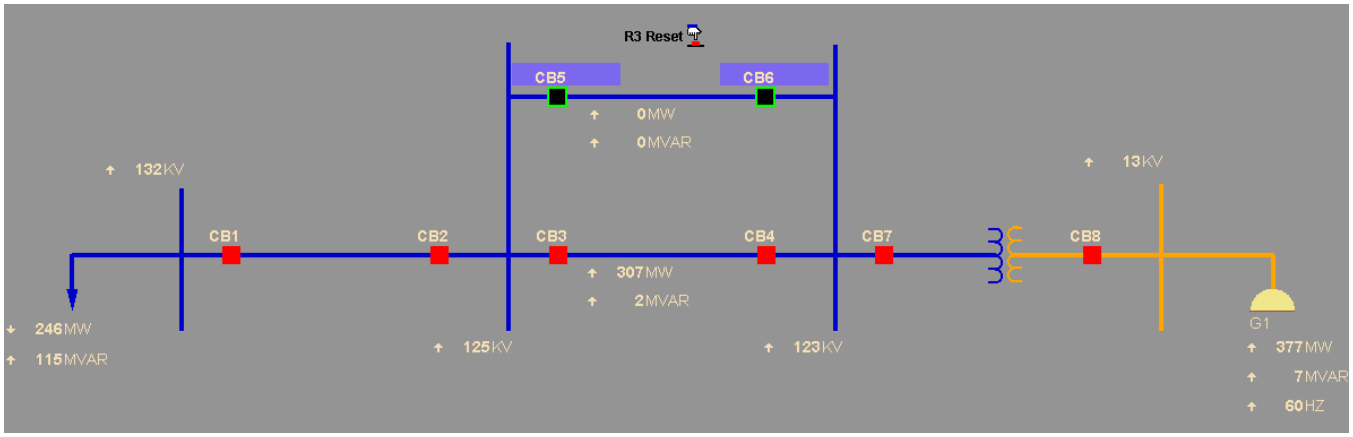

Figure 6. SCADA Display at CAPS: Correct SCADA Data

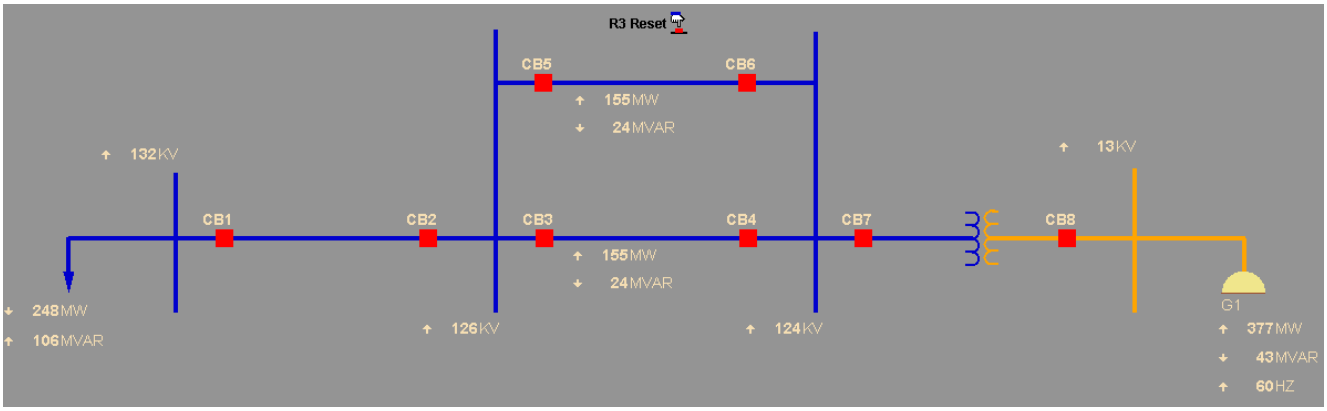

Figure 7. SCADA Display at SNL: Corrupted SCADA Data

the transmission lines allow single pole tripping with a high speed reclose.

The plan is to render the system more vulnerable during the afternoon peak load period on a day when thunderstorms are likely in the area. He first removes one of the parallel lines from the system shortly before the peak load period. He masks this action by maintaining the previous control center switch positions. Figure 6. and Figure 7. are data displays. Figure 6. is the screen on the display connected directly to the CAPS simulator which shows the correct switch positions and power flow. Figure 7 is the screen at the SNL control center which is corrupted by the hacker. Based on this screen the operator will go ahead and raise the power level above the 70% limit when required. The remaining line is heavily loaded when it suffers a flashover caused by a lightning strike on one phase. (The fault was initiated through the RTDS run time environment at the CAPS end.) Subsequent events are described in order. First, the local line distance relay detects the fault and executes the correct 'single pole trip and reclose'. Then a significant power swing sets in after reclosing which takes the measured positive sequence impedance just into the zone 1 region of the relay and results in a three phase trip. Thus, the generator G1 is separated from the network by losing both of the parallel lines. The generator will overspeed and over- voltage while the governor and AVR regain control of the now isolated machine.

Figures 8-9 show the dynamics. Apparatus connected to the generator busbar could be damaged by the momentary over-voltage and higher frequency. It takes several seconds for the governor and AVR to get the generator voltage back to normal after separation (RHS of Figure 8 &9).

It is important to recognize that a load flow analysis would not reveal this vulnerability since the system is steady state stable with only one line in and 90% power. A stability program could demonstrate the power swing but would require a sophisticated relay model to be incorporated to reveal the trip.

Conclusion

Once a hacker gains access to any of the networks shown in Figure 2 there is a great variety of vulnerabilities available to him in the various measurement, control and protection apparatus. The CAPS-SNL test bed allows most of those vulnerabilities to be explored and consequently points to counter measures which could be taken to recognise and mitigate the effects of such attacks. Once the power system under consideration grows beyond the simple system used to demonstrate the principle of the CAPS-SNL test bed it will

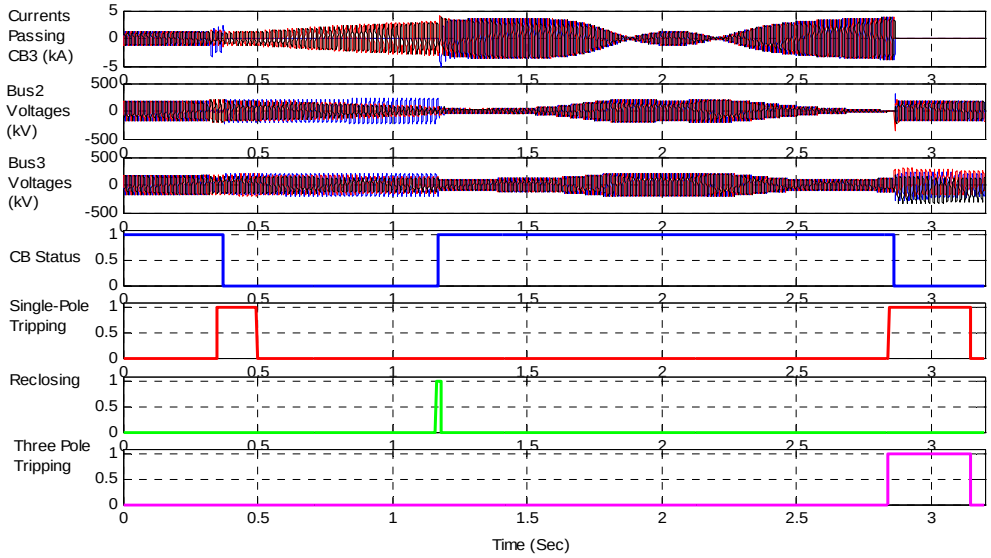

Figure 8. Currents, Voltages, Relay Trips

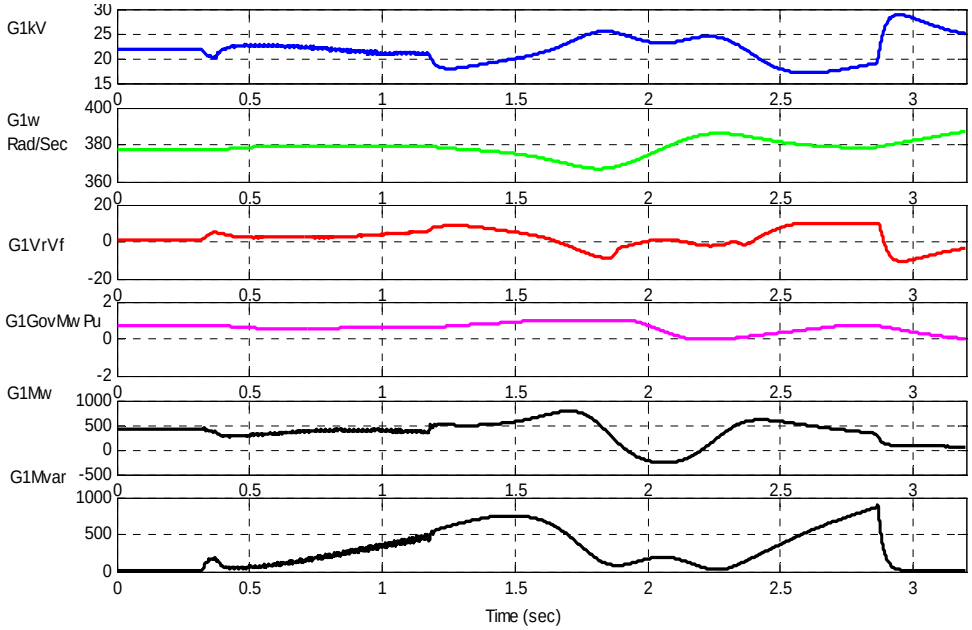

Figure 9. Generator Terminal Voltage (G1kV), Speed (G1W), Regulator Output (G1VrVf), Governor Output (G1GovMuPu), Active Power (G1Mw) and Reactive

become an excellent training simulator for system operators where they can be exposed to system events in a realistic real time environment.

Newer protocols used in the communication systems (DNP3 and IEC 61850) are generally more informative, which means they will also convey more information to a hacker compared to some of the older protocols presently in use. There is clearly a need to harden each element in the system to better resist cyber attacks which get past the first line of defence in the communication network.

The ability to thoroughly explore the consequences of control system cyber-attacks on the power system made possible by this approach becomes a valuable tool for risk assessment and development of the business case for cyber security, which have been identified by energy sector stakeholders and the U.S. government as key challenges and barriers to securing control systems [2]

References

1. Purdy, Jr., D.A., "Written Statement of Donald (Andy) Purdy, Jr., Director (Acting), National Cyber Security Division, Information Analysis and Infrastructure Protection Directorate, U.S. Department of Homeland Security", testimony to U.S. House of Representatives, Committee on Science, September 15th, 2005.

2. U.S. Department of Energy, U.S. Department of Homeland Security, "Roadmap to Secure Control Systems in the Energy Sector", January 2006.