Protecting Intelligent Distributed Power Grids against Cyber Attacks
- Final Scientific Report

December 10, 2010

This project “Protecting Intelligent Distributed Power Grids against Cyber Attacks” was conducted for the Department of Energy Office of Electricity Delivery and Energy Reliability under Contract DE-FC26-07NT43313.

Authors:

Dr. Dong Wei	Siemens Corporate Research
Dr. Yan Lu	Siemens Corporate Research
Dr. Mohsen Jafari	Rutgers University
Paul Skare	Siemens Energy, Inc.
Kenneth Rohde	Idaho National Laboratory

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, makes 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.

Protecting Smart Grid against Cyber Attacks

Dong Wei, Yan Lu, Mohsen Jafari, Paul Skare, and Kenneth Rohde

***Abstract*—Like other industrial sectors, the electrical power industry is facing challenges involved with the increasing demand for interconnected operations and control. The electrical industry has largely been restructured due to deregulation of the electrical market and the trend of the Smart Grid. This moves new automation systems from being proprietary and closed to the current state of Information Technology (IT) being highly interconnected and open. However, while gaining all of the scale and performance benefits of IT, existing IT security challenges are acquired as well. The power grid automation network has inherent security risks due to the fact that the systems and applications for the power grid were not originally designed for the general IT environment. In this paper, we propose a conceptual layered framework for protecting power grid automation systems against cyber attacks. The following factors are taken into account: 1) integration with existing, legacy systems in a non-intrusive fashion; 2) desirable performance in terms of modularity, scalability, extendibility, and manageability; 3) alignment to the ”Roadmap to Secure Control Systems in the Energy Sector” [1] and the future smart grid [2], [3], [4]. The on-site system test of the developed prototype security system is briefly presented as well.**

***Index Terms*—Smart grid, cyber attacks, network security, vulnerability, Quality-of-Service (QoS).**

I. Introduction

THe recent discovery that hackers have inserted software into the US electrical grid [5], which would allow the grid to be disrupted at a later date from a remote location, clearly demonstrates the fact that the utility infrastructure is quite vulnerable and that its overall mission of serving the population could be severely compromised as a result of unexpected man-made or natural disasters. Another study [6] reports that cyber attacks can destroy the electrical power grid of the western United States due to cascading failures.

As other industry sectors are already experienced with arming automation systems with modern IT (Information Technology) technology, the power grid is also facing the trend of integrating the electrical infrastructure with information infrastructure, and it is experiencing a profound change toward the Smart Grid [2], [3], [4], [7], [8], [9], [10]. This change not only moves power automation systems from outdated, proprietary technology to the use of common technologies - personal computers, Microsoft Windows and TCP/IP/Ethernet, but also brings the isolated, closed network of power control systems to the public network. The integration brings in tremendous cost and performance benefit to the power industry, as well as arduous challenges of protecting the automation systems from security threats from hackers. It is misleading to suggest that IT people take the full responsibility for power grid network security including automation and control networks. Compared with regular IT systems, power automation systems have definite different goals, objectives and assumptions concerning what needs to be protected [11]. It is important to understand what ”real time performance” and ”continuous operation” of a power automation system really means and to recognize that power automation systems and applications were not originally designed for the general IT environment. Therefore, it is necessary to embrace and use existing IT security solutions where they fit, such as communication within a control center, and develop unique solutions to fill the gaps where IT solutions do not work or apply.

This paper is organized as follows: Section II presents an in-depth analysis on the current power automation system’s 3-level configuration - corporate, control center and substation; it discusses communication specifications in terms of possible communication topologies, protocols, performance requirements in terms of delay and bandwidth, etc., and associated vulnerabilities, as well as the potential cyber attack sources, scenarios and the adverse impacts on smart grid operation from different perspectives; Section III presents the major challenges and design strategies of security solutions for smart grid; the basic principles , functionalities and implementations and system test of the proposed Integrated Security System (ISS) are presented in Section IV; Section V concludes this paper and discusses potential future work based on the ISS.

II. Background

The power grid system physically connects power generation (such as fossil fuel power plants) and power consumers. The major function of the power grid is to deliver electricity economically subject to the constraints of capacity and reliability of power equipment and power lines. The power grid system includes two parts - transmission and distribution. Power transmission is the bulk transfer of electrical power, which operates at a high voltage (100 kv or above) and delivers electrical power from power plants to substations close to populated centers. Power distribution delivers electricity from the substations to consumers, and operates at medium and low voltage levels (less than 100 kv).

A. Scope and functions of the power grid

From the power flow viewpoint, the input to the power grid is high voltage (100 kv or above) power, stepped up by the

This is the final scientific report of the project ”Protecting Intelligent Distributed Power Grids against Cyber Attacks”, which was conducted for the Department of Energy Office of Electricity Delivery and Energy Reliability under Contract DE-FC26-07NT43313.

Dr. Dong Wei and Dr. Yan Lu are with Siemens Corporate Research, Inc, 755 College Road East, Princeton, NJ 08540 (e-mails: dong.w@siemens.com and yanlu@siemens.com).

Prof. Mohsen Jafari is with Rutgers University, New Brunswick, NJ 08854 (e-mail: jafari@rci.rutgers.edu).

Paul Skare is with Siemens Energy, Inc., Minnetonka, MN 55305 (e-mail: paul.skare@siemens.com).

Kenneth Rohde is with the Idaho National Laboratory, Idaho Falls, ID 83415 (e-mail: kenneth.rohde@inl.gov).

Manuscript received on October 1, 2010; revised on xxxx, 2011.

power plant transformer from the low voltage power produced by the generators. The output of the power grid is electricity at medium or low voltage (less than 100 kv), stepped down by transformers in substations, and delivered to commercial, industrial and residential consumers.

The major functions of power grid are performed in three different levels: corporate, control center, and substation. At the corporate level, the following major functions of both business management and operation management are performed:

- Planning - plan of equipment and line upgrades based on forecast of load and generation sources, market conditions and system utilization;
- Accounting - management of contracts and bids with other market participants;
- Engineering - system design and engineering for transmission and distribution lines and automation systems;
- Asset Management - monitoring, replacement and maintenance plan of equipment and lines;
- Historical Information System - An on-line historical database is commonly used to retain all telemetry data, operator actions, alarm summaries, etc., for a periodic of time that ranges typically from 3 to 24 months.

At the control center level, the following major real-time and non-real-time functions are performed:

- Forecast - short-term forecasting of load and power generation sources;
- Monitoring - monitoring of system state, activity, load, equipment conditions;
- Operation - switching operation, changing setups, starting emergency procedure, performing system restorations, etc.;
- System Analysis - model update, state estimation, contingency, and stability analysis, power flow analysis;
- Recommendation - recommendation of preventive, corrective, and optimized operations;
- Fault/Alarm Processing - locating fault and intelligent processing of alarms;
- Training - operator training;
- Logging -archiving logs and reports;
- Data exchange - exchanging data with ISO/RTOs, power plants, consumers and peer transmission and distribution system operators.

At the substation level, the following major real-time and non-real-time functions are performed:

- Normal Operation - collecting data and alarms and sending them to control center, executing commands issued by control center;
- Exchange of protection data between the RTU and IEDs within the substation. Relay devices perform protection, control and indication gathering functions.
- Emergency Operation - power system protection, load shedding, recovery from load shedding, shunt control, compensation control, etc.;
- Engineering - protection engineering, automation engineering, line engineering;
- Logging - archiving logs;
- Maintenance - equipment and line maintenance.

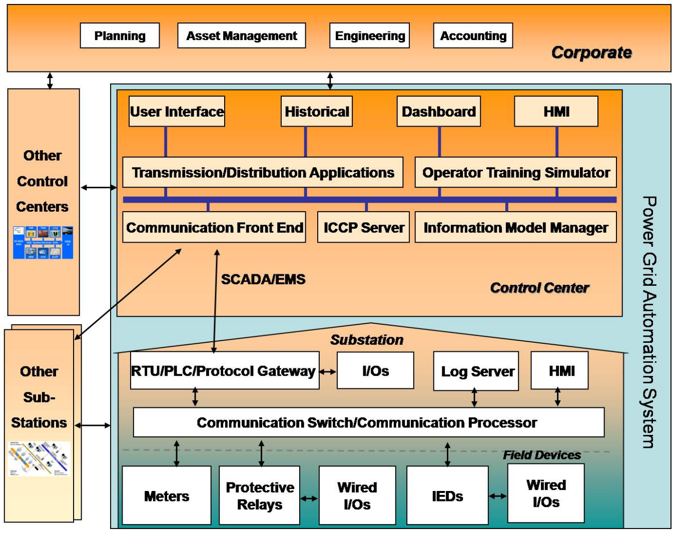


Fig. 1. Power Grid Automation System

B. Power Grid Automation Systems

A typical grid automation system, as shown in Fig. 1, is a horizontal integration of one or more control centers, with each center supervising the operation of multiple substations. The power grid automation system is a layered structure and performs data collection and control of electricity delivery. A control center typically includes an EMS (Energy Management System) and a SCADA (Supervisory Control and Data Acquisition) master. Substations contain RTUs (Remote Terminal Unit, also called a SCADA slave), PLCs (Programmable Logical Controller), GPS (Global Positioning System) Sync. Timers, HMIs (Human Machine Interface), communication devices (switch, hub, and router), log servers, data concentrators, and a protocol gateway. IEDs (Intelligent Electronic Device) are field devices, including an array of instrument transducers, meters, tap changers, circuit re-closers, phase measuring units, and protection relays.

C. Power Grid Communications Systems

In order to deliver electrical power from power producers to consumers economically, power grid system operators have to exchange data with power producers, ISOs (Independent System Operator), RTOs (Regional Transmission Organization), consumers and peer system operators. This is performed at the corporate level and control center level. Power grid system operators also possess communication links between corporate and control centers, and control centers and substations. As shown in Fig. 1, at control/operation center level, dedicated lines are widely used and ICCP (Inter Control Center Protocol) is deployed as the communication protocol. LAN (Local Area Network) and IP-based (Internet Protocol) protocols are usually used for the communication link between corporate and control center; serial link and DNP3.0 (Distributed Network Protocol) are widely used for the communication link between control center and substations. Wireless technology is also deployed for communication between control center and substations.

Communication		Typical Applications	Topology	Protocols	QoS Requirements
Intra-substation	Time critical	Protective relays exchange data to coordinate protection scheme	1.Point-to-point 2.Point-to-many	1. DNP3 2. IEC-61850	1. Delay≤1ms 2. Refresh rate≤1 ms 3. Bandwidth≤10 kbps 4. Time sync. required
	Non time critical	Configuration and setting updating, load shedding, fault processing	Point-to-point	3. Proprietary protocols (ModBus Plus, ProfiBus, etc.)	1. Delay≤ 100ms 2. Refresh rate – event-driven 3. Bandwidth low 4. Time sync. required
Inter-field and Substation-field		1. Pole-top automated switches exchanging of non-protection-related loading data. The data later is sent to different masters for load-sharing purposes. 2. Data concentrator collects equipment-monitoring data	1.Point-to-point 2.Multicast 3.Broadcast 4.LAN	1. DNP3 2. IEC-61850 3. Proprietary protocols (ModBus Plus, ProfiBus, etc.) 4. Wireless protocols, such as IEEE 802.15.4	1. Delay≤1s 2. Refresh rate ≤1s 3. Bandwidth low 4. Time sync. required
Control-center to substation	Operation critical	1. Substation automation control and monitoring 2. Configuration and setting updating; 3. Alarm/fault processing	Point-to-point	1. DNP3 2. IEC-61850 3. Proprietary protocols (ModBus Plus, ProfiBus, etc.) 4. Wireless protocols	1. Delay≤100 ms 2. Refresh rate≤2 s 3. Bandwidth 1.2 kbp ˜ 100 Mbps 4. Time sync. required
	Non operation critical	1. Non-power system equipment monitoring 2. Power quality monitoring 3. Customer metering			1. Delay≤10 s 2. Refresh rate≤1 hour 3. Bandwidth low
Intra-control-center		Updating databases and HMIs with data collected by FEP	LAN	IP-based protocols, such as ssh, and HTTPs	1. Delay≤10 ms 2. Refresh rate≤10 ms 3. Bandwidth 10 Mbps ˜ 100 Mbps
Inter-control-center		1. Fault and alarm data exchanging for contingency analysis and emergency operations 2. Metering data exchanging between territorial boundaries to initialize state estimation or load distribution applications.	1.Point-to-point 2.WAN	ICCP (Inter-Control-Center Protocol)	1. Delay≤10 s 2. Refresh rate 10 ˜20 s 3. Bandwidth 10 kbps ˜ 100 kbps
Control-Center to Corporate		1. Exchanging historical data for mid-term and long-term planning 2. Collecting data for asset management 3. Collecting data for automation system engineering and troubleshooting.	1. LAN 2. WAN	IP-based protocols, such as FTP, and HTTP	Real-time communication is not required
Intra-Corporate		1. Exchanging data for long-term planning 2. Collecting data for asset management	1. LAN 2. WAN	IP-based protocols, such as FTP, and HTT	Real-time communication is not required
Inter-Corporate		Exchanging data for contracts, e-mails, orders, and invoices, etc.	WAN	IP-based protocols, such as FTP, and HTT	Real-time communication is not required

TABLE I

COMMUNICATIONS AND THEIR CHARACTERISTICS IN POWER GRID AUTOMATION SYSTEMS

D. Potential Cyber Attacks and their Impacts on Power Grid

The complicated communication network makes power grid automation systems more vulnerable to cyber attacks. We classify cyber attacks into three categories:

- Component-wise: Field components commonly used by power transmission and distribution systems include RTU, and IEDs. These devices frequently support a user interface to allow engineers to perform configuration or diagnostic functionality from a remote location (maintenance ports may be IP based). Remote access may allow an intruder to take over the device and cause faulty conditions, such as: 1) mislead data presented to control system operator; 2) damage to field equipment if operator performs supervisory control operations based on inaccurate field data or; 3) loss of service due to intruder shutting down the device.
- Protocol-wise: Virtually all modern data communication protocols adhere to a messaging protocol that is well documented and available in the public domain. The DNP protocol is widely used by electric utilities throughout

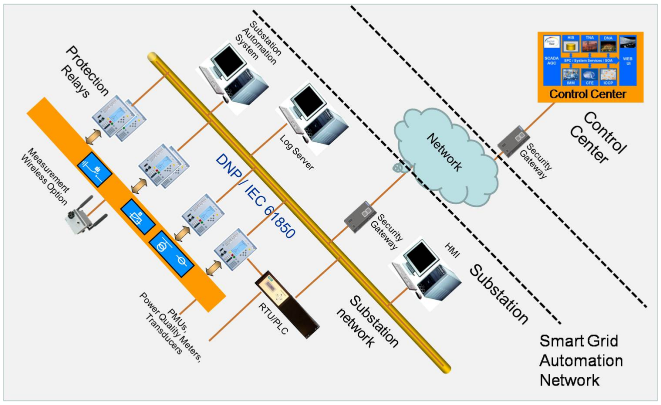


Fig. 2. Gateway Security Solution

North America. The DNP protocol specification can be attained for a nominal user fee. Using these documented protocols allows an intruder to do reverse engineering of the data acquisition protocol and exploit the protocol using a ”Man-in-the-middle” attack. The adverse effects could include sending misleading data to the field device or control center operator resulting in 1) financial loss if the attack leads to excess generation output; 2) safety vulnerability if a line is energized while linemen are in the field servicing the line; 3) equipment damage if control commands are sent to the field resulting in overload conditions.

- Topology-wise: Network topology vulnerability can be exploited by intruders. For example, DoS (Denial-of-Service) attack, by flooding the SCADA master or RTU with valid protocol messages, will saturate the CPU computational power, memory or communication bandwidth, and will result in delay or inhibition of real-time data exchange. As a consequence, control center operators may fail to have a complete view of the electrical power grid system status, leading to incorrect decision making.

Common cyber security vulnerabilities is reported in [12]. More cyber security issues in power automation systems are reported in [13], [14], [15], [16], [17], [18], [19], [20]. Specifically, the requirements for QoS and security are discussed in [14], [15], [16], [18], [21], [22], [23], [24], [25], [26], [27]. Here we summarize the communication links, their typical applications, topologies, protocols and QoS requirements for power grid as listed in Table I. Some potential network attacks, their adverse impacts and corresponding security requirements are listed in Table I as well. Some security solutions for power grid are discussed in [13], [15], [16], [17], [18], [20], [21], [23], [24], [25], [26], [28], [29], [30], [31], [32].

E. *Current security solution*

A “gateway” security solution, as shown in Fig. 2, is currently widely used to protect power automation system from external cyber attacks. All incoming data packets to a substation are inspected by the security gateway. Control center has a similar security gateway to process incoming data packets. This solution assumes that the attacking access point is somewhere between two security gateways in the “Network” cloud. Imagining an automation engineer who enters the substation to upgrade HMI or RTU - when he connects his laptop to the substation network, he can bypass the security gateway and change the settings of protection relays, which he is not supposed to. This could be an internal attack or “friendly fire”. Another issue is that, if the substation has more than thousands of electronic devices, the “white list” (which states who is able to access which electronic devices) in the substation gateway could be very long. Hence, it would lead to unacceptable delay for some time-critical data packets.

F. *A general SCADA cyber attack process*

Due to the vulnerabilities aforementioned, power grid automation systems are under the risk of cyber attacks. This subsection outlines the typical attack methodology that may be used by a dedicated hostile entity wishing to cause more than a simple disruption of service or random havoc on a SCADA system in power grid automation system. It will illustrate the details of a cyber attack, describing the scenario in which a hacker gains unauthorized access to a SCADA system. Attacking a SCADA system in an intelligent and deliberate way is a difficult task. It requires a skilled hacker and many hours of research. To gain control of a power grid automation system, there are three necessary steps: access, discovery and control [12]. Additionally, one optional step employed by sophisticated intruders is to conceal their attacks by deleting or manipulating auditing log files which are intended to detect and report the intruders’ presence in the automation systems. In the following section, we discuss the three necessary steps to gain control of a power grid automation system in detail.

1) Access: The first step required by an attacker is to gain access to the SCADA system. If this is an internal threat, access should be assumed, though the level of access might be limited. The three most common methods for unauthorized access are: corporate network to SCADA network communications, external VPN access to the SCADA, and remote site communications.

The business owners of the SCADA systems almost always require data from the SCADA network for normal operations. These data sources can vary dramatically from one company to another, but the most common sources of information flow to and from the SCADA system is by some form of a database system. This includes large relational database systems such as Oracle or MSSQL, but can also include custom real-time databases or historical databases. Because data is crossing a network boundary between the SCADA and the corporate network, these communication paths may be exploited to gain unauthorized access.

Another common communication path between the SCADA network and the corporate network is the use of client systems. These can be single-user systems such as those used by engineering personnel but can also be multi-user systems such as Citrix or terminal services. This remote access is often granted to specific personnel within the corporate network to provide information required for running the business. If one of these client systems were to be compromised, an attacker

Communication	Potential Cyber Attacks	Adverse Impacts	Security Requirements
Intra-Substation	1. Sensor data missing 2. Sensor data misrepresented 3. Control command injected 4. Data delayed	1. Circuit breaker open at wrong times 2. System run exceeding limits 3. System outage 4. Personnel injuries or death 5. False alarms 6. EMS applications failure, such as state estimation, contingency analysis, shifting power transmission and distribution system from its optimal running point.	1. Data integrity 2. Data availability
Inter-field and Substation-field	1. Corrupt data from potential transducer or current transducer 2. Modify data from meters	1. Tripping the circuit breakers and leading to outage 2. Changing reporting and accounting information	1. Data integrity 2. Data availability
Control-Center-substation	1. Collected data, from substation to control center, becomes missing or misrepresented 2. Inject control command from control center 3. Delay data on this link by flooding SCADA master or slave	1. System run exceeding limits 2. System outage 3. Personnel injuries or death 4. False alarms 5. EMS applications failure, such as state estimation, contingency analysis, shifting power transmission and distribution system from its optimal running point.	1. Data integrity 2. Data availability 3. Non-repudiation
Intra-control-center	Modify data exchanged between different application servers, HMIs, etc.	1. System run exceeding limits 2. System outage 3. Personnel injuries or death 4. False alarms 5. EMS applications failure, such as state estimation, contingency analysis, shifting power transmission and distribution system from its optimal running point.	1. Data integrity 2. Data availability 3. Non-repudiation
Inter-control-center	1. Modify the exchanged data 2. Illegally access price and cost information	1. Failure to perform desirable transaction 2. Penalties due to transaction based on false cost or price information 3. Failure to fulfill contracts 4. Competitors gain competitive advantage	1. Data integrity 2. Data availability 3. Data confidentiality 4. Non-repudiation
Control-center to Corporate	Modify the exchanged data	1. Non-optimal planning 2. Non-optimal asset management	Data integrity
Control-center to Corporate	Modify the exchanged data	1. Non-optimal planning 2. Non-optimal asset management	1. Data integrity 2. Data availability 3. Non-repudiation
Control-center to Corporate	Modify the exchanged data	1. Non-optimal planning 2. Non-optimal asset management	1. Data integrity 2. Data availability 3. Data confidentiality 4. Non-repudiation

TABLE II
POTENTIAL NETWORK ATTACKS, THEIR IMPACTS AND SECURITY REQUIREMENTS FOR POWER GRID

may be provided with a simple pathway into the SCADA network.

Remote access using a VPN is another common external communication link into the SCADA network. VPN access is often used for vendor support, but is also commonly used by SCADA personnel who require access from home or from their offices. Problems arise from poor VPN configuration or from poor configurations on the client systems. An attacker might be able to gain access to the SCADA network if a client system can be compromised, or if the VPN server relies upon the VPN client to enforce access rights.

Remote site communications is another potential entry point for an attacker. Remote sites include back-up facilities, development or quality systems, or even substations. It is often observed these communication links are not protected by firewalls or VPN and rely upon the remote site being a trusted and secure network. It is possible for these communication links to be compromised, which provide a means for an attacker to gain access to a SCADA from a remote location without the need to hack their way through the corporate network. A valid example is the compromise of an FEP from a substation by impersonating a controller (PLC, RTU, etc.).

2) Discovery: Once access to the SCADA network is obtained, the next step is to understand the SCADA network by discovering the SCADA process. The complexity of SCADA systems is one of the best defenses against attack and forces the attacker to perform extremely time consuming tasks in order to understand the system well enough to intelligently attempt an attack or control.

Shortly after access to the SCADA has been accomplished, the attacker is likely to have only a single point-of-presence on the network. This is probably a single host somewhere on the SCADA network, perhaps even on the DMZ. Before any additional exploitation attempts are made, simple sources of information are first sought after. These sources include web servers, engineering workstations, Samba shares, and exported HMI screens (e.g. HTML screens shared to client systems) - information sources that were not necessarily available at the starting location of the attack. Oftentimes these information sources are available to any node on the SCADA network regardless of location or credentials. These basic information sources are often the most profitable and are usually discoverable without the need for exploitation or actions that might trip network defenses such as Intrusion Detection Systems.

The next best source of information comes from passive network discovery. This is a time consuming process as the attacker will have to wait for information to pass on the network where the point-of-presence is located. This information is not always useful as it greatly depends on the location of the compromised system. However it can often reveal a great wealth of data, including network credentials (FTP, Telnet, SMB, HTTP, etc.). All of this is done without writing a single packet onto the SCADA network.

If the point-of-presence is located on a network with core SCADA components (HMI, FEP, controllers), the attacker might be able to passively monitor SCADA-specific communications. Although most SCADA vendors use proprietary protocols for a majority of their communications, these protocols can usually be distinguished between the various SCADA system vendors. The attacker may not understand or be able to decode the SCADA protocol at this time, but will use the uniqueness of that protocol in an effort to identify the specific SCADA vendor in use.

The last method of discovery employed is active network scanning. Active network scanning generally requires root level access on the compromised system so that custom packet crafting is possible. This is certainly the noisiest of all discovery methods since the attacker is now required to use scanning techniques that are often easily caught by network defense tools. Advanced level attackers will have very quiet scanners, but regardless of speed, packets are being sent on the SCADA network and might trigger alerts. However this discovery method is most rewarding as it will provide the attacker with a picture of what systems and devices are reachable from the point-of-presence.

Although discovering systems and the specifics regarding the type of SCADA employed is a difficult task, the most difficult part of the discovery process lies in understanding the SCADA process. The discovery methods listed above will give the attacker a good picture of what the SCADA network is but does not necessarily help the attacker understand what it controls or how it works. The end goal is to take these many pieces of information and correlate them together in an attempt to understand how the SCADA is implemented. An example of this process can be illustrated with the discovery of some device on the network named ”Valve 4A” - a tag name sent in plain-text on the network. The goal is to find out what Valve 4A controls and what impact it might have on the system.

Understanding the SCADA process is an extremely difficult task and is also very time-consuming. This is the best opportunity for the network defenses to find malicious activity on the SCADA network. The attacker is more than likely going to make a mistake during this time and perform a task that could be easily recognized as an anomaly on the network. Because perimeter defenses might only be able to do so much to prevent unauthorized access to the SCADA, internal defenses need to be enhanced enough to prevent malicious activity that occurs during discovery. This case study will assume that the attacker is interested in full discovery and understanding of the SCADA system so that intelligent control and disruption of the process can be accomplished. This raises the bar for the defenders of SCADA systems to be ready to deal with a highly skilled attacker or even an insider threat. These are the most difficult threats to defend against, yet at the same time are the ones that have the potential for the highest level of impact.

3) Control: Once the SCADA process is understood by the attacker, there are several methods that might be used in an attempt to control the system. These various methods will provide different levels of control, though only a few of these methods may be available depending upon the success of the discovery process.

One of the highest value targets on a SCADA is the FEP. Though the SCADA system might be so large that it utilizes several FEP systems, the FEP remains the best target for attack and control due to its centralized control capabilities. The FEP is responsible for communicating all commands from the SCADA out to the various process controllers. These controllers might all communicate using different protocols, but the FEP understands how to communicate with each one. If an attacker can access the FEP, it is no longer a requirement to understand the numerous protocols in use by the controllers. Instead the attacker only needs to understand the protocol used to send commands to the FEP. Often times, the FEP does not even require authentication or validation of the commands it receives, and logging of commands is rarely performed by the FEP. Attacking the FEP is a protocol level attack since the attacker will have to understand and decode the specific protocol used by the FEP. This is often a proprietary protocol developed by the SCADA vendor.

Another high value target on the SCADA system is the HMI. This system is one of the easiest to understand since it is designed to provide the information required to run the SCADA system. If access to the HMI is gained by the attacker, the attacker might be able to use the same screens used by the operator and arbitrarily control the system. The scope of the attack may be limited, however, since the functionality provided to the attacker is usually the same level of functionality that a normal operator is allowed. Hence, the attacker may not be able to operate the system to a failure point.

Attacking the HMI is a component level attack since unauthorized access to the HMI system is required. This attack is generally one of the easiest since standard (not SCADA specific) exploitation methods can be used to gain access, and abundant information is provided to the attacker by the HMI.

The other benefit is that actions taken from the HMI will appear as if the operator of the HMI requested the actions. The EWS (Engineering Workstation) is also another high value target, comparable to the type of attack conducted against the HMI. The EWS is generally used by the SCADA engineers to perform development on the SCADA system and provide the software and screens to the HMI. The main difference between the EWS and the HMI arises from the EWS's ability to override the limitations normally enforced on the HMI. If an attacker gains control of the EWS, there may be arbitrary commands available beyond those normally accessible to an operator (e.g. engineering override). Spoofing is another attack method that involves the HMI or the EWS. This is a method where the attacker understands the protocol used by the HMI or the EWS well enough to falsify information going to the HMI so that the operator display is changed and no longer reflects reality. This can be useful for two reasons: hiding activity taking place elsewhere on the SCADA from the operator, or creating a display for the operator that leads the operator to take action and perform commands on the SCADA system.

Spoofing network messages on the SCADA system is a complex task. Injecting commands into an existing TCP or UDP session is non-trivial. The attacker will need an extensive background in network communication methods and have extensively decoded the protocols in use. This is a network based attack as it will usually require some form of a MITM (Man-In-The-Middle) attack such as ARP (Address Resolution Protocol) poisoning, ICMP (Internet Control Message Protocol) redirection. It is also a protocol level attack because the attacker will be manipulating SCADA messages while they are in transit.

Database systems are another potential target for the attacker. These systems can be relational databases, real-time databases, batch processing systems, or historical databases. These systems are utilized in many different ways depending on the vendor of the SCADA system, but in some cases, manipulation of these data sources can cause the SCADA system to automatically change state (i.e. automation in the SCADA watches the data and takes action accordingly). This is one of the more difficult methods of exploitation and may not always yield control of the SCADA to the attacker, but manipulation of data alone is a major attack vector and may have critical impact.

Attacking data systems can be considered a component level of attack if the system is a common system (e.g. Oracle, MSSQL), but might also be a protocol level attack if custom systems are used and the attacker is attempting to inject data and commands into the network. Another difficult target on the SCADA network is the application server. The application server usually hosts a number of applications used by the SCADA system. These applications rarely use the same protocol, utilizing, instead, proprietary protocols developed by the SCADA vendor. The challenge for the attacker is to determine what applications on the server might provide control of parts of the SCADA system. Once this is discovered, the attacker might be able to communicate with the application server in such a way as to cause the application server to issue commands to the FEP. This method of attack is more common if communicating directly with the FEP is not possible.

Attacking the application server is a protocol level attack. The various messages sent to the application server need to be understood so that the attacker can inject arbitrary commands onto the network. Although this is a difficult target, attacking the application server usually provides access to commands that are normally unavailable to an operator, and these commands are usually logged as being issued by the HMI or the EWS.

One of the lowest priority attack methods, though involving what may be the easiest target in a SCADA network, is a direct attack on a controller. This can be performed by an attacker talking directly to the controller in a similar fashion as the FEP, but can also be performed by using remote access methods often used on the controllers themselves.

Direct commands will require that the attacker understand the specific protocol used by the controller, along with the logic embedded in the controller. These commands will look similar to the commands generated by the FEP.

Many controllers also provide a means for remote access. This can include web services, dial-up modems, and telnet. Authentication is rarely required. Not only does remote access allow the attacker to issue commands to the controller, it is also likely to provide the attacker with a means for harvesting programming logic or firmware information.

Directly attacking a controller is a component level attack when unauthorized remote access methods are allowed, but can also be considered a protocol level attack when commands are generated by the attacker and sent to the controller. This is a low priority target, however, since this only provides a small subset of system control to the attacker. The only SCADA control available from this target concerns the control devices that are connected to the target controller.

DoS attacks by saturating the targeted device memory, CPU computational power or bandwidth can degrade the system performance, making the system to be blind and unable to response to change in the system.

III. Major challenges and strategies of security solutions for the smart grid

To address security issues of the smart grid, it is necessary to identify those unique challenges. There are four major challenges when developing new network security solutions for power grid automation systems:

1) Many automation components (such as RTU) use proprietary operating systems, which are designed for control functionality and performances, but not security.
2) Automation systems use heterogeneous network technologies, such as ProfiBus, ModBus, ModBus Plus, ICCP, DNP. Most technologies and protocols were designed for connectivity, without consideration of cyber security.
3) Most automation systems are combinations of new and legacy components with many systems expected to run up to 20 or 30 years, perhaps even longer. Many legacy devices (such as RTU) were tailored to control functionality and may not have reserved computational power or

memory space to perform security functionalities. Thus, one desirable feature of the newly developed security solutions is the ability to be integrated to the existing, legacy systems in a non-intrusive fashion, without compromising their control performance.

4) Since power grid is experiencing a profound change and moving to smart grid, there are new applications (such as using Phasor Measuring Units and smart meters) and corresponding new requirements for data communication in terms of bandwidth, delay and new communication protocols. Therefore, one challenge is how to avoid early obsolescence when developing a new security solution.

Standard security services must be supported by the new solution, which should be able to integrate security management (such as authorization and authentication), security operations (such as logging and auditing), and other security technologies (such as access control and intrusion detection) in a seamless fashion. The strategies to design a security solution for smart grid are as follows:

- Scalability is the system's ability to increase or decrease its capacity to protect larger or smaller size of power grid automation systems (e.g. more or less electronic devices and users) in a graceful manner. It also refers to the ability to increase or decrease size or capability in cost-effective increments with minimal impact on the unit cost of business and the procurement of additional functionalities. During design, scalability must be considered in order to maintain the same level of growth experienced by the power grid. The security performance of the solution must remain unabated as the power infrastructure increases in load and system volume.
- Extensibility - which refers to a system designed to include hooks and mechanisms for expanding and enhancing the system without having to make major changes to the system infrastructure. Since newly developed cyber attack methods can always be found, the security framework needs to ensure its extensibility. It also must be considered such that the proposed solution is able to handle any future state of the power grid, including new technologies and communication protocols.
- Interoperability - a property referring to the ability of diverse systems to work together. Since power grid automation systems use various technologies with respect to hardware, operating systems, and communications protocols, the security framework and components must be able to work together regardless of the technology on which they are executed or developed.
- Non-intrusiveness - which refers to the system's ability to be subject to security activities without compromising its control functionalities and performance. This requirement addresses the challenge that the existing, legacy systems may not have the reserved computational power or memory space to perform security functionalities. It must be considered to integrate the new security solution into the existing, legacy systems in a non-intrusive fashion without compromising their control performance, reliability, stability, and availability.
- Flexibility - which is the ability to adapt to various needs in the development and at runtime. It includes the ability to extend a system with e.g. new features/ components without the loss of previous functionality or qualities that have been negotiated as well as to reduce it respectively. Since, unlike the relatively static power grid automation system, the future smart grid can be highly dynamic logically due to more participants get involved, the flexibility of extensions/reductions to the system can be made either through the addition/removal of new functionality or through modification of existing functionality, and the addition/removal of new entities in the power grid automation system can be made readily.

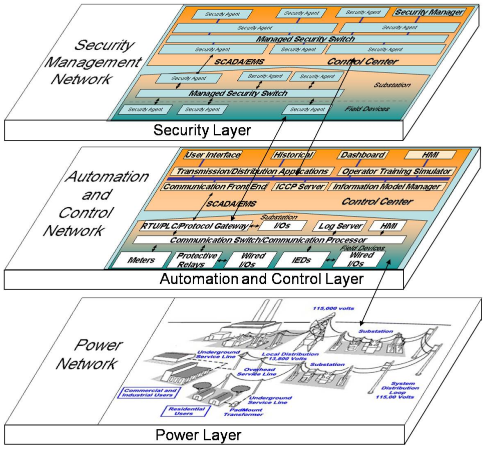


Fig. 3. Proposed 3-layer architecture

IV. The Integrated Security System

To meet the challenges discussed in the previous section, we propose an integrated security framework with 3 layers (power, automation and control, and security), also called common security platform, as shown in Fig. 3. The automation and control system layer monitors and controls power grid processes, while the security layer provides security features. Since the security layer provides clear demarcation of responsibilities, control functionalities and security functionalities can be decoupled during design stage. Data related to security management flows on this layer. Another important idea is that the proposed security solution replaces the "gateway" security solution by a "security service proxy" solution, which is shown in Fig. 4. There are three key security subsystems: Security Agent, Security Switch and Security Manager. Security Agents and Security Switches, which are security enforcement devices, run as security service proxies; and Security Manager runs as a security management device either in the control center or in a substation. The proposed integrated security framework operates on three hierarchical levels, as shown in Fig. 5. Each of these levels is protected by a component of our security system listed below:

- Device level in which electronic devices, such as RTU, IED, are protected by the Security Agent

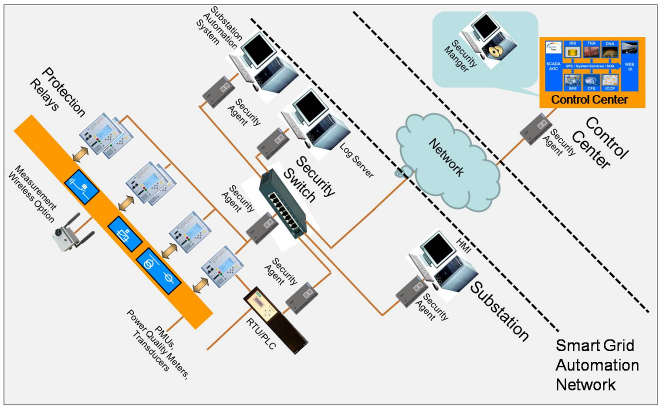


Fig. 4. Security Service Proxy Solution

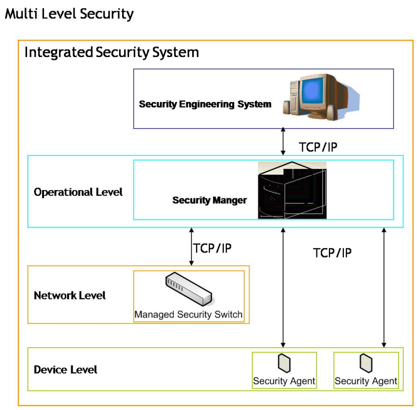


Fig. 5. Multi-layered Integrated Security Framework

- Network level in which communication bandwidth is protected and delay is guaranteed by the Managed Security Switch
- Operation level, in which security policies are orchestrated and managed by the Security Manager

In addition, a Security Engineering System designed to manage, administrate, monitor and troubleshoot the integrated security system makes the system more user-friendly. The security manager has multiple secure TCP/IP connections to each individual security agent and managed security switch. The security manager will act as PDP (Policy Decision Point), which will create the actual security policy used. Once the policies are created, the PEPs (Policy Execution Points) - managed security switch and security agents, will execute those policies.

A. Security Agent

The security agents bring security to the edges of the system by providing protection at the device level - it applies to both wired and wireless devices. These agents are firmware or software agents depending on the layer of the control hierarchy. At the field device layer (e.g., IEDs), these agents will be less intelligent - containing simple rules and decision making capabilities - and whose primary responsibilities consist of event logging and reporting. At the substation level (e.g., RTUs), these software agents will be more intelligent with more complex rules for identification and detection of intrusive events and activities within the controllers. In particular, a security agent will be commissioned to accomplish the following functions:

- To translate between different protocols.
- To acquire and run the latest vulnerability patches from its security manager.
- To collect data traffic patterns, system log data and report to the security manager.
- To analyze traffic and access patterns with varying complexity depending on the hierarchical layer.
- To run host-based intrusion detection.
- To detect and send alarm messages to the security manager and designated devices, such as HMI.
- To acquire access control policies from the security manager and enforce them.
- To encrypt and decrypt exchanged data (end-to-end security).

One important function of the security agent is access control. In the IT world, firewalls perform this function, passing all data packets except those of applications and addresses that are explicitly stated in the ACL (Access Control List). On the contrary, security agents only pass data packets whose source address, destination address, port numbers, or protocol number, matches the ones in the ACL, and blocks the rest.

B. Managed Security Switch

Managed switches are used across the automation network to protect bandwidth and prioritize data packets. These switches, working as network devices, will connect controllers, RTUs, HMIs, and servers in the substation and control center. Managed security switches possess the following functionalities:

- To separate external and internal networks, trusted and non-trusted domains.
- To run as a DHCP (Dynamic Host Configuration Protocol) server.
- To run NAT/NPAT (Network Address Translation and Network Port Address Translation) and to hide the internal networks.
- To acquire bandwidth allocation patterns and data prioritization patterns from the security manager.
- To separate data according to prioritization patterns, including operation data, log data, trace data and engineering data.
- To ensure QoS for important data flow, such as operation data, guaranteeing its bandwidth, delay, etc.
- To manage multiple VLANs (Virtual Local Area Network).
- To run simple network-based intrusion detection

C. Security Manager

Security managers, with a GUI (Graphical User Interface), reside in the automation network and directly or indirectly connect to the managed switches across the automation networks. They can be protected by existing IT security solutions and will be able to connect to a vendor's server and managed switches via VPN. The security manager will possess the following functionalities:

- To collect security agent information.
- To acquire vulnerability patches from a vendor's server and download them to the corresponding agents.
- To manage keys for VPN.
- To work as an AAA (Authentication, Authorization and Accounting) server, validating user identifications and passwords, authorizing user access rights (monitor, modify data), and recoding user changes to controllers.
- To collect data traffic pattern and performance matrix from agents.
- To collect alarms and events.
- To generate access control policies based on collected data (using data mining techniques) and download them to agents.
- To run complex intrusion detection algorithms at control network levels.
- To generate bandwidth allocation patterns and data prioritization patterns (possibly through data mining techniques) and download them to managed switches.

The security manager sits in the center of the power grid automation network, managing what and how security functions are performed by security agents and QoS functions are performed by the managed security switch. For instance, access control policies for each security agent are not static. They should be modified accordingly by the security manager if the automation system runs in different modes - regular operation, maintenance, or troubleshooting. Bandwidth allocation and data prioritization policies in the switch can be managed by the security manager as well.

D. Security Engineering System

Security engineering system is used to create, configure, manage, monitor and troubleshoot the integrated security system project. The project navigator is the common view for all tools of the engineering system. It offers a common list of all controls and data, and generates the runtime configuration data. The engineering system acts as a centralized data and program administration. In this project, the security engineering system will not be developed. Some functions of the security engineering system will be implemented in the security manager.

E. Intrusion Detection

Traditionally, automation systems are subject to more constrained behavior as compared to enterprise networks. Automation networks possess:

- Relatively static topology
- Regular communication patterns
- Limited number of protocols
- Simple communications protocols

Therefore, anomaly-based Intrusion Detection System (IDS) techniques are often sufficient for detection of intrusions, whereas signature-based IDS techniques are widely used in IT world [33]. Anomaly-based IDS techniques sound alarms when observed behavior is outside of a pre-defined specification, whereas signature-based IDS techniques send alarms when observed behavior matches known malicious threats. An anomaly-based IDS [30] has a high potential for generalization and leverage against new attacks, but at the same time is subject to more false alarms than the other. With power grid infrastructures, this may change due to remote engineering and troubleshooting though IP addressable devices. Under such circumstances, automation networks will be subject to more random traffic patterns and higher than usual levels of disturbances. To protect against this extra traffic of random patterns while fully utilizing the inherent determinism of the control networks, we propose combining anomaly-based techniques with model-based probabilistic techniques and/or techniques that use empirical models and signatures of normal behavior and usage. As discussed earlier, intrusion detection will be performed at three levels:

- Security agent performs intrusion detection based on the CPU and memory utilization of the protected device (such as RTU/PLC), scan time, protocol pattern, communication pattern (such as round trip time, bandwidth usage), etc.
- Managed security switch performs intrusion detection function based on the delay of data packet, the allocated bandwidth profile, protocol pattern, etc.
- Security manager performs intrusion detection at the highest level, by monitoring power grid system and its automation system state. For example, with a known power loss range, the input power and output power of the power grid system can be monitored. The security manager sounds an alarm when these numbers do not match, in which case mis-represented data could be received.

Note that the ISS also exposes raw packet data from a dedicated port on the security switch to a third-party IDS product. This feature enables the third-party IDS to integrate into the proposed ISS without accessing to all encryption keys.

F. Managed Security Service

Automation system vendors are responsible for providing patches on their public servers for newly found vulnerabilities on their systems, such as for PLCs or HMIs. The security manager automatically obtains new patches via a public network according to the firmware version and types of devices, and downloads these patches to security agents accordingly. System vendors and system integrators may also provide co-managed security service to power grid system operators by helping generate access control policies for security agents, which protect system vendors' systems.

G. Implementations of Security Agents

It would be very costly if one stand-alone security agent protects each electronic device. To make it more cost effective, security agents are implemented in four different ways, as shown in Fig. 6:

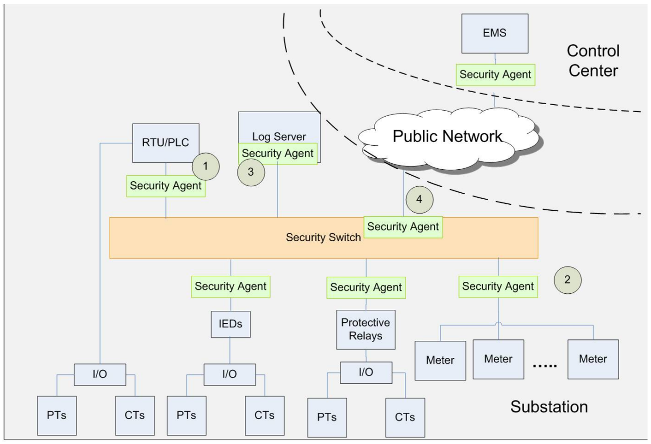


Fig. 6. Different Implementations of security agents

- An individual two-port module - the internal is connected to the protected device (such as RTU and HMI), the external port connected to a network device (such as switch, router).
- An individual two-port module - the internal is connected to a group of electronic devices (such as meters or protection relays), the external port connected to a network device (such as switch, router).
- Agent resides in a managed security switch - a virtual security agent runs on an internal port connected to the protected device.
- Agent resides in all newly developed devices (such as log server, PLC, RTU) - runs independently of control firmware.

Each implementation has its advantages and disadvantages. Some legacy electronic devices (such as protection relays, RTUs) with embedded controller were tailored for the specific control tasks, and may lack computational power or memory to perform security functions, such as encryption/decryption. To address this issue, the first three implementations can integrate new security solution into the legacy systems in a non-intrusive fashion, i.e., there is no need to modify the legacy systems. In the last implementation, security agent functions can be ported to newly developed log servers, HMIs and RTUs with sufficient computational power and memory space.

H. Prototypes

A security system prototype and demo of the proposed framework, as shown in Fig. 7, was developed based on Windows XP. The prototype includes a stand-alone security agent, a security agent application which can run on a protected device, a managed security switch and a security manager. However, only some functionality described in the previous section was implemented, due to time limit, to prove the concept.

I. On-site System Test

The prototype system was installed in a test configuration at the INL and tested to validate the proof-of-concept features, as follows:

Fig. 7. The ISS prototype and demo system

- Create a typical, simplified power grid automation system with EMS, RTU and two protection relays. They are all connected via a hub. Record communication performance in terms of round trip delay, used bandwidth and time to build up a 3-way handshake TCP connection. Then find all vulnerability by using a set of public available penetration test tools, such as port scanning, password cracking and data flooding; record all vulnerability and adverse impacts on control performance;
- Place the integrated security system in SCADA system - replace the regular hub with a managed security switch, place two stand-alone security agents next to EMS and RTU, respectively, and connect a security manager to the managed security switch; record communication performance such as round trip delay, used bandwidth and time to build up a TCP connection; then do the same vulnerability test by using the same set of penetration test tools; record all vulnerability and adverse impacts on control performance;
- Compare testing results in the above two scenarios.

The results of the proof-of-concept system test results are:

- the security components do not have significant adverse impact on SCADA communication - the maximum round trip time by using the ISS is 110, as shown in Fig. 9, where it is 105 ms, as shown in Fig. **??**, by using the regular hub; the maximum time to build a TCP connection is 135 ms by using the ISS where it is 130 ms by using the regular hub; the used bandwidth by using the ISS needs at most 10% more (due to security management activities) than using the regular hub, , as shown in Figs. 10 and 11;
- some vulnerabilities are successfully mitigated, such as clear text communication, port scanning, and unused open ports; some vulnerabilities are partially mitigated, such as vulnerability to flooding-based DoS attacks;
- the intrusion detection mechanism is able to report most

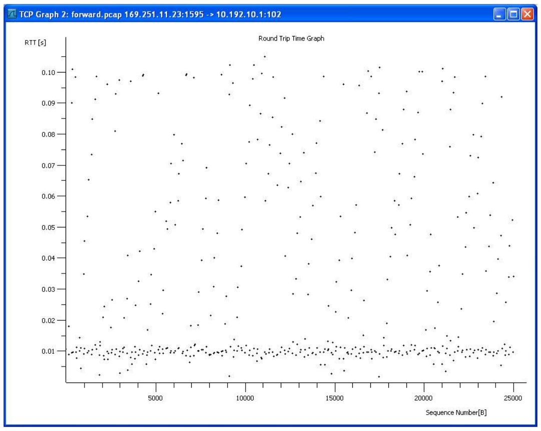


Fig. 8. Round Trip Time of Clear Text Communication without the ISS

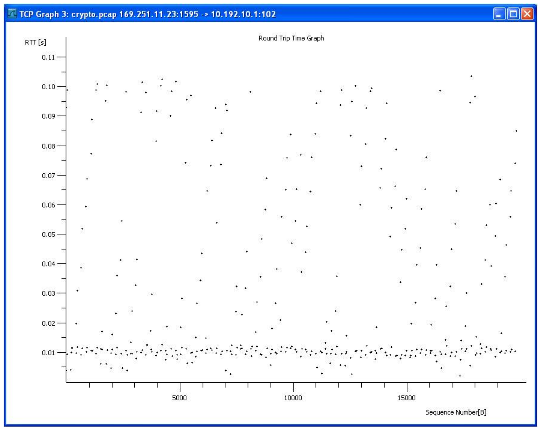


Fig. 9. Round Trip Time of Cyphered Text Communication with the ISS

cyber attacks, such as access control violation, flooding-based DoS and brute force key cracking.

The proof-of-concept system test showed that the developed Integrated Security System is able to report most cyber attacks and mitigate some cyber attacks without significant adverse impact on control system communication.

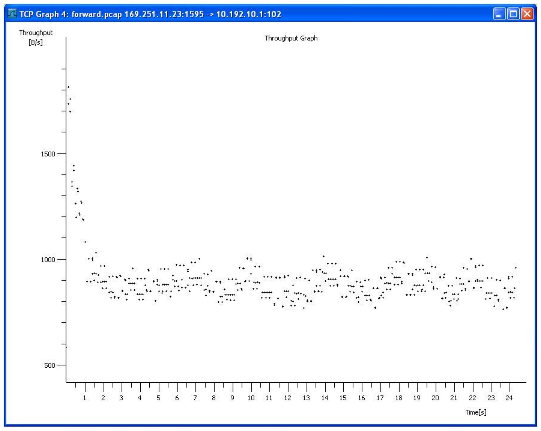


Fig. 10. Bandwidth Used for Clear Text Communication without the ISS

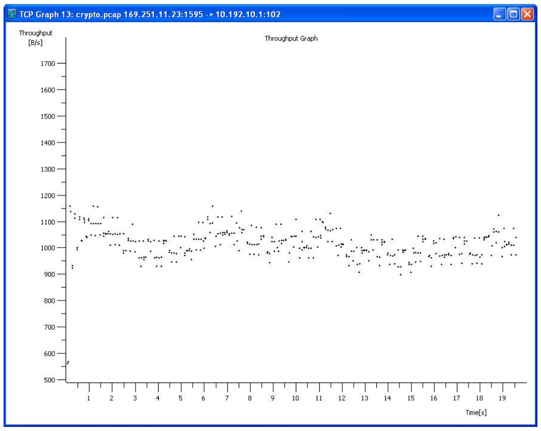


Fig. 11. Bandwidth Used for Cyphered Text Communication with the ISS

V. Conclusion and Future Work

We propose a conceptual layered framework for protecting power grid automation systems against cyber attacks, which may come from either the Internet or internal networked sources. The proposed framework possesses the desirable performance in terms of scalability, modularity and manageability. It can be integrated into existing, legacy automation systems in a non-intrusive fashion. The prototype of the security system has been tested at the Idaho National Lab - it is proved that the developed security system is able to address and mitigate some common vulnerability of power grid automation systems.

The Integrated Security System discussed in Section IV addresses cyber attacks at layer 2, 3 and 4 of the seven-layer OSI model. However, Layer 7, application layer, communication is the weakest link in terms of security since it supports many protocols, and most of them were originally not designed with consideration of security. Thus those protocols have vulnerabilities and provide many access points for attackers. Therefore, application layer attacks are hard to protect against. According to a report [34], over 80% of all existing system vulnerabilities are based in the application layer. More than half (58%) of the application software contain vulnerabilities that could be used to launch large-scale cyber attacks similar to those suffered by Google earlier this year, according to a report ”The State of Software Security” [35]. It is reported that close to 90% of attacks are aimed at the application layer [36]. Although application layer security issues have been addressed in the IT world, especially for web services [37] and database applications [38], the unique challenges of smart grid applications have not been addressed yet. Therefore, layer 7, the application layer, security of smart grid should be addressed next.

Acknowledgment

The authors would like to express their gratitude to Dr. Diane Hooie and James Briones of the Department of Energy who provided project management, with support from the DoE contract manager Jeffrey Kooser and Tom Flowers. The authors gratefully acknowledge the contributions of Salman Siddiqui, Chao Zhang, Kun Ji, Hongming Jin, Livio Dalloro, Natasha Kalenchits and Prithvi Raju for the prototyping development, and Jason Larsen and May Robin for the system test at Idaho National Lab.

References

[1] U. D. of Energy, U. D. of Homeland Security, and E. Incorporate, “Roadmap to secure control systems in the energy sector,” U.S. Department of Energy, U.S. Department of Homeland Security, Energetics Incorporate, Tech. Rep., January 2006.

[2] U. D. of Energy, “Smart grid system report,” U.S. Department of Energy, Tech. Rep., July 2009.

[3] ——, “Smart grid system report - annex a and b,” U.S. Department of Energy, Tech. Rep., July 2009.

[4] U. D. Energy, “”grid 2030” - a national vision for electricity’s second 100 years,” U.S. Department Energy, Tech. Rep., July 2003.

[5] S. Gorman, “Electricity grid in u.s. penetrated by spies,” *The Wall Street Journal*, p. A1, April 2009.

[6] J.-W. Wang and L.-L. Rong, “Cascade-based attack vulnerability on the us power grid,” *Safety Science*, vol. 47, no. 10, pp. 1332–1336, December 2009.

[7] U. D. of Energy, “The smart grid: An introduction,” U.S. Department of Energy, Tech. Rep., 2008.

[8] H. Farhangi, “The path of the smart grid,” *IEEE Power and Energy Magazine*, vol. 8, no. 1, pp. 18–28, February 2010.

[9] S. Massoud Amin and B. F. Wollenberg, “Toward a smart grid: power delivery for the 21st century,” *IEEE Power and Energy Magazine*, vol. 3, no. 5, pp. 34–41, October 2005.

[10] E. Santacana, G. Rackliffe, L. Tang, and X. Feng, “Getting smart,” *IEEE Power and Energy Magazine*, vol. 8, no. 2, pp. 41–48, March 2010.

[11] D. Wei, Y. Lu, and M. Jafari, “On protecting industrial automation and control systems against electronic attacks,” in *IEEE International Conference on Automation Science and Engineering 2007*. IEEE, September 2007, pp. 176–181.

[12] I. N. Laboratory, “Common cyber security vulnerabilities observed in control system assessments by the inl nstb program,” Idaho National Laboratory, Tech. Rep., November 2008.

[13] P. McDaniel and S. McLaughlin, “Security and privacy challenges in the smart grid,” *IEEE Security & Privacy*, vol. 7, no. 3, pp. 75–77, June 2009.

[14] C. H. Hauser, D. E. Bakken, and A. Bose, “A failure to communicate: next generation communication requirements, technologies, and architecture for the electric power grid,” *IEEE Power and Energy Magazine*, vol. 3, no. 2, pp. 47–55, March 2005.

[15] M. Brundle and M. Naedele, “Security for process control systems: An overview,” *IEEE Security & Privacy*, vol. 6, no. 6, pp. 24–29, December 2008.

[16] D. Dzung, M. Naedele, T. P. Von Hoff, and M. Crevatin, “Security for industrial communication systems,” *Proceedings of the IEEE*, vol. 93, no. 6, pp. 1152–1177, February 2005.

[17] A. Miller, “Trends in process control systems security,” *IEEE Security & Privacy*, vol. 3, no. 5, pp. 57–60, October 2005.

[18] U. D. of Homeland Security, “Cyber security procurement language for control systems,” U.S. Department of Homeland Security, Tech. Rep., August 2008.

[19] I. C. I. P. Center, “Study of security attributes of smart grid systems current cyber security issues,” Idaho National Laboratory, Tech. Rep., April 2009.

[20] R. M. Gardner and G. Consortium, “A survey of ict vulnerabilities of power systems and relevant defense methodologies,” in *Proceedings of IEEE Power Engineering Society General Meeting, 2007*. IEEE, June 2007, pp. 1–8.

[21] N. I. of Standards and Technology, “Nist framework and roadmap for smart grid interoperability standards, release 1.0,” National Institute of Standards and Technology, Tech. Rep., January 2010.

[22] U. Amisecasap, “Ami system security requirements,” UCAIUG: AMISE-CASAP, Tech. Rep., December 2008.

[23] W. Allen, D. W. Fletcher, and K. J. Fellhoelter, “Securing critical information and communication infrastructures through electric power grid independence,” in *Proceedings of The 25th International Telecommunications Energy Conference 2003*. IEEE, October 2003, pp. 170–177.

[24] A. Sologar and J. Moll, “Developing a comprehensive substation cyber security and data management solution,” in *Proceedings of The 2006 IEEE Power Engineering Society General Meeting*. IEEE, October 2006, pp. 6+.

[25] A. M. T. Oo, A. Kalam, and A. Zayegh, “Effective power system communication requirements for deregulated power industry,” in *Proceedings of The 2004 IEEE Asia-Pacific Conference on Circuits and Systems*, vol. 2. IEEE, December 2004, pp. 653–656.

[26] K. Tomsovic, D. E. Bakken, V. Venkatasubramanian, and A. Bose, “Designing the next generation of real-time control, communication, and computations for large power systems,” *IEEE Proceedings*, vol. 93, no. 5, pp. 965–979, May 2005.

[27] G. N. Ericsson, “On requirements specifications for a power system communications system,” *IEEE Transactions on Power Delivery*, vol. 20, no. 2, pp. 1357–1362, April 2005.

[28] R. J. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd ed. Wiley, April 2008.

[29] F. Sheldon, T. Potok, A. Loebl, A. Krings, and P. Oman, “Managing secure survivable critical infrastructures to avoid vulnerabilities,” in *Eighth IEEE International Symposium on High Assurance Systems Engineering, 2004. Proceedings.* IEEE, 2004, pp. 293–296.

[30] *Defending Distributed Systems Against Malicious Intrusions and Network Anomalies*, 2005.

[31] W. Tolone, G.-J. Ahn, T. Pai, and S.-P. Hong, “Access control in collaborative systems,” *ACM Comput. Surv.*, vol. 37, no. 1, pp. 29–41, March 2005.

[32] M. Amin, “Energy infrastructure defense systems,” *IEEE Proceedings*, vol. 93, no. 5, pp. 861–875, May 2005.

[33] S. Axelsson, “Research in intrusion-detection systems: A survey,” Department of Computer Engineering, Chalmers University of Technology, Goteborg, Sweden, Tech. Rep. 98–17, dec # 1998.

[34] I. Cenzic, “Web application security trends report q1-q2, 2009,” Cenzic, Inc., 2009.

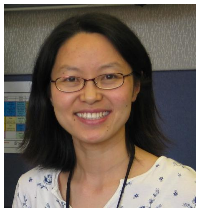
[35] Veracode, “The state of software security,” Veracode, Inc., Tech. Rep., March 2010.

[36] L. Briggs, “Application security comes under attack,” *Application Development trends*, January 2006.

[37] C. Gutiérrez, E. Fernández-Medina, and M. Piattini, “A survey of web services security,” in *Computational Science and Its Applications ICCSA 2004*, 2004, pp. 968–977.

[38] E. Bertino and R. Sandhu, “Database security - concepts, approaches, and challenges,” *IEEE Transactions on Dependable and Secure Computing*, vol. 2, no. 1, pp. 2–19, January 2005.

Dr. Dong Wei is a research scientist at Corporate Research, Siemens Corporation. He has worked at Siemens for 10 years. He received his Bachelor degree in Electrical Engineering from Tsinghua University in Beijing, China. He received his master and Ph.D degrees from New Jersey Institute of Technology, both in Electrical Engineering. He has worked on factory automation system, PLC, motion control, Human-Machine Interface, drive system, and industrial communication networks for more than 10 years. Dr. Wei has 20 publications, including book chapters, journal papers. He is also an active reviewer of IEEE Transactions on Smart Grid, IEEE Transactions on Automation Science and Engineering, IEEE Transactions on Industrial Informatics, IEEE Transactions on System, Man, and Cybernetics, Computer in Industry, Journal of the Network and Systems Management, etc.



Dr. Yan Lu is Research Scientist at the Automation and control (AC) department of Siemens Corporate Research (SCR). Dr Yan Lu's main field of work is automation system research and development, including Industrial automation, building automation and energy automation. Her research interest covers distributed agent-based control, fault detection and diagnosis, robust control systems and control system security. Dr. Lu has led and successfully delivered several government funded projects in the areas of robust and survivable control systems, including Robust Tape Control project funded by NIST ATP Program, Survivable Ship Control project funded by ONR and DOE funded Securing Power Grid Security from Cyber Attacks project. She is also the PI of two newly funded ARRA projects from DOE, on building energy efficiency and demand response respectively. Dr. Lu obtained BS and MS from Tsinghua University and her Ph. D from Carnegie Mellon University, all majored in Electrical Engineering with specialty in Control System. Before joining Siemens Corporate Research in 2004, Dr. Lu worked for Seagate Research Center for two years focus on hard drive servo control.

Dr. Mohsen Jafari is a full professor of Industrial and Systems Engineering at Rutgers University. He has been with Rutgers U. since 1987. He received his Ph.D. in Systems Engineering and Operation Research and M.S. in Computer Science from Syracuse University. His research areas of interest are in systems optimization and control, intelligent distributed systems, simulations, and data modeling in transportation, energy, manufacturing and health care. He has directed or co-directed funding from various government agencies such as the NSF, DOE, ONR, DoD/DLA, FHWA, US/NJ Department of Transportation, NJ Dept. of Health and Senior Services. He has also been consultant to several fortune 500 companies as well as local and state government agencies. He has published over seventy refereed articles and has made many invited and contributed presentations nationally and internationally. He has been thesis advisor to seventeen Ph.D. students, nine MS students and six post doctoral fellows.

Paul M. Skare is the Director of Cyber Security for Siemens Energy Inc., Transmission and Distribution, Energy Automation (EA). Paul is responsible for Cyber Security services and consulting, and provides requirements to product management on Cyber Security on a global basis. Paul is the Convenor of the International Electrotechnical Commission (IEC) Technical Committee (TC) 57 (Power systems management and associated information exchange) Working Group (WG) 19 responsible for the overall architecture of IEC TC 57 standards and the harmonization of all the TC 57 standards in the long term. Paul is a technical expert for WG 15 for Cyber Security (IEC 62351), and WG 13 for the Common Information Model (IEC 61970/IEC 61968-CIM). Paul was a recipient of the IEC 1906 award in 2007. Paul is a member of the NIST Cyber Security Coordination Task Group, and smart grid groups IEEE P2030 and SGIP. Paul has also been in the DOE 'Roadmap to Secure Control Systems in the Energy Sector' group, the Siemens EA liaison to Idaho National Laboratory (INL) and the National SCADA Testbed (NSTB) for cyber security issues, the DHS contact via the CSSP at INL, a sponsor of the University of Illinois's Cyber Trust program funded by NSF, the NERC Control Systems Security Working Group, the NIST Process Control Security Requirements Forum, the DHS ICSJWG (formerly Process Control Systems Forum), and the IEEE P1686 and P1689 groups on cyber security. Paul has twice testified to the U.S. Congress about cyber security and control systems. Paul has 30 years experience in the Power Industry. Previously at Siemens, Paul has been the Product Manager of SCADA and Substation Automation Products, SCADA and Communications R&D Manager, a Development Project Manager, a Proposal Manager, a Sales Support Engineer, and an Electrical Engineer. Prior to working for Siemens, Paul worked for Northern States Power Company (Now Excel Energy).

Kenneth Rohde is a member of the Cyber Security Research and Development Department at the Idaho National Laboratory in Idaho Falls, Idaho. Mr. Rohde is part of the SCADA and Control Systems security research team primarily focused on identifying and mitigating vulnerabilities in computer systems responsible for the Nation's critical infrastructure. He is also and active member of the INL Cyber Security Red Team. He has served as Adjunct Faculty with the University of Idaho Computer Science Department and also been a guest lecturer at the Idaho State University. Mr. Rohde received his Bachelor's Degree in Computer Science from the University of New Mexico in 2000.