Security Challenges of Reconfigurable Devices in the Power Grid *

Suvda Myagmar Roy Campbell Marianne Winslett

Department of Computer Science
University of Illinois at Urbana-Champaign
{myagmar, rhc, winslett}@uiuc.edu

Abstract

SCADA systems utilized in the electric power grid infrastructure typically cover large geographic areas with hundreds or thousands of remote sensors and controllers. The remoteness of monitoring sites, the lack of a need for wired communication network, and the ability to accommodate future communication needs make Software Defined Radios (SDR) a suitable wireless media to replace legacy communication devices in power grids. Reconfigurability of SDR supports integration and co-existence of multiple radio access technologies on general-purpose radio equipment and the ability to update and reconfigure software on these devices over-the-air, enabling implementation and fast upgrade of complex SCADA networks.

In this paper, we investigate the security challenges of deploying reconfigurable devices as communication platforms for substations and field instruments in the power grid. The security goals are to prevent installation and execution of unauthorized software, ensure the device operates within allowed frequency bands and power levels, and prevent the device from operating in a malicious manner. The main challenges are how to dynamically and securely configure software components that are supplied by different vendors and how to attest the validity of the device configuration to a master node. We present these and other security challenges in detail. Based on our analysis, we formulate security requirements for a trusted configuration framework.

*This work was undertaken as part of the TCIP Project: Trustworthy Infrastructure for the Power Grid. It was funded by the National Science Foundation under grant number CNS-0524695.

Keywords
security, power grid, reconfigurable device, software radio

1 Introduction

Critical infrastructures are systems whose failure or destruction would have a debilitating impact on the defense or economic security of the nation [1]. These systems include electrical power systems. The North American power grid involves nearly 3,500 utility organizations delivering electricity over more than 200,000 miles of transmission lines to 300 million people. And yet this critical infrastructure is not able to cope with grid-wide phenomena such as the 2003 Northeast Blackout that affected 50 million people and caused financial losses of up to $6 billion due to the power outage. A major culprit is the inadequate communication infrastructure of the power grid.

The power grid's existing communication architecture limits the deployment of control and protection schemes to manage electric power generation, transmission, and distribution effectively. Ideally, grid companies want fine grain monitoring and control of their distribution network, even down to the last transformer. Supervisory Control and Data Acquisition (SCADA) systems have been used for years in the power grid to monitor and control substations and field instruments. However, there are still many distribution substations that are not equipped with SCADA and require manual, human maintenance. During a recent field trip to AmerenIP's sites, we found that out of their 550 substations in Illinois, only 200 were equipped with SCADA systems.

A SCADA system gathers information (such as where high voltage has occurred) from field instruments, transfers the information back to the substation and control center, alerts the control center of any alarms, carries out any necessary local analysis and control such as determining if the voltage level has risen above or dropped below a critical level, and allows the control center to modify control on the distribution system. The importance of this

system is that it can provide early warning of potential disaster situations and provides safe, non-destructive operation of devices and transmission lines. Unfortunately, many of those substations that require SCADA would require installing necessary communication lines to the control center and to field instruments such as pole-top Remote Terminal Units (RTUs). The technology of field instruments has evolved beyond simple RTUs, with increasing deployment of Intelligent Electronic Devices (IEDs) and synchronous Phaser Measurement Units (PMUs) that give a much more detailed insight into grid dynamics and post-incident analysis [2]. However, this data cannot easily be utilized beyond the substation when the grid has limited communication lines.

There is also a need for point-to-point communication between substations to implement Special Protection Schemes (SPS). SPS address some of the wide-area control issues where the occurrence of particular events or measurements at one point in the grid triggers actions (such as a breaker tripping) at another. The existing approaches to communication architecture do not link substations directly. In short, communication networks are needed to connect SCADA control centers with substations and fields instruments, and to link substations with other substations. Such a network can be very expensive to build and maintain.

Traditional solutions for implementing communication lines have been to lease lines from telecom providers at very high installation and maintenance costs. Leased telephone channels also provide limited reliability and sometimes may not be even available at the substation site. During our field trip to AmerenIP, it was disclosed to us that the local phone company will no longer give them dedicated copper lines for their substations. The other difficult aspect of installing physical communication lines is that distribution networks cover very large geographic areas.

One might think that the Power Line Carrier (PLC) is a good solution for this problem. PLC uses the power lines to transmit radio frequency signals in the range of 30-500 kHz [3]. PLC is not subject to the unreliability of leased telephone lines. However, power lines are a

hostile environment for signal propagation, with excessive noise levels and cable attenuation. Also PLC is not independent of the power distribution system, thus making it unsuitable for emergency situations when the communication lines must operate even if the power lines are out of service.

Such difficult networking problems can be solved with wireless radio technologies. In general, wireless communication offers lower installation and maintenance costs than fixed communication lines, and they provide more flexibility in network configuration. There are many different types of wireless technologies such as satellites, very high frequency radio, ultra high frequency radio, and microwave radio. Each has its own advantages and disadvantages. The satellite system contains a number of radio transponders which receive and retransmit frequencies to ground stations within its coverage on the earth's surface. Advantages of the satellite system are wide area coverage, easy access to remote sites, and low error rates. Its disadvantages are transmission time delay, and continual leasing costs incurred on time-of-use basis.

The Very High Frequency (VHF) radio operates in 30-300 MHz band and mostly reserved for mobile services. On the other hand, Ultra High Frequency (UHF) systems operate in 300-3000 MHz band, and can be Point-To-Point (PTP), Point-To-Multipoint (PTM), Trunked Mobile Radio (TPR), or spread spectrum systems. VHF radios, PTP and PTM radios in UHF have advantages of propagating over non-line-of-sight paths, low cost radios, and available frequency assignments. Their disadvantages are low channel capacity and low digital data bit rate. Spread spectrum systems are the basis for many wireless applications including 802.11 networks, and can operate with low power radios without licenses. However, these radios are subject to interference from co-channel transmitters and have limited path lengths because of restrictions on RF power output.

Microwave radio is a UHF radio operating at frequencies above 1 GHz. These systems have high channel capacities and data rates. However, microwave radios require line of sight clearance, are more expensive to develop than VHF and UHF, and sometimes the

appropriate frequency assignments are not available in urban areas.

A SCADA radio device can be implemented using any of the above mentioned radio technologies. Figure 1 illustrates how wireless communication could be deployed in the power grid. Researchers have conducted experiments and evaluations of these radios including 802.11, GPRS, and 900 MHz [4, 5, 6]. Each one has one or more disadvantages, and the technology may become outdated in the long term. It is no easy task to upgrade thousands of equipment in the power grid. It is costly and time consuming. The existing power grid communication lines and equipment are outdated for a reason- they have been installed decades ago.

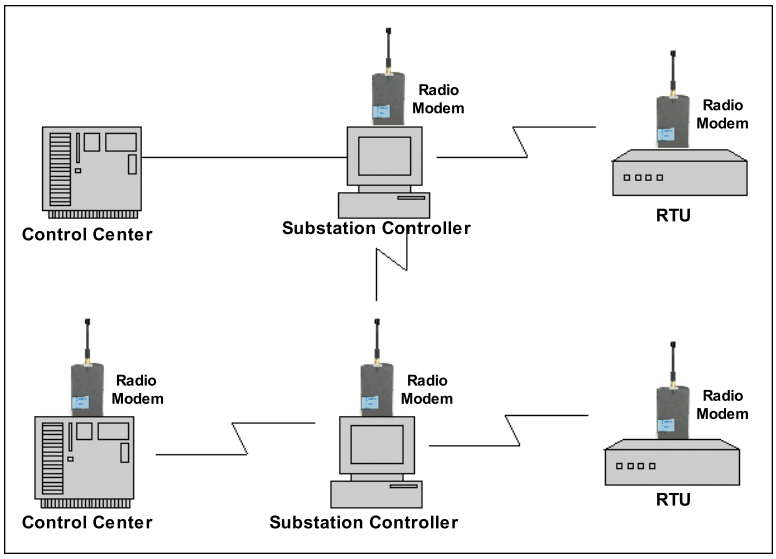

Figure 1: Wireless communication in the power grid.

Thus, the ideal radio platform for the power grid should accommodate future wireless communication needs, have low installation and maintenance costs, and be capable of reconfiguring and updating its operation and software. Such considerations favor examining Software Defined Radio (SDR) as a possible radio platform. SDR implements the functions of radio devices such as modulation, signal generation, coding and link-layer protocols as software modules running on a generic hardware platform. Traditional radios are built for a particular frequency range, modulation type and output power. In SDR, these radio fre-

quency (RF) parameters can be configured when the radio device is in use rather than when it is manufactured. This enables highly flexible radios that can switch from one communication technology to another to suit a particular application or environment. Furthermore, the protocols that implement various radio technologies and services can be downloaded over-the-air onto the radio device.

Software radio is a suitable wireless media to replace legacy communication devices in power grids. The reconfigurability of SDR supports the integration and co-existence of multiple radio access technologies on a general-purpose radio equipment, enabling implementation of powerful SCADA networks. At the same time, the wireless and reconfigurable nature of SDR introduces potentially serious security problems such as unauthorized access to the SCADA system, spoofing or suppression of utility alarms, and configuration of a malfunctioning or malicious radio equipment.

In this paper, we investigate the security challenges of deploying software radios in the power grid. To the best of our knowledge, this problem has not been addressed before. The security goals are to prevent installation and execution of unauthorized software, ensure the device operates within allowed frequency bands and power levels, and prevent the device from operating in a malicious manner. The main challenges are how to dynamically and securely configure software components on the radio that are possibly originating from different vendors as the power industry is shifting from proprietary protocols toward open and standard protocols, and how to attest the validity of the radio configuration to a master node. We present these and other security challenges in detail, and based on our analysis, we formulate security requirements and design of a trusted configuration framework for SDR in the power grid.

The rest of this paper is organized as follows: Section 2 provides an overview of the software-defined radio concept. Section 3 presents the security challenges of a reconfigurable radio in the power grid and enumerates its security requirements. We describe a secure configuration framework for SDR in Section 4. We summarize the related work in Section

5, and conclude in Section 6.

2 Overview of Software Defined Radio

The Federal Communications Commission (FCC) adopted the following regulatory definition for SDR [7].

> *Software Defined Radio.* A radio that includes a transmitter in which the operating parameters of frequency range, modulation type or maximum output power (either radiated or conducted) can be altered by making a change in software without making any changes to hardware components that affect the radio frequency emissions.

Let us explain how a software radio differs from a regular digital radio. Figure 2 shows the block diagram of a digital radio transceiver consisting of the radio frequency (RF) front-end, the intermediate frequency (IF) section and the baseband section. The RF front-end functions as the transmitter and receiver for the RF signal transmitted/received via the antenna. It down-converts the RF signal to IF signal, or up-converts the IF signal to RF signal. The IF section is responsible for analog-to-digital conversion (ADC) and digital-to-analog conversion (DAC). The digital down converter (DDC) and digital up-converter (DUC) jointly assume the functions of a modem.

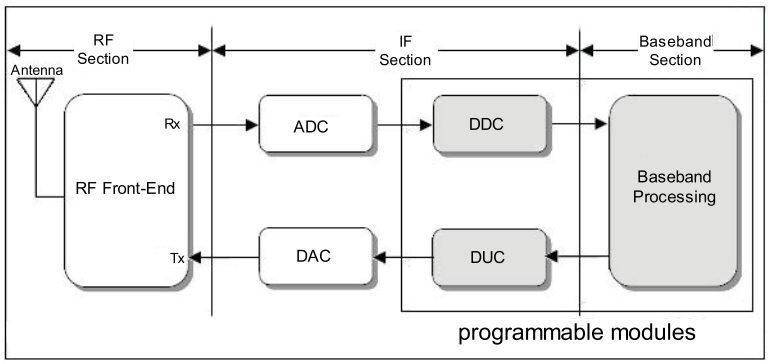

Figure 2: A digital radio transceiver.

The baseband section performs baseband operations such as connection setup, equalization, frequency hopping, timing recovery and correlation. In SDR, the baseband processing and the DDC and DUC modules (highlighted in the figure) are designed to be programmable via software [8]. The link layer protocols, modulation and demodulation operations are implemented in software.

For utilities, system upgrades and bug fixing becomes easier with reconfigurable devices compared to fixed devices. SDR enables the fast introduction of new utility applications into the SCADA system. However, SDR technology has numerous technical challenges that need to be resolved before it can be successfully deployed. General SDR challenges are the provision of: advanced spectrum management for dynamic allocation of spectrum according to traffic needs, robust security measures for secure configuration of terminals, secure software download, prevention of system misuse, and open software architecture with well defined interfaces.

As it relates to the deployment of SDR in the power grid, the problem of secure configuration of a radio and attestation of a radio configuration to a master node within the power grid must be addressed. We discuss the security issues in Section 3. Next, we briefly introduce configuration and attestation problems.

2.1 Software Radio Configuration

Radio configuration challenge is to provide composition of radio software components with certain constraints (e.g. regulatory body requirements, wireless communication requirements for the power grid, and device hardware specifications.) These constraints are provided in machine-readable policies and specify the radio access technology (e.g. GSM, UMTS), allocated frequency band (e.g. 806-902 MHz), and hardware parameters (e.g. IF, power, interfaces). The difficulty lies in mapping configuration policies into a functional dataflow graph and then, further, into an executable dataflow graph. The executable dataflow graph states which software modules implement functional blocks, and it is used to activate a new

radio mode.

We can describe the configuration process as a sequence of the following steps: first, the utility application or SCADA master node requests a new configuration of the terminal. Rules and policies specifying regulatory and power grid communication requirements are downloaded to the terminal. The requester will send its specifications for a new configuration along with the request if the specific configuration has not been activated on this terminal before.

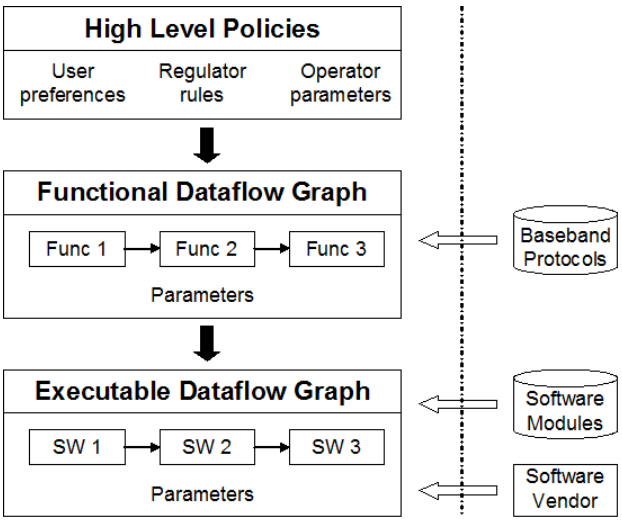

Figure 3: Composition Model.

At the heart of configuration composition is a problem of *mapping high-level policies into an executable dataflow graph*. High-level policies are a collection of regulator's rules (e.g. FCC) and wireless communication parameters for the power grid. First, these policies are mapped into an intermediate graph that we call a *functional dataflow graph*. A functional graph is constructed according to a baseband protocol specified in high level policies and consists of functional blocks and their parameters. Then, the functional graph is mapped into an *executable dataflow graph* consisting of software modules and their parameters. If the suitable software modules cannot be found in the local store, they need to be downloaded from a software vendor via SCADA control center. Figure 3 shows the big picture of the composition model.

A baseband protocol specifies the order and type of mathematical functions used to process a signal stream. For example, if the desired radio access technology is GSM, its corresponding baseband protocol specifies the order and types of modulators, encoders, and filters to be used for processing the signal.

2.2 Remote Attestation

The substation or control center may request a proof of conformity with the standards before allowing the field instrument or another substation to participate in the utility operation. The remote attestation challenge is to provide an attestation scheme enabling the terminal to prove to its master node that its current configuration is in compliance with standards and regulations, and it is not a rogue or malfunctioning device. Should the configuration be found as non-conforming at any point, the terminal rolls back to a prior validated configuration. This implies that the last working configuration should be kept in ready-to-load state.

Remote attestation process starts with a request from a master node to attest the configuration of a remote device before participating in a utility communication. This is to ensure that the terminal is configured correctly to fully benefit from the service, and also to prevent a misconfigured terminal interfering with other network nodes' communication. Normally, the master node would perform a validation once in the beginning, and afterwards it verifies that the configuration has not been modified with its knowledge.

3 Security Challenges

The "IEEE Guide for Electric Power Substation Physical and Electronic Security" [9] points out that the increased use of computers to remotely access substations may be exposing control and protection devices to the same vulnerabilities as all other computer systems. Concerns about cyber threats to the critical infrastructures such as the power grid has become widespread and there are plenty of examples of successful attacks to justify these

concerns.

President's Commission on Critical Infrastructure Protection (PCCIP) [1] and IEEE issued reports [9] listing threats to utilities. The general category of threats that are specific to SCADA systems, substation controllers, and field instruments are [10]:

- Blunders, errors, and omissions
- Fraud and theft, criminal activity
- Disgruntled employees and insiders
- Curiosity and ignorance, recreational and malicious hackers
- Industrial espionage
- Malicious code
- Foreign espionage and information warfare

Security issues that pertain to a general RTU, substation, or a wireless device are discussed in other works- some mentioned above, others are summarized in Section 5. In this work, we focus on security issues that are unique to software radios. Since the distinguishing characteristic of software radio is its reconfigurability, when talking about security, we mainly refer to configuration security.

Before designing protection mechanisms for SDR in the power grid, we should identify security challenges that exist in the system. For this purpose we utilize a threat modeling technique consisting of these steps:

- Characterizing the system- Involves understanding the system components and their interconnections, and creating a system model emphasizing its main characteristics.
- Identifying assets and access points- Involves identifying abstract or concrete system resources that must be protected from misuse by an adversary, and identifying accesses to these resources.

- Identifying threats- Examine identified security-critical assets, review a list of attack goals for each asset that violate Confidentiality, Integrity, or Availability. Create a threat profile of the system describing potential attacks that need to be mitigated.

First, let us clarify some important concepts of the radio architecture. In the previous section, we discussed the steps of configuration process, but have not explained how a radio configuration is represented in the system. We define SDR configuration as follows:

> *A configuration of a SDR terminal describes which waveforms or digital signal processing (DSP) modules drive the radio operating mode, what input parameters are specified for each DSP module, and how these modules are interconnected.*

At the core of a radio configuration is a set of pipelines, each containing DSP modules stringed one after another. This type of pipeline is also referred to as a *flow graph* because it clearly depicts the flow of transmitted/received data as it gets processed by one DSP module after another. Figure 4 shows a generic flow graph characterizing the configuration of a SDR terminal. The vertices of the graph are DSP modules that perform various mathematical manipulations such as modulation, filtering and mixing on the input signal stream. The edges of the graph indicate the direction of data flow as well as connect adjacent DSP modules via memory buffers. These buffers are used to temporary store the signal stream that is being processed.

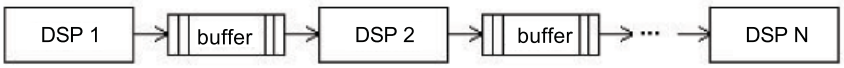

Figure 4: Generic flow graph of DSP modules.

Reconfigurability of SDR allows to alter properties of the radio equipment that have previously been determined and fixed by their design. This improved flexibility introduces a security vulnerability that a radio terminal is configured in such a way that the hardware cannot withstand, or contradicts the restrictions placed by the master node, utility provider,

equipment manufacturers, and regulatory authorities. SDR threats may result from the deliberate overt or covert actions of third parties (e.g. hackers, viruses), or through human error (e.g. software bugs). The point of attack can be either the communication infrastructure or the end terminal. The main assets controlled by SDR configuration that attackers may target are: configuration manager and processes, configuration parameters and files, flow graph generator, DSP modules, DSP parameters, memory buffers, and signal stream.

3.1 Security Threats

For brevity, here we describe only the end result of our threat modeling effort, instead of describing it step-by-step in detail. Based on the threat modeling approach outlined in the previous section, we identified the following security threats that relate to SDR configuration. For each threat, we name the threat, provide its classification, and describe its effects and consequences.

- Configuration of a malicious device - (DoS, Disclosure) - A malicious user may configure the SDR terminal in such a way that it is used as an eavesdropping or jamming device. The malicious device using too high power could force other devices within the communication network to operate at higher power level and drain their batteries, or simply disrupt their communication if the local network devices do not change their power output level.

- Violation of regulatory constraints - (DoS) - The device may be configured without adherence to regional regulations and equipment specifications (EMC emission requirements). This may render the device inoperable. Also the device may unintentionally operate in unauthorized bands such as military use bands.

- Invalid configuration - (DoS) - A configuration could be installed and activated that does not work or works incorrectly. Received or transmitted signal stream may be

processed incorrectly resulting in garbled messages. Wireless protocol specified by the master node or the utility provider could be disregarded.

- Insecure software download - (Tampering) - Configuration and waveform software may be illegally modified en route, or an adversary may supply its own software. This opens doors for launching other attacks such as configuration of a malicious device or exhaustion of system resources.

- Exhaustion of system resources - (DoS) - A malicious or buggy software may launch DoS attack against legitimate processes by using up system resources such as memory.

- Improper software functionality - (Tampering) - Even if software was supplied by a certified vendor and downloaded from a trusted master node, it could be buggy. It might not work properly or implement the expected functionality. Such software can accidentally modify parameters of other processes or garble the signal stream, for example, through buffer overflow.

- Illegitimate access to private data - (Information Disclosure) - Sensitive information is involved in the configuration process. Access to information about the power grid's communication specifications, and configuration data has to be protected.

There are other threats such as unauthorized use of network services and unauthorized login into a radio device that concern SDR in general but outside the scope of this paper. The above identified threats serve as valuable basis to derive security objectives and requirements of our configuration framework described in the next sections.

3.2 Security Requirements

To mitigate the above security threats, we specify the following security requirements for the proposed configuration framework for SDR:

- It shall prevent the loading, installation, and instantiation of unauthorized or unproven software.
- It shall ensure the secrecy and integrity of over-the-air software download.
- It shall verify that downloaded software is supplied by a certified vendor.
- It shall ensure that the SDR terminal operations are limited to those frequency bands and power levels at which the terminal is authorized to operate by the local regulatory bodies and the power grid operators.
- It shall implement a trusted configuration module responsible for a flow graph construction.
- It shall provide fault domain isolation for reconfigurable modules so that each has access only to its own memory area.
- It shall ensure that software already installed on the terminal has not been modified or tampered with while the terminal was in a power down condition.
- It shall ensure confidentiality, integrity, and authenticity of information used in the configuration process.
- It shall provide trusted configuration information to other nodes in the power grid on request.

4 Security Framework for Reconfigurable Devices

Figure 5 illustrates the architecture of the SDR configuration framework that enables a trusted radio platform for field instruments and substations in the power grid. This framework consists of the following modules:

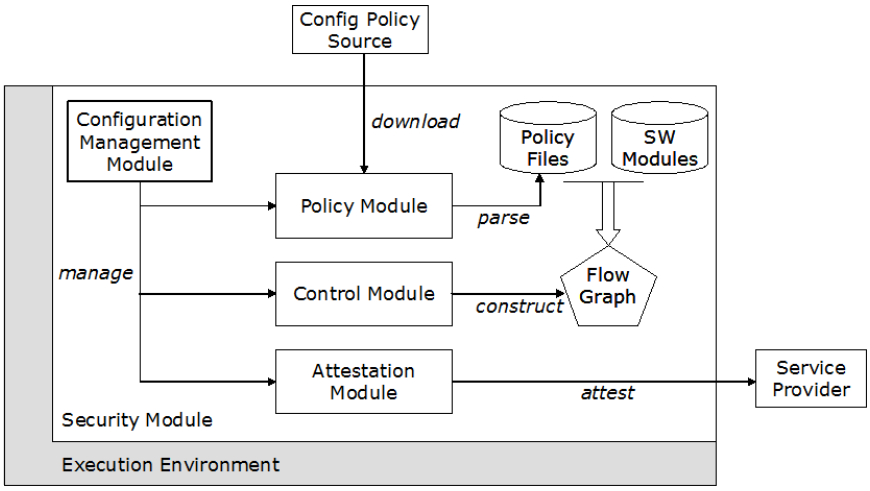

Figure 5: Architecture of the configuration framework.

- *Execution Environment*- A platform for executing all equipment functions including configuration management and control. The challenge for SDRs is to ensure that applications cannot access, nor interfere with the flow of information at a higher security classification such as configuration. To support multiple levels of security on a single processor, a secure partitioning method is needed. We propose a secure Memory Management Unit (MMU) using hardware-enforced memory protection to ensure data isolation in different partitions.

- *Security Module*- This module ensures that all the security requirements specified for the configuration process are satisfied. It provides the basic security functions to all other configuration modules. For example, it provides authentication function to the MMU when a digital signal processing module attempts to access the shared memory buffer of the flow graph.

- *Configuration Management Module (CMM)*- A functional entity responsible for the management of all configuration tasks. It initiates, coordinates, and performs configuration functions, and manages the communication between all configuration related components. It supports such tasks as mode selection, download of configuration policies and software modules, and approval of new radio configurations.

- *Configuration Control Module (CCM)*- A supporting entity for CMM, it controls and supervises reconfiguration execution. The selected and verified configuration policy is handed over to the CCM for construction of a flow graph composed of DSP modules specified in the policy. The flow graph is then executed by the runtime environment activating the requested radio operating mode. This module also ensures that the new configuration is in compliance with regulatory requirements before executing the configuration.

- *Policy Management Module (PMM)*- Provisions a configuration policy for a new configuration approved by the CMM. Parses and verifies downloaded configuration policies, manages the update and versioning of the local policy repository. We use XML to describe configuration policies and descriptors of reconfigurable software modules such as DSP modules.

- *Configuration Attestation Module (CAM)*- Software attestations will enable a SDR device to prove to its master node that it is configured properly. This module provides trusted configuration information to the service provider upon request.

Other modules within the framework are local repositories of configuration policies and reconfigurable software modules. The repository of software modules containing DSP modules and link protocols is not strictly a part of the configuration framework. However, these software modules are the main target of the configuration process as it composes these modules into a flow graph according to the appropriate configuration policy to activate a particular radio operating mode.

This framework satisfies the security requirements listed in the previous section. The implementation details and proof of security properties is left for our future publication. In this work we aimed at identifying security challenges of deploying SDRs in the power grid.

5 Related Work

A few research works investigated the use of various wireless protocols in the power grid, although none of them address the usage of SDRs. Shea [6] describes deployment of 900/928/952 MHz radios in SCADA on Houston Lighting & Power company distribution lines. Their experience showed that these radios can be deployed for master-RTU communication at lower installation and maintenance costs and provide higher reliability than leased phone lines. There were occasional interferences from systems operating in neighboring bands and problems with FCC regarding frequency licensing and distance restrictions between master and RTUs.

Eichelburg [5] presents a wireless communication architecture that uses GPRS modems to connect many medium voltage substations for a German municipal utility. GRPS modems combined with VPN routers allow substations to communicate with the SCADA control center through the public Internet. Risley et al. [4] discuss security risks associated with the use of 802.11 radios in the power grid. They point out some generic wireless security risks and recommendations, and breakdown the security flaws inherent in the WEP encryption of the 802.11 protocol.

Research related to security of SDR can be categorized into two groups. In the first group, Michael et al. [11] propose a framework for establishing secure download for SDR that includes employment of tamper resistant hardware and four different cryptographic techniques: secret key encryption, public key encryption, cryptographic hashing, and digital signature. This framework provides solutions for verification of the declared identity of the downloaded software, verification of the integrity of the downloaded data, disabling the ability to run unauthorized software on the SDR device, and the secrecy of the downloaded data. They assume the existence of tamper-resistant hardware that provides secure storage for the terminal keys. This work also assumes that software is created and distributed by the hardware maker. Sugita et al. [12] propose an electronic commerce scheme that

utilizes the ability of SDR to switch between different security algorithms. The following issues are identified, but without precise specifications: a) encryption of download channel, hardware key, and terminal ID to prevent illegal copying of the downloaded program; and b) certification against alteration of the downloaded program.

In the second group, Brawerman et al. [13] propose a lightweight LSSL protocol that uses less bandwidth than SSL to securely connect a manufacturer's server and SDR devices for downloading radio configuration files. In addition to securing the download connection, their secure protocol includes mutual authentication, public/private key mechanisms for data encryption and decryption, and fingerprint calculations to check data integrity. Uchikawa et al. [14] propose a secure download system that uses the characteristics of the field programmable gate arrays (FPGAs). The wiring of configuration logic blocks on FPGAs can be arranged in many different ways (astronomical number), enabling high security encipherment to prevent illegal acquisition of software using replay attack. These works assume that SDR devices download software only from their manufacturers.

6 Conclusion

The current communication infrastructure in the electrical power systems is inadequate to cope with cascading power outages and increasing cyber attacks. However, installation of new communication lines based on leased phone lines is very costly. Wireless technologies such as VHF, UHF, and microwave radios offer low cost, more reliable communication alternatives. However, each of these radios have some disadvantages, making it difficult for utility companies to commit to one of them as a long term solution.

Software defined radios appear to be an ideal radio technology to accommodate future wireless communication needs. Like all radio solutions, it has low installation and maintenance costs. In addition, new wireless protocols may be downloaded and configured to activate a new radio mode.

In this work, we have investigated security issues specific to the deployment of software radios in the power grid. Configuration of a malicious device, insecure software download, and violation of regulatory constraints are some of the security vulnerabilities that we have identified. We presented the design of a configuration framework that supports secure radio configuration and remote attestation of SDR.

References

[1] J. Ellis, D. Fisher, T. Longstaff, L. Pesante, and R. Pethia, "Report to the Presidents Commission on Critical Infrastructure Protection," Special Report, January 1997.

[2] C. Hauser, D. Bakken, and A. Bose, "A Failure to Communicate," *IEEE Power & Energy Magazine*, April 2005.

[3] National Communications System, "Supervisory Control and Data Acquisition (SCADA) Systems," Technical Information Bulletin 04-1, October 2004.

[4] A. Risley and J. Roberts, "Electronic Security Risks Associated with Use of Wireless, Point-to-Point Communications in the Electric Power Industry," Technical Report, 2003.

[5] W. Eichelburg, "Using GPRS to Connect Outlying Distribution Substations," in *Proceedings of 18th International Conference on Electricity Distribution*, June 2005.

[6] M. Shea, "900 MHz Radio Signals Operational Control," *IEEE Computer Applications in Power*, October 1992.

[7] Federal Communications Commission, "Authorization and Use of Software Defined Radios," First Report and Order, September 2001.

[8] Wipro Technologies, "Software-Defined Radio," White Paper, August 2002.

[9] IEEE Power Engineering Society, "IEEE Guide for Electric Power Substation Physical and Electronic Security," IEEE Standard 1402-2000, April 2000.

[10] P. Oman, E. Schweitzer, and D. Frincke, "Concerns About Intrusions into Remotely Accessible Substation Controllers and SCADA Systems," Technical Report, 2000.

[11] L. B. Michael, M. J. Mihaljevic, S. Haruyama, and R. Kohno, "A Framework for Secure Download for Software-Defined Radio," *IEEE Communications Magazine*, July 2002.

[12] M. Sugita, K. Uehara, and S. Kubota, "Flexible Security Systems and a New Structure for Electronic Commerce on Software Radio," in *Proceedings of the 13th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, 2002.

[13] A. Brawerman, D. Blough, and B. Bing, "Securing the Download of Radio Configuration Files for Software Defined Radio Devices," in *Proceedings of the 2nd International Workshop on Mobility Management & Wireless Access Protocols*, October 2004.

[14] H. Uchikawa, K. Umebayashi, and R. Kohno, "Secure Download System Based on Software Defined Radio Composed of FPGAs," in *Proceedings of the 13th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, 2002.