Cyber Security for Power Grids *

Frank Mueller, Subhashish Bhattacharya, Christopher Zimmer
Dept. of Computer Science, / Electrical and Computer Engineering,
North Carolina State University, Raleigh, NC 27695-7534

Abstract

Power grids worldwide are undergoing a revolutionary transition as so-called "smart grids" that exploit renewable energy sources are emerging. As such distributed power generation requires networked control, future power systems will become more exposed to cyber attacks.

This paper discusses cyber security challenges for a future power grid. It highlights deficiencies and shortcomings of existing power devices and identifies areas of urgent need particularly on the software side to establish security as a first-class paradigm in cyber-physical control systems. Such actions are urgent as a cyber compromise of power systems can lead to physical outages or even damaged power devices. Hence, security and fault resilience of power as a utility must be a prime objective for power grids. Security compromises should be contained to only present themselves as localized faults and to prevent faults from cascading.

We expose these challenges in detail and also highlight novel opportunities for cyber security specifically for a smarter power grid, which can be generalized to the wider domain of cyber-physical control systems.

1 Introduction

The power grid in the US is one-century old and aging in terms of infrastructure. However, the power industry is slowly undergoing a revolution and modernization through new technologies: distributed power generation (DG) from renewable energy sources, power electronics-based control devices at transmission and distribution levels, and new computing and communication technology [9, 4, 1, 6]. By coordinating and controlling individual DG micro power generation sources through power electronics, the microgrid has unique features and more control flexibility to fulfill system reliability and power quality requirements than the traditional distribution systems. In addition, the microgrid can provide many ancillary services to the up-stream power system through proper control and communication.

DG requires automated control in a distributed control-systematic manner, which relies on networked coordination of power devices. The embedded controllers in such a large-scale and complex cyber network are the enabling technology for distributed power generation. Yet, the exposure of such systems to cyber attacks also increases due to its inherently networked nature. Furthermore, sustained reliability and resilience to faults, both physical and cyber, becomes a challenge.

To address the security needs of power grids, both microgrids and regional grids, we identify a severe shortcoming in industry practice to meet challenges of both security and reliability/resilience to faults. These shortcomings are exacerbated by the power industry's reliance on devices whose hardware and software design is often a decade old or more and provides to be unsuitable for distributed control.

We see an urgent need in a complete overhaul of both hardware and software control platforms for the power grid and power devices in particular. Instead of aging, standalone controllers, latest hardware platforms combined with a systematic software methodology specifically for power devices is required to meet the demand for distributed control and to provide security and fault resilience.

Such a systematic software design methodology poses an urgent need for

1. static and dynamic analysis and protection methods to remove bugs as well as security vulnerabilities in software for intelligent power devices in microgrids;
2. techniques and tools to ensure software integrity on intelligent power devices and control computers in microgrids, including
   - secure/trusted bootstrap to guarantee that power devices only boot authorized software, and
   - runtime monitoring mechanisms that prevent and/or detect compromises of software integrity on power devices; and

*This work was supported in part by NSF grants CCR-0237570, EEC-0812121, and U.S. Army Research Office (ARO) grant W911NF-08-1-0105 managed by NCSU Secure Open Systems Initiative (SOSI).

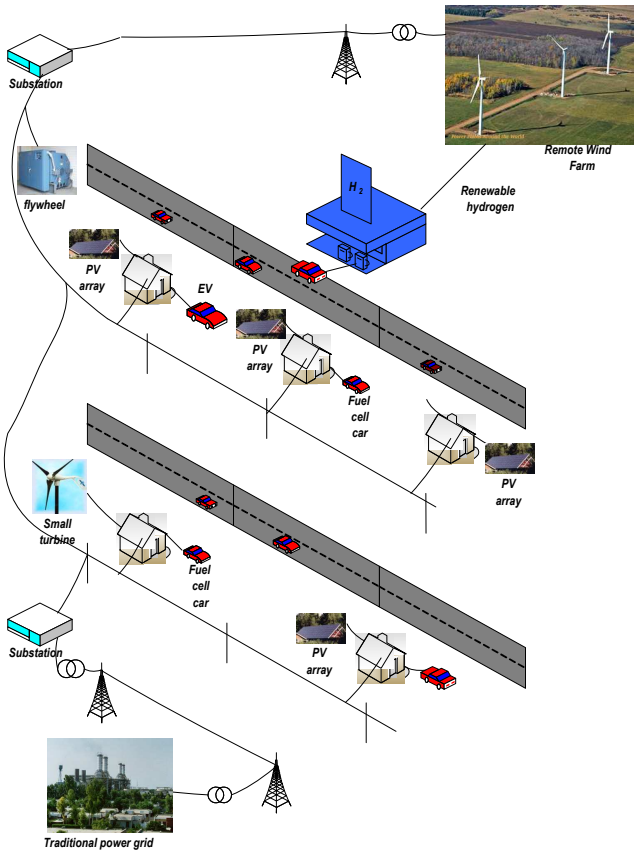

Figure 1. FREEDM: Architectural View

3. attack-resilient techniques for the monitoring and control of microgrids, specifically for attack modeling to determine if an adversary has gained control of a power device controller.

Addressing these shortcomings, we highlight several problems and solutions specific to CPS security in power grids in the following.

2 Timed Security

Many cyber-physical control systems are embedded systems with real-time constraints, and power systems are just one such example. As these systems are increasingly networked and affect our daily life, insuring that they are secure from intrusion and tampering by adversaries is a design challenge of utmost importance.

Cyber-physical real-time systems not only benefit from general-purpose software security mechanisms but also lend themselves to novel and complementary security methodologies beyond reach in general-purpose systems. CPS applications within the real-time systems domain have inherent knowledge about their timing behavior, *i.e.*, worst case and best case execution times (WCET/BCET). WCET and BCET derived from static analysis safely bound the upper and lower execution time of specific code sections [8, 7, 5]. Hence, execution times above or below the respective bounds provide indications for a system compromise.

We propose to exploit this observation to develop *timed security* mechanisms. Timed security utilizes instrumentation and analysis from within real-time applications in order to detect the execution of unauthorized code. Using actual timing metrics and comparing them with WCET/BCET bounds allows the detection of security breaches due to intrusion within the system. Beyond security, the mechanism also serves as a detector for predicting deadline overruns, *i.e.*, it can determine if an application is going to exceed its timing requirements prior to the actual deadline miss. This provides ample time to transition to a fail-safe state as a security protection or fault resilience action.

Timed security can be employed at different levels, including a *macro* and a *micro* view of timing bounds constraining selected code sections of the overall system in a complementing manner to fend off attacks and provide safeguards at different system abstraction and protection levels.

The first instance of timed security is to check actual execution time at the micro level along the return path of routines against WCET/BCET bounds. Preliminary results of experiments with this method indicate that the window of vulnerability is restricted to a sensitivity of 10-51 cycles without and 10-82 with caches on a SimpleScalar cycle-level simulation platform. Any code injections exceeding this tight limit are detected. Utilizing an embedded power device controller platform, experiments with an embedded DSP clocked at 150 MHz indicate that code injections of one microsecond are already being detected. With timestamp counter hardware, even finer grained injections are detectable, as reported for the simulation environment above.

The second instance of timed security mechanism utilizes a real-timed scheduler and relies on macro WCET bounds of longer code sections within the application delimited security checkpoints. These checkpoints allow timing validation in a synchronous fashion with program execution. Preliminary results indicate a sensitivity of 14-6k cycles for intrusion detection depending on the placement of synchronous checkpoints in the application code. This approach complements the return path inspection as it can uncover attacks where large portions of application code are skipped or control even fails to return to the original control flow.

In a third instance of timed security, the periodic scheduler is utilized in an asynchronous manner relative to program execution. Upon periodical activation, the scheduler validates WCET/BCET bounds for code sections executed since the last scheduler activation. Execution tracking through scheduler-sensitive progress indicators in the application allows sufficiently accurate correlation between

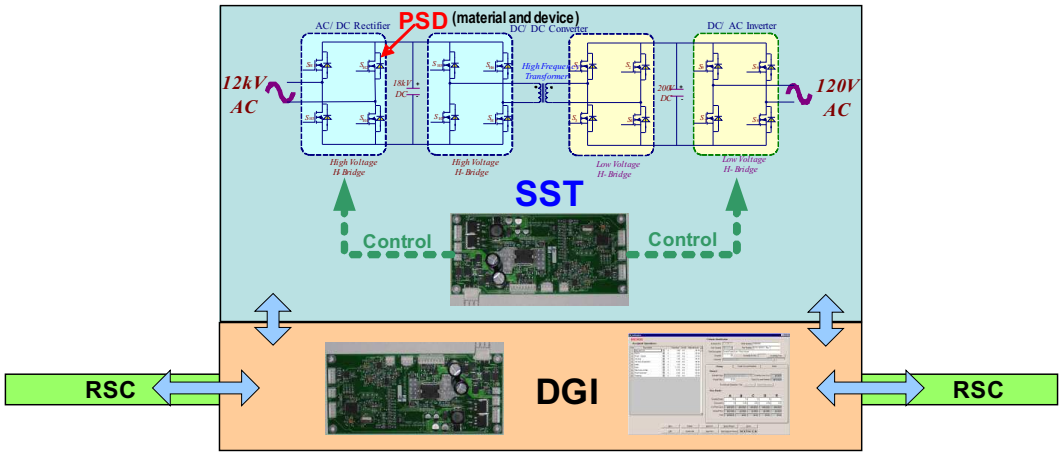

Figure 2. IEM Subsystem

execution progress and the respective code sections covered. Preliminary results indicate a sensitivity of 1k-14k cycles for intrusion detection, yet at a much lower overhead than prior approaches due to the asynchronous nature of the method. The benefit of this method is its ability to bound the WCET of PC-constrained code sections within or across loops and to verify that the job's execution meets these bounds. Bounds violations are a sufficient indication of intrusion for a given code section.

3 FREEDM

The Future Renewable Electric Energy Delivery and Management (FREEDM) Systems Center, headquartered on NC State University's Centennial Campus, is one of the latest Gen-III Engineering Research Centers (ERC) established by the National Science Foundation in 2008. Our vision for the ERC for Future Renewable Electric Energy Delivery and Management (FREEDM) Systems is to develop a revolutionary electric power grid integrating highly distributed and scalable alternative generating sources and storage with existing power systems to facilitate a green energy based society, mitigate the growing energy crisis, and reduce the impact of carbon emissions on the environment. In the FREEDM System illustrated in Fig. 1, the users will have the ability to plug-and-generate, plug-and-store energies at home and in factories, as well as will have the ability to manage the energy consumption (load management). The successful development of such an infrastructure will empower all us to be a participant of the energy innovation, spurring more innovations in the renewable energy generation and energy storage technologies. To address the transportation energy consumption issue, we envision the use of electric energy storage in plug-in electric vehicles (PEVs) will be the best solution in which electric energy is generated by renewable and clean sources. The FREEDM System will have the ability and strength to manage large amount of distributed energy storage devices to maximize the renewable energy generation and utilization based on energy pricing and emission requirement.

The proposed FREEDM system is a green energy grid infrastructure that will:

- Allow plug and play of any Distributed Energy Resources (DRER) or Distributed Energy Storage Devices (DESD), anywhere and anytime;
- Manage DRER and DESD through Distributed Grid Intelligence (DGI) software;
- Have a communication infrastructure backbone;
- Have the capability of being totally isolated from the main grid, if necessary, autonomous continuing to operate based on 100
- Have perfect power quality and guaranteed system stability; and
- Have improved efficiency, operating the alternating current system with unity power factor.

In the electric configuration of the FREEDM system shown in Figure 3, low voltage (120V), residential class DRER, DESD, and loads are connected to the distribution bus (12kV) through a revolutionary, highly efficient power electronics based Intelligent Energy Management (IEM) subsystem. Each IEM will have bi-directional energy flow control capability allowing it to provide key plug-and-play features and isolate the system from faults on the user side. An Intelligent Fault Management (IFM) subsystem will be used to isolate potential faults in the 12 kV primary circuit. IEMs and IFMs will communicate with each other by a Reliable and Secured Communication (RSC) network.

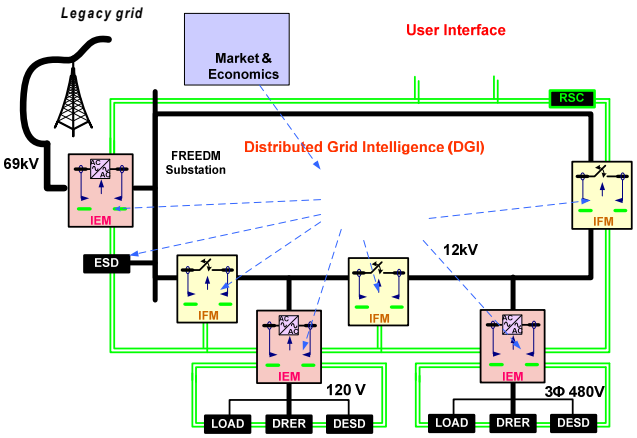

Figure 3. FREEDM: Power System Schematic

The brain of the FREEDM system will be provided by the Distributed Grid Intelligence (DGI) software embedded in each IEM and IFM. Most energy storage requirements are provided by DESDs, but an additional energy storage device may be considered necessary to satisfy the global need. The FREEDM system will be connected to the traditional grid through a higher power IEM. Industry users requiring 480V three-phase power will be connected to the FREEDM system through a medium power IEM. The FREEDM concept will work equally well with an AC or DC distribution bus, with either a radial or loop configurations. By using an AC bus, however, it will be able to co-exist with today's electric power infrastructure. Devices not connected by IEMs will work, but will lack intelligence and control. From a business standpoint, the utility company or subdivision homeowner association would be the owner of the local FREEDM system, while users (customers) would own DRERs and DESDs and any loads.

The IEM consists of a "Solid State Transformer" (SST) which enables bi-directional power flow and also enables active management of DRER, DESD and loads, rather than a traditional transformer. Acting very much like an energy router, each IEM will have bi-directional energy flow control capability allowing it to control active and reactive power flow and to manage the fault currents on both the low voltage and high voltage sides. Its large control bandwidth provides the plug-and-play feature for distributed resources to rapidly identify and respond to changes in the system.

The Figure 2 shows a single IEM node which is like an energy router. It is controlled by a DSP based dedicated controller for bidirectional power flow and also has communication to enable interface with usb/Ethernet so that two (multiple) such IEM nodes can communicate as shown in Figure 4. This hardware platform then enables implementation of distributed control for large distribution grids with multiple DRER, DESD and loads [2, 3].

This control platform will be investigated for implementation of standard utility communication protocols such as IEC 61850 and DNP3. From the grid security and resiliency point of view it is critical to determine the impact of time delays in communication between such two IEM nodes on the design of the SST hardware itself. For example, time delays in the power transaction between two IEMs will determine the minimum reservoir (energy storage capacity) required in each IEM to serve loads. This work will also investigate the control bandwidth requirements of the SST controller to effectively work with the various types of DRERs and DESDs. This can then be "programmed" in the IEM controller and communicated to coordinate between other IEM nodes. This will be the focus of this work.

4 Conclusion

We identified discusses cyber security challenges for a future power grid highlighting areas of urgent need on the software side to establish security as a first-class paradigm in cyber-physical control systems. This includes a proposal to employ these time-bounds checking techniques to detect intrusions in cyber-physical control systems as a means to strengthen their security and resilience to faults.

Overall, a systematic software design methodology for security in power grids is in need of (1) static and dynamic analysis, (2) systematic techniques and tools as well as (3) monitoring and control mechanisms. While the discussed aspects are specific to cyber security for a smarter power grid, they can be generalized to cyber-physical control systems in general.

References

[1] M. Barnes, J. Kondoh, H. Asano, J. Oyarzabal, G. Ventakaramanan, R. Lasseter, N. Hatziargyriou, and T. Green. Real-world microgrids: An overview. In *Proceedings of IEEE International Conference on System of Systems Engineering (SoSE '07)*, April 2007.

[2] R. Godbole. Development of a flexible multi-purpose controller hardware system for power electronics and other industrial applications. Master's thesis, North Carolina State University, 2007.

[3] R. Godbole and S. Bhattacharya. Design and development of a flexible multi-purpose controller hardware system for power electronics and other industrial applications. In *IEEE Industry Applications Society (IAS) Annual Meeting*, pages 1–6, Oct. 2008.

[4] N. Hatziargyriou, H. Asano, R. Iravani, and C. Marnay. Microgrids. *IEEE Power and Energy Magazine*, 5(4):78–94, July/August 2007.

[5] C. A. Healy, R. D. Arnold, F. Mueller, D. Whalley, and M. G. Harmon. Bounding pipeline and instruction cache performance. *IEEE Transactions on Computers*, 48(1):53–70, Jan. 1999.

Figure 4. DSP Controller for IEM

[6] R. Lasseter and P. Piagi. Control and design of microgrid components: Final project report. Technical Report PSERC Publication 06-03, Power Systems Engineering Research Center, University of Wisconsin-Madison, January 2006.

[7] S. Mohan, F. Mueller, D. Whalley, and C. Healy. Timing analysis for sensor network nodes of the atmega processor family. In *IEEE Real-Time Embedded Technology and Applications Symposium*, pages 405–414, Mar. 2005.

[8] F. Mueller. Timing analysis for instruction caches. *Real-Time Systems*, 18(2/3):209–239, May 2000.

[9] F. Peng. Guest editorial of special issue on distributed power generation. *IEEE Transactions on Power Electronics, Special Issue on Distributed Power Generation*, 19(5):1157–1158, September 2004.