Co-Design of Security Aware Power System Distribution Networks as Resilient Cyber Physical Systems

Osama Mohammed, Tarek Youssef and Ali Mazloomzadah
Energy Systems Research Laboratory
Department of Electrical and Computer Engineering
Florida International University
Miami, Florida

The increased penetration levels of renewables and distributed energy resources lead to increased challenges in maintaining reliable control and operation of the grid. Integrating a wide variety of systems governed by different regulations and owned by different entities to the grid increases the level of uncertainty not only on the demand side but also in terms of generation resource availability. This complicates the process of achieving generation versus demand balance. Renewable energy sources vary by nature and require intelligent forecasting and prediction systems to determine how and when this energy can be used. Controlling distributed resources that owned by customers which have enough capacity to support the grid during peak hours and provide ancillary service, is another challenge. Most of these distributed resources will be installed on the distribution network, which already in its current state lacks the proper communication and control network necessary to control the applicable resources. Moreover, the large number and widespread use of these resources makes them difficult to control from a central location.

To overcome these problems, deep integration between intelligent measurement nodes, communication systems, IT technology, artificial intelligence, power electronics and physical power system components will be implemented to manage the modern smart grid resources. On one hand, this type of integration can dramatically improve grid performance and efficiency, but on the other, it can also introduce new types of vulnerability. The risk of vulnerability escalates when the level of integration between physical and cyber components of the power system increases.

The design and optimization of such complex systems requires coordination between the cyber and physical components in order to obtain the best performance while minimizing the risk of vulnerability. In other words, the physical power system must be designed as a security-aware system. A variety of distributed system architectures could be considered ideal for a given application purely from a power system perspective. However, determining which distributed system architecture would be the best choice from the cyber component aspect is significantly more challenging given the communication system topology required for control and management capabilities as well as the resiliency issues embedded in the cyber components of the system. The design of the cyber environment must correlate with the requirements and sensitivity of the physical component, for example taking into account such matters as the sensitivity of protection devices for communication delay.

Security is an essential factor to be considered in the design of the grid architecture and communication system infrastructure. The cyber-attack detection and defense mechanisms chosen must not only included in cyber environment but also need to be considered in the design of power. For example, the defense mechanism for distributed denial of service (DDoS) attack in cyber systems isolates the affected area to separate the source of attack. However, this solution is not appropriate for the power system applications because it may cause a loss of service for the isolated area. Another type of vulnerability can result from integrating newer technologies. For example PMUs which are dependent on the satellite signal for time synchronization. An adversary can spoof a weak GPS signal by broadcasting a signal with incorrect time data from any location close to the GPS antenna. By spoofing the GPS signal, an adversary can inject the wrong phase shift through substation measurements. Moreover an expert adversary with adequate knowledge about the power system architecture can design a stealth error vector that cannot be detected by the state estimator. These types of attacks are feasible by using low-cost radio equipment such as a Universal Software Radio Peripheral (USRP) and an open source software package. In another case, some commercial PMUs cannot roll back to the correct time after receiving spoofed GPS signal with the future time because the internal time counter cannot count down. An adversary with equipment costing less than $2000 can cause permanent damage to expensive PMU equipment and render it unusable. Even an expert adversary can produce more serious stability problems to the power system.

The Advanced Metering Infrastructure (AMI) can introduce a new security risk to the power system. The AMI network is open to external unsecured environments such as cellular channels, power line carriers and radio signals. The AMI also can provide a communication path to customer system and equipment such as building management systems through the customer gateway. If the adversary succeeds in penetrating into the AMI network and pretending to be a valid smart meter management system, he can easily send a disconnection signal to millions of customers.

The possibility of a zero day attack always exists (attack occurs on "day zero" of awareness of the vulnerability). No matter how strong security systems are implemented to encrypt or authenticate data, with a wide spread system there is always a possibility for an adversary to exploit a previously unknown vulnerability.

Considering these types of potential issues in the original design (which some examples are mentioned in the above) will lead to an optimized design for both the cyber and physical components that insure the continuity of service and system resiliency under various types of faults and threats. Modern grid security should not only consider how to protect the measurements and control commands from cyber-attacks but also the power system network should be designed to be resilient in cases of successful attacks.

The power system survivability and its ability to maintain operation and provide services in the case of multiple faults and cyber-attacks not only relies on the power system architecture but greatly depends on the control system architecture as well. The distributed control system architecture ensures proper operation under challenging conditions and has the ability to interact autonomously under different scenarios. Distributed multi-agent control provides the means to decentralize the power system control and avoids central decision-making problems. During the normal operation of the power system these agents will exchange data to optimize the operation of the grid. During faults or loss of communication agents will work autonomously to keep normal service in the local area through fault detection and isolation, reconfiguration and a self-healing mechanism.

Moreover the distributed multi-agent control uses high level command structures instead of raw data which minimizes the bandwidth required for communication. Distributed control can provide methods of local control to improve the security of the power system in case of an area isolation caused by an attack or communication failure. In order to achieve optimized design of the grid architecture involving both of the cyber and physical components, a co-simulation technique is needed to model the integrated system in response to various cyber and physical events. This technique must be multi-scale and multi-resolution to address the concerns at various levels of modeling details. On the one hand, a detailed packet-level simulation of the network protocols is essential to achieve the necessary fidelity in capturing detailed interactions with the underlying power and communication infrastructure in order to expose potential system vulnerabilities. On the other hand, network-scale models are important for capturing large-scale network behavior under normal operating conditions and during cyber-attacks. The same is true for simulating the power system where a multi-resolution model could be used to capture large-scale power system behaviors during steady state or transient operation.

The co-simulation system must be able to seamlessly integrate various communication and power system components such that one can both study emergent global-scale phenomena and expose detailed system vulnerabilities. The system should incorporate various models (including mathematical, commercial, legacy models), which must to be synchronized with respect to the simulation clock. In addition, the system should also provide necessary mechanisms to allow consistent data exchange between models at potentially a different resolution so that interesting events can be propagated properly for decision-making and system evaluation. The co-simulation system will include components that need to be evaluated in real time thus the performance of the co-simulation system must allow processing events at a rate no slower than the real system clock which may include: hardware-in-the-loop studies of real power system components, real communication system protocols and services, software-in-the-loop management framework, distributed control framework, human-in-the-loop decision-making processes, studies using real time application traffic and finally cyber-attack scenarios.

The co-simulation system will consist of three components: the power system simulator, the communication network simulator, and the multi agent platform. To develop the co-design process of the power system to be security aware, an integration among these components is required. *The power system simulator* needs to provide multi-resolution model for smart grid physical components. To include the cyber environment in the power system simulation, an integration between the power system simulation package, the communication network simulator and the multi agent platform is required. The main purpose of *the integration mechanism* is to provide time synchronization and data exchange between the power system simulation software package, the communication network simulator and multi-agent platform.

The High Level Architecture (HLA) standard provides the means to exchange information between different simulation packages and allow time synchronization through Real Time Infrastructure (RTI). The data distribution service (DDS) can also be used to integrate and facilitate data exchange between the simulation systems in real time. There are two main methods for the any simulator to interact with the physical system (for hardware/software-in-the-loop studies). *Real-time simulation* allows execution of potentially large-scale models in real time so that the simulated entities can interact with real implementations and real devices. *On-line simulation*, on the other hand, refers to the use of simulation as an integrated service for management, control and optimization.

Integrating the co-simulation system into the smart grid test bed at Florida International University (FIU) provides unique a facility to investigate modern complex architectures of the smart grid. The smart grid test bed features a small-scale power system with generators, transmission lines, reconfigurable network architectures, a complete SCADA system, smart meters, commercial phasor measurement units (PMUs), measurements and a communication infrastructure. Integrated renewable energy resources in multiple microgrids provide an excellent platform to verify the controllability and resiliency of the physical system in addition to the security of cyberspace. A state estimation method is under development which combines measurements from SCADA and PMUs to detect possible wrong data injections.

A new method which has a trusted area in the analog side of measurements along with encryption capabilities was developed on the FIU test-bed to secure and validate measurement data. Studies showed that by creating an isolated area in the analog environment, attackers will not have access to that area which is why it has earned the title "Trusted Sensing Base".

An embedded platform for distributed multi-agent control is being developed to integrate the distributed control and embedded controller with the smart grid test bed. All aspects of fault and attack scenarios can be verified experimentally in the hybrid power system while being integrated with the communication and multi agent control platform to investigate vulnerabilities introduced into the modern power system as a cyber-physical system. The goal of this investigation and study is to develop new methodology and rules for designing a security aware power system distribution networks as resilient cyber physical systems.