Areas that need to be considered while designing CPS-CDC.

Background / Current Situation

Cyber security of the power grid - encompassing attack prevention, detection, mitigation, and resilience - is among the most important R&D priorities today. The ongoing threat to our national cyber-physical infrastructures, including Supervisory Control and Data Acquisition (SCADA) systems, demonstrates the need for professionals trained in the science, as well as the art, of cyber defense, computer and network security, and cyber-physical system protection. By leveraging Iowa State's PowerCyber testbed and the ISEAGE platform, we can provide a high-fidelity, real-time, scalable cyber-physical infrastructure to enable realistic attack-defense as a unique, first-in-the-nation CPS-CDC promoting inquiry-based learning.

Iowa State's ISEAGE has long hosted Cyber Defense Competitions. Cyber Defense Competitions are a chance to learn and teach about practical Information Assurance in a fast-paced and real-world environment. Teams of competitors are given a limited amount of time to build and secure a network that provides required services. These networks are then attacked by a team of experienced intrusion specialists whose only goal is to compromise these networks, and even bring them down. Teams are scored based upon the security of their networks, quality of their documentation, usability of their systems (as scored by competition guests on the Green Team), and their participation in other fun events during the course of the competition. (From ISU INFAS Student Group). As PowerCyber has grown over the years the interest along with the importance of SCADA systems have grown and in an effort to spread knowledge and interest in SCADA systems the CPS-CDC idea was born.

Current PowerCyber System Overview

The PowerCyber testbed provides a realistic electric grid control infrastructure based on a combination of physical, simulated, and emulated components. The testbed integrates industry standard control software, communication protocols, and field devices combined with power system simulators to provide an accurate representation of a cyber-physical grid. We are continuing to improve the testbed to provide numerous cyber-security and power system research capabilities. Continued improvement of the PowerCyber testbed will provide better demonstration and information regarding cyber vulnerability assessment, attack impact analysis, and cyber-physical system studies.

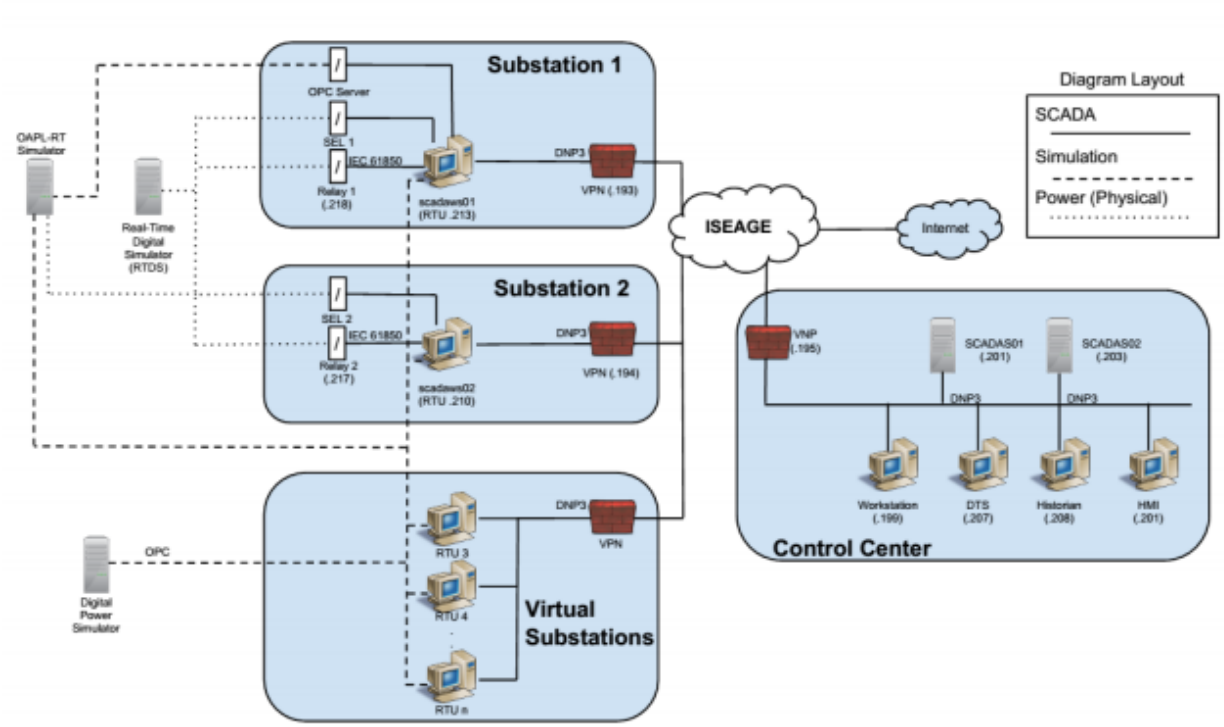
The SCADA system can be broken down into key components:

Control Center: An interface designed for human operators to view simulation data and control testbed processes.

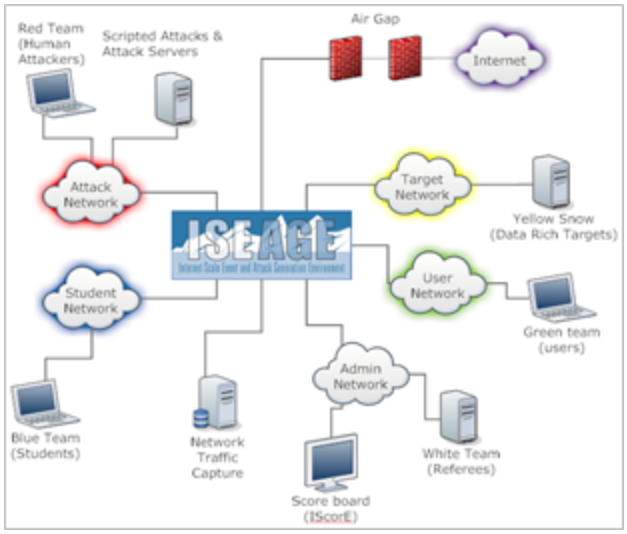
Supervisory Station: Servers, software and stations responsible for providing communication between the Control Center and the RTU's.

Remote Terminal Unit (RTU): The RTU's in this testbed are both physical and emulated. The RTU is used to convert electrical signals from hardware sensors to digital data which is collected by the supervisory station and processed by the real-time digital simulator.

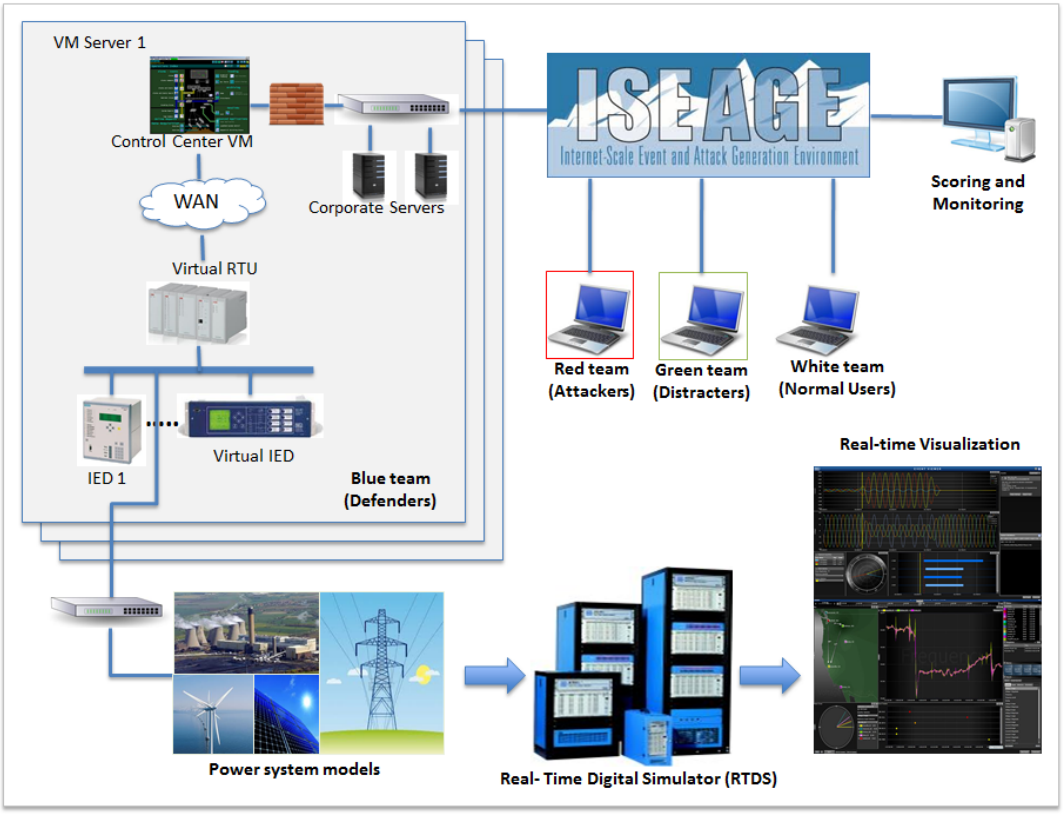
Sensor: A device that measures an analog or status value in some element of a process. Sensors collect the raw process data used to make decisions about the system.



Current CDC System Overview



Operating Environment



The above layout is one of several proposed designs

Requirements

Goals for CPS-CDC

1. Enhance knowledge of students studying cyber security to protect smart grid.
2. Develop a framework to integrate cyber-physical components into the CDC model.
3. Develop scenarios, real-time anomalies, visualizations, score board & learning modules
4. Creation and Dissemination of inquiry-based CPS-CDC modules to other universities.

Features of CPS-CDC

1. Cyber-Physical System integration
2. High-fidelity, real-time, HIL power system simulators included in CDC
3. Realistic Attack-Defense exercise: discovery of new vulnerabilities, security best practices.
4. Interdisciplinary research, education, training, outreach, and workforce development.

Green Team

With just a simple SCADA network there is not much of a role for Green team to play. Because of this the idea of rolling in some of the more traditional aspects of the CDC comes into play. By also adding some of the traditional services that the Blue team needs to host it creates an actual

sizable amount of work and use for a Green team. Right now the Green team is involved with the SCADA network simply in the sense that they could be involved with making sure that all of whichever model is being used works. In addition to general use anomalies involving SCADA will need to be developed.

Red Team

When designing the CPS-CDC it needs to be kept in mind what the red team will be able to attack, to actually make this a competition. For the Red Team we need to be able to offer the ability for more than simple man in the middle attack. Additional methods of attacks to consider will be discussed at a later time. While the Red team will still be able to attack services in the tradition, but the focus need to be held on the SCADA attacks. Keeping with traditional CDC red team be will be required to capture flags that the Blue team had to secure on their SCADA system.

Blue Team

There has been a lot of discussion in terms of what the blue team would be responsible for in terms of SCADA systems. At least in terms of beginning stages of the CPS-CDC blue teams would be responsible for just a subsystem. It was decided that giving a team a full SCADA system would be to much for them to learn right away, largely because there are very few that have actually worked with SCADA systems before. As the CPS-CDC evolves it could be decided that students have become familiar enough with the SCADA environment that teams would be able to handle a full SCADA environment. Blue team would also be responsible for services that they have always been responsible for during a CDC.

SCADA System

The follow will dive into the overall design and use of the SCADA system throughout the CPS-CDC. Topics covered will type of control systems used, scenarios, types of attacks, configuration of the network for the competition. Due to considerations in cost and scalability, the SCADA system and network will need to be heavily virtualized; however, this will be discussed in greater detail later. To start consider part of the core of the SCADA system, the control software. PowerCyber traditionally uses Siemens Power TG, this can be used for the CPS-CDC, but it would be advised to switch it up from competition to competition. The idea behind using products other than Power TG is that it provides students the opportunity to learn more than one system. An option to consider for an alternative to Power TG is openSCADA. This document will not spend much time discussing the use of openSCADA because it is much more a forward looking idea than what currently needs to be expressed. For those interested more information on openSCADA can be found at http://openscada.org/.

One of the largest discussions was what the blue team would be responsible for in terms of a SCADA environment. As mentioned in the blue section it was decided at least early on in the evolution of the CPS-CDC that the blue team should only be responsible for one SCADA substation as opposed to being responsible for an entire SCADA system. This decision was made because of the assumed lack of SCADA knowledge on the blue team side.

To improve scalability, the SCADA environment must be virtualized.

Learning SCADA

The CPS-CDC will be a first of its kind because of this it can be implied that a large number of students that make up the blue team will be unfamiliar with SCADA. One of the large focuses of the CDC has always been the advancement of knowledge and this is no different with the CPS-CDC. The focus on learning and the general lack of knowledge leads to a need to assisted learning of the SCADA systems. Traditional CDC have provided plenty of resources of learning and the CPS-CDC will be no different. Because of the lack of knowledge the availability of these resources will need to much higher. It has been decided that providing resources through the following will provide the most benefit to blue teams: online tutorials, open forums, SCADA workshops, online chat help room. There is also the possibility that a handful of the red team member will also not have SCADA experience which means that we will also have to provide red team focused learning experiences.

Scoring of CPS-CDC

The CDC already has a well-developed scoring system known as IScorE. IScorE INFORMATION FOR PRESENTATION HERE. THEN TALKING ABOUT WHAT NEEDS TO BE ADDED.

Risk/Mitigation

Risk	Mitigation
Since the CPS-CDC is the first of its kind, a large number of students will be unfamiliar with SCADA systems.	Provide online tutorials, open forums, SCADA workshops, and an online chat help room to educate participants in the CPS-CDC
System needs to be easily scaled as the CPS-CDC grows in size.	Use virtualized environments so specialized hardware is not required.

Definitions

SCADA - Supervisory Control and Data Acquisition

Smart Grid - Electrical grid that uses information and communication technology to gather and act on information

Testbed - A platform for simulation of large developmental projects that cannot be experimented on in

their real world/implemented versions

ISEAGE - Internet-SCale event and Attack Generation Environment

PMU - Phasor Measurement Unit

RTDS - Real Time Digital Simulator

Citations

http://www.opal-rt.com/

http://www.wecc.biz/Pages/Default.aspx

http://info.deterlab.net/

http://www.nerc.com/Pages/default.aspx

http://www.ferc.gov/

https://cdc.iseage.org/

http://www.iac.iastate.edu/iseage/