**Abstract** - Electric power grid is a complex cyber physical system (CPS) that forms the lifeline of modern society, and its reliable and secure operation is of paramount importance to national security and economic vitality. Cyber security of the power grid — encompassing attack prevention, detection, mitigation, resilience, and deterrence — is among the most important R&D priorities today. Iowa State's PowerCyber testbed provides a unique cyber-physical integration for bulk power system wherein, vulnerability analysis, system impact studies, risk assessment, and attack-defense evaluations are being carried out. Also, it has potential to offer high-fidelity, highly-scalable, remotely accessible, and federated environment for cyber security experiments.

**CPS Security Testbed – What do we have?**

<table>
<thead>
<tr>
<th>Capabilities</th>
<th>Architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Vulnerability Assessment</td>
<td>SCADA DB</td>
</tr>
<tr>
<td>- System Impact Analysis</td>
<td>Operator Display</td>
</tr>
<tr>
<td>- Risk Assessment</td>
<td>Application Server</td>
</tr>
<tr>
<td>- Risk Mitigation Studies</td>
<td>Web Server</td>
</tr>
</tbody>
</table>

**Salient Features**

1. **Cyber-in-the-Loop Real-Time Simulation** environment modeling bulk power system for cyber security experiments.

2. **Scalability:**
   - Real-Time simulators, RTDS/Opal-RT, provide ability to simulate large power systems with monitoring, protection, control functions.
   - Multi-area, substation architecture enabled through virtualization.

3. **High Fidelity:**
   - Industry-grade SCADA/EMS and substation automation.
   - WAN emulation using ISEAGE; DNP3 and IEC61850 protocols used for SCADA; Industry-grade security appliances for VPN/firewall.
   - Local/wide-area control and protection applications emulated with programmable IEDs and PMUs interfaced with RTDS/Opal-RT.

4. **Remote Access**: Web-based access for remote experimentation with custom power/cyber system models and attack templates.

**CPS Security – What can we do?**

- **Vulnerability Assessment**
  - Vulnerability assessment of field devices (relays, IEDs, PMUs), protocols, automation software
  - Penetration testing
  - Responsible vulnerability disclosure

- **Risk Assessment and Mitigation**
  - Risk = Threat * Vulnerability * Impacts
  - Risk Assessment & Risk Mitigation
  - Model: Advanced Persistent Threats (APT)
  - Security Investment Analysis

- **Attack-Defense Evaluations**
  - Generation of stealth attack vectors
  - Quantification of system impacts
  - Evaluation of mitigation schemes

**Case Study: Attack on Remedial Action Scheme**

**Real-time Monitoring**

**Threat and Vulnerability Analysis**

**Impact Analysis**

**Defense Measures**

- **High risk**
- **Low risk**

- **Data integrity attack to trip R1 + DoS on RAS controller; R2 trips due to thermal overload; Instability; Load shedding**

**Industry Partners**

- SEL
- RTDS Technologies
- Siemens
- Mu Dynamics

**NSF Grants:** CNS-0915945, ECCS 1202542