The goal of the CPS security training is to provide practical scenario-based hands-on learning experience for the participants in cyber-attack-defense methodology for smart grid using industry-grade SCADA platform and state-of-the-art security practices and tools.

**Objective**

- Cyber Attack-Defense Evaluation
- Vulnerability Assessment
- Systems Impact Analysis
- Security Product Testing

**Use Cases**

- Hardware-in-the-Loop CPS Training (WAMPAC and SCADA)
  - Industry-grade SCADA/EMS and Substation platform
  - GNS3-based and ISEAGE-based WAN emulation; DNP3 and IEC-61850 SCADA protocols; Industry-grade cybersecurity software systems.
  - Wide-area control and protection applications interfaced with Hardware-in-the-Loop (HIL) CPS Testbed including Opal-RT/RTDS.

2. **Scalability, Modularity and High Fidelity:**
   - RTDS/Opal-RT provide ability to simulate large power systems with control and protection functions in real-time.
   - Multi-area substation architecture enabled through virtualization.
   - Testbed-based federation for smart grid applications.

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

**Advanced CPS Security Training**

**Training Modules**

**Applicable NERC CIP Standards**

<table>
<thead>
<tr>
<th>Training Modules</th>
<th>Applicable NERC CIP Standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module 0: Introduction</td>
<td>CIP – 004: Personnel and Training</td>
</tr>
<tr>
<td>Module 1: Network Scanning</td>
<td>CIP – 0010: Configuration Change Management and Vulnerability Assessments</td>
</tr>
<tr>
<td>Module 2: Vulnerability Assessment</td>
<td>CIP – 0010: Configuration Change Management and Vulnerability Assessments</td>
</tr>
<tr>
<td>Module 4: Defense: Firewall configuration</td>
<td>CIP – 003: Security Management Controls</td>
</tr>
<tr>
<td>Module 5: AttackSurface Host Analyzer (AHA)</td>
<td>CIP – 005: Electronic Security Perimeter(s)</td>
</tr>
<tr>
<td>Module 7: Attack-Defense case studies</td>
<td>CIP – 010: Configuration Change Management and Vulnerability Assessments</td>
</tr>
</tbody>
</table>

**Year**

- 2015/2016: GridSecCon 2015, GridSecCon 2016, EPRC
- 2017: MidAmerican Energy Company, CIPCO, Cedar Falls Utilities

**Cybersecurity for Smart Grid**

Learning Outcomes

- Ability to identify and analyze attack vectors to the grid environment
- Ability to use modern cybersecurity tools for attack-defense such as network reconnaissance, vulnerability assessment, firewall configuration, intrusion detection/prevention.
- Ability to perform scenario-based risk analysis
- Ability to perform impact characterization for cyber-attack scenarios