Motivation & Objective

**Motivation**
A hardware-in-the-loop testbed provides an economic real-time simulation platform for cyber physical system (CPS) vulnerability & impact analysis, modern CPS security technologies validation and evaluation, and can greatly assist the R&D of novel resilient Wide Area Monitoring, Protection and Control (WAMPAC) functions for smart grid.

**Objective**
- Construct hybrid CPS testbed with satisfactory performance in terms of of accuracy, scalability and cost.
- Implement possible cyber threats, analyze and evaluate power system vulnerabilities & impacts.
- Develop and test novel countermeasures at both cyber layer and physical layer to validate the efficacy and resiliency.

Testbed Architecture

**ISU PowerCyber Testbed**
Provides a unique cyber-physical integration for bulk power system with high-fidelity and high-scalability.

**Critical Components**

- **Physical layer**
  - RTDS
  - Opal-RT simulator

- **Cyber layer**
  - Siemens EMS/SCADA
  - Relays/PMU
  - iSERINK
  - Web-based remote access
  - Federation potential

CPS Security of WAMPAC

**Remedial Action Scheme (RAS)**
Coordinated attack Impact analysis

**Automatic Generation Control**
Model-based ARC design

**Ukrainian Attack (2015)**
Replication of a real attack

R&D Applications

- Vulnerability Assessment
- System Impact Analysis
- Risk Assessment
- Risk Mitigation Studies
- Attack-Defense Evaluations
- Security Product Testing Education & Industry Short Course
- Guidance for NERC CIP compliance

Several Early Users

<table>
<thead>
<tr>
<th>Organization</th>
<th>Use Case</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pacific Northwest National Lab</td>
<td>CPS security of AGC study and Attack Resilient Control (ARC) design.</td>
</tr>
<tr>
<td>accenture</td>
<td>Validating Alert Correlation Engine (as part of Anomaly Detection System) in a realistic ICS environment.</td>
</tr>
<tr>
<td>Symantec</td>
<td>Validating Siemens/ICSC Anomaly Detection System (AD) in a SCADA environment.</td>
</tr>
<tr>
<td>John Hopkins University</td>
<td>Novel IPS design based on PLC/DNP and TCP packet features considering varying CPU load levels.</td>
</tr>
<tr>
<td>University of Minnesota Duluth</td>
<td>CPS experiment sessions of an EE graduate course.</td>
</tr>
</tbody>
</table>