CPS: Synergy: High-Fidelity, Scalable, Open-Access Cyber Security Testbed for Accelerating Smart Grid Innovations and Deployments

Iowa State University

PI: Manimaran Govindarasu NSF Award # CNS 1446831 PMs: Dr. Corman (NSF), Dr. Massey (DHS)

CLIENT: Symantec **Collaborator : Preeti Agarwal,** preeti_agarwal@symantec.com

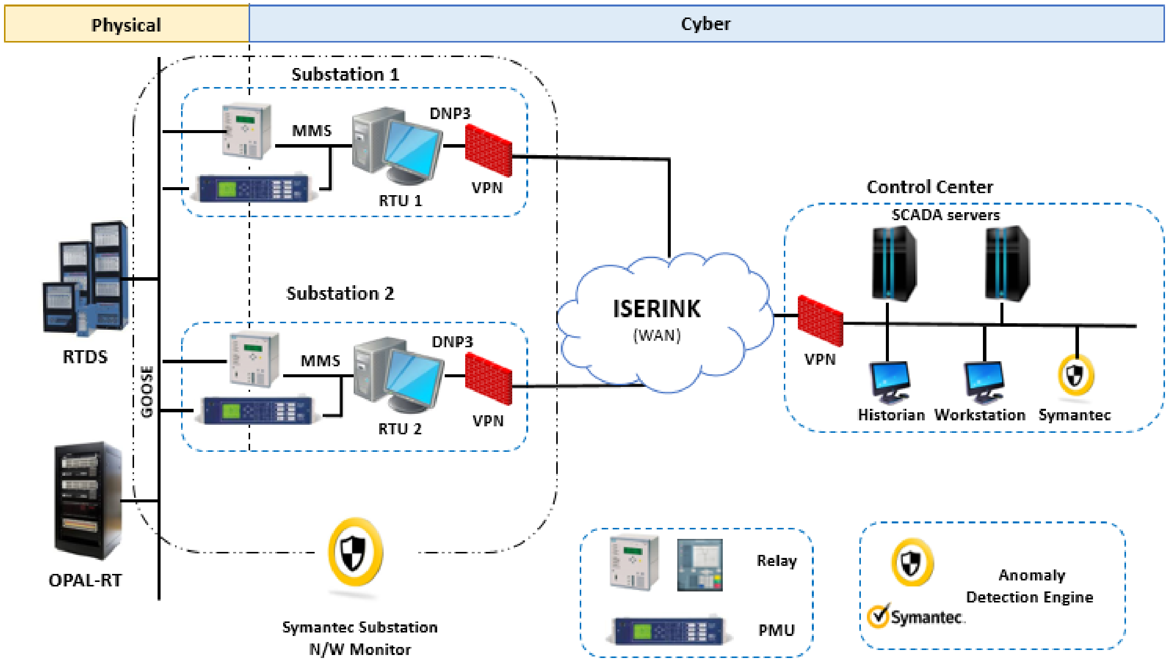
User Goal

- ✓ **Validating Symantec ICS Anomaly-Detection System (ADS) in a SCADA environment**

Approach

- ✓ **Integrating Symantec ADS product within ISU's PowerCyber testbed**
- ✓ **Executing test-plan by remotely accessing testbed**
- ✓ **ISU team to assist Symantec team in testing and evaluation**

Deployment Topology



Outcome

- ✓ **ICS-ADS product testing and evaluation results**
- ✓ **Trained to profile normal and anomalous SCADA traffic using network traffic monitoring**

CPS: Synergy: High-Fidelity, Scalable, Open-Access Cyber Security Testbed for Accelerating Smart Grid Innovations and Deployments

IOWA STATE UNIVERSITY

PI: Manimaran Govindarasu NSF Award # CNS 1446831 PMs: Dr. Corman (NSF), Dr. Massey (DHS)

CLIENT: accenture
High performance. Delivered.

Collaborators: Dr. Amin Hassanzadeh, amin.hassanzadeh@accenture.com
Dr. Malek Ben Salem malek.ben.salem@accenture.com

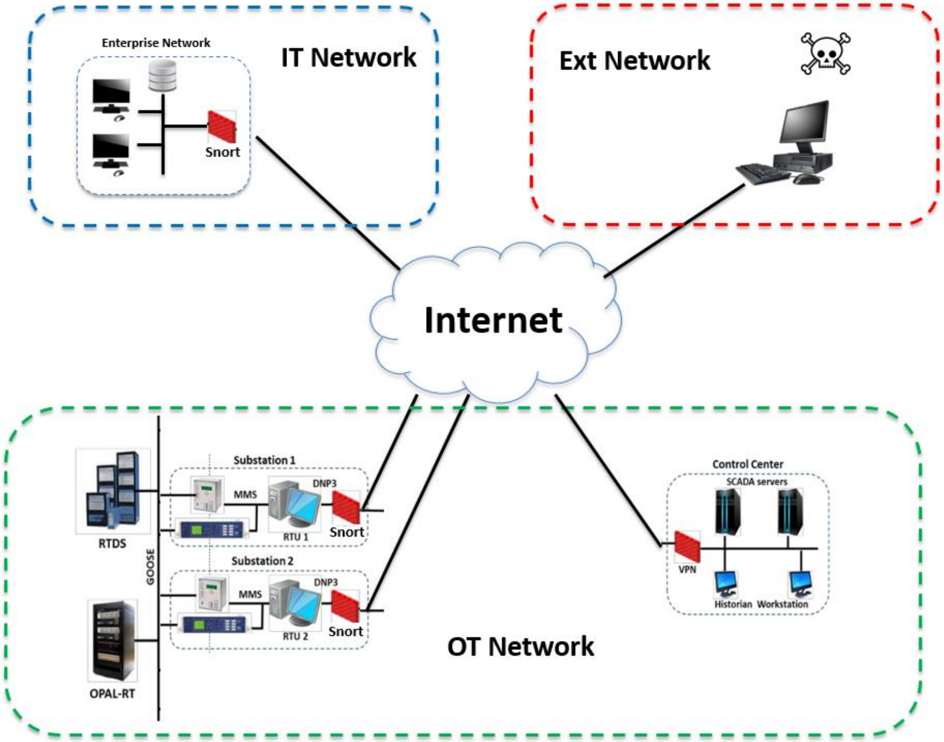
User Goal

- ✓ **Validating Alert Correlation Engine (as part of Anomaly Detection System) in a realistic ICS environment.**

Approach

- ✓ ICS topology with separate IT, OT and External networks.
- ✓ Realistic attack scenarios that include accessing the OT network through the IT network.
- ✓ ISU team contributed to Accenture's goal in design, implementation, and execution of scenarios.

Deployment Topology



Outcome

Datasets (system logs, firewall logs, IDS logs) that contributed to the design and evaluation of Alert Correlation Engine. Students have gained valuable experience working with industry professionals.

CPS: Synergy: High-Fidelity, Scalable, Open-Access Cyber Security Testbed for Accelerating Smart Grid Innovations and Deployments

IOWA STATE UNIVERSITY

PI: Manimaran Govindarasu NSF Award # CNS 1446831 PMs: Dr. Corman (NSF), Dr. Massey (DHS)

CLIENT: Pacific Northwest NATIONAL LABORATORY *Proudly Operated by* Battelle *Since 1965*

Collaborators: Dr. David McKinnon, Dr. Siddharth Sridhar, Aditya Ashok

User Goal

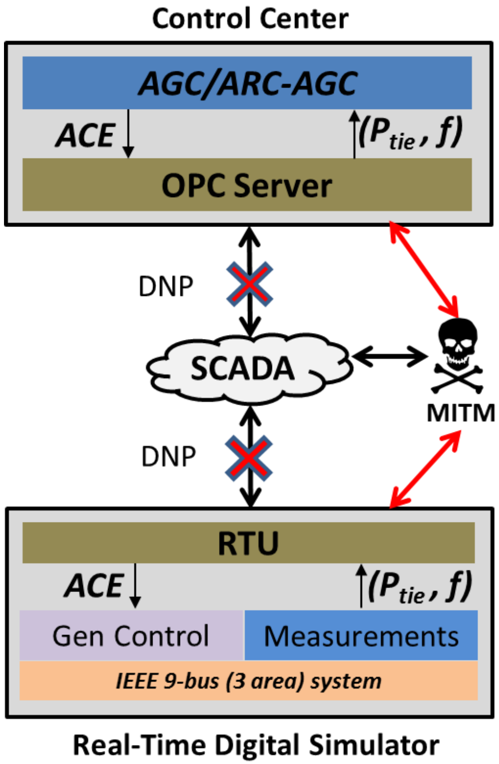
✓ **Validating Attack-Resilient Control (ARC) algorithm for Wide-Area Control on a realistic testbed environment.**

Approach

✓ **Implemented the ARC algorithm on the PowerCyber testbed.**

✓ **Performed realistic cyber attack experimentation involving a typical Man-in-the-Middle attack manipulating AGC measurements.**

Implementation Architecture



- Control center – RTU communication used DNP3 protocol.
- Man-in-the-middle (MITM) attack performed using ARP spoofing.
- Attack modified AGC measurements between control center and RTU.
- Attack injected malicious frequency and tie-line flow measurements based on stealthy attack vectors.

Outcome

✓ **Performance evaluation of ARC on the testbed validated earlier simulation-based studies.**

✓ **Experimental results were published in Resilience Week 2016. Paper awarded 'Best Paper Award.'**

CPS: Synergy: High-Fidelity, Scalable, Open-Access Cyber Security Testbed for Accelerating Smart Grid Innovations and Deployments

IOWA STATE UNIVERSITY

PI: Manimaran Govindarasu NSF Award # CNS 1446831 PMs: Dr. Corman (NSF), Dr. Massey (DHS)

CLIENT: JOHNS HOPKINS UNIVERSITY

Collaborator: Dr. Lanier Watkins, lanierwatkins@gmail.com

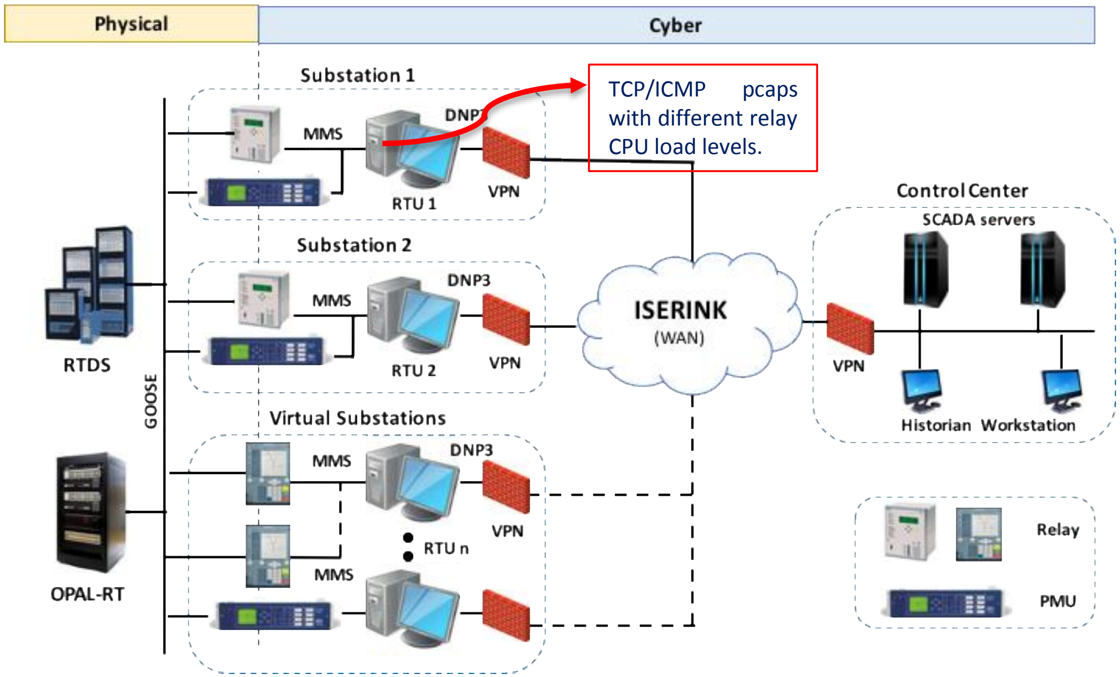
User Goal

- ✓ **Novel IPS design based on PLC ICMP and TCP packet features considering varying CPU load levels.**

Approach

- ✓ **Configure the EMS/SCADA system with specific SIEMENS RTUs and relays located at the substation.**
- ✓ **Configure the relay with CFC charts such that relays can have different CPU usage levels.**
- ✓ **ICMP data collected on the RTU side are delivered as raw data source.**

Deployment Topology



TCP/ICMP pcaps with different relay CPU load levels.

Outcome

Datasets (mainly PLC pcaps captured under different PLC CPU load levels) are delivered and the effectiveness of IPS algorithm has been well verified.

CPS: Synergy: High-Fidelity, Scalable, Open-Access Cyber Security Testbed for Accelerating Smart Grid Innovations and Deployments

IOWA STATE UNIVERSITY

PI: Manimaran Govindarasu NSF Award # CNS 1446831 PMs: Dr. Corman (NSF), Dr. Massey (DHS)

CLIENT: UMD UNIVERSITY OF MINNESOTA DULUTH Driven to Discover	COLLABORATOR: Dr. Desineni Subbaram Naidu dsnaidu@d.umn.edu
Engagement Goal Experimentation on cyber-attack impact characterization on power grid using remote interface to PowerCyber testbed	**UMD Course** Course: EE5533 Grid: Resiliency, Efficiency & Technology Level: Graduate Background: Electrical Engineering Number of Students: 14
Approach ✓ Presenting an overview about CPS Security for UMN-D Smart Grid class ✓ Introducing Power Cyber testbed with architecture details ✓ Providing overview of Remote access framework with user interface guide	**Lab Assignment** ✓ Experimenting cyber attack impact characterization – quantify power flow, voltage, frequency ✓ Performing cyber-attacks on different power system models – a Wide Area Protection Scheme ✓ Experimenting different types of attacks on each model – Coordinated attacks (DoS, data integrity)

Students Learning

✓ Identifying most impactful cyber attack by comparing pre & post attack values on power system.