Cyber Physical Substation Security: Insights from Real Time Digital Simulation

Michael Breuhl, RE&S

Senior Engineer

Southern Company

RTDS APPLICATIONS & TECHNOLOGY CONFERENCE

2026 APPLICATIONS & TECHNOLOGY CONFERENCE

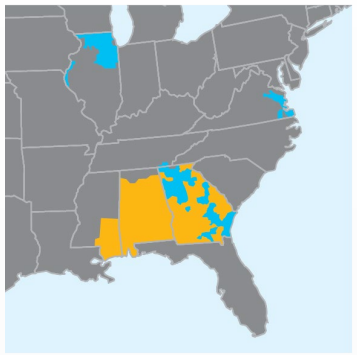
IRWINDALE, CALIFORNIA, USA

RTDS Technologies

AMETEK

Southern Company

We provide clean, safe, reliable, affordable energy and customized solutions

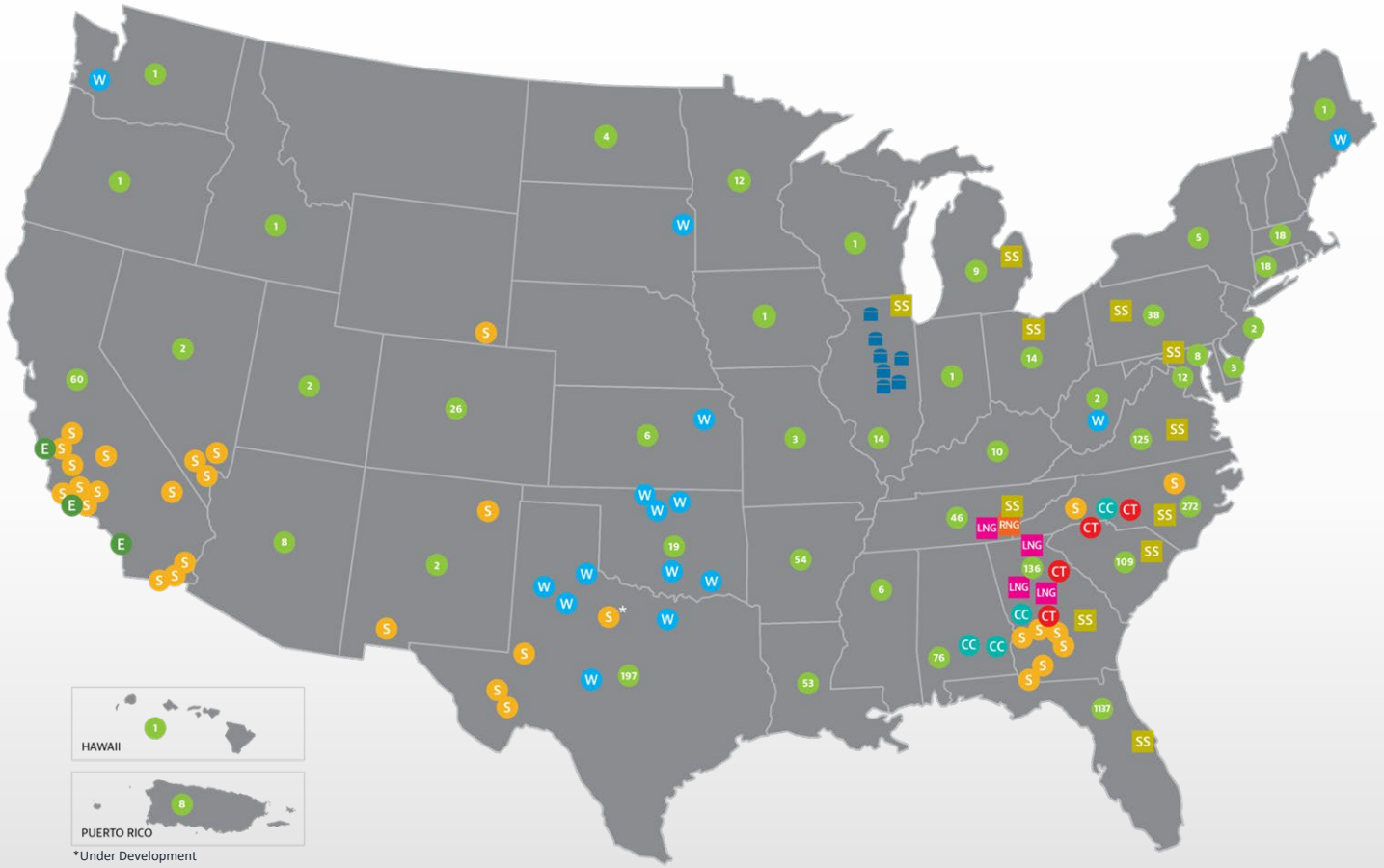


Service territories

- Electric
- Gas

Gas pipelines

- Southern Natural Gas
- Southern Company Gas



*Under Development

Southern Power

- Combined-cycle facility
- Peaking facility
- Solar facility
- Wind facility
- Energy storage

Southern Company Gas

- LNG facilities
- SouthStar
- Natural gas storage
- Renewable natural gas

PowerSecure

- Owned and/or managed sites per state

7
Electric & Natural Gas Utilities

9 Million
Customers

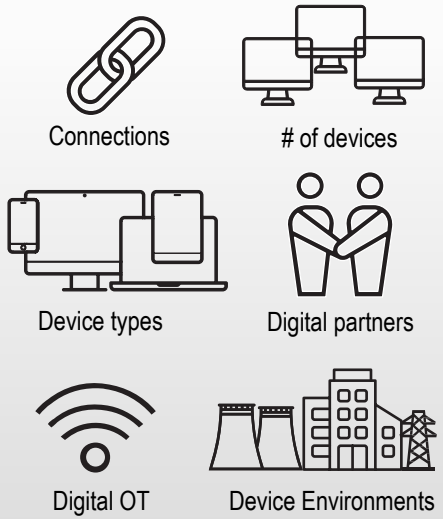
More than
28,000
Employees

Approximately
45,000 MW
of Generating Capacity

The Threat Landscape Facing US Electric Utilities

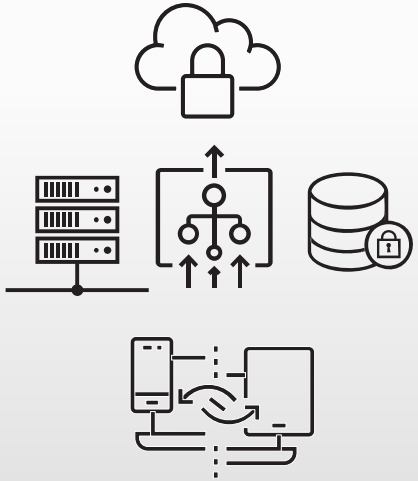
Nation State Cyber Attacks

Expanding Attack Surface



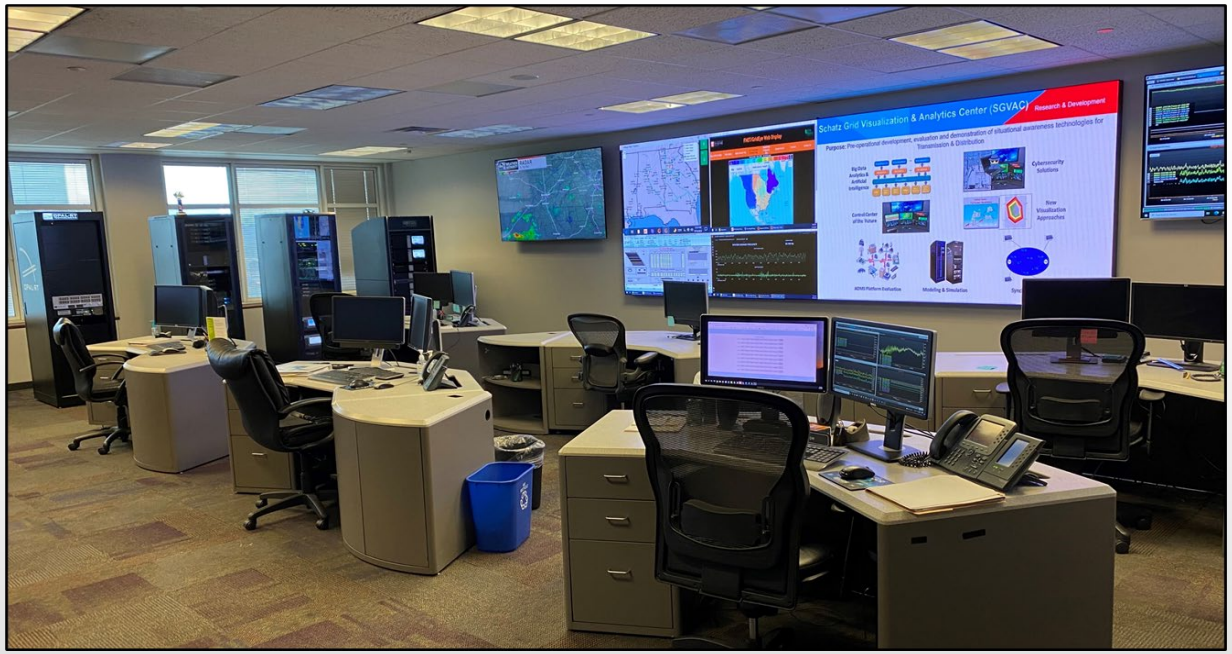
Attacks on critical infrastructure are no longer theory

Increasing dependency on technology and connectivity

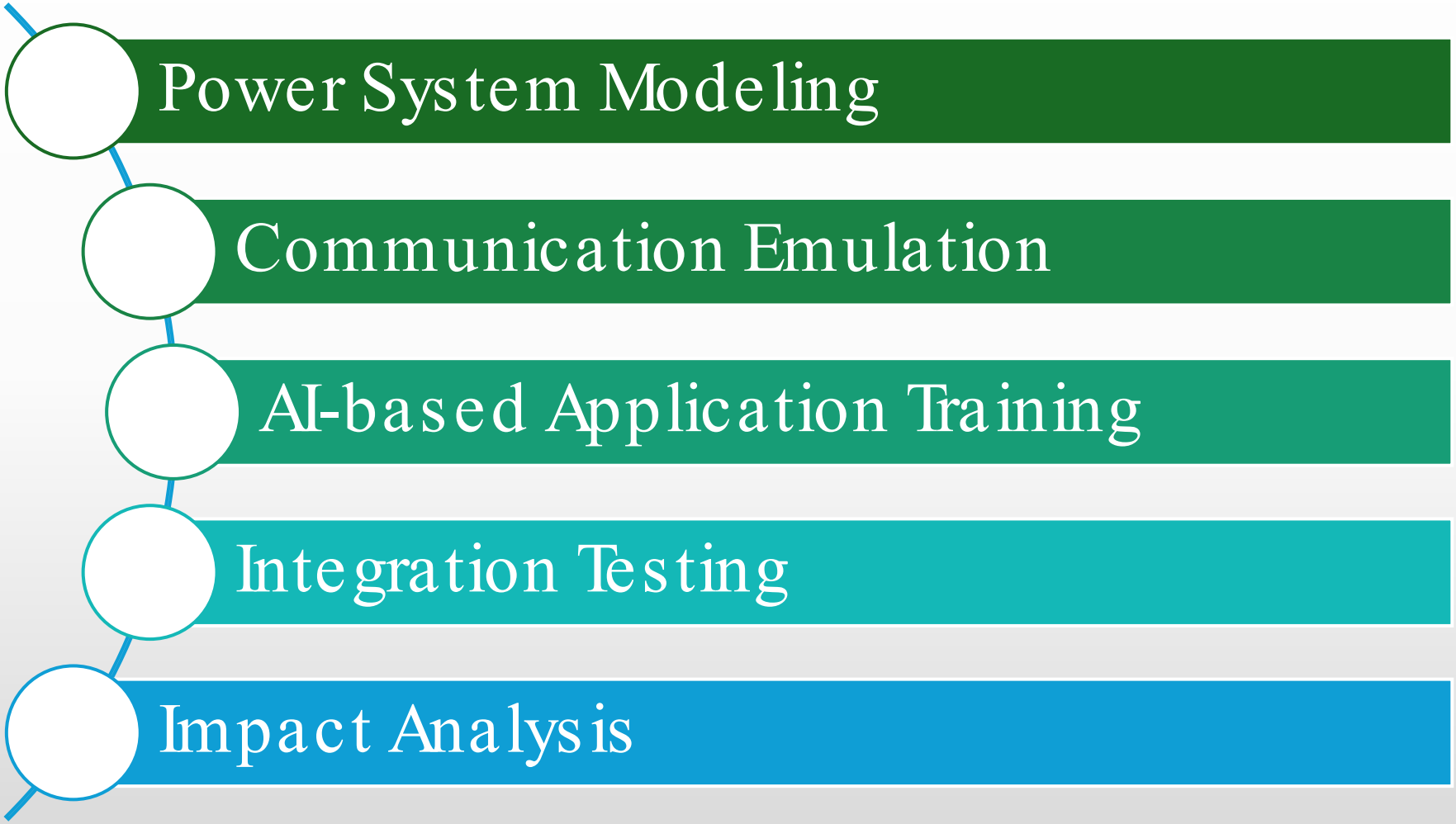


Schatz Grid Visualization & Analytics Center (SGVAC)

Secure innovation environment for pre-operational development, evaluation and demonstration of situational awareness technologies for Transmission & Distribution

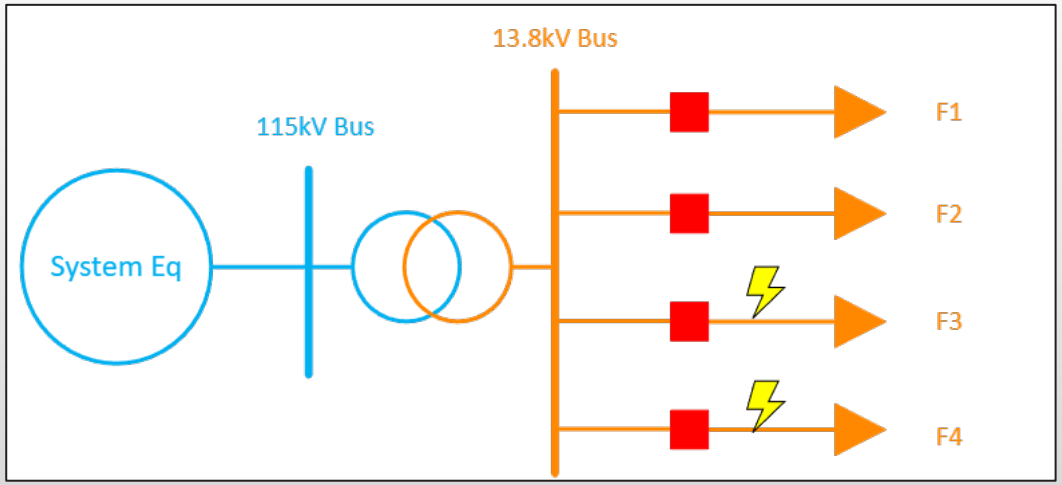


Real Time Simulation Benefits



Power System Modeling

- Needs
  - Emulate real systems
  - Generate complex waveforms
  - Automate scenario testing
- Uses
  - Digital twins
  - Equipment testing
  - High-risk operating scenarios
- Learnings
  - Existing models
  - Equipment parameters

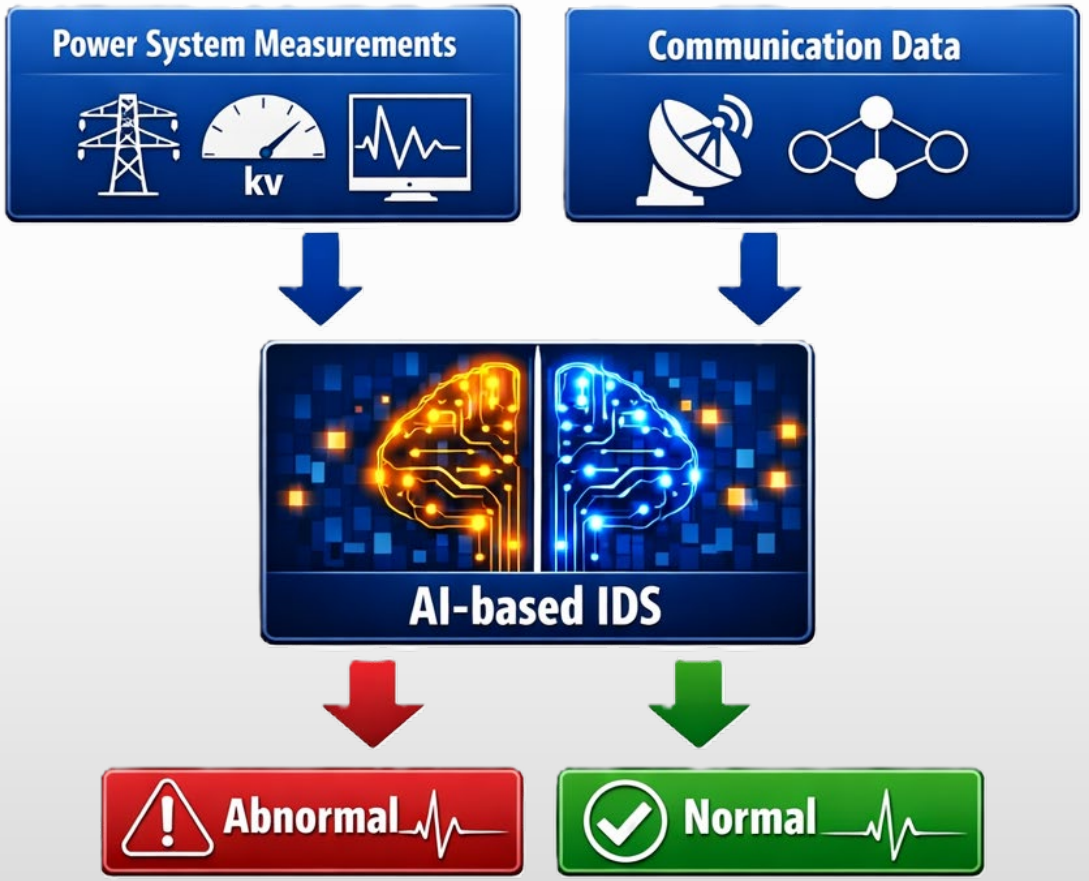


Communication Emulation

- Needs
  - Validate equipment behavior
- Uses
  - Enable cyber-physical simulations via HIL
  - Recreate substation environment
- Learnings
  - Lab versus field deployments
  - Substation requirements
  - Equipment configuration

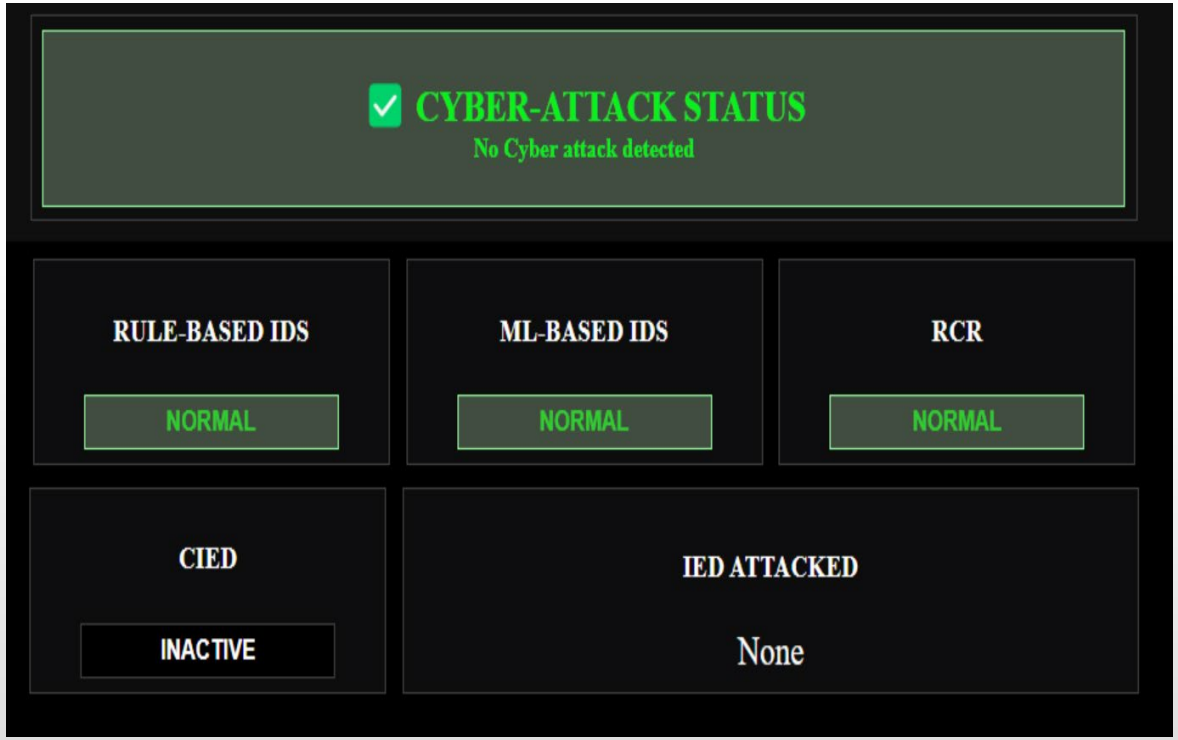
AI-Based Application Training

- Needs
  - Managing increased grid complexity
  - Understanding what is abnormal vs normal
- Uses
  - Inform AI applications
  - Validate AI applications
- Considerations
  - Role of AI
  - Acceptable error
  - Data Availability
- Gaps
  - Various substation configurations

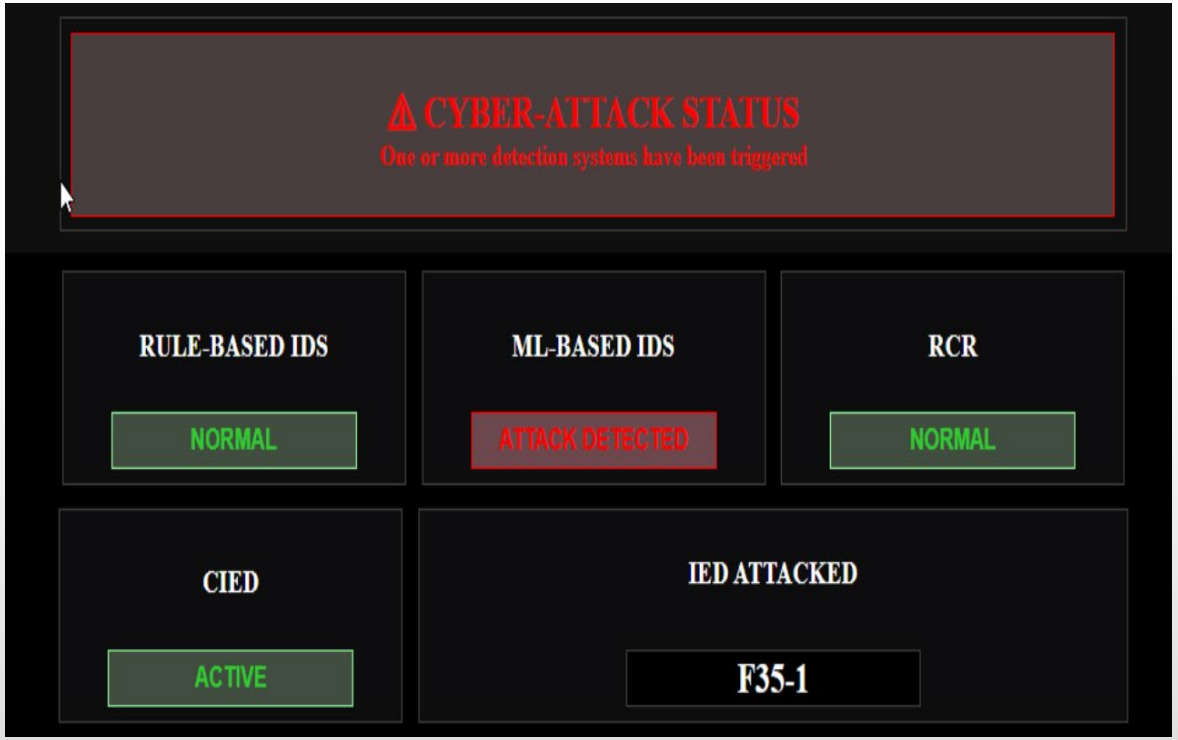


AI-Based IDS Example

Normal Operation

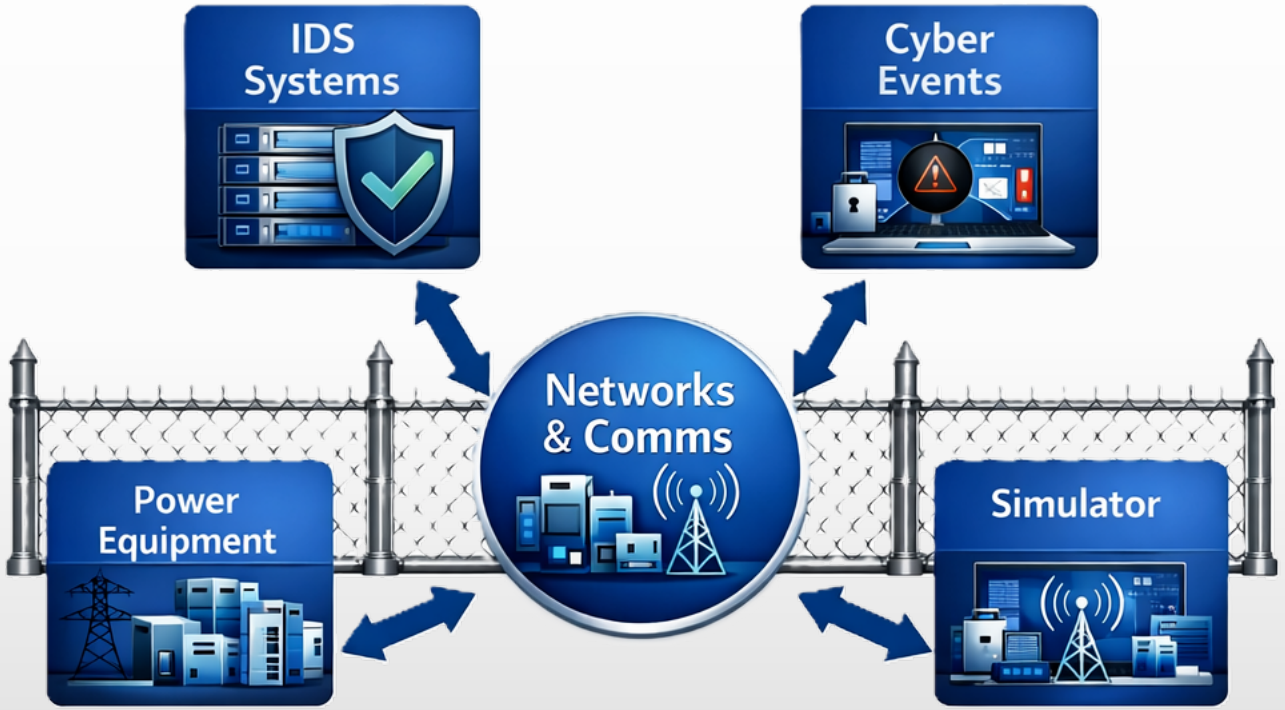


Attack Detection, Mitigation & Recovery



Integration Testing

- Needs
  - Closed, Controlled Environment
  - Limit impact to real grid
- Uses
  - Stress testing equipment
  - Identifying operational/functionality gaps
- Considerations
  - Field vs Lab
  - Stakeholder Engagement
  - Architecture Needs



Impact Analysis

- Needs
  - Evaluate high-risk scenarios
  - Identify technology limits
- Uses
  - Understand cyber attack impacts
  - Develop mitigation and restoration strategies
- Considerations
  - System conditions
  - Adequate scenario analysis
  - Automation approaches are valuable

Key Takeaways

- RTDS enables complex cyber-physical technology evaluation
- Cross-collaboration is required in the cyber-physical space
  - Operational scenarios
  - Stakeholder needs
  - Lab vs field considerations


Southern
Company