GridStat Middleware Communication Framework: Application Requirements

Overview and Problem Statement

GridStat is a middleware framework architecture tailored for power system data delivery. Power system applications set specialized requirements in terms of delay, rate, availability, etc., and GridStat needs to be tested and validated to meet the specific application requirements. Communication requirements also need to be investigated for conventional SCADA and PMU-based wide-area network systems. Cyber-physical test cases need to be developed for such validation and testing. Developed test cases can also be utilized for cyber-physical vulnerability analysis.

Research Objectives

- Understand the real-time communication requirements for wide-area power system applications for the emerging smart grid.
- Develop a technical approach to assess those requirements.
- Develop a testbed integrating a power grid, sensors, communication, and applications to create real-life scenarios to validate the GridStat middleware communication and other communication architecture.
- Conduct cyber-physical vulnerability analysis with incomplete data availability.
- **Smart Grid Application Area:** Vulnerability analysis, wide-area applications, and real-time simulation.

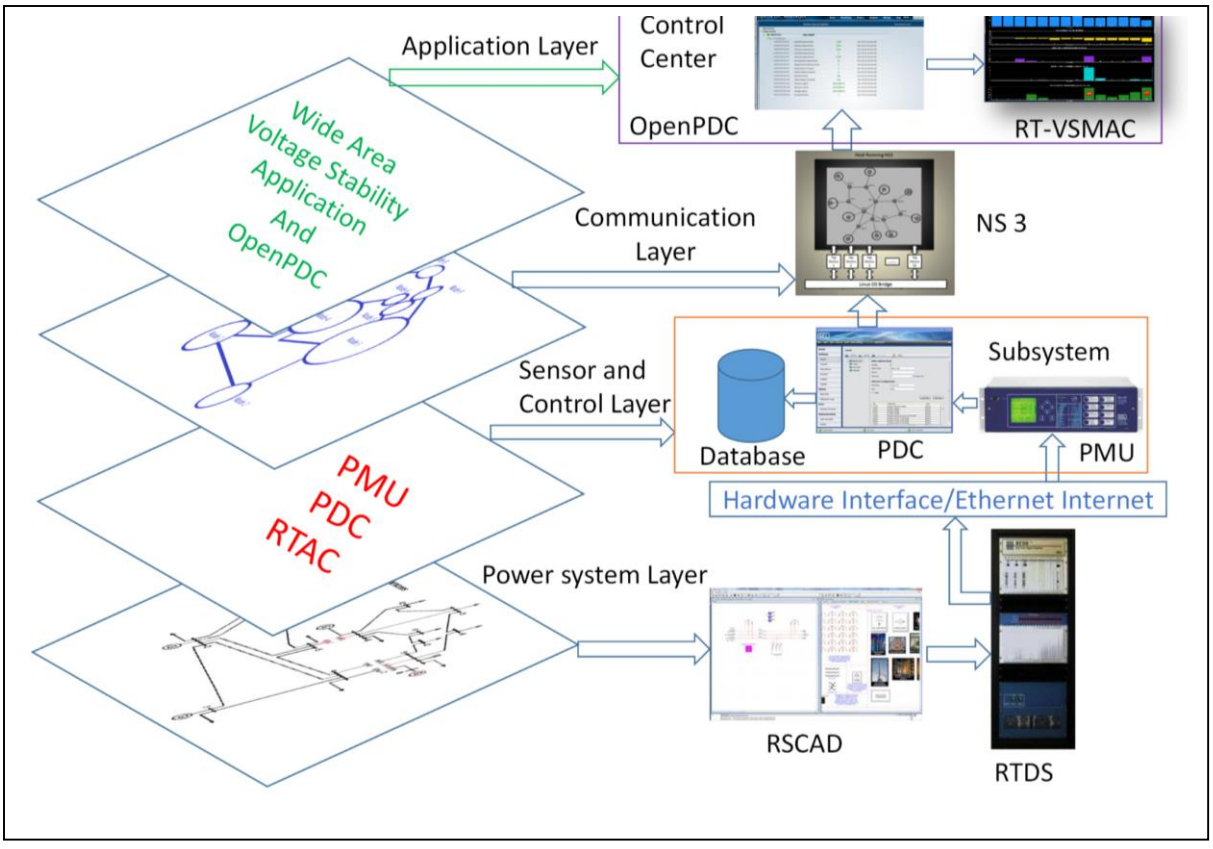

Fig. 1: Integrated Cyber-Power Simulation with Real Time Digital Simulator and Communication Emulator

Technical Description and Solution Approach

- A real-time testbed has been developed using a real-time digital simulator (RTDS) to interface with communication emulator NS-3 and a real-time voltage stability application, as shown in Fig. 1. Interfacing with DeterLab and GridStat is in progress.
- In addition, integrated modeling and simulation in real time using Power Tech software and GridStat have been developed. (This part of the effort is separately funded by DOE.)
- Graph theory-based vulnerability indices for the power grid are being used to analyze multiple contingencies with limited information. Developed vulnerability analysis indices have been integrated with cyber vulnerability indices for integrated cyber-physical vulnerability analysis.
- Cyber vulnerability analysis and attack models for man-in-the-middle attacks, denial of service attacks, and communication line outages have been analyzed using the developed testbed.

Results and Benefits

- RTDS-based testbed development is in progress (partially funded by TCIPG). Communication emulator NS-3 has been interfaced to deliver the data from physical and simulated sensors to wide-area voltage stability applications.
- Cyber vulnerability index has been integrated with graph theory-based physical vulnerability indices given incomplete information. Developed cyber-physical vulnerability indices have been validated for standard IEEE test systems with Aurora-like attacks.
- A real-time man-in-the middle-attack (MITM) has been simulated using the developed testbed. Additional cyber attacks will be modeled and analyzed using the developed testbed.
- DeterLab has already been integrated into the developed testbed to replace NS-3 to emulate the communication network. With the communication features supported by DeterLab, we are able to observe and interact with real malicious software, operating in realistic network environments at scales found in the real world.
- Development of cyber-physical training simulator using the cyber-physical vulnerability index and integrated cyber-physical simulation is in progress.
- Partnerships and External Interactions: Prof. Saman Zonouz, Rutgers University; Prof. Thomas Morris, Mississippi State University; Prof. Thoshitha Gamage, Southern Illinois University.
- **Technology Readiness Level:** Research in progress.

Researchers

- Carl H. Hauser, hauser@eecs.wsu.edu
- David E. Bakken, bakken@eecs.wsu.edu
- Anurag K. Srivastava, asrivast@eecs.wsu.edu

Industry Collaborators

- SEL
- RTDS