TCIPG

Trustworthy Cyber Infrastructure for the Power Grid

CONES – Converged Networks for SCADA

tcipg.org

Overview and Problem Statement

The CONES project is a TCIPG activity exploring many aspects of network convergence as they apply to power grid cyber networks. Many currently deployed cyber-communications systems in the electric sector consist of multiple communication networks and devices to carry out communications. That is an expensive and inefficient approach, but trying to achieve convergence simply by replacing those channels with a single high-bandwidth connection would also create problems. Those problems include the inability to segregate channels, guarantee timings, and enforce network entry limitations. CONES attempts to address those problems using as much off-the-shelf hardware and software as possible, augmenting them with specialized components when necessary. This project has already been successful in identifying and solving several of the problems in this space, and is actively transferring the knowledge gained to various industry partners. At the same time, CONES research is continuing to explore and refine more convergence techniques.

Research Objectives

- Enable network convergence for control system applications (e.g., SCADA, monitoring, engineering).
- Explore and understand networking needs for existing and future electric sector communication networks.
- Provide solutions to problems not currently addressed.
- Identify best practices and off-the-shelf technologies for convergence in the electric sector.
- **Smart Grid Application Area:** Communications technology.

Technical Description and Solution Approach

- Work with research, government, and industry partners to identify current needs in communications networks, and examine trends in equipment requirements to identify future networking requirements.
- Compare the gathered requirements and data on modern communication networks, identifying solutions or partial solutions for use in the electric sector. This step will also identify areas in which new solutions are needed in order to meet the requirements fully.
- Create solutions, based on minimal customization of off-the-shelf components, that will meet the identified needs of the electric sector. This process includes not only building technology, but also vetting it with current equipment manufacturers' compliance issues and technical issues previously unknown to the researchers.

Results and Benefits

- Soft-real-time process and network scheduling in Linux kernel: this gives devices the ability to report even under duress.
- Identification of a realistic traffic profile in electric sector communications networks, for future research.
- Identified many security concerns for electric sector communications, particularly if they are converged.
- Created many software tools useful to the wider TCIPG research mission.
- **Partnerships and External Interactions:** Entergy, PNNL, GPA, TVA, NASPI.
- **Technology Readiness Level:** Lessons learned and techniques already being transferred; software results currently in use in other research.

Researchers

- Erich Heine, eheine@illinois.edu
- Tim Yardley, yardley@illinois.edu
- Klara Nahrstedt, klara@cs.uiuc.edu

Industry Collaboration

- Grid Protection Alliance

funded by the U.S. Department of Energy and the U.S. Department of Homeland Security