TCIPG

CONES: Converged Networks for SCADA

Erich Heine, Tim Yardley, Kate Morrow

Goals

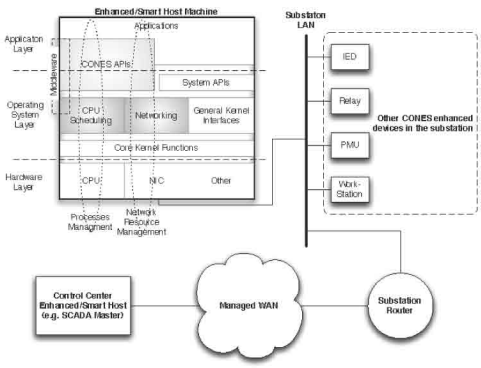
The CONES project is a TCIPG activity exploring many aspects of network convergence as they apply to power grid cyber networks. Many currently deployed cyber-communications systems in the electric sector consist of multiple communication networks and devices to carry out communications. That is an expensive 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 these 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.

Fundamental Questions/Challenges

- What are the traffic properties of power grid communications networks?
  - Traffic flows.
  - Packet patterns between devices.
  - Bandwidth requirements.
  - Timing requirements.
- Does COTS equipment meet the requirements?
- Can COTS equipment and software be minimally customized to do so?
- What is the best convergence plan for the electric sector?

Research Plan

- Working with industry, government, and research partners, gather information about traffic in networks.
  - Identify packet frequency, size, paradigm (e.g., one-way, request-response, etc.), and timeliness concerns.
  - Validate our model of traffic with our partners.
- Create tools to emulate the power grid network communication profile.
- Create a testbed to examine various COTS systems.
- Identify best approaches for convergence by testing various equipment in the testbed.
  - Also identify shortcomings!
- Develop and test customizations to software that can address identified shortcomings.



Research Results

- Created traffic generation tool emulating SCADA and other power grid data flows.
- Created a soft-real-time stack for Linux with process and network guarantees.
  - Systems running this CONES-enabled kernel perform better than stock kernels under various forms of resource contention.
- Submitted a technology report to DOE.
- Paper in ISGT 2011.
- Knowledge dissemination within TCIPG and to research partners.

Broader Impact

- Lessons learned and technology understanding applied to projects with:
  - GPA.
  - Entergy.
  - DOE.
- NASPI involvement with input to the DNMTT working group.
- Provides data for shaping future communication and convergence efforts.

Interaction with Other Projects

- Traffic generation tool transferred to greater TCIPG Lab efforts.
- Networking stack available for other researchers in TCIPG.
- General domain knowledge applied to several TCIPG projects.
- Follow-up work by graduate students for master's theses.

Future Efforts

- Continuing tech transfer to partners and researchers.
- Better data-gathering tools for understanding various communication networks in the electricity sector.
- Porting CONES stack to lightweight and embedded systems.
- Better lab integration of CONES tools.