Technology Transition Case Study

Trustworthy Cyber Infrastructure for the Power Grid (TCIPG)

1. Case Study Context

TCIPG (www.tcipg.org) is a project funded by DOE and DHS under DOE Cooperative Agreement award number DE-OE000097 at a level of $18M ($15M federal funding, $3M cost share). The period of performance is September 30, 2009 – August 30, 2015. The partnership includes the University of Illinois at Urbana-Champaign (lead institution) with partner institutions Arizona State University (previously UC Davis), Dartmouth College, and Washington State University.

TCIPG's technical focus is cyber security and resiliency of the power grid, with research activities combining disciplines of computer science, computer engineering, electric power, education, and economics. Research addresses multiple issues in cyber-physical resiliency in generation-transmission, distribution, vehicle-to-grid integration, demand response, synchronization of wide area measurements, and demand response.

TCIPG has no investors. Benefits to the technology transfers that benefit the taxpayer include:

- A commercial tool to assess security of utility networks by identifying routable paths to critical cyber assets (the tool is NP View and is the portfolio centerpiece of the startup Network Perception (www.network-perception.com)).
- A Pilot deployment in real-world utility environments of innovative technologies to secure Advanced Metering Infrastructure (AMI)
- The open-source transition (in the BRO framework) of security tools that detect attacks against SCADA protocols, considering cyber and physical aspects of the defended system
- Prototypes to secure device firmware that have transitioned into vendor products
- Outreach to the sector in the form of an annual workshop, a bi-annual summer school, and a modular training course to advance workforce and faculty development
- Emphasis on results and in developing roadmaps, standards, guidelines, best practices, and policy recommendations.
- Workforce training: student researchers, internships, post-doctoral fellowships, industry participation in the biannual summer school, and placement of graduates in industry and laboratories.
- Outreach to K-12 and to the public promoting issues of security awareness and "smart energy" on the part of consumers

2. Partnership Formation

TCIPG follows from the NSF-funded TCIP project, which dates to 2005. At that time, awareness of cyber security and resiliency in grid systems (and in control systems in general) was low, and the term "smart grid" was not in wide use. The partnership was formed from a team of academic researchers with a shared vision for the importance of research in this area, and a commitment to producing impactful results by early

Prepared by the leadership of TCIPG in response to formal guidance and a request by Sam Baldwin, Ellen Williams and Charles Russomanno of the U.S. Department of Energy (DOE) for input into the DOE Industrial Consortia Initiative and the 2015 DOE Quadrennial Technology Review.

involvement of industry. From the TCIPG standpoint, “industry” consists of utilities (investor-owned as well as cooperatives) and system vendors (who sell technology to the utility sector). At a high level, interaction involves:

- Identifying needs in security and resiliency (in consultation with utilities and vendors)
- Developing solutions
- Validating solutions in a utility setting, leveraging testbeds for technology development, validation, and risk mitigation.
- Technology transition, as licensed technologies, startups, open source, and training

An ongoing challenge to research in this sector is the sensitivity of utility operational data. We have addressed this through NDAs, through analysis on air-gapped systems, through data collection on utility test systems, through data anonymization, and mainly by earning the trust of the sector through our reputation for responsibility and integrity.

Although the partnership, strictly defined, consists of the four member academic institutions, TCIPG also partners with industry in the form of technology demonstration and deployment, student internships, workshops, and training. Some of our collaborative relationships include Schweitzer Engineering Laboratories (SEL, a leading vendor of substation equipment, and a generous donor of equipment to the TCIPG testbed), Ameren (validation of the predecessor of NP View, interaction on substation security research), FirstEnergy (AMI Security), and American Transmission Company (PMU data quality and security), and the Association of Illinois Electric Cooperatives (various outreach efforts), among others.

The partnership is funded by DOE and DHS under DOE award number DE-OE000097.

In addition to TCIPG, Illinois has synergistic projects funded by DOE in partnership with SEL, ABB, EPRI, and the Grid Protection Alliance. These are not as broad in scope as TCIPG, but take a deep, focused look at specific topics of interest, such as software defined control networks in utilities and the security of time-critical distributed substation protection schemes. TCIPG has also partnered with the DOE National Laboratories on topics such as quantum key distribution (with Sandia) and integration of NP View with the INL Sophia visualization tool.

3. Partnership Governance

TCIPG is led by the University of Illinois at Urbana-Champaign. Professor William H. Sanders, head of Illinois Department of Electrical and Computer Engineering (ECE), is the overall PI. He is supported by Co-PI’s Professor Pete Sauer, a leading authority on power systems, and Professor David Nicol, who heads the Information Trust Institute (ITI) at Illinois. Site leads at respective academic partner institutions are Professor Carl Hauser (WSU), Professor Anna Scaglione (Arizona State University), and Professor Sean Smith (Dartmouth). Professor Scaglione and her team are transitioning from UC Davis in January 2015. The leadership team also includes Mr. Alfonso Valdes (Managing Director, Smart Grid Technologies), Mr. Tim Yardley (Associate Director, Testbed), and Ms. Cheri Soliday (Research Program Manager), all from the University of Illinois. This leadership team meets weekly via teleconference.

Prepared by the leadership of TCIPG in response to formal guidance and a request by Sam Baldwin, Ellen Williams and Charles Russomanno of the U.S. Department of Energy (DOE) for input into the DOE Industrial Consortia Initiative and the 2015 DOE Quadrennial Technology Review.

TCIPG participates in formal quarterly technical reviews with both funding agencies. These alternate between teleconference and in-person meetings.

TCIPG has an External Advisory Board (EAB) that participates in quarterly reviews and serves as a resource for identifying critical sector needs as they evolve. The current advisory board consists of:

- Dennis Gammel, SEL
- Marija Ilic, Carnegie Mellon University
- Jeff Katz, IBM
- Himanshu Khurana, Honeywell
- Doug McGinnis, Exelon
- Scott Mix, NERC
- Paul Myrda, EPRI
- David Norton, FERC
- William Souza, PJM

The EAB was formed by identifying and recruiting thought leaders and stakeholders involved in technology, management, or research that supports electricity delivery and energy control systems.

The EAB is supplemented by a larger Industry Interaction Board (IIB) composed of industry stakeholders who participate in TCIPG events such as the annual workshop, the summer school, or monthly seminars. While TCIPG actively recruits the EAB, stakeholders may request to join the IIB.

4. R&D Execution

TCIPG is divided into technical clusters addressing resiliency and trust in wide area systems (generation and transmission, including wide area measurement systems such as PMUs), local area (distribution, AMI, home area networks), cyber event management and response, and trust assessments. We have cross-cutting thrusts focused on education and workforce development, industry interaction and technology transition, and research analysis and validation with an advanced cyber-physical testbed facility. Research activities are identified from industry interaction, the EAB, or anticipation of cyber security issues that are likely to emerge as smart grid or EDS technology evolves.

Research activities typically consist of a faculty research lead and one or more student researchers. As an academic consortium, an important output of our effort consists of publications in conferences and journals, as well as student theses and dissertations. We also actively seek opportunities to validate our solutions in realistic utility environments, which is not typical of an academic consortium. For example, our pilot deployment of the AMIlyzer AMI security technology has been in place at First Energy for two years, and has grown in that time from 12,000 to 50,000 meters monitored.

The entire team meets most weeks via an All-Hands teleconference, which typically consists of technical presentations from student, faculty, or visiting researchers. In addition, student researchers meet in a weekly reading group to develop cross-discipline knowledge and understanding of computer and power engineering as it applies to power grid cybersecurity.

Faculty and student researchers are encouraged to collaborate closely with industry at all stages of research, forming what an advisory board member has termed the “engagement journey.” Industry stakeholders are invited and encouraged to participate in our Annual Industry Workshop and serve as part of our Industry Interaction Board. These efforts have resulted in numerous opportunities for pilot technology deployments, as well as synergistic projects with individual industry partners.

The leadership and senior researchers meet periodically to plan project direction, and we hold workshops with sector stakeholders to identify gaps and research needs. One outcome of our leadership-researcher meetings is an internal research activity proposal mechanism, where researchers have their ideas vetted by the cluster lead and the senior leadership.

5. Partnership Results

TCIPG support has contributed to a variety of technologies that are in some stage of transition to the sector, via licensing, pilot deployment, and open source. Some examples include:

- Startups Network Perception (NP View; www.network-perception.com) and River Loop Security (ZigBee security, applicable to home area networks)
- Software to secure Linux embedded systems kernels . These are part of the architecture for the kernel security solutions in new SEL products, and are in parallel being transitioned through the GPL parth.
- Security of SCADA protocols using protocol specification and real-time systems state, open sourced in the BRO security framework.
- AMILyzer for security of AMI, in pilot deployment at First Energy.
- Open-source training for security in utility systems.
- Patents applied for in secure time synchronization of wide area measurement systems

We recommend that the government retain government-use rights to developed IP, while the partner institutions retain commercial rights. We routinely enter NDAs with industrial partners as appropriate, although this typically addresses confidentiality of sensitive data rather than jointly-developed IP.

6. Lessons Learned

TCIPG has been successful by following its vision of leading-edge research with real-world impact. This has been achieved by involving industry early, and maintaining ongoing contact through all stages of research effort. We have learned that different solutions call for different transition models. In an academic consortium, it is important to establish relationships with university tech transfer organizations (for example, the Office of Technology Management at Illinois). For an academic consortium, the existence of an associated technology incubator (i.e., EnterpriseWorks at Illinois) is useful in the early stages of a startup.

The following are aspects of TCIPG that have been critical to its success:

- Multi-university consortium
- Research activities organized into clusters led by senior faculty, complemented with cross-cutting research efforts
- External Advisory Board
- Activity proposal process that resulted from our 2012 Summer Retreat
- Reading Group/Student Development
- Quarterly Review of research activities
- Mechanisms to deliver Industry guest lectures, and to arrange visits to industry by faculty and students
- Internships by students to industry, Industry hiring graduates
- Collaboration with other organizations such as PSERC, FREEDM, CURENT
- Teaming with industry on responses to FOAs. Engage industry early and often.

The following are some suggestions for a new consortium of this type. In some cases, they present changes from what TCIPG presently does. In others, they consist of increased emphasis on the more effective practices TCIPG currently follows.

- Expand scope of impact for research (i.e., broader energy sector or critical infrastructure (CI))
- Agile teaming, in which the core consortium can be augmented by additional partners and subject matter experts for specific activities as appropriate.
- More effort on specific industry interaction/collaboration, student internship placement/interaction, and technology transfer.
- In our experience, some industry partners desire deep involvement, while others are mostly interested in information. The consortium should develop mechanisms for more meaningful involvement with the former while serving the needs of the latter.
- More gap analysis workshop/working groups that involve utility/industry/CI stakeholders. Outcome of these efforts to result in research activity proposals, internship placements, technology transfer, etc..
- Establish and regularly review/re-evaluate milestones for individual research activities and initiatives.
- Identify more ways to engage industry in testbed efforts, beyond contributing equipment/technology.

Prepared by the leadership of TCIPG in response to formal guidance and a request by Sam Baldwin, Ellen Williams and Charles Russomanno of the U.S. Department of Energy (DOE) for input into the DOE Industrial Consortia Initiative and the 2015 DOE Quadrennial Technology Review.