Critical Infrastructure Cybersecurity Laboratory (CICL)

Technical Details

BCIT’s Critical Infrastructure Cybersecurity Laboratory (CICL) has been designed and developed to provide a utility-grade real-time R&D platform, enabling researchers and educators alike to conduct research and educational programs in power systems, digital substations, smart microgrids, and critical infrastructure cybersecurity applications. This unique installation emulates the required power-flow layer of the desired SuT (System under Test) using HIL (hardware-in-the-loop) emulation, while the command & control layers are implemented using the leading-edge components (Relays, MU, etc.) from industrial partners.

This provides the platform with a unique capability to be used for research, design, and validation of substation architectures, communication protocols, protection schemes, DER integrations, and what-if scenarios related to cyber vulnerability and mitigation strategies of critical infrastructure. In particular, this real-time platform is designed to enable vulnerability studies of critical infrastructure, which includes provisions for initiating, observing, and mitigating various categories of cyberattacks on the grid.

The CICL platform uses an advanced IEC-61850 communication protocol and emulates a fully functional medium voltage substation and a microgrid with various types of loads and Distributed Energy Resources such as PV, BESS, and EV chargers using a Real-time Digital Simulator (RTDS). RTDS enables the lab to fully implement three key levels of substation topology, i.e., process level, bay level, and station level. The lab includes real-field substation protection and controls IEDs such as protection relays, merging units, and fault recorders using IEC 61850 Goose, SMVs, and MMS protocols. The lab is comprised of a real HMI system that is able to control and monitor the whole system in real-time.

With the support of the Future Skills Centre fund, the CICL lab has been recently equipped with advanced virtualization technologies and cloud-based applications. This provides this platform with the tremendous opportunity to be used for remote hands-on training purposes. Using advanced virtualization technologies such as digital twins, and cloud-based dashboard and navigator applications at the cyberspace layer connected to the real-field devices & systems, trainees will be able to get the same level of understanding and experience with physical assets even from their homes.

By offering vocational training remotely, the CICL lab will be of substantial value to Canadian academic institutions, utilities, industries, and specifically to remote and underserved communities that might not have adequate resources to get involved in such training programs in person. In summary, this test platform is now ready to be used for the following aims:

- Providing professional in-person and remote training and educational programs for utility personnel, students, and scholars on critical energy infrastructures, their cybersecurity challenges, solutions, and technologies
- Conducting real-time testing, validation, and emulation of critical energy infrastructure operations such as smart microgrids and modern IEC 61850 compliant substations

- Testing and validating the flexibility of implementing different Substation Automation (SA) topologies and protocols
- Understanding and analyzing potential vulnerabilities and cyber threats to critical infrastructure.
- Developing, testing, and validating mitigation and early warning system solutions and technologies against smart grid cyber vulnerabilities
- Facilitating the development of best practices and cybersecurity regulations to increase Canada's infrastructure's defense potency against cyberattacks

To get more information about BCIT's CICL, please contact:

Dr. Moein Manbachi P.h.D., P.Eng., SMIEEE | Project Leader
Smart Microgrid Applied Research Team, BCIT
T 604.451.6929 | E mmanbachi@bcit.ca