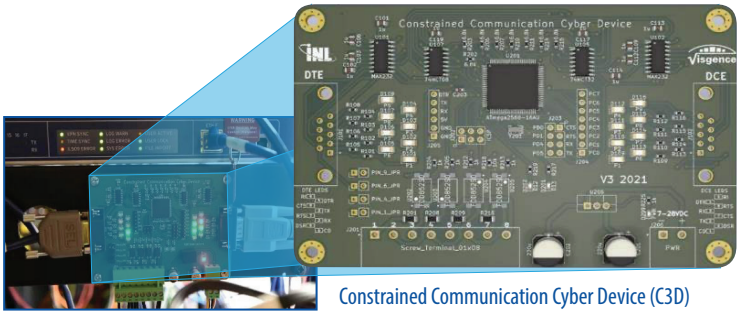
Protective Relay Permissive Communication

Electricity or electrical energy delivered by the power grid is an essential part of modern life and important to the U.S. economy. People use electrical energy for lighting, heating, cooling, and refrigeration and for operating appliances, computers, electronics, machinery, and public transportation systems. One of the most important components of the electric power grid is the protective relay. When equipment fails or under adverse conditions, protective relays protect power systems from damage and blackout. Protective relays act under adverse and faulted conditions on the power grid to prevent loss of life, damage to equipment, and insure stability of the grid. But, sophisticated cyber threats can deceive, alter, or stop a relay from performing its job and ultimately impacting safety of people, equipment, and the economy.



Constrained Communication Cyber Device (C3D)

The Protective Relay Permissive Communications (PRPC) concept is studying ways to transition protective relay equipment to a limited communications state. In a limited communication state, different business functions which provide access to critical relay resources, such as, changes to configurations, software, and firmware are unavailable to remote users while other business process such as operation and monitoring of the relay are uninterrupted. This constrained state represents an additional depth of defense of cybersecurity, while maintaining important business functions for the utility and grid.

Research Proposal: 18-month project & full-scale demonstration at Idaho National Lab's Critical Infrastructure Test Range Complex to test their theory

Challenges

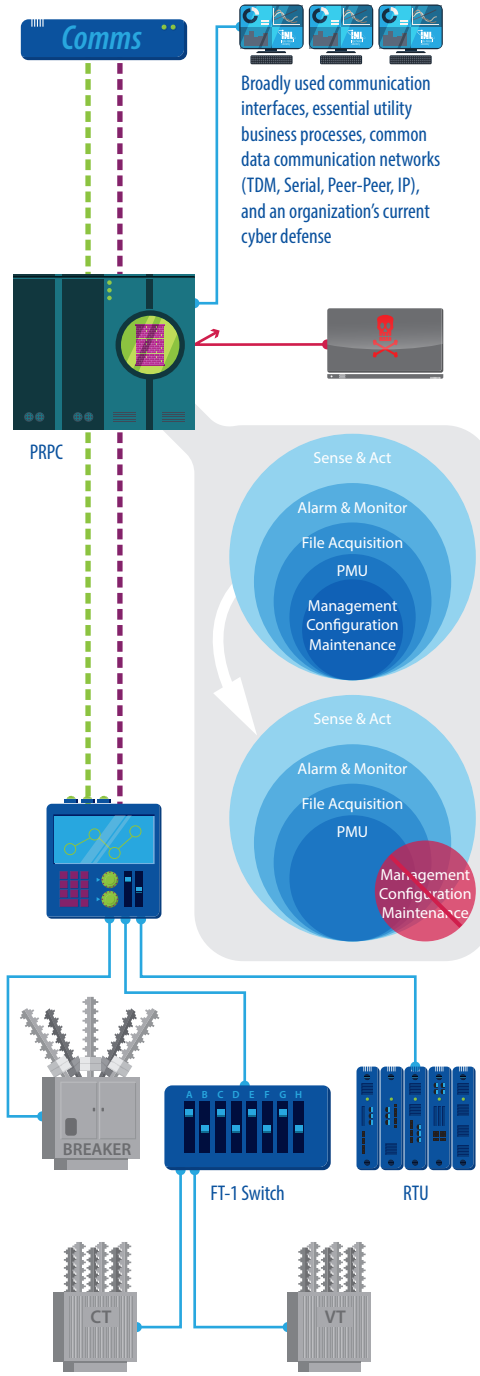
- Multiple device communication architectures
- Multiple implementation designs
- Multiple organizational business practices
- 18-month project with field demonstration

Desired Outcomes

A field deployable solution for the Western Area Power Administration demonstrating a constrained communication state limiting business process and relay configuration and software/firmware updates functions

A broad recommendation to industry on improving cybersecurity depth- of-defense for protective relays, and a simple technology device to support relay owners that has minimal impact to existing CIP requirements

How it works:



Research approach focuses on relays that have legacy serial connections for monitoring and control, and a second type of connection for engineering access

Contact: Jake Gentle – 208.526.1753 – jake.gentle@inl.gov | Stephen Bukowski – 208.526.4364 – Stephen.Bukowski@inl.gov

Idaho National Laboratory