Technology Innovation Project

Closing Project Brief

TIP 397: Cyber Attack Resilient HVDC System – DOE CEDS Initiative*

Context

Because of grid modernization efforts, High Voltage Direct Current (HVDC) is expected to grow far beyond its traditional position as a supplement to alternating current (AC) transmission. HVDC is now the becoming the method of choice for interconnecting asynchronous AC grids, providing efficient, stable transmission and control capability. HVDC is also used for long-distance bulk power transmission because it is able to send large amounts of electricity over very long distances with low electrical losses. HVDC is a key technology in overcoming problems with renewable generation like wind, solar and hydro – that these resources are seldom located near the population centers that need them. HVDC transmission owners and operators must secure these new assets with up-to-date cybersecurity technologies. To do this, the defense of industrial control system devices within an HVDC station and the power system control center should be enhanced.

This will require fast, secure inter-device communication (within and between HVDC substations and control centers), a decision framework that cross-checks device actions for correctness in a particular system state, and swift response to maintain system stability and safety in the presence of malicious or erroneous commands. The determination that a command is malicious or incorrect depends not on conventional cyber intrusion detection methods, but on the consistency with sound engineering principles and the real-time physical state of the underlying mixed AC-DC system.

Description

The project develops a security domain layer that enables HVDC controllers, wide area measurement, protection and control systems, and SCADA/EMS systems to defend against cyber-attacks. We will demonstrate our distributed defense system, having incorporated it into the firmware of HVDC controller, SCADA/EMS applications server, and wide area monitoring based protection and control (WAMPAC) at the BPA testbed.

The focus is on defenses against hacker and insider attacks that aim to disrupt electric power service by maliciously changing HVDC system control device's set points, spoofing spurious power system data, or altering a device configuration, even if commands and data are compliant with respect to syntax, protocol, and targeted device. We leverage and improve upon DNP3, IEC 60870-5-104, MODBUS, and IEC 61850 and related cyber-security standards, which makes our results widely applicable to the energy sector and future proof.

The project had four phases.

Phase 1, Concept Development and Validation: specify the threat models against which the system provides a defense, from the HVDC controller to the SCADA/EMS and WAMPAC utility systems that interoperate with HVDC systems. The models will be expressed in terms of attack trees and verified in hardware in a loop laboratory set up for feasibility. The output of this phase will be the concepts coded and validated in application development platforms and design documents to prepare for prototyping.

Phase 2, Design and Prototyping: Design and prototype robust cyber security systems to achieve the design objectives. The robustness of the developed functions will be tested in a simulated laboratory environment - the goal is to achieve designs with no false positives in real world conditions.

Phase 3, Demonstration: Integration of enhanced HVDC controllers, IEDs, a test harness, and necessary attack and monitoring infrastructure in a realistic utility test environment.

Phase 4, Knowledge Transfer: Transfer will engage ABB HVDC business units to build firmware into control and monitoring devices implementing the developed power system aware cyber security solution, and promulgation of the results to standards organizations for use by the community as a whole. In addition, we will vigorously disseminate findings in the form of journal and conference papers, and presentations at industry forums.

Benefits

Incorrect control of HVDC systems can cause system wide outages and costly interruption to the electric delivery system. The project mitigates such incorrect control, arising from malicious cyber intrusion or operator error, by implementing fast, distributed security framework that intelligently incorporates the physical state of the defended system and blocks incorrect HVDC device actions. We address challenges arising from advanced cyber security measures in systems with stringent real-time requirements.

Accomplishments

The project team developed algorithms that defend against cyber-attacks intended to disrupt electric power service by

maliciously changing HVDC set points, spoofing spurious power system control commands, or altering a device configuration, even if commands and data are compliant with respect to syntax, protocol, and the targeted device. The team designed, improved, and tested the defense system to achieve robust capability in performance with component level validation in a laboratory setting using real time digital simulators. Upon completion, the team demonstrated the system in a utility environment and validated the timing and security aspects.

Deliverables

The results of this research will provide input to standards organizations and support commercially viable products with these features:

- Power system state aware HVDC cybersecurity.
- Implemented and prototyped HVDC, WAMPAC, and SCADA / EMS system security layer.
- Enhanced HVDC controllers, SCADA / EMS servers, and other devices with new firmware to support cyber defense mechanisms.

The products are described in a series of technical reports delivered when the project completed.

These include reports on the following subjects: Threat Modeling; Concepts for Securing the HVDC Station and HVDC Systems; the Defense Mechanism Design; HVDC System Security Layer Design; Prototype Algorithms Implementation; HVDC Security Defense System Test(s); Field Demonstration and Validation Results; Commercialization Plan.

TIP 397: Cyber Attack Resilient HVDC System – DOE CEDS Initiative*

Project Start Date: October 1, 2016

Project End Date: September 30, 2019

For More Information Contact:

BPA Technology Innovation Office
technologyinnovation@bpa.gov

Participating Organizations

BPA leverages its investment in the DOE CEDS initiative by partnering with the following technology leaders:

ABB Inc. (ABB)

University of Idaho (UI)
University of Illinois at Urbana-Champaign (UIUC),
Argonne National Laboratory (ANL)

Related Projects

TIP 289: Wide-Area Damping Control Proof-of-Concept Demonstration

Conclusions:

The project presented a method for checking the operational security of DC power order commands. The method is designed to detect malicious commands from cyber intrusion and/or inadvertent commands from the dispatch center. Testing results in a real time environment suggests that this function is a valuable tool for HVDC operators to thwart malicious commands resulting from cyber intrusion as well as incorrect dispatch orders. Testing in a real time environment using actual HVDC controllers confirms the value of this function in existing HVDC controllers.

* Cybersecurity for Energy Delivery Systems (CEDS)

CEDS projects are funded through the Department of Energy's (DOE) Office of Electricity Delivery and Energy Reliability (OE) research and development (R&D) program, which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of energy disruptions due to cyber-attacks.
For more information Contact:
DOE OE http://energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity