U.S. DEPARTMENT OF ENERGY | OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

Cyber Attack Resilient High Voltage Direct Current (HVDC) Systems

Securing HVDC transmission infrastructure by ensuring received commands do not jeopardize grid stability

Background

Because of grid modernization efforts, 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 can also be used for long-distance bulk power transmission, 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.

Objectives

The project team will develop 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 will design, improve, and test 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 will then demonstrate the system in a utility environment and validate the timing and security aspects.

Project Description

The project will develop a security domain layer that enables HVDC systems to defend against cyber-attacks. Detection is based not on conventional cyber network defense, but on the controllers assessing correctness in the context of a physical power system state, with application of physical laws and engineering principles. The demonstration will include a cyber-attack resilient HVDC system defense scheme in a laboratory environment, and then integrated in a realistic utility test bed.

Benefits

- Detects and mitigates cyber-attacks, in real-time, that seek to destabilize HVDC systems
- Anticipates how the grid would react should a received command be executed and avoids taking any action that would jeopardize grid stability while still executing legitimate commands in time
- Firmware enhancements to HVDC controllers, SCADA/EMS and WAMPAC servers
- Publications and standards recommendations available to the community as a whole

Partners

- ABB, Inc. (lead)
- University of Illinois at Urbana-Champaign (UIUC)
- Bonneville Power Administration
- Argonne National Laboratory (ANL)
- University of Idaho (UI)

Period of Performance

October 2016 – September 2019

Project Cost

Total: $3,018,089

Federal: $2,302,831

Cost Share: $715,258

Content last updated: May 2017

Cybersecurity for Energy Delivery Systems (CEDS)

CEDS projects are funded through the Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) 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 emergency disruptions due to cyberattacks.

For more information: https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/cybersecurity-research-development-and

Initial Leads

Carol Hawk
Program Manager

Reynaldo Nuqui
Principal Investigator
ABB, Inc.
919-807-5039
reynaldo.nuqui@us.abb.com

Current Contact as of Aug. 2020

Akhlesh Kaushiva
Program Manager
DOE CESER
202-287-6062
akhlesh.kaushiva@hq.doe.gov

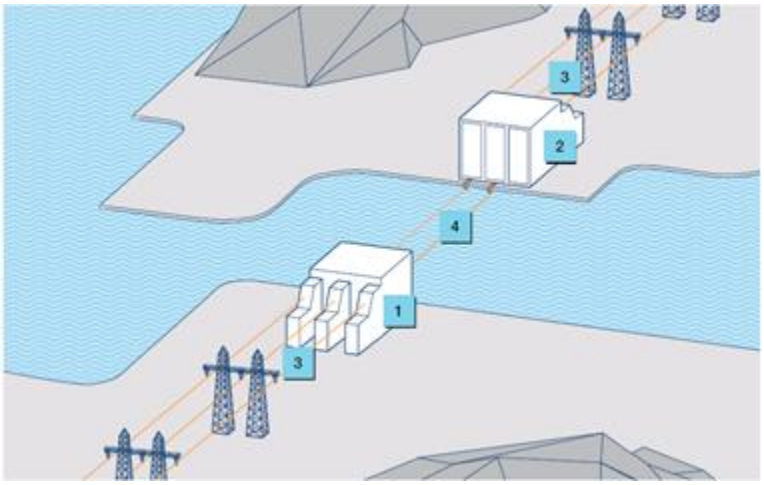

Figure 1. HVDC Diagram. (1) HVDC converter station rectifier, (2) HVDC converter station inverter, (3) AC, (4) DC

Technical Approach

The U.S. national electric grid has more than 20 HVDC installations composed of transmission links and back-to-back systems. Therefore, cybersecurity of HVDC systems and the utility control systems interacting with them is critical to the reliable delivery of energy in the nation's energy infrastructure.

Project innovations include detection of adversarial manipulation by cross-checking commands and configuration changes for consistency with the physical state of the system. This approach does not require additional instrumentation, will be deployable in existing installations, and will be interoperable with communication standards. This project implements a fast, distributed security framework that intelligently incorporates the physical state of the defended system and blocks incorrect HVDC device actions.

Project Phases

The project will be conducted in four phases: concept development and validation, design and prototyping, demonstration, and commercialization planning.

Phase 1: Concept Development and Validation

In Phase 1, the team will specify the threat models that the HVDC system provides a defense against; develop the defense mechanisms using domain-based principles; and validate soundness of the concepts in a simulation environment that captures the dynamics of the HVDC system.

Phase 2: Design and Prototyping

In Phase 2, the defense system will be designed, improved, and tested to achieve robust performance capability. This phase culminates with component-level validation in a laboratory setting with real time digital simulators. HVDC controllers, supervisory control and data acquisition (SCADA)/ energy management system (EMS) servers, and other devices will be enhanced with new firmware to support the defense mechanism.

Phase 3: Demonstration

In Phase 3, the HVDC controllers, wide area monitoring protection and control (WAMPAC) and SCADA/EMS servers, and necessary attack and monitoring infrastructure will be integrated into a utility facility for testing. The demonstration will focus on cyber-attacks that result in maliciously changed control commands such as dispatcher's power orders, spoofed HVDC converter control data, or an intentionally misconfigured HVDC controller.

Phase 4: Commercialization Planning

In Phase 4, the team will build firmware prototypes into commercially available devices to implement the HVDC system defense solution. Research results will be disseminated to standards organizations.

Anticipated Results

Project results will include the following:

- 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.