RTDS Technologies

RTDS NEWS


Training course at TU Delft, the Netherlands

WHAT'S NEW: DECEMBER 2016

RTDS Simulator included in BPA'S HIL test bed for addressing cyber security threats

New functionality added to MMC valve models — and other new features in RSCAD V5

Upcoming Training Courses

We are currently accepting registrations for the following courses. **Click here for more details and registration.**

INTRODUCTORY RTDS® SIMULATOR TRAINING

March 13-17, 2017
Winnipeg, Canada

ADVANCED APPLICATIONS TRAINING: VSC-BASED HVDC AND FACTS

March 20-24, 2017
Winnipeg, Canada

Upcoming Events

DistribuTECH 2017

January 31-February 2, 2017
San Diego, California, USA

2017 RTDS Technologies Southern Africa UGM

February 2-3, 2017
Cape Town, South Africa

ACDC 2017

February 14-16, 2017
Manchester, United Kingdom

CEATI Spring 2017 Industry Conference

March 7-8, 2017
Indian Wells, California, USA

GUEST ARTICLE

Mitigating cyber security threats with the collaborative defense of transmission and distribution protection and control devices: the CODEF project

Bonneville Power Administration, DOE, ABB US Corporate Research Center

Cyber security is becoming a major concern among electric utilities fueled in part by increased use of automation in utility operations. The attack on the Ukrainian power grid in December 2015 underlined the need for more distributed security in electrical infrastructure. CODEF, or Collaborative Defense of Transmission and Distribution Protection and Control Devices against Cyber Attacks, is a research project funded by the US Department of Energy under the Cyber Security for Energy Delivery Systems (CEDS) program. CODEF advances the state of the art for cyber defense methods for transmission and distribution grid protection and control devices by enabling them to collaboratively defend against cyber -attacks. It contributes to cyber security using an inter-device level solution for smart detection of cyber -attacks using power system domain knowledge, IEC 61850 and other standard security extensions. CODEF's cyber security solutions are designed to increase the resiliency of electric substations against cyber-attacks by introducing an inner domain based layer within the IT layer that is capable of blocking cyber-attacks. Unlike traditional IT based cyber security solutions that only detects intrusion, the CODEF functions actively blocks malicious attempts to control substation switching equipment. This feature including its intrusion capabilities were demonstrated at BPA (Bonneville Power Administration) using a hardware in the loop set up including an RTDS Simulator. The successful demonstration validated the CODEF functions ability to detect and block dependably and securely malicious cyber-attacks in an electrical substation with speeds commensurate with the secured protection systems.

The Sickler substation selected for the CODEF project is an existing ring bus connecting two transmission lines to a single 500kV/230kV transformer located in central Washington near a high concentration of hydro-power generation. The same class of relays from a single vendor is applied for the protection of the transmission lines and transformer located at Sickler substation. Line protection relays included line differential, line distance, and over current elements. The transformer protection relay included transformer differential and phase overcurrent elements.

To demonstrate a successful cyberattack on an electrical substation and the mitigation methods against such attacks, a hardware-in-the loop (HIL) simulation testbed was used. The demonstrated HIL simulation testbed has the commercially available substation protection, control and communication field devices that are integrated in to a power system model running in a real-time simulated environment. The testbed consists of five major parts – an RTDS Simulator, in which the Sickler substation and surrounding transmission network is modelled, as well as substation protective devices, substation communication gateway, power amplifiers, and time synchronization of physical protection and control hardware with the simulated environment.

Continued on next page

RTDS Technologies

Visit us online!

Don't miss our 2017 User's Group Meetings!

RTDS Technologies' User's Group Meetings are a great opportunity to connect with other users of the RTDS Simulator, explore new applications and stay informed on new developments. The events are open to all RTDS Simulator users regardless of location, and to all power industry colleagues who are interested in real time digital power system simulation.

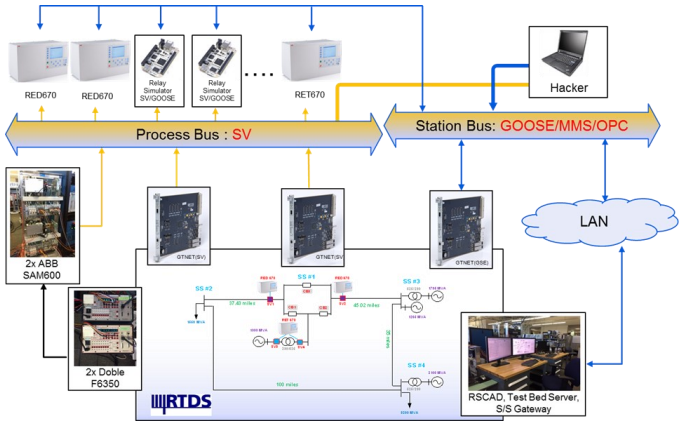
2017 Southern Africa User's Group Meeting
February 2-3, 2017

Both registration and abstract submission are now open for this exciting event, which will be hosted by the Cape Peninsula University of Technology in Cape Town, South Africa.

2017 North American User's Group Meeting
May 16-19, 2017

Abstract submission is now open. Don't miss your chance for a tour of the RTDS Technologies headquarters - this event will take place in the RTDS Simulator's hometown (and power system research hub) of Winnipeg, Canada.

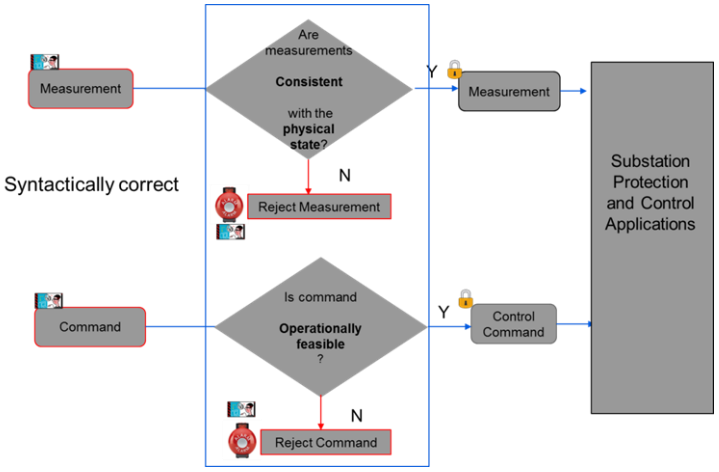
Click here to learn more



BPA power system and HIL testbed

The basic concept of CODEF is that the hacker has breached the intrusion detection system and assumes a position where they can control or influence the operation of the control systems in a substation. They could inject false measurements into the data network, causing relays to subscribe to that measurement and act on it instead of identifying it as a gross error. CODEF would be able to filter out such measurement attacks. Yet another attack could comprise of injecting a false command into the substation automation system, such as a direct command to open a circuit breaker. CODEF double checks the consistency of switching breaker commands to their operational outcome and flags commands that are inconsistent with their intended action.

The CODEF research project explored, researched, and evaluated the main cyber security problems in a substation automation system when the IT security layer is breached. The proof of concept demonstration at BPA proved that the CODEF function can perform sufficiently in a field setting. The CODEF demonstration at BPA has validated the use of physics as an effective tool in blocking cyber attacks.



CODEF filters out malicious measurements and commands

This article has been abridged. **Click here** to access the full article online.

More features of RSCAD V5

RSCAD V5 is compatible with racks containing PB5 and/or GPC Processor Cards only.

- There are now three new versions of the Generic Model for MMC valves (MMC_FPGA_GM) available in the RSCAD library. Each new model provides new functionality:
  - ◊ MMC_FPGA_GM_V2 supports up to 1024 submodules (SMs) per valve (increased from 512)
  - ◊ MMC_FPGA_GMT3 supports an internal node to ground fault (from a terminal between SMs or after reactor)
  - ◊ MMC_FPGA_GMMX supports a mixed half– and full-bridge topology
  - ◊ MMC_FPGA_GM_damp and U5_damp support the addition of a damping submodule for fault current reduction
  - ◊ TLINE_FPGA_FDP supports the modelling of a frequency dependent transmission line on the GTFPGA Unit
- The new GTAI V2 card contains a user-defined digital filter and synchronously samples all channels (and sends to the processor card) every 1 microsecond

Click here to log in to the RTDS client area, where you can access the full RSCAD release notes.

If you have an idea for a new feature, please send it to **feedback@rtds.com**. We want to hear from you!