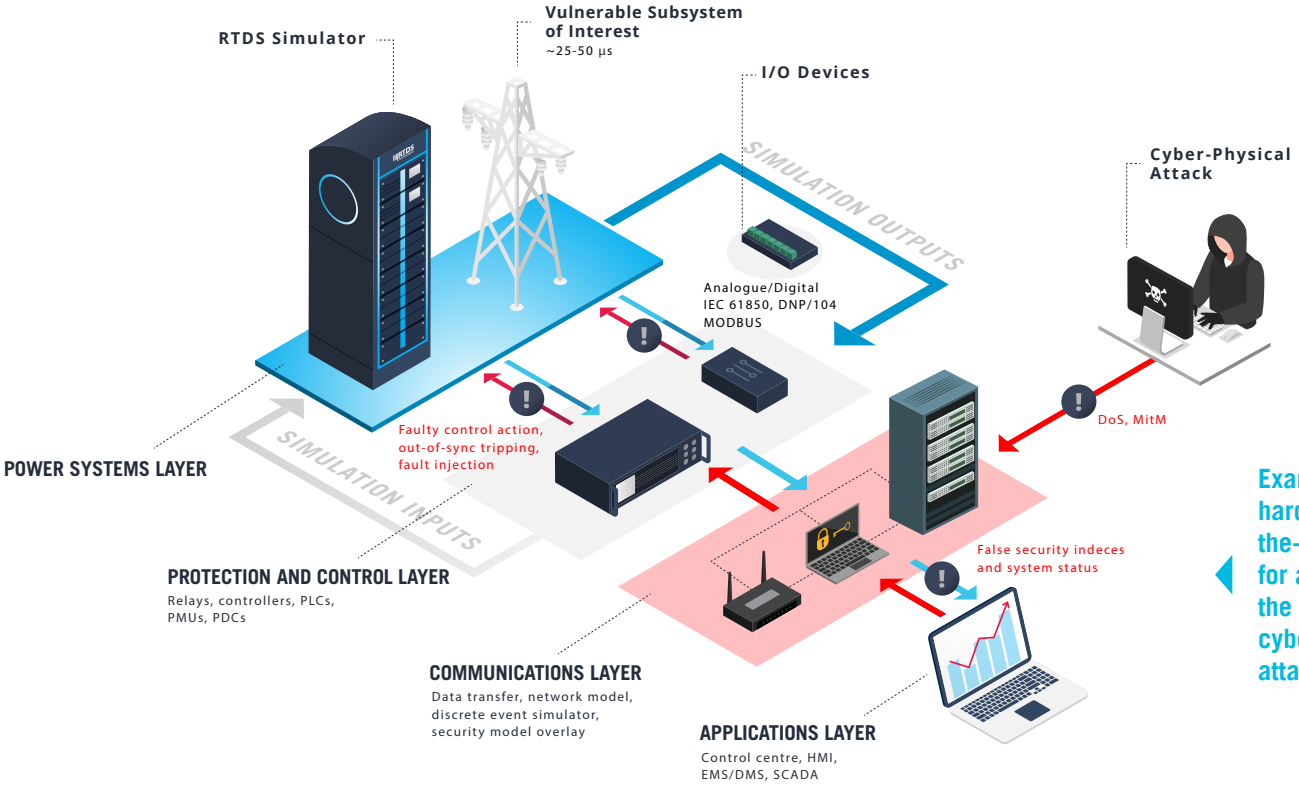
APPLICATIONS

REAL-TIME SIMULATION FOR CYBERSECURITY

RTDS Technologies

In our increasingly connected and intelligent grid, a vital issue in power system reliability is maintenance of the network's cybersecurity. A cyber attack on power system protection and control devices could result in critical power disruption and/or damaged equipment. Appropriately designed and implemented cybersecurity measures aim to prevent and survive cyber incidents while sustaining the critical functions of the power system. The RTDS® Simulator is used worldwide as a crucial component of cybersecurity testbeds, in which the simulated power system can be subjected to both intentional and unintentional cyber events and the effect on real protection, control, and measurement equipment can be determined. This provides a realistic, flexible, and safe environment for the validation of energy system security technologies.



Example of a hardware-in-the-loop testbed for assessing the impact of cyber-physical attacks

CYBERSECURITY PROJECT OPPORTUNITIES

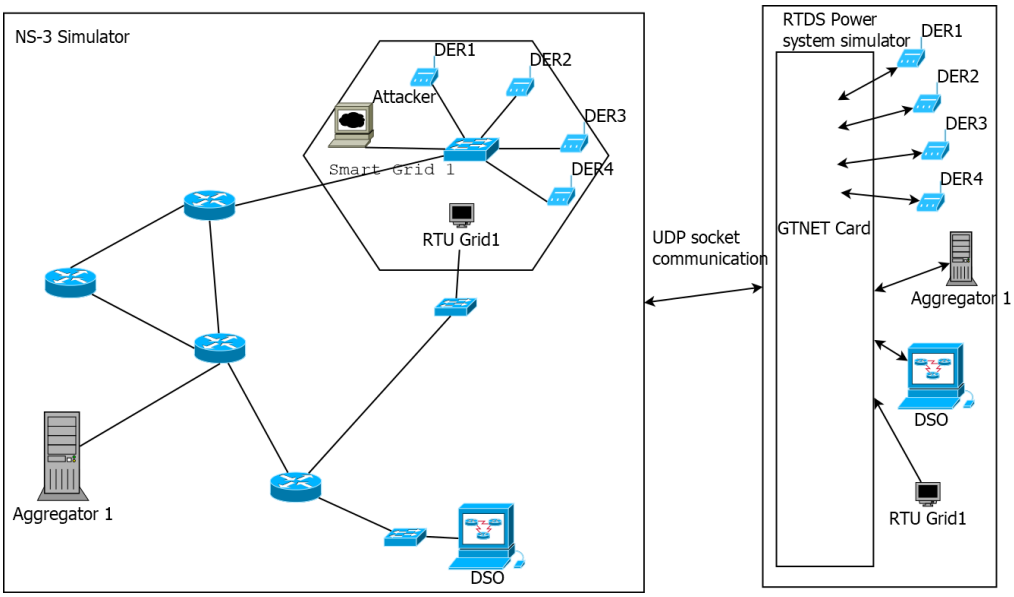
- Cyber and physical fault injection analysis
- Coordinated cyber-physical attack assessment
- Testing of PMU operation with low-integrity data
- Benign and malicious control action analysis
- GPS spoofing detection and mitigation studies
- State estimation robustness studies
- Quantum cryptography applications
- Contingency-based shipboard power system reconfiguration
- Man in the Middle (MITM) attack simulation
- Denial of Service (DoS) attack simulation

100-150 Innovation Drive, Winnipeg, Canada R3T 2E1 • + 1 204-989-9700

YOUR WORLD IN REAL TIME.
RTDS.COM

CONNECTING THE RTDS SIMULATOR TO A THIRD-PARTY COMMUNICATION NETWORK SIMULATOR

The RTDS Simulator is designed for the real-time simulation of electrical power systems. Often, the detailed study and replication of cybersecurity events requires a network simulator to be connected to the power system simulation. The RTDS Simulator has been successfully interfaced in **cybersecurity co-simulation** with network simulators such as **NS-3, an open source discrete event network simulator.**



In the graphic on the left, a network simulator is connected to the RTDS Simulator via real-time UDP socket communication.

The RTDS Simulator represents a distribution feeder with several distributed energy resources. When the system is in a healthy state, an external program representing an Aggregator takes control action over the DERs based on requests from the DSO such as load-shedding.

However, a Man in the Middle or Denial of Service attack could cause significant adverse effects on the grid. The network simulator can be used to simulate these attacks, and the power system simulator provides an opportunity for quantifying these vulnerabilities and/or the effectiveness of countermeasures.

In this case, a TCP SYN flood attack was used carry out DoS, and ARP spoofing was used to carry out MITM. Many different approaches are possible, and other discrete event network simulators can be interfaced with the RTDS Simulator.

USER SPOTLIGHT: SIMULATION OF A MAN IN THE MIDDLE ATTACK ON PMU DATA
AT THE TRUSTWORTHY CYBER INFRASTRUCTURE FOR THE POWER GRID (TCIPG), UNIVERSITY OF ILLINOIS

TCIPG is supported by the U.S. Departments of Energy and Homeland Security and is comprised of four partner universities. Their large-scale cyber-physical testbed includes an RTDS Simulator, a wide range of relays, PMUs and PDCs, substation computers, security gateways, and data analytics and visualization tools. Because many utilities still transit PMU data with no cyber protection controls integrated, mitigation of MITM attacks in the context of synchrophasors is an important research area.


The cyber-physical testbed at TCIPG

The attacker manipulated each IEEE C37.118 synchrophasor data packet by changing the payload, which in this case is data related to the calculation of the voltage stability assessment index for the local power system. Various attack methods and data manipulations were simulated. In one case, manipulated data at multiple buses caused two additional, unnecessary load shedding actions to be taken by the control system. A significant voltage angle difference between the control centre and substation was observed for various events, including increasing real and/or reactive power loading, connecting shunt capacitor banks, and load shedding.

LEARN MORE ABOUT CYBERSECURITY TESTING AT RTDS.COM/APPLICATIONS/CYBERSECURITY