RTDS Technologies

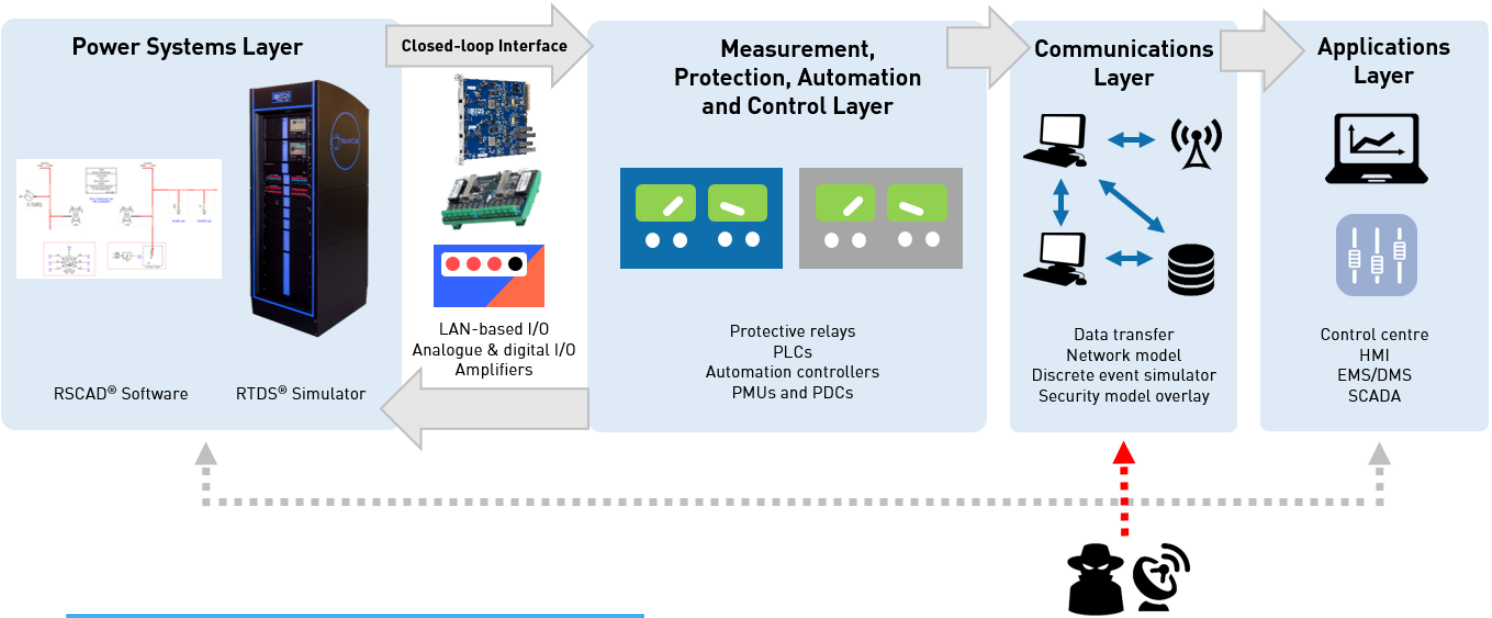
the world standard for real time digital power system simulation

Cyber Security

As the modern power grid employs increasingly complex devices, operational methods, and communication networks, new methods are required in order to maintain the reliability, resiliency, and efficiency that we require from our power infrastructure. Today, a vital issue in power system reliability is maintenance of the network's cyber security. A cyber attack on power system protection and control devices could result in critical power disruption and/or damaged equipment. Appropriately designed and implemented cyber security 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 cyber security testbeds, in which the simulated power system can be connected to real protection, control, and measurement equipment and subjected to both intentional and unintentional cyber events. This provides a realistic, flexible, and contained environment for the validation of energy system security technologies.

Real time simulation in a cyber security testbed



Power Systems Layer

RSCAD® Software

RTDS® Simulator

Closed-loop Interface

LAN-based I/O
Analogue & digital I/O
Amplifiers

Measurement, Protection, Automation and Control Layer

Protective relays
PLCs
Automation controllers
PMUs and PDCs

Communications Layer

Data transfer
Network model
Discrete event simulator
Security model overlay

Applications Layer

Control centre
HMI
EMS/DMS
SCADA

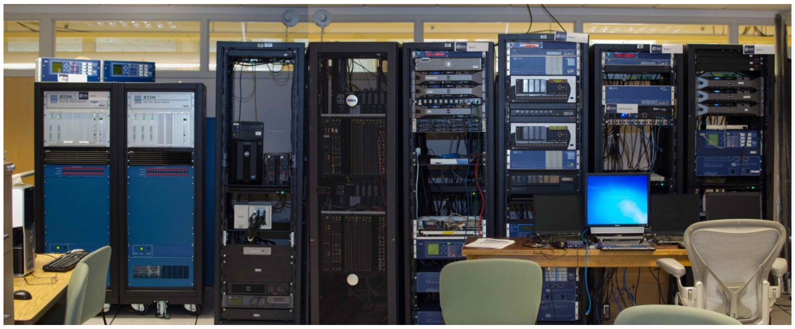
Learn more about cyber security with the RTDS Simulator at:
www.rtds.com/applications/cyber-security

Cyber security application examples

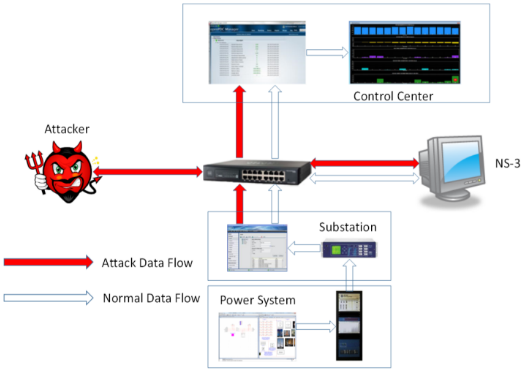
- Cyber and physical fault injection analysis
- Coordinated cyber-physical attack assessment
- Testing of PMU operation with low-integrity data
- Benign and malicious control action analysis
- GPS spoofing detection and mitigation studies
- State estimation robustness studies
- Quantum cryptography applications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

Case study: Simulation of a man-in-the-middle attack on PMU data

@ TCIPG, University of Illinois, USA



Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) is supported by the U.S. Departments of Energy and Homeland Security and is comprised of four partner universities. Under these efforts, the Information Trust Institute at the University of Illinois operates a large-scale cyber-physical testbed including an RTDS Simulator, a wide range of relays, PMUs and PDCs, substation computers, security gateways, and data analytics and visualization tools. The testbed, shown here, has been used for various cyber security research projects, including fault injection analysis, coordinated attack assessment, GPS spoofing, and more. Because many utilities still use IEEE C37.118 via normal UDP protocol to transmit PMU data – with no cyber protection controls integrated – mitigation of Man in the Middle (MITM) attacks is an important research area.



The MITM attack setup is shown here. The attacker manipulates each IEEE C37.118-based data packet by changing the payload, which in this case is synchrophasor data related to the calculation of the voltage stability assessment index for the local power system.

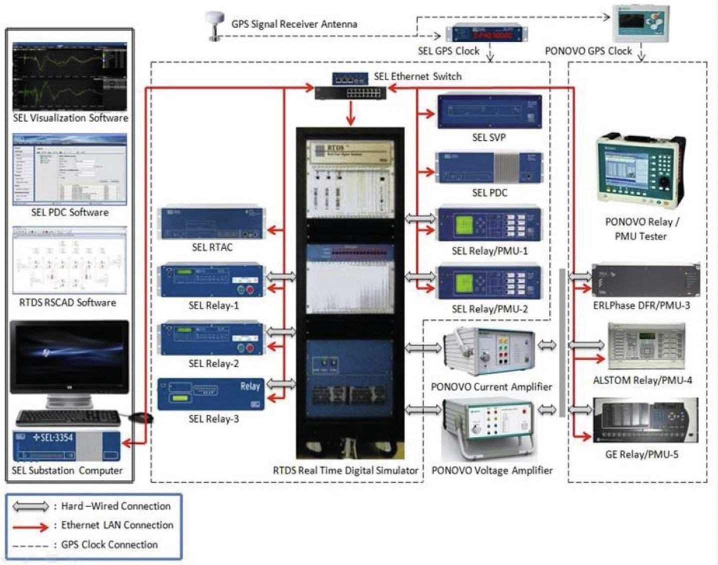
Various attack methods and data manipulations were simulated. In one case, manipulated phasor data at multiple buses caused two additional, unnecessary load shedding actions to be taken by the control system. The significant resulting voltage angle difference between the control centre and substation was observed for various events, including increasing real and/or reactive power loading, connecting shunt capacitor banks, and load shedding.

Case study: Aurora attack re-simulation

@ Washington State University, USA

In 2007, Idaho National Laboratories ran the Aurora Generator Test, demonstrating the potential for a cyber attack to cause major damage to physical components of the power grid. In the experiment, a 2.25 MW diesel generator was connected to a substation, and a protective relay controlling the generator's breaker was accessed via a digital interface. An attacker proceeded to open and close the breakers out of phase from the grid. Each time the breakers were closed out of sync, the torque from the synchronization caused the generator to undergo severe mechanical stress. The unit was destroyed in a matter of minutes. As the failure of even a single generator is a serious concern due to potential cascading failure (as seen in the Northeast blackout of 2003), prevention and mitigation of such attacks is a critical research area.

The cyber security testbed at Washington State University, shown here, was used to re-simulate the attack. Real time simulation via the RTDS Simulator provides a safe and flexible environment to reproduce and alter the attack scenarios.


GPS Signal Receiver Antenna
SEL GPS Clock
PONOVO GPS Clock
SEL Ethernet Switch
SEL Visualization Software
SEL PDC Software
RTDS RSCAD Software
SEL Substation Computer
SEL SVP
SEL PDC
SEL RTAC
SEL Relay/PMU-1
SEL Relay-1
SEL Relay/PMU-2
SEL Relay-2
SEL Relay-3
PONOVO Relay / PMU Tester
ERLPhase DFR/PMU-3
ALSTOM Relay/PMU-4
GE Relay/PMU-5
PONOVO Current Amplifier
PONOVO Voltage Amplifier
RTDS Real Time Digital Simulator
⇔ : Hard –Wired Connection
→ : Ethernet LAN Connection
----- : GPS Clock Connection