

Operator Response Training Simulator (OPSIM)

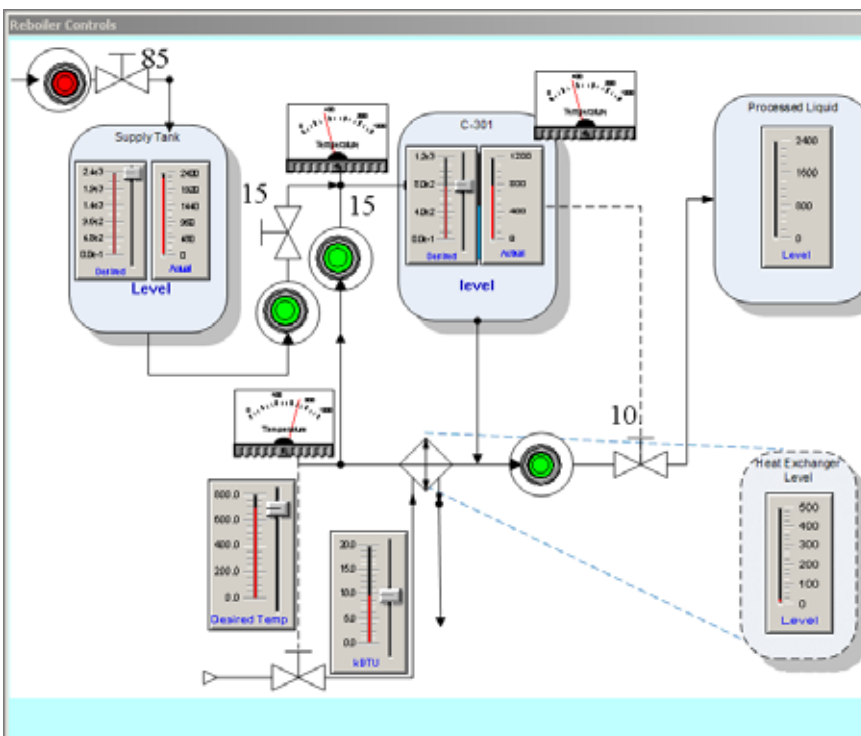
Training operators to respond to network anomalies

Overview

The Operator Response Training Simulator (OPSIM) will allow a cyber security team to train control system operators interactively in a game-like environment. This tool will provide the operators with critical new understanding of cyber attacks. The training will teach operators how to recognize a cyber attack, respond properly to cyber attacks and just how dangerous a motivated cyber attacker can be in an interactive environment. Operators will emerge from this training better able to recognize and handle real-life cyber attacks in an operational environment.

Features

OPSIM will use a graphical display, driven by a virtual representation of a control system, to convey current system state and response options to the operator being trained. An advanced attack tool will give the security team realistic situational awareness and response. This arrangement will provide the necessary insight to incorporate cyber security issues into standard troubleshooting heuristics.



A graphic display of the Operator Simulation User Interface is depicted here.

Why interactive training?

Cyber-based threats to control systems not only include “hit Enter” types of attacks, such as worms and viruses, but also include attacks designed and executed by intelligent adversaries. These adversaries will not idly sit by while their attack is executed, but instead will approach the attack as if it were a game of chess, watching how their opponent reacts before determining their next move. Operators need to understand how intelligent adversaries design and execute attacks, how such adversaries approach the execution of an attack, how to appropriately troubleshoot and respond to these attacks while minimizing operational impacts, and how existing troubleshooting heuristics could be compromised during a cyber attack.

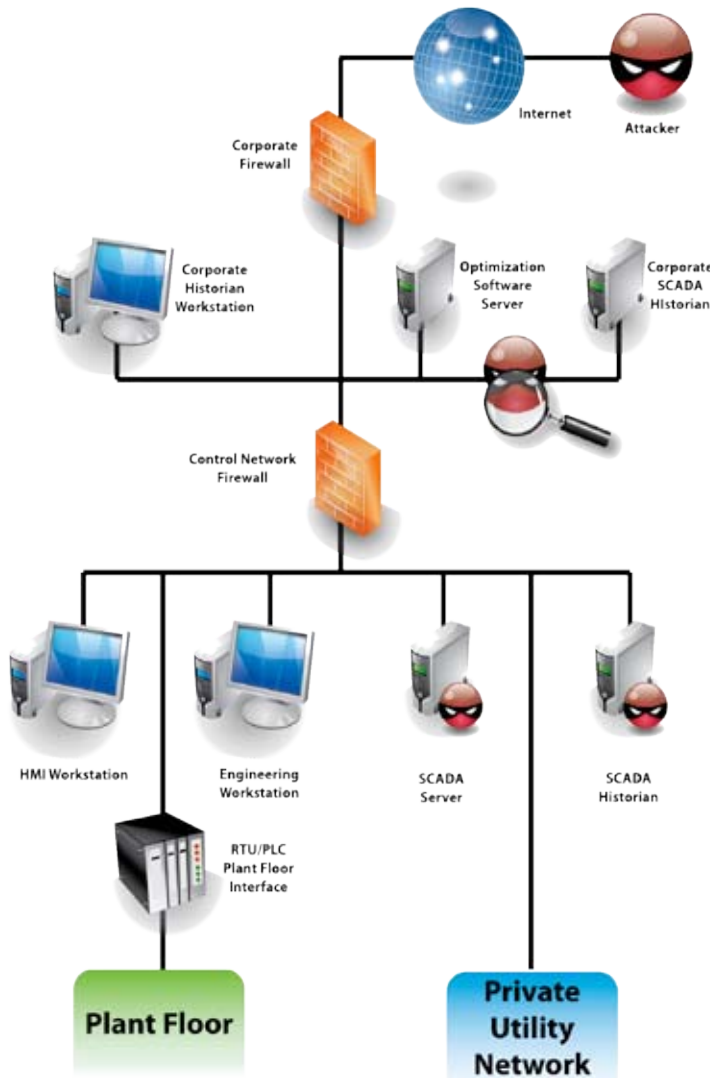
Key Benefits

- During the development of OPSIM, researchers will be able to document common troubleshooting heuristics and understand how they rely on cyber networks and tools.
- OPSIM will help asset owners and operators better understand:
 - Intelligent adversaries and their methods of attack
 - How to detect and respond to cyber attacks
- OPSIM provides an understanding of how troubleshooting heuristics and a reliance on cyber networks can be used by an adversary to mislead an operator.
- OPSIM provides a foundation for
 - The evaluation of mitigation effectiveness
 - The development of response best practices

Technical Description

OPSIM uses simulation, emulation, and real hardware and software to model a fully operational control system. The model simulates realistic plant processes and generates accurate plant sensor and control data that can be used by third party software.

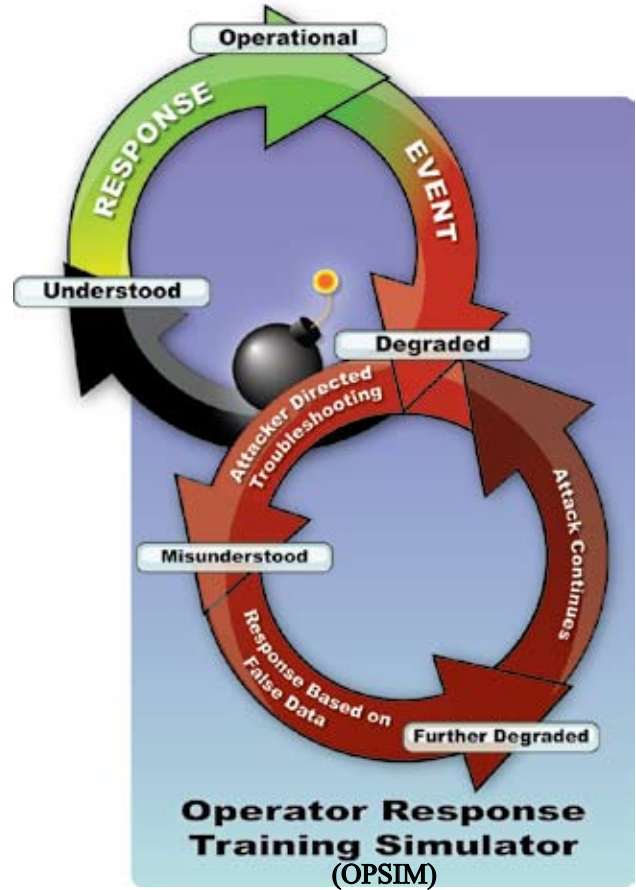
Attack scenarios are described in OPSIM using graphical attack modeling software, allowing attacks to be described in a generic fashion.



OPSIM models how a cyber attacker can penetrate a business/control system network.

For more information about the Survivability and Recovery of Process Control Systems project, visit:

<http://www.thei3p.org/research/srpcs.html>



Functional Description

OPSIM provides a real human-machine interface (HMI) with realistic data and controls to the operator being trained. As cyber attacks are executed by the security team, the operator will be exposed to the effects of the attacks and will be able to take actions to sustain safe plant operations.

Actions taken by the operator will be considered countermeasures to the attack being conducted and will be used by the attack modeling software when determining the next step of an attack.

Technology Transfer and Readiness

The current process model being simulated in OPSIM (a refinery process) and the data being generated by the simulation (status points, control traffic, etc.) are currently being validated by industry participants in the oil & gas sector.

OPSIM is currently still in its initial development and testing phase. It will be demonstrated at the I3P PCS Workshop in April 2009, for more info please visit www.thei3p.org.

This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Numbers 2006-CS-001-000001 and 2003-TK-TX-0003, under the auspices of the Institute for Information Infrastructure Protection (I3P) research program. The I3P is managed by Dartmouth College. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security, the I3P, or Dartmouth College.

Researcher Contact Information

Bryan Richardson btricha@sandia.gov



The I3P is managed by Dartmouth College.