Scalable Hybrid Attack Graph Modeling and Analysis

Challenge:

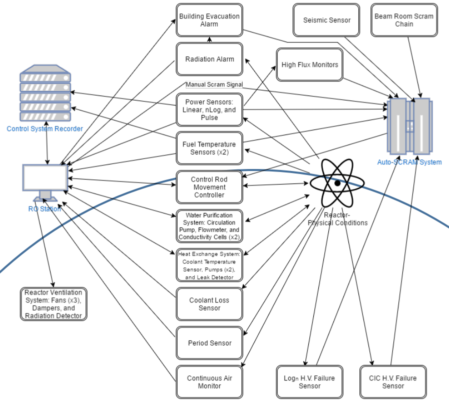
How can we conduct effective security analysis for large cyber physical systems (CPSs)?

- Modeling – Acquisition & representation
- Analysis – computationally intensive
- Research and Education – access to environments for CPS security experimentation and learning

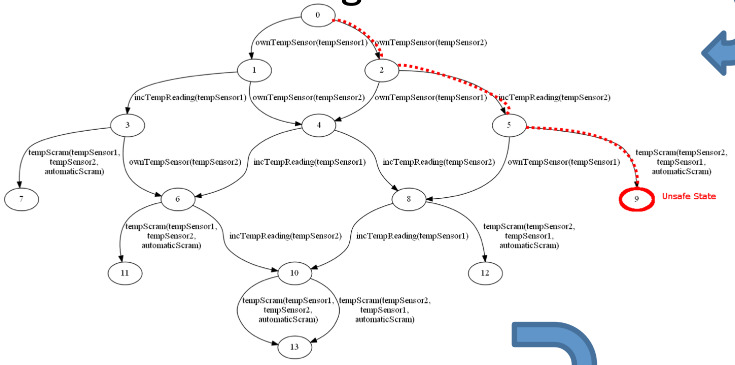
Solution:

- Build practical tools for distributed model acquisition and integration
- Develop scalable techniques for hybrid attack graph analysis, exploiting parallelism and high performance computing (HPC)
  - Intelligent heuristics
  - Markov decision process analysis
- Construct a CPS test bed based on competitive learning for researchers and students

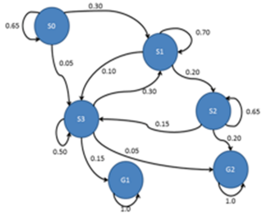
NSF Award #1524940, The University of Tulsa, John Hale (john-hale@utulsa.edu) and Peter Hawrylak (peter-hawrylak@utulsa.edu)


Building Evacuation Alarm
Seismic Sensor
Beam Room Scram Chain
Radiation Alarm
High Flux Monitors
Manual Scram Signal
Control System Recorder
Power Sensors: Linear, nLog, and Pulse
Fuel Temperature Sensors (x2)
Auto-SCRAM System
Control Rod Movement Controller
RO Station
Reactor-Physical Conditions
Water Purification System: Circulation Pump, Flowmeter, and Conductivity Cells (x2)
Heat Exchange System: Coolant Temperature Sensor, Pumps (x2), and Leak Detector
Reactor Ventilation System: Fans (x3), Dampers, and Radiation Detector
Coolant Loss Sensor
Period Sensor
Continuous Air Monitor
Logn H.V. Failure Sensor
CIC H.V. Failure Sensor

HAG Modeling and Generation


0
ownTempSensor(tempSensor1)
ownTempSensor(tempSensor2)
1
2
incTempReading(tempSensor1)
ownTempSensor(tempSensor2)
ownTempSensor(tempSensor1)
incTempReading(tempSensor2)
3
4
5
tempScram(tempSensor1, tempSensor2, automaticScram)
ownTempSensor(tempSensor2)
incTempReading(tempSensor1)
incTempReading(tempSensor2)
ownTempSensor(tempSensor1)
tempScram(tempSensor2, tempSensor1, automaticScram)
7
6
8
9
Unsafe State
tempScram(tempSensor1, tempSensor2, automaticScram)
incTempReading(tempSensor2)
incTempReading(tempSensor1)
tempScram(tempSensor2, tempSensor1, automaticScram)
11
10
12
tempScram(tempSensor1, tempSensor2, automaticScram)
tempScram(tempSensor2, tempSensor1, automaticScram)
13

HAG Analysis



THE UNIVERSITY of TULSA

Scientific Impact:

- HAGs offer the potential to provide a full attack surface characterization of CPSs
- New analytical techniques can offer new insights on the effect of counter measures
- Application of HPC to security analytics may inspire new lines of inquiry previously thought impractical

Broader Impact:

- CPSs underpin society's critical infrastructures – their security is of paramount importance
- Practical solutions coping with challenges in CPS security analysis will encourage adoption of HAGs and other analytical techniques
- A CPS security test bed for researchers and students will advance the state of the art, create new training opportunities, and inspire new lines of inquiry