ILLINOIS
Information Trust Institute

CREDC

An Ontology for Reliability and Security Assessment of Energy Delivery Systems

Ken Keefe, Alfonso Valdes

Acknowledgment:
This material is based upon work supported by the Department of Energy under Award Number DE-OE0000780.

Research Vision

We propose to develop a theoretically sound methodology and associated tools to enable EDS stakeholders to model cyber adversaries, identify likely attack paths through an EDS, and identify candidate countermeasures to thwart attacker objectives.

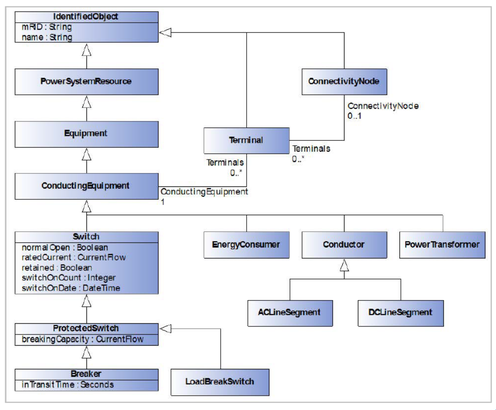
Threat Models for Risk Analysis

Energy sector stakeholders lack risk assessment tools that

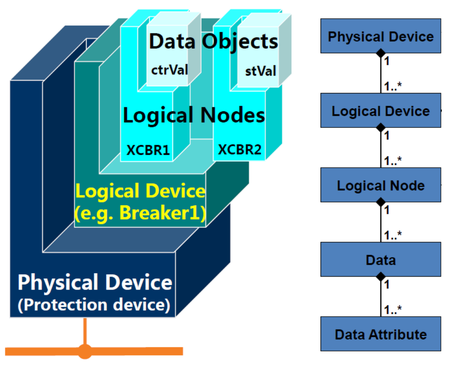
- Are theoretically sound
- Consider cyber and physical aspects
- Consider malicious actions and unintentional faults

Ontology-Based Threat Modeling

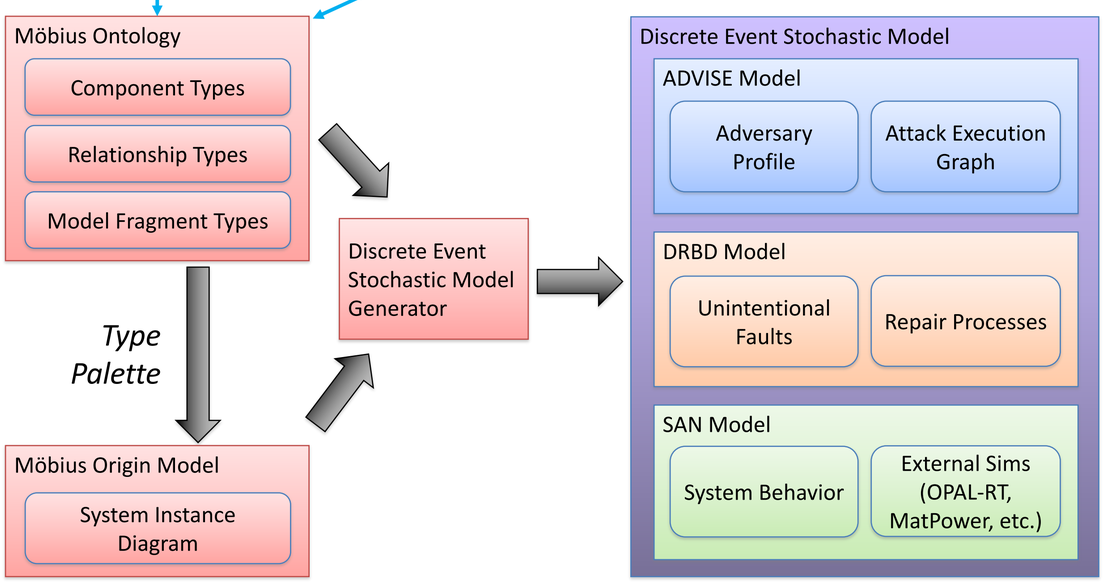
- Ontology describes the set of all types: Components, Relationships, Attributes, DES Model Fragments. Ontology can be reused across multiple system studies.
- Origin model describes a specific system instantiation by defining instances of types contributed by the ontology.
- Discrete event stochastic system model generator constructs detailed, DES models that can be examined in simulation by the Möbius tool to calculate quantitative metrics.
- The ontology will be based on IEC CIM and IEC 61850 Object Model.
- The approach is applicable to oil and gas systems with some alteration.



Common Information Model Primer, EPRI 2015 Technical Report

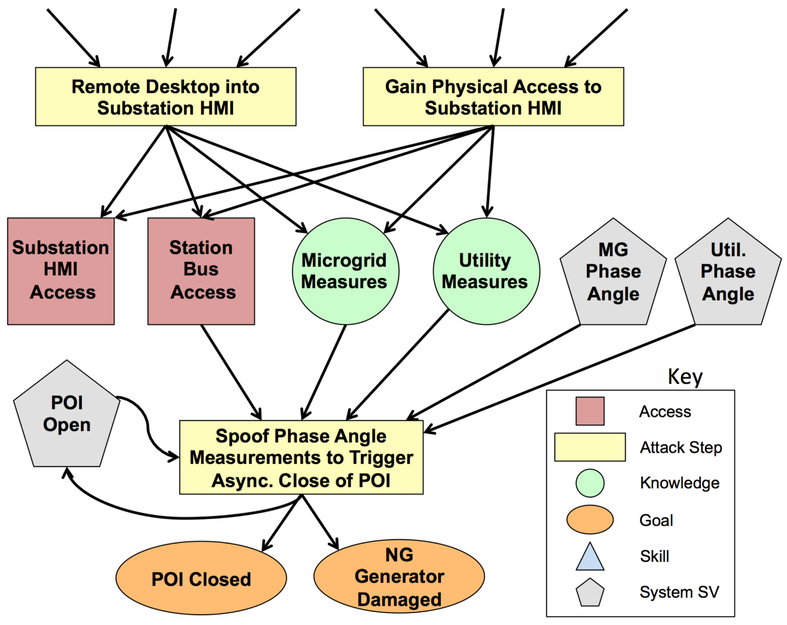


seclab.illinois.edu/wp-content/uploads/2011/03/iec61850-intro.pdf



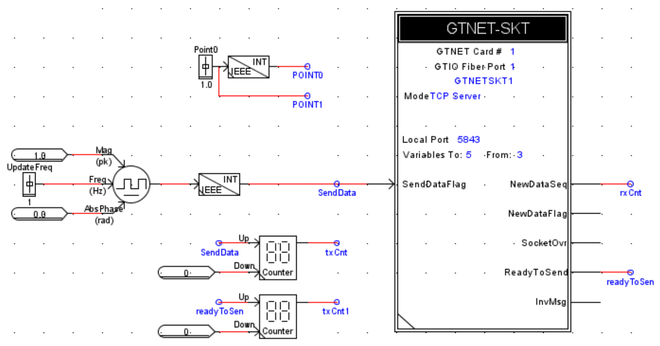
Discrete Event Stochastic Models

- Adversary View Security Evaluation (ADVISE) defines formal models of adversary behavior while compromising cyber-physical systems.
- Dynamic Reliability Block Diagram (DRBD) defines formal models of component and system level unintentional failure and repair behavior.
- Stochastic Activity Network (SAN) defines formal models of system operation and behavior. SAN model also interfaces with external simulations such as OPAL-RT and MatPower to understand electric power flow.
- The Möbius tool evaluates DES models using discrete-event simulation with respect to custom, quantitative metrics such as value to the adversary of a particular attack step or the expected operational time for a specific period.



Coupling with External Simulation

- DES state transitions change parameters in a coupled system simulation
- The system simulation is updated for the new state
- The output in turn updates the DES model
- Concept is applicable to O&G
  - Just need a process simulation



RTDS or Opal Simulation

Collaboration Opportunities

- This is a new project
- We are looking for energy delivery stakeholders to validate the approach and provide reference architectures for case studies
- We are soliciting input from O&G as to integrating process models for, e.g., pipeline SCADA
- Contact: **kjkeefe@Illinois.edu** **avaldes@illinois.edu**

References

1. Communication Networks and Systems in Substations - Basic Communication Structure for Substation and Feeder Equipment, IEC Standard 61850-7, August 2010.
2. Common Information Model: Energy Management System Application Program Interface, IEC Standard 61970, December 2013.
3. M. Backes, K. Keefe, and A. Valdes. A microgrid ontology for the analysis of cyber-physical security. In 2017 Workshop on Modeling and Simulation of Cyber Physical Energy Systems (MSCPES), April 2017, Pittsburg, PA, USA, pp. 1-6.
4. G. Clark, T. Courtney, D. Daly, D. D. Deavours, S. Derisavi, J. M. Doyle, W. H. Sanders, and P. G. Webster. 2001. The Möbius Modeling Tool. In Proc. of the Ninth Int. Workshop on Petri Nets and Performance Models (PNPM 2001), September 2001, Aachen, Germany, pp. 241–250.
5. K. Keefe, B. Feddersen, M. Rausch, R. Wright, and W. H. Sanders. 2018. An Ontology Framework for Generating Discrete-Event Stochastic Models. Proceedings of the 15th European Performance Engineering Workshop (EPEW 2018), October 2018, Paris, France, pp. 173–189.
6. A. Kushner, S. Amin, and S. Sastry. Research Challenges for the Security of Control Systems. Proceedings of the 3rd Conference on Hot Topics in Security, July 2008, San Jose, CA, USA, pp. 1–6.
7. E. LeMay, M. D. Ford, K. Keefe, W. H. Sanders, and C. Muehrcke. Model-based Security Metrics Using ADversary VIew Security Evaluation (ADVISE). In 2011 Eighth International Conference on Quantitative Evaluation of SysTems, September 2011, Aachen, Germany, pp. 191–200.