Reliability and Cyber-Physical Threat Model Generation from a Standards Influenced Ontology

Ken Keefe and Al Valdes, University of Illinois

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

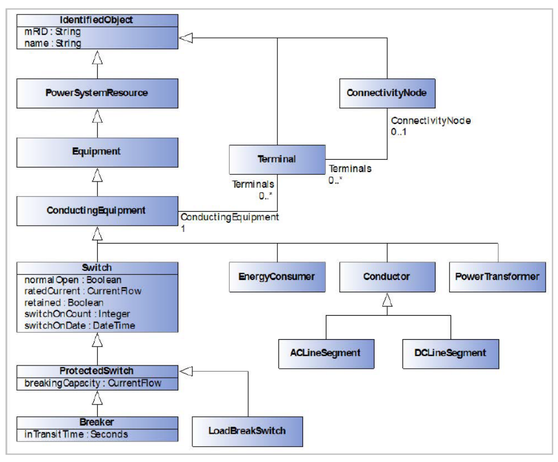
THREAT MODELS ENABLE INFORMED RISK ANALYSIS

Energy sector stakeholders lack risk assessment tools that

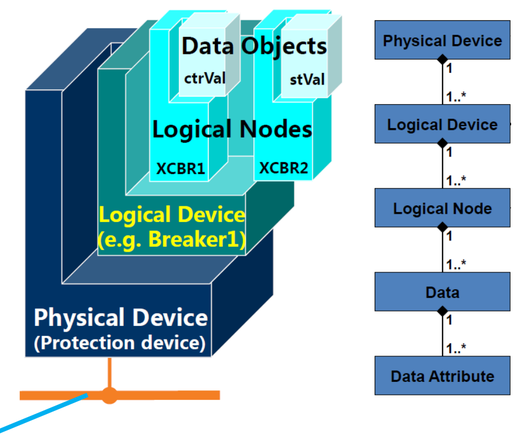
- **Are theoretically sound**
- **Consider cyber and physical aspects**
- **Consider malicious actions and un-intentional faults**

ONTOLOGY-BASED ADVERSARY MODELING

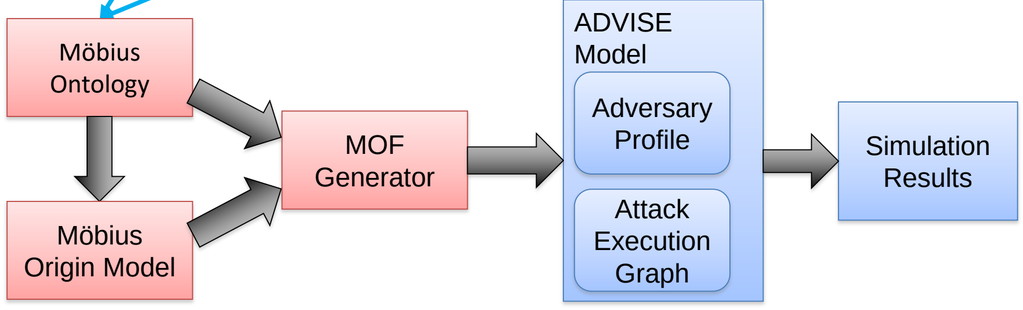
- **Adversary View Security Evaluation (ADVISE) defines formal models of adversaries compromising cyber-physical systems**
- **The Möbius tool evaluates ADVISE models using discrete-event simulation with respect to custom metrics such as value to the adversary of a particular attack step**
- **The Möbius Ontology Framework uses an ontology of component types, semantic relationships, and model fragments to generate a full ADVISE model from a high-level system definition**
  - **The ontology is based on IEC CIM and IEC 61850 Object Model**
- **The research will couple the resultant executable model to a real-time power system simulation (Opal or RTDS)**
  - **The approach is applicable to O&G given a suitable simulation of the underlying process**



Common Information Model Primer, EPRI 2015 Technical Report

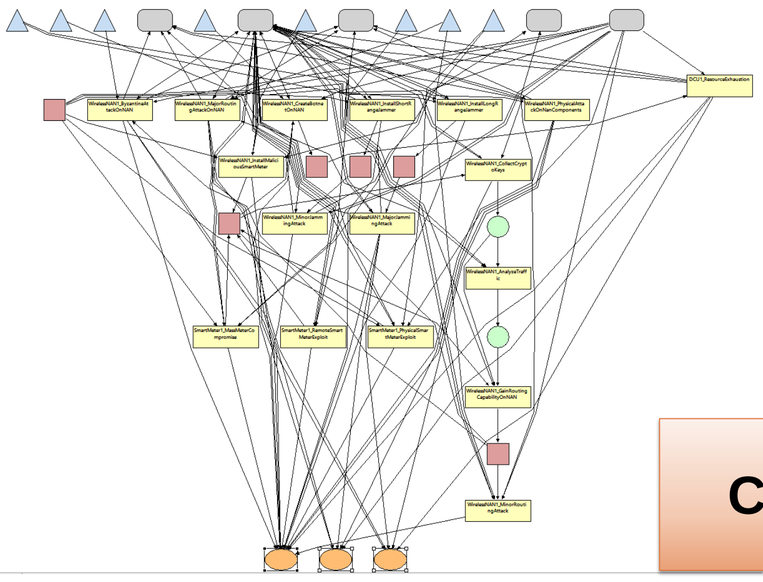


seclab.illinois.edu/wp-content/uploads/2011/03/iec61850-intro.pdf

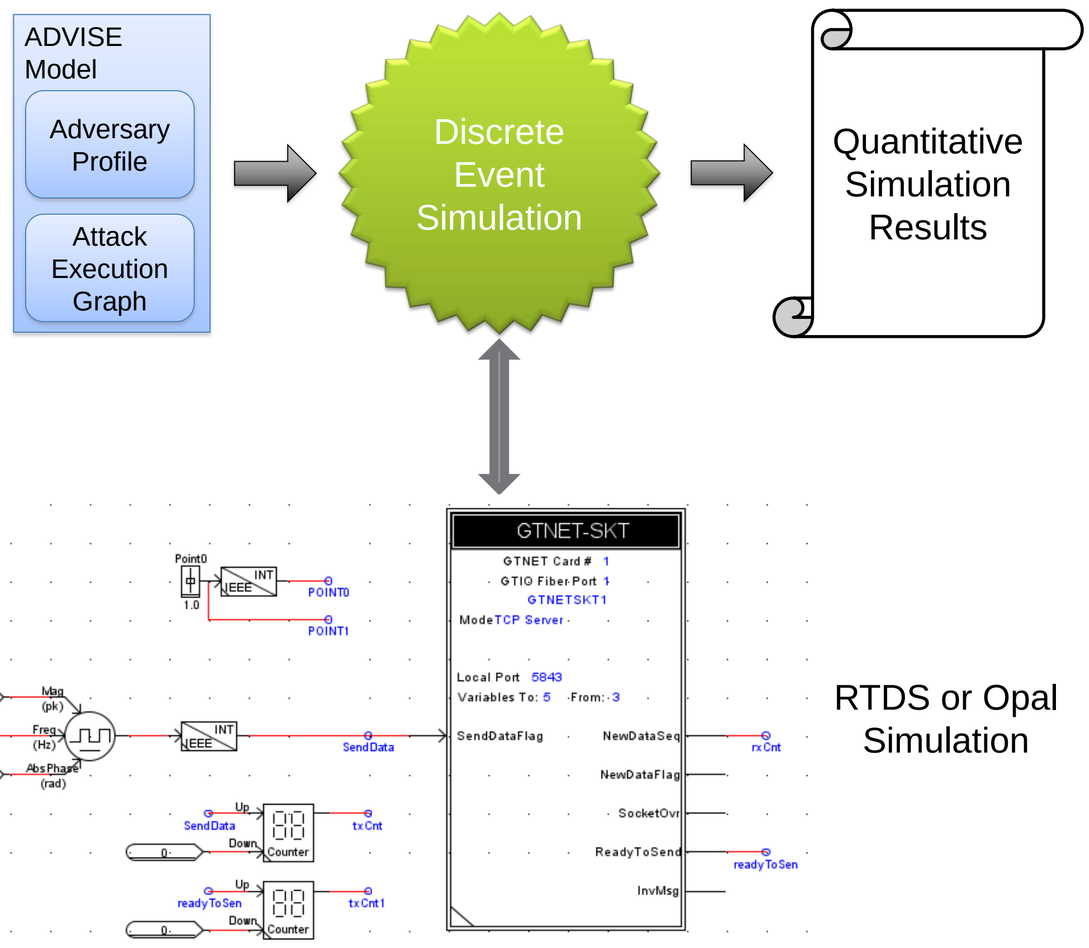


ADVISE ATTACK EXECUTION GRAPHS

- **AEG describe potential attack paths**
- **Precondition based on linked state variables**
- **Stochastically selected outcome updates model state variables**
- **Quickly expand in terms of state space**
- **Heuristics limit state space expansion, based on adversary objectives**
  - **Maximum impact**
  - **Stealth**
  - **Other objectives**



GETTING REAL: COUPLING TO SIMULATION (OPAL OR RTDS)



RTDS or Opal Simulation

- **ADVISE state transitions change parameters in a coupled system simulation**
- **The system simulation is updated for the new state**
- **The output in turn updates the ADVISE model**
  - **Has the attacker objective function changed**
  - **Is the critical attack path changed due to new state**

BENEFITS TO YOUR ORGANIZATION

- **Model adversary paths of maximal impact**
- **Identify critical attack paths**
- **Components on multiple critical paths are candidates for additional security measures**
  - **Cost effective, risk-based security hardening**
- **The modeling enables qualitative comparison of configuration alternatives with respect to adversary work factor**

OIL & GAS – WE NEED YOU!

- **We are looking for O&G stakeholders to expand this work and validate the approach.**
- **Collaborators will meet regularly to advise in the development of**
  - **An Oil & Gas ontology**
    - **Preferably based on existing standards**
  - **An example reference system**
    - **Real or manufactured**
  - **A set of cyber-physical attack scenarios on components from the ontology**
- **Collaborators will also provide feedback on the process and tool.**

Contact: kjkeefe@illinois.edu avaldes@illinois.edu

FUNDING SUPPORT PROVIDED BY THE U.S. DEPARTMENT OF ENERGY AND THE U.S. DEPARTMENT OF HOMELAND SECURITY