INL/MIS-19-54196-Revision-0

Risk and Resilience Assessment of Cyberattacks on Electric Grids: Informing Risk Characterization using Dynamic Probabilistic Risk Assessment

June 2019

Katya L Le Blanc, Craig G Rieger, Timothy R McJunkin, Carol Smidts, Briam E Johnson, Ronald Laurids Boring PhD, Thomas A Ulrich

Idaho National Laboratory

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/MIS-19-54196-Revision-0

Risk and Resilience Assessment of Cyberattacks on Electric Grids: Informing Risk Characterization using Dynamic Probabilistic Risk Assessment

Katya L Le Blanc, Craig G Rieger, Timothy R McJunkin, Carol Smidts, Briam E Johnson, Ronald Laurids Boring PhD, Thomas A Ulrich

June 2019

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

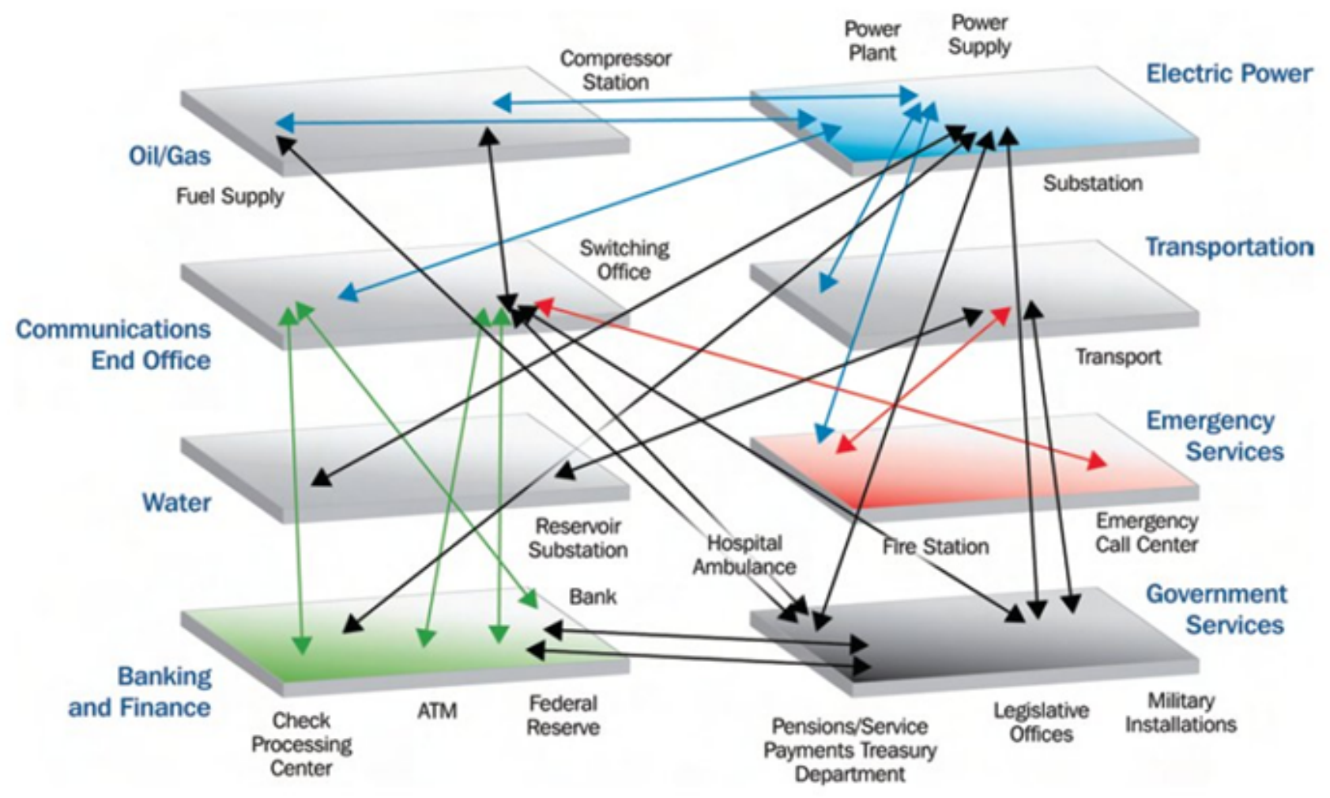
Risk and Resilience Assessment of Cyberattacks on Electric Grids: Informing Risk Characterization using Dynamic Probabilistic Risk Assessment

Katya Le Blanc (PI), Craig Rieger, Tim McJunkin, Carol Smidts, Brian Johnson, Ron Boring, Tom Ulrich

Challenge: Cost of a targeted cyber attack to critical infrastructure is in the tens of billions of dollars (and potential loss of human life) and there aren't mature, scientifically-based methods to quantify risk in the complex landscape

Background

- This project will develop the scientific basis for evaluating risk in high consequence cyber-physical systems that make up critical infrastructure
- Critical infrastructure is a complex interconnected system with many components that contain general purpose computing power that could be misused for malicious purposes.
- Current methods to characterize the cyber risk are not mature and have not been scientifically evaluated



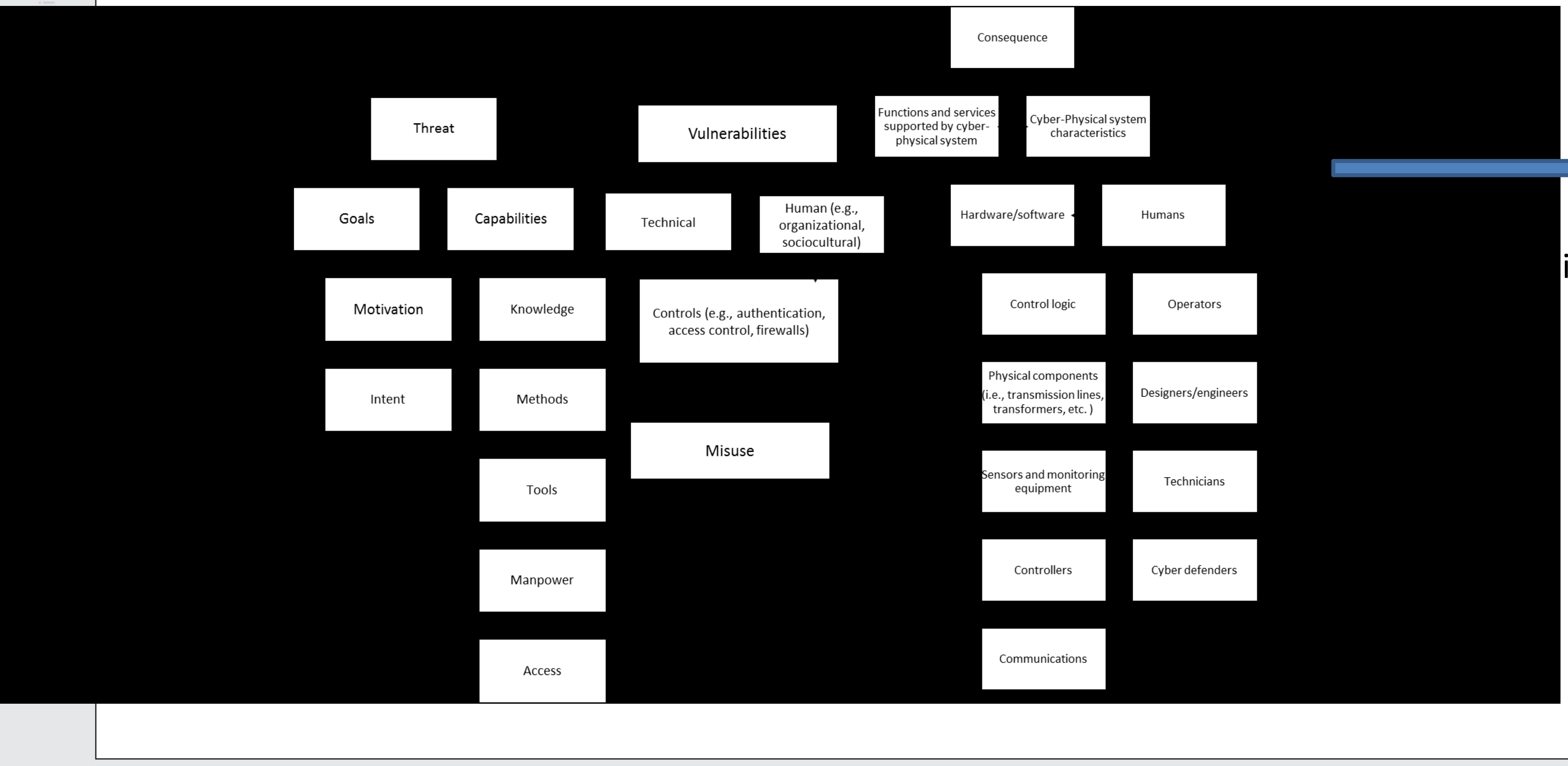
Expected Outcomes

- Evidence-based risk quantification methods
  - – Risk Equations
  - – Quantification based on
    - Empirical data collected in project
    - Modeling
  - – Framework for extending methods and data to other systems
- Clear identification of gaps in quantifying risk, and robust framework for addressing gaps with empirical methods
- Robust documentation of assumptions and limitations
- Better tools for decision making
  - – Better basis and documentation for cyber protection decisions

Method

Characterize the risk landscape

- Identify what would we need to know to make a perfect decision
- Identify dependencies and interactions
- Gather/ generate information



Consequence

Threat
Goals
Capabilities
Motivation
Intent
Knowledge
Methods
Tools
Manpower
Access

Vulnerabilities
Technical
Human (e.g., organizational, sociocultural)
Controls (e.g., authentication, access control, firewalls)
Misuse

Functions and services supported by cyber-physical system
Cyber-Physical system characteristics
Hardware/software
Control logic
Physical components (i.e., transmission lines, transformers, etc.)
Sensors and monitoring equipment
Controllers
Communications
Humans
Operators
Designers/engineers
Technicians
Cyber defenders

ify,

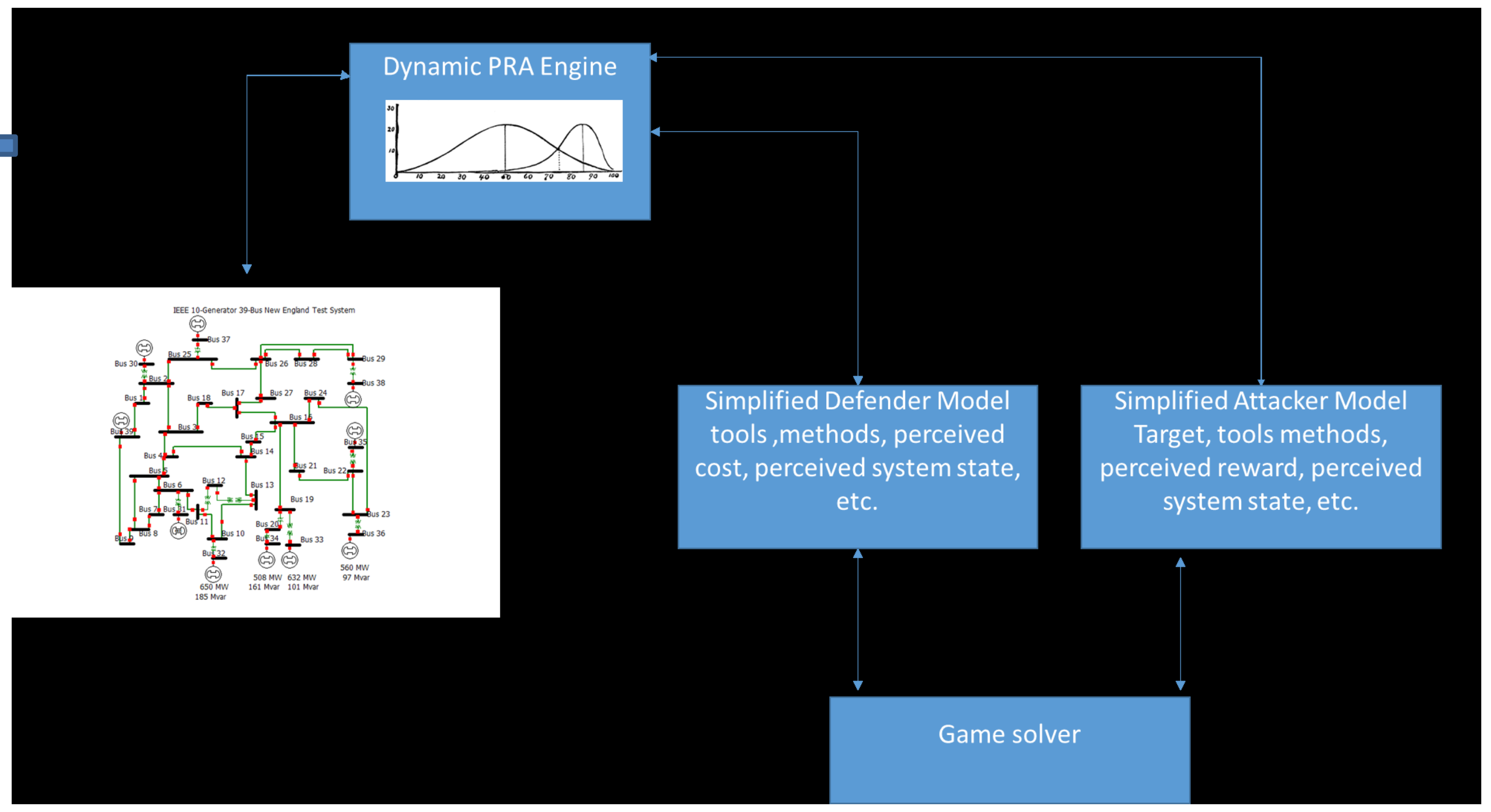
Risk characterization

- Risk equations
- Risk and Resilience metrics
- Identification of gaps for future research
- Framework for scaling and extending models
- Framework for incorporating new data and models

Develop integrated simulation to model specific system

- What are the distribution of outcomes given certain attack characteristics?
- What variables have the largest effect on the distribution of outcomes?

Generalize and develop scaling factors



Dynamic PRA Engine

Simplified Defender Model tools ,methods, perceived cost, perceived system state, etc.

Simplified Attacker Model Target, tools methods, perceived reward, perceived system state, etc.

Game solver