This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

Toward a game-theoretic metric for nuclear power plant security

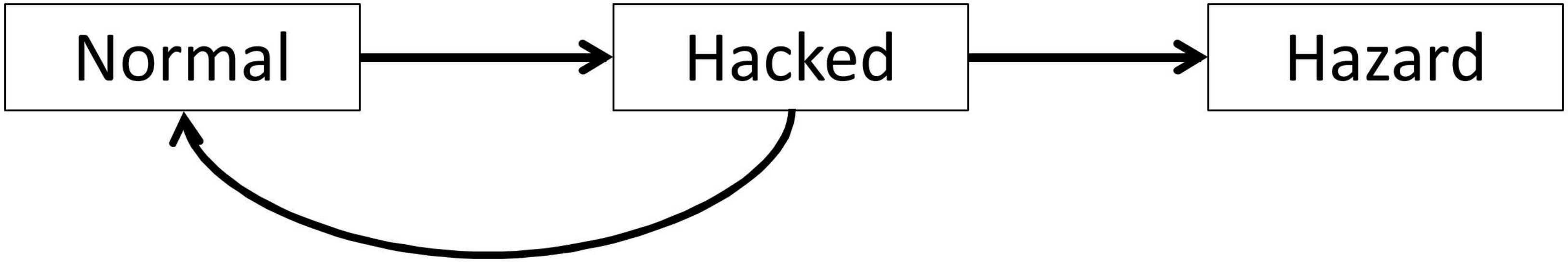
SAND2019-15361C

International Conference on Nuclear Security
10-14 February 2020
Vienna, Austria

Lee T. Maccarone
Jacob R. James
Timothy R. Ortiz
Daniel R. Sandoval
Robert J. Bruneau
Daniel G. Cole
Christopher C. Lamb

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

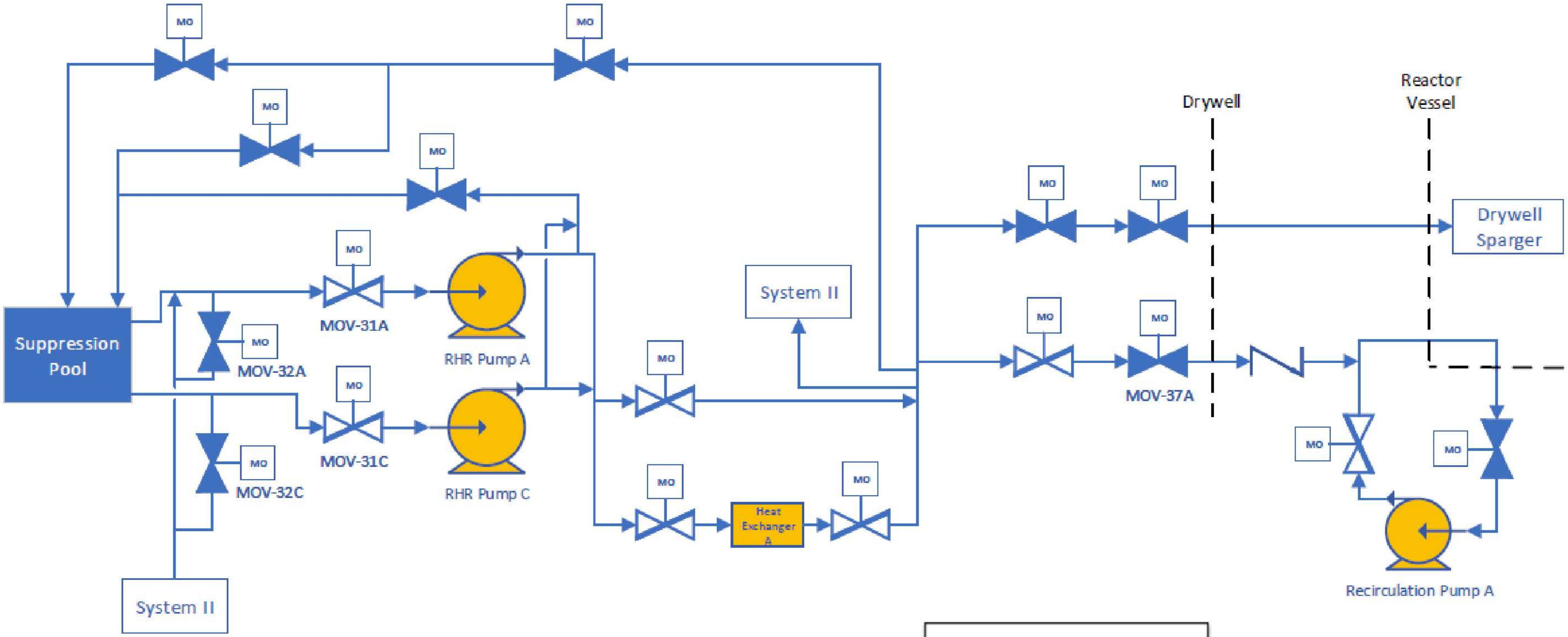
Stochastic game theory is used to analyze interactions where the outcome is uncertain

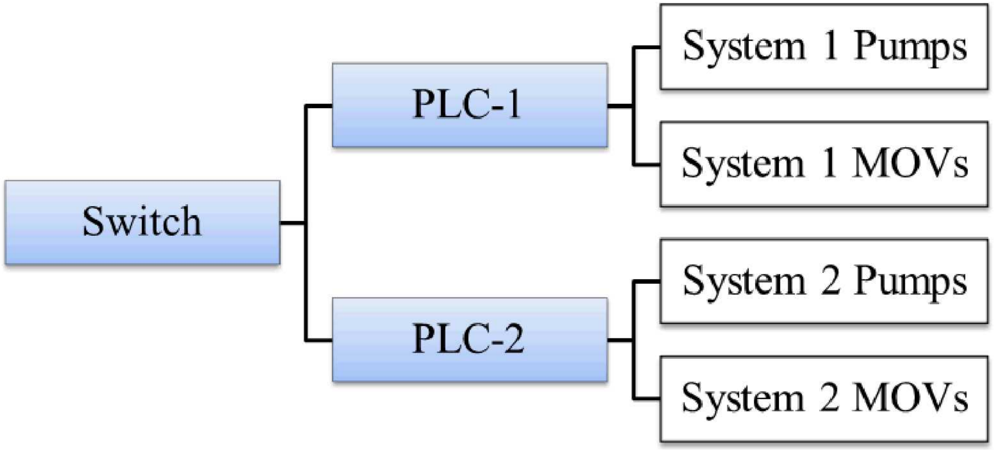


Challenges:

- Managing the size of the state space
- Defining transition probabilities
- Optimizing the solution

The residual heat removal system maintains reactor water level during a loss of coolant accident





Switch

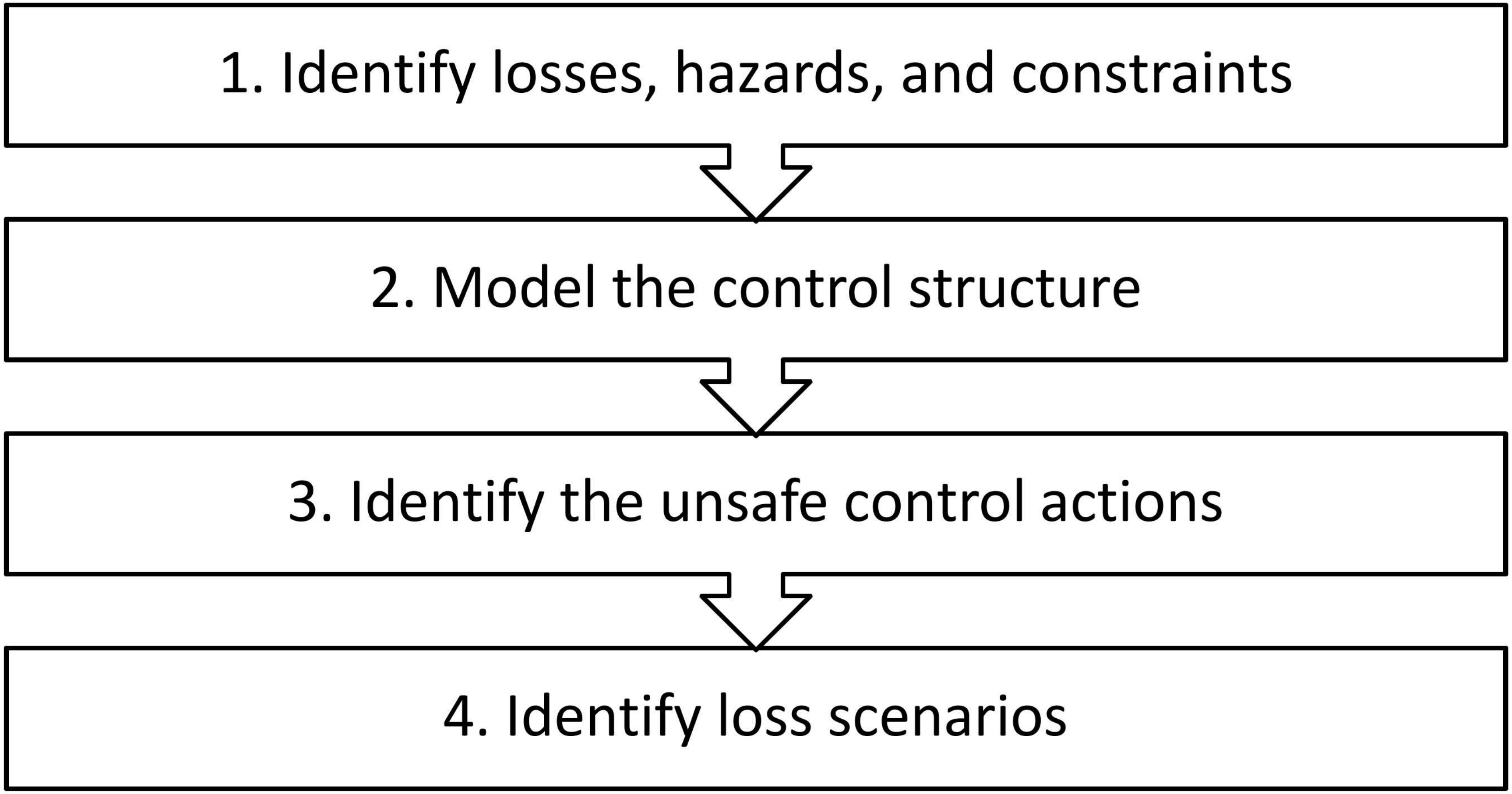
PLC-1

- System 1 Pumps
- System 1 MOVs

PLC-2

- System 2 Pumps
- System 2 MOVs

System-theoretic process analysis was used to identify scenarios of interest



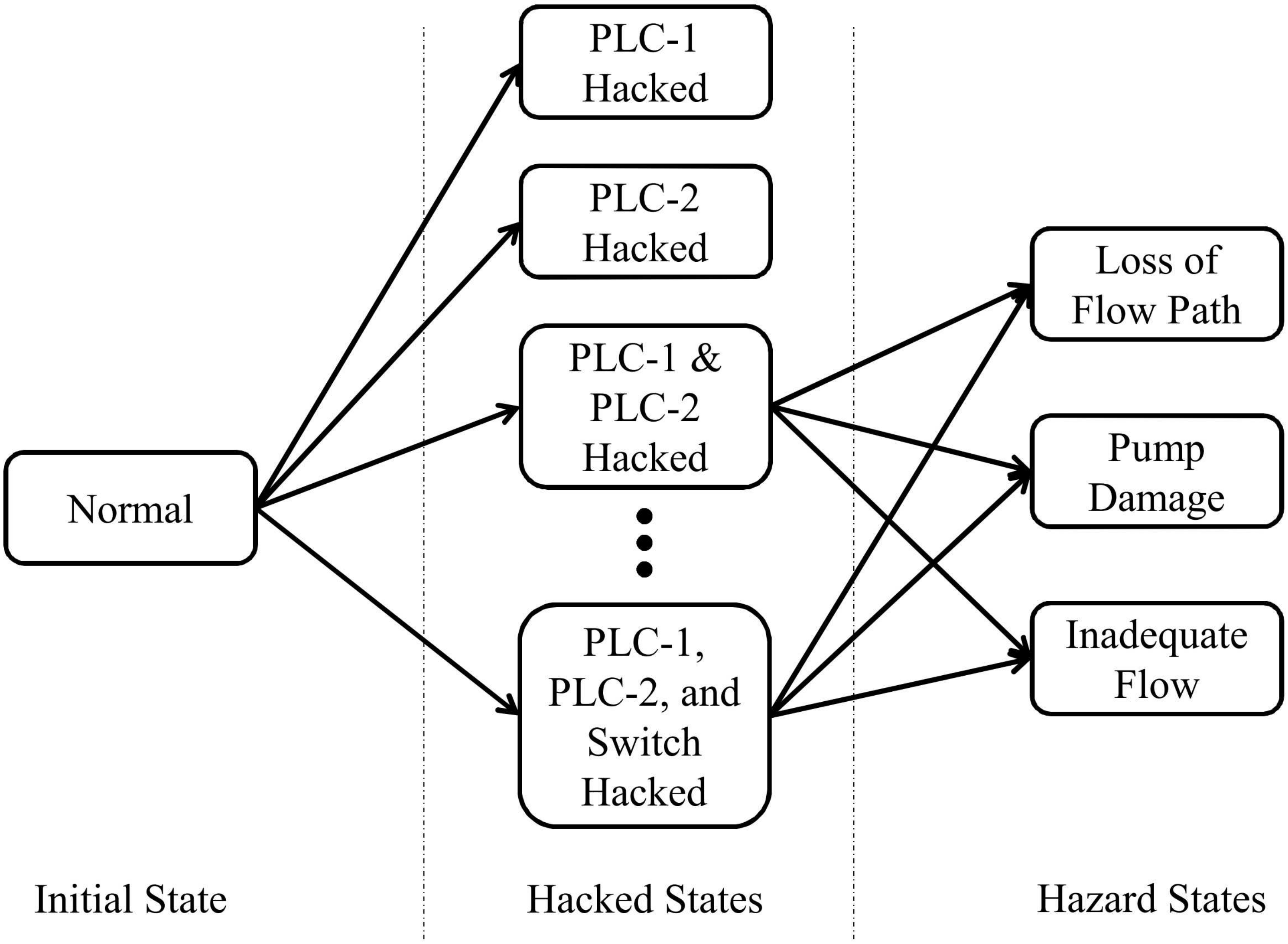
1. Identify losses, hazards, and constraints

2. Model the control structure

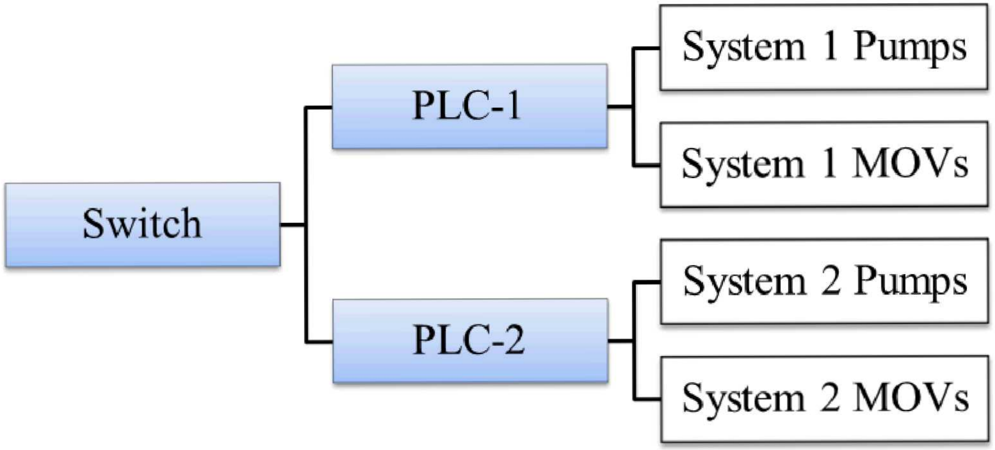
3. Identify the unsafe control actions

4. Identify loss scenarios

The stochastic states define the environment of the players' interactions



Actions were defined for both players at each state



	PLC-1 & PLC-2	**Switch**	**Communication Network**
Defender's Choices	Authentication: on/off Wireless: on/off	Authentication: on/off Firewall: on/off	Encryption: on/off
Attacker's Choices	Join: yes/no Wireless Exploit: yes/no	Join: yes/no Attack: yes/no	Decryption: yes/no

The Common Vulnerability Scoring System was used to estimate state transition probabilities

CVSS Exploitability Metrics

1. **Attack vector**
2. **Attack complexity**
3. **Privileges required**
4. **User interaction**

$$\Longrightarrow \quad p(s_j | s_i, a_D, a_A)$$

Probabilities may be validated with capture the flag games

Reward functions were defined to quantify the costs and benefits for both players

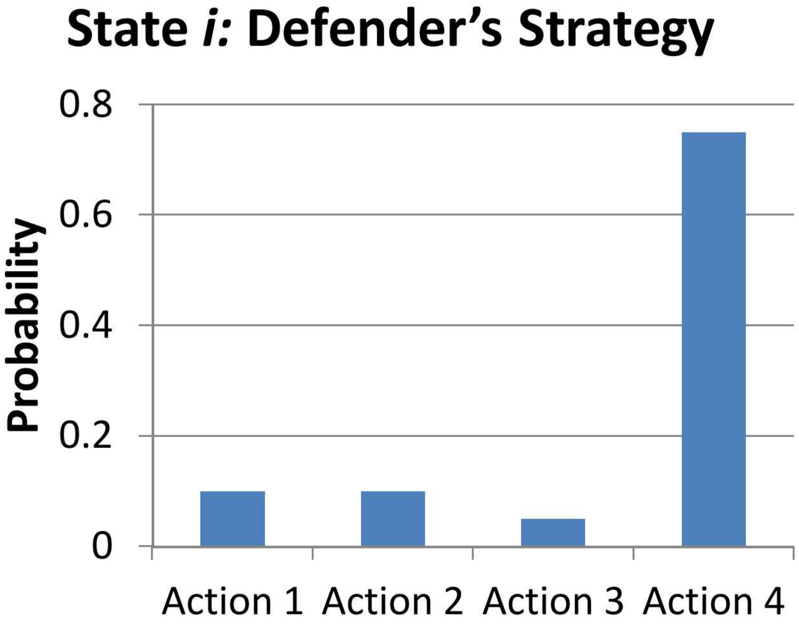
Immediate reward function for player A/D:

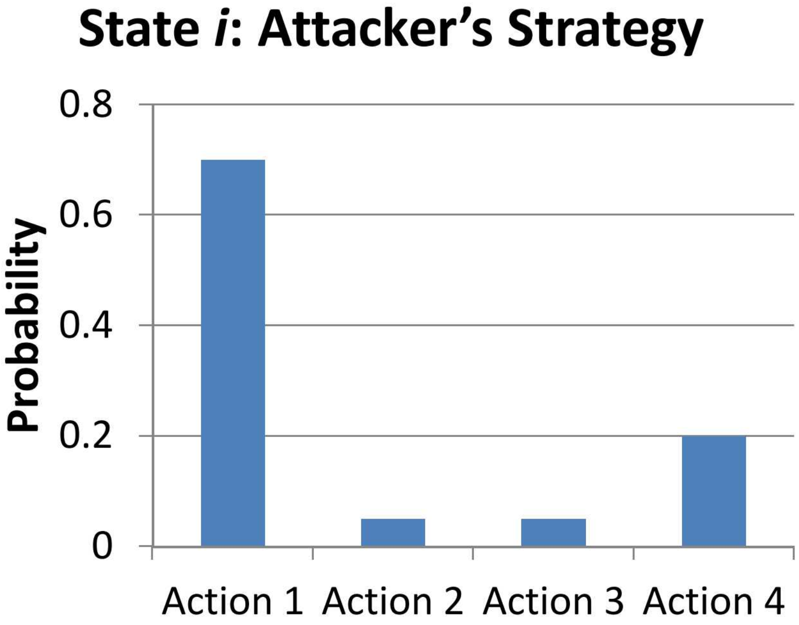
$$r_{A/D}(s_i, a_D, a_A, s_j) = \phi_{A/D}(s_j) - E_{A/D}(a_{A/D})$$

Cumulative utility function for player A/D:

$$u_{A/D}(s_N, \pi_A, \pi_D) = \sum_{t=0}^{\infty} \beta^t \mathbb{E}[r_{A/D}(s^t, a_D^t, a_A^t, s^{t+1})], \quad s^0 = s_N$$

The Nash equilibrium provides the optimal action for each player at each state





There are several challenges to finding the solution.

1. Large parameter space: 576 probabilities
2. Parameter constraints: probability laws
3. Solution uniqueness

Stochastic game theory is a promising method for selecting cybersecurity control actions for nuclear power plants.

- Threat actor was defined using threat agent libraries
- System-Theoretic Process Analysis was used to manage the stochastic state space
- The Common Vulnerability Scoring System was used to estimate transition probabilities
- Solving the game presents additional optimization challenges

Christopher C. Lamb
Sandia National Laboratories
cclamb@sandia.gov

Lee T. Maccarone
University of Pittsburgh
LTM10@pitt.edu