SAND2019-2454PE

LDRD

Laboratory Directed Research and Development

SECURE Uncertainty Quantification Thrust

Team Members:
Laura Swiler
Bert Debusschere
Gianluca Geraci
Jonathan Crussell

Presenter:
Laura Swiler

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and 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.

SECURE: **S**cience and **E**ngineering of **C**ybersecurity by **U**ncertainty quantification and **R**igorous **E**xperimentation

The Goal: Bring rigor into cyber experimentation

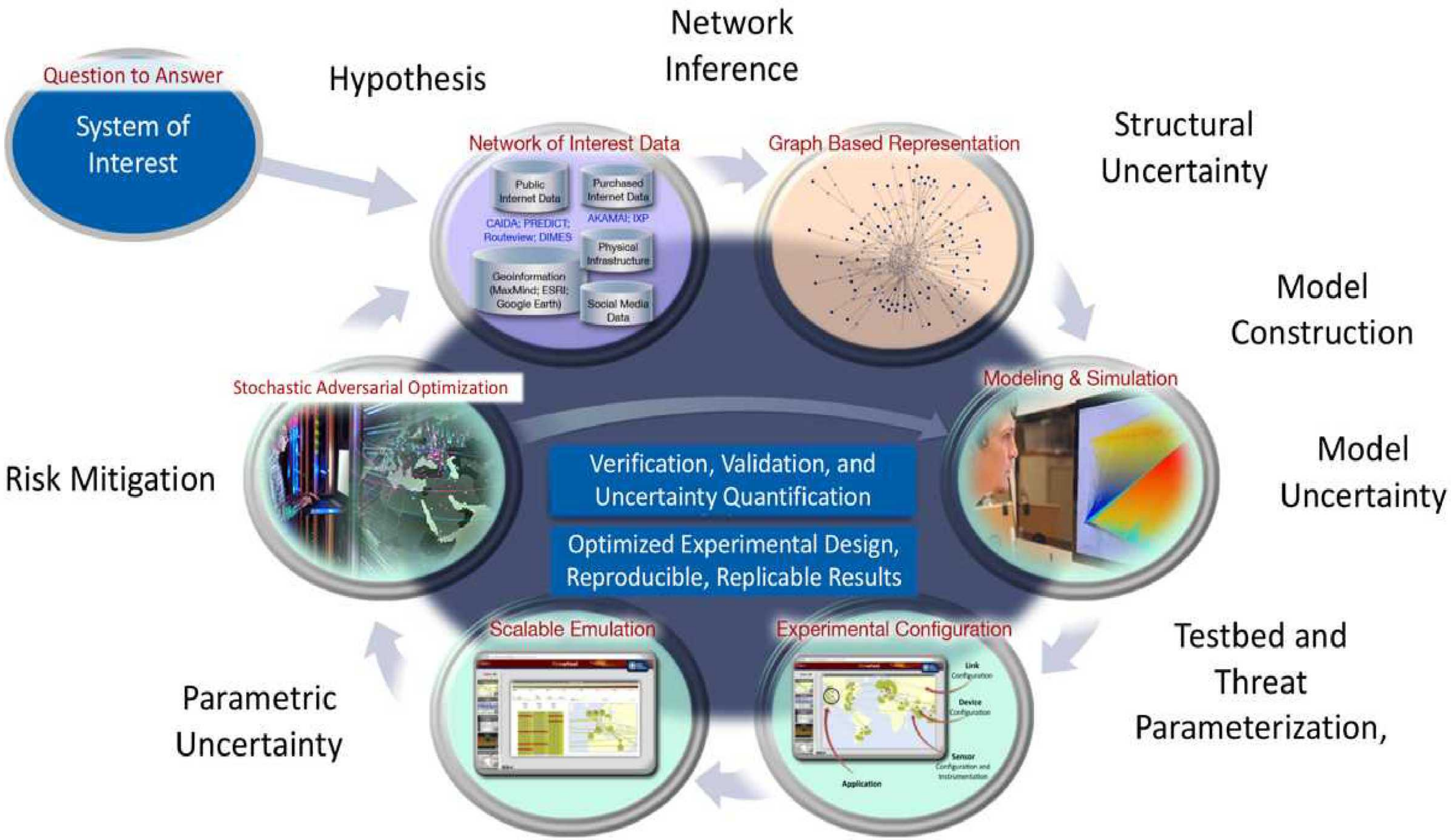
The Idea: Follow the principles of Computational Science and Engineering (CSE)

The Challenge: Cyber systems are different than those in traditional CSE applications.

UQ Team: Develop and deliver approaches which allow uncertainty quantification to be performed on Emulytics efficiently.

What does success look like?

Run experiments to answer "what if" questions at scale with confidence, characterizing and propagating uncertainties.



Hypothesis

Network Inference

Structural Uncertainty

Model Construction

Model Uncertainty

Testbed and Threat Parameterization,

Parametric Uncertainty

Risk Mitigation

Verification, Validation, and Uncertainty Quantification

Optimized Experimental Design, Reproducible, Replicable Results

What does success look like?

STEPS **Year 1**

1. Demonstrate that we can sample Emulytics models reproducibly across platforms
   - Establish interface to Emulytics models for running ensembles
   - Sampling strategies
   - Characterization of input distributions
2. Validate a specific Emulytics problem (e.g. a particular network and threat)
3. Develop methods that can perform the forward UQ problem more efficiently
   - Sampling of discrete variables, experimental design
   - Dimension reduction
   - Multi-fidelity approaches
4. Demonstrate a full UQ workflow that is generalized over multiple threats and networks at scale.

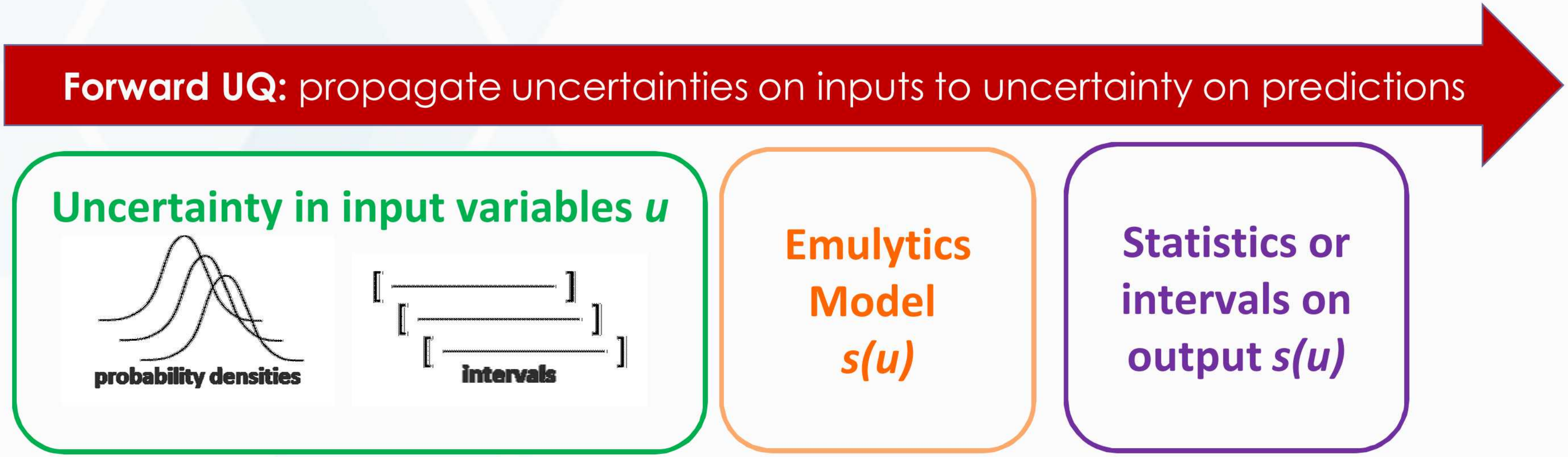
The UQ team is tightly interconnected with other teams

Uncertainty Quantification needs:	Emulytics	Optimization
Low and High Fidelity Emulytics Models (Cyber and Cyber physical)	✓	
Threat Models and threat representation	✓	
Identification of worst case scenarios to compare with UQ studies, provide bounding analyses and baseline scenarios		✓

Uncertainty Quantification provides:	Emulytics	Optimization
Experimental Design	✓	
Analysis capabilities (UQ and sensitivity analysis for threat models and for consequence analysis)	✓	✓
Assessment of convergence of coarser grained models	✓	
Uncertain scenarios for stochastic adversarial programs		✓

Research Thrust: Propagating Uncertainties

- **Discreteness and discontinuities**
- **Dimensionality Reduction**
- **Multifidelity Modeling**
- **Optimal Experimental Design**



Forward UQ: propagate uncertainties on inputs to uncertainty on predictions

Uncertainty in input variables *u*

Emulytics Model *s(u)*

Statistics or intervals on output *s(u)*

Dakota

- Toolkit of uncertainty quantification, sensitivity analysis, calibration, and optimization algorithms
- Flexible interface to simulation codes: one interface; many methods
- Continual advanced algorithm R&D to tackle computational challenges:
  - Treats non-smooth, discontinuous, multi-modal responses
  - Focus on methods that are as efficient and accurate as possible assuming simulations are very costly.
- Scalable parallel computing from desktop to HPC
- Started under LDRD in 1995, continued investment from NW Advanced Simulation and Computing program

Emulation Workflow

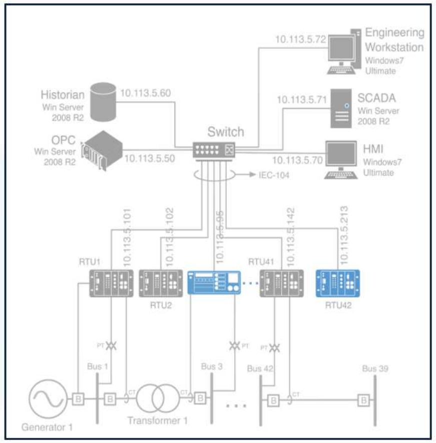
DAKOTA

Inputs

System Specification
- Devices
- Configuration
- Topology
- Connectivity
- Physical Processes

Threat Scenario:
- Actual malware
- Specify threat effect (e.g., kill RTU1)
- Red Team

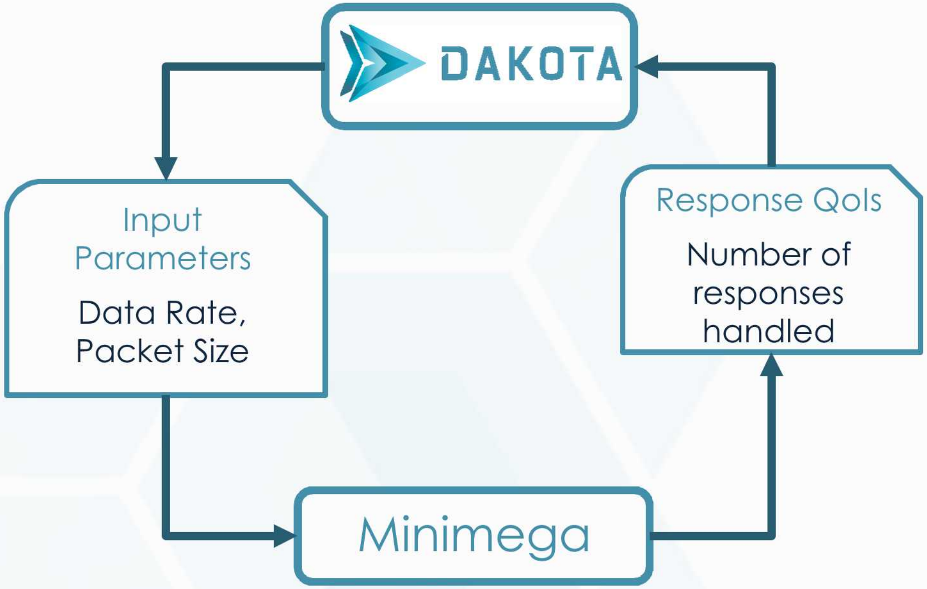
Emulation Platform: VMs, HITL, Simulation



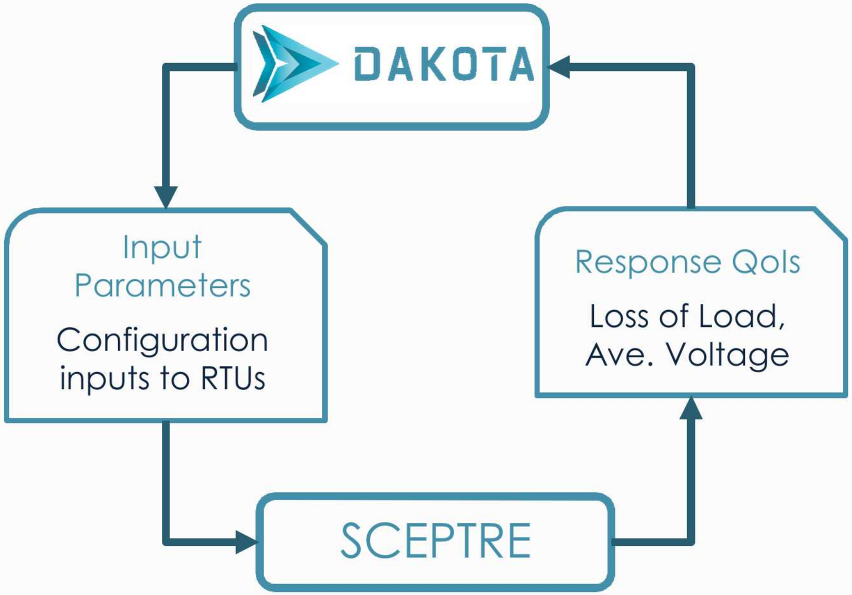
Outputs

Lots of options…
- Packets
- Host data
- Network data
- Physical Processes

Example of early Dakota studies



Simple model to examine HTTP traffic between client and server and demonstrate multi-fidelity methods

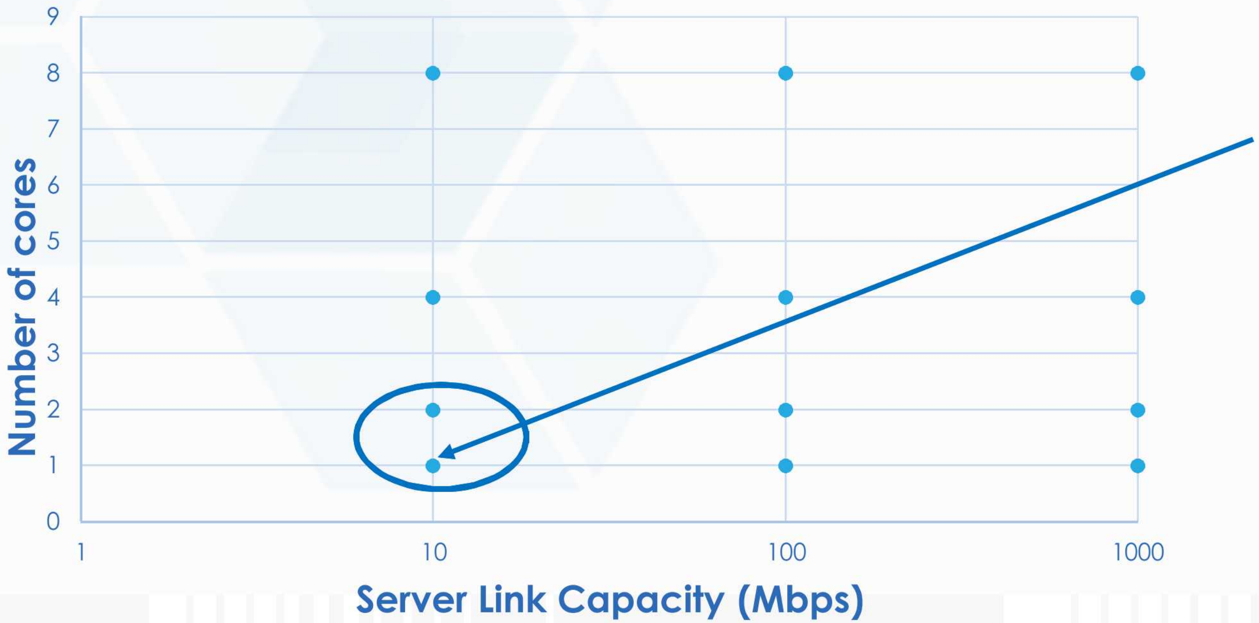


Parameter study performed where we take out a single RTU at a time by changing the value of the IP address of the RTU affected by the CRASH malware

Discreteness and discontinuities

- Want efficient ways of sampling large numbers of discrete variables when we can't enumerate all combinations
  - Continuous relaxation approaches
  - Sampling with PCE using polynomials for discrete variables
- Importance Sampling for discrete variables

$$E\left(r(x)\right) = \int r(x)\frac{f(x)}{h(x)}h(x)dx$$



How do we identify samples in a large combinatorial space which are of interest?

Experimental Design: which design is best?

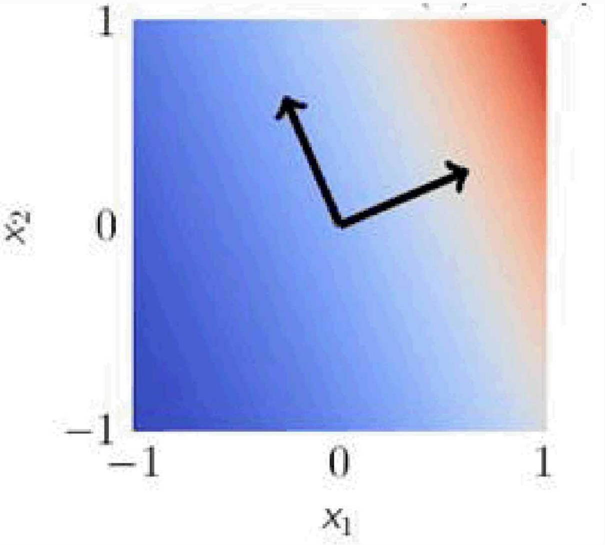
	Var 1	Var 2	Var 3	Var 4	Var 5	Var 6	Var 7	Var 8	Var 9	Var 10	Var 11	Var 12	Var 13	Var 14
D-optimal	1	4	2	3	1	2	2	1	2	3	2	4	2	3
	1	4	2	2	2	3	1	1	1	2	2	3	1	3
	2	2	2	2	1	2	2	4	2	1	2	1	2	3
	2	3	1	4	1	1	1	1	1	1	1	3	1	3
	1	2	1	1	1	2	2	3	2	1	1	4	1	2
	1	2	1	1	1	1	1	1	1	4	1	3	1	4
	2	2	2	2	1	4	1	1	1	2	2	3	2	1
	2	3	2	2	1	1	1	4	1	3	2	3	2	1
Supersaturated	2	3	1	2	2	1	1	4	1	2	2	4	2	3
	2	3	2	3	1	2	2	1	1	4	1	2	2	4
	2	4	2	3	2	3	1	2	2	1	1	4	1	2
	1	2	2	4	2	3	2	3	1	2	2	1	1	4
	1	4	1	2	2	4	2	3	2	3	1	2	2	1
	2	1	1	4	1	2	2	4	2	3	2	3	1	2
	1	2	2	1	1	4	1	2	2	4	2	3	2	3
	1	1	1	1	1	1	1	1	1	1	1	1	1	1
LHS	1	1	1	2	2	3	2	1	1	2	1	3	2	2
	2	4	2	3	1	1	2	2	2	2	1	4	1	3
	1	1	2	4	1	4	2	1	2	1	1	1	2	3
	1	3	2	2	2	4	1	3	1	4	2	2	1	4
	2	3	1	3	2	1	2	2	1	3	2	4	2	4
	1	4	1	1	1	3	1	4	1	4	2	1	2	1
	2	2	1	1	1	2	1	3	2	3	2	3	1	2
	2	2	2	4	2	2	1	4	2	1	1	2	1	1

Experimental Design

- Want to identify best points at which to sample M variables, where the number of samples we can afford may be less than N: N < M
- Want to handle mixed discrete and continuous variables
- Comparison of D-optimal, supersaturated, and LHS designs showed that traditional metrics don't work.
    - For example, the determinant of the information matrix $|(X^T X)|$ is singular. The determinant = 0 for all three cases.
- Plan to investigate other measures of dependency between factors and orthogonality between columns.

Efficiency Improvements for UQ

- **Dimension Reduction**
  - Determine a reduced or compressed representation of the Emulytic model's inputs and/or outputs.
  - Reduced space techniques involve a linear or nonlinear mapping between the full space to a reduced space of meta variables. Example: Principal components analysis (XPCA), active subspace



- **Multifidelity approaches**
  - Take a large number of low fidelity runs and a small number of high fidelity runs to achieve statistics on high fidelity responses
  - Relies on variance reduction: must have correlation between the low and high fidelity model
  - Active work on continuous problems→ translate to discrete

XPCA: eXtending PCA for Combinations of Discrete and Continuous Data, Kincher-Winoto, Kolda, and Anderson-Bergman, SAND2018-8213C. Also at: arXiv:1808.07510

UQ Support of Validation for Emulytics Models

- **Validation:**
  - Fundamental question: "Is this Emulytics model acceptable for this application?"
    - What level of network aggregation is acceptable?
    - Which quantities of interest should be used to make meaningful comparisons?
    - What are the validation metrics?

  - **Compare QoI distributions from Emulytics with Physical System**
  - **Compare QoI sensitivities from Emulytics with Physical System**

  - For small systems, Emulytics tools can be validated through *direct comparison* with experiments on actual networks.
  - As complexity increases, we will verify convergence in the sense that uncertainties and discrepancies *decrease* as more data and fidelity is added to the Emulytics model.

Publication Plan

Publication	Milestone Date
International Conference on Uncertainty Quantification in Computational Sciences and Engineering	19Q3
12th USENIX Workshop on Cyber Security Experimentation and Test (CSET)	19Q4
Multifidelity approaches for network Emulytics models: SIAM/ASA Journal on Uncertainty Quantification	20Q4
Experimental Design/Dimension reduction for Emulytics models: Journal of Network and Computer Applications	21Q4

Communication Plan

Venue	Year
International Conference on Uncertainty Quantification in Computational Sciences and Engineering	19Q3
12th USENIX Workshop on Cyber Security Experimentation and Test (CSET)	19Q4
SIAM Conference on Uncertainty Quantification	20Q2
13th USENIX Workshop on Cyber Security Experimentation and Test (CSET)	20Q4
SIAM Computational Science and Engineering	21Q2
14th USENIX Workshop on Cyber Security Experimentation and Test (CSET)	21Q4

Software Plan

Software Package	New Science & Technology
Dakota	Multi fidelity UQ methods handling discrete variables and Emulytics models Dimension Reduction
SECUREtk.uq	Experimental Design and Sampling Methods

Backup

Structural / Model Uncertainties

- **Structural uncertainties** can manifest either as an ensemble of possible network structures. We will start with a fixed network structure but with some probability about degradation of various nodes and edges.
- **Model form uncertainty:** how do we pose a discrepancy or error term/function that represents the difference:
  - Between the emulytics model and physical, observed data
  - Between emulytics models A and B
  - Between emulytics model A and mathematical program B (or discrete event simulation or …)