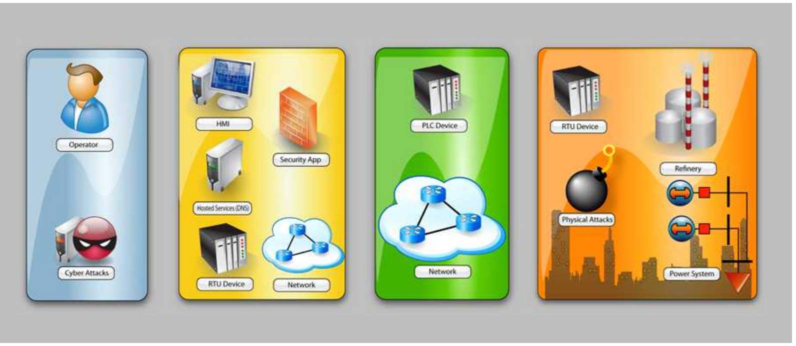
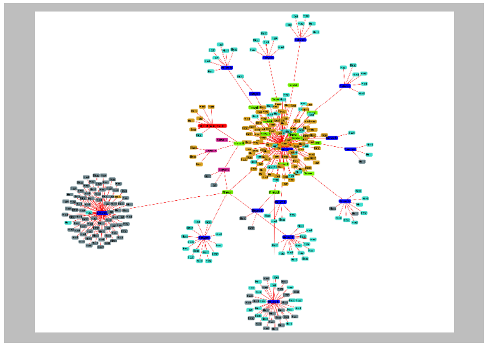
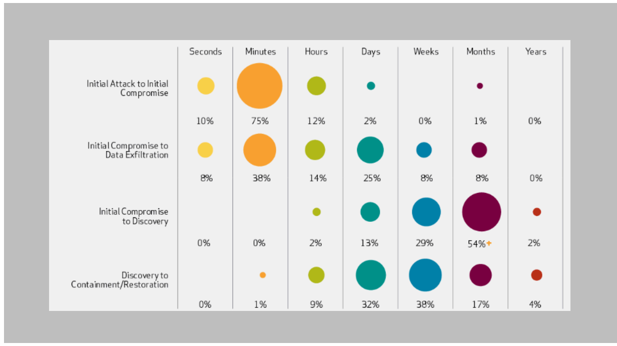
SAND2015-8605PE

Exceptional service in the national interest

Sandia National Laboratories







Seconds
Minutes
Hours
Days
Weeks
Months
Years
Initial Attack to Initial Compromise
10%
75%
12%
2%
0%
1%
0%
Initial Compromise to Data Exfiltration
8%
38%
14%
25%
8%
8%
0%
Initial Compromise to Discovery
0%
0%
2%
13%
29%
54%+
2%
Discovery to Containment/Restoration
0%
1%
9%
32%
38%
17%
4%

Emulytics™ Overview

Shawn Taylor

(505) 845-3693, setaylo@sandia.gov

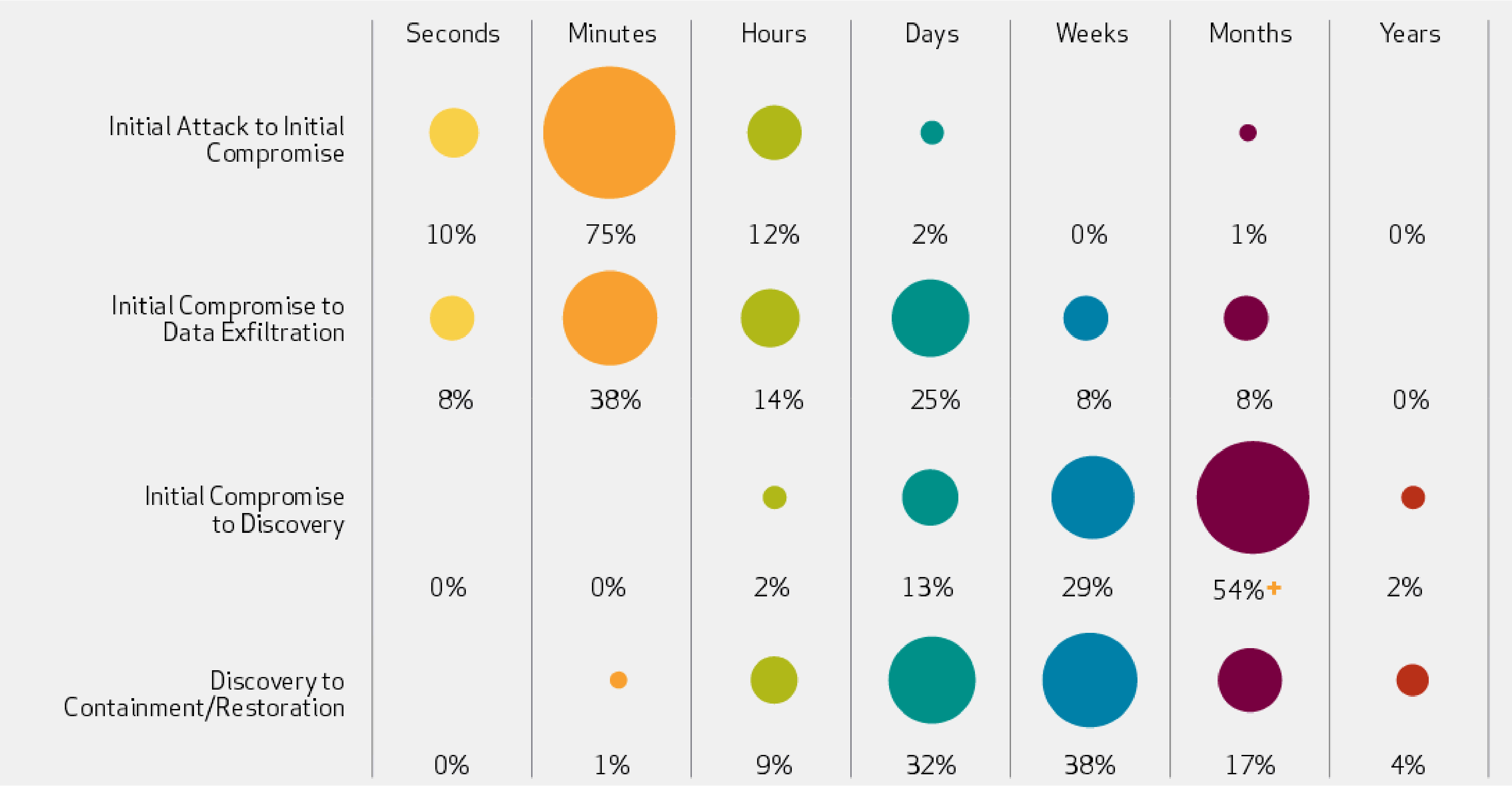
U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Why Modeling & Simulation?

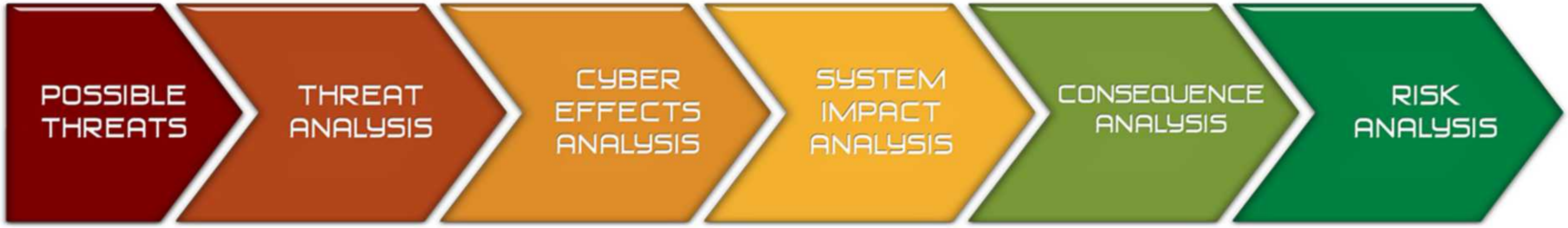
855 breaches, 174 million compromised records in 2011



	Seconds	Minutes	Hours	Days	Weeks	Months	Years
Initial Attack to Initial Compromise	10%	75%	12%	2%	0%	1%	0%
Initial Compromise to Data Exfiltration	8%	38%	14%	25%	8%	8%	0%
Initial Compromise to Discovery	0%	0%	2%	13%	29%	54%+	2%
Discovery to Containment/Restoration	0%	1%	9%	32%	38%	17%	4%

Source: Verizon Data Breach Investigation Report 2012

Risk-Based Approach



GOAL: Reduce risk of disruptions & failures due to cyber attacks on control systems

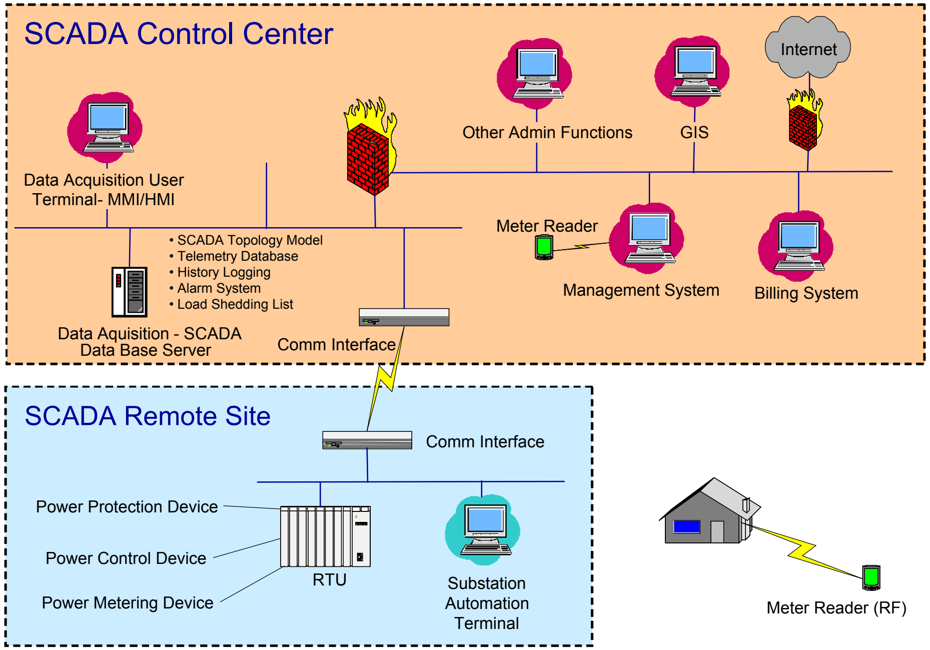
$$\text{Risk} = D \times C$$

Difficulty

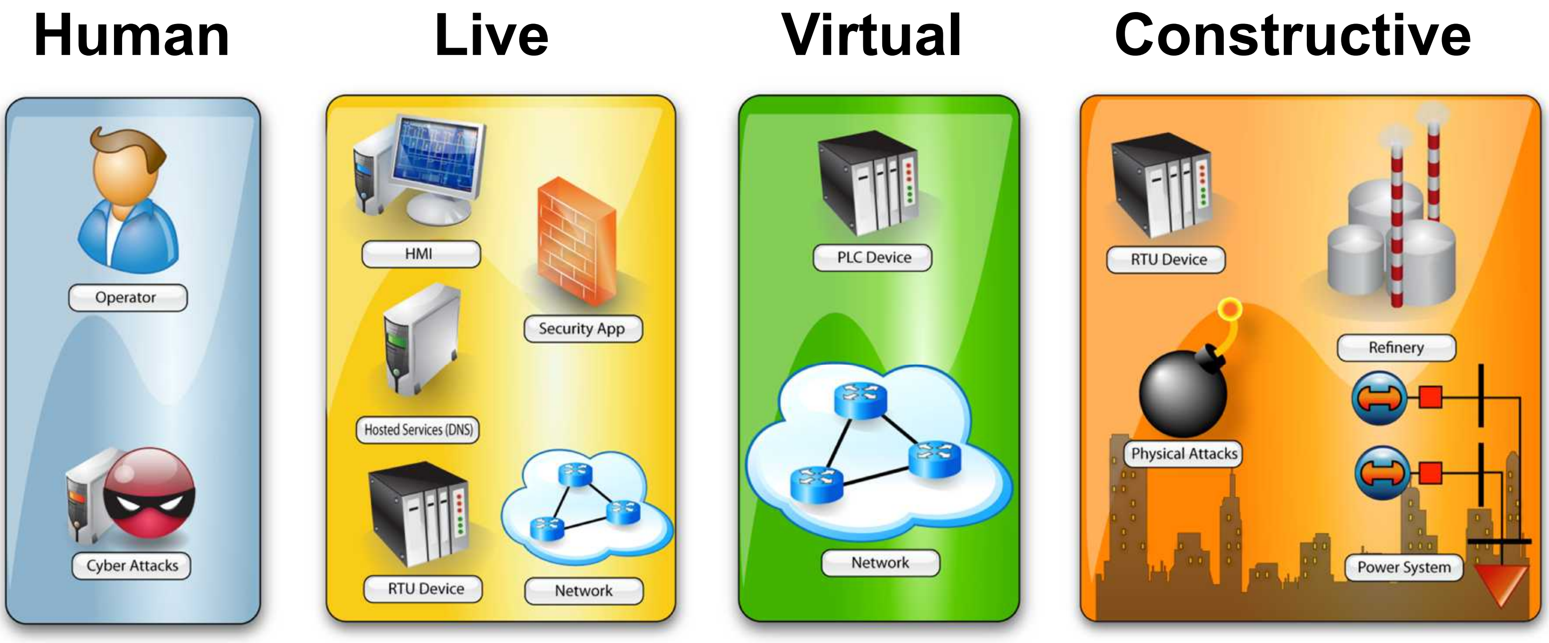
Consequence

Trends Causing Increased Risk

- Adoption of standardized technologies with known vulnerabilities
- Connectivity of control systems to other networks
- Insecure connections
- Increasing reliance on automation
- Widespread availability of technical information about control systems



What is Emulytics™?



Human

Operator

Cyber Attacks

Live

HMI

Security App

Hosted Services (DNS)

RTU Device

Network

Virtual

PLC Device

Network

Constructive

RTU Device

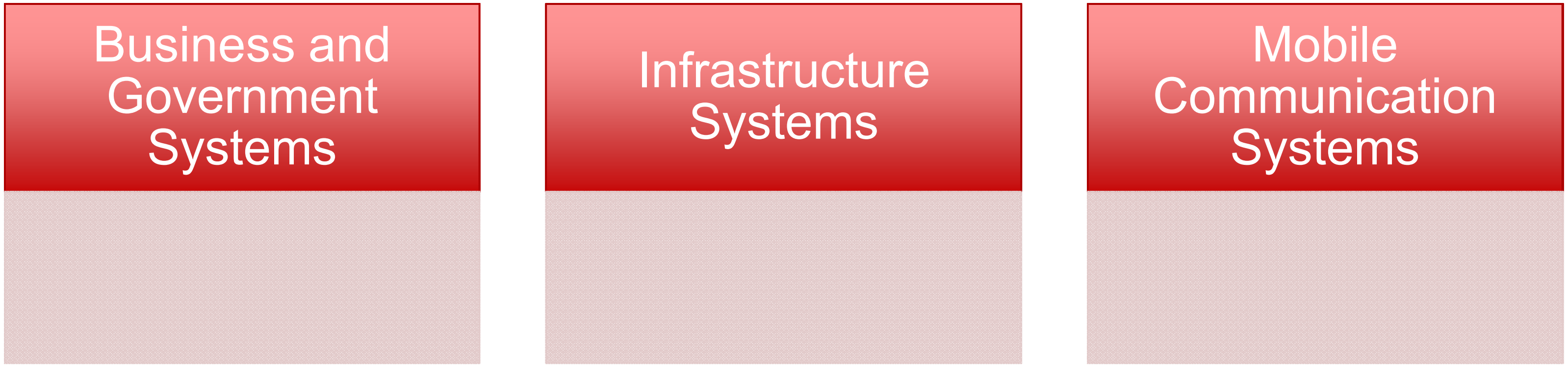
Refinery

Physical Attacks

Power System

What is Emulytics™?

- Capability to:
  - Create model of system of interest (operational or conceptual)
  - Create scenarios that transition modeled system into states of interest
    - Architecture, devices, configuration (correct/incorrect), traffic, …
    - Cyber defender scenarios
  - Extensive instrumentation for data collection
  - Perform analytics on resulting data
  - Answer questions about system

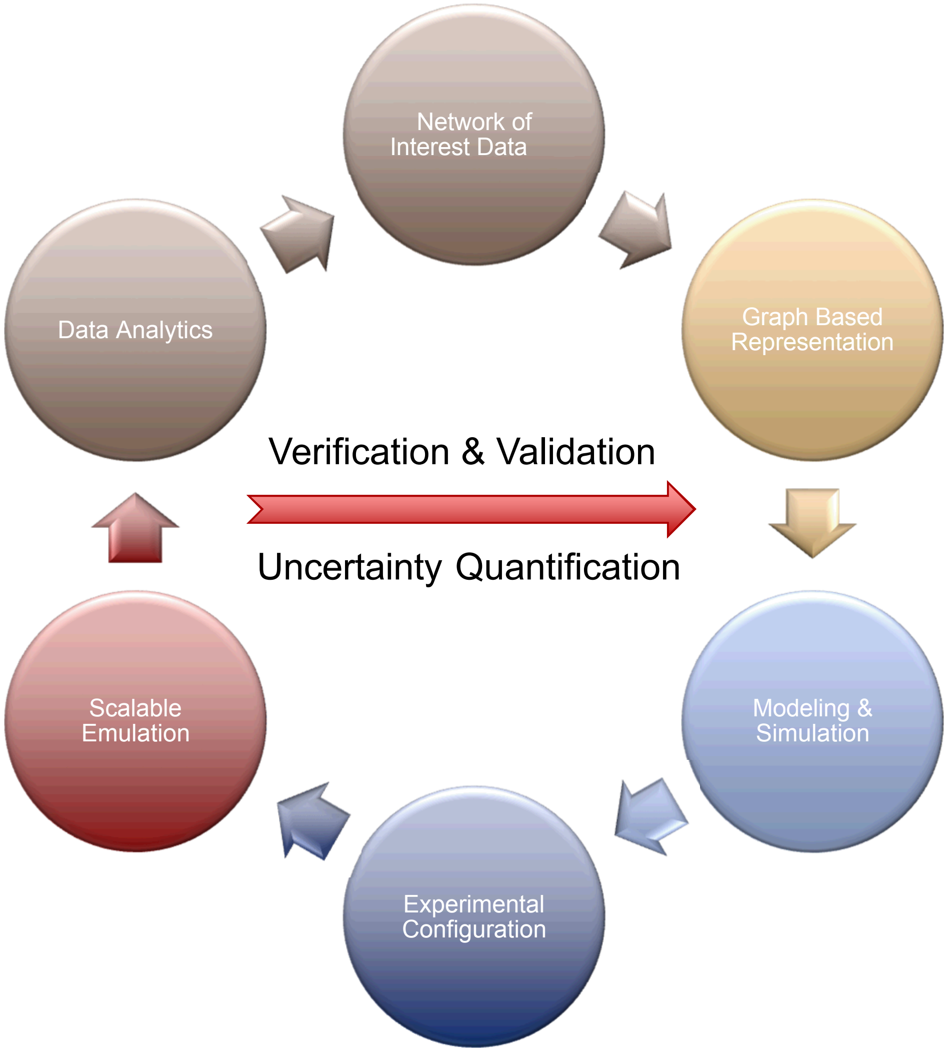


Business and Government Systems

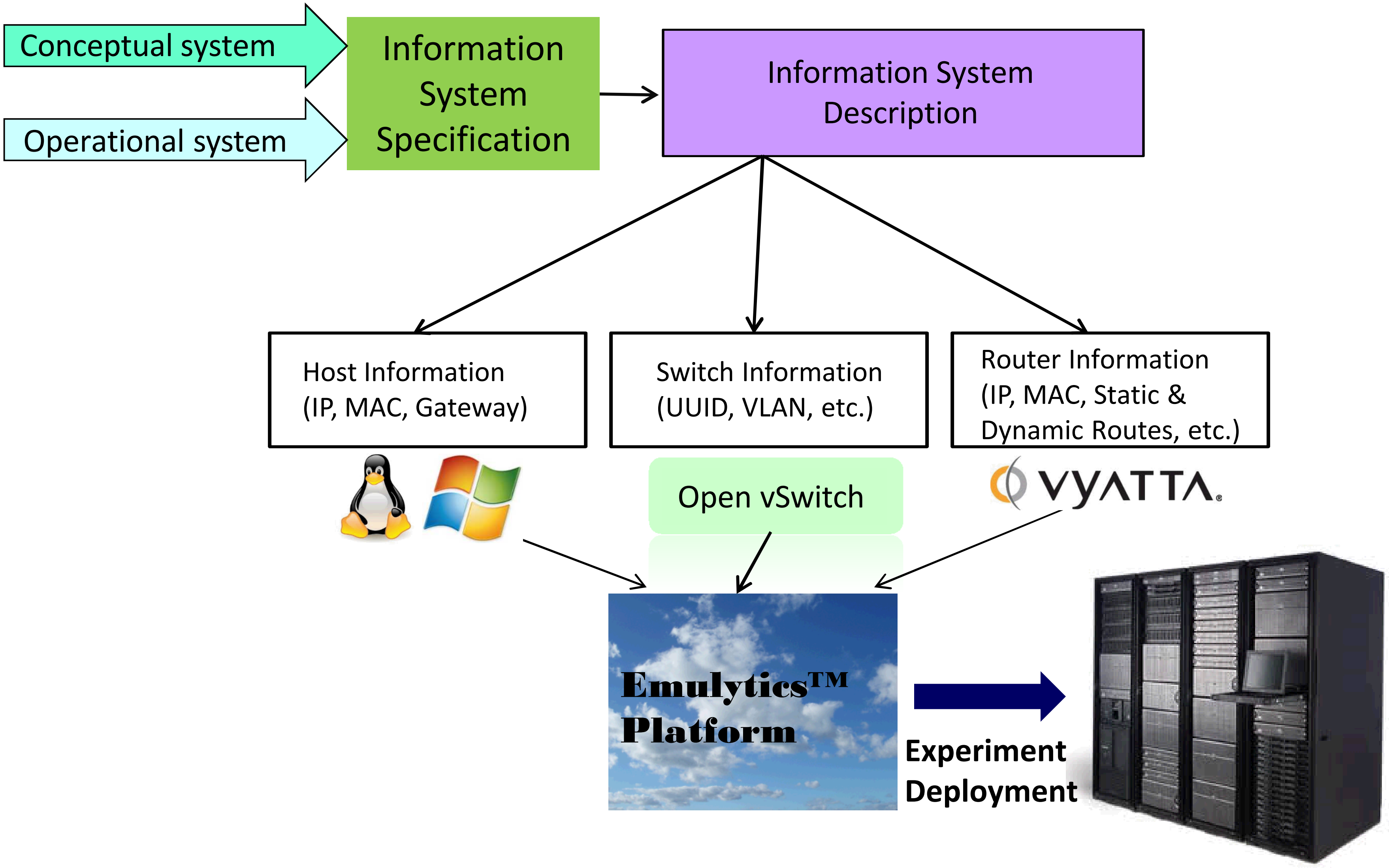
Infrastructure Systems

Mobile Communication Systems

The Emulytics™ Process


Network of Interest Data
Graph Based Representation
Modeling & Simulation
Experimental Configuration
Scalable Emulation
Data Analytics
Verification & Validation
Uncertainty Quantification

The Emulytics™ Process



Conceptual system

Operational system

Information System Specification

Information System Description

Host Information (IP, MAC, Gateway)

Switch Information (UUID, VLAN, etc.)

Router Information (IP, MAC, Static & Dynamic Routes, etc.)

Open vSwitch

Emulytics™ Platform

Experiment Deployment

Network

- Arbitrary network topologies with Open vSwitch
- Scales (load is distributed to physical network hardware)
- Routers Supported
  - Juniper vMX
  - Vyatta (Brocade)
  - Cisco (NEXUS)
  - Arista (Eos)
- Connectivity
  - Enterprise: switched vlans, routed
  - Core: ISP - BGP

External Connectivity

- Hardware in the Loop (HITL)
  - Any IP addressable device
- Ability to bridge experiment network to real network
- Simulation in the loop (SITL)

Performance

- ~Minutes to bring up nearly all experiments
  - Generally bounded by boot time of guest OS and services on the guest
- Platform setup/teardown near instantaneous
  - Well suited for iterating multiple variants of a single experiment

Verification and Validation

"essentially, all models are wrong, but some are useful"

George E. P. Box