SAND2006-6088C

Evidence-Based Techniques for Evaluating Cyber Protection Systems for Critical Infrastructures

J. Darby, J. Phelan, P. Sholander, B. Smith, A. Walter and G. Wyss

October 25, 2006

James Phelan
Distinguished Member of Technical Staff
Sandia National Laboratories

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Technical Overview and Assumptions

Overall Research goal:

- Develop a risk assessment methodology that supports analysis of integrated physical and cyber security elements within Critical Infrastructure (water, power, gas, etc.) systems

Most important outcomes:

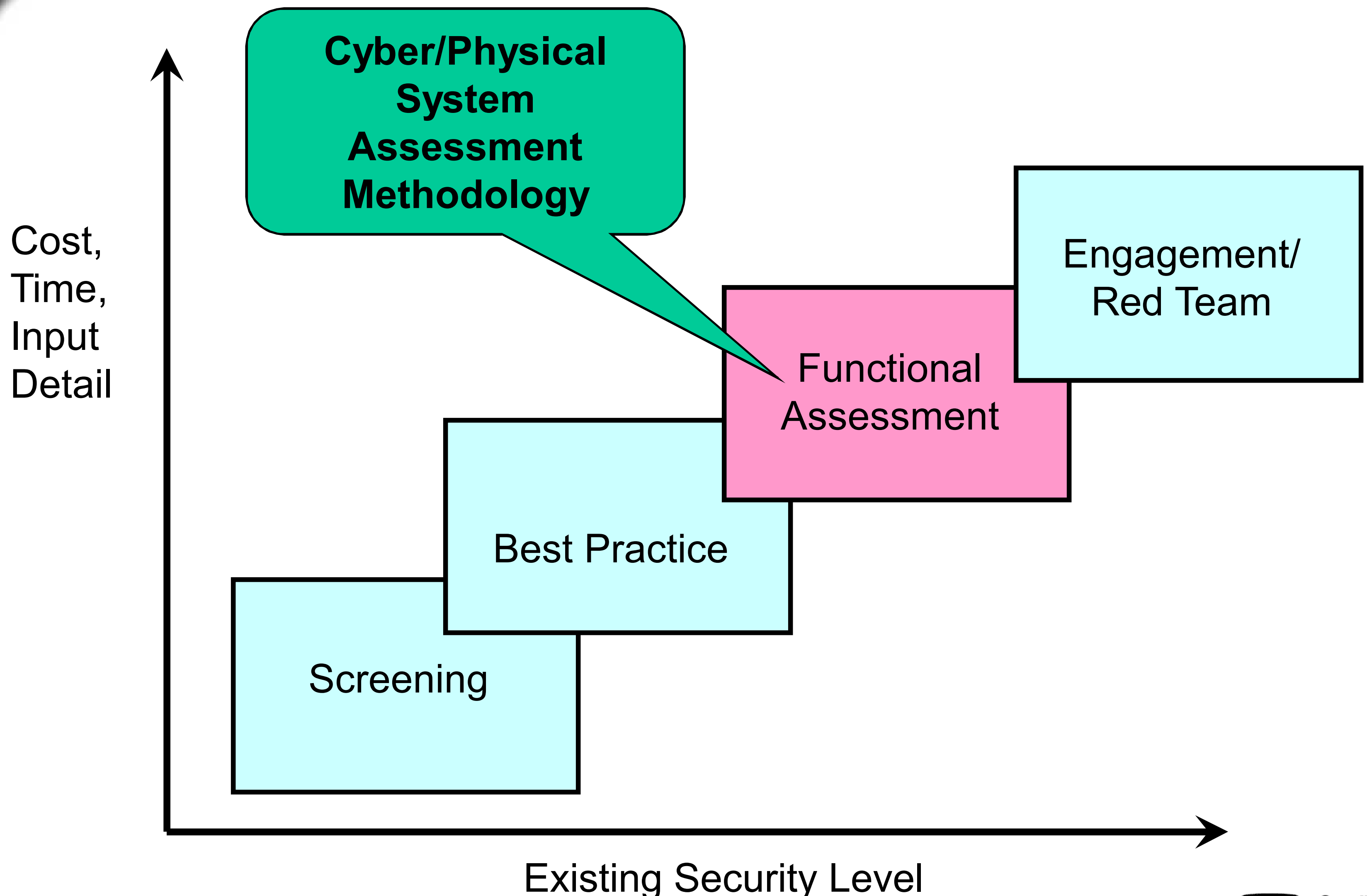
- A better understanding of the interrelation between cyber and physical security and its implications for unidentified vulnerabilities
- Provide decision makers with integrated and comprehensive risk results.
  - Cost-effective security upgrades that reduce overall risk

This talk's focus:

- Evidence-based techniques for evaluating cyber protection system effectiveness

Sandia National Laboratories

Capability-Based Structured Analysis Methodology



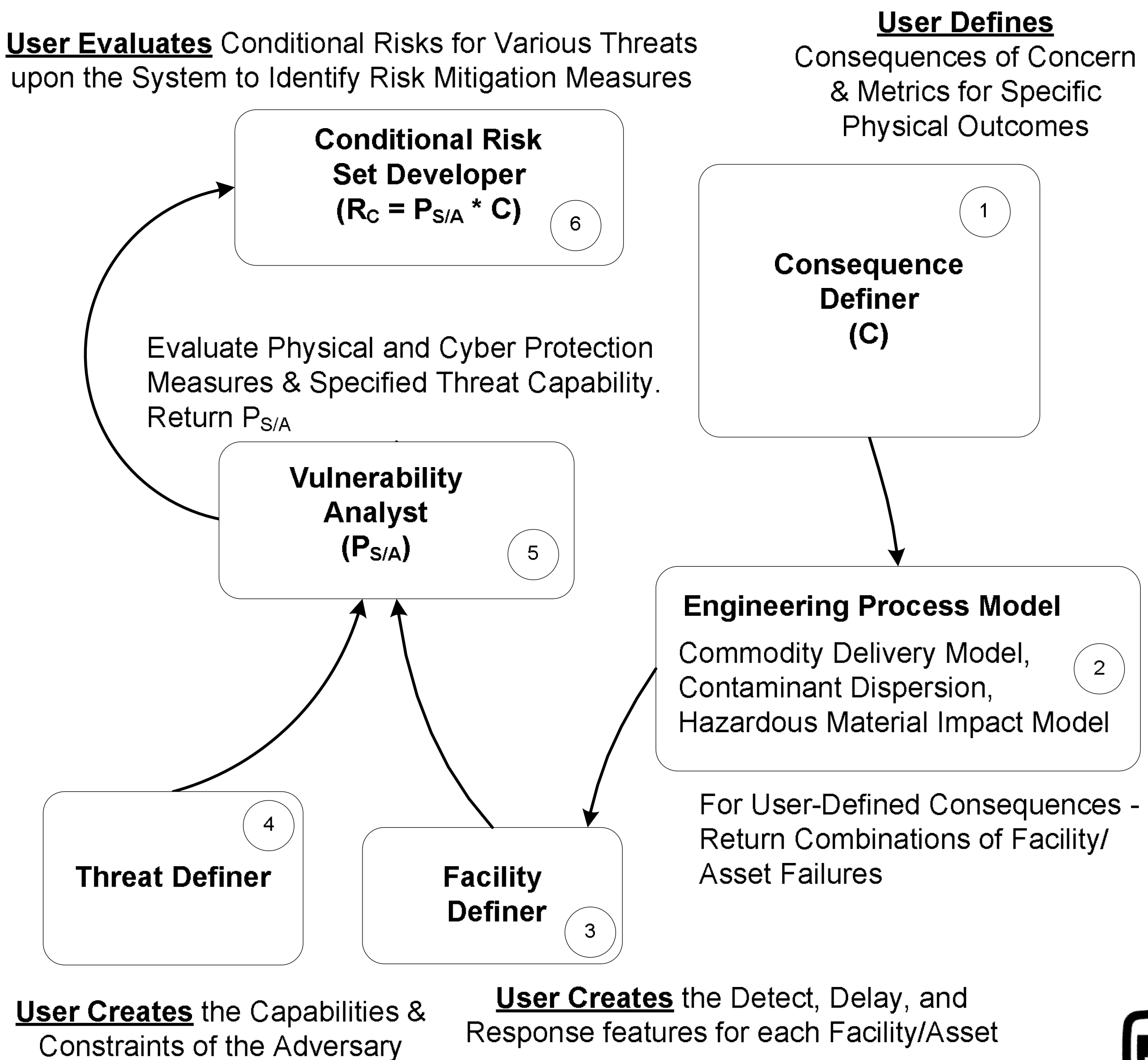
Sandia National Laboratories

CPSAM Methodology Highlights

- Conditional risk
  - Risk, given a defined attack
- Consequence based
  - Loss of fire fighting, loss of potable water, …
  - Consequence common measure (i.e., willingness to pay)
- Physical security
  - Detect, delay, and respond approach
- Cyber security
  - Category-based approach for comparing cyber threat against security primitives
  - Cyber protective system effectiveness quantified for joint evaluation of cyber/physical system effectiveness
- Evidence-based techniques
  - Belief/plausibility methods generalize probabilistic uncertainty using degree of evidence
    - Cyber vulnerability
    - Consequence

Sandia National Laboratories

CPSAM User Modules



Sandia National Laboratories

Blended Attack Types

- **Physical Attack**
  - Physical only
  - Cyber-enabled physical

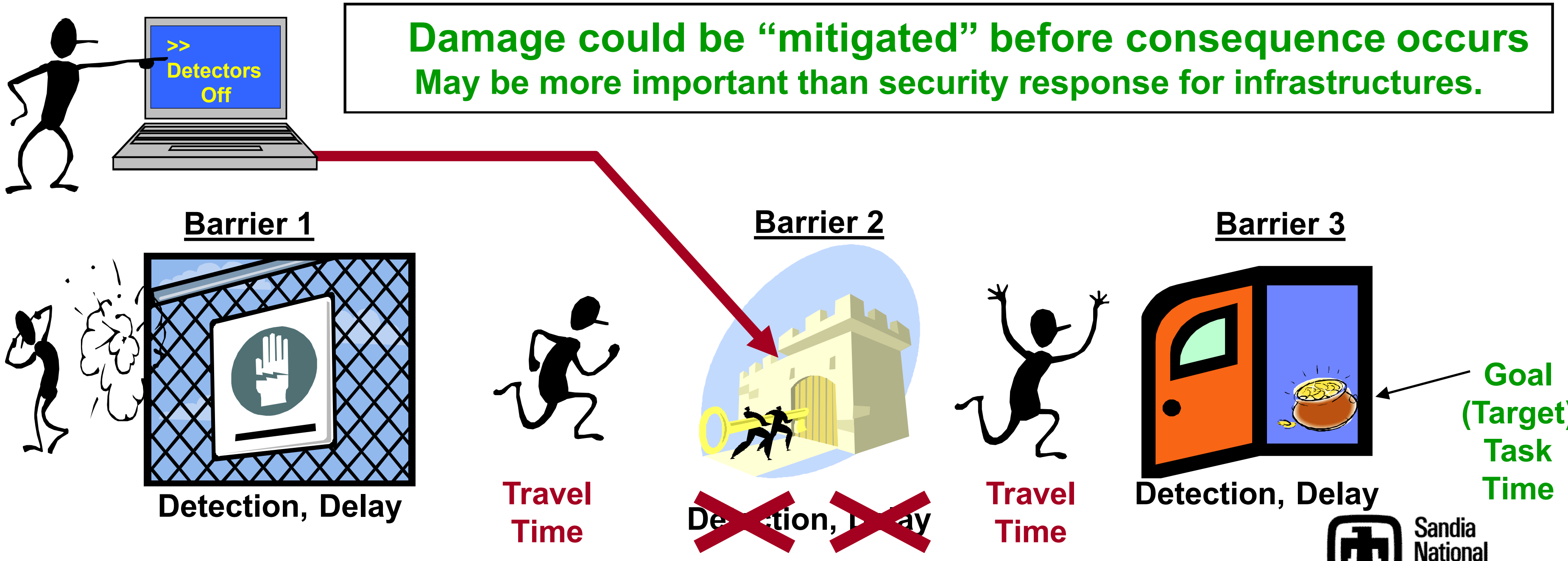
> - Adversary must gain physical access to asset
>   - Asset failure induced at asset location
> - Includes cyber-enabled physical attack
>   - Cyber-controlled PPS elements disabled by cyber means
>   - Can occur only if PPS elements are cyber-controlled

- **Cyber Attack**
  - Cyber only
  - Physically enabled cyber

> - Adversary causes asset failure without gaining physical access to it
> - Occurs only if asset is cyber-controlled and can be caused to fail by cyber means
> - Includes physically enabled cyber attack
>   - Launched from on-site location
>   - Physical attack to gain access to location from which cyber attack occurs

Assessment of Blended Security Systems

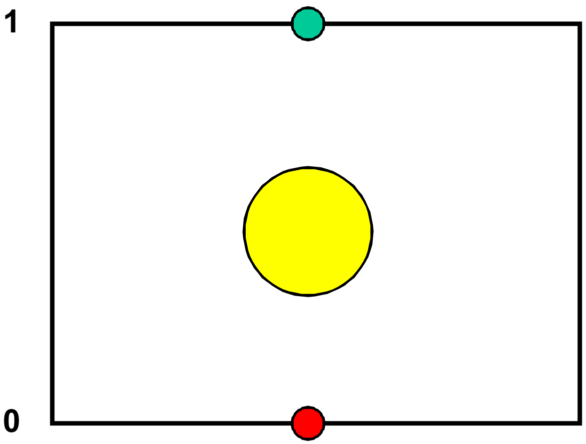
- **Evaluation is based on "timely detection": Can the good guys respond before the bad guys accomplish their goal?**
  - Each barrier has a task or delay time and a probability of detection
  - Cyber attacks can shut off security delay or detection elements
    - Cyber attacks can disable security elements before physical attack starts
    - Bad guys' optimal path depends on which elements can be defeated, given their cyber and physical attack skills



Sandia National Laboratories

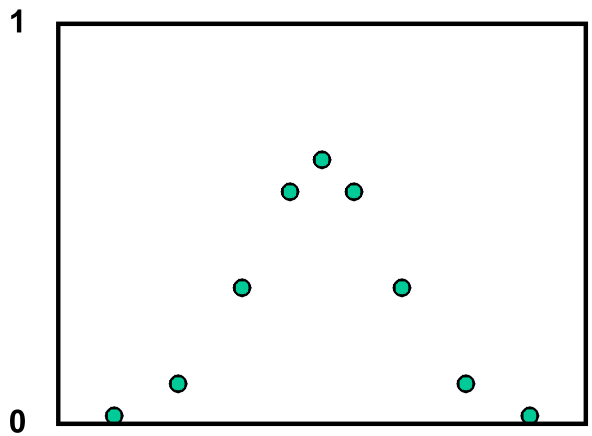
Estimating Security System Effectiveness

Certainty



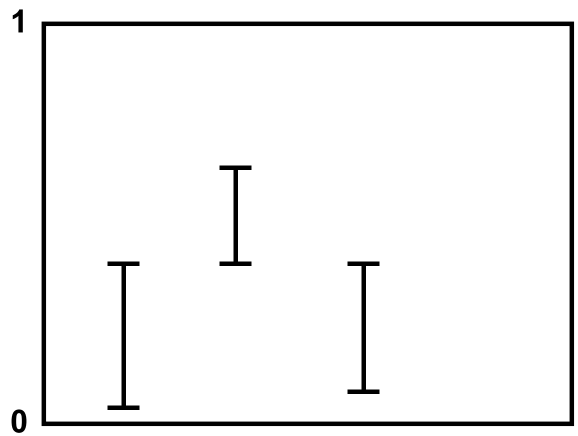
Yes/No/Maybe

Probability



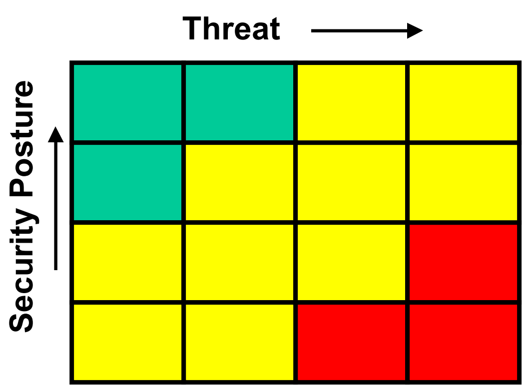
Mean/StdDev

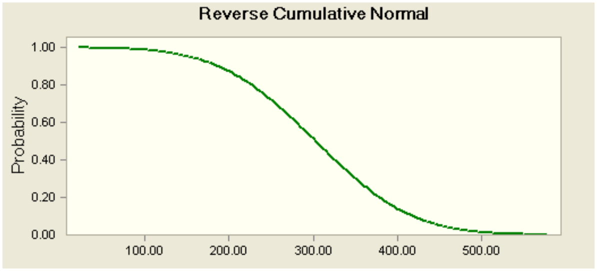
Belief/Plausibility



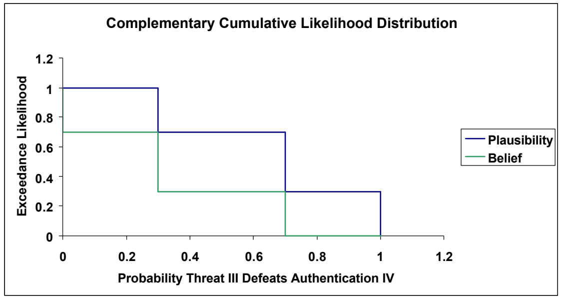
Interval

Likelihood that Threat Beats Cyber or Physical Protective System





Response Force Time: Mean 300 sec, Stdev 90 sec



Evidence	
[0,0.3)	0.3
[0.3,0.7)	0.4
[0.7,1.0]	0.3

Sandia National Laboratories

Why Use Evidence-Based Techniques?

- Risk from a random event, such as an earthquake is "aleatory" (stochastic or random)
  - Probability is well suited for analyzing aleatory uncertainty
- Terrorist acts are not a random event
  - Intentional act by a thinking, malevolent adversary who carefully selects, plans and executes the attack.
  - Uncertainty of the risk of a terrorist act is "epistemic" (state of knowledge).
  - Act is not a random event but we have significant uncertainty as to what the adversary will do.
- Belief captures the uncertainty in the inputs to the risk analysis process and propagates that uncertainty through to the outputs
- Research Goal
  - Combine evidence-based math techniques with attack graph techniques for evaluating CPS
  - Make attack graphs applicable to conditional risk calculations for blended security systems

Sandia National Laboratories

Threat Definer

- **Specify specific adversary capabilities**
  - Based on perceived threat level
- **Physical-attack capabilities**
  - Examples are hand-tools, power-tools, explosives and vehicles
- **Cyber-attack capability attributes**
  - Funding
  - Goal Intensity Commitment
  - Stealth
  - Physical Access
  - Cyber Skills
  - Implementation Time
  - Cyber Organization Size

Sandia National Laboratories

Cyber Adversary Model

Category	Funding	Goal Intensity	Stealth	Physical Access	Cyber Skills	Implementation Time	Cyber Org Size
I	H	H	H	H	H	Decades/Years	Hundreds
II	H	H	H	M	M	Years	Tens of Tens
III	M	H	M	M	M	Months	Tens
IV	L	M	H	L	H	Months	Tens
V	L	M	M	L	M	Months	Ones
VI	L	L	L	L	L	Weeks	One

- Based on seven adversary characteristics
- Purposefully avoids labels such as “hacker”
- Adversary types should “well-cover” the range of possible values for the seven attributes

Sandia National Laboratories

Authentication (A) Security Primitive

Category	Cyber Security Posture
I	No Passwords
II	Weak passwords. No periodic changes.
III	Strong passwords. No periodic changes.
IV	Strong passwords. Periodic Changes.
V	Strong passwords. Periodic Changes. Limits on failed password attempts. Passwords are cracked every month to find users with easily guessed passwords.

	Threat Category					
Authentication Category	**I**	**II**	**III**	**IV**	**V**	**VI**
I (No Passwords)	[1] 1	[1] 1	[1] 1	[1] 1	[1] 1	[1] 1
II (Weak passwords. No periodic changes.)	[1] 1	[1] 1	[1] 1	[1] 1	[0.9,1] 1	[0.8,1] 1
III (Strong passwords. No periodic changes.)	[1] 1	[0.7, 1) 0.1 [1] 0.9	[0.7, 1) 0.2 [1] 0.8	[0.7, 1) 0.2 [1] 0.8	[0.7, 1) 0.4 [1] 0.6	[0,0.3) 0.8 [0.3,0.7) 0.1 [0.7,1.0] 0.1
IV (Strong passwords. Periodic changes.)	[1] 1	[0.7, 1) 0.3 [1] 0.7	[0,0.3) 0.3 [0.3,0.7) 0.4 [0.7,1.0] 0.3	[0] 0.5 (0,0.3] 0.5	[0] 0.7 (0,0.3] 0.3	[0] 0.9 (0,0.3] 0.1
V (Strong passwords. Periodic changes. Limits on failed password attempts.)	[1] 1	[0.7,1.0) 0.5 [1] 0.5	[0,0.3) 0.6 [0.3,0.7] 0.4	[0] 0.9 (0, 0.3] 0.1	[0] 0.9 (0, 0.3] 0.1	[0] 1

Sandia National Laboratories

Network Access Control (N) Security Primitive

Category	Cyber Security Posture
I	Remote login via password-protected dial-up connections. No Firewall.
II	Remote logins allowed from Internet. IP Address Filtering and Port Blocking.
III	Remote logins allowed via VPN connection
IV	No remote logins. SCADA Controls accessible only from LAN terminals.
V	No remote logins. SCADA LAN is physically separate from other LANs.

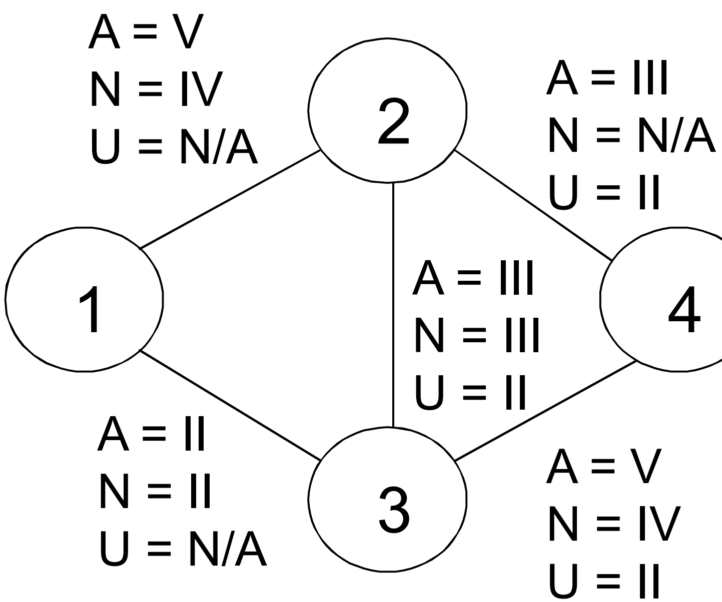
	Threat Category					
Network Access Control (N) Category	**I**	**II**	**III**	**IV**	**V**	**VI**
I (Password-protected dial-up. No firewall.)	[1] 1	[1] 1	[1] 1	[1] 1	[0.7,1] 1	[0.3, 0.7) 0.5 [0.7,1] 0.5
II (Remote login from Internet. Firewall.)	[1] 1	[0.3, 0.7) 0.2 [0.7, 1.0] 0.8	[0.3, 0.7) 0.5 [0.7, 1.0] 0.5	[0.3, 0.7) 0.2 [0.7, 1.0] 0.8	[0.3, 0.7) 0.5 [0.7, 1.0] 0.5	[0, 0.3) 0.8 [0.3, 0.7] 0.2
III (Remote logins via VPN.)	[1] 1	[0, 0.3) 0.5 [0.3, 0.7] 0.5	[0, 0.3) 0.8 [0.3, 0.7] 0.2	[0.3, 0.7) 0.8 [0.7, 1.0] 0.2	[0, 0.3) 0.8 [0.3, 0.7] 0.2	[0] 1
IV (No remote logins. SCADA net not physically isolated from other LANs.)	[1] 1	[0.3, 0.7) 0.2 [0.7, 1.0] 0.8	[0.3, 0.7) 0.8 [0.7, 1.0] 0.2	[0] 0.6 (0, 0.3] 0.4	[0] 0.8 (0, 0.3] 0.2	[0] 1
V (No remote logins. SCADA LAN physically isolated from other LANs.)	[1] 1	[0, 0.3) 0.5 [0.3, 0.7] 0.5	[0, 0.3) 0.8 [0.3, 0.7] 0.2	[0] 0.8 (0, 0.3] 0.2	[0] 0.9 (0, 0.3] 0.1	[0] 1

User Access Control (U) Security Primitive

Category	Cyber Security Posture
I	Physical Access unmonitored. Rights given to everyone.
II	Physical Access monitored. Rights assigned to individual users.
III	Rights assigned to groups. All cyber equipment is physically secured.

	Threat Category					
User Access Control (U) Category	**I**	**II**	**III**	**IV**	**V**	**VI**
I (Physical access unmonitored. Rights given to everyone.)	[1] 1	[0.7,1] 1	[0.3, 0.7) 0.2 [0.7, 1.0] 0.8	[0.3, 0.7) 0.5 [0.7, 1.0] 0.5	[0.3, 0.7) 0.8 [0.7, 1.0] 0.2	[0, 0.3) 0.8 [0.3, 0.7] 0.2
II (Physical access monitored. Rights given to individuals.)	[1] 1	[0.3, 0.7) 0.2 [0.7, 1.0] 0.8	[0.3, 0.7) 0.5 [0.7, 1.0] 0.5	[0, 0.3) 0.8 [0.3, 0.7] 0.2	[0, 0.3] 1	[0] 0.8 (0,0.3] 0.2
III (Rights given to groups. All equipment is physically secured.)	[1] 1	[0.3, 0.7) 0.5 [0.7, 1.0] 0.5	[0, 0.3) 0.8 [0.3, 0.7] 0.2	[0] 0.8 (0,0.3] 0.2	[0] 0.9 (0,0.3] 0.1	[0] 1

Example Cyber Network



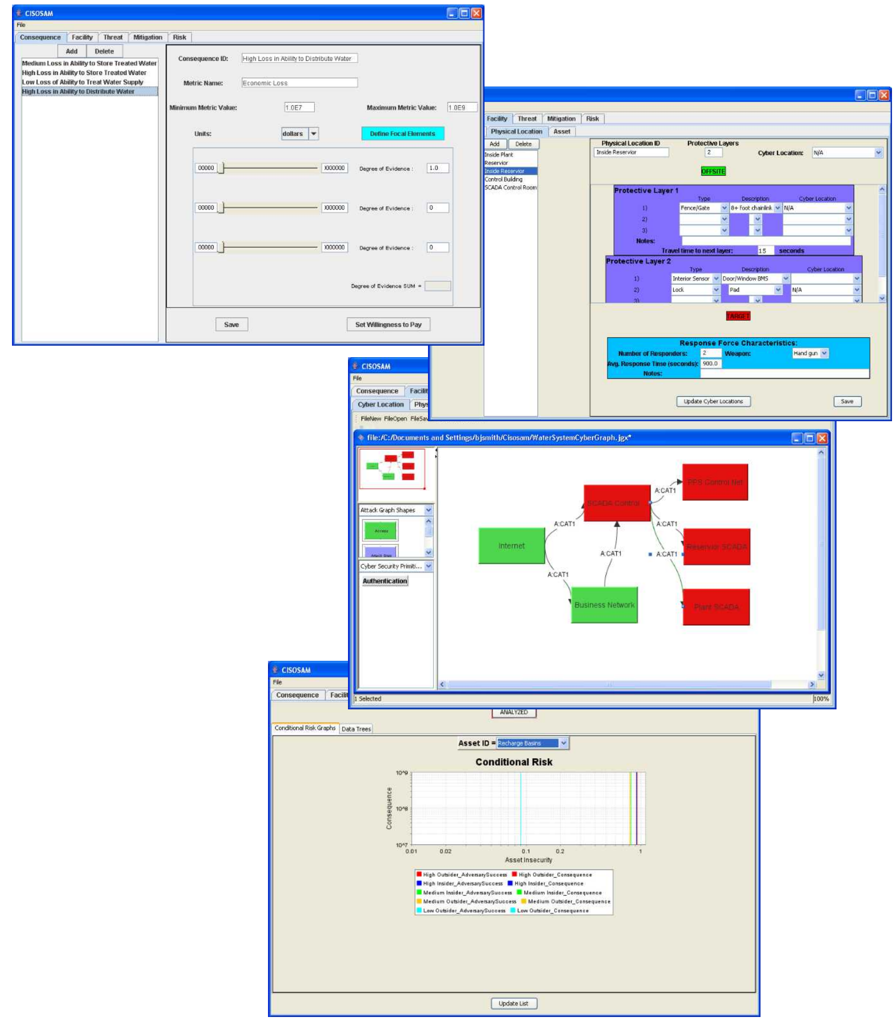
Cyber Threat Category	CPS Effectiveness Interval	Easiest Attack Path
I	[0]	(1,3,4)
II	[0.12, 0.68]	(1,2,4)
III	[0.7, 0.98]	(1,2,4)
IV	[0.9, 1.0]	(1,3,2,4)
V	[0.97, 1.0]	(1,3,2,4)
VI	[1]	No Possible Path

- Example Network
  - 1 = Internet
  - 2 = Business Network
  - 3 = Business Partner's Network
  - 4= PCS Control Network
- Results
  - Threat Category V never wins
  - Threat Category I always wins
  - Some uncertainty for the other threat categories
  - Easiest path makes qualitative sense

Sandia National Laboratories

Key Features of Cy/Phy Security Assessment Methodology

- Generate risk index based on:
  - Consequences of Concern (CoC)
  - Asset failures that lead to a CoC
  - Adversary capabilities
  - Physical and cyber protective measures for each asset
- Evaluates physical protection systems (PPS) and cyber protection systems (CPS) as part of an integrated analysis
  - Explicit linkage of PPS and CPS models
- Initial focus on Critical Infrastructure, but concepts are also applicable to high-security facilities
  - See MILCOM 2005 Paper and SAND Report for more details



Sandia National Laboratories

Future/Ongoing Work

- Enhanced user interfaces that better elicit data needed to apply the model
- Enhanced visualization of risk values for different CoCs, asset classes and threat levels.
- Cut sets that include multiple assets / targets
- Integration with Engineering Process Models (EPMs) for various infrastructures
  - Power distribution and generation
  - EPANET for water distribution
- Better assessment of mitigation effectiveness
- Improved techniques for evaluating CPS effectiveness
  - Attack paths that include both physical and cyber steps
  - Applications to large graphs
- Integration with network and process control simulation tools
  - Joint evaluation of system performance and blended security posture

Sandia National Laboratories