NUCLEAR SECURITY RISK ANALYSIS OF AN HIGHER EDUCATION INSTITUTION RESEARCH REACTOR

Jason Harris, Ph.D., Shraddha Rane, M.S., Emily Bragers, M.S., and Destiny White

jtharris@purdue.edu

International Conference on Nuclear Security: Sustaining and Strengthening Efforts
10-14 February 2020, IAEA, Vienna, Austria

Presentation Outline

PURDUE UNIVERSITY
CENTER FOR RADIOLOGICAL AND NUCLEAR SECURITY

- Introduction
- Methodology
  - Decomposing Risk
  - Risk Index
  - Threat Groups
  - Pathway Analysis
- Results
- Conclusion

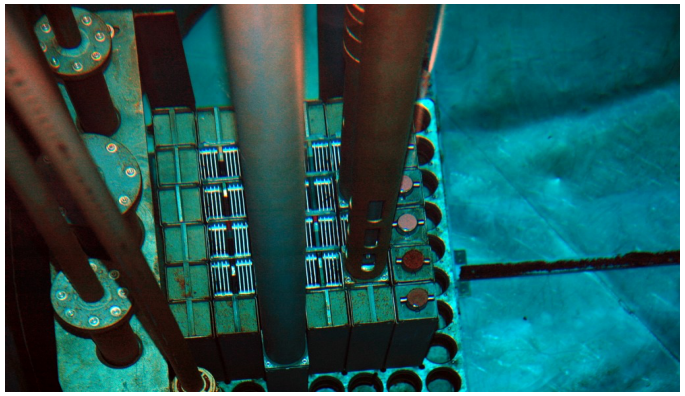
Introduction

PURDUE UNIVERSITY
CENTER FOR RADIOLOGICAL AND NUCLEAR SECURITY

- There are about 250 operating research reactors in the world, located in 55 countries.
- Many research reactors are situated at educational institutions (universities) with large student populations.
- Their lower uranium mass, enrichment, and power levels allow them to have less strict security measures.
- Given these attributes, research reactors may be targets to unauthorized access in the absence of rigorous controls.
- This study implements the principles of probabilistic methods and pathway analysis to quantify the risk of credible threats to a research reactor (PUR-1).

Introduction – PUR-1

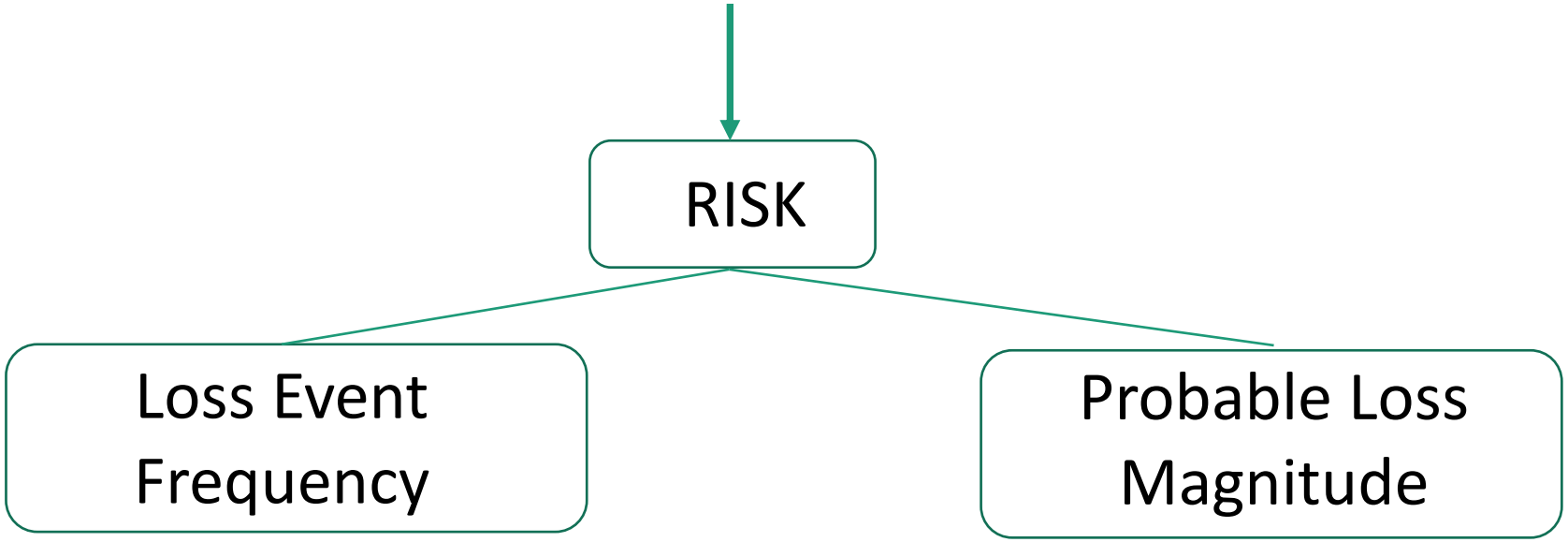
- Purdue University's research reactor, PUR-1, holds the titles of the state of Indiana's first and only reactor, and the first all-digital reactor in the United States.
- Its fuel is 19.75% enriched uranium, it is designed to produce up to 10 kW of power, and the maximum thermal flux is 2.1×10^{10} n cm^{-2} s.
- The reactor welcomes over 2000 visitors annually, with the tour groups ranging from 10-20 people and tours running one day a week.
- Aside from tours, the reactor is used for custom irradiation projects, hands-on classroom learning, and to train students to receive reactor operator licenses.
- There is a range from 100-200 door openings per day when classes are held in the reactor room, and class sizes average 25 people.



Decomposing Risk

R = P *C

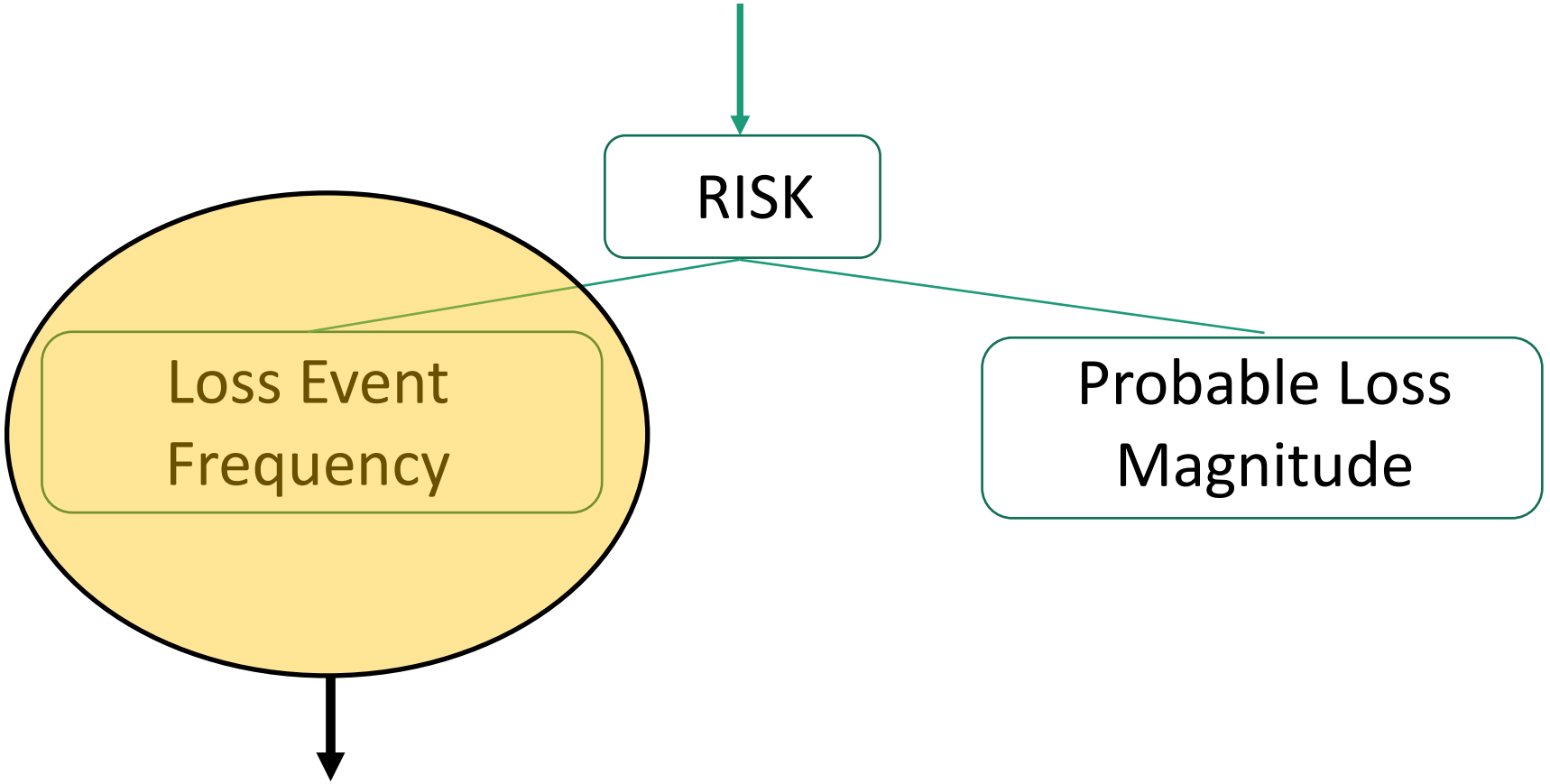
where R= Risk, P=Probability, C= Consequences



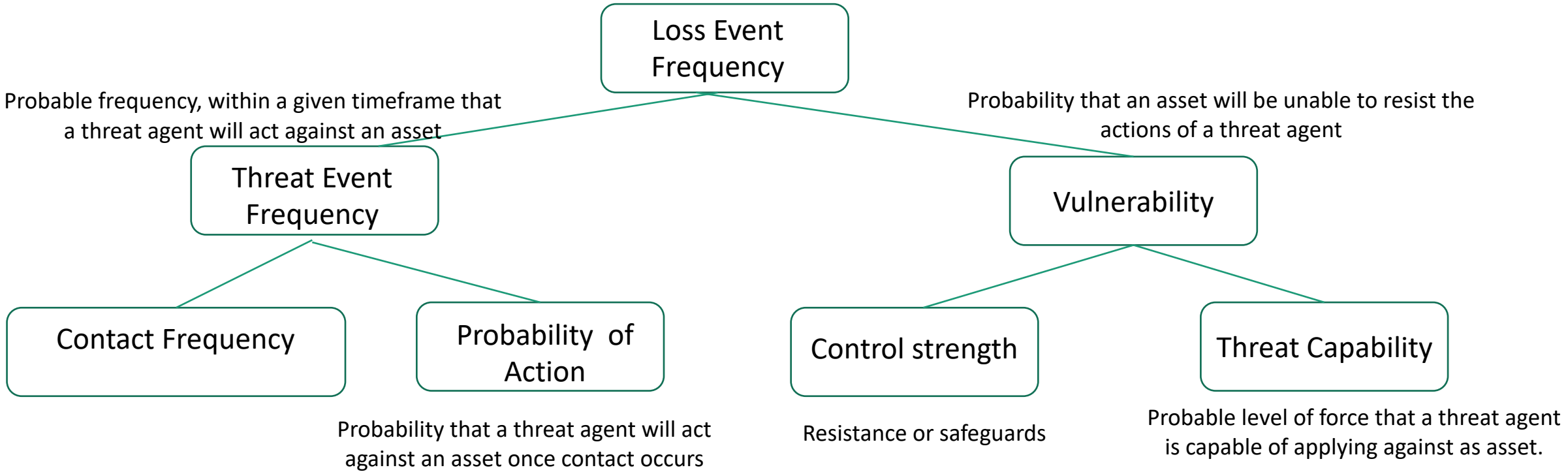
Decomposing Risk

R = P *C

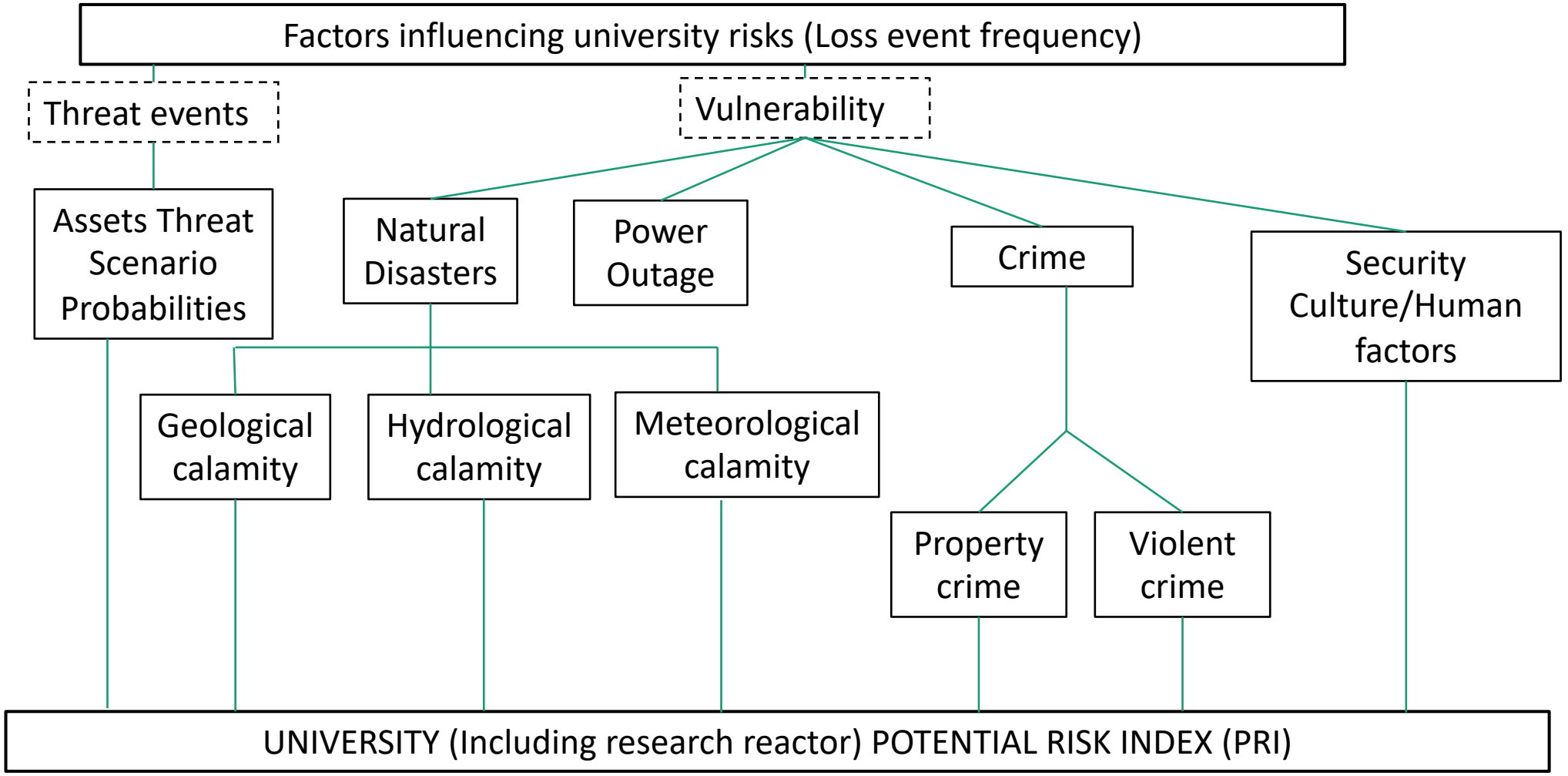
where R= Risk, P=Probability, C= Consequences



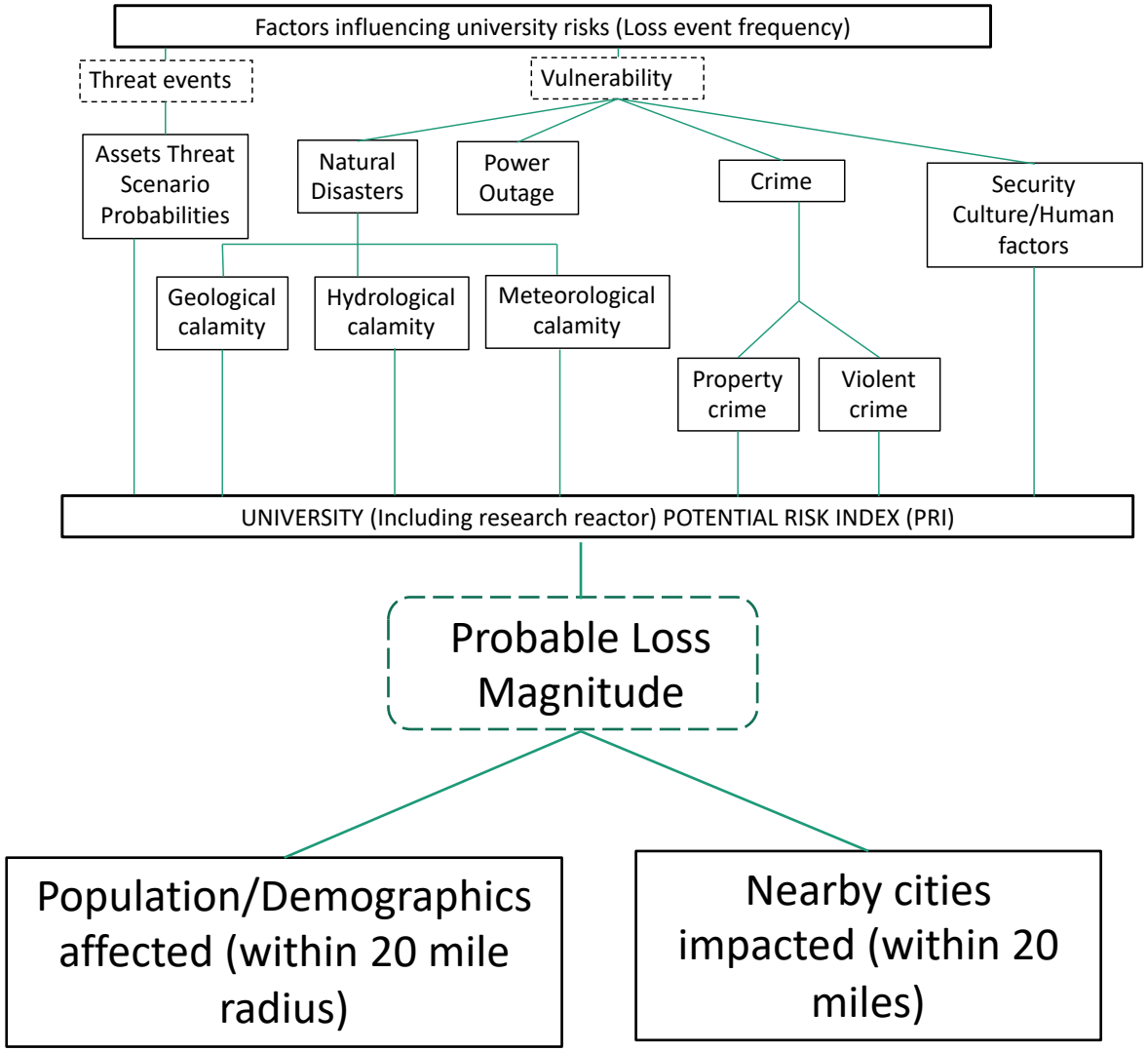
Risk Taxonomy



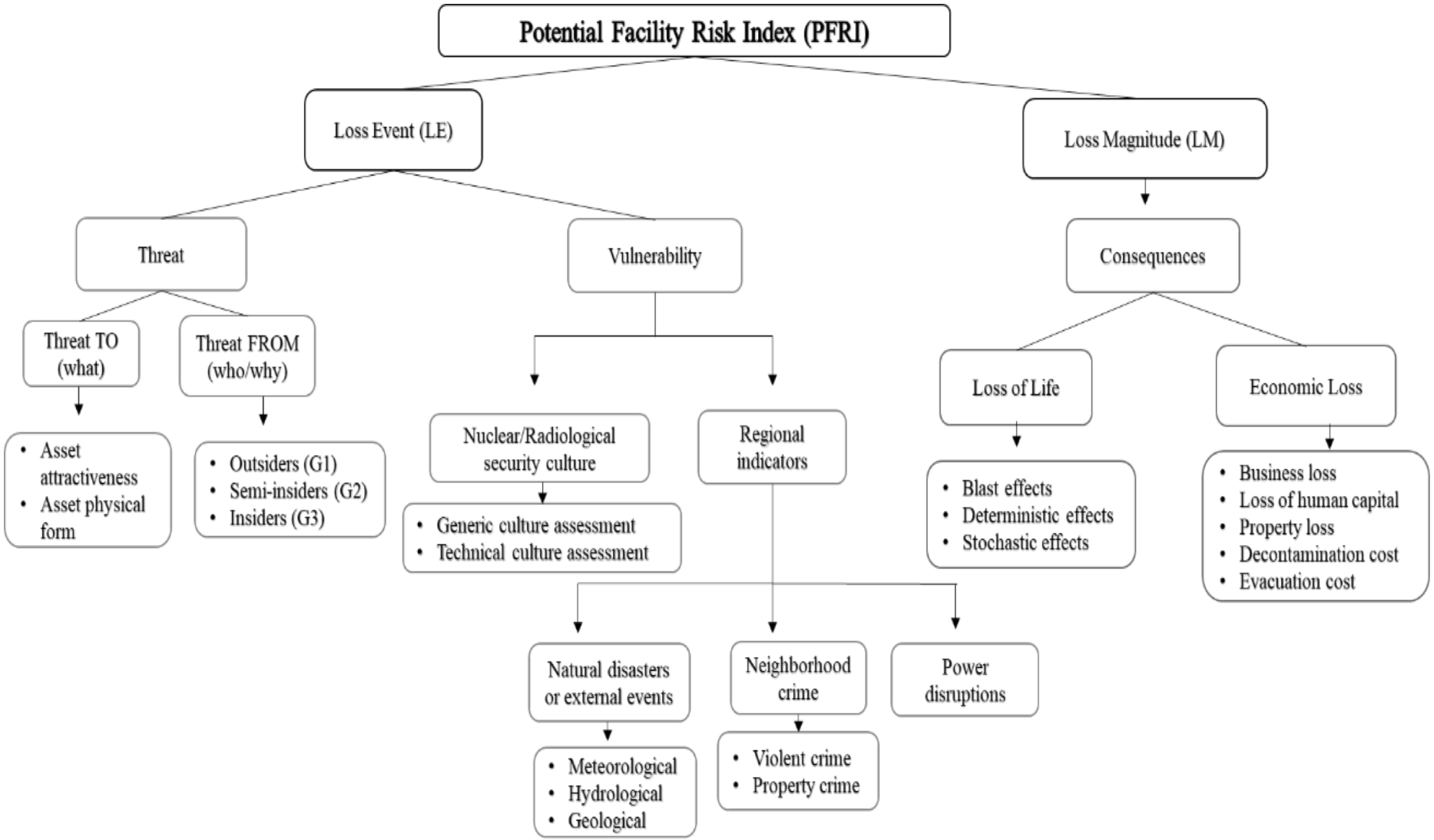
Conceptual Framework for Risk Index



Conceptual Framework for Risk Index



Potential Facility Risk Index (PFRI)



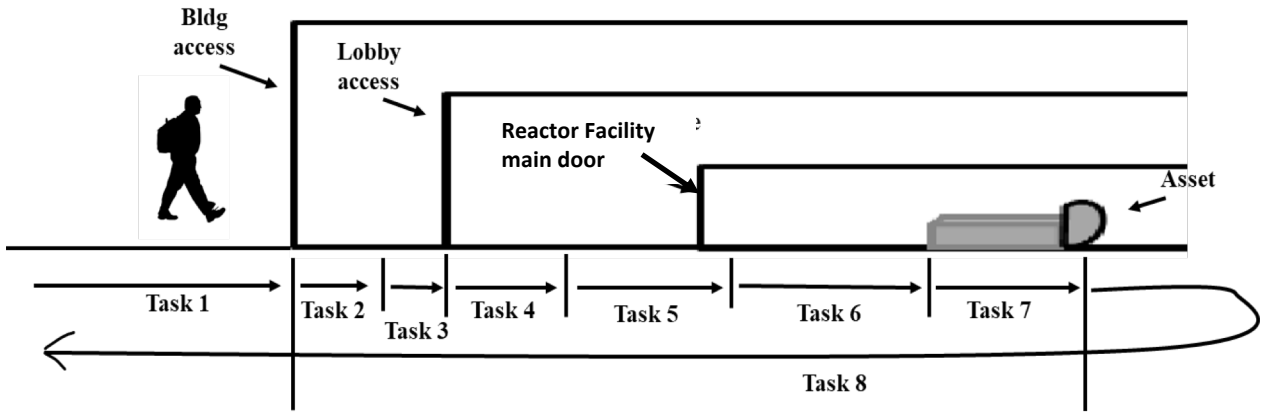
Threat Groups

PURDUE UNIVERSITY
CENTER FOR RADIOLOGICAL AND NUCLEAR SECURITY

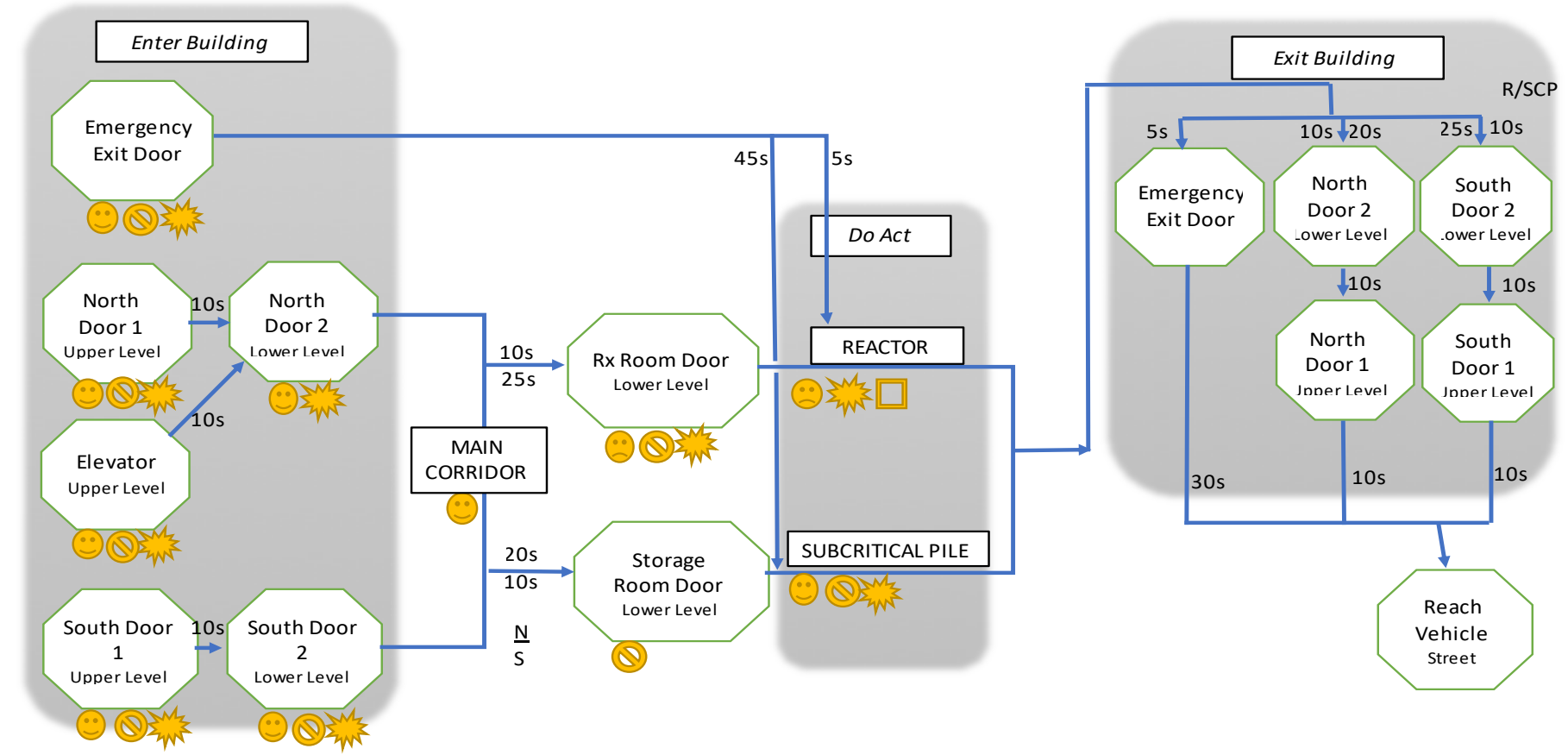
Threat Groups	Description	Resources/Capabilities
Group 1 (G1)	Access through each security feature and be supervised (i.e. tour visitors).	Low-Moderate
Group 2 (G2) S U	G2S: Access with supervision (i.e. students with access cards for class, cleaning staff) G2U: Un-escorted access (i.e. university radiation safety staff, students training as reactor operators)	High-Very high
Group 3 (G3)	Insiders: Access to all assets in the reactor facility (i.e. reactor supervisor, reactor technicians)	Moderate-High

Pathway Analysis

- To realistically represent adversary malicious intent, assumptions made on parameters, like physical protection system, initiating events, and adversary capabilities were obtained from PUR-1 (sensitive information not included).
- Adversary pathway analysis (Garcia) was used.
- Adversary pathway interruption analysis tool was used to quantitatively illustrate the effect of changing physical protection parameters along a specific path.
- Scenario of theft of reactor fuel (all possible pathways) used.



Results –Sequence



Results –Interruption

- G1 threat group used
- Researchers ”acted” out all scenarios to get accurate values
- P(I) = 0.16
- Incorporating realistic shorter response time
  - Overall success probability of adversary theft = 0.30.

Estimate of Adversary Sequence Interruption

Probability of Guard Communication		Response Force Time(sec)	
		Mean	Standard Deviation
0.95		300	90

Task	Description	P(Detection)	Location	Delay (seconds) Mean	Standard Deviation
1	N Door 1 (Crowbar)	0.9	B	12	2.4
2	Stairwell, Walk down stairs	0	B	10	3
3	N door 2 (Crowbar)	0.9	B	12	2.4
4	Walk main corridor to Reactor Room	0	B	10	3
5	Break open Door to Reactor Room (Crov	0.9	B	12	2.4
6	Steal Fuel Assemblies (Walk, Free dive)	0	B	3	0.9
7	Pull up fuel and place in bag (8 assembli	0	B	127	7.99
8	Exit through Emergency Door to Vehicle	0.9	B	10	3
9	Drive off Campus	0	B	20	6
10					
11					
12					

Probability of Interruption:	0.162775856

Conclusions

- Pathway model and probabilistic methods were combined to define the actions of different threat groups with in the form of attack scenarios.
- Method applied to PUR-1 (theft of reactor fuel).
- The computed probabilities of theft outlined in the study, along with vulnerabilities and magnitude of loss, will serve as an input towards the assessment of an overall security risk index for the reactor facility.
- Risk metric obtained from the calculations of the proposed tool is anticipated to yield a meaningful result of threat based on computed scenario probabilities, vulnerabilities, human factors, and net consequence loss.

Acknowledgements

The authors would like to thank Purdue University and the staff of PUR-1 for allowing us to access the reactor to obtain data needed to conduct this study.

PURDUE UNIVERSITY

150 YEARS OF GIANT LEAPS

CENTER FOR RADIOLOGICAL AND NUCLEAR SECURITY

Thank You!

Questions?