SAND2023-04308C

Sandia National Laboratories

Exceptional service in the national interest

MANAGING RISKS FOR RADIOACTIVE MATERIALS IN TRANSPORT: Understanding Likelihoods and Consequences

Mark Ekman, PhD, PMP

>>PATRAM22

The International Symposium on the Packaging and Transportation of Radioactive Materials

Juan-les-pins, Antibes, French Riviera

11 - 15 June 2023

EVERYONE UNDERSTANDS THE CONCEPT OF RISK

People make decisions regarding risk every day

People identify risks, evaluate them, and make decisions with risks in mind (consciously or otherwise)

Assess what can go wrong in an activity and our ability to mitigate or control it and comparing to the benefit of the activity

Everyone has their own threshold of risk acceptance that drives the risks they are willing to take

The amount of risk that a person is willing to accept varies over time and with other circumstances

2

RISK MITIGATION DOES NOT EQUAL RISK ELIMINATION

Similarly, States make decisions on risk based on the severity of the associated consequences and the likelihood of the initiating events.

For example, States license and allow citizens to drive automobiles knowing that a certain number will be killed in accidents every year.

This risk is mitigated by enforcing speed limits and other regulations for driving, requiring seatbelts and other safety equipment, and requiring certain levels of competence and skill of drivers.

These risk mitigation steps are designed to reduce the likelihood and/or consequence severity of accidents related to driving, but they do not eliminate the risk.

CALCULATING RISK

Risk is the combination of two factors: the severity of an event (consequence) and the probability (likelihood) that the event will occur

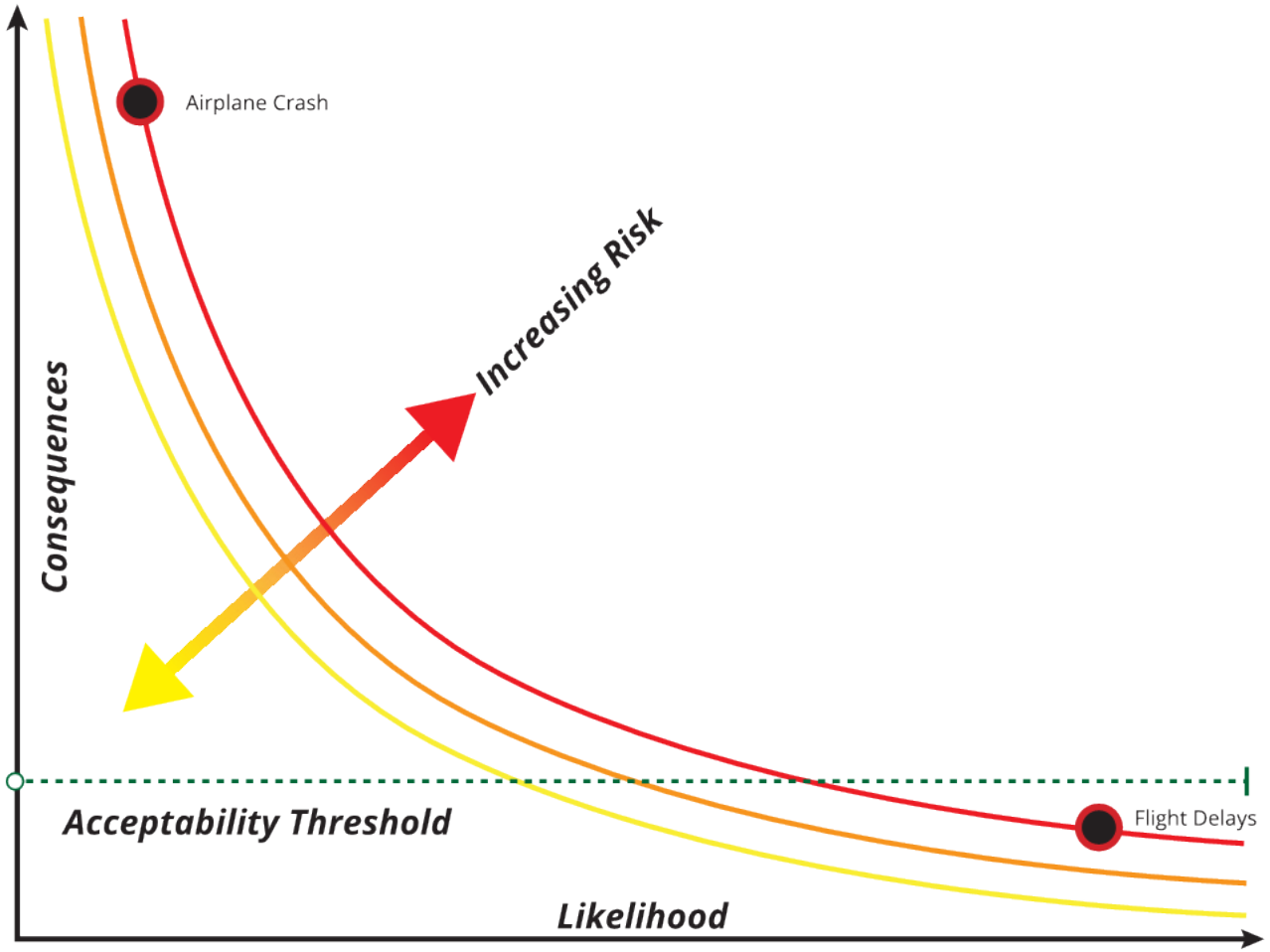
This is often expressed mathematically as

$$Risk = Consequence \times Likelihood$$

If we can determine quantitative values for *Consequence* and *Likelihood* for a variety of scenarios, we can determine the risk space for which controls should be implemented

For security applications, the definition can be slightly modified to clarify that security risk is the combination of the severity of an intentional, malicious action (consequence) and the probability (likelihood) that the action will occur

RISK CURVES



Each line represents constant risk, i.e., the products of Consequence and Likelihood are the same at any point on the line

Risk increases as go to upper right

Risk decreases as go to lower left

Risk is reduced by reducing the likelihood of an event occurring and/or reducing the consequence severity of an event

The space above a curve (upper right) represents unacceptable risk, and the space below (lower left) represents acceptable risk

SETTING ACCEPTABLE RISK LEVELS

Where the consequence severity is so low that expenditure of additional resources is not justified

Where the likelihood of occurrence is so low that the continuous expenditure to reduce risk further cannot be financially justified

Where the costs of reducing the risk any further do not justify the benefit of the risk reduction

Where the impact of reducing risk negatively impacts the operation severely enough that the benefits provided are diminished

DETERMINING NUMERICAL VALUES IS CHALLENGING

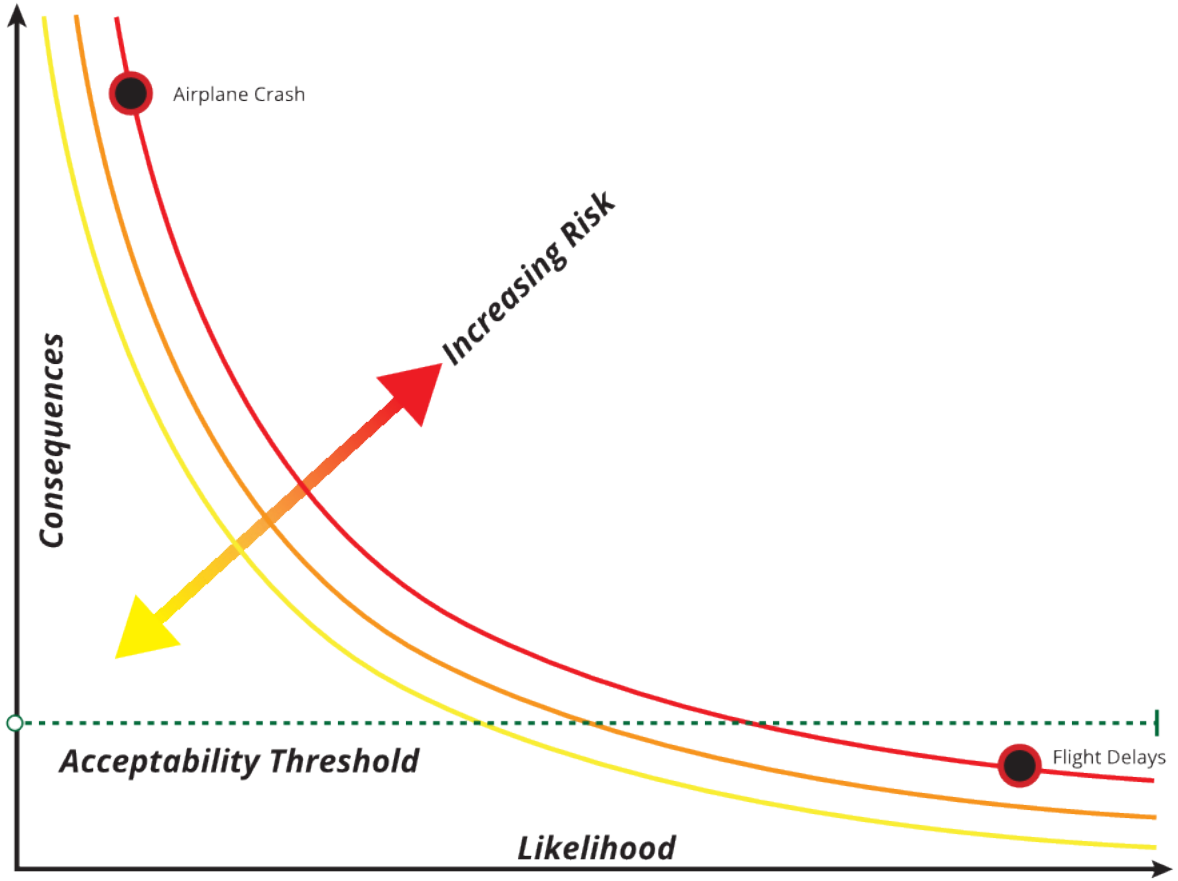
The complexity and uncertainty in determining quantitative values for consequences and likelihoods for events make it unreasonable or impossible to generate a risk graph.

Due to the difficulty in quantifying risk along with the need to clearly define an acceptable risk threshold, States usually estimate risk by ignoring likelihood and using consequence severity as a surrogate for risk.

This means that an acceptable risk threshold is estimated by an acceptable consequence severity

From prior slide, “Where the consequence severity is so low that expenditure of additional resources is not justified”

OFTEN EQUATE RISK WITH CONSEQUENCE SEVERITY



Risks that are higher likelihood, but lower consequence are ignored or at least under categorized.

Low risk events are protected at higher levels than necessary.

These thresholds frequently focus on health effects and tend to underestimate financial and other risks.

DETERMINING QUALITATIVE RISK

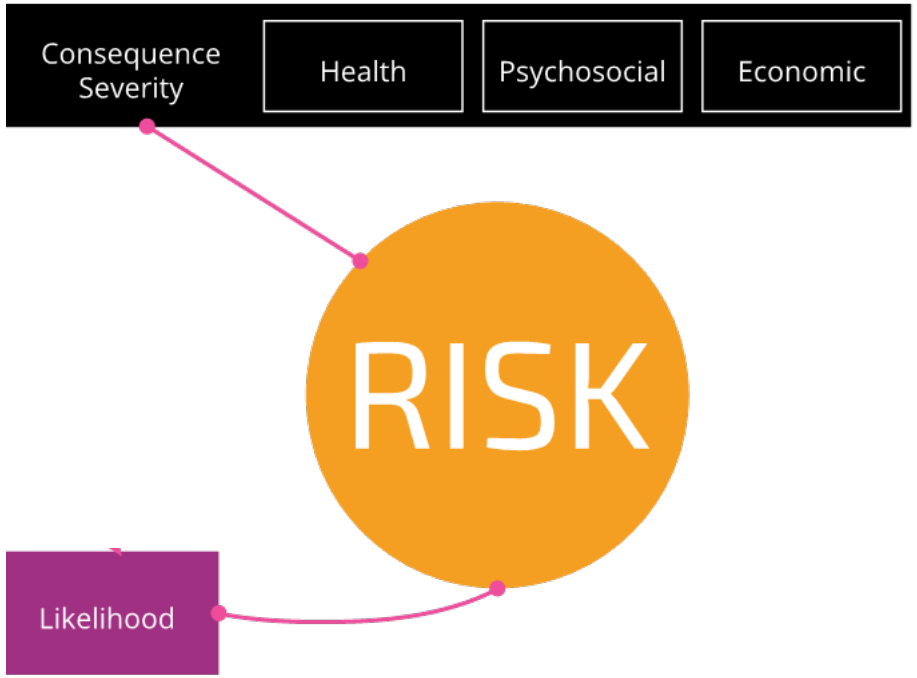
Risk is composed of consequence severity and likelihood.

If either goes up, risk goes up.

If either goes down, risk goes down.

For radioactive materials, consequence severity is frequently grouped into

- Health effects – deterministic and stochastic health effects and fatalities
- Psychosocial effects – public fear and panic, loss of confidence in government, lifestyle changes, etc.
- Economic effects – costs of clean up, evacuation and displacement of people, monitoring and medical care, lost revenue due to closed facilities, etc.

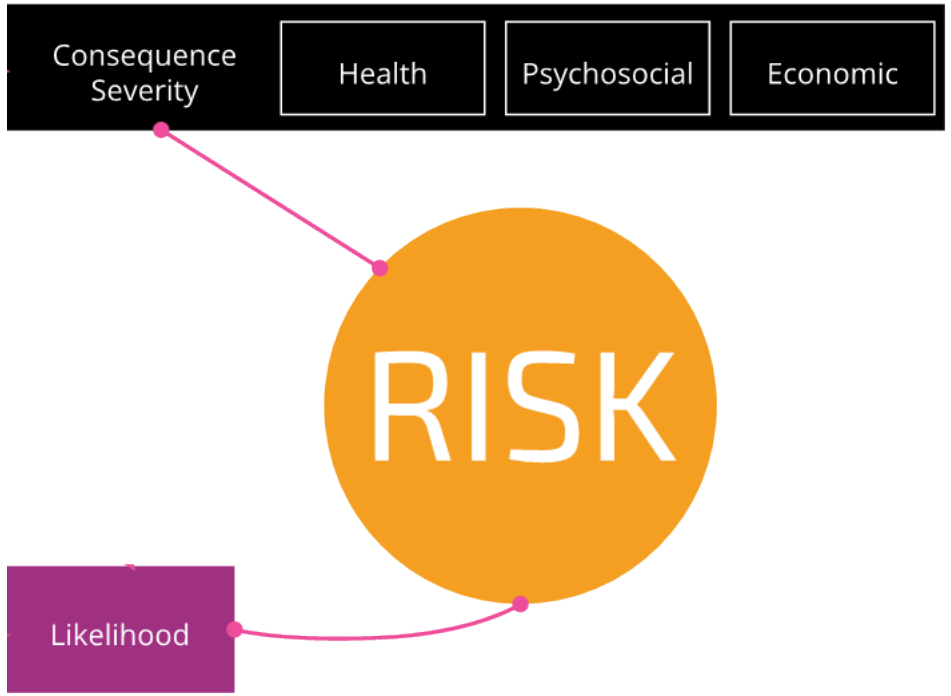


START WITH WHAT WE KNOW

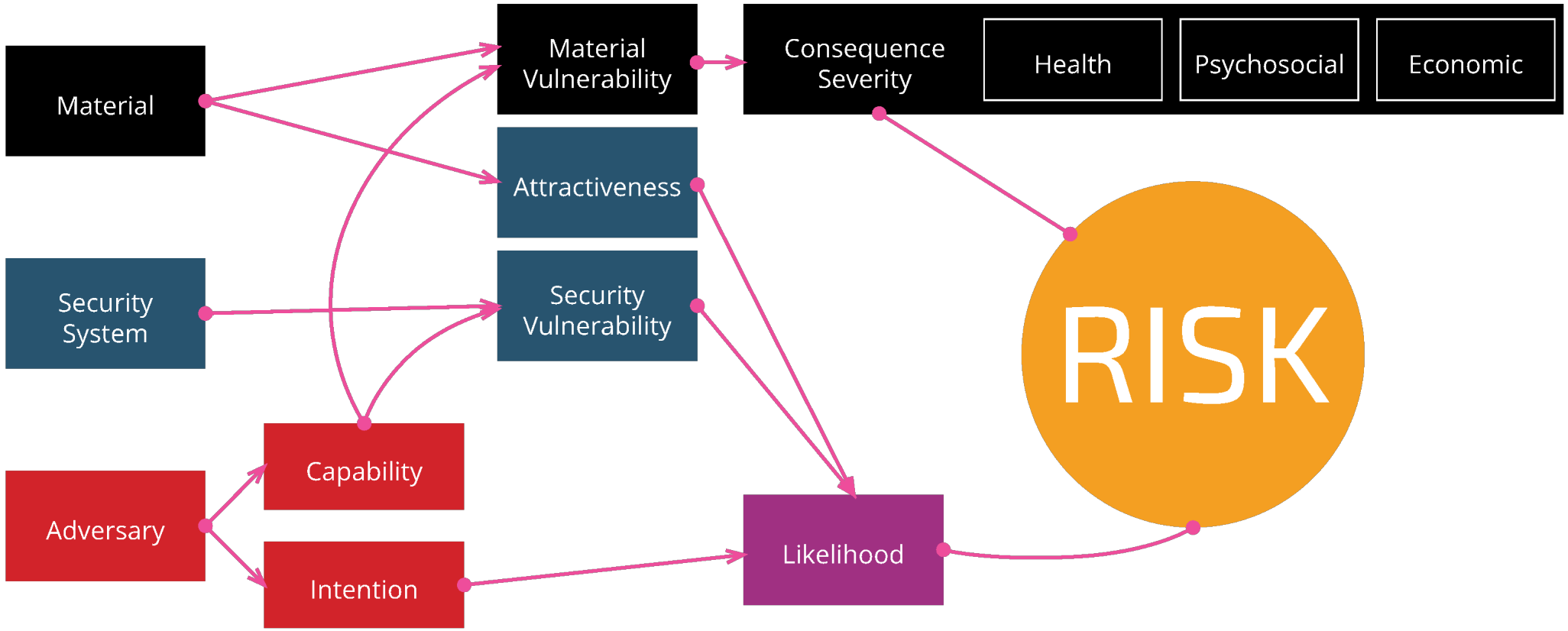
Material

Security System

Adversary



FACTOR WHAT WE KNOW INTO WHAT WE CAN MEASURE



RISK-INFLUENCING FACTORS

Material Vulnerability
- Physical properties – isotope, activity, physical form

Material Attractiveness
- Accessibility, availability, ease of handling

Security Vulnerability
- How well security fundamentals are implemented (detection, delay, response)

Adversary Capability
- Ability to execute a malicious act involving radioactive material

Adversary Intention
- Motivation consistent with committing a malicious act with radioactive material

PUTTING IT ALL TOGETHER

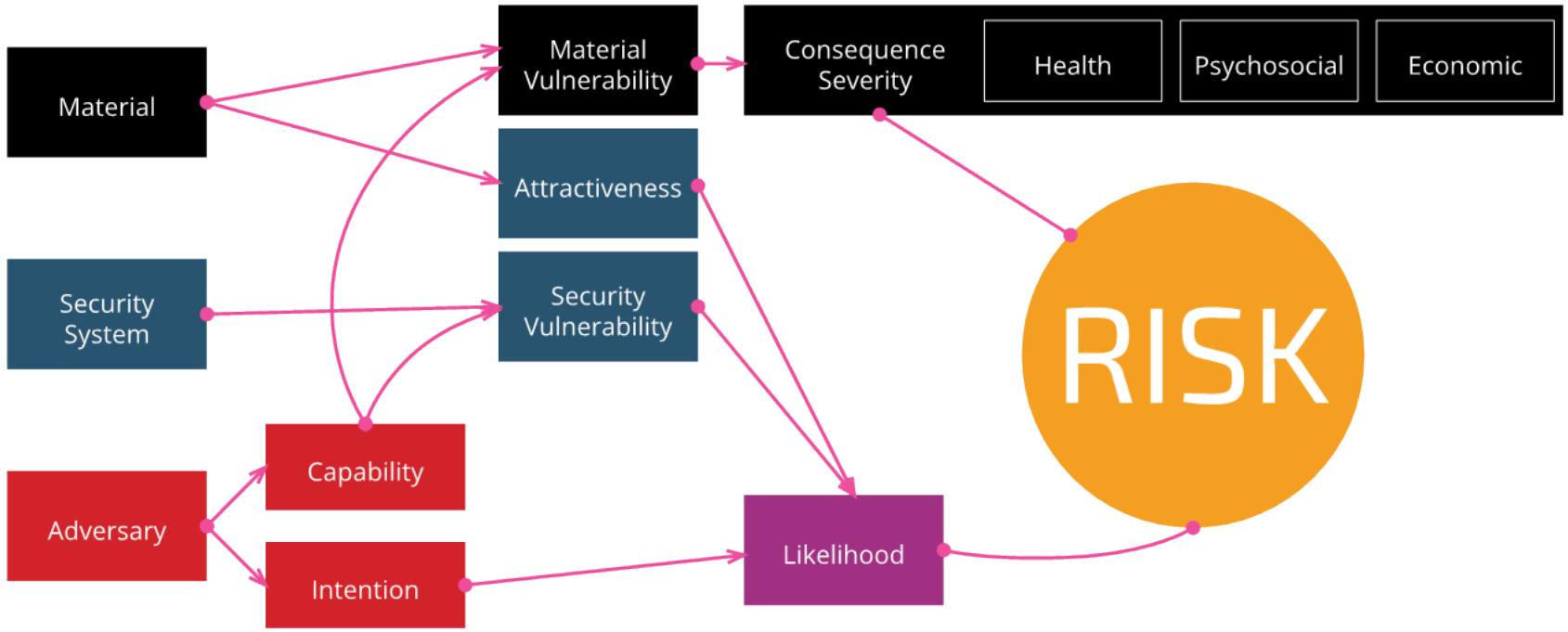
Material Vulnerability influences the consequence severity

Attractiveness influences how likely a radioactive source will be selected

Security Vulnerability influences likelihood of theft

Adversary Capability influences how vulnerable a security system is and consequence severity.

Adversary Intention influences likelihood of a malicious act involving a particular source



RISK ASSESSMENT RATING TABLES – "WORD LADDERS"

Can create tables to define clear, distinguishable, and assessable criteria for the different ratings

Similar tables can be developed for each risk-influencing factor

Subject matter experts are best positioned to analyze specific scenarios to assign ratings

Adversary Assessment Rating	Capability	Intention
Very High	Adversaries have an established capability to attack the target	Adversaries have current intention to attack the target
High	Adversaries have the capability to attack the target	Attack of the target is consistent with the intentions of the adversary
Medium	Adversaries have some capability to attack the target	Attack is not consistent with adversary intention, depending on current circumstances
Low	Adversaries have little capability	Adversaries have little intention to attack the target
Very Low	Adversaries currently have no capability	Adversaries currently have no intention to attack target

COMBINING QUALITATIVE RATINGS

Ratings for factors contributing to consequence severity and factors contributing to likelihood can be combined.

Rules for combining must be established

Completion of this analysis will give a final rating for likelihood in this example. A similar table can be developed for consequence severity

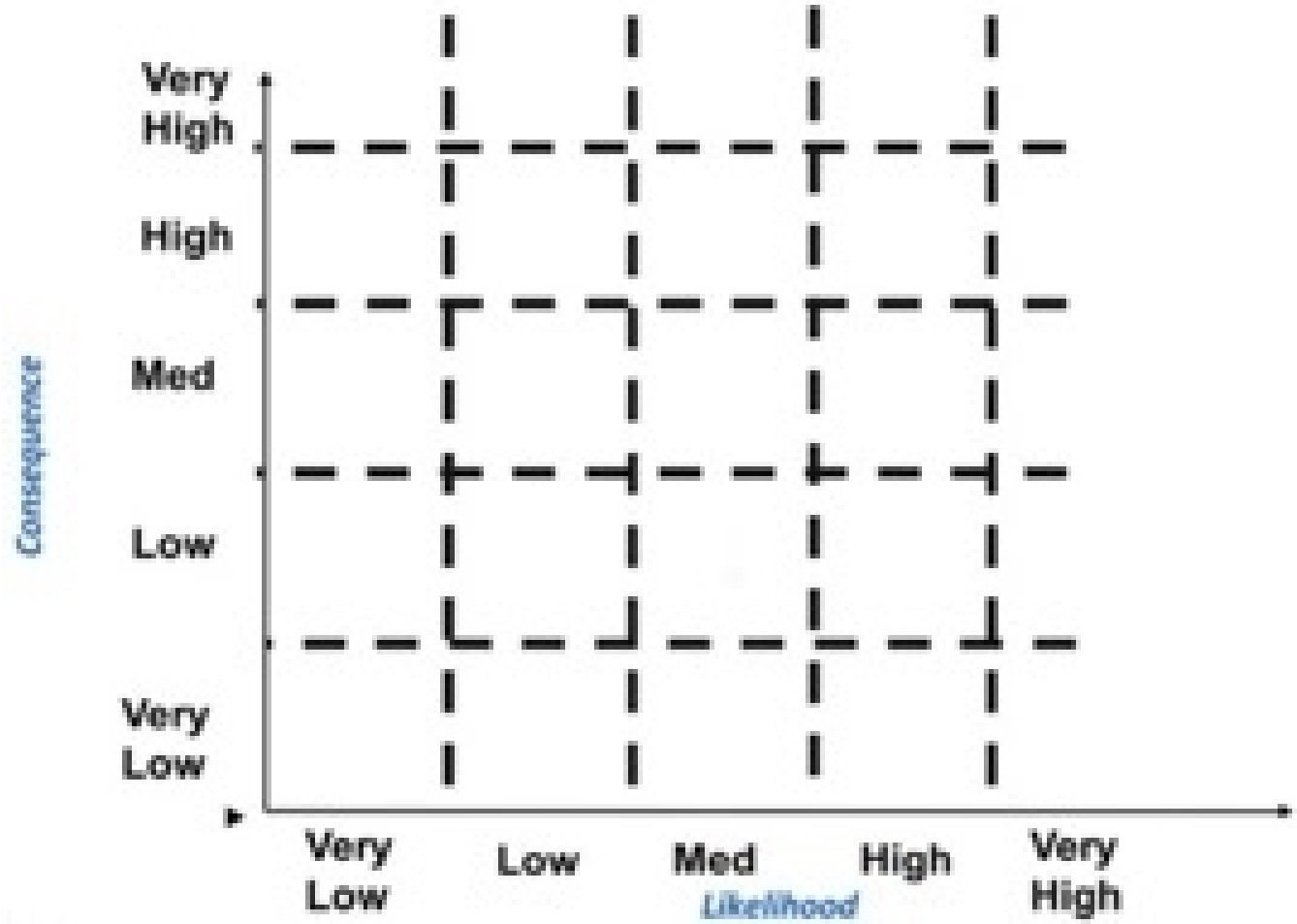
Likelihood Rating	Attractiveness Qualitative Rating	Security Vulnerability Qualitative Rating	Adversary Intention Qualitative Rating
Very High	2 Very High Ratings and either 1 Very High or High		
High	2 High Ratings and either 1 Very High, High, or Medium 2 Very High and either 1 Low or Very Low		
Medium	2 Medium Ratings and either 1 High, Medium, or Low 1 Medium Rating, 1 Low Rating, and either 1 High or Very High		
Low	2 or more Low Ratings 1 Low Rating, 1 Very Low, and either 1 Very High, High, or Medium 1 Very Low Rating, 1 Medium, and either 1 High or Very High		
Very Low	2 or more Very Low Ratings 1 Very Low Rating and 2 Low		

OVERALL RISK SPACE CAN BE DETERMINED

Overall risk is determined by the final consequence severity and event likelihood

Overall view of the risk space due to the use, storage, and transport of radioactive sources can be plotted

The qualitative nature of these assessments is imprecise, and the imprecision, assumptions, and associated uncertainty should be documented in the interpretation of the results



SUMMARY

To conduct an effective risk assessment of radioactive materials in use, storage, and transport

- Likelihood and consequences must be analyzed using qualitative and quantitative risk-based methods
- In practice, the complexity and uncertainty in determining quantitative values for consequences and likelihoods for events make it unreasonable or impossible to generate quantitative risk values and measurements.

Reasonable estimates of security risks associated with the use, storage, and transport of radioactive materials can be made by decomposing consequence severity and threat likelihoods into more understandable and analyzable components and using qualitative approaches to determine overall risk.

- Likelihood factors include material attractiveness, security system vulnerability, adversary capability, and adversary intention.
- Consequence factors include material vulnerability and adversary capability, resulting in health effects, psychosocial effects, and economic effects.
- While there is uncertainty in estimating these factors, the process can inform relative risks necessary to guide radioactive material security policy and guidance.

These qualitative assessments can be useful in providing insights into risks associated with the use, storage and transportation of radioactive materials and can serve as a basis of risk management decisions as long as it is recognized and documented that the qualitative nature of these assessments is imprecise and based on key assumptions.

CONTACT INFORMATION

Mark Ekman, PhD, PMP
Sandia National Laboratories
meekman@sandia.gov
+1-505-844-1771