SAND2013-5299C

Exceptional service in the national interest

Sandia National Laboratories

Risk-Informed Management of Enterprise Security: Methodology and Application for Nuclear Facilities

Felicia A. Durán, Ph.D.

Research Team: Gregory D. Wyss, Sabina E. Jordan, and Benjamin B. Cipiti

U.S. DEPARTMENT OF ENERGY | NNSA 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. SAND NO. 2013-XXXXP

Assessing Security Risk

- Determine Protection Objectives
  - Define target & (design basis) threat; characterize facility
- Design Protection System
  - Detection – Delay – Response – Consequence Mitigation
- Analyze Protection System
  - Vulnerabilities – Attack Paths – Probability of Effectiveness PE
  - Detailed analysis using tools like EASI, ASSESS, and others
- Issues:
  - Comparing security risk between facilities is difficult
    - Different assumptions about threat, scenario credibility
    - Threats can change rapidly
    - Attack likelihood (PA) is very uncertain – often neglected to compute risk that is conditional on the attack occurring
  - Doesn't specifically find the security system's breaking point

Source: Garcia, The Design & Evaluation of Physical Protection Systems, Elsevier, 2001.

Security Risk Management Recommendations from the National Academy of Sciences

Sandia National Laboratories

- Our goal must be ***effective security risk*** management.

  National Academy of Sciences, 2010, emphasis added

Risk management is the process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring, or controlling it to an acceptable level at an acceptable cost.

- Key risk management recommendations include:
  - Focus on risk management rather than "how much or little risk exists"
  - Qualitative risk assessment methods may be suitable
  - Use a risk-informed, not risk based, approach to security risk management
    - Informed by PRA tools, but not relying on PRA

What is Risk?

Sandia National Laboratories

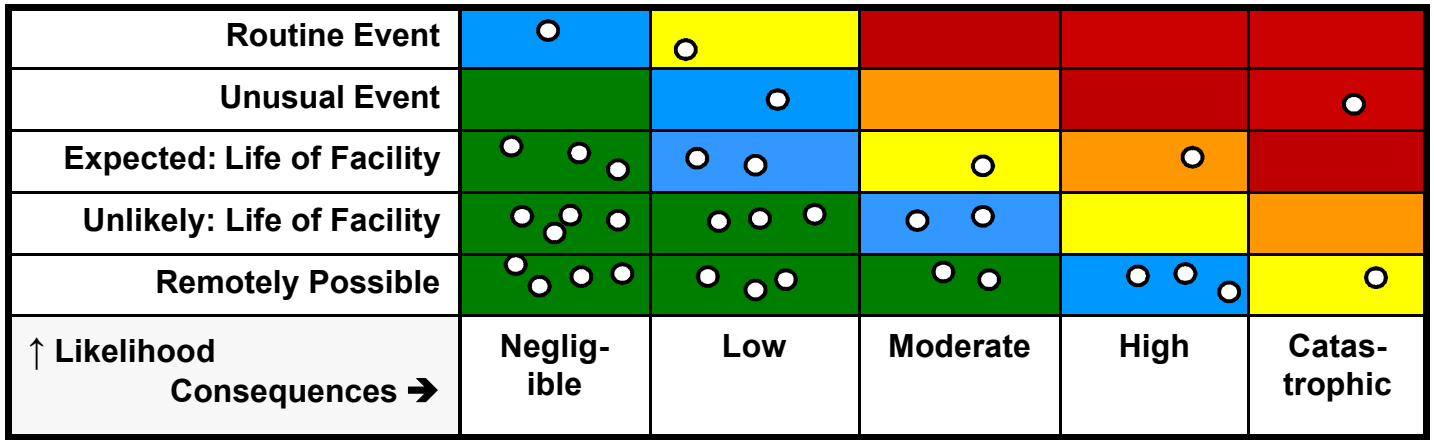
Scenario	Consequence	Likelihood
S_1	C_1	F_1
S_2	C_2	F_2
S_3	C_3	F_3
S_4	C_4	F_4
S_5	C_5	F_5
S_6	C_6	F_6
…	…	…

This *table* *IS* the risk!

- Risk is the *potential* to incur adverse consequences.
- Risk can be thought of as answers to 3 questions:
  - *What can happen?* *(scenario)*
  - *How likely is it?* *(probability / frequency)*
  - *How bad is it?* *(consequence)*

"If [a] table contains all the scenarios we can think of, we can then say that it (*the table*) is the answer to the question and therefore *is the risk*."

Kaplan & Garrick, Risk Analysis 1:1(11) 1981, emphasis added.



Goal: Manage Security Risks

Sandia National Laboratories

- Problem: attack likelihoods are highly uncertain and change rapidly.
  - Depends on attacker's capability, motivation & intent
  - Depends on attacker's other opportunities inside *and* outside the system.
  - Predicting likelihood makes risk hard to use for security decision making

- A different risk management approach: examine adversary criteria for selecting which attack scenario to pursue, including:

Adversary's Decision Criterion	How we make an attack less likely
"Could I do it if I wanted to?" ***(Is success likelihood high?)***	
"Would I do it if I could?" ***(Worthy investment of resources?)*** ***(Does it violate my doctrine?)***	
"Are the expected consequences high enough?"	

Attack scenarios:

Easy

&

High-Consequence

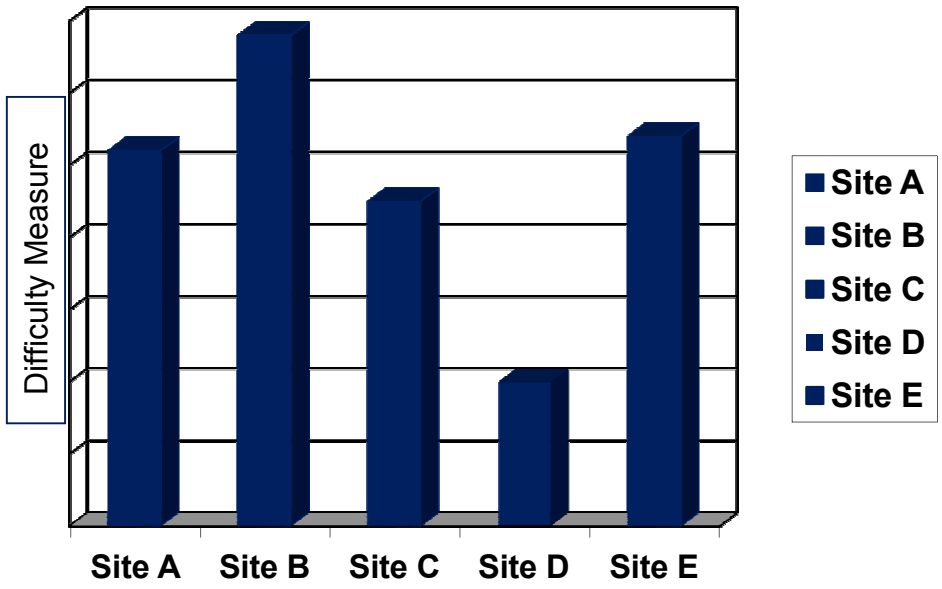
=

High Risk

Security Risk Management: Making Easy Attacks More Difficult

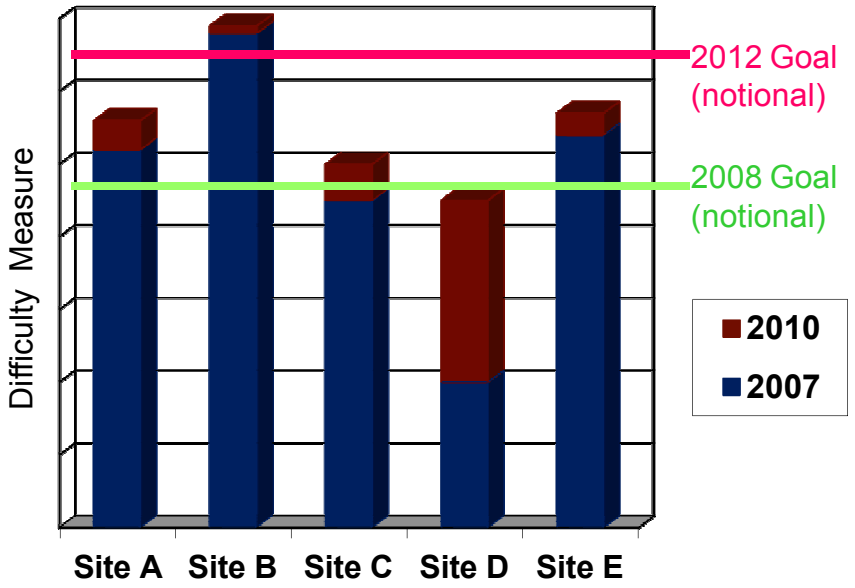
Sandia National Laboratories

Illustration based on sites assumed to have the same consequence for a successful attack.



- Are sites balanced?
- Where should I spend my next dollar?

- How much have I improved?
- Why do my sites not meet the new security goal?



Considerations for Estimating Attack Scenario Difficulty

Sandia National Laboratories

Attack Preparation

- Outsider attack participants
  - *Number of engaged participants*
  - *Training & expertise required*
- Insider attack participants
  - *Number and coordination*
  - *Level of physical and cyber access required, sensitivity, vs. security controls*
- Organizational support structure
  - *Size, capabilities & commitment*
  - *Training facilities, R&D, safe haven, intelligence & OPSEC capabilities…*
- Availability of required tools
  - *Rarity, signatures for intelligence or law enforcement, training signatures…*

Attack Execution

- Ingenuity & inventiveness
- Situational understanding
  - *Observability & transience of vulnerabilities*
- Stealth & covertness
- Dedication & commitment of participants
  - *Risk to both outsiders & insiders includes personal risk, willingness to die, etc.*
  - *Risk to the "cause" or support base*
- Operational complexity/flexibility
  - *Precision coordination of disparate tasks*
  - *Multi-modal attack (cyber+physical+???)*

Example characteristics used to establish levels of difficulty for each dimension

Eas
publ
spec

Scenario difficulty is a property of the *target.*

It estimates how capable the adversary must be to have a successful attack.

Risk managers can then ask, "Are the easiest attacks difficult enough to deter the adversaries we are concerned about?"

Difficulty of Example Scenarios

Sandia National Laboratories

		Easier	*Moderate*	*High*
Attack Planning & Preparation	Participants	2 (3)	2 (3)	3 (9)
	Training	2 (3)	3 (9)	3 (9)
	Support	1 (1)	1 (1)	4 (27)
	Tools	2 (3)	1 (1)	3 (9)
	# of Insiders	1 (1)	1 (1)	3 (9)
	Insider Access	1 (1)	1 (1)	3 (9)
	Ingenuity	1 (1)	2 (3)	3 (9)
Attack Execution	Situational Understanding	1 (1)	2 (3)	2 (3)
	Stealth & Covertness	1 (1)	3 (9)	4 (27)
	Outsider Commitment	2 (3)	2 (3)	3 (9)
	Insider Commitment	1 (1)	2 (3)	1 (1)
	Complexity	1 (1)	2 (3)	4 (27)
	Flexibility	1 (1)	2 (3)	3 (9)
Aggregated Score		-- *(21)*	-- *(43)*	-- *(157)*

Level ***(Score)*** *[1, 2, 3, 4, 5 → 1, 3, 9, 27, 81]*

Score for each level is 3x that of the next lower level in this example.

Easier:
Oklahoma City Bombing

Moderate Difficulty:
Cyber Theft of Personal Information

High Difficulty:
Sabotage at a High Security Temporary Facility

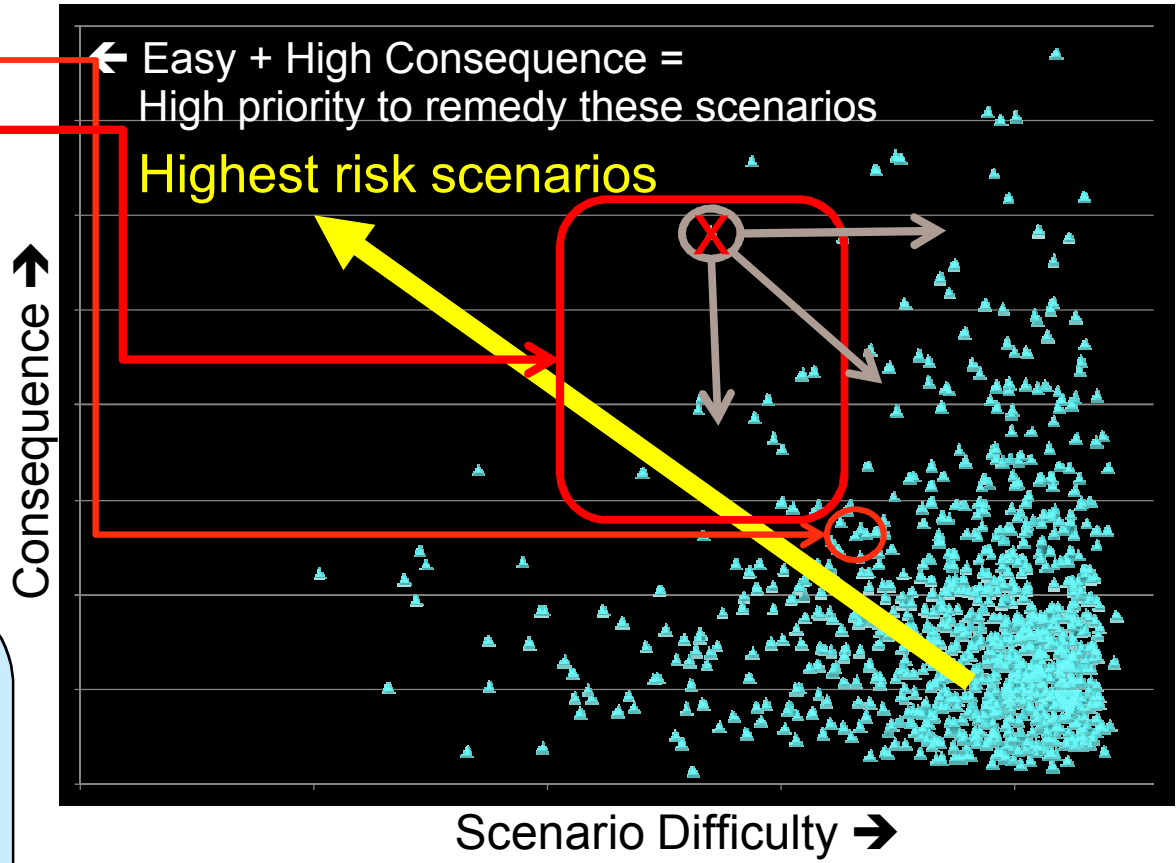
The Next Step: Manage Risk with Both Scenario Difficulty *and* Consequence

If we fix this…

Without fixing this…

We may not have improved security. *Because…*

Many scenarios still exist that are both easier to achieve AND provide higher consequences!



Why use scenario difficulty in security risk management?

- Difficulty better reflects the adversary planning process
- Difficulty changes more slowly and predictably than likelihood
- We have developed a qualitative (semi-quantitative) method to rank attack scenario difficulty

To "fix" a scenario we must

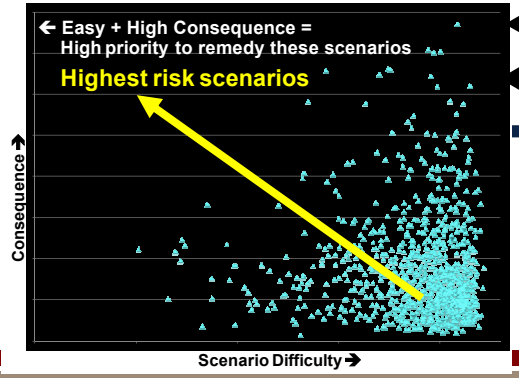
- Eliminate it (make it impossible to achieve)
- Reduce the consequences if it is completed
- Make it harder to accomplish successfully

… or any combination of these

Observations From Examples

Sandia National Laboratories

Scenario	Objective	Example Adversary Alternatives	Observations
Cyber Attack	Large $$ from Use of Info	• Few can generate a comparable return on investment	Attack *routinely* occurs
Large Truck Bomb	Destroy Building	• Burn down building	Alternative is easier for same consequences
	Mass Casualties	• Shootings in crowded areas • Suicide bomber vest • Car bomb in crowded area	Alternative is easier, but lower consequences

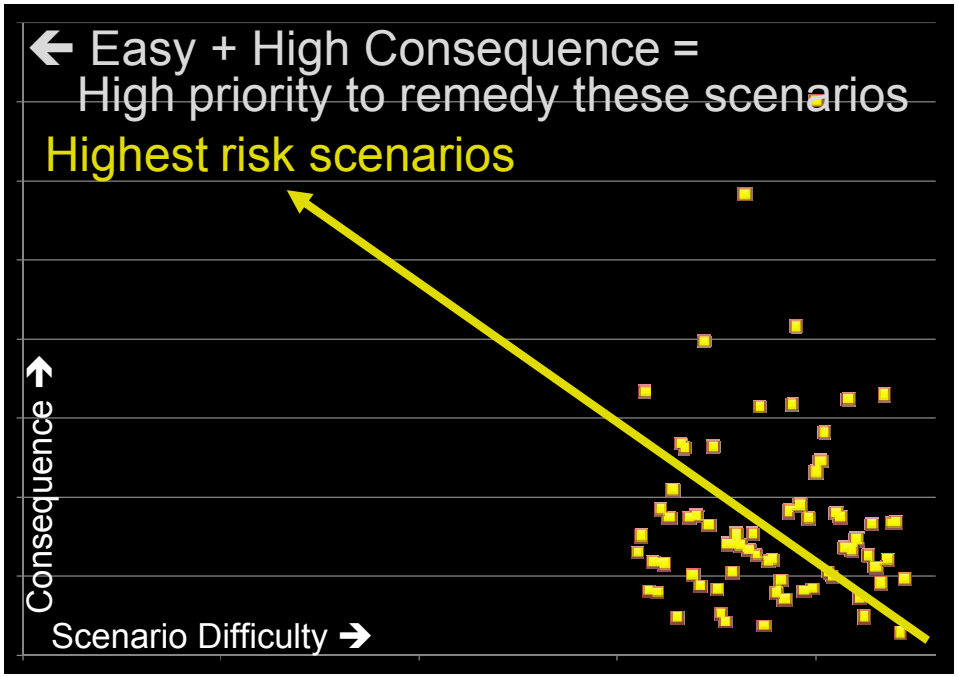


These factors are key inputs to the risk management method!

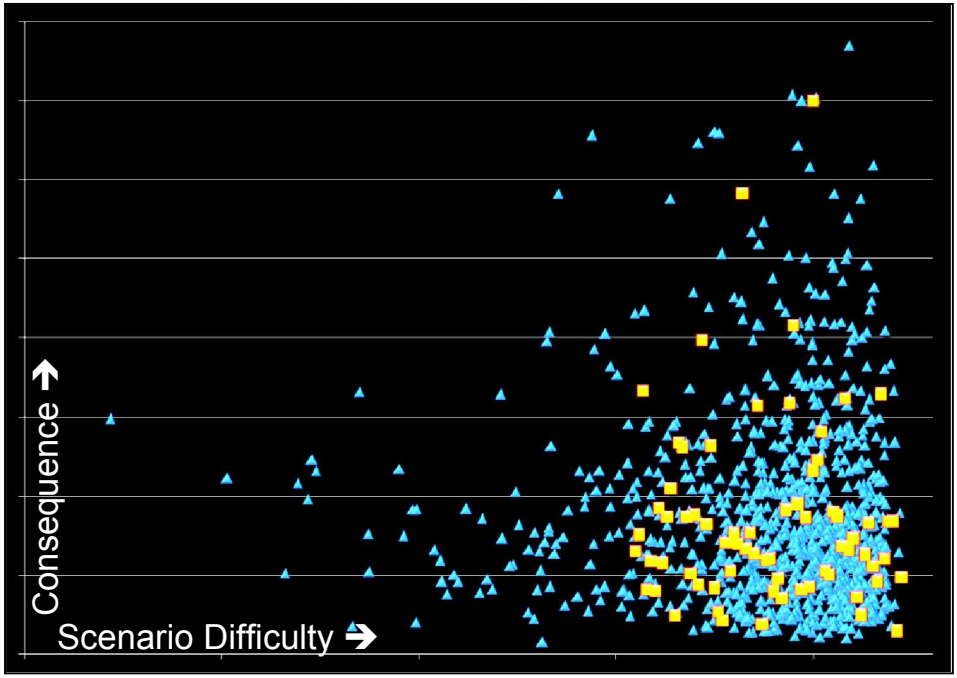
Notional Enterprise Security Management

Sandia National Laboratories

Facility Owner's View of Security Risk



Composite (Enterprise/Facility) View of



How do we decide which vulnerabilities should be addressed first?

- Generally, work on scenarios that are both easy to do & high consequence.
- Scenarios far from the "risk frontier" are less attractive to the adversary – addressed only after easier scenarios with higher conseq.
- Facility owner may have different opinion from enterprise owner
- Enterprise decisions may be affected by intelligence data

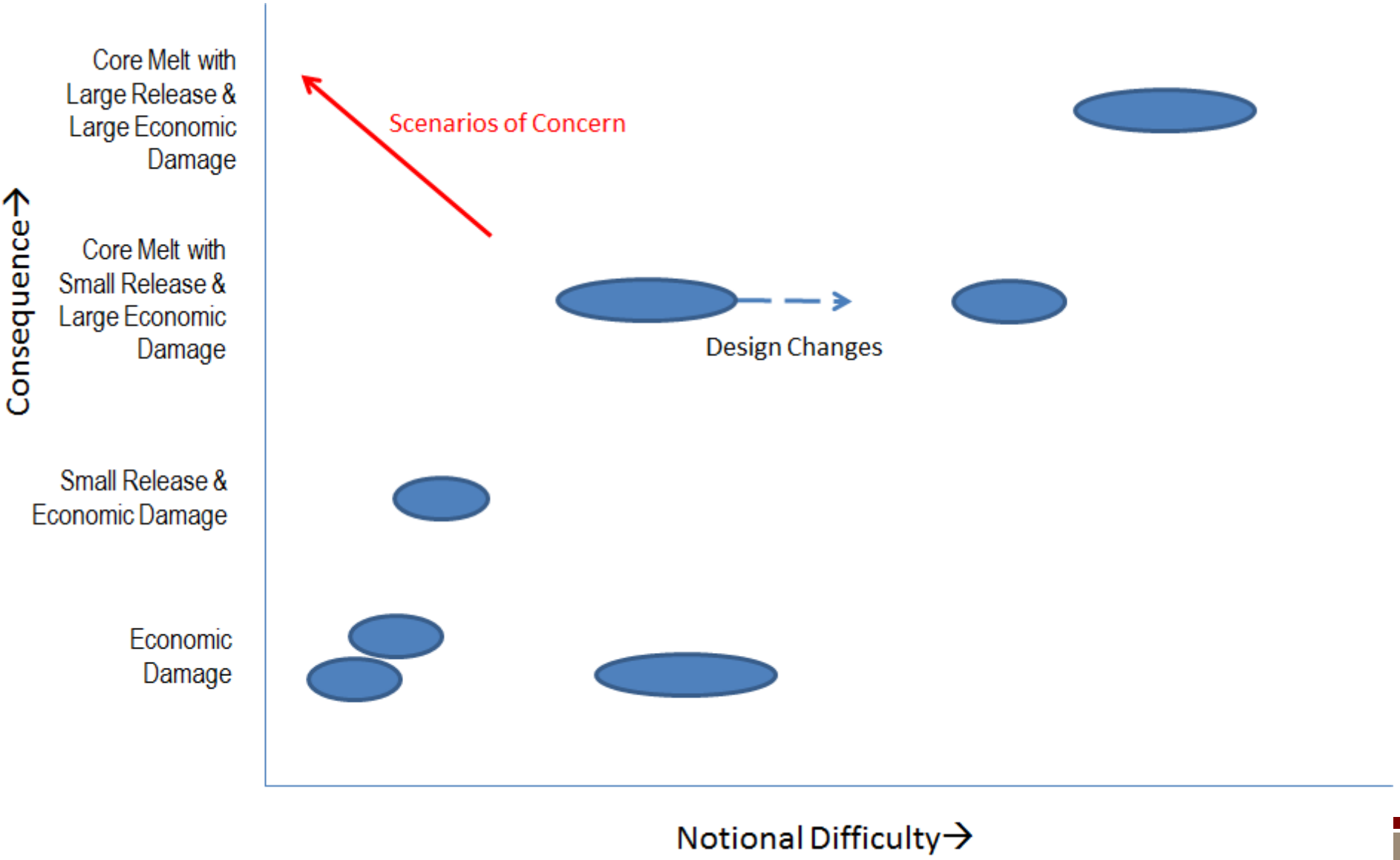
RIMES for Used Fuel Storage Security

Sandia National Laboratories

- Application for Used Fuel Storage Security
  - Development of baseline storage sabotage and theft scenarios
  - Scoring for Attack Difficulty – Preparation and Execution
  - Preliminary evaluation of factors that change over the timeframe of extended storage
  - Basis for developing recommended protection strategies for extended storage
- Additional assessment efforts
  - Consequences and changes in conditions over time
    - Used fuel characteristics (dose rate, material attractiveness, other)
    - Evolution of attack characteristics
    - Other storage system conditions
  - Assessment for changes over time and other storage configurations

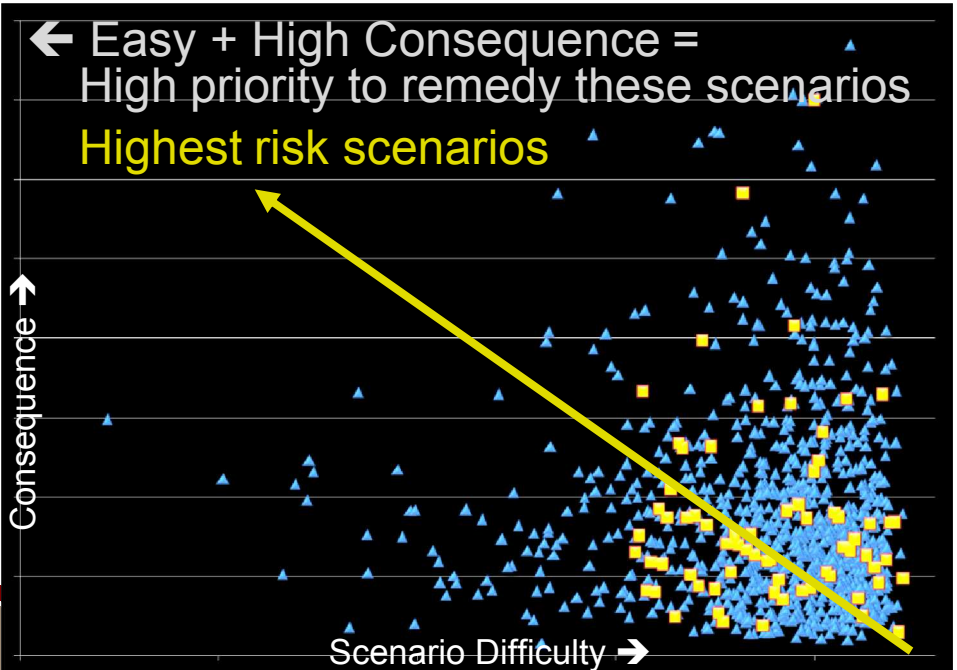
RIMES for Small Modular Reactors Notional Results

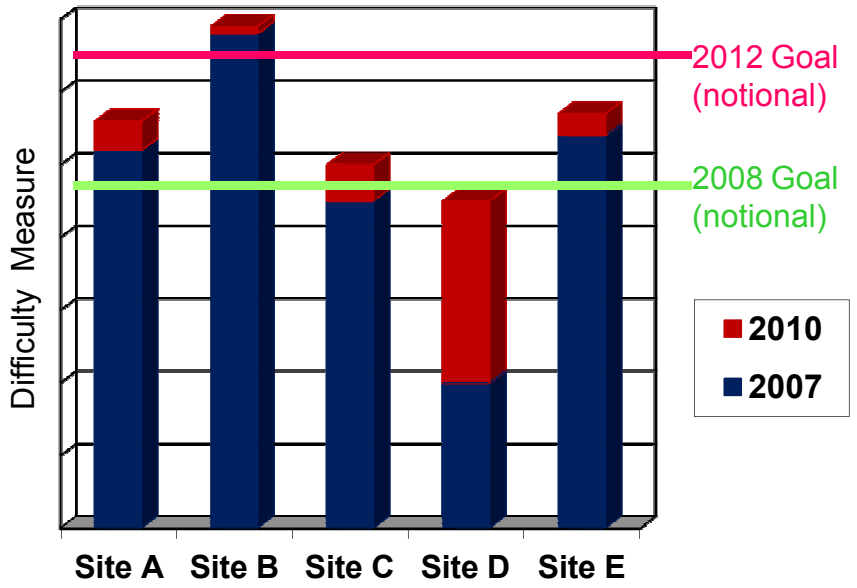
Sandia National Laboratories



Summary

- Focus on security risk *management*.
- Benefits of security investments can be inferred from two metrics:
  - How much harder has the scenario become for an adversary?
  - How much have expected consequences been reduced?
- Robust assessment of scenario difficulty is feasible.
- Method is scalable and encourages productive dialog among security professionals.





Sandia National Laboratories

BACKUP SLIDES

Estimating Difficulty of Attack Scenarios

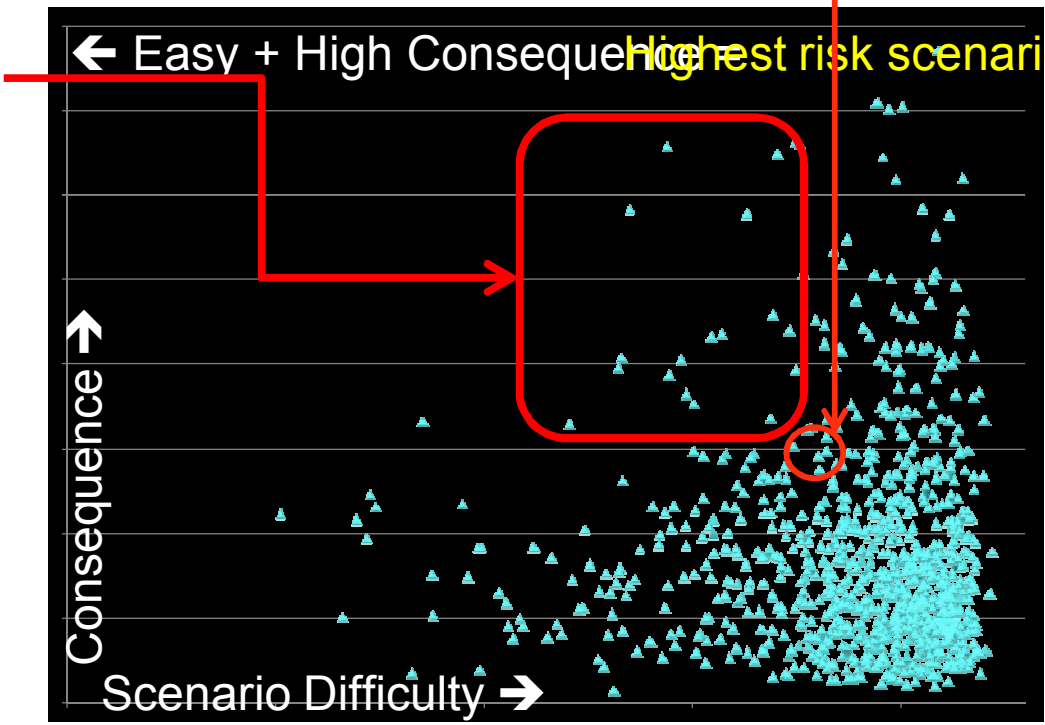
Sandia National Laboratories

General characteristics used to establish levels of difficulty for dimensions.

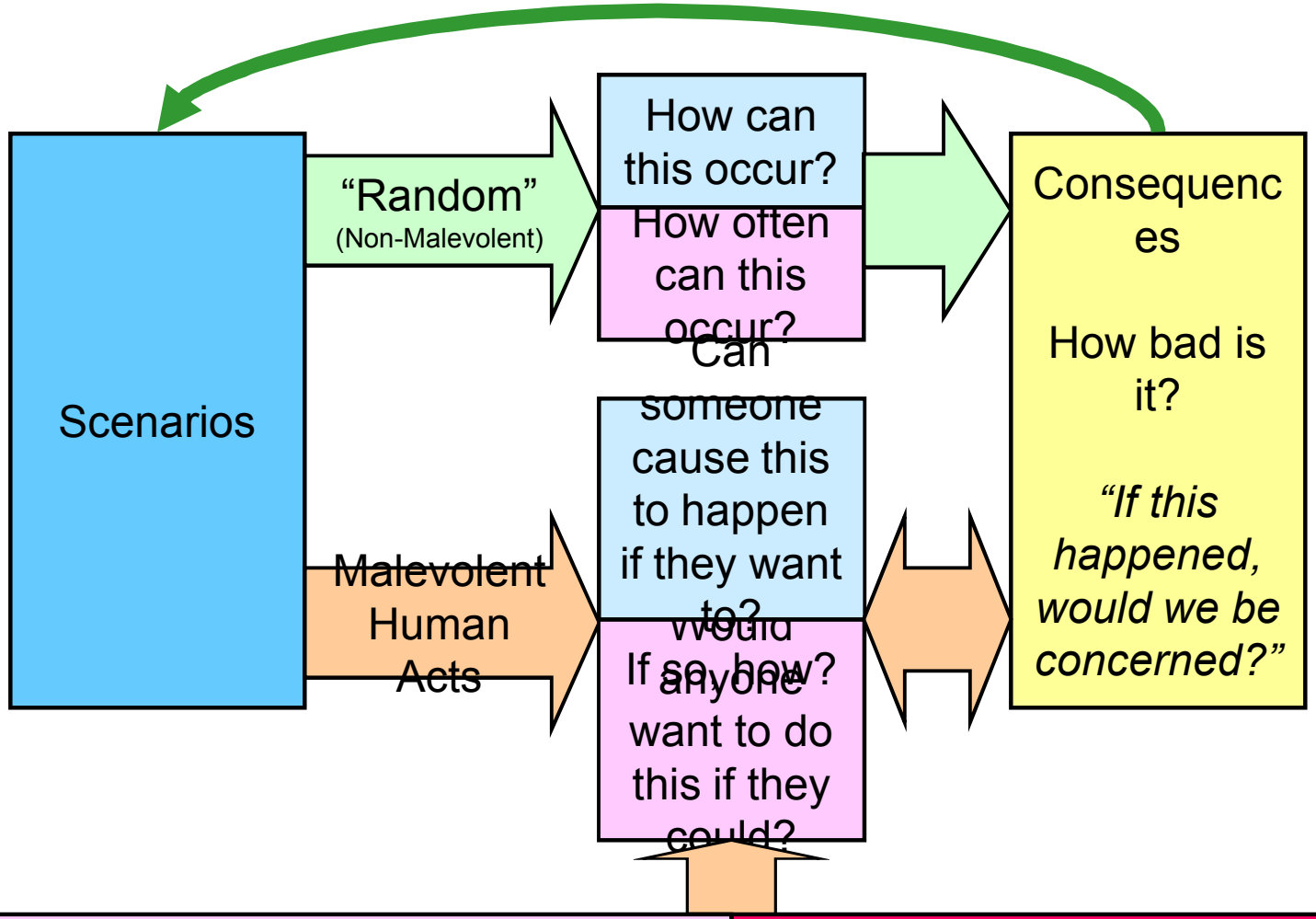
Level 1	Level 2	Level 3	Level 4	Level 5
Easy to get/do	Moderately easy to get/do	Difficult	Very difficult	Extremely difficult to get / do
Capability available by legal means	Requires capability similar to criminal activity	Requires capability similar to organized criminal activity	Requires sophisticated capability similar to large corporation	Requires state-supported capability
Requires no special skills	Requires low-level skills (~days of training)	Requires moderate-level skills (~months of training)	Requires high-level skills (~years of training)	Requires highly specialized skills (~multiple years of training, such as an advanced degree)
Easily accessible by general public	Accessible by public that has moderate-level knowledge	Typically accessible by criminal, paramilitary, or terrorist enterprises	Accessible by highly specialized organizations	Typically accessible only by elite forces
Essentially no early warning signatures - little risk to adversary of disruption	Some early warning signatures that may elevate general concerns of authorities – some risk of disruption			Very large early warning signatures – great risk of disruption

Practical Security Risk Management

- Identify vulnerabilities or defeat methods
- Work these into scenarios that result in consequences
  - *Identify the expected consequences*
- Identify other easier ways for an adversary to generate comparable or greater consequences
  - *Initial security risk screening and prioritization*
- Use good systems engineering to find & rank mitigation options for higher risks
  - ↓ *consequence and/or* ↑ *difficulty*
- Continue throughout project lifecycle



Risk Assessment Overview



Results

Risk
The potential for realizing adverse consequences

Risk Assessment
Give a judgment about the importance or significance of risk

Risk Management
Understand and accept, control, or mitigate risk