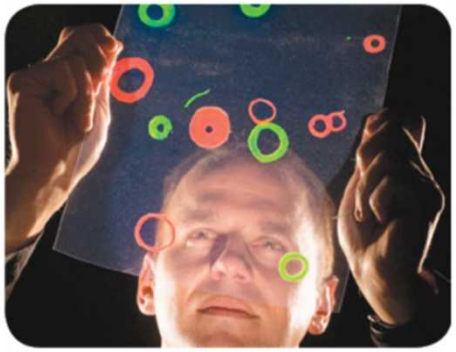
SAND2014-18655PE

Exceptional service in the national interest

Sandia National Laboratories


Supply Chain Lifecycle Integrity Decision Analytics

IEEE ICCST 2014

Technical Lead: Gio K. Kao
gkkao@sandia.gov
Program Manager: Han W. Lin
hwlin@sandia.gov
Sandia National Laboratories

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.

Supply Chain Dilemma…

Top Pressures Driving SC Management

- Cost
- Time
- Quality

Decision to

Buy Make Outsource

Vulnerabilities

How much risk are you willing to take?

How to manage risk when much of the SC are overseas?

Supply Chain Vulnerability: Access, Targeting, Influence and Control

Problem Statement – Why are we here?

- **Current approaches in addressing supply chain security and integrity…**
  - Do not address complexity and scalability
  - Prioritize on cost without security in mind
  - Lack scientific and engineering foundation
  - Provide localized point-based solutions
  - Are reactive
  - Are disjoint (lack visibility and cooperation along the supply chain)

Supply Chain is a global problem!

We are making tools that will analyze supply chain integrity and provide decision support to strengthen your supply chain

Bottom Line Up Front

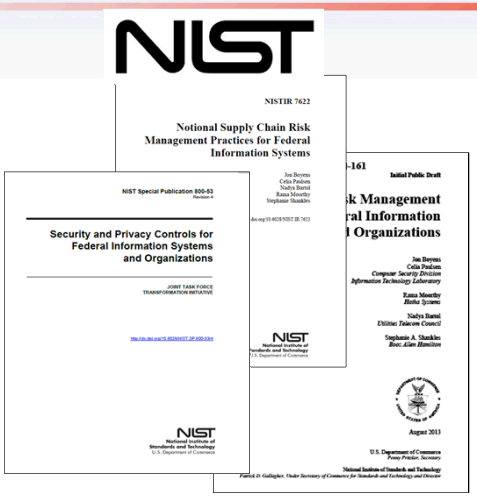
- **Key Contributions (paradigm shift)**
  - Developed supply chain integrity analytic framework
    - Holistic lifecycle-based approach for full spectrum supply chain flow analysis
    - Reduce subjectivity while increase objectivity
  - Developed optimization tool for cost-benefit decision analysis
    - Repeatable, concise, rational decision making

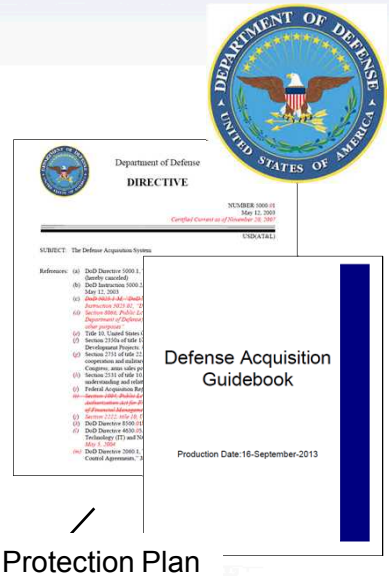
Provide insights for decision makers and analysts to perform risk-based, cost-benefit decision support under uncertainty.

Unique Key Benefits

- Reduced complexity (bounding the problem)
- Incorporate continuous monitoring methods
- Risk-based, cost-benefit analysis
- Bird's-eye view of the supply chain lifecycle representation

Related Work



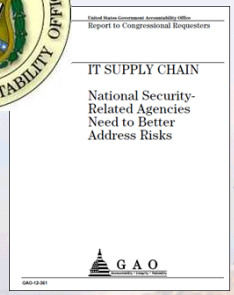


IATAC

- Decision/Control Points
- Best Practices Guidelines
- Threat Generalizations
- Mitigations Classes

- Program Protection Plan
- Criticality Analysis
- Program Lifecycle

Sandia
OGA



- Supply Chain State of the Union
- Recommendations

Supply Chain Integrity
Lifecycle Analytics
R&D

Supplier Analysis

Differentiation: A framework that leverages existing work and provides solutions on how/where/when to apply mitigation options.

What is missing from today's body of work?

- How do we actually implement these mitigations?
- How do we know if these mitigations are effective?
- How do we leverage data collected?

Provides a method to *measure* and *analyze* supply chain risk

IATAC

NIST

Data
Intelligences
SMEs

Supply Chain Lifecycle Analytics
- **Vulnerability Analysis**
- **Mitigation Analysis**
- **Metrics/Trade-off Analysis**

Very good at answering what!

Goal: To show how it can be done, and how to mitigate risk!

Perform novel analyses on the amalgamation of supply chain structures and on potential attack structures.

Leveraging Sandia's Expertise

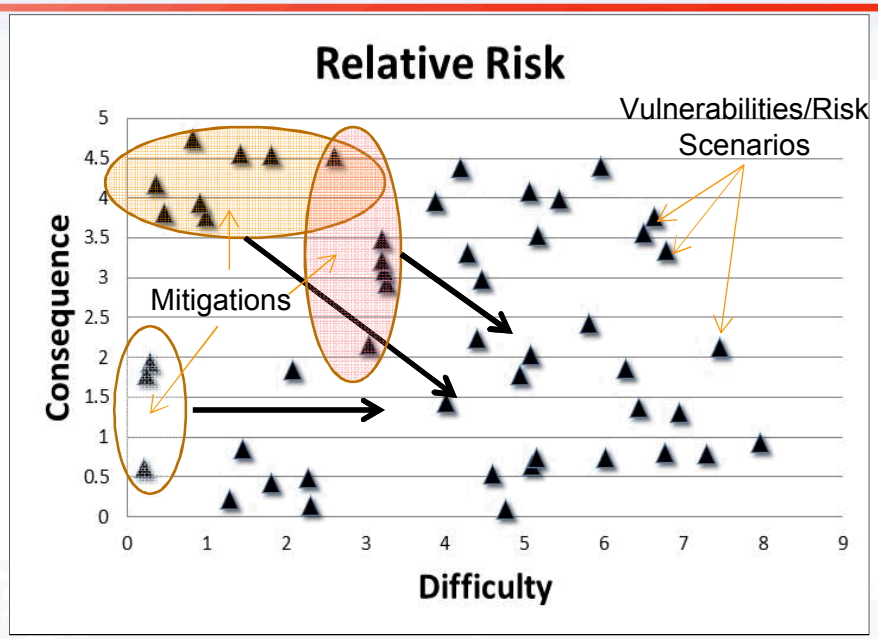
- **Internally funded effort to investigate the bigger problem will leverage**
  - Supplier analytics
  - Wyss et al., "Risk-Based Cost-Benefit Analysis for Security Assessment Problems", IEEE 44th ICCST, San Jose, CA, 2010.
  - Sandia's decision analytics expertise
  - Sandia's cyber security expertise
  - Sandia's physical security expertise
- **External OGA supply-chain-related collaboration**

Establish Sandia as a center of excellence in supply chain analytics

Supply Chain Integrity Decision Analytics

- **Purpose:** Provide analytics for decision makers to identify, assess and mitigate risk in the supply chain lifecycle, enabling a more secure national infrastructure.

- **Challenge:** A gap in supply chain integrity exposes the national security infrastructure to potential vulnerabilities



- **Technical Approach:** Build a Decision Analytics Tool Suite that helps analysts discover, analyze (measure) and mitigate supply chain risk.

Major Components

1. Supply Chain Representation
2. Vulnerability and mitigation attack graph assessment
3. Risk assessment
4. Optimization and decision analytics

Scope Associated to Supply Chain Lifecycle

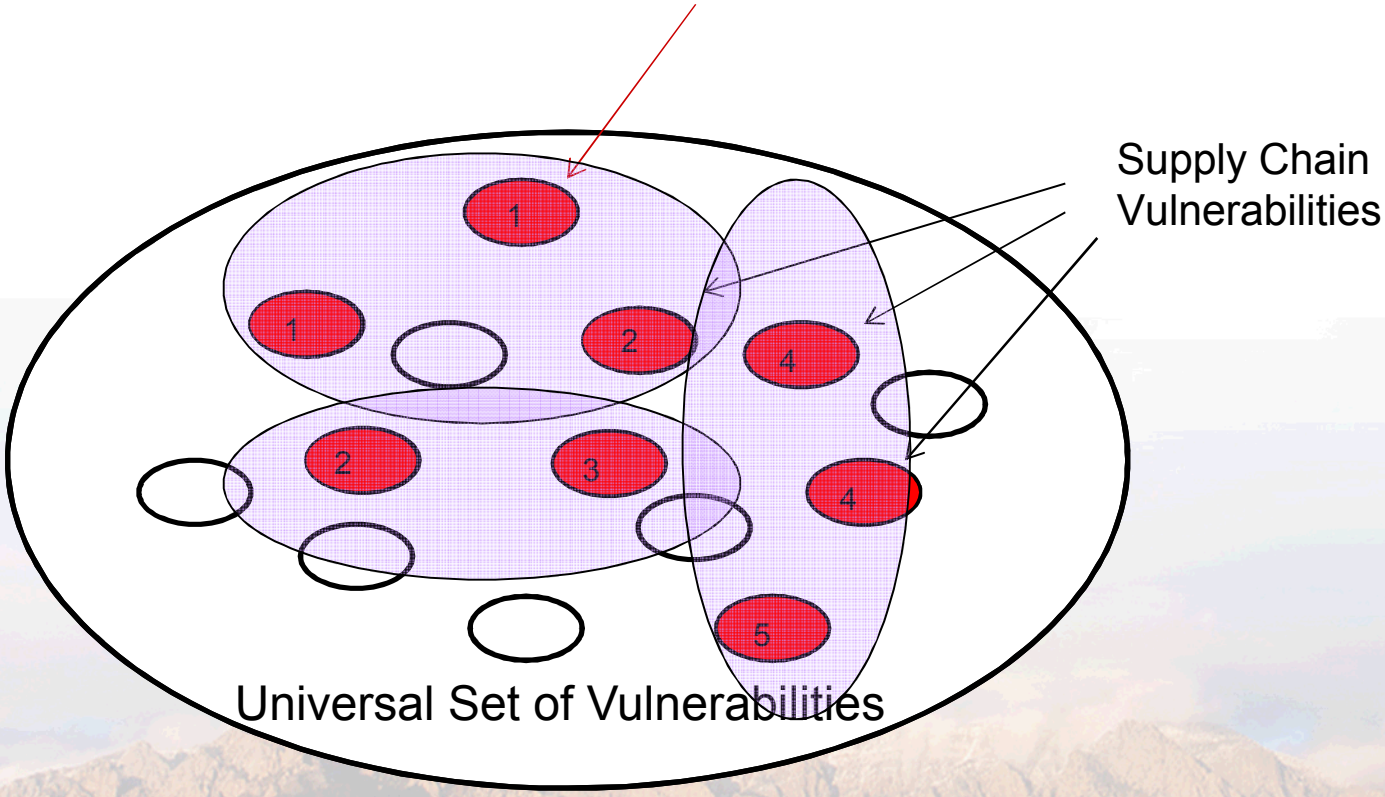
- **Supply Chain Vulnerabilities include**
  - Counterfeit parts integrated into product
  - Nefarious activities during testing to affect quality of shipped parts
  - Malicious alterations of product (function)
  - Disruption of distribution network
  - Psychological impact to the perceived confidence in the supply chain

Supply Chain Vulnerability: Access, Target, Influence and Control

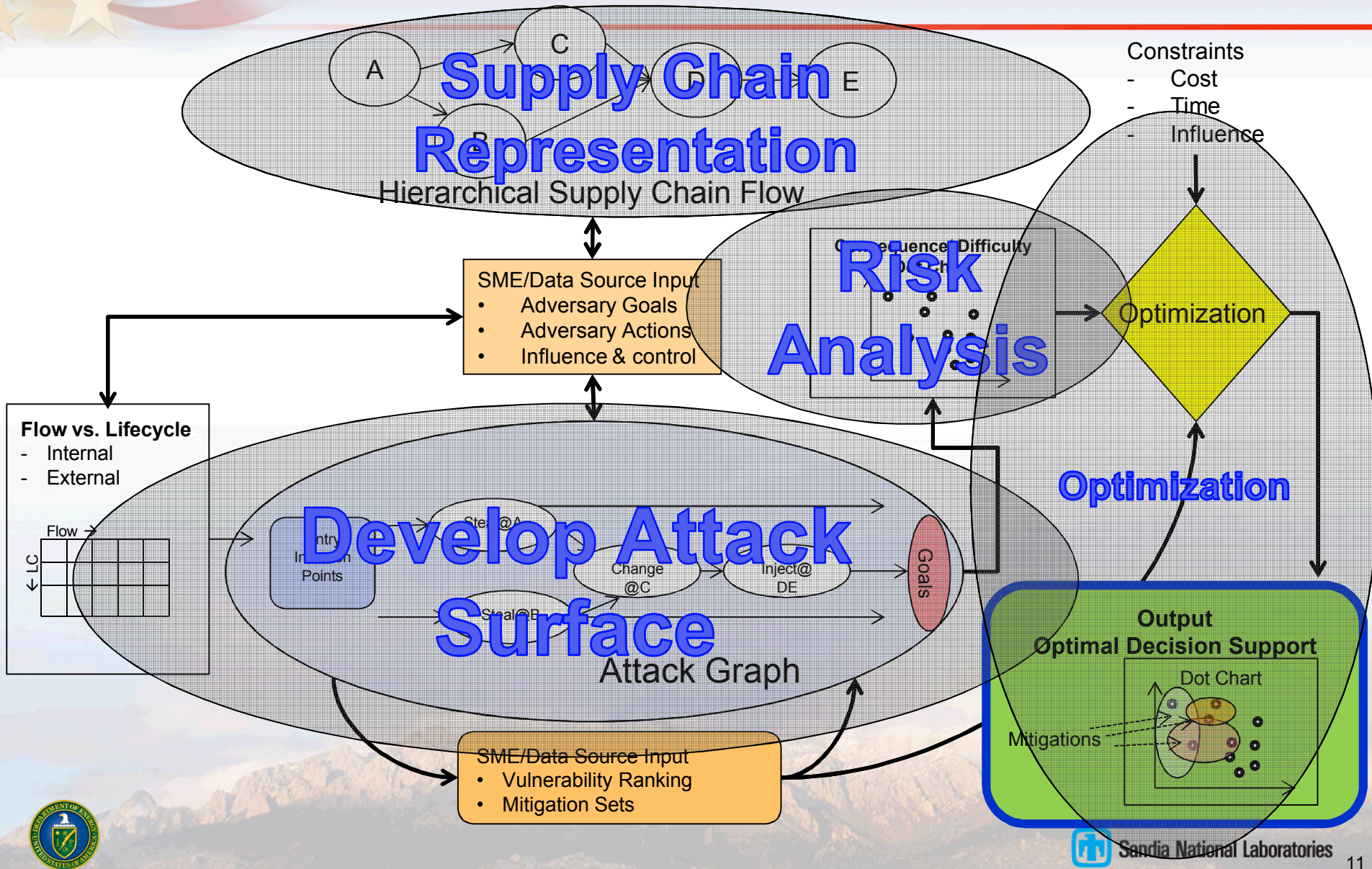
Sandia National Laboratories

Supply Chain Integrity Decision Analytics

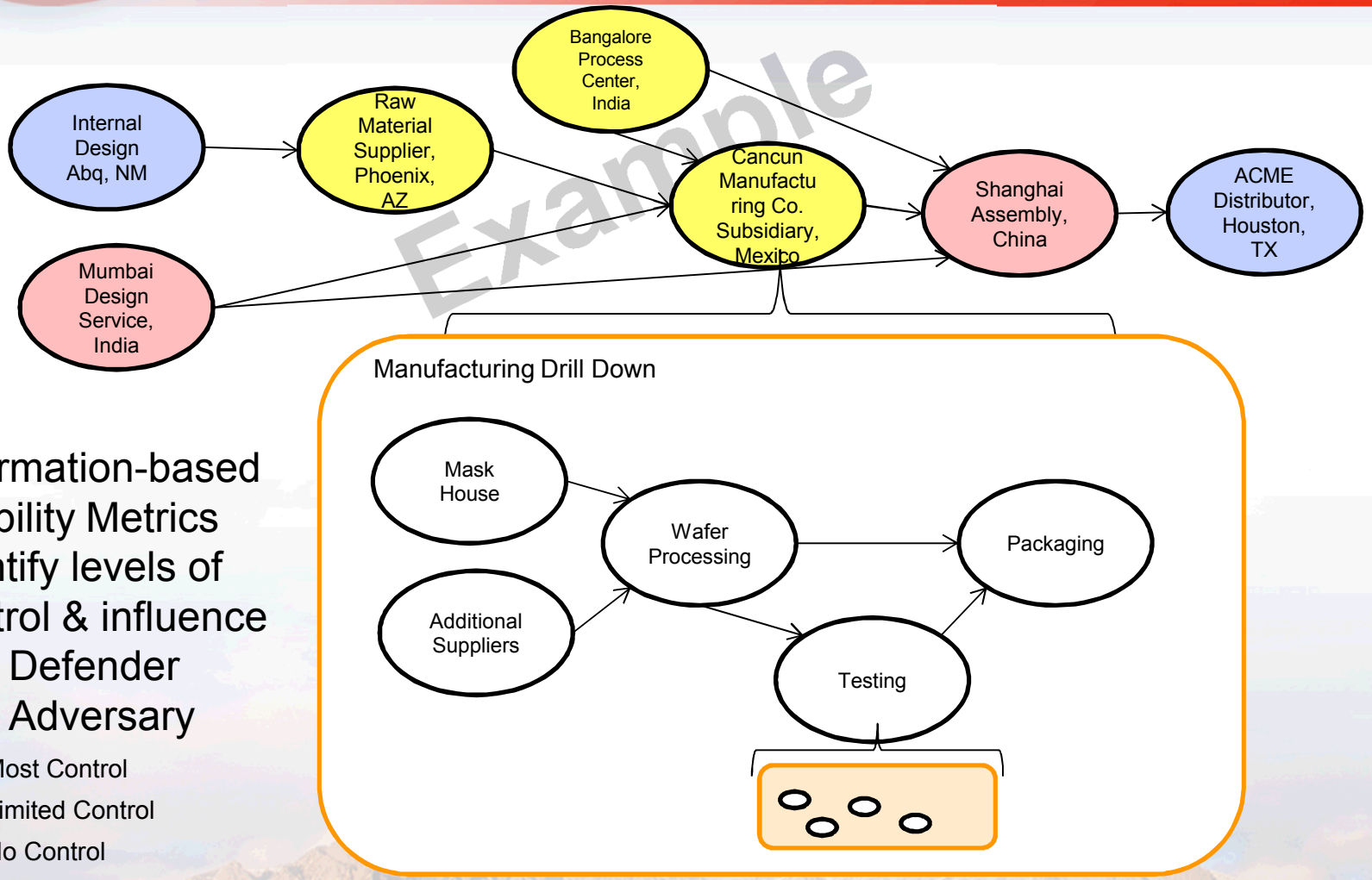
- The steps of the analytic framework:
  - Discover supply chain vulnerabilities
  - Assess and rank (consequences and difficulties)
  - Apply optimal mitigation(s)



Supply Chain Integrity Analytics Framework - Overview



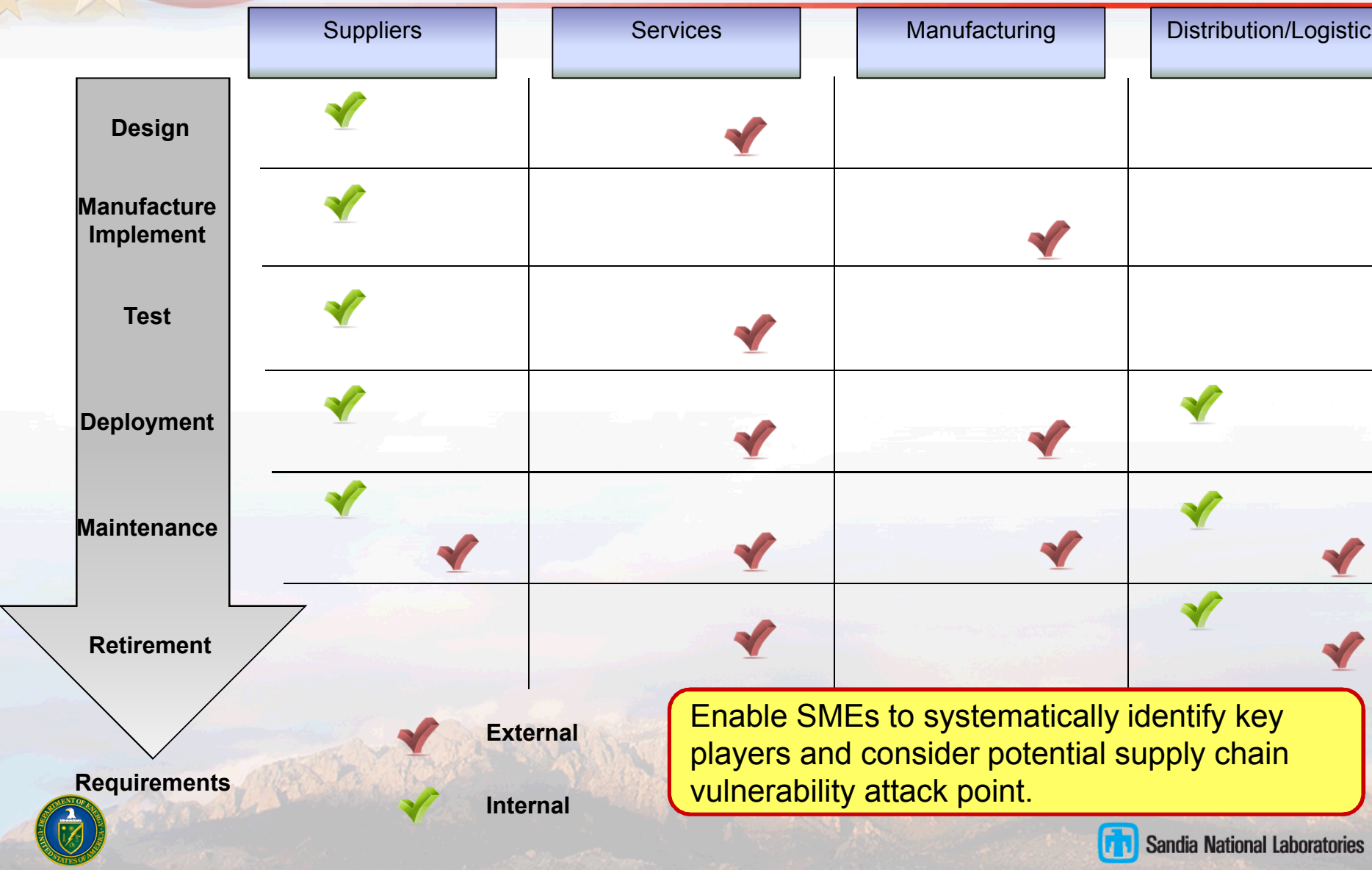
Hierarchical Supply Chain Flow Scenario



- Information-based
- Visibility Metrics
- Identify levels of control & influence
  - Defender
  - Adversary

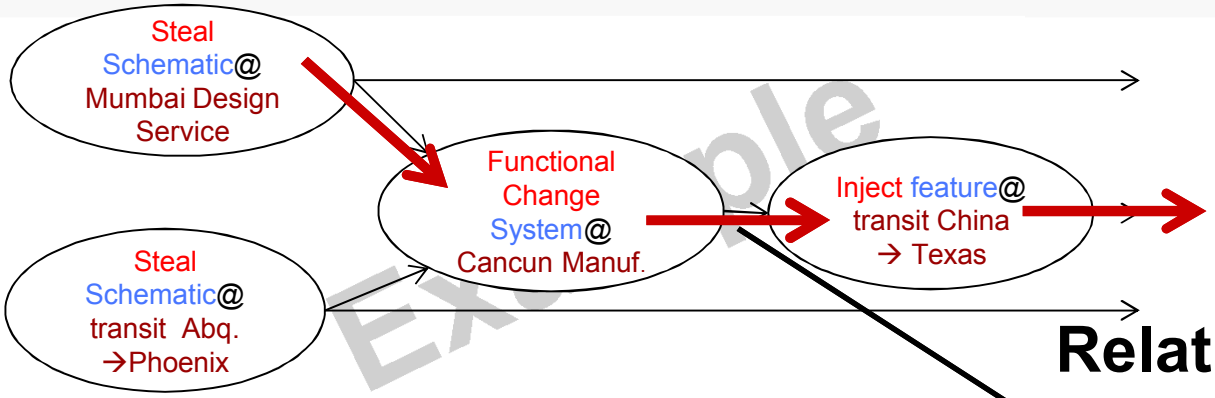
Most Control
Limited Control
No Control

Supply Chain Flow and Lifecycle Matrix

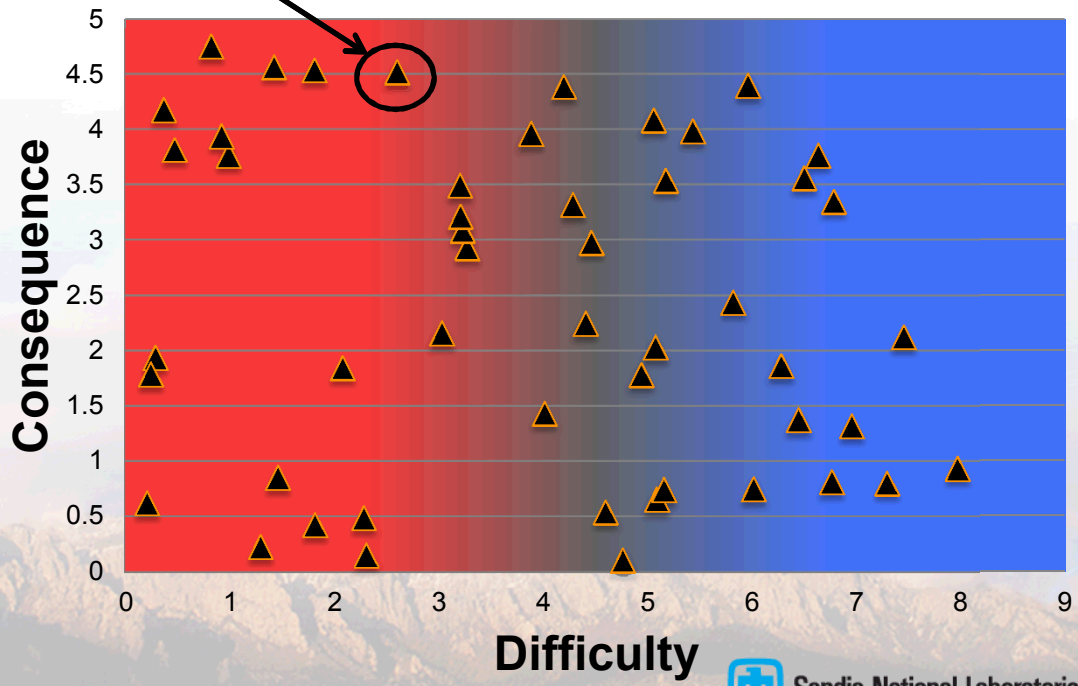


Enable SMEs to systematically identify key players and consider potential supply chain vulnerability attack point.

Scenario Path



Relative Risk

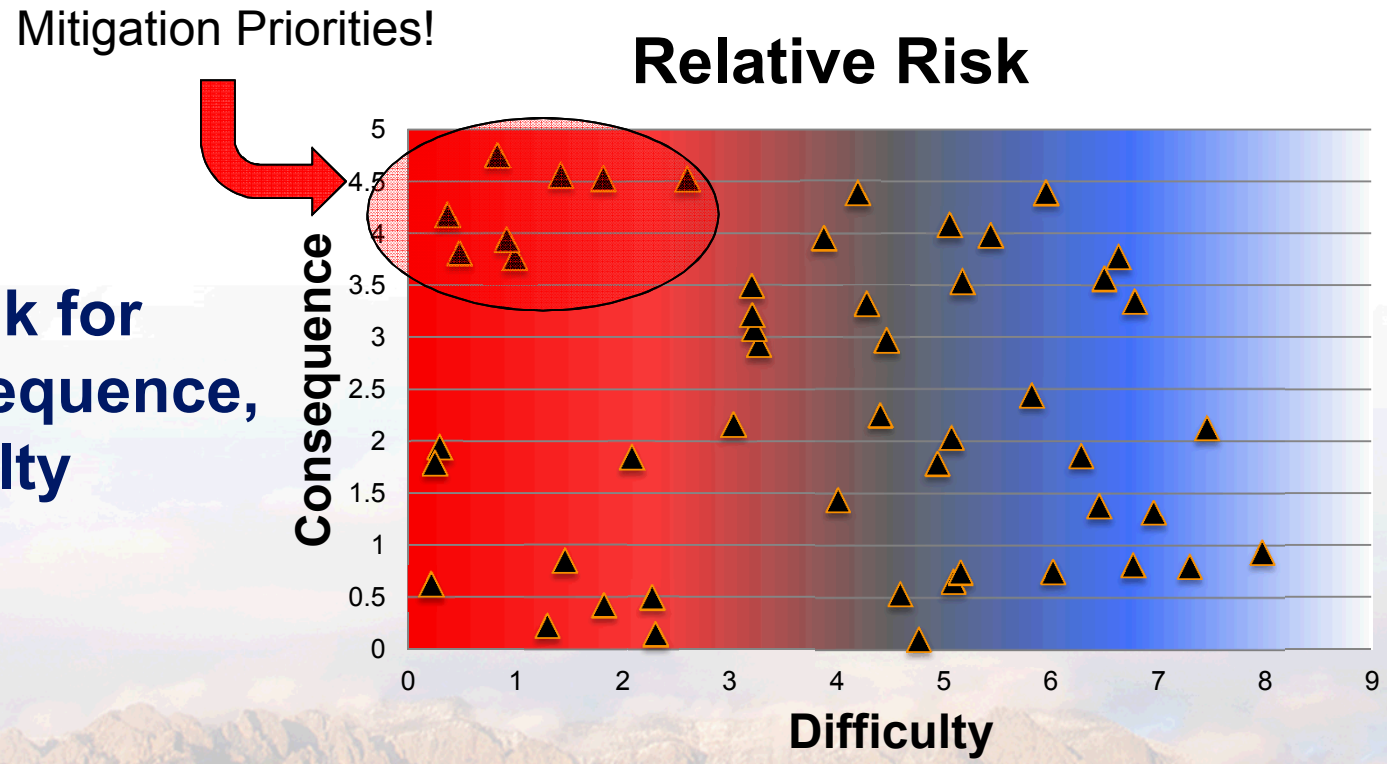


A path is represented by a dot with associated level of difficulty and consequence

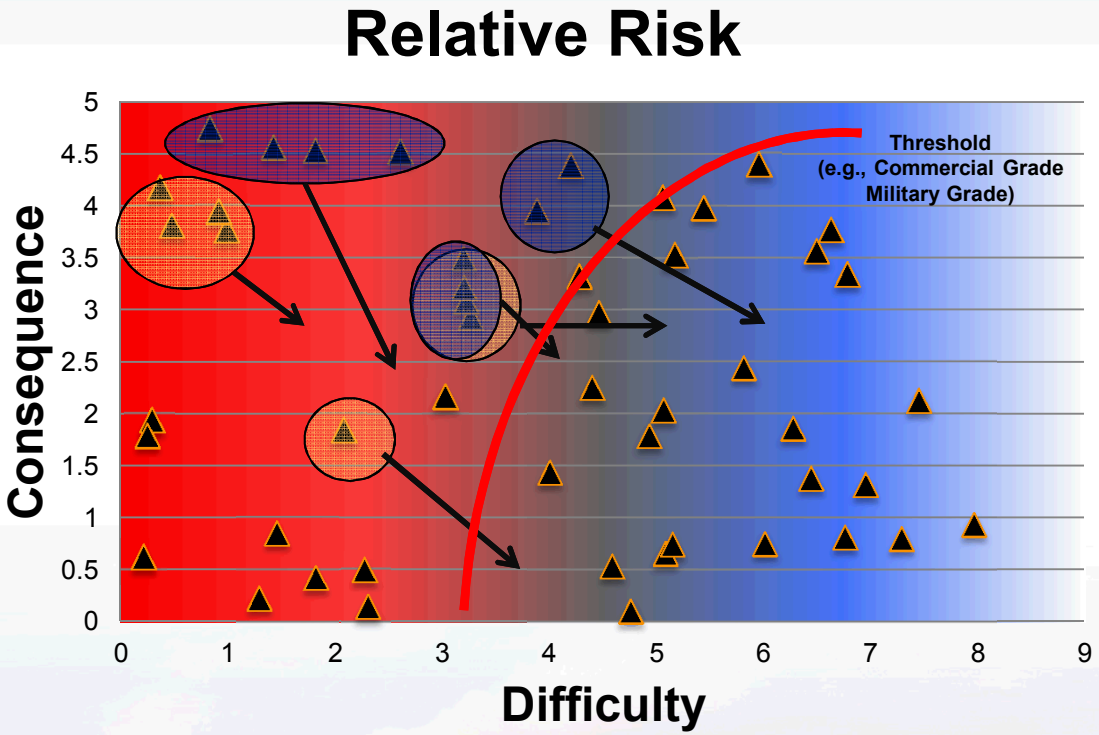
Risk Analysis

- How do we prioritize where to apply mitigations?

- Reduce risk for high-consequence, low-difficulty attacks



Composing Mitigations?



- Multiple mitigations must be applied to ensure coverage of high priority vulnerabilities
- But…
  - Double coverage / Sufficient coverage?
  - Wasted cost from over-coverage?
  - How do we predict the impact of aggregated mitigations?

Solution: Optimization

- **Open questions for determining which mitigations to apply**
  - What is the minimal coverage to maintain confidence?
  - Can we quantify risk by coverage of vulnerabilities?
  - Subject to cost constraints
    - Several mitigation options may exist, but applying all is not feasible
    - Cost of loss
- **Facilitate development of robust best practices requirements and processes**
- **Through optimization, analyze current and future mitigations to build optimal investment portfolio**
  - Cost-benefit analysis on technology investment
  - Proactive vs. reactive
  - Help identify gaps between mitigations

What are the best mitigations to apply under constraints?

Sandia National Laboratories

Path Forward

- **Research**
  - Continue to refine the integrity assessment methodology
  - Difficulty composition problem (reconciling overlapping attacker efforts)
  - Mitigation composition problem (mitigation option interaction)
  - Advanced optimization techniques
  - Uncertainty quantification
- **Development**
  - Tool suite development and integration
  - Visualization and filtering methodologies
  - Use case application and demo