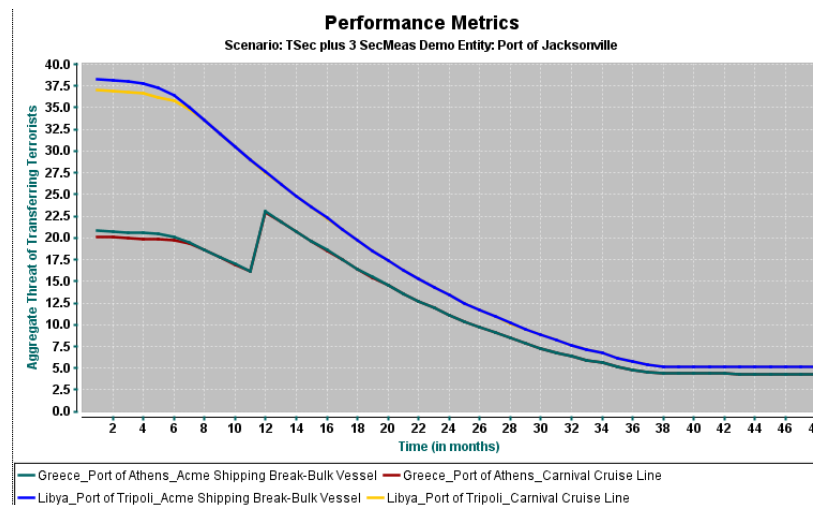


# TRANSEC: Risk Management Decision Support for Transportation Networks

## Model-Simulate-Analyze



**Dr. Richard Adler**  
DecisionPath, Inc.  
[rich@decpath.com](mailto:rich@decpath.com)  
617.794.9036

**Jeff Fuller**  
Teledyne Brown Engineering, Inc.  
[jeff.fuller@tbe.com](mailto:jeff.fuller@tbe.com)  
703.731.2093

# Agenda

- Who we are
- Managing risk from terrorist threats
  - Our perspective
  - Our methodology
- TRANSEC
  - History
  - Decision Model
  - Demo / Screen Shots
- Conclusions
- Questions



# DecisionPath

- HQ in Boston area
- Focus
  - Help Govt & bus. orgs make & execute critical decisions more effectively
  - Software solutions for critical decision support
  - ForeTell-DSS® software platform
- Markets
  - Government, Pharmaceuticals, Financial Services
- Background
  - Mgmt. consulting, software architecture & start-up execs
  - AI, simulation, distributed systems, component frameworks, KM
  - Mission-critical operations & decision support applications



# Teledyne Brown Engineering

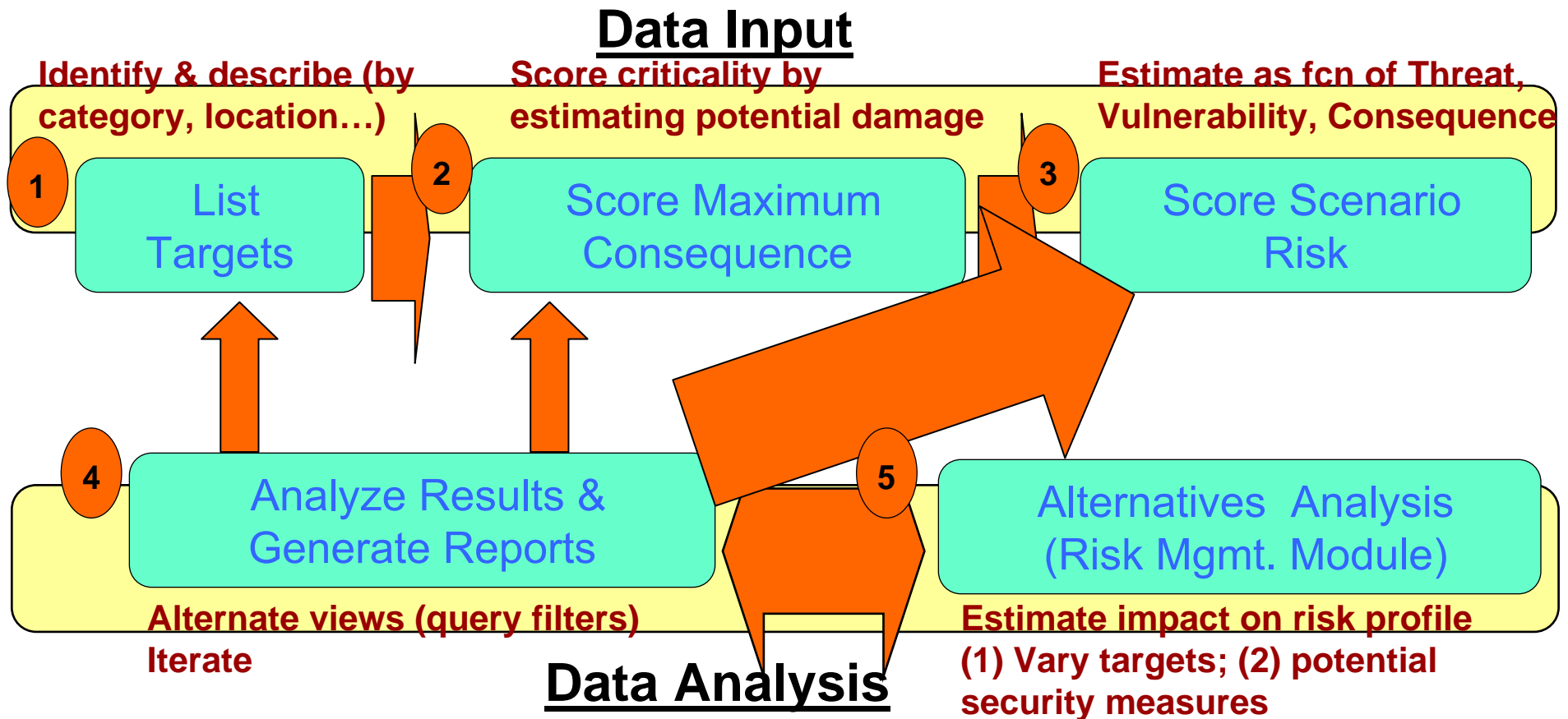
- HQ: Huntsville AL
- Focus
  - Engineering Services, Systems Engineering and Integration, and Hardware Design, Development and Manufacturing
  - Modeling and simulation support including force capability analysis, air defense, medical planning
  - Maritime security services and products
- Markets
  - Defense, space and homeland security markets
- Background
  - Civilian and military space engineering
  - Wide range of DOD support services and products



# Example Risk Analysis System

- Maritime Security Risk Analysis Model - MSRAM

- US Coast Guard Domestic Port Security Evaluation Division
- MS Access DB desktop application (ABS/Teledyne-Brown Eng.)



# Issue 1: Risk Management is Dynamic

- Risk Management is an extended process
  - Security programs take time to develop, deploy, and perfect
  - Meanwhile...
    - Security environment evolves over time
      - Social, economic, political, and technological forces, trends, events
    - Terrorist groups evolve over time
      - New groups form; existing groups dissolve or split into factions
      - Develop new capabilities
      - Change targeting and attack strategies and tactics
      - Adapt to environmental changes and to our security programs
- Dynamic vs. static approach
  - Assess how risk mitigation strategies buy down risk over time while the world changes
  - Requires “what-if” simulation vs. “before-after” snapshots



# Issue 2: Structure of Strategies Matters

- Model structure & impact of security strategies **over time**
- Strategy = set of prospective security measures
  - Reallocate existing resources
  - Invest in new personnel, systems, technology, training..
  - Security Measure
    - Schedule (Start time => End time)
    - Estimate Costs: initial program costs and annual (O&M) costs
    - Estimate impact over time on security performance metrics
- Why?
  - Enables critical cost-benefit studies
    - How much does it cost to buy down risk from level x to level y
  - Enables benefit vs. time studies
    - How much is risk reduced while programs are being implemented
    - Potential overlaps & synergies
    - **Study potential impact of program-level implementation risk**
      - Schedule, resources, technology, critical path problems
  - Compares any # of competing approaches, not just pairwise



# Issue 3: Risk is Broader than Attack

- DHS/USCG focus to date has been primarily on direct attack (boat or truck bomb) & exploitation threats (hijacked vessel)
  - Presuppose terrorists already in place & prepared/preparing
- However, risks arise “upstream” that require attention
  - Reduce risk of attack by reducing transfer threat risks
    - Transfer of personnel & materiel into the country
- Problem
  - Transfer threats arise before targets & attack modes are known
  - Cannot easily apply standard  $R = T * V * C$  risk construct
- Need an alternate construct for analyzing risk
  - Adapt failure models used by reliability engineers
- Broader objective
  - Analyze risk and risk mitigation strategies for direct attack, exploitation, transfer and WMD threat risks



# Issue 4: Need Adaptive Security Strategies

- Objective of asymmetric warfare
  - Carry out (or threaten) one attack via new attack mode
  - Trigger costly programs to counter/defend on national scale
  - Attack our national economy
- One approach: real options theory
  - Leverage value of uncertainty (offshoot of financial derivatives)
  - Re-design security programs as sequence of modules
    - Each segment yields increased risk reduction at incremental cost
    - Go/No-Go decision points
  - Complete initial segment & reassess risk landscape before committing to proceed
  - Adaptive strategies to counter adaptive adversaries
    - But... this requires explicit modeling of program structure, costs, and dynamics



# Methodology

- Model risk and risk mitigation dynamically
  - Focus on drivers of change over time vs. discrete snapshots
- Employ scenario planning & “what-if” simulation (ForeTell®)

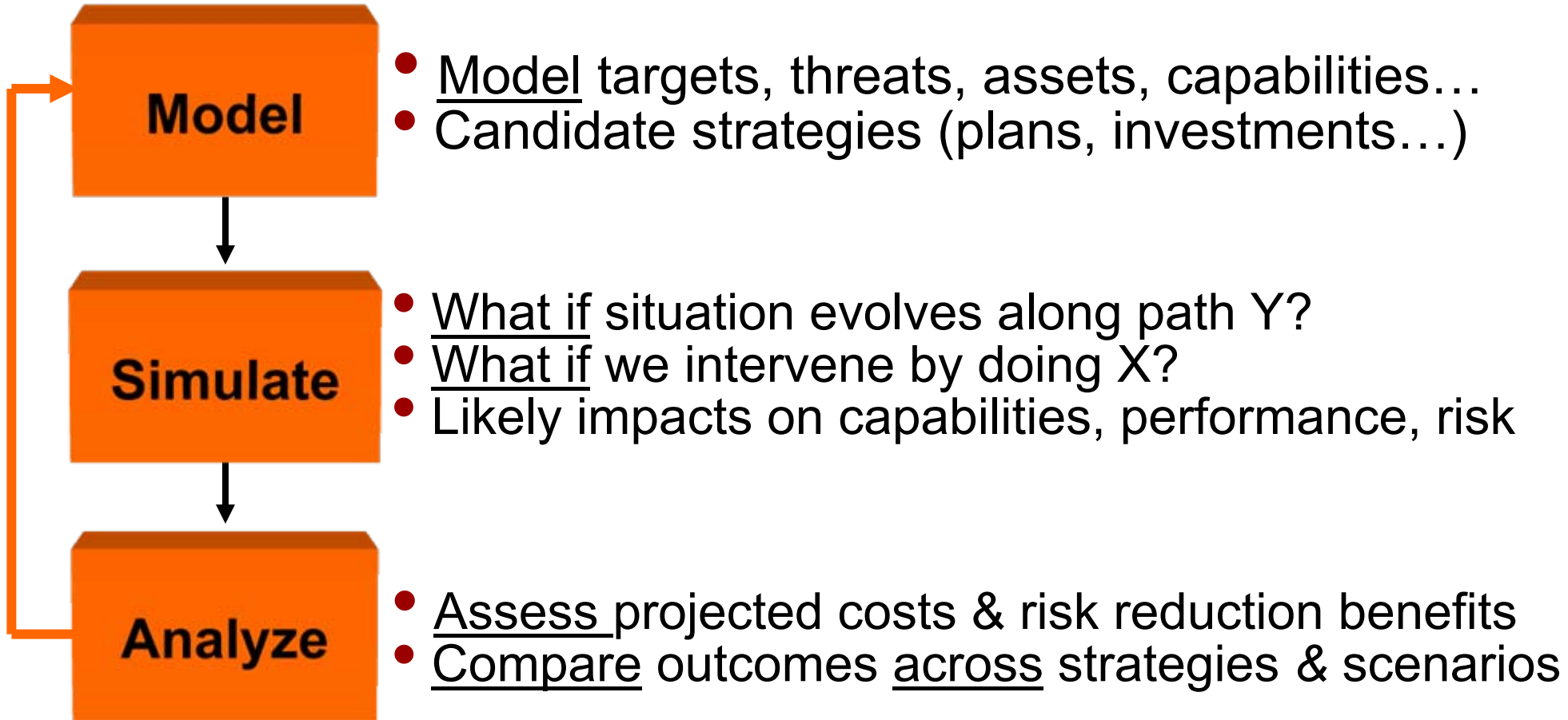
=>

- “Test drive” your critical decisions
  - Practice & learn in a low-risk virtual environment
- Provide process-level support across lifecycle
  - Must execute strategy to be successful
  - Employ method at point of decision / execution / continuous learning
  - Apply in training and field environments
- Reduce risk while improving confidence & consistency



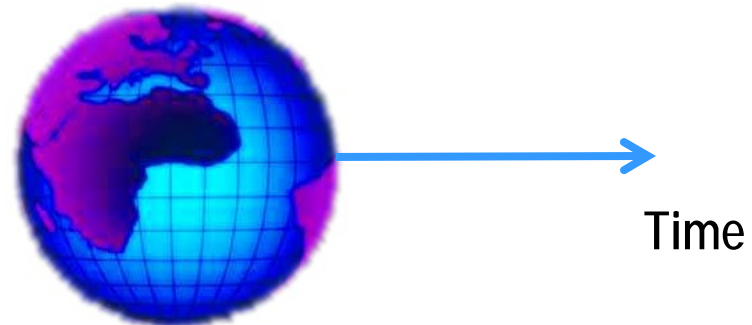
# ForeTell<sup>®</sup> Platform

Low-risk virtual environment to test-drive critical decisions

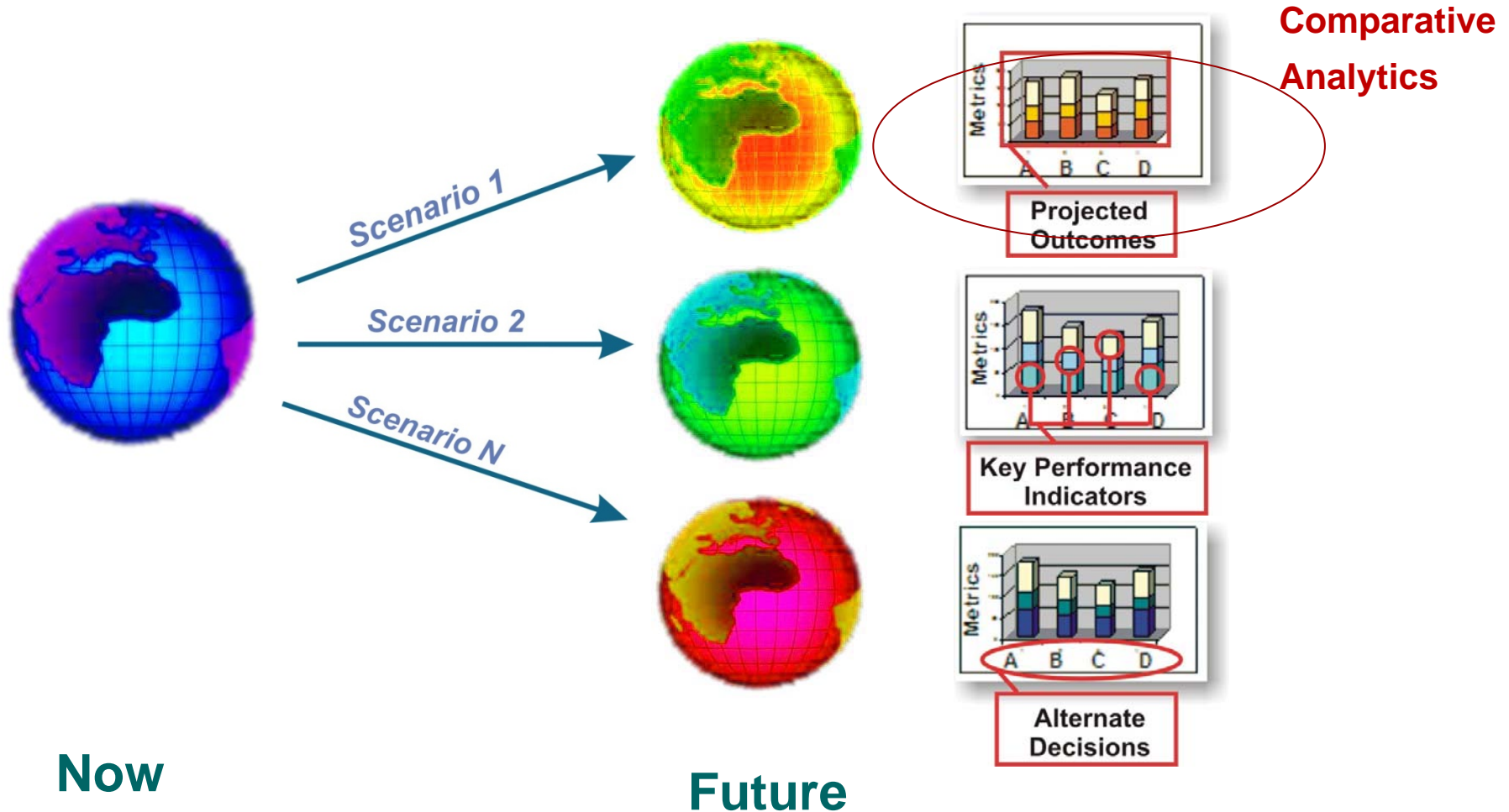


# ForeTell<sup>®</sup> Scenario

- Expand from {target, attack mode} construct
  - Focus on drivers of change over time vs. discrete snapshots
- Baseline situation
  - Initial conditions & state of actors of interest
  - Initial values of key performance metrics
- Assumptions about environmental forces, trends, events
  - How the world is likely to evolve
- Prospective decision strategy
  - Prepare for that future



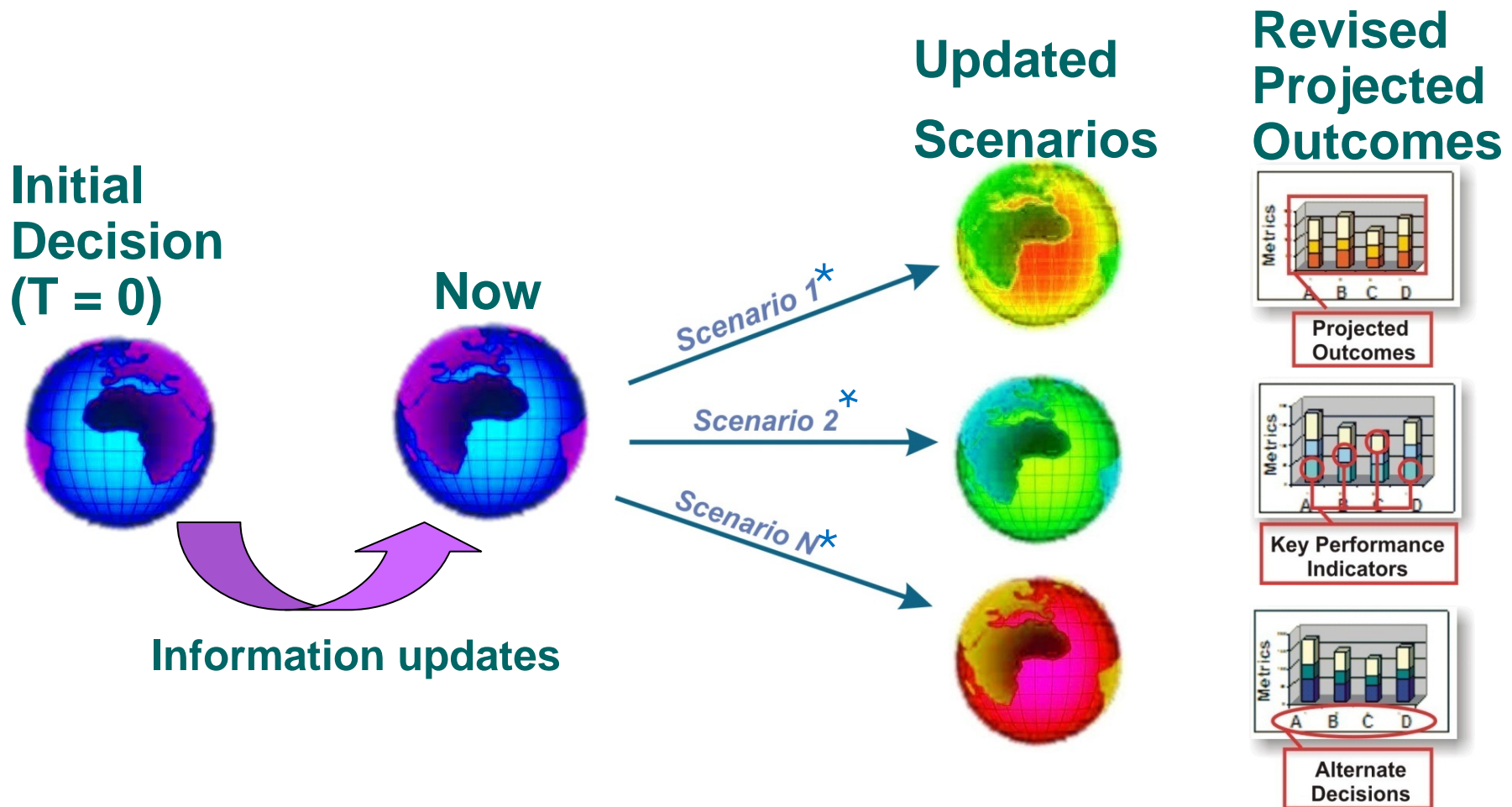
# Scenario Planning + Simulation



Goal: Identify best outcomes across scenarios

# LifeCycle Decision Support Execution Phase: Sense & Respond

Goal: Re-validate decision or detect risk & adapt rapidly



\* = Updated or possibly new plausible scenarios

# TRANSEC History

- 2003
  - Initial prototype based on Silent Vector exercise (CSIS)
  - Counter-terrorism planning, situational response & GIS integration
- 2006-2007
  - Partnered with **Teledyne Brown Engineering** (TBE)
    - Contractor for US Coast Guard Port Security Program
    - **Maritime Security Risk Analysis Model (MSRAM)**
  - Extend MSRAM risk analysis with risk management
  - TRANSEC pilot focused on (maritime) terrorist transfer threat
- 2008 (with TBE)
  - Pilot for Joint Counter-Terrorism Centre, Govt. of Singapore
  - Extend TRANSEC to address direct attack threats (aviation security)
- 2009 (with TBE & USCG)
  - Validate TRANSEC with USCG data on small vessel threat (**MSRAM+**)



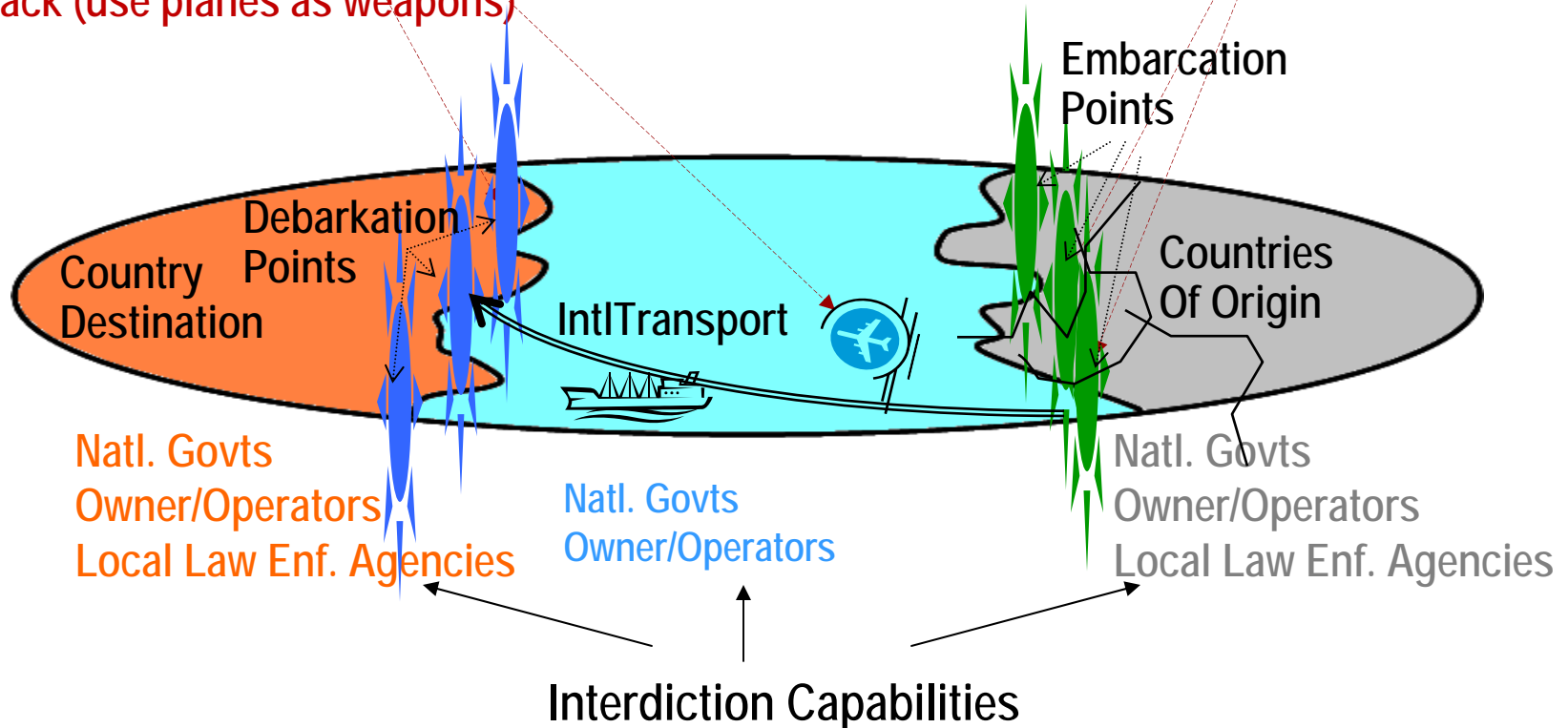
# TRANSEC Terrorist Threat Concept

## Terrorist Group Attack Threats

- Target Airports & Airlines  
(DebarcationPoints, IntlTransport)
- AttackModes:
  - Emplaced
  - Standoff
  - Hijack (use planes as weapons)

## Terrorist Group Transfer Threats

- Terrorist personnel – leaders, skilled support, shooters
- Materiel - weapons, weapon components, sensors...
- Presence in countries of origin



# TRANSEC Dynamic Decision Model

## Vulnerability & Consequence Factors

Effectiveness System Security to Interdict Attacks Emplcd or Standoff

Inputs

Attack Threat

Attack Threat Emplcd/StdOff | Vulnerability Emplcd/StdOff | Consequence  
Risk of Attack Emplcd/StdOff

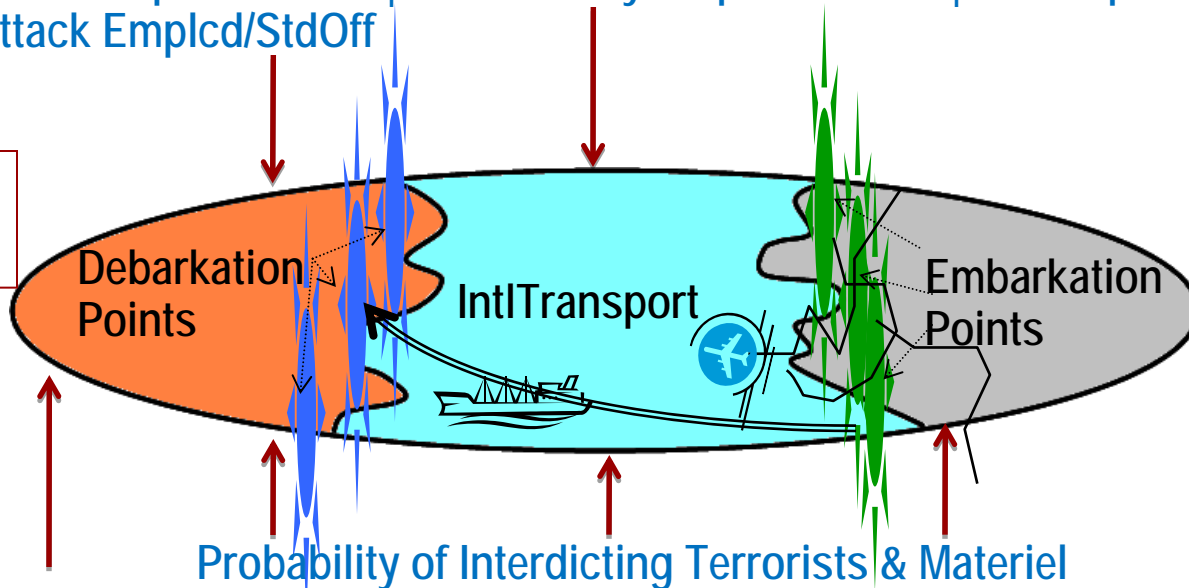
Outputs

Counter-Terror Security Measures

Terrorist Group

Capability & Intent for Transfer & Attack Threats

Cost, Schedule Est. Impact on Security Metrics



Total Costs

Probability of Interdicting Terrorists & Materiel  
Reduction of Risk of Transferring Terrorists & Materiel

Outputs

Transfer Threat

Effectiveness System Security vs. Terrorists and vs. Materiel

Inputs

Natl. Govts

Natl. Govts

Natl. Govts

Owner/Operators

Owner/Operators

Owner/Operators

Local Law Enf. Agencies

Local Law Enf. Agencies

Counter-Terror Security Actors

# Assess Risk & Risk Mitigation Strategies

TargetCategory	Emplaced	Standoff	Hijack-Weapon
Commercial Jet	70	60	40
Private Jet	50	40	20
Cargo Jet	20	15	10
Airport	80	65	0

$$\text{Risk} = \text{Threat} * \text{Vulnerability} * \text{Consequence}$$

- TerroristGroup
- Capability
  - Intent
  - Relative Weights

- Airplanes
- EffectivenessOnBoardSecurity
  - AgeTransport
  - Capacity (Passengers, Cargo)
  - Symbolic Value
  - Relative Weights

- Airports
- EffectivenessAttackResponse

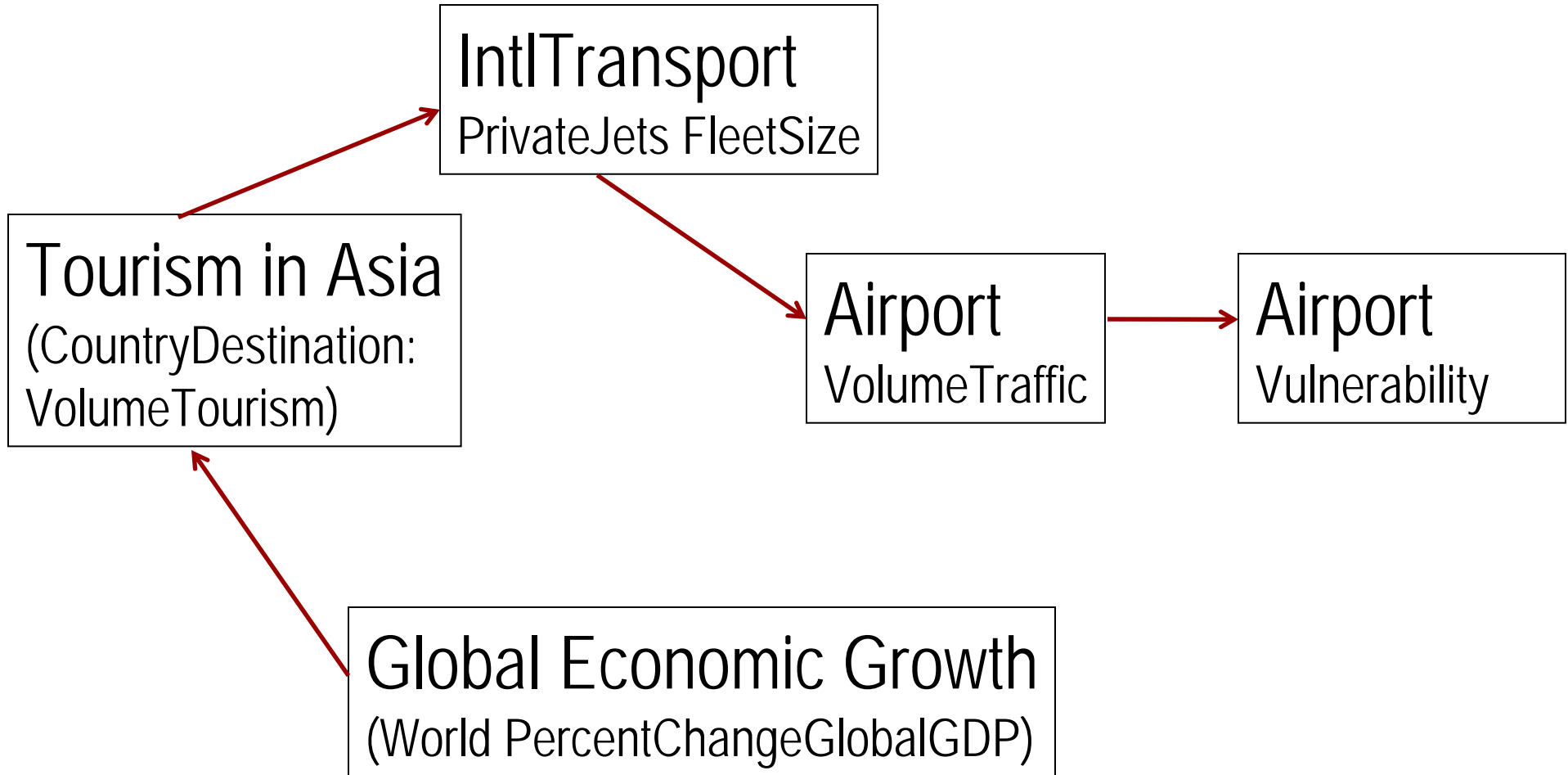
- Airports
- EffectivenessAttackInterdiction
  - Passenger Volume
  - Cargo Volume
  - LinksToHostileAirports
  - Relative Weights

SecurityMeasures  
impact these factors

Model generalizes to other Transport Modes & potential target locations



# Example: Environmental Dynamics



# Illustrative Counter-Terror Strategies

## 1. vs. Attack Threats

- 1. Security Training Program for aircraft crew**
  - Reduce vulnerability to emplaced attack on aircraft
- 2. Passenger Scanning Program for airport**
  - Reduce vulnerability to emplaced attack on airport
- 3. Procurement Program to develop EMS capability**
  - Reduce consequence of (and kind of) attack on airport
- 4. Combine Measures 1, 2, and 3**

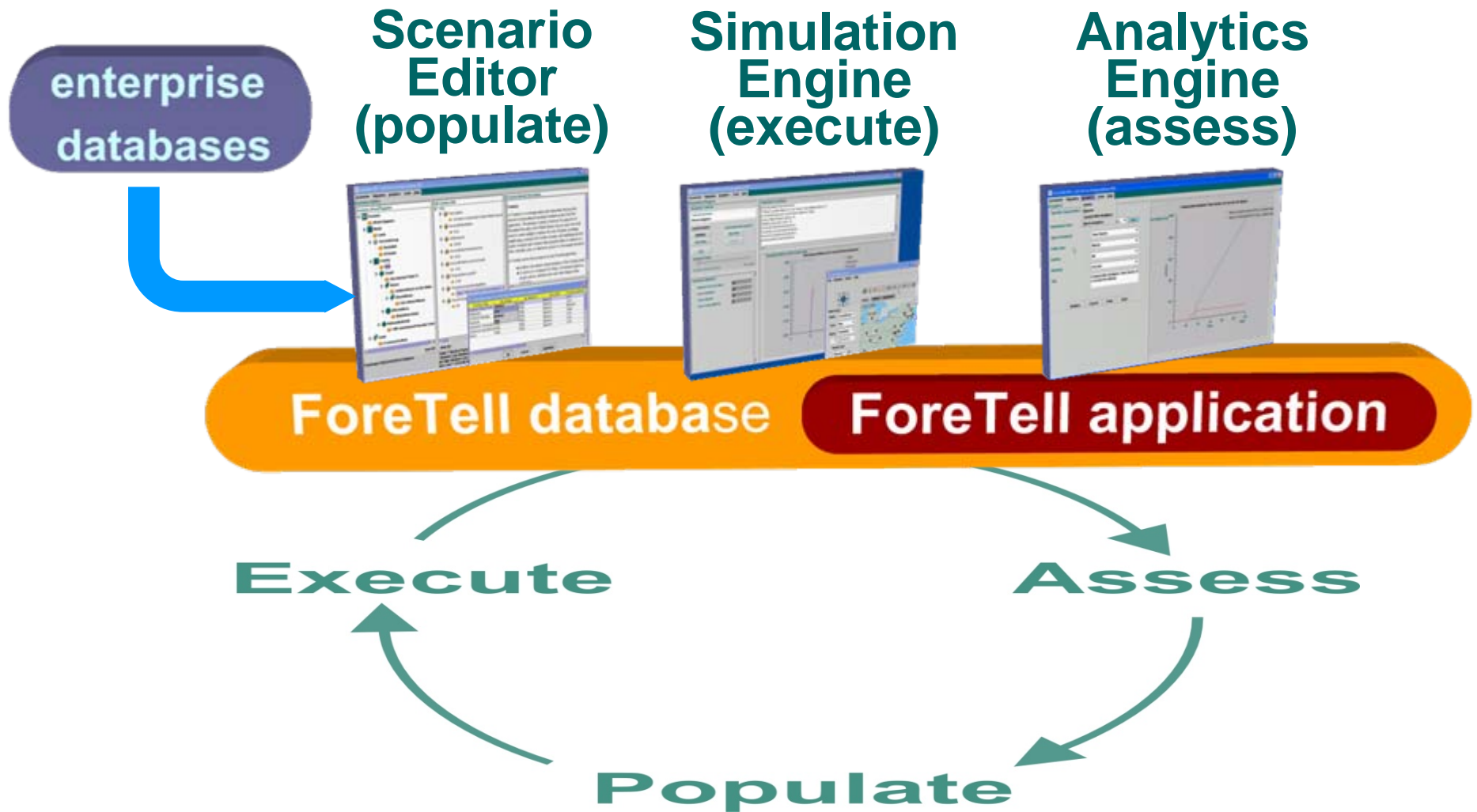
## 2. vs. Transfer Threats

- 1. Transportation Worker Identity Credential (TWIC) program**
  - Improve security by controlling individual access to ports & vessels
- 2. Overseas Port Security Program**
  - Coordinate with & certify security practices of foreign ports & authorities
- 3. Intl Maritime Org. (IMO) Shipper Security program**
  - Coordinate with & certify security practices of owner/operators of vessels
- 4. Combine Measures 1, 2, and 3**



# ***TRANSEC Demonstration...***

# ForeTell DSS Architecture



# Summary of Benefits

- ForeTell provides model-simulate-analyze platform
  - Virtual environment for low-risk decision “test-drives”
  - Lifecycle utility: point of decision thru execution
    - Decision audit trail drives continuous improvement
- TRANSEC: strategic analysis of transportation security
  - Covers terrorist transfer and direct attack threats
  - Leverages existing risk analysis methods, software, data (e.g. MSRAM), open source intelligence, expert analyst judgments
  - Generalizes to other Homeland Security decision areas
- Adaptive, portfolio management approach to security strategy
  - Cost-benefit impact analysis
  - Scenarios reflect dynamic risk landscape, realities of program dev.
  - Reduce risk & improve confidence & consistency in key decisions

