Georgia Tech Tennenbaum Institute

Securing Supply Chains from Counterfeiting Threats in a Transformed Open and Collaborative Enterprise

Doug Bodner

This material is based upon work supported in part by the U.S. Department of Defense through the Systems Engineering Research Center (SERC) under Contract HQ0034-13-D-0004. SERC is a federally funded University Affiliated Research Center managed by Stevens Institute of Technology. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the United States Department of Defense.

Counterfeiting Problem

- Global trend drivers
  - Globalization
  - Electronics proliferation
  - System/product complexity
  - Long deployment & obsolescence
- Supply chain drivers
  - Multi-tiered network
  - Limited visibility
  - Extended enterprise

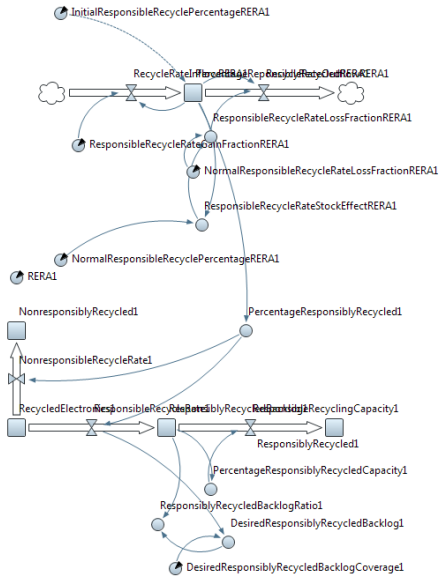
Why Is This an Enterprise Problem?

- No locus of control
  - Multiple agency/industry stakeholders
  - DoD can promulgate policy, but must be cognizant of reaction from industry base
  - Programs have methods of addressing counterfeits
  - Customs & Border Patrol, Dept of Justice and Congress play roles
- Adaptive behavior
  - Counterfeiters adapt to new technology and new policies
  - Policy-makers must adapt
- Complexity
  - Socio-technical (human behavior and social behavior interacting with technical system)
  - Multiple systems interacting with unpredictable effects

Enterprise Simulation Model

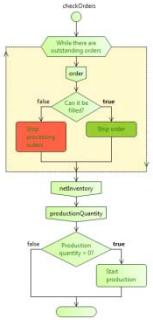
Exogenous Model

Recycling market
Obsolescence rates

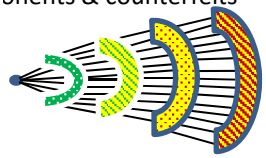


Enterprise Actor, Supply Chain Operations, and Systems & Constituents Models

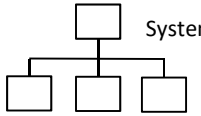
Suppliers & supply network
Counterfeiters

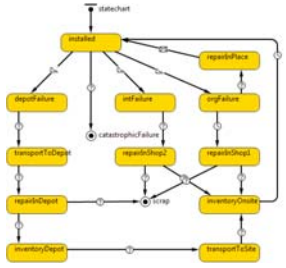


onents & counterfeits



System





Policy Model

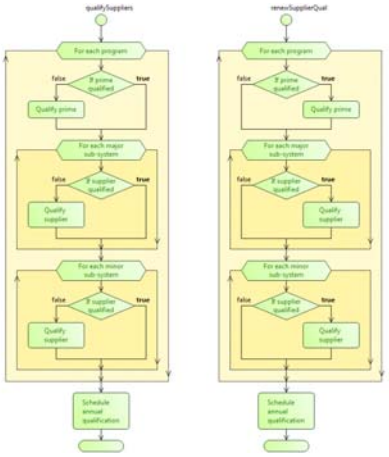
DoD
- Policy (supplier qualification)

DoD programs
- Acquisition/sustainment design & management

DoJ
- IP enforcement

Customs
- Inspection

Legislation

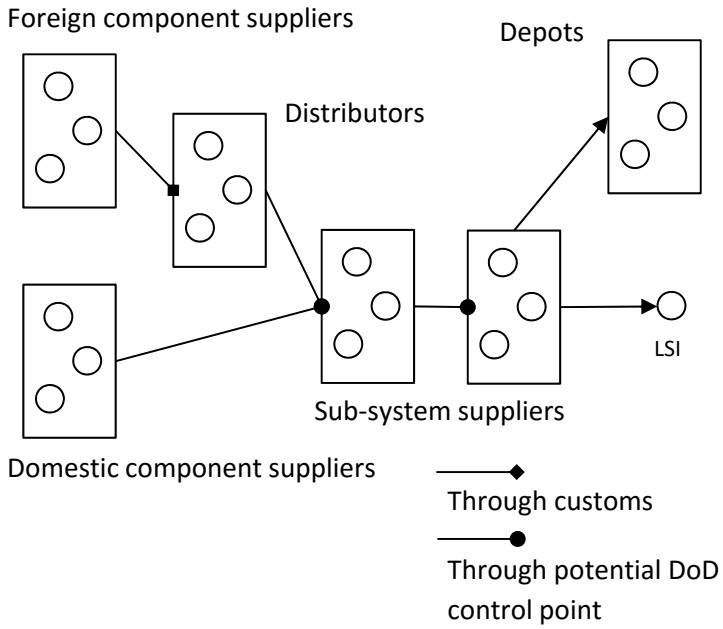


Implementation Platform

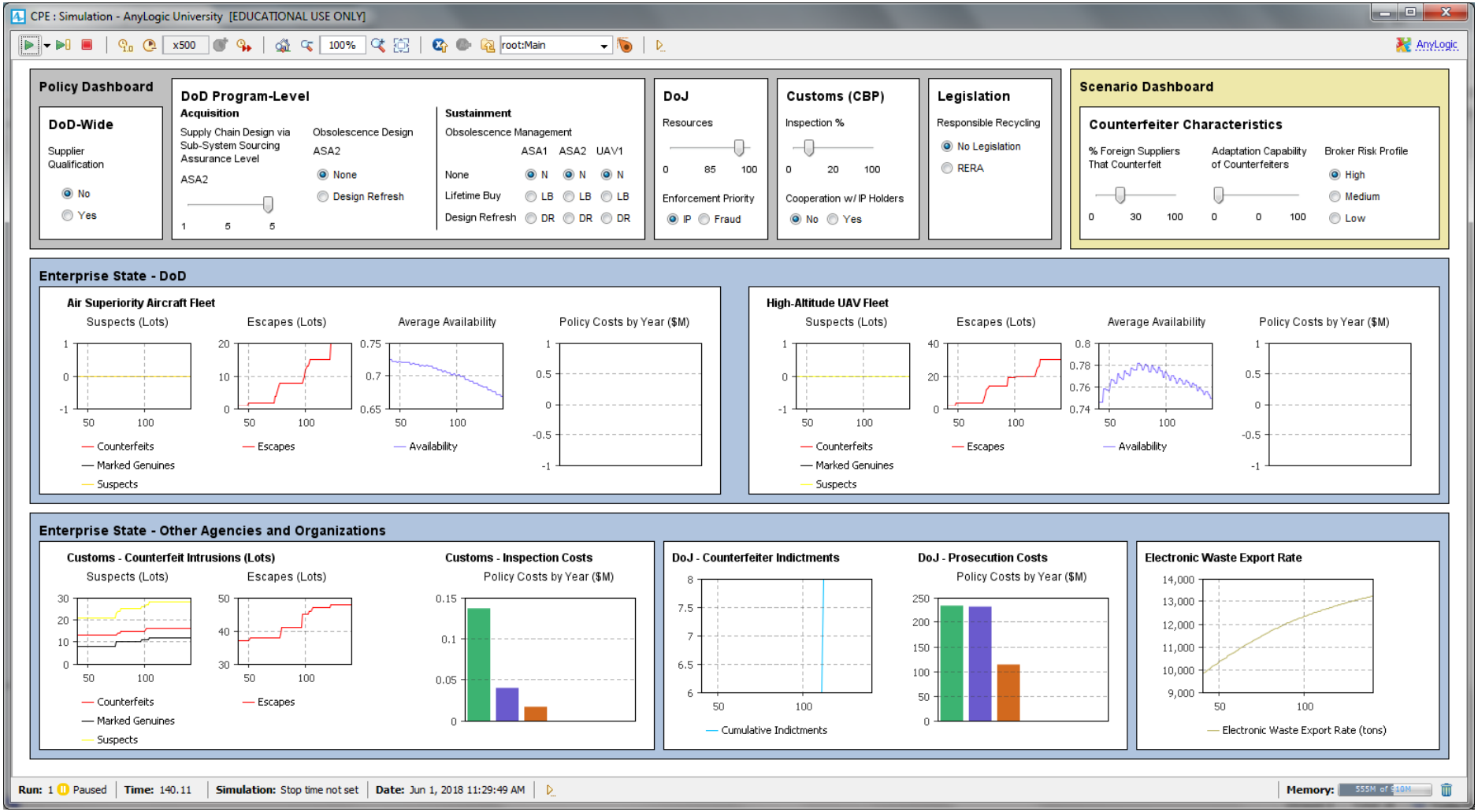
- AnyLogic 7 simulation software
- Supports discrete-event, agent-based and system dynamics simulation
  - Useful for potential model composition
- Provides API for Java class extensions
  - Useful for development of reusable model component libraries
- Model implemented primarily as an agent-based model
  - Complex agents for enterprise actors and policy actors
  - Simple agents for systems and components
  - System dynamics for external influence factors
  - Advantage: Reasonably well-suited suited to handle multi-scale enterprise modeling and organizational decision-making
  - Disadvantage: Too many agents could require excess computational resources

Model Description

- Two programs
  - Fighter jet
  - UAV
- Four tiers in supply chain
- OEMs, franchisee and brokers
- Inspection points
- Depots that perform repairs and replacements



Model Dashboard



Policy Analysis Supported

- Supplier qualification with criticality levels (DoD level)
- Acquisition
  - Supply chain design via sourcing
  - Design refresh planning (not implemented fully)
- Obsolescence management in sustainment
  - Design refresh
  - Lifetime buy
- Customs policies
  - Inspections frequency
  - Cooperation with IP holders
- DoJ policies
  - Resources
  - Priorities
- Electronic waste export legislation

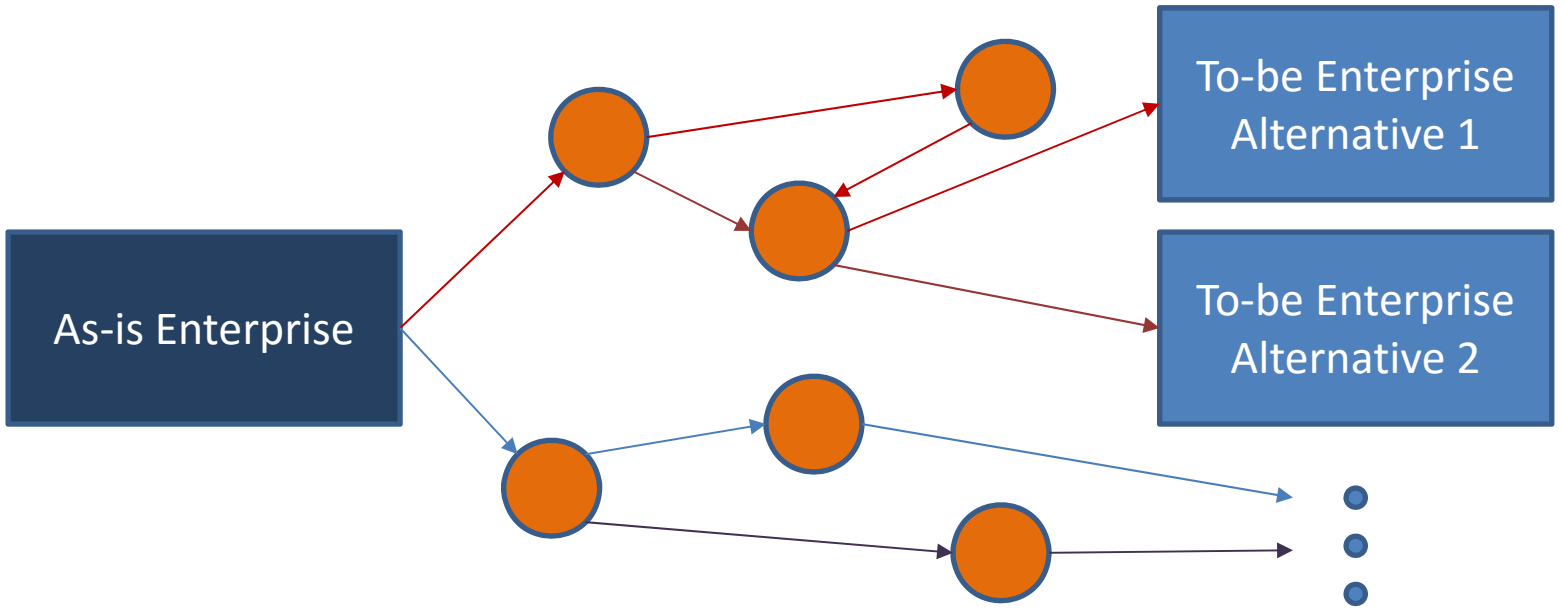
Example Analysis

- Scenario 1 – Baseline scenario
  - No supplier qualification
  - No obsolescence management
  - Customs inspects 20% of incoming
  - Baseline DoJ enforcement resources
- Scenario 2 – Baseline scenario plus supplier qualification for all sub-systems
- Scenario 3 – Baseline scenario plus increased resources for prosecution (50%)
- Scenario 4 – Scenarios 2 and 3 combined

Example Results

Model outputs	Scenario 1	Scenario 2	Scenario 3	Scenario 4
Escapes – fighter jet program (lots)	56.3	13.8	53.8	12.1
Suspects – fighter jet program (lots)	0	72.3	0	70.3
Policy cost – fighter jet program ($M)	0	30.4	0	30.7
Escapes – UAV program (lots)	51.7	11.6	48.9	11.4
Suspects – UAV program (lots)	0	69.7	0	65.2
Policy cost – UAV program ($M)	0	31.9	0	32.5
Escapes – Customs (lots)	640.2	636.0	635.2	632.1
Suspects – Customs (lots)	595.3	608.7	598.8	580.5
Policy cost – Customs ($M)	56.1	55.7	57.9	57.1
Indictments – DoJ	0	0	65.4	66.5
Policy cost – DoJ ($M)	0	0	53.6	52.1

Transformation to Physical Internet



Transformation Framework

Transformation Elements

Transformation Element	Related PI Principle	Likely Effect on Counterfeits
Standardized tamper-proof packaging for part environment control	World standard smart modular containers; smart networked containers	Ensure sensitive parts kept in controlled environments
Supplier reliability ratings	Open performance monitoring	Reduce bad actors in supply chain
Lifecycle tracking of parts	Smart networked containers	Reduce counterfeit instances/intrusions
Supplier visibility through tiers	Open global supply web	Reduce bad actors in supply chain
Modular open systems and use of commercial technology	Open global supply web	Reduce counterfeit instances/intrusions via additional non-risky sources of supply
Expanded trusted foundry capabilities	Open global supply web; business model innovation; digitally transmitting knowledge and materializing objects	Increase sources of reliable obsolete components

PI Model Elements

- Systems & constituents
  - Lifecycle tracking log
  - Smart containers with self-documentation
  - Open system architecture
- Supply chain
  - Reliability ratings for facilities
  - Updating function for component and sub-system histories
  - Expanded use of commercial parts
- Enterprise actors
  - Supplier reliability ratings
  - Use of reliability ratings in sourcing decisions
  - Expanded trusted foundry
- Transformation agent

Future Work

- Identify case study with dataset
- Enhance interface
  - Alerts
  - Supply chain visualization
- Model enhancements
  - Penalties for counterfeit pass-throughs
  - Supply chain reconfiguration by counterfeiters