Multi-Level Modeling of Socio-Technical Systems – Volume 2

Technical Report SERC-2013-TR-020-3

December 2, 2013

Principal Investigator: Dr. William B. Rouse, Stevens Institute of Technology

Co-Principal Investigator: Dr. Douglas Bodner, Georgia Institute of Technology

Team Members:

Dr. José E. Ramirez-Marquez

Pallavi Prasad,

Vishakha Sharma,

Adriana Compnoni

Contract Number: H98230-08-D-0171 Task Order: 0029, RT 044a

Report No. SERC-2013-TR-020-3 Volume 2

The Systems Engineering Research Center (SERC) is a federally funded University Affiliated Research Center managed by Stevens Institute of Technology.

This material is based upon work supported, in whole or in part, by the U.S. Department of Defense through the Office of the Assistant Secretary of Defense for Research and Engineering (ASD(R&E)) under Contract H98230-08-D-0171 (Task Order 0029, RT 044a).

Abstract

SERC-2013-TR-020-3, Volume I discussed the initial development of a methodology for modeling complex socio-technical problems.

SERC-2013-TR-020-3, Volume II is the companion report that discusses an in-depth case study of the occurrence of counterfeit parts in the supply chains for Department of Defense weapon systems. These two reports reflect the balance of this research between more theoretical developments and in-depth case studies.

Table of Contents

Figures and Tables

1. INTRODUCTION

Increasingly, the Department of Defense (DoD) is concerned about the problem and potential consequences of counterfeit parts in its supply chain. Counterfeit parts have different performance and failure characteristics than genuine parts and can result in degraded system availability, reliability and performance in the field, not to mention critical safety issues. Thus, there is an imperative to understand counterfeiting and potential ways in which it can be prevented or contained.

Counterfeiting certainly is not a new phenomenon. However, counterfeiting has taken on new characteristics in this age of complex electro-mechanical platforms and systems, and these new characteristics make it a substantially different problem than the traditional counterfeiting of currency or consumer products.

Today's DoD platforms and systems are composed of multitudes of constituent elements. At the first level of breakdown, they consist of major sub-systems, which in turn consist of other sub-systems, which consist of components, and so on. The counterfeiting problem has become not that the end-product is a counterfeit, but rather that some of its constituent elements may be counterfeit. Given the wide array of part types for a particular system, this raises the question of how to detect counterfeit parts and prevent them from being installed in a system, or to detect counterfeits already installed.

These constituent elements typically come from a variety of suppliers in a many-tiered supply network. A component may originally come from one supplier and pass through several others as it is installed in a sub-system, which is in turn installed in a major sub-system, and finally in an end-product system. Thus, identifying the source of counterfeits to prevent future counterfeit occurrences is not trivial. This is compounded by the globalization of the DoD supply chain, especially in the area of electronic parts.

Finally, DoD systems increasingly are kept in use for decades, often past their expected lifetime. Most systems consist of constituent parts specifically designed for that system or platform, and the number of such systems may only be in the hundreds. Thus, the defense supply base tends to be smaller and more specialized than the commercial supply base. It is also susceptible to supplier diminishment, whereby the original manufacturers (OEMs) of a component or sub-system exit the market, necessitating procurement of replacement parts for deployed systems from other sources. Finding these sources can be difficult.

Even though the foregoing primarily addresses the technical aspects of the counterfeiting problem, it is clear that socio-behavioral aspects come into play. These include social, economic and cultural phenomena. Systems are composed of increasing numbers of constituent elements to meet new threats and requirements, not only technical threats and requirements from adversarial systems, but also social and behavioral threats and imperatives, such as terrorism and the desire to use unmanned systems rather than put personnel in harm's way. As more complex functionality is required, the number of specialized components and

sub-systems increases, and the number of suppliers and complexity of the supply chain grows. Thus, socio-behavioral aspects of the environment are in many ways driving technical aspects of the counterfeiting problem.

Looking from a supplier's perspective, there are strong economic influences at work that affect the counterfeiting problem. A responsible supplier experiences risk from its own suppliers in that they may provide parts with counterfeit elements, and that passing on counterfeit elements exposes the supplier to potential sanctions. This disincentivizes suppliers from participating in DoD work, and thus may result in an increased number of irresponsible suppliers or increased cost of parts.

Finally, from the counterfeiter's perspective, there are two main motivations – economic profit and strategic advantage. The former is used by those who would pass fraudulent goods in pursuit of monetary gain, while the latter is used by those who would pass intentionally designed defective goods to degrade U.S. capabilities. Counterfeiters have the ability to adapt to new circumstances, such as policies or procedures designed to detect or prevent counterfeit parts, with new methods to pass counterfeits onto their targets. Thus, those who would combat counterfeiting must adapt, as well. Such adaptive behavior is a hallmark of socio-technical systems.

Clearly, counterfeiting can be defined as a socio-technical problem with aspects of different disciplines:

- Systems engineering for system design & development, system sustainment, configuration management and reliability modeling;
- Industrial engineering for supply chain modeling and design;
- Economics for modeling actor motivations and responses to information, incentives and risk;
- Organizational behavior for modeling group dynamics, and
- Sociology for modeling cultural and societal phenomena.

Each of these disciplines studies and models a different aspect of the overall problem. These models allows us to understand different phenomena, conduct experiments, determine which solutions work best under which circumstances, discard bad options, identify unintended or counter-intuitive consequences, and perform what-if analysis on new scenarios. However, models within each discipline typically use formalisms that have assumptions, data requirements and outputs unique to a particular discipline, with the result that incompatibilities between disciplines arise. In studying and modeling socio-technical systems, it is critically important to be able to use these types of models in a coherent fashion, to understand the overall system. However, in practice it is a major challenge to combine such models developed for different purposes.

This report addresses a case study involving the modeling and analysis of the counterfeit parts problem in the DoD supply chain as a socio-technical system. A companion report (Rouse & Pennock, 2013) proposes a methodology for such modeling that facilitates coupling or

combining models from different disciplines in pursuit of studying a complex socio-technical problem. The overall approach in these reports is to use a bottom-up case study approach in conjunction with a top-down methodological approach to refine and advance an overall methodology for studying complex socio-technical systems. As such, these two reports represent the initial steps in this refinement and advancement.

The remainder of this report is organized as follows. Section 2 describes the evolution of the problem of counterfeit parts in the DoD supply chain, concerns and responses from DoD, and potential future developments. In Section 3, the modeling methodology proposed by Rouse and Pennock (2013) is applied in summary form to the problem of counterfeit parts. Section 4 specifies various sub-models used to address the overall counterfeit parts problem. The composition framework is discussed in Section 5. Section 6 describes methodological support to be provided by the model. Section 7 concludes the report.

2. The Problem of Counterfeit Parts in the DOD Supply Chain

In recent years, the Department of Defense has grown concerned about the issue of counterfeit parts infiltrating its systems from various sources in its supply chain. DoD has taken a number of steps to address this emerging problem, mostly in the form of policies and guidance. However, the problem is not yet fully understood, and additional counter-measures are likely to be needed to contain the problem. Thus, models are needed to can provide recommendations for effective counter-measures.

Concern centers around two types of counterfeiting – fraudulent counterfeits and malicious counterfeits. Fraudulent counterfeits derive from the traditional motivation of a counterfeiter to make a profit through fraud, by substituting an inferior product that is inexpensively produced relative to the cost of the genuine article. These types of counterfeits fall into several categories. First are parts that are re-marked to appear that they are original equipment manufacturer (OEM) parts. Second are defective parts that are passed as good OEM parts. Third are parts that are removed from scrapped assemblies and passed as new. Malicious counterfeits are designed to appear to perform correctly, but then malfunction at critical times or open security breaches so that adversaries gain advantage.

Concerns about counterfeit parts, in particular electronics, have been aired for almost a decade (McFadden & Arnold, 2010; Pecht & Tiku, 2006; Stradley & Karraker, 2006; Villasenor & Tehranipoor, 2013). There have been a number of studies pointing to the potential consequences of counterfeit parts infiltrating DoD systems (ABA, 2012; AIA, 2011; Dept. of Commerce, 2012; GAO, 2010; GAO, 2011; GAO, 2012a; Senate Armed Services Committee, 2012). Also, there have been published reports on the risks that other countries, most notably China, may engage in malicious counterfeits (Business Insider, 2012; Economist, 2012).

While much of the concern is speculative, especially as relates to malicious counterfeits by adversaries, there are a number of documented instances of counterfeit parts.

- Fraudulent parts from China were found in a number of aircraft, including the C-130 (Capaccio, 2011).
- The Government Accountability Office (GAO) conducted an investigation in 2012 and found sixteen instances of suspect counterfeit parts available on internet purchasing platforms used by DoD (GAO 2012b). These parts fall into three categories requested by GAO – authentic part numbers for obsolete parts, authentic part numbers for post-production parts, and non-existent (i.e., bogus) part numbers.
- Fraudulent testing was discovered in engines made by a major manufacturer and defense contractor (Pasztor, 2013).
- Numerous incidents of re-marked components and scrapped components that were defective, but passed as genuine, are reported in the GIDEP (Government-Industry Data Exchange Program) database, which is the official reporting site for defense suppliers to report incidents of counterfeit detection (Livingston, 2007b).

The potential of counterfeit parts to cause serious problems in DoD systems has a number of drivers:

- Increased system complexity;
- Globalization of commerce and supply chains, especially in semiconductors and electronic;
- Globalization of DoD programs causing inducements to use foreign suppliers;
- Outsourcing of design and manufacturing of major sub-systems by primes;
- Extended lifespan of systems and diminishment of OEMs providing replacement parts over the lifecycle horizon;
- Weak IP protection outside of U.S.;
- Increasing sophistication of design and manufacturing technology used by counterfeiters;
- Use of internet as a purchasing platform;
- State “ownership” (i.e., influence or control) of potential foreign suppliers; and
- Decreased cost of counterfeits vs. genuines (e.g., movement toward environmentally-friendly electronics that are more expensive to produce).

DoD has developed a number of policies and guidelines aimed at addressing the counterfeit parts problem. It should be noted that these are beginning efforts, and due to their recent adoption, it is not known how successful they are or will be.

- DFARS Case 2012-D055 (DFARS, 2013).
- Defense Acquisition Guidebook Sec. 4.4.18.3 – Anti-Counterfeiting (DAU, 2013).
- DoD Instruction 4140.67 – DoD Counterfeit Prevention Policy (DoD, 2013).
- National Defense Authorization Act (NDAA) for FY 2012 (Congress, 2011).
- DoD Instruction 4140.01 – DoD Supply Chain Materiel Management Policy (DoD, 2011).
- DoD Instruction 5200.44 – Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN) (DoD, 2012).
- USD(AT&L) Memo – Overarching DoD Counterfeit Prevention Guidance (Kendall, 2012).

These policies address such things as definitions of counterfeiting, applicability of policies to classes of suppliers, guidelines for program management, and sanctions against sources that supply counterfeit parts or sub-systems (or systems) with counterfeit parts. A number of concerns have been raised in public comments, among them:

- What is the precise definition of counterfeit?
- What is the scope of applicability to contractors?
- What is the risk to suppliers, and how will this affect their willingness to do DoD business?
- What are limits on liability (especially at system level)?
- What is the prime contractor's liability as systems and sub-systems face obsolescence and end-of-production as circumstances over which the prime has little control?
- There is a conflict between low price contracts (existing practice) vs. high assurance (new requirement) vs. system availability and support effectiveness/efficiency (desired goal).
- Are commercial and COTS items excluded from coverage?
- What is the precise definition of risk-based detection and avoidance of counterfeit parts?

These are socio-technical in nature, and many relate to the risks faced by honest suppliers and how they will react to those risks. Included in the existing policy set, as well as with proposed additions the following counter-measures are potentially available.

- Acquisition
    - Use of trusted suppliers
    - Program Protection Plan
    - Criticality analysis
    - Software assurance
    - Robust system design (system can still function with counterfeit components, graceful degradation)
    - Trusted system design (system detects/disallows counterfeits)
- Sustainment
    - Use of trusted suppliers
    - Subsidy of OEMs
    - Supply chain monitoring (prevent, detect, respond)
    - Incentives to primes and secondaries to monitor
    - Reporting and information-sharing (GIDEP/PRDEP)
    - Traceability of components
    - Penalties for counterfeiting (or allowing counterfeits to be passed in sub-systems or overall systems)
    - Intelligence

Since these have costs and interaction effects, the question is where to invest effort and funds so as to minimize the risk of adverse effects from counterfeit parts.

3. SUMMARY APPLICATION OF SOCIO-TECHNICAL MODELING METHODOLOGY

This section summarizes the application of the socio-technical modeling methodology proposed by Rouse and Pennock (2013) to studying the problem of counterfeit parts in the DoD supply chain. The primary focus at this stage of research is steps 1 through 7.

Step 1: Decide on the Central Questions of Interest

The key question of interest here is to specify and test the effectiveness of policies to minimize adverse effects of counterfeit parts in DoD operational systems. This involves multiple questions at a lower level of detail, such as how to disincentivize counterfeiters at the outset; whether resources should be invested in system design to prevent adverse effects from counterfeit parts at the point of installation or usage, or in sustainment to prevent counterfeits from reaching installation; which constituent elements of a system should be targeted for counterfeiting counter-measures; what are the appropriate trade-offs between counterfeiting counter-measures and costs; and how supplier governance should incorporate anti-counterfeiting measures.

Step 2: Define Key Phenomena Underlying These Questions

The types of phenomena underlying the questions of interest are summarized below:

- Systems
  - Work breakdown structures (major sub-systems, minor sub-systems, components, etc.)
  - Vulnerabilities of system designs to counterfeiting
  - Mission profiles for deployed systems
  - System performance criteria (KPP/TPM performance, availability, lifecycle cost, reliability and security)
  - Nominal system performance vs. counterfeit-induced performance
  - Technology upgrade policies and schedules
  - Configuration management
  - System characteristics over lifecycle
  - Counterfeit parts
- Supply chains
  - Globalized nature of DoD supply chain
  - Programs and supplier networks
  - Supplier governance models
  - Evolution of suppliers and part flows over program lifecycle
  - Supplier risk and incentive behavior
  - Supplier diminishment
  - Counterfeit detection protocols and capabilities
- Counterfeiters

  - Counterfeiter motivations and capabilities
  - Counterfeiter risk and incentive behavior
  - Counterfeiter adaptation
- Policy-makers
  - Policies
  - Ability to have policies enforced
- Exogenous world
  - Technological progress over program lifecycle
  - Technology off-shoring
  - Threat profiles

Step 3: Develop One or More Visualizations of Relationships among Phenomena

Previous work (Rouse & Bodner, 2013) has resulted in a series of systemigrams that provide a useful visualizations of relationships among the various phenomena, as well as a context for the overall problem. Systemigrams are a visualization tool used to illustrate relationships between different elements (Blair et al., 2007). The systemigrams, shown below in Figure 1 through Figure 4, view the problem and its context in four different levels – eco-system, organizational structure, delivery operations, and work practices. This is a useful framework for decomposing large-scale, enterprise modeling problems, although other frameworks can be used.

Figure 1 illustrates the domain eco-system for the counterfeit parts case study. This eco-system consists of the Department of Defense, the U.S. government and relevant security-related agencies, the defense industrial base, the overall economy and tax base that supports defense appropriations, macro-trends that impact current and future defense programs, and policies and laws that govern acquisition, sustainment and counterfeiting.

The industrial base provides platforms, major sub-systems, sub-systems and components for defense systems. The industrial base is influenced by macro-trends such as globalization, outsourcing and off-shoring, joint ventures with foreign governments, and new business models for system design and production. Such trends may expose programs in the ecosystem to counterfeiting risks from sources that have either strategic or economic motivations.

As a program transitions from acquisition to sustainment, its industrial base shifts from design and production to sustainment. Sustainment typically operates as a private-public partnership, as government depots play a substantial role. Such concepts as performance-based logistics come into play, as well, whereby a prime contractor is contracted to provide a certain performance level in terms of metrics such as system availability. Macro-trends in sustainment include increased system life spans and technology advancements. The ecosystem sees aggregate outcomes from counterfeiting in terms of the effect on overall mission.

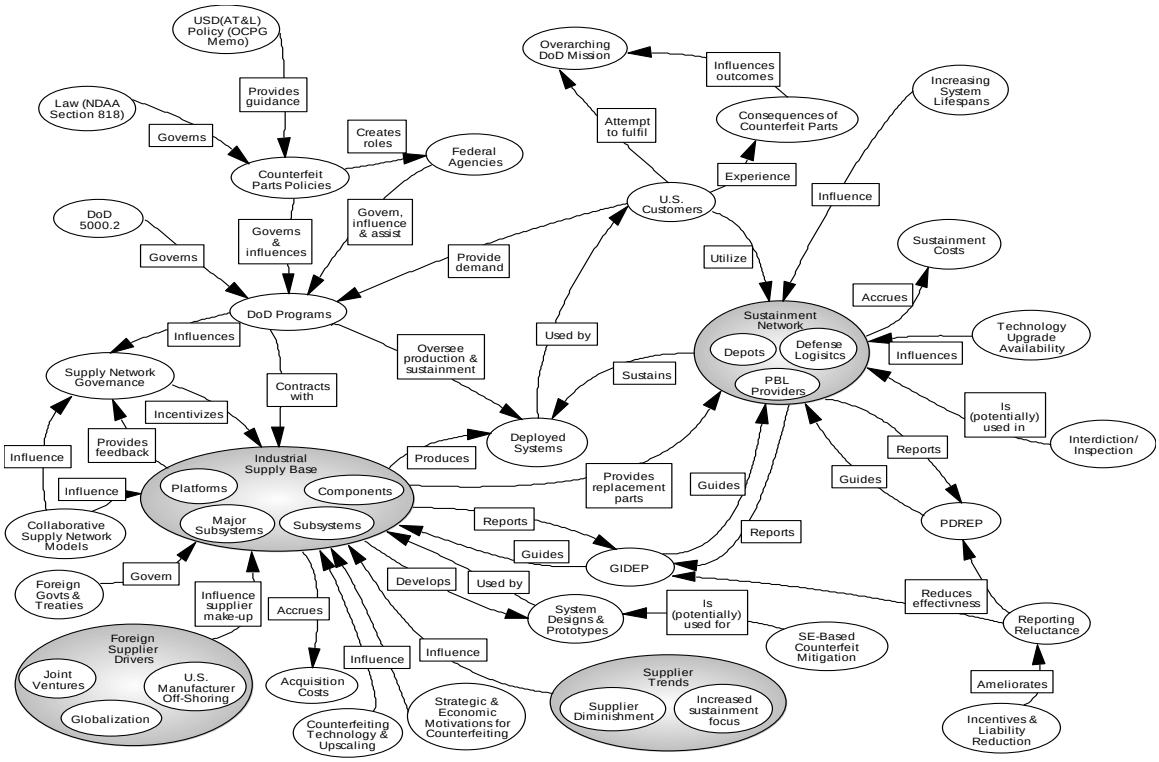

Figure 1. Eco-system for counterfeit parts problem

The system structure, shown in Figure 2, focuses on the various organizations (agencies and firms) that interact with one another in the acquisition and sustainment enterprise. There is typically a networked structure here, with some amount of hierarchy.

Any particular program is overseen by DoD's Acquisition, Technology & Logistics office. The industrial base provides suppliers, plus the prime contractor, for a program. A program's supply chain typically is organized as a set of tiers consisting of hundreds or even thousands of suppliers. A supplier in the second tier, for example, provides parts to suppliers in the first tier. This tiered organization is not necessarily hierarchical, as a particular firm may be in more than one tier. In addition, a firm may be in multiple programs and may collaborate with another firm in one program and compete with the same firm for another program's contract.

As a program moves from acquisition to sustainment, many of its suppliers will continue to supply replacement parts for use at different sustainment facilities. However, other firms from the industrial base will be added to the program as the original suppliers may elect not to continue, or not be able to continue. Contractors are supposed to report counterfeit incidents to GIDEP, which is accessible by other firms for supplier monitoring. Likewise, government agencies are supposed to report such incidents to PDREP (Product Data Reporting and Evaluation Program).

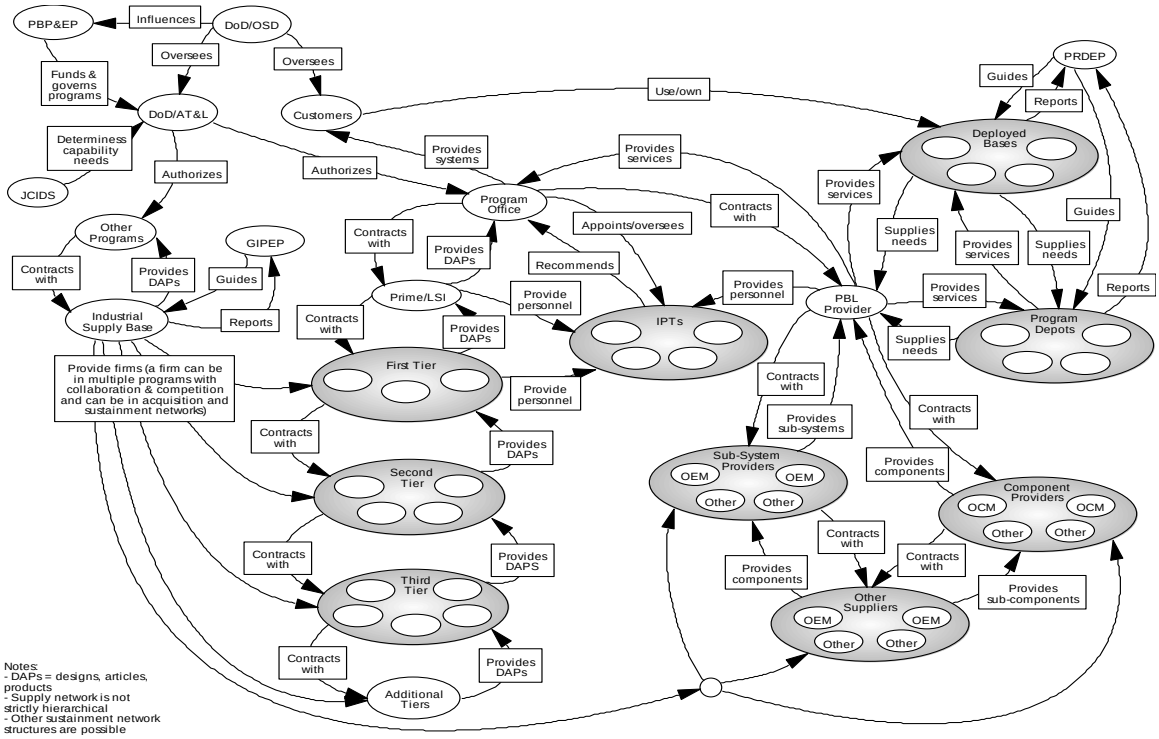

Figure 2. System structure for counterfeit parts problem

The delivery operations level focuses on the various processes and facilities at which they are performed (Figure 3). The supply network is cast as a series of facilities that engage in design collaboration between the prime and sub-contractors, part flows that eventually result in major sub-systems being integrated in final assembly and finally cost accruals. These activities take place in the context of acquisition phases as spelled out in DoD 5000.2. Designs and articles pass from one acquisition phase to another as the acquisition matures. The program office oversees this set of processes and communicates and enforces various regulations, including counterfeiting counter-measures.

Systems are delivered to deployed bases from the production processes and facilities. Field maintenance and repair is done at these facilities, while systems are sent to depots or contractor maintenance and repair facilities for depot-level work. Parts for maintenance and repair are held in inventories. Inspection procedures may be used there.

While the figure does not show it explicitly, it should be understood that the supply network facilities evolve over time, with new ones being added and current ones falling out of the network, as a program moves from acquisition and production to sustainment. It is here that the phenomenon of diminishing supply takes hold.

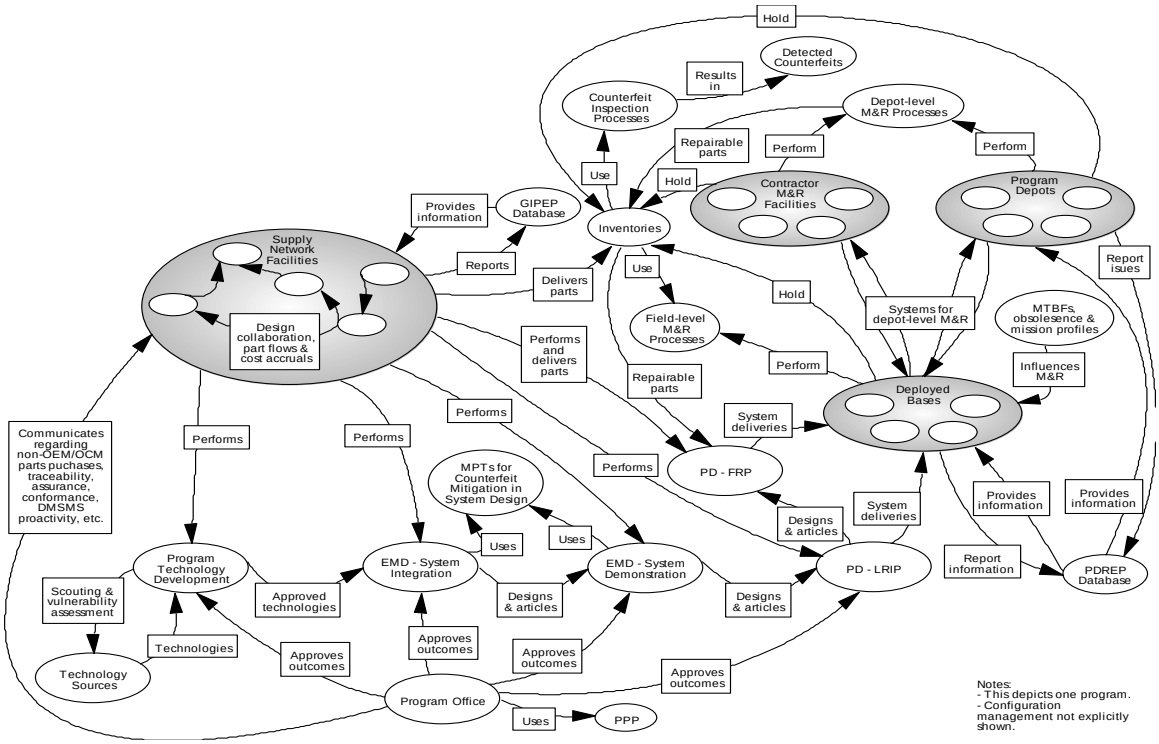

Figure 3. Delivery operations for counterfeit parts problem

The work practices model consists of the individual people in the acquisition and sustainment enterprise, as well as the work that they perform and how they interact with one another. The emphasis is on acquisition and sustainment professionals in a program setting, as shown in Figure 4. A program manager oversees the program and has a variety of government professionals reporting to him or her in functional roles.

For instance, a chief systems engineer would report to the program manager. The chief systems engineer may have other engineers reporting to him or her. The government systems engineers would then provide oversight for the systems engineers of the prime contractor to ensure that the government's interests are represented. Typically, the systems engineers of the contractor(s) provide most of the work for system design and development. However, different philosophies of division of labor between government and contractor may come into play over time. Thus, the model should provide flexibility in this regard. The systems engineers of the prime contractor then provide oversight for the systems engineers of each sub-contractor. Usually, the government systems engineers do not have direct oversight or contact with those of the sub-contractor unless it is through the prime.

Similarly, there is government oversight of the prime workforce in the other functional areas, with the prime then providing oversight of the functional areas of the various sub-contractors. The workforce performs tasks as governed by DoD 5000.2 related to design, development, testing, maintenance, repair, etc. To address specific issues that overlap functions, workforce

members participate in integrated product teams (IPTs). There are likely specific counterfeiting counter-measures done at the individual level (e.g., adherence to guidelines or testing regimens) called out explicitly.

The overall workforce is affected by several phenomena such as training (skills and skill levels), social networks (cooperation among individuals), collaboration (cooperation between functions) and trust. Social networks can be shown in much more detail as relationships between individuals within a program, whereas trust tends to be more of a field effect.

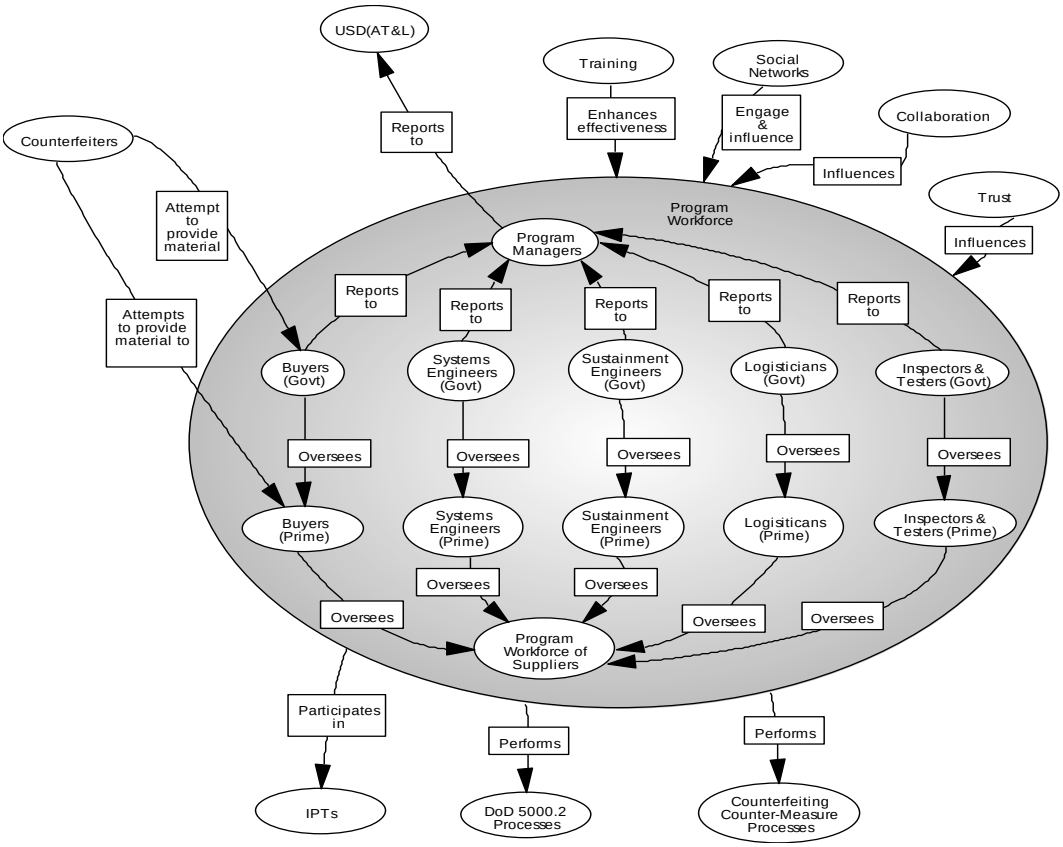

Figure 4. Work practices for counterfeit parts problem

Each level has relationships with the other levels, as shown in Figure 5. For instance, the ecosystem provides the incentive structure (e.g., contract types, penalties for counterfeiting, available funding) and policies downward, while it receives performance information (cost, mission effects) from below. Figure 5 also shows the typical relationships between elements within each level on the left side of the figure.

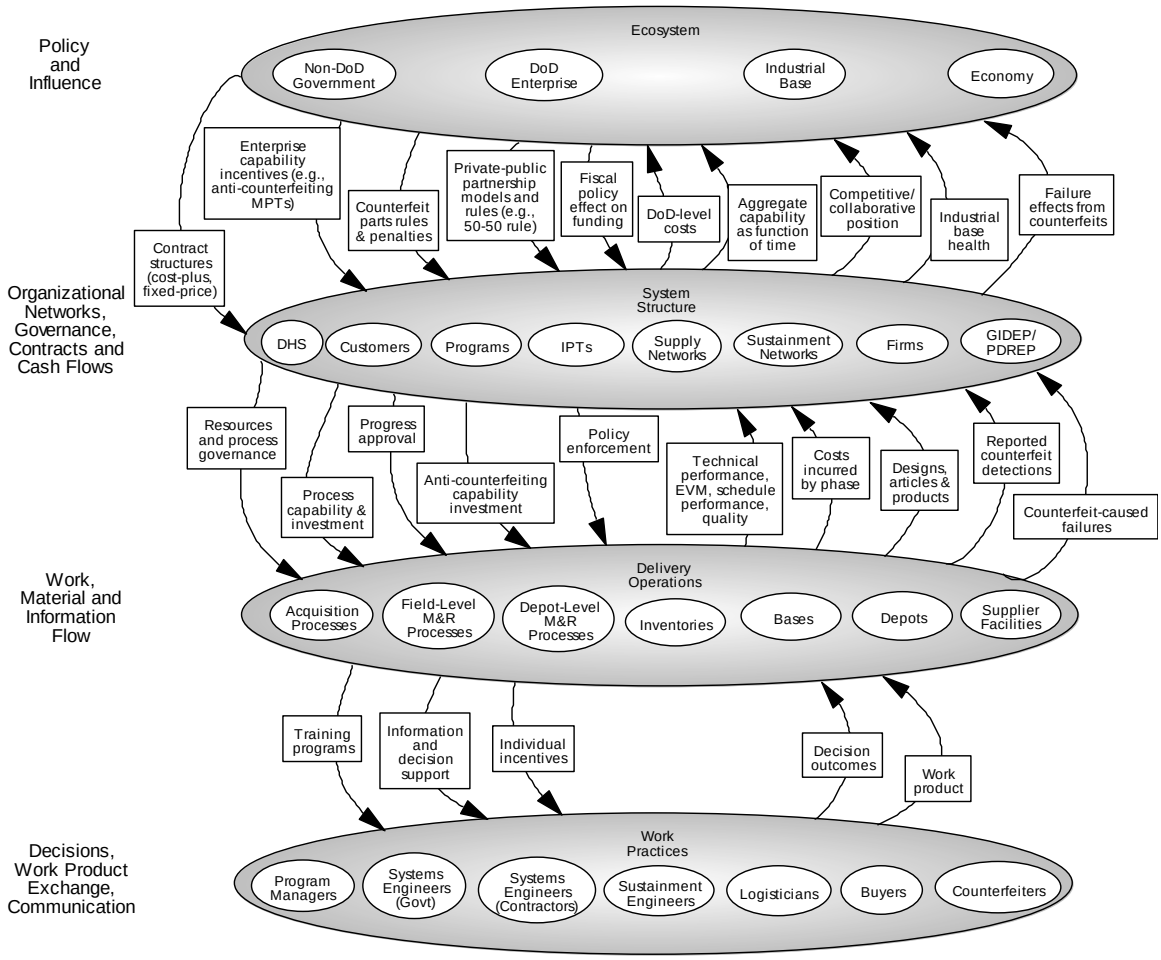

Figure 5. Interactions between different system models

Step 4: Determine Key Tradeoffs That Appear to Warrant Deeper Exploration

Step 1 identified several key trade-offs that result from the central question of interest. Here, we elaborate and expand on these trade-offs. Additional trade-offs are depicted in the visualizations of Step 3. Here, the trade-offs are provided in more detail.

- Should investments be directed to system design and development, to make systems less vulnerable to adverse effects of counterfeiting, or to supply chain management, to prevent or minimize counterfeits from being installed in operational systems?
- In developing tracking methods for parts in the supply chain, what is the trade-off between cost and effectiveness of these methods in minimizing negative effects of counterfeiting?
- In targeting critical sub-systems for counterfeiting counter-measures, what is the trade-off between the scope of the definition of critical sub-systems (i.e., wide versus narrow) and the resources needed to address that scope and performance impacts caused by

that scope? For instance, a wide scope helps ensure that counterfeit parts in many/most sub-systems have likelihood of being detected or prevented. On the other hand, the more sub-systems are defined as critical, the more effort and cost are needed to monitor them, and fewer suppliers may be available.

- What is the trade-off between limiting foreign and/or non-trusted suppliers and the availability and cost of replacement parts in a restricted market?
- What is the trade-off between the scope of liability and penalties for counterfeiting (including allowing pass-through counterfeits in sub-systems and systems) versus supplier availability across the program lifecycle?
- What is the trade-off between the scope of supply chain inspections for counterfeits versus costs of inspection programs and delays caused by them?

Step 5: Identify Alternative Representations of These Phenomena

The following representations constitute important building blocks of an enterprise model for the counterfeit parts problem.

- Discrete-event, transactional simulation for representing part flows through the supply chain and various processes that they encounter (Law, 2007). Such processes include transport, storage, inspection, assembly into sub-systems, then systems, repair and maintenance, etc.
- State-transition model for components, sub-systems and systems representing different operational states resulting from missions, counterfeit failures, repair, etc.
- Reliability models representing failure and maintenance needs of components, sub-systems and systems under different circumstances (e.g., mission effects, counterfeit presence, etc.).
- Economic behavior of the firm models representing supplier counterfeiter behavior. In particular, a principal-agent model would be useful to represent government-supplier interactions (Kreps, 1990). A first-order representation would be based on rational actors. Adversary modeling (Rothschild et al., 2012) could being incorporated to represent counterfeiter behavior of state-sponsored actors motivated by geo-political advantage.
- Network models representing supplier relationships.
- Policy models representing decisions that constrain or otherwise impact the behavior of other models (e.g., inspection behavior in the supply chain model).
- Exogenous models that impact the behavior of other models (e.g., technological progress that enhances or impedes the ability of counterfeiters to make effective counterfeit parts over time).

Step 6: Assess the Ability to Connect Alternative Representations

Two widely-used modeling formalisms of relevance here are discrete-event simulation (Law, 2007) and agent-based simulation (Holland & Miller, 1991). Discrete-event simulation traditionally has been used to model technical aspects of systems, such as factory or supply

chain behavior. Agent-based simulation has been used in social science to model social behavior. These two modeling formalisms are compatible in that agents from agent-based models can be mapped to entities that traverse through processes in discrete-event models (Bodner & Rouse, 2010; Park et al., 2012). In addition, supplier agents can be linked to facilities and locations in the discrete-event supply chain model, representing ownership. A supplier agent, based on its behavior, may decide to enter or exit the market for a particular sub-system, for instance.

The agent-based approach is useful for modeling state-transition behavior of components, sub-systems and systems. Reliability models naturally fit with the notion of state transitions, as a component for example has a time-to-failure from its reliability that maps to the transition between an operational state and a failed state. Agent-based models also generally provide representations for network structure, such as relationships between suppliers and principal-agent interactions. Finally, micro-economic models can be embedded within agents to represent individual actor decisions and behavior based on global state or interactions with other agent/actors, plus incentive and utility models within the agent/actor.

For now, policy models and exogenous models are likely to be implemented as global variables whose values cause behavior to be realized in other models. For example, a policy dictating use of trusted suppliers only for critical sub-system, coupled with an expansive definition of critical sub-systems, would result in a number of suppliers in the supplier and supply chain models not being used.

While there is composition synergy among the formalisms for the counterfeit parts model, one concern that must be addressed in the overall composition design is the computational load of particular interactions between agent-based representations and discrete-event representations. Clearly, this is critical as the model scales to a full DoD program or multiple programs across their lifecycles.

Step 7: Determine a Consistent Set of Assumptions

The assumptions for the overall model include the following:

- The sub-systems and components to be modeled.
- Missions to be included and their effect on system behavior.
- Types of counterfeit parts to be included and their effect on system performance.
- Availability of information among supplier agents.
- Interplay between government counter-measure against counterfeiting and counterfeiter adaptability based on ingenuity and technological progress.
- Unrealistic boundary conditions without recourse via model support. For example, policy effects and economic incentives may drive the number of suppliers for a critical sub-system to zero, when in the real world, this would typically not be allowed.

Much of the detail in the assumptions is dependent on the data available for use in the model and the level of accuracy that these data can support.

Step 8: Identify Data Sets to Support Parameterization

The following types of data sets have been identified as potentially useful in parameterizing the model.

- GIDEP database of reported counterfeit incidents (frequency, component types, detection method effectiveness, system types and vulnerabilities, counterfeit sources, effects of counterfeits on performance etc.).
- Program data (work breakdown structure, supplier network structure and evolution, baseline system performance, part flows in sustainment network and evolution over program lifecycle; counterfeiting incidents and effects on performance, etc.);
- Subject matter expert opinion on system vulnerabilities, effects of counterfeiting, likely effectiveness of counter-measures (and unintended consequences of counter-measures); and
- Synthetic data based on data structures needed to populate model, with data structure and values validated by subject matter experts.

Step 9: Program and Verify Computational Instantiations

This step is performed first using well-established simulation software. In particular, we are using software that is Java extensible, so that class libraries can be developed for reuse in model extension and development of related models. Verification must address both the correctness of individual sub-model behavior and correctness of composed model behavior and outputs.

Step 10: Validate Model Predictions, at Least against Baseline Data

This step is dependent on the data sources outlined in step 8. Since the counterfeiting problem is fairly new, and effects from counterfeits in DoD systems are not well-known, it is likely validation will consist mostly of comparisons of the model with baseline system/program outcomes and behaviors. Sensitivity analysis will be used to explore different counterfeiting scenarios, along with subject matter expert feedback on the authenticity of the results.

4. SUB-MODEL SPECIFICATIONS

This section discusses the various sub-models being developed for the counterfeit parts case study.

4.1. SYSTEM SUB-MODEL

The system model considered here consists of a number of constituent sub-systems, which in turn consist of components. The term system and product are used interchangeably in this section, as the terms reference a military system such as an aircraft, ship or vehicle, and these systems can also be considered as products. The components are the system elements that may be counterfeit. We assume that a sub-system is not counterfeit.

4.1.1. GENERIC STRUCTURAL AND PERFORMANCE MODEL

Let S_i be a system type considered in the model, where i = 1, 2…, I. An instance of system S_i is styled as S_i^a. S_i is then composed of sub-systems R_{ij}, where j = 1, 2…, J_i. An instance of R_{ij} is styled as R_{ij}^b and is a member of R_{ijg}, where g = 1, 2…, G_{ij}. R_{ijg} is a variant of R_{ij} based on the generation of technology used for the sub-system of interest, where the first generation is styled as 1, the second as 2, and so on. Finally, Each R_{ijg} is composed of a set of components Q_{ijgk}, where k = 1, 2…, K_{ijg}. Let the following functions be defined, as well.

$$Cr(R_{ij}) = \begin{cases} 1, & \text{if } R_{ij} \text{is a critical sub-system} \\ 0, & \text{otherwise} \end{cases}$$

$$Co(Q_{ijgk}) = \begin{cases} w, & \text{if } Q_{ijgk} \text{is a counterfeit of type } w, \text{ where } w = 1, 2\ldots, \\ 0, & \text{otherwise} \end{cases}$$

It is assumed if R_{ij} is a critical sub-system, the R_{ijg} is a critical sub-system for all g. It should be noted that the model need not include those components or sub-systems not relevant to counterfeiting. For instance, fasteners may not be relevant in a particular application.

Each sub-system has a set of functions associated with its performance, where performance is considered in a broad context. Here, we distinguish between technical performance, reliability performance and security performance. Each of the functions below is a matrix, in that there may be multiple metrics associated with it, and within each metric, multiple parameters.

$$Technical\ performance = Tec_{ijg}\left(Co(Q_{ijg1}), Co(Q_{ijg2}), \cdots, Co\left(Q_{ijgK_{ijg}}\right), \bar{p}_{ijg}\right)$$

$$Reliability\ performance = Rel_{ijg}\left(Co(Q_{ijg1}), Co(Q_{ijg2}), \cdots, Co\left(Q_{ijgK_{ijg}}\right), \bar{p}_{ijg}\right)$$

$$Security\ performance = Sec_{ijg}\left(Co(Q_{ijg1}), Co(Q_{ijg2}), \cdots, Co\left(Q_{ijgK_{ijg}}\right), \bar{p}_{ijg}\right)$$

Thus, performance is a function of whether the installed components of the sub-system are genuine or counterfeit, plus an additional parameter set $\bar{p}_{ijg}$. This additional parameter set is typically dependent on the type of sub-system and may include such things as velocity, altitude or weather conditions. Generally, it also includes age, measured in hours of usage, for example. In the baseline case, where $Co(Q_{ijgk}) = 0$ for all k, and the age is zero, the performance functions are simply the baseline performance of a new sub-system of type ijg. Various types of counterfeit components cause different performance degradations, often dependent on the topology of the sub-system.

For system behavior over time, these performance functions yield a set of metrics (i.e., rows in the output matrix) and for each metric a set of parameters and a distributional form (entries in the columns for that row). Thus, at any point in time, a value for each metric may be computed by sampling from its associated distributional form using the parameter set. An example set of outputs is shown in Table 1 for a navigational sub-system.

Table 1. Example performance function outputs for a navigational sub-system

Performance Type	Metric	Distributional Form	Parameters
Technical	Positional accuracy	Normal	Mean accuracy, standard deviation
Reliability	Time to next failure	Exponential	Mean time to failure
Reliability	Time to repair	Triangular	Mean time to repair, upper bound, lower bound
Security	Breaches/year	Triangular	Mean breaches/year, upper bound, lower bound

Of course, a system may be complex enough that it has major sub-systems and minor sub-systems. The formalism outlined above can be extended to address such situations.

Overall system performance is derived from the performance of the various sub-systems. In some instances, it is a direct derivation. In others, sub-systems interact to determine overall performance. This can be done analytically via formulae or computationally. For instance, the range of an aircraft system is dependent on weight of sub-systems, drag of the airframe, and propulsion efficiency of the engine sub-system, among other things. From a modeling perspective, this can be determined via Breguet range equation (Ruijgrok, 2009). Reliability, on the other hand, may be determined computationally by simulating failures of sub-systems and components within them, due to the complexity of the work breakdown structure. The dynamic system model addresses such computational behavior.

4.1.2. Dynamic Model

The previous sub-section has address the work breakdown structure of systems. We are interested also in their behavior and performance over time. Thus, we adopt the notion of state-charts (Harel, 1987). States are important especially when considering system reliability, when a system or sub-system can be operational or failed, and also when considering technical performance, when a system may or may not be deployed on a mission.

State-charts are used to represent states, as well as transition rates and transition conditions between them.

4.1.3. Example Aircraft System

We select an aircraft system, the F/A-18, as an example system for this case study. The F/A-18 was first flown as a production article in 1980 and is a carrier-based fighter. It has undergone several variants and is a very mature system well into the sustainment phase of its lifecycle. Thus, there are datasets available for parts replacement and potentially for counterfeit parts analysis. It is not clear that additional F/A-18 systems will be purchased, as the strategy of the

DoD is to replace it and other aircraft with the multi-purpose F-35 platform. The F-35 would make an interesting socio-technical case study due to the enterprise nature of its program (joint-service, multi-national). However, it is still in low rate initial production. Thus, its sustainment is not well-defined, and it is not amenable to counterfeit parts analysis.

Figure 6 depicts a state-chart for an aircraft system in sustainment. At fly-off, it exists production and is assigned to a fleet, to be stationed at a base. There, it undergoes flights and is grounded for maintenance and repairs. It may be deployed for missions, typically on a carrier. There it flies missions and also is grounded for maintenance and repairs. Once done with deployment, it returns to base. Note that multiple systems are likely deployed at a time on a carrier. Availability can be computed as the time that the aircraft is not grounded for maintenance and repair.

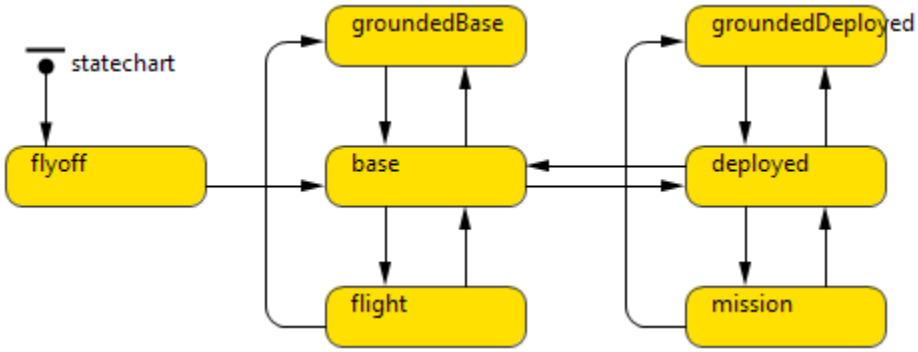

Figure 6. Aircraft system state-chart

The sub-systems are modeled as line-replaceable units (LRUs). There are three levels of maintenance and repair that these LRUs undergo, as shown in Figure 7. The most superficial is organizational level maintenance and repair. The LRU may undergo maintenance or be repaired in place on the aircraft, or it may be removed to be repaired or maintained in an onsite shop. The next level of maintenance and repair is intermediate-level, which takes place in an onsite shop. This is for more significant maintenance and repair operations. The most significant level is depot level. The LRU is removed from the aircraft and transported to a depot. This level is for such operations as rebuilds. When an LRU is removed for repair at an onsite shop or a depot, it is replaced on the aircraft by another LRU that is in inventory. LRUs include the following:

- Engines
- GPS navigation systems
- Radios
- Radar systems
- Imaging systems

- Weapons systems

LRUs fail or need maintenance at certain rates. These rates are influenced by whether the LRU has counterfeit component parts. They wait for maintenance and repair resources, then undergo a time duration for the maintenance and repair operation. They then return to inventory either on site or at the depot. LRUs inventoried at a depot are transported eventually to a base or mission location.

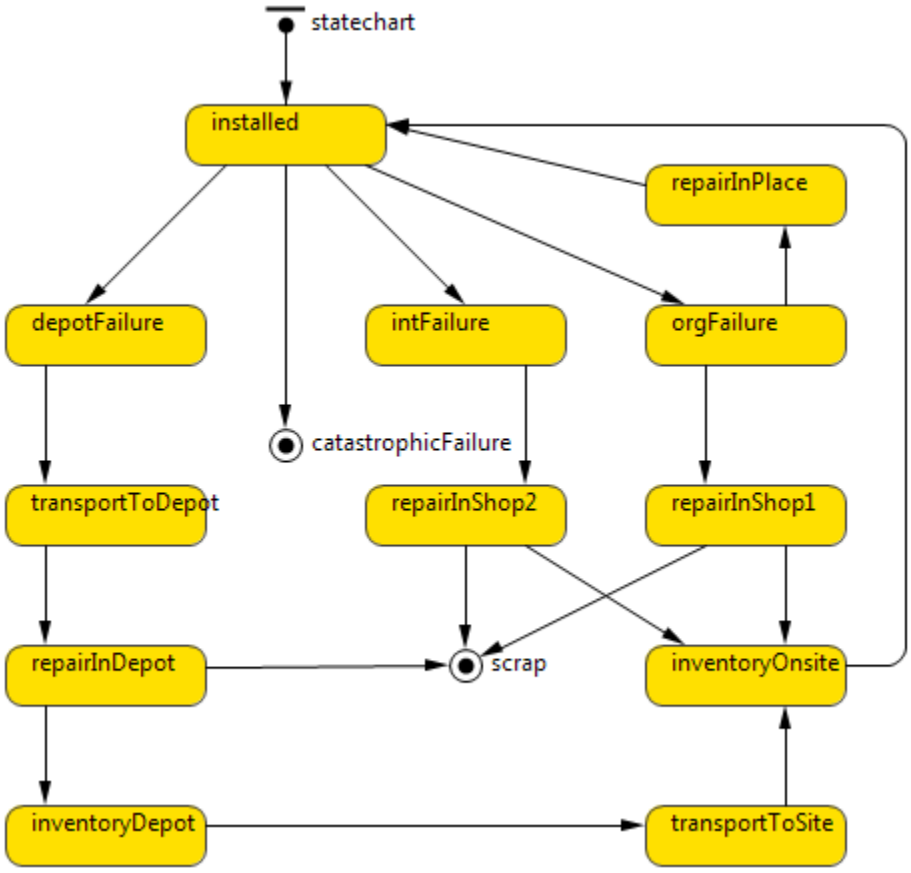

Figure 7. Example LRU state-chart

An LRU may be scrapped if it is beyond repair. Likewise, it may cause a catastrophic failure that destroys the aircraft (in flight). If there is no catastrophic failure, a maintenance or repair operation that becomes needed in a flight is assumed to be handled when the aircraft lands. Thus, when an LRU needs to be repaired or replaced, the aircraft's state transitions to 'grounded" while this operation is performed.

The repair and maintenance needs of the LRUs are dependent on whether they contain any counterfeit parts, as discussed in Section 4.2.

4.1.4. IMPLEMENTATION

The system model is implemented using AnyLogic, a commercial simulation software package that integrates discrete-event simulation, agent-based simulation and systems dynamics simulation (www.anylogic.com). The agent-based formalism is chosen, since it supports state change behavior and interactions between different agents (e.g., LRU failures causing an aircraft to be out of service).

AnyLogic is Java-extensible. This means that the existing simulation modeling constructs can be extended and new ones can be developed in Java. Thus, the basic agent class can be customized to represent complex behaviors of different sub-systems, for instance. This is a powerful method for modeling complex systems and enterprise-level behaviors.

4.2. COUNTERFEIT PART SUB-MODEL

In this section, we discuss the computational modeling approach for counterfeit parts and study their effects. This sub-model is developed for the case of an unverified source of system components introducing counterfeit components for the purpose of economic advantage (i.e., fraudulent type counterfeiting).

4.2.1 METHODOLOGY

The rationale behind the model is that for economic advantage the unverified source may produce components of lower quality thus affecting the expected performance of the system. Thus, our modeling is rational in that for any given system we can obtain an expected performance dictated from baseline requirements. For example, system users and maintenance crews usually have an intuitive "in-the-field" knowledge of how systems and components should operate and for how long. And, thus perturbations (i.e. degradation) of system's performance can be identified. Our modeling follows this idea as follows:

Step 1: Select a system to be modeled. This system may be a sub-system within a larger system. Identify and index all components in the system and populate subsets **P** and **CP** appropriately. If $P_i \in \mathbf{P}$, P_i is a component from a verified source (i.e., OEM or trusted supplier). If $P_i \in \mathbf{CP}$, P_i is a component from an unverified source.

Step 2: Baseline the system performance as per contractual component performance requirements.

> Note that in this section reliability is used as the primary proxy for measuring system performance. Thus, to identify baseline system performance it is necessary to know component time-to-failure (*T*) distribution along with system topological configuration.

Step 3: Understand counterfeiting effects through the following two sub-steps.

> Step 3.a: Define a counterfeit component percentage for each of the components in the unverified set and run our computational tool, an agent based modeling approach,

implemented using Stochastic Pi Machine (SPiM). The output of the SPiM model is a comma-separated values (csv) file to visualize the system and study the effects of counterfeiting. Briefly, the output provides a count of systems with counterfeit components for all combinatorial possibilities in set **CP**.

This step will allow the analyst to identify the economic gains and performance degradations as a function of counterfeit component percentage.

Step 3.b: This test uses a proportions test to statistically identify changes in performance based on the failure counts obtained in Step 3.a.

Step 4: In this step we will develop a set of tables that can be used by system users or system analysts to check for potential counterfeit components. This step is future research.

Figure 8 illustrates the agent-based model and its data and visualization outputs.

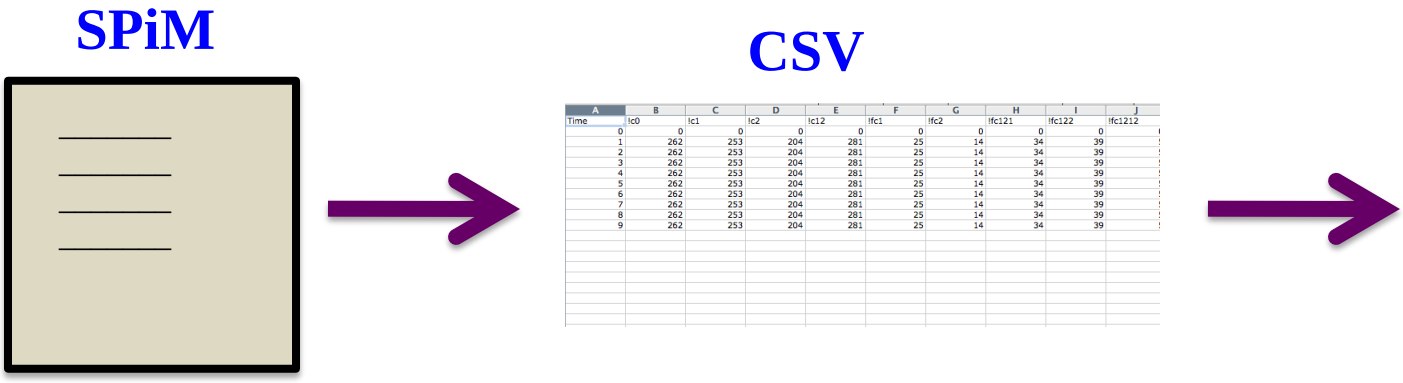

Figure 8. Computational modeling approach

4.2.2 CASE STUDY SYSTEM

For the case study to illustrate our computational model, we select a subcomponent of the Magellan GPS 315 a handheld and waterproof GPS (global positioning system) used for hiking. The analogy is to GPS units used in military navigation systems. An unassembled Magellan GPS 315 is shown in Figure 9. Figure 10 depicts the five-component subsystem considered for illustration.

Figure 9. Components of the Magellan GPS 315

Figure 10. Five component sub-system of Magellan GPS 315

4.2.3 Description of Agent Based Model

We have used SPiM to build the agent-based model of Magellan GPS 315 by considering a subsystem of five critical components of the Magellan GPS 315 system. The following assumptions have been made,

We assume that out of the five critical components of the Magellan GPS 315 system, the first two components are obtained from unverified suppliers. For the remaining components (components 3, 4 and 5), we assume they are all verified.

We have assumed that time to failure follows an exponential distribution and that the components in the subsystem follow a series configuration. It is important to note that the time-to-failure distributions can be changed, and SPiM has the ability to consider different configurations and performance assumptions.

Figure 11 depicts a schematic of the agent-based model of this subsystem of the Magellan GPS 315:

- P_1, P_2, P_3, P_4 and P_5 are the five critical original components of the Magellan GPS 315 subsystem. Since components P_1 and P_2 are purchased from an unverified supplier so that CP1 and CP2 are the possible counterfeits of the original components P_1 and P_2.
- Original components P_1, P_2, P_3, P_4 and P_5 and the potential counterfeit components assemble to form an assembled system (or in SPiM lexicon, a unit). An assembled system is labeled as AUnit in the computational model.
- Assembled systems may fail over a mission time as a function of their baseline time to failure distribution. At the end of the mission time (defined by the user) the system may be working or failed. If failed, the failed system is abbreviated as FUnit in the computational model.
- Finally, we assume that counterfeit and non-counterfeit components assemble randomly once components enter the supply chain.

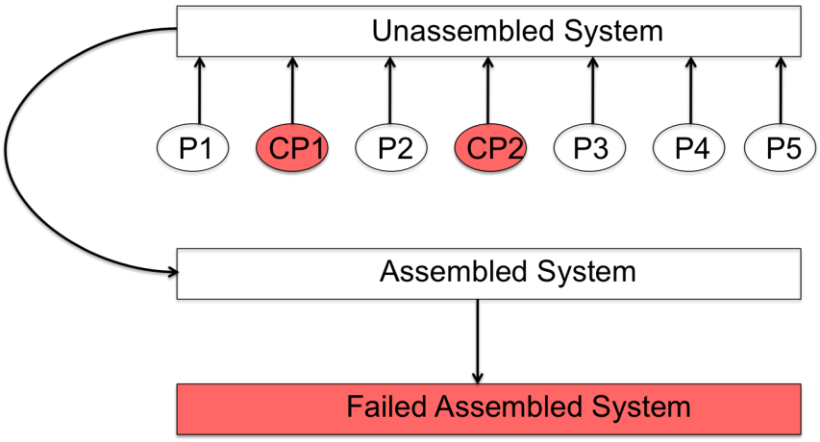

Figure 11. Agent-based model of Magellan GPS 315

4.2.4. COMBINATORIAL COMPLEXITY

Stochastic Pi Machine (SPiM) is developed by Luca Cardelli's group at Microsoft research. SPiM is a programming language used for designing and building large computational models

incrementally, by composing simpler models of subsystems. Computational models built using SPiM explain how complex agents or entities interact through communication channels and exchange information. Stochastic behavior of the systems is expressed by associating an interaction rate with each communication channel and each rate characterizes an exponential distribution. The simulation results obtained from SPiM depict the number of agents or entities over a period of time (Philips & Cardelli, 2007; Wang et al., 2009). SPiM is open source and is available at http://research.microsoft.com/en-us/projects/spim/. Our group at Stevens led by Prof. Adriana Compagnoni has used SPiM to build computational models for "Activation cycle of G-proteins by G-protein-coupled receptors" (Bao et al., 2010) and "JAK-STAT Signal Transduction Pathway" (Sharma & Compagnoni, 2013).

Stochastic Pi Machine (SPiM) addresses the combinatorial complexity of the agent-based model. Our computational model yields failure counts of original and counterfeit components over the course of time to depict the reliability of the system.

We define four types of assembled units, namely, AUnit1, AUnit2, AUnit3 and AUnit4 in our computational model. Figure 12 depicts the visual implementation of four types of assembled units (AUnit). In Figure 12, counterfeit components are represented with smaller rectangles as compared to the original components.

- AUnit1 is the assembled unit with no counterfeit components.
- AUnit2 is the assembled unit with 1 counterfeit component, CP1.
- AUnit3 is the assembled unit with 1 counterfeit component, CP2.
- AUnit4 is the assembled unit with 2 counterfeit components, CP1 and CP2.

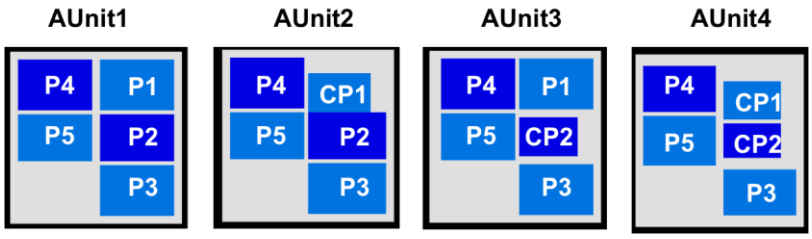

Figure 12. Visualization of four types of assembled units (AUnit)

An assembled unit is declared as a failed assembled unit when one or more of the original or counterfeit components fail. We have implemented the following possible scenarios of failures for the four types of assembled units, AUnit1, AUnit2, AUnit3 and AUnit4 in our computational model.

A failure due to just one original component can lead to five combinations of failed assembled units. Figure 13 depicts the visual implementation of failed assembled units (FUnit) due to single component failure. $FUnit1_i$ represents failed assembled unit of component i =1, 2…, 5 due to failure of original component, P_i. In the remaining figures in this section, light blue and dark

blue rectangles represent functional components, while red rectangles represent failed components.

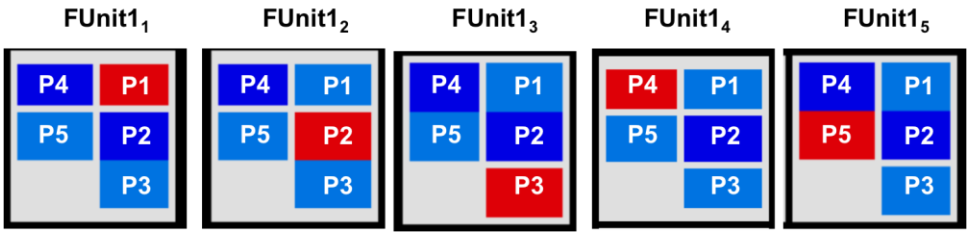

Figure 13. Visualization of failed assembled units (FUnit) due to single component failure

In general, failure due to *r* original components out of *n* subsystem components leads to *n*!/(*n* - *r*)!*r*! potential failure combinations. Figure 14, Figure 15, Figure 16 and Figure 17 depict the component interactions within the system.

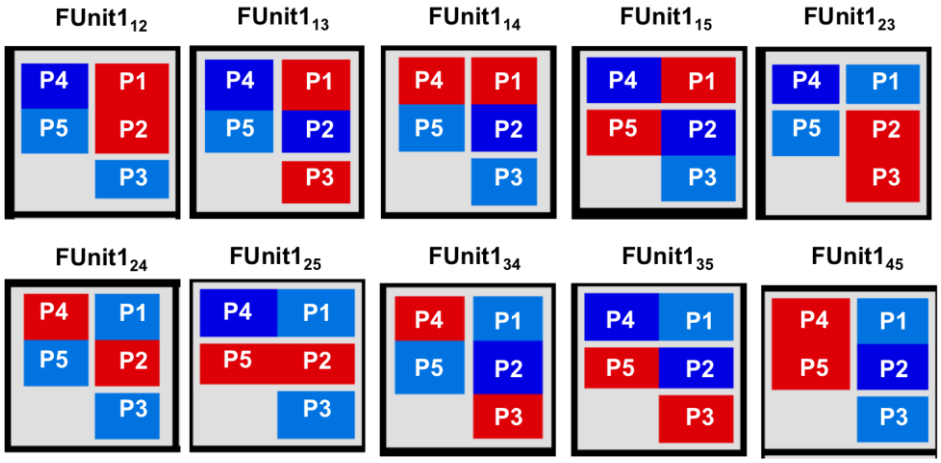

Figure 14. Visualization of failed assembled units (FUnit) due to two original component failures

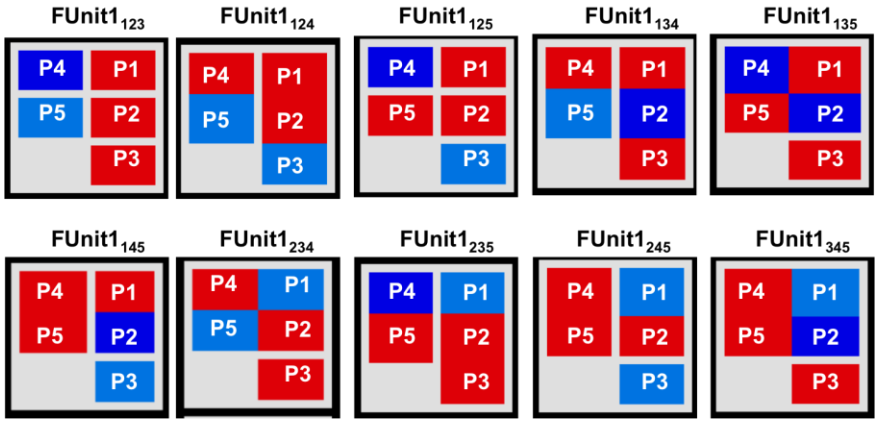

Figure 15. Visualization of failed assembled units (FUnit) due to three original component failures

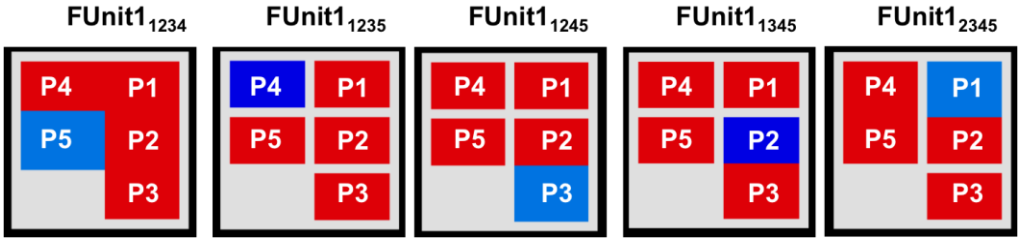

Figure 16. Visualization of failed assembled units (FUnit) due to four original component failures

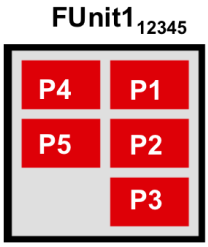

Figure 17. Visualization of failed assembled units (FUnit) due to five original component failures

A failure due to the presence of one counterfeit component, described as CP_1, can lead to one failed assembled unit. Figure 18 depicts the visualization of failed assembled units (FUnit) due to one counterfeit component, in this case components 1 or 2. Figure 19 depicts the visualization of failed assembled units with two counterfeit components, in this case components 1 or 2 or both 1 and 2 at the same time frame. As explained in Figure 12, AUnit2 and AUnit3 can fail and form FUnit2 and FUnit3. These units typically do not fail at the same. During the simulation the failures occur at different time frames.

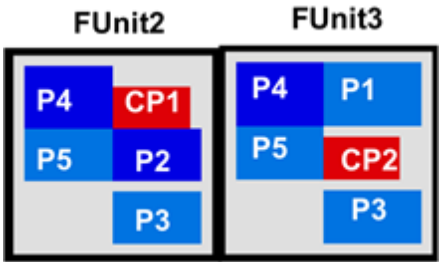

Figure 18. Visualization of failed assembled units (FUnit) due to single counterfeit component failures

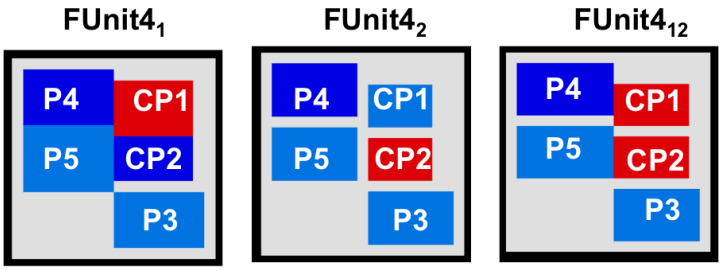

Figure 19. Visualization of failed assembled Units (FUnit) due to one or more counterfeit component failures

4.2.5. Input Data for Computational Model

To simulate the effect of counterfeits introduced into the supply chain, we use the input data shown in Table 2.

Table 2. Input data for computational model

Number of Original Components	Number of Counterfeit Components	Unassembled Units	Failure Rates of Original Components	Failure rates of Counterfeit Components	Simulation Time
P1 = 700 P2 = 800 P3 = 1000 P4 = 900 P5 = 1000	CP1 = 300 CP2 = 200	1000	P1 = 0.0001 P2 = 0.0002 P3 = 0.0003 P4 = 0.0004 P5 = 0.0005	CP1 = 1.0 CP2 = 2.0	250 Time Units with 10 sampling time intervals

Failure rates determine how often the original and counterfeit components fail over a period of time. In our computational model we assume that the probability of failure of counterfeit components is more often than that of the original components.

4.2.6 SIMULATION RESULTS

The output of the computational model contains two parts:

- a graphical description of failure counts for both original and counterfeit components and
- 3D-rendered videos of the assembled and failed assembled units due to failure of original and counterfeit components to enhance the visualization of the system.

Figure 20, Figure 21 and Figure 22 depict the failure counts of original and counterfeit components for three different runs of the computational model. The simulation results highlight the stochastic (SPiM) computational modeling. Stochastic Pi Machine outputs the stochastic variation of the results and can expose the failures of original and counterfeit components.

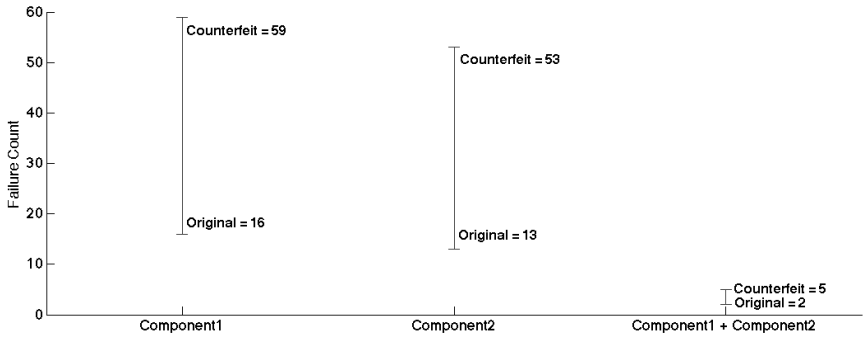

Figure 20. Simulation result of 1st run – comparison of failure counts for original P_1 and P_2 versus counterfeit components, CP_1 and CP_2

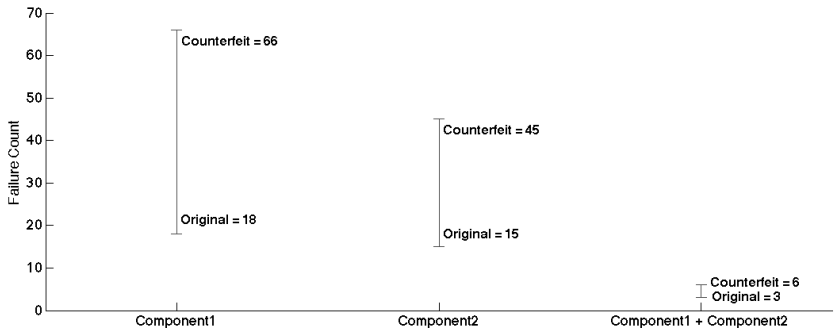

Figure 21. Simulation result of 2nd run – comparison of failure counts for original P_1 and P_2 versus counterfeit components, CP_1 and CP_2

Figure 22, Simulation result of 3rd run – comparison of failure counts for original P_1 and P_2 versus counterfeit components, CP_1 and CP_2

4.2.7. VISUALIZATION OF THE SUB-SYSTEMS

Figure 23 and Figure 24 depict the visualization of the simulated sub-systems for the same input data as explained previously. The simulation results in Figure 23 depict the configuration of assembled units (AUnit) in the first timestamp.

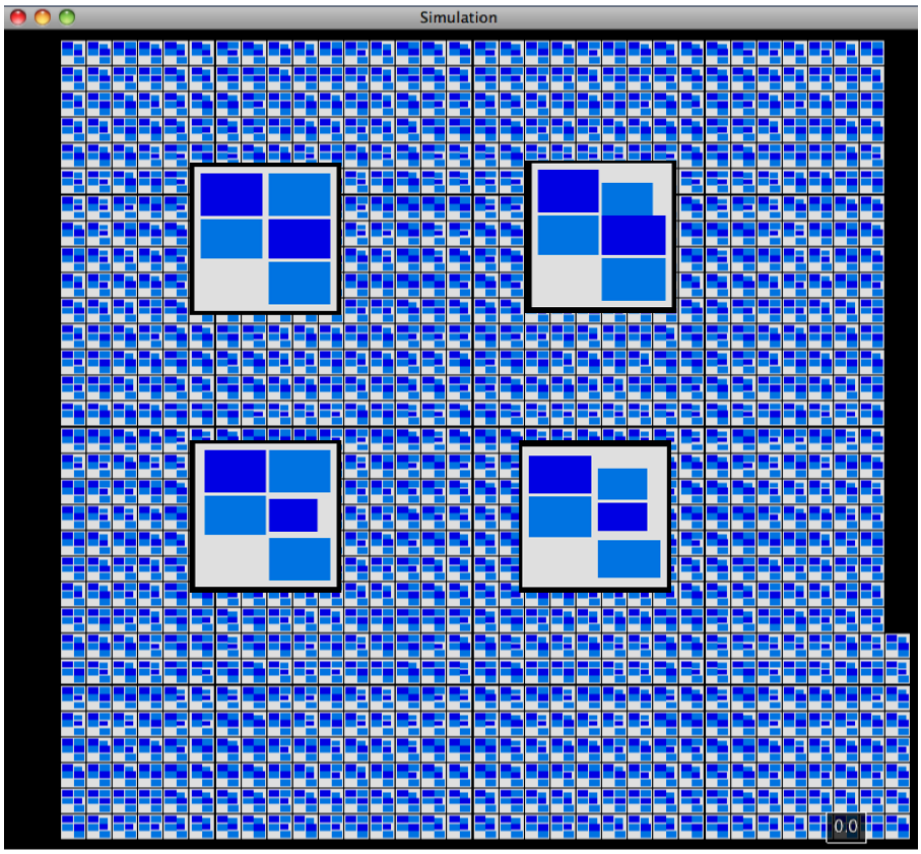

Figure 23. Simulation results for the 1st time stamp to depict the configuration of assembled units (AUnit)

The simulation results in Figure 24 depict the failed assembled units (FUnit) in the last timestamp.

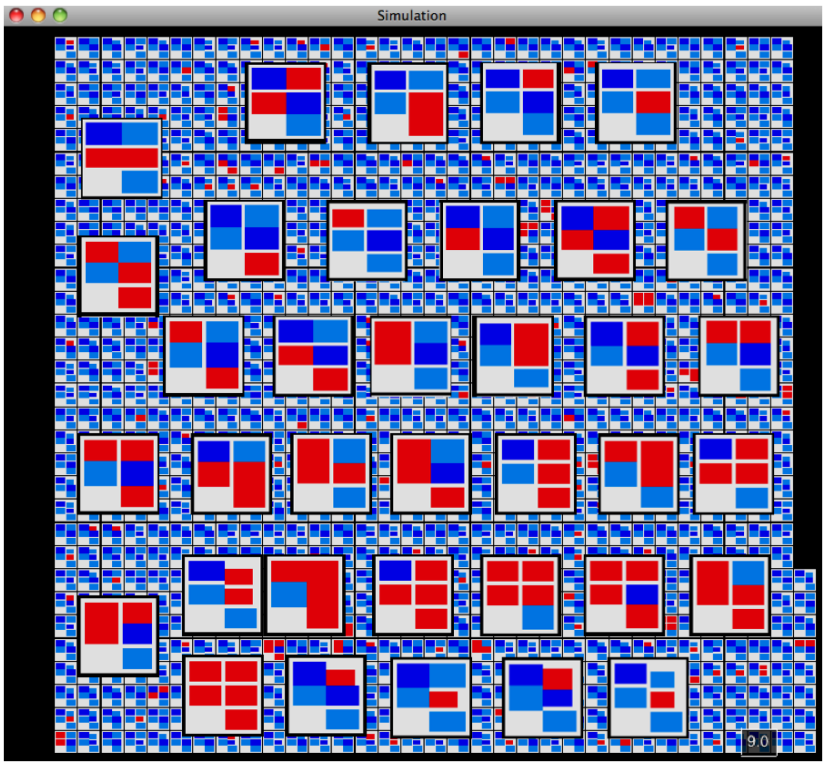

Figure 24. Simulation results for the last time stamp to depict the failed assembled units (FUnit)

4.2.8. STATISTICAL TESTS

We run statistical tests to analyze the difference in proportions for simulations results discussed in Section 4.2.5. We run the hypothesis testing procedure for component1 in Figure 20.

Step 1: The parameters of interest are p_1 and p_2, the proportion of original and counterfeit components, respectively.

Step 2: The alternate hypothesis is, H_1: $p_1 \neq p_2$

Step 3: Set the significance level □ = 0.0001

Step 4: The test statistic is

$$Z_0 = (p_2' - p_1')/\sqrt{p'(1-p')(1/n_1 + 1/n_2)}$$

where

$$p_1' = 16/100 = 0.016$$

$$p_2' = 59/100 = 0.059$$

$$n_1 = n_2 = 1{,}000$$

$$p' = (x_1 + x_2)/(n_1 + n_2) = (16 + 59)/(1{,}000 + 1{,}000) = 0.0375$$

Step 5: Reject the null hypothesis H_0: $p_1 = p_2$ if $Z_0 > Z_{\square} = 0.5$

Step 6: Computations: The value of the test static is

$$Z_0 = (0.059 - 0.016)/\sqrt{0.0375(1 - 0.0375)(1/1{,}000 + 1/1{,}000)} = 5.082$$

Step 7: Conclusions: Since $Z_0 = 5.082$ exceeds $Z_{0.0001} = 0.5$, we can reject the null hypothesis.

The results from hypothesis testing of the simulation results in Figure 20, Figure 21 and Figure 22 are summarized in Table 3, Table 4 and Table 5, respectively.

Table 3. Hypothesis testing for simulation results in Figure 20

Components	α	Z_0	Zα	Rejection Criterion ($Z_0 > Z\alpha$)
Component1	0.0001	5.082	0.5	Reject
Component2	0.0002	5.012	0.5	Reject

Table 4. Hypothesis testing for simulation results in Figure 21

Components	α	Z_0	Zα	Rejection Criterion ($Z_0 > Z\alpha$)
Component1	0.0001	5.39	0.5	Reject
Component2	0.0002	3.94	0.5	Reject

Table 5. Hypothesis testing for simulation results in Figure 22

Components	α	Z_0	Zα	Rejection Criterion ($Z_0 > Z\alpha$)
Component1	0.0001	9.31	0.5	Reject
Component2	0.0002	8.07	0.5	Reject

4.2.8. Extendibility

This section has presented an agent-based model of counterfeit parts within assemblies or sub-systems. This approach is extendible in the following ways.

- Thus far, it has been used to model sub-systems with several hundred components. It seems to scale well computationally. This will need to be tested, especially in conjunction with models of other elements of the overall counterfeit parts enterprise model.
- The sub-systems modeled thus far have components in series with a failure assumed if any of the components fail. More complex behavior can be modeled, such as parallel components, redundancy, performance degradation rather than failure, etc.

4.3. Supply Chain Sub-Model

The supply chain model addresses the flow of parts and systems; maintenance, repair and inspection processes; system usage; sustainment costs; and network evolution over time.

4.3.1. Processes and Flow

The supply chain model focuses on the sustainment of the aircraft. The following nodes in the supply chain are modeled.

- Final assembly – Planes fly off from here, a factory owned by the prime contractor, to be delivered to the government.
- Bases – Planes are stationed here for routine operations. A base has an onsite repair shop and an inventory of sub-systems and components. It is assumed that sub-system upgrades can be performed at a base. An upgrade occurs when a sub-system based on an older technology is replaced with one of the same overall type, but newer technology.
- Deployed locations – Planes are stationed here for missions (e.g., on a carrier). Like bases, these have repair shops and an inventory of sub-systems and components. It may be the case that the repair shops can perform fewer types of repairs than those at bases, and that the inventory may not be as extensive.
- Sub-system factories – Various sub-systems are manufactured here, with each factory owned by the supplier charged with manufacturing the sub-system. A particular sub-system can have more than one supplier.
- Component sources – Components are shipped from sources to sub-system factory or to a supplier warehouse.
- Supplier warehouses – These store sub-systems and components and are owned privately. For now, owners consist of the prime contractor, sub-system suppliers, and prime sustainment contractor (if different from the prime acquisition contractor).
- Government warehouses – These store sub-systems and components, but are owned by the government.
- Depots – A depot is a government facility that performs major repair and maintenance work (e.g., sub-system rebuilds). In the current model, sub-systems are transported to a depot, rather than having the entire system transported there.

- Supplier repair and maintenance facilities – These perform major, depot-level repair and maintenance operations and are used when sustainment is contracted to a private firm.

Each factory has a production capacity that governs how many systems or sub-systems can be turned out per time period. Each warehouse and other inventory location has a storage capacity and an inventory policy. For now, these inventory policies use simple reorder points to replenish inventory. Note that deployed locations often cannot easily implement a reorder point inventory policy, since replenishments may be difficult to accomplish depending on the circumstances of the mission being supported. A schematic of system and sub-system flows is shown in Figure 25.

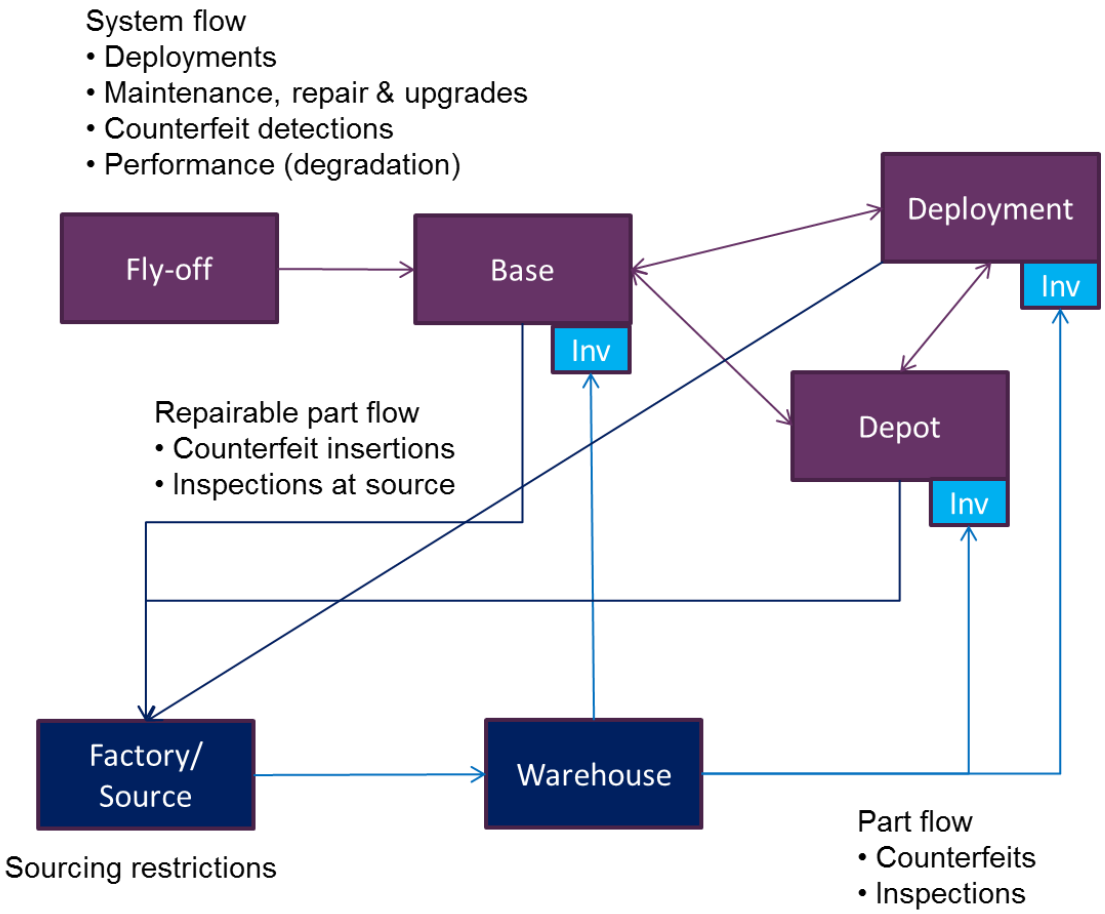

Figure 25. Supply chain flow

Component flows are not shown. It is assumed that they arrive at various locations from their sources according to inventory policies. One of the potential policy decisions to evaluate using the model is counterfeit inspection and testing regimen to adopt. Aspects of the regimen are as follows:

- Points at which inspections of components are performed (e.g., upon arrival of components to sub-system supplier, prime contractor or government facilities),
- Points at which inspections of sub-systems are performed for counterfeit components (e.g., arrival at prime contractor or government facilities, either as new or repaired),
- Sampling plan for inspections (e.g., how many components or sub-systems to inspect out of an arrival lot), and
- Inspection and testing methodology (e.g., technical details of tests and inspections, such as destructive testing of components versus non-destructive functional tests versus visual inspection of markings).

Thus, there are inspection processes at various points in the supply chain that implement the inspection regimen.

4.3.2. COSTS

The supply chain model accrues costs over time. Costs include the following.

- Maintenance and repair costs for each system and across a fleet of systems.
- Upgrade costs for each system and across a fleet of systems.
- Loss of sub-systems or systems due to catastrophic failures.
- Cost of inspection processes.
- Potential cost increases of critical sub-systems if trusted suppliers are used (due to limited competition)

Costs can then be traded off against other costs and against such performance impacts as:

- Improved technical performance from reduced counterfeits (e.g., from successful inspections or upgrades less vulnerable to counterfeiting).
- Improved system availability and security from reduced counterfeits.
- Fewer system losses from reduced counterfeits.
- Fewer counterfeits from use of trusted suppliers for critical sub-systems (and expansion of definition of critical sub-systems).

4.3.3. SUPPLY CHAIN EVOLUTION

The supply chain evolves over time, as suppliers enter and exit the market for a particular program. Generally, OEM suppliers are more trustworthy with respect to counterfeit parts than others. However, programs tend to evolve such that OEM supplier exit the market and are replaced by others. The changing nature of the supplier base clearly impacts the supply chain by changing the facilities and part flows. It may be necessary to change inspection regimen, upgrade schedules and other anti-counterfeiting strategies as the supply chain evolves.

Figure 26 shows the risks from counterfeiting as a function of part sources and technology age.

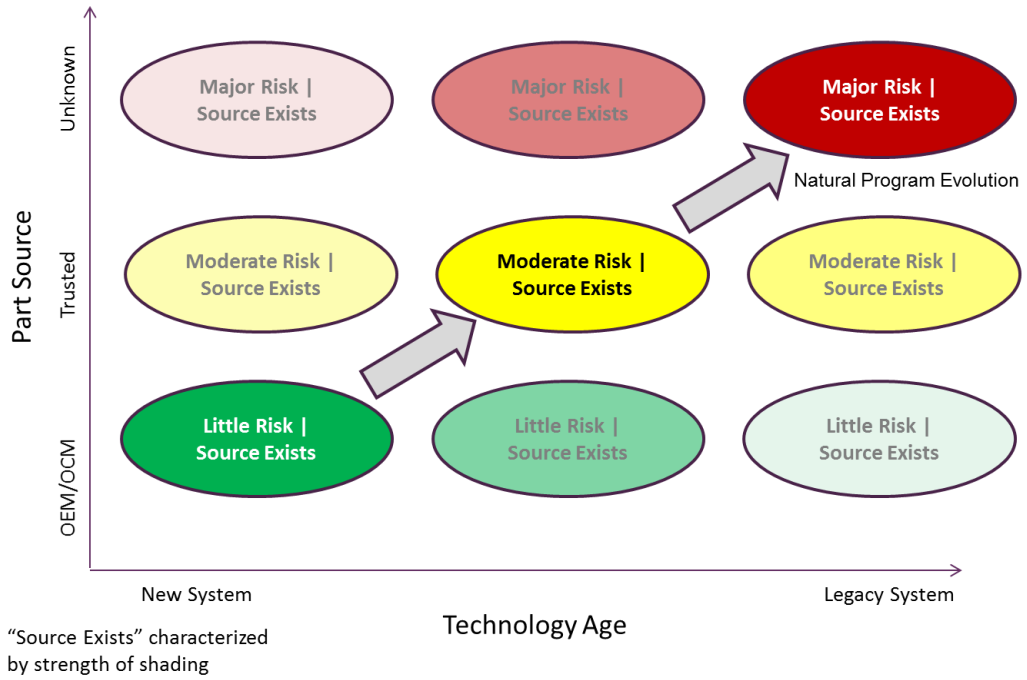

Figure 26. Risks as a function of part source and technology age

4.3.4. IMPLEMENTATION

The supply chain model is currently implemented using AnyLogic, in conjunction with the system model. It uses an object-based framework augmented by discrete-event representation for part movements between the various facility objects. System and sub-system agents are transitioned to various facilities via associated simulation entities in the discrete-event model, and their states change accordingly (i.e., from their state-charts).

4.4. SUPPLIER AND COUNTERFEITER SUB-MODEL

The supplier model is under development and will incorporate the following:

- Notion of utility based on expected profit (for honest suppliers and fraudulent counterfeiters)
- A simple adversarial model for government and counterfeiters.
- Supplier actions to enter or exit the market based on expected utilities.
- Linkages from supplier agents to locations in the supply chain.
- Decisions from supplier agents to locations affecting increases in production capacities, decrease in production capacities, etc.
- Network relationships among suppliers (e.g., from a component supplier to the supplier of a sub-system that contains the component)

A collection of suppliers and relationships for a particular program is shown in Figure 27. It is assumed that each supplier has a production facility. The prime has a final assembly facility. It and first tier (sub-system) suppliers maintain warehouses with inventories.

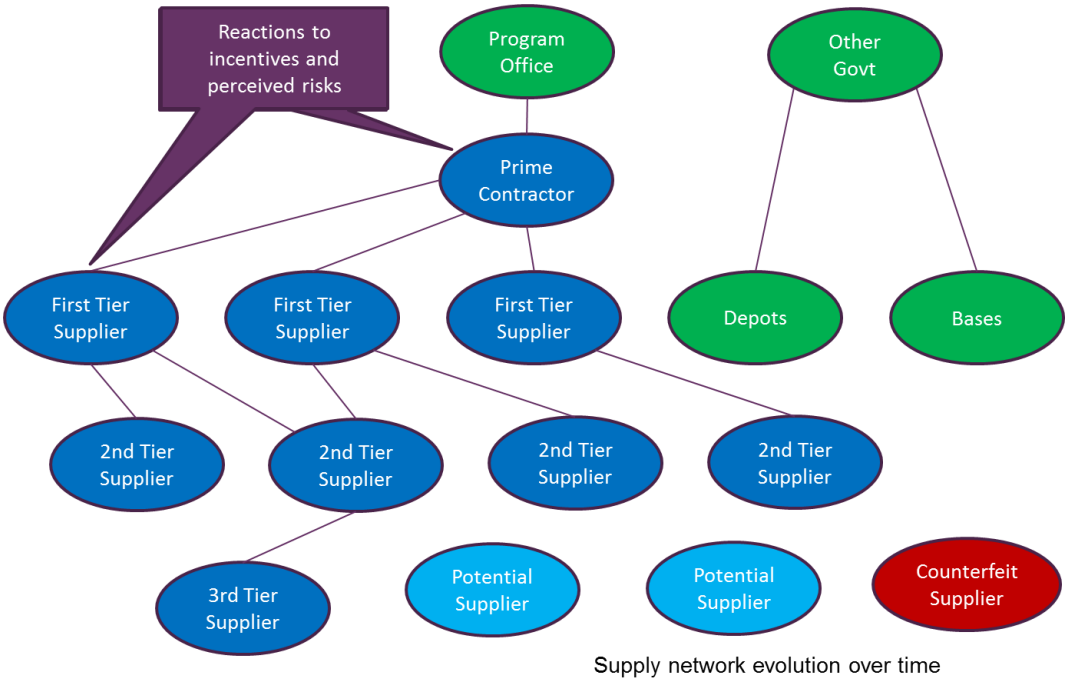

Figure 27. Supplier relationships

4.5. POLICY SUB-MODEL

The policy sub-model is under development. It will consist of a selection of choices, which may be discrete or continuous in nature. These choices will change variables or activate/de-activate aspects of other sub-models. Examples are presented below.

- Inspection regimen. Alternative policies may be to have no inspections or have inspections of components from non-trusted suppliers prior upon receipt at a sub-system production or maintenance and repair facility. The former alterative deactivates all inspection points implemented in the supply chain sub-model. The latter activities only those at point of component receipt. It may further allow selection of a sampling plan, providing parameters for the plan to the supply chain sub-model.
- Selection of critical sub-systems. The policy dictates which sub-systems are considered critical and restricts suppliers for those sub-systems to be trusted suppliers in the supplier sub-model, with implications for sources of components to those sub-systems. Alternate policies may range from a fairly narrow scope of critical sub-systems to many/most being classified as critical.

- Penalties for counterfeiting. Alternate policies may hold sub-system suppliers liable for counterfeits found in their articles, setting the value of the penalty.
- Tracking. Alternate policies may be to track all components from source to installation in an operational system, a subset of components, or not to engage in tracking. This policy then activates tracking in the supply chain sub-model for those components selected.

4.6. EXOGENOUS SUB-MODEL

The exogenous sub-model is under development. Similar to the policy sub-model, it either feeds variable values to other sub-models or it activates/de-activates parts of them. Example exogenous sub-model elements include:

- Globalization and technology off-shoring rates. These feed into the supplier sub-model, affecting the rate at which certain technologies increasingly are made by foreign suppliers.
- Technological progress rates. These feed into the supplier and supply chain sub-models, affecting the rate at which upgraded sub-systems become available to be installed on systems. These may also affect the rate at which counterfeiters have access to improved technologies to make better counterfeits.
- Fiscal trajectories. These feed into the supply chain and system sub-models and affect the ability of programs to fund maintenance and repair, counterfeit inspections, system upgrade schedules, mission deployments, etc.

5. MODEL COMPOSITION ARCHITECTURE

The initial model combines various sub-models under a discrete-event and agent-based formalism, as discussed in Section 3. This is supported by the AnyLogic simulation software, which integrates the two formalisms. Figure 28 shows the composition framework for the overall model.

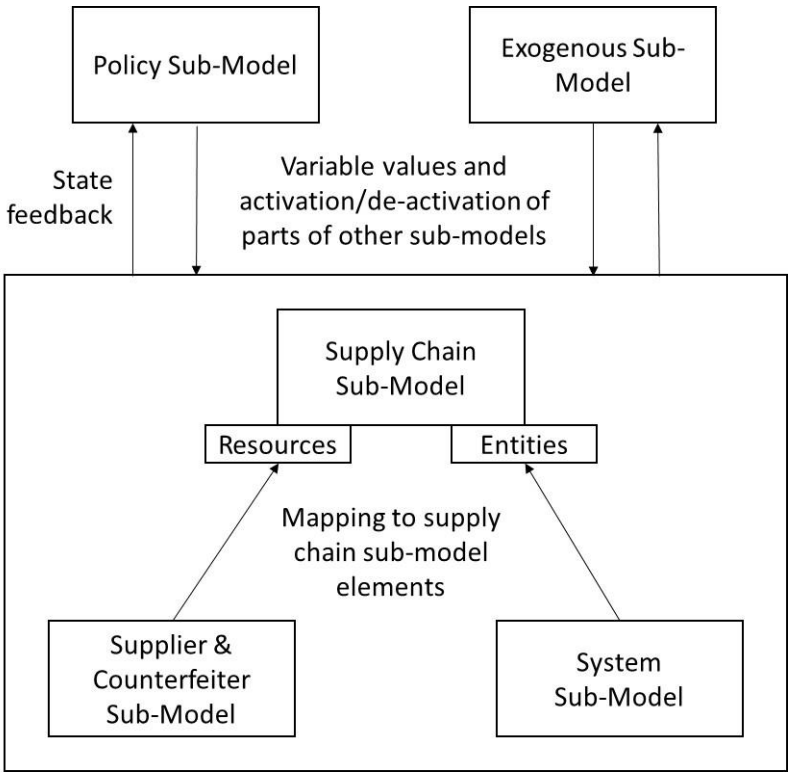

Figure 28. Model composition framework

The supply chain, supplier & counterfeiter and system sub-models are combined using the discrete-event and agent-based formalisms. The policy and exogenous sub-models are combined with the other sub-models in the current implementation. However, in future implementations, they may be coupled, depending on the evolution of the model and needs of stakeholders.

To support coupling, the interactions between the policy and exogenous models on the one hand and the other three models on the other hand should be one-way only at discrete points during model execution. For instance, inputs from the policy and exogenous models would be fed to the other models at initiation of execution. The three models would execute for a period of time (either fixed or until certain conditions are met), at which time the policy and exogenous sub-models receive state updates from them. The policy and exogenous models than compute new inputs to the other three models based on their internal logic. This represents the reaction of the external world and policies to new states in the other three models.

Another possible interaction is that policies or exogenous world states update at various time points and provide revised input to the other three models. To be practical, there must be methods to reconcile any incompatibility between these inputs and the state of the other three sub-models.

Finally, the periodic input revision from the policy and exogenous models could be performed by an analyst or model stakeholder, rather than automatically computed by either of those sub-models. This interactivity would provide valuable decision support for model stakeholders.

Of course, if the periodic updates occur too frequently, it may make more sense from a computational perspective to keep all sub-models combined. Thus, it makes sense for the policy and exogenous models not to have too frequent interaction with the other three sub-models. This is an avenue for future research.

6. METHODOLOGICAL SUPPORT TO B PROVIDED

Rouse and Pennock (2013) outline two classes of users for this type of modeling framework – consumers of analyses and producers of models for analysis. The former need the right tools, interfaces and datasets to support the analyses that they wish to conduct. The latter need to right formalisms and compositions of formalisms, implemented as tools, to enable analysis. They also find libraries of models useful.

They identify five categories of methodological support for future research -- visualization methods and tools, interactive visualization infrastructure, economic and policy models, physical and organization models, and behavioral and social models. These five areas are shown in Table 6, along with examples of their application in the counterfeit parts problem.

Table 6. Examples of methodological support

Need Area	Example Usage
Visualization methods and tools	Tools that visualize trade-offs and interaction effects between different elements of a systemigram-type figure to allow stakeholders to define which counterfeiting problem aspects should receive priority.
Interactive visualization infrastructure	Tools that allow different classes of stakeholders to see the effects of their decisions on other stakeholder types and vice-versa, promoting mutual understanding of needs across the acquisition and sustainment community.
Economic and policy models	Firm reactions to incentives, information and policies for anti-counterfeiting. Counterfeiter reactions to counterfeiting disincentives.
Physical and organization models	Interaction between contractual relationships among government and suppliers versus delivery of parts and counterfeiting counter-measure effectiveness.
Behavioral and social models	Definitions in anti-counterfeiting policies versus

	the understanding of those definitions by key stakeholders, and stakeholder decisions based on those understandings.

7. CONCLUSIONS AND FUTURE RESEARCH

This report has documented a case study and associated model for addressing counterfeit parts in the DoD supply chain. This problem has socio-technical aspects and cannot be solved without considering multiple perspectives. This, of course, requires multiple different model types, necessitating a model composition approach.

This report is a companion to another that documents a methodology for creating composed models to address socio-technical enterprise problems. Using this methodology, the counterfeit parts model was posed, and various sub-models were developed. A composition framework was then presented for these sub-models.

Future work involves elaborating the model, populating it with data, validating it, and then performing analyses. From this process, the methodology for developing and composing such overall models will be enhanced. Additional sub-models will be developed and composed in the counterfeit parts model, leading to new knowledge of how to do this for other, similar models.

8. REFERENCES

ABA (2012). A White Paper Regarding Department of Defense Implementation of Section 818 of the National Defense Authorization Act for Fiscal Year 2012. Report issued by Task Force on Counterfeit Parts of the Committee on Acquisition Reform and Emerging Issues of the American Bar Association Section of Public Contract Law, October 5, 2012.

AIA (2011). Counterfeit Parts: Increasing Awareness and Developing Countermeasures. Arlington, VA: Author.

Bao, Y., Compagnoni, A.B., Glavy, J., & White, T. (2010). Computational modeling for the activation cycle of G- proteins by G-protein-coupled receptors. In MeCBIC, pp. 39–53.

Blair, C.D., Boardman, J.T., & Sauser, B.J. (2007). Communicating strategic intent with systemigrams: Application to the network-enabled challenge. Systems Engineering, 10 (4), 309-322.

Bodner, D.A, & Rouse, W.B. (2010). A Framework and Tools for Organizational Simulation. Report. Atlanta, GA: Georgia Institute of Technology.

Business Insider (2012). Counterfeit Chinese microchips are getting so good they can't be identified. http://www.businessinsider.com/counterfeit-parts-from-china-raise-grave-concerns-for-both-us-companies-and-national-security-2012-6.

Capaccio, T. (2011). China counterfeit parts in U.S. military aircraft. Bloomberg, Nov 8, 2011.

Congress (2011). H.R. 1540 National defense authorization act for fiscal year 2012. Legislative act. Washington, DC: Author.

DAU (2013). Anti-counterfeiting. Defense Acquisition Guidebook. https://acc.dau.mil/CommunityBrowser.aspx?id=638350&lang=en-US.

Davis, P. (2003). Thoughts on higher-level adversary modeling. In *Proc. SPIE* 5091.

Dept. of Commerce (2012). Defense Industrial Base Assessment: Counterfeit Electronics. Report. Washington, DC: Author.

DFARS (2013), DFARS Case 2012-D055. Federal Register 78 (95), 287-85.28780-

DoD (2013). DoD Counterfeit Prevention Policy. DoD Instruction 4140.67. Washington, DC: Author.

DoD (2011). DoD Supply Chain Materiel Management Policy. DoD Instruction 4140.01. Washington, DC: Author.

DoD (2012). Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN). DoD Instruction 5200.44. Washington, DC: Author.

Economist (2012). Huawei: the company that spooked the world. Author, August 4, 2012.

GAO (2012a). Additional Efforts Needed by National Security-Related Agencies to Address Risks. Report GAO-12-579T. Washington, DC: Author.

GAO (2010). DOD Should Leverage Ongoing Initiatives in Developing Its Program to Mitigate Risk of Counterfeit Parts. Report GAO-10-389. Washington, DC: Author.

GAO (2011). Periodic Assessment Needed to Correct Parts Quality Problems in Major Programs. GAO-11-404. Washington, DC: Author.

GAO (2012b). Suspect Counterfeit Electronic Parts Can Be Found on Internet Purchasing Platforms. GAO-12-375. Washington, DC: Author.

Harel, D. (1987). Statecharts: a visual formalism for complex systems. Science of Computer Programming, 8 (3), 231–274.

Holland, J.H., & Miller, J.H. (1991). Artificial adaptive agents in economic theory. American Economic Review, 81 (2), 365-371.

Kendall, F. (2012). Overarching DoD counterfeit prevention guidance. Memorandum from Under Secretary of Defense dated March 16, 2012. Washington, DC: Department of Defense.

Kreps, D. (1990). A Course in Microeconomic Theory. Princeton, NJ: Princeton University Press.

Law, A.M. (2007). Simulation Modeling and Analysis (4th Edition). McGraw-Hill.

Livingston, H. (2007a). Avoiding counterfeit electronic components. IEEE Transactions on Components and Packaging Technologies, 30 (1), 187-189.

Livingston, H. (2007b). Avoiding counterfeit electronic components – Part 2: Observations from Recent Counterfeit Detection Experiences. Report. BAE Systems.

McFadden, F. E., & Arnold, R. D. (2010). Supply chain risk mitigation for IT electronics. Proceedings of the 2010 IEEE International Conference on Technologies for Homeland Security, 49-55.

Park, H., Clear, T., Rouse, W.B., Basole, R.C., Braunstein, M.L., Brigham, K.L., & Cunningham, L. (2012). Multi-level simulation of health delivery systems: a prospective tool for policy, strategy, planning, and management. Service Science, 4 (3), 253-268.

Pasztor, A. Pratt reveals faulty testing. Wall Street Journal, Mar 4, 2013.

Pecht, M., & Tiku, S. (2006). Bogus: Electronic manufacturing and consumers confront a rising tide of counterfeit electronics. IEEE Spectrum, 43 (5), 37-46.

Phillips, A., & Cardelli, L. (2007). Efficient, correct simulation of biological processes in the stochastic pi-calculus. In Computational Methods in Systems Biology, volume 4695 of LNCS, 184–199. Springer, September 2007.

Rothschild, C., McLay, L., & Guikema, S. (2012). Adversarial risk analysis with incomplete information: a level-k approach. Risk Analysis, 32 (7). 1,219 – 1,231.

Rouse, W.B., & Bodner, D.A. (2013). Multi-Level Modeling of Complex Socio-Technical Systems. Hoboken, NJ: Systems Engineering Research Center.

Rouse, W.B., & Pennock, M.J. (2013). A Methodology for Modeling Complex Socio-Technical Systems. Hoboken, NJ: Systems Engineering Research Center.

Ruijgrok, G.J.J. (2009). Elements of Airplane Performance. VSSD.

Senate Armed Services Committee (2012). Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain. Report issued May 21, 2012. Washington, DC: Author.

Sharma, V., & Compagnoni, A. (2013). Computational and mathematical models of the JAK-STAT signal transduction pathway. To appear in the Proceedings of the 2013 Summer Computer Simulation Conference.

Stradley, J., & Karraker, D. (2006). The electronic part supply chain and risks of counterfeit parts in defense applications. IEEE Transactions on Components and Packaging Technologies, 29 (3), 703-705.

Villasenor, J., & Tehranipoor, M. (2013). Chop-shop electronics. IEEE Spectrum, 50 (10), 40-45.

Wang, D., Cardelli, L., Phillips, A., Piterman, N., & Fisher, J. (2009). Computational modeling of the EGFR network elucidates control mechanisms regulating signal dynamics. BMC Systems Biology, 3(1), 118.