

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/384677779>

The impact of counterfeit components and LRUs in the navy surface warfare supply chain: A systems dynamics approach

Article in *Systems Engineering* · October 2024

DOI: 10.1002/sys.21785

CITATION

1

READS

74

5 authors, including:



Wayne Porter

Naval Postgraduate School

10 PUBLICATIONS 63 CITATIONS

SEE PROFILE



Jason Bickford

Naval Postgraduate School

2 PUBLICATIONS 76 CITATIONS

SEE PROFILE




Douglas Lee Van Bossuyt

Naval Postgraduate School

135 PUBLICATIONS 936 CITATIONS

SEE PROFILE

The impact of counterfeit components and LRUs in the navy surface warfare supply chain: A systems dynamics approach

Wayne Porter¹ | Cody Reese² | Jason Bickford² | Seth Bourn² |
Douglas L. Van Bossuyt² 

¹Department of Defense Analysis, Naval Postgraduate School, Monterey, California, USA

²Department of Systems Engineering, Naval Postgraduate School, Monterey, California, USA

Correspondence

Douglas L. Van Bossuyt, Naval Postgraduate School, Monterey, California, USA.
Email: douglas.vanbossuyt@nps.edu

Abstract

Microelectronics integrity is a critical issue for many industries including the Department of Defense (DoD). The military systems the DoD operates are particularly vulnerable to counterfeiting, with potentially costly or even catastrophic consequences. Counterfeits, regardless of production intent (malign or ersatz), raise significant concerns for industry and the DoD because they often demonstrate operational performance shortcomings, have lower reliability, or make components or organizations more vulnerable to attack. This article uses a systems dynamics modeling approach to explore the economics of counterfeiting for a sample system, the interactions between counterfeiters and the US Navy supply chain, and the impacts of counterfeit surveillance and detection to address the question: Is it more effective to target detection efforts at the component level or at the Line Replaceable Units level? A case study of an engine control module for the LM2500 propulsion turbine used on US Navy Arleigh Burke class guided missile destroyer (DDG-51) platforms is provided to demonstrate the approach.

KEYWORDS

counterfeit components, lowest, navy, replaceable unit, supply chain, system dynamics

1 | INTRODUCTION

Microelectronics integrity is a critical issue for the Department of Defense (DoD), and most modern defense systems include microelectronic components that share commonality with commercial systems. These defense systems are particularly vulnerable to counterfeiting, with potentially costly or even catastrophic consequences. A 2011 hearing by the Senate Armed Services Committee found that up to 15% of all DoD purchases of spare and replacement semiconductors may be counterfeit.¹ In response, section 818 of the 2012 National Defense Authorization Act (NDAA) established DoD requirements for counterfeit avoidance in electronics parts, and in May 2014, DFARS 252.246-7007 was issued to implement the NDAA provisions.² A counterfeit component may be malign (with adversarial intent to degrade capability or exfiltrate information) or ersatz (an inferior

substitute driven by a profit motive). Counterfeits, regardless of production intent, raise significant concerns for industry and the DoD because they often demonstrate operational performance shortcomings, have lower reliability, or make components or organizations more vulnerable to attack.³

Malign and ersatz counterfeits are driven by different motives with different underlying economic models. With malign counterfeits, competing state actors or other entities acting in bad faith are willing to fund the high costs associated with component development, insertion, and production and to accept a poor return on investment because profit is not the motive; the objective is degradation of operational readiness, or exploitation via other means. Strategic geopolitical competitors are capable and willing to invest in disruptive threats that can avoid verification and validation (V&V) detection in integrated circuits destined for national security and defense systems used by their

adversaries such as the case of the US and allied nations, Russia, and China.⁴ Ersatz counterfeits, on the other hand, tend to follow more traditional supply and demand economic models. In this case, suppliers use lower grade (including recycled) or lower cost parts to enhance profit margins. Over the years, a wide range of counterfeit microelectronic items have been observed, ranging from parts manufactured to lower quality standards, to legitimate parts that are recycled and already have significant usage time but are marketed as new and inserted into otherwise legitimate logistics chains.⁵ Regardless of the type of counterfeit part, significant risk exists that either the parts will not operate in the specified range of conditions, or operate at the necessary reliability levels.⁶

The following definitions are key to understanding this document:

1. Component: In this document, the term component refers to individual microelectronic elements (e.g., chips, resistors, inductors, etc.) that are assembled into a system's assemblies, including various line replaceable units (LRUs).
2. LRU: The LRU is the smallest element of a system replaced by field maintenance personnel. For microelectronics, this typically represents an individual circuit board (i.e., field technicians are not de-soldering and replacing individual chips on a board during normal maintenance and repair activities).
3. Counterfeit: SAE AS5553 – Counterfeit Electrical, Electronic, and Electromechanical (EEE) Parts; Avoidance, Detection, Mitigation, and Disposition defines a counterfeit component as “1. An unauthorized (a) copy, (b) imitation, (c) substitute, or (d) modified EEE part, which is knowingly, recklessly, or negligently misrepresented as a specified genuine item from an original component manufacturer or authorized aftermarket manufacturer; or 2. A previously used EEE part or a part which has been modified, and is knowingly, recklessly, or negligently misrepresented as new without disclosure to the customer that it has been previously used.”⁷
4. Ersatz: is defined as “being a usually artificial and inferior substitute or imitation.”⁸ The term is used in this article to identify counterfeits produced purely for-profit motive.
5. Malign: Is defined as “evil in nature, influence, or effect.”⁹ The term is used in this article to identify counterfeits produced with the goal of causing intentional harm.

Economic models and the impact of counterfeit prevention efforts are of high interest for the DoD to aid in policy and strategy decision making. The modeling presented in this article simulates counterfeit detection efforts at different points in a notional supply chain to explore the overall interdiction effectiveness and predicted economic effect of focusing efforts earlier or later in the process. This article explores the macroeconomics of counterfeiting for a sample system, the interactions between counterfeiters and the US Navy supply chain, and the impacts of counterfeit surveillance and detection to address the question: Is it more effective to focus detection efforts at the component level or at the LRU level? To understand the interplay between these concepts, Systems Dynamics Modeling is employed, with simulation performed using Stella Architect software, version 3.2.1, by ISEE

Systems. This work is relevant to systems engineering because the impacts of counterfeit components on supply chains must be understood early during the system design process, so that the risk can be appropriately managed throughout the system design lifecycle.¹⁰ The specific system of interest modeled for this analysis is a notional engine control module for the LM2500 propulsion turbine used on US Navy Arleigh Burke class guided missile destroyers (DDG-51). While the system of interest and the supply chain are specific to the US Navy, the broader implications of this article are applicable to the defense sectors and the national defense of many countries. Further, the growing understanding of the integral role of the 16 critical infrastructure sectors,¹¹ including the defense sector, in ensuring both short-term safety and welfare and long-term standards of living of all countries shows that counterfeit surveillance and detection is important writ large. The modeling and simulation results presented here will be of interest to DoD acquisition professionals, including Secretariat positions that set acquisition policy, Program Managers who lead systems acquisition efforts, and In-Service Engineering Agents and logisticians who support fielded systems throughout their lifecycle. In addition, the article will be of interest to standards organizations that establish and maintain the industrial standards that drive counterfeit detection processes, and prime contractors that supply complex defense systems.

2 | BACKGROUND

In July 2017, President Trump issued Executive Order (EO) 13806, Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States. The EO recognized that, “The ability of the United States to maintain readiness, and to surge in response to an emergency, directly relates to the capacity, capabilities, and resiliency of our manufacturing and defense industrial base and supply chains,” and states that, “Strategic support for a vibrant domestic manufacturing sector, a vibrant defense industrial base, and resilient supply chains is therefore a significant national priority.”¹² EO 13806 ordered the Secretary of Defense, in coordination with Secretaries and heads of agencies deemed appropriate, to conduct an “Assessment of the Manufacturing Capacity, Defense Industrial Base, and Supply Chain Resiliency of the United States.”¹² The report, delivered in 2018, was developed by a DoD-led interagency task force comprised of 16 working groups with approximately 300 subject matter experts. The report identified several risks, vulnerabilities, and shortfalls in the Defense Industrial Base (DIB) and Supply Chain that affect national security. This included the finding that “Imports of electronics lack the level of scrutiny placed on US manufacturers, driving lower yields, higher rates of failure in downstream production and raising the risk of ‘trojan’ chips and viruses infiltrating US defense systems.”¹³

Subsequently, in September 2021, President Biden issued EO 14017 that directed six Federal Agencies to review industrial bases in order to strengthen and secure a spectrum of America's supply chains, and directed the Secretary of Defense to submit a report to include key

vulnerabilities and courses of action intended to strengthen the DIB.¹⁴ In February 2022, the DoD released their report, "Securing Defense-Critical Supply Chains: An action plan developed in response to President Biden's Executive Order 14017." The subsection of that report entitled Microelectronics, cited the Senate Armed Services Committee Report on Counterfeit Components in the DoD Supply Chain (# 112-167, May 21, 2012) reiterating that "Counterfeit microelectronics components represent a serious safety and national security threat due to their degraded reliability. Counterfeit microelectronics components have been identified in multiple DoD systems."¹⁵

America's and Europe's Semiconductor foundry capability has predominantly moved offshore. North and South America, Africa, and Europe are heavily dependent on foreign manufacturers and suppliers for most of their semiconductors, including those that are used in defense systems. The Semiconductor Industry Association's State of the Industry's Report in 2022 stated that 75% of global manufacturing capacity, from fabrication to packaging of leading-edge chips, is located in Asia.¹⁶ To build trusted defense systems, the DoD and other national defense organizations need a secure supply chain so that the DIB has access to trusted and assured microelectronics. To complicate matters, there is no standardized V&V process to ensure the software and tools being used in the manufacturing process can be trusted. The scope of the problem extends from design to fabrication to operations, and without a solution, the DIB and commercial industry have no clear path to obtain trusted components for national security or commercial purposes. Microelectronics supply chains that have become highly disaggregated, primarily through facilities in Asia, represent potential security vulnerabilities. The outsourcing of fabrication and testing by fabless semiconductor companies represents an opportunity for the introduction of security vulnerabilities, whether inadvertent or through malign intent. This is of particular concern for chips intended to be used in critical national security infrastructure or defense systems purchased by national defense organizations such as the DoD.³

2.1 | Current practices

Current industrial practice is to mitigate the risk of counterfeit microelectronics via policy. Prime contractors (principal end-item suppliers, final system providers, that is, the brand associated with the final product) require compliance with standards that specify microelectronics procurement from authorized sources such as original equipment manufacturers (OEMs), original component manufacturers (OCMs), or approved distributors, and entail risk assessments and elevated approvals when components must be purchased from other sources. This appears to have been historically successful, as according to Meshel in Aerospace Report TOR-2014-02161, only 0.4% of Government-Industry Data Exchange Program (GIDEP) documents on counterfeit parts from 2009 to 2013 were related to those from Authorized Distributors¹⁷; however, the problem of counterfeit products persists, especially in the context of Diminishing Manufacturing Sources and Material Shortages (DMSMS).

The prevailing industrial standard used to address counterfeit microelectronics in both the civilian and defense sectors is SAE International's AS5553 Counterfeit Electrical, Electronic, and Electromechanical (EEE) Parts: Avoidance, Detection, Mitigation, and Disposition.¹⁸ AS5553 refers to many associated standards including: ARP6178 Counterfeit Electrical, Electronic, and Electromechanical (EEE) Parts: Tools for Risk Assessment of Other than an Authorized Source¹⁹; AS6081 Counterfeit Electrical, Electronic, and Electromechanical (EEE) Parts: Avoidance, Detection, Mitigation, and Disposition—Independent Distribution²⁰; and AS6171 Test Methods Standard; Counterfeit Electronic Parts.²¹ Primes and integrators specify AS5553 and the requirements are flowed down to all sub-contractors and suppliers. There are additional standards and certifications in this domain such as Components Technology Institute, Inc. certification CCAP-101 – Counterfeit Components Avoidance Program, Certification For; and the Independent Distributors of Electronics Association (IDEA) IDEA-STD-1010 – Acceptability of Electronic Components Distributed in the Open Market. The following three examples demonstrate the commonality of this policy-based approach.

Lockheed Martin, a major defense company, has a dedicated web page²² related to counterfeit management, which states "Lockheed Martin requirements are to always procure from the OCM/OEM or their authorized distributors. If an occurrence arises where that is not possible, prior approval from Lockheed Martin is required. When requesting approval through your supply chain representative a risk mitigation plan will be needed which details the inspections and tests that will be performed to authenticate the product, including acceptance criteria. ... Typical control plan requirements are defined in industry standards such as AS5553 for electrical parts ... It is required that counterfeit avoidance requirements be flowed down to the lowest level of the supply chain." This indicates the seriousness that Lockheed Martin ascribes to the potential of counterfeit parts in their supply chains, and their policy approach to addressing the issue.

Boeing, a major defense and commercial aviation company, publishes the contract clause they use related to counterfeit microelectronics.²³ The clause states "If Seller provides Electronic, Electrical or Electromechanical (EEE) parts or assemblies containing EEE parts, Seller shall implement a counterfeit electronic parts detection and avoidance system compliant with the requirements of SAE standard AS5553. ... Seller bears responsibility for procuring authentic parts or items from its subcontractors and shall ensure that all such subcontractors comply with the requirements of this Article." This shows that Boeing puts the impetus of counterfeit detection upon their suppliers.

Teledyne FLIR, a major commercial and consumer electronics, and defense supplier, publishes their "Quality Assurance Provision 26 – Counterfeit Parts" on the web.²⁴ It states that "Supplier shall comply with SAE AS5553 to prevent and mitigate the use of counterfeit parts for both electrical and non-electrical components supplied to FLIR. ... The supplier shall flow down the applicable requirements of AS5553 to applicable sub-suppliers." Like Boeing, Teledyne FLIR requires suppliers to ensure that parts are not counterfeit.

Each company refers to specific functional personnel in their counterfeit management process. Per the publicly available documents referenced above, Lockheed directs subcontractors and suppliers to engage with their “supply chain representative,” Boeing refers inquiries to a “buyer’s authorized procurement representative,” and FLIR refers inquiries generically to the “buyer and/or contracting officer.”

Information is not readily available on the counterfeit mitigation practices of small businesses and other non-major system developers. Many such businesses may not be large enough to sustain their own in-house capability for counterfeit mitigation. To service this need, there are a multitude of companies^{25–28} that provide services related to counterfeit electronics mitigation such as supply chain management, inventory management, sourcing and authentication, assessment and inspection, and sales of pre-inspected/validated components.

AS5553 and associated standards address counterfeit electronics avoidance, detection, mitigation, and disposition. For avoidance, AS5553 prescribes procurement of parts via authorized sources, defined as “Original component manufacturers and OCM-authorized sources of supply for an EEE part (i.e., franchised distributors, authorized distributors), and authorized aftermarket manufacturers.”¹⁷ When authorized sources are unavailable, ARP6178 recommends the supplier risk assessment outlined in AS6081, which assesses suppliers based on business records (e.g., company name history), history of reported counterfeits, quality management system certifications, geographic locations, material control procedures, personnel training, facilities, etc.¹⁹

For detection, the standards first specify the validation of authenticity through supply chain traceability records. In addition, for any suspected counterfeit parts or for parts for critical applications, standard AS6171 specifies multiple detection methods including “external visual inspection, radiological inspection, x-ray fluorescence, de-lid/de-capsulation or destructive physical analysis, electrical tests, acoustic microscopy, optical/SEM (Scanning Electron Microscope) inspection, and thermal analysis.”²⁰

AS5553 specifies that risk mitigation is planned and documented in a risk mitigation plan. The plan must include a classic risk assessment, which assesses the likelihood of receiving a counterfeit part and the consequence of installing that counterfeit part. In addition, the plan must outline the process for risk mitigation, including the inspections, tests, documentation, and criteria for part acceptance or rejection.¹⁷

AS6081 addresses disposition of counterfeit parts. The standard prescribes a quarantine of suspected and confirmed counterfeits, with physical barriers and personnel access controls to ensure items are not reintegrated with the legitimate inventory. Parts are not to be removed from quarantine except to perform independent verification testing, and parts are to be retained in accordance with all customer, statutory, and regulatory requirements. Once testing has been completed, parts are to be destroyed or surrendered to the authority having jurisdiction.¹⁹

Counterfeit microelectronics present an intriguing risk construct, with multiple risk stakeholders. Per the aforementioned standards, the requirements for counterfeit mitigation are flowed down through the entire supply chain. As such, the financial and legal risk are flowed

down as well; however, the Prime contractor retains the predominance of the reputational risk, and the end user retains the operational risk. For example, if a Lockheed Martin aircraft crashed because of a counterfeit component, the component supplier may be liable, but Lockheed Martin would suffer substantial loss of reputation and product confidence, and the aircraft crew would experience the acute risk to life. Gaining insight into the contractual, financial, and legal relationships between companies in the supply chain to inform how they share risk would require targeted investigation and willing transparency, and is beyond the scope of this article.

Much progress has been made over the last 5 years to mitigate both defense industry and commercial microelectronic industry supply chain vulnerabilities. This includes the DoD’s Trusted and Assured Microelectronics activities (including the SCALE²⁹ academic consortium), the CHIPS and science ACT,³⁰ and an increased awareness of the need for technological advances in semi-conductor fabrication, more rigorous V&V of microelectronic components and LRUs, more visibility into both ersatz and malign counterfeiting of LRUs and components, and supply chain risk management (SCRM) strategies to counter the threat counterfeiting poses to the DoD and commercial supply chains.³¹ That said, the authors of this article posit that the US and specifically the DoD need to agree upon a focused and comprehensive strategy to increase US microelectronics resilience, security, and competitive economic viability in both the near and long term. The authors suggest that the rest of the world should follow suit.

2.2 | Employment strategy

The model described in this article explores the time-phasing of counterfeit detection efforts, not the process or technical approach for detecting counterfeits. As such, it delivers unique insights to supply chain managers, standards committees, policy developers, and investigation agencies. These stakeholders may all benefit from enhanced information regarding the level of effort, effectiveness, and predicted economic impacts of counterfeit inspections at various stages of the supply chain. In addition, once calibrated and validated with actual data, the model could be used “in reverse” to predict levels of counterfeit activity based on economic conditions and trends.

There is substantial ongoing research in counterfeit detection methods^{32,33} and product quality validation techniques,³⁴ and ongoing development of specs and standards by various professional societies and committees. To the authors’ knowledge, there is no other ongoing work related to the timing of counterfeit detection efforts in the supply chain and associated economic effects.

In an applied context, the concepts developed in this article could be employed by DoD and industry when developing program acquisition strategies (e.g., identifying specific points of counterfeit inspection in the supply chain for new systems) and in the sustainment of currently fielded systems (e.g., accepting more risk with regards to item suppliers for out of production components, when counterfeit inspection efforts are available to be performed at the end of the supply chain immediately prior to acceptance.) In addition, the modeling demonstrated

here could be adapted and validated with specific information for a variety of defense systems for which a program manager may have specific data, to inform overall counterfeit risk for the system under their purview.

2.3 | System dynamics

System dynamics (SD) was developed by Jay Forrester in the 1950s. SD entails both qualitative and quantitative techniques to model and simulate the behavior of systems based upon their structure and the relationships of system elements. SD modeling is employed across many disciplines including “engineering, manufacturing, economics, and social sciences to enhance decision-makers’ understanding of systemic behavior in real-world systems.”³⁵ SD modeling helps decisionmakers understand potential behavioral outcomes of a system over time.³⁶

Within the systems engineering domain, SD modeling has been used for a variety of purposes including systems engineering studies of supply chains.³⁷ SD has also been adapted to analyze systems engineering design processes,³⁸ to estimate project performance from a systems engineering perspective,³⁹ to understand safety culture in manufacturing plants,⁴⁰ and to support the rapid evaluation of supply chain and demand signals at the national level.⁴¹ System dynamics has long been considered for modeling the optimization of inventory and production dynamics for policy analysis.⁴² Two common techniques in system dynamics modeling include causal loop diagrams (CLDs), and Stock and Flow models. Research in 2005, for example, used CLDs and system dynamics modeling to analyze Taiwan’s semiconductor industry.⁴³ A variety of systems analyses have been supported by SD and are available in the literature.⁴⁴ Thus, it is within the scope of systems engineering practitioners to use SD for many different activities within the systems engineering design process.

3 | A NOTIONAL SYSTEM DYNAMICS MODEL OF COUNTERFEIT COMPONENTS AND LRUS IN THE US NAVY DDG SUPPLY CHAIN

3.1 | Description of the notional system dynamics model

The model developed for this study is structured as a network of four interdependent modules, including (1) an LRU Demand module, (2) an LRU Production and Counterfeit Detection module, (3) a Production Control module, and (4) an Economics module. The model also includes a dedicated user interface with a constrained set of adjustable model parameters to facilitate analysis. The overall architecture of the model, showing the four interdependent modules, is shown in Figure 1.

The LRU Demand module simulates the demand for LM2500 engine control LRUs over the ten-year simulation period by aggregating DDG demand for new and replacement LRUs as well as industrial demand. LRU demand was calculated using Department of Navy historical data

Impact of Counterfeit Components and LRUs on US Navy LM 2500 Engine Control LRU Supply

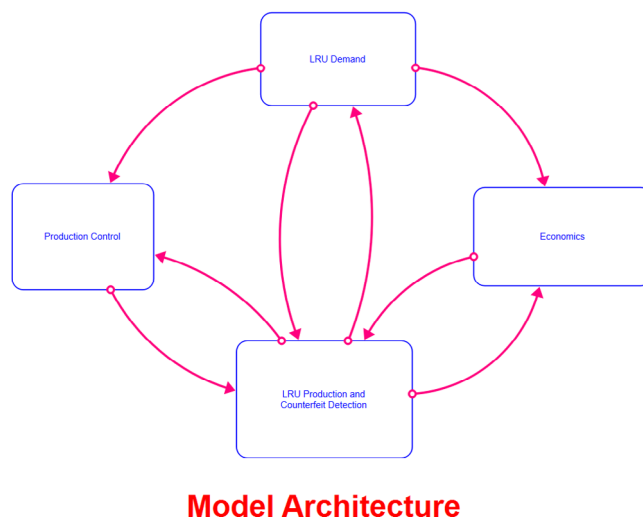


FIGURE 1 Basic architecture of the system dynamics model developed for this investigation.

for DDG production (i.e., DDG demand for new LRUs),⁴⁵ the authors’ estimated failure rates for the blended pool of genuine and counterfeit LRUs (i.e., demand for replacement LRUs), and estimated historical LRU production based on GE press release materials (i.e., industrial demand for new LRUs).^{45,46} The output of the LRU Demand module serves as an input to both the LRU Production and Counterfeit Detection module and the Production Control module.

The LRU Production and Counterfeit Detection module models the production of legitimate LRUs, the production of counterfeit LRUs, and the detection and removal of counterfeit components and LRUs from the supply chain. The model represents production of LRUs through four steps of a simplified supply chain process, including (1) component production, (2) component distribution, (3) LRU assembly, and (4) LRU distribution. At each of these four steps, the model applies a probability that some of the items become counterfeit (via insertion of counterfeit product or tampering with legitimate product). The counterfeit supply chain is modeled as a logically parallel process that is fed by the counterfeit items that branch off from the legitimate production process. The counterfeit detection portion of this module implements counterfeit detection and removal steps on both the counterfeit component inventory and the counterfeit LRU inventory along the counterfeit production path. Any detected counterfeits are removed from the counterfeit supply chain process at these two points and are aggregated in a quarantine stock. The overall output of this module is a mix of legitimate LRUs to the supply inventory, counterfeit LRUs that made it into the supply inventory, and a count of the detected and quarantined counterfeits from the simulation run.

The production process is tuned by the Production Control module, which applies a proportional-integral-derivative (PID) control logic to adjust production rates based on LRU supply versus LRU demand. To mitigate various model limitations, this common control logic approach

was applied to govern production and ensure that production tracks demand as the simulation evolves so that the market price is not driven to extremes by significant supply/demand misalignments. The module implements a simple PID control approach that compares the LRU production volume versus the LRU order volume (the “error”) and calculates a proportional term (based on the instantaneous error), an integral term (based on the cumulative error), and a derivative term (based on the rate of change of the error). These terms are each tuned by a user-adjustable gain factor and then aggregated into a single value that is applied as a multiplier to component production at the beginning of the supply chain. Note: the production control value is constrained as non-negative because logically it cannot drive the supply chain in reverse (i.e., a component producer cannot produce negative amounts of product.)

The Economics module simulates the market price of the notional LM2500 engine control LRU based on LRU supply versus demand and a projected economic inflation rate over the simulation period. In this model, a market price stock is influenced by LRU order volume (i.e., demand), LRU production (i.e., supply), and a price growth value based on actual inflation rates over the time period of the simulation.

Each module is comprised of a detailed stock and flow model structure. While Figure 1 shows the overall module relationships, Figure 2 reveals some of the complexity within each module. The models within each module are described in detail in Appendix A.

3.2 | Constraints and limitations

It is important to note the model’s limitations. This is not a comprehensive supply chain model, and it does not fully represent the complex supply chain dynamics associated with a multi-step production and assembly process with variable and uncertain demand (such as the supply chain bullwhip effect). The model is simplified in several ways. First, production is tuned to fulfill the demand with no consideration for economic outcomes for component or LRU producers (i.e., there is no profit calculation at any step along the production flow, or corresponding business decisions by any of the performers to stop, slow, maintain, or accelerate their production). Second, component production rates are driven directly by the total end-product demand, and not by a demand signal from the next logical step in the supply chain (i.e., product demand is a direct input to the beginning of the supply chain at the first production step, as opposed to a realistic supply chain with demand signals cascading from the final supplier down progressive steps of the supply chain through assemblers and integrators to original component sources). Third, the model does not account for decommissioning of LM2500 propulsion turbines used on Navy DDG platforms (i.e., in the model, all LM2500s ever produced are presumed still to be operational and feeding the demand for spare parts). Fourth, the model does not include variable failure rates to represent the dynamic operating environment of the Navy including things like battle damage, variations in operating tempo, deferred maintenance, etc. Fifth, the model does not include Navy demand for turbines on platforms other than the DDG. Last, LM2500 production was estimated

to be uniform and linear over time (i.e., exactly 55 per year, every year, since 1969) and does not reflect production ramp-up or high/low production years.

3.3 | Model initialization

To maximize the utility of this model, it is initialized with the most accurate open-source data available to the authors at the time of model development. The model simulation start time is initialized as November 2012 to achieve 120 months (10 years) of run time through November 2022. The initial quantity of DDGs is set to 62 to match the actual starting quantity of active DDGs in the year 2012. Each DDG has four LM2500 turbine engines per ship, and it is presumed that each LM2500 has redundant engine control systems with 2 LRUs per turbine, totaling 8 LRUs per ship. Initializing the model with 62 DDGs equates to 496 LRUs installed in the fleet ($62 \times 8 = 496$). For this simulation, it is assumed that the Navy maintains 10% spares resulting in 50 LRUs in supply inventory.

To model commercial demand for the same engine control LRU, LM2500 turbine production was calculated to be approximately 55 per year since 1969 based on General Electric press release materials.^{46,47} At 55 turbines per year, with two LRUs per turbine control system, this equates to approximately nine LRUs needed per month to support new production ($55 \times 2 / 12 = \sim 9$). The deployed commercial inventory of LRUs on LM2500s at simulation start time (t_0) is $(2012 - 1969) \times 55 \times 2 = 4730$. Of note, based on the model architecture that employs a blended inventory of genuine and counterfeit components, and the lack of available data on Navy and commercial failure rates for authentic and counterfeit LRUs, the authors estimated the LRU failure rate distribution.

4 | SIMULATION RUNS/RESULTS

This model can be used to explore a variety of counterfeit production, detection, demand, and economic issues. As an example of the utility of the model, this study now explores the research question: Is it more effective to target detection efforts at the component level or at the LRU level? Effectiveness herein refers to the percentage of counterfeits that are detected and removed from the supply chain—the more effective the approach, the fewer counterfeits make it through into the inventory.

To illustrate its potential utility, the model was used to run a series of 33 simulations, varying the component detection percentage from 100% to 0% while inversely varying the LRU detection percentage from 0% to 100%. These factors were varied in 10% increments and performed via three runs at each setting. The results are shown in Table 1.

Although this represents a limited number of runs and there are other model variables which may affect the outcome, the data shows that it is more *effective* (in overall percentage of counterfeits detected) to target detection efforts at the LRU level instead of at the component level, but more *efficient* (counterfeits detected per labor hour of

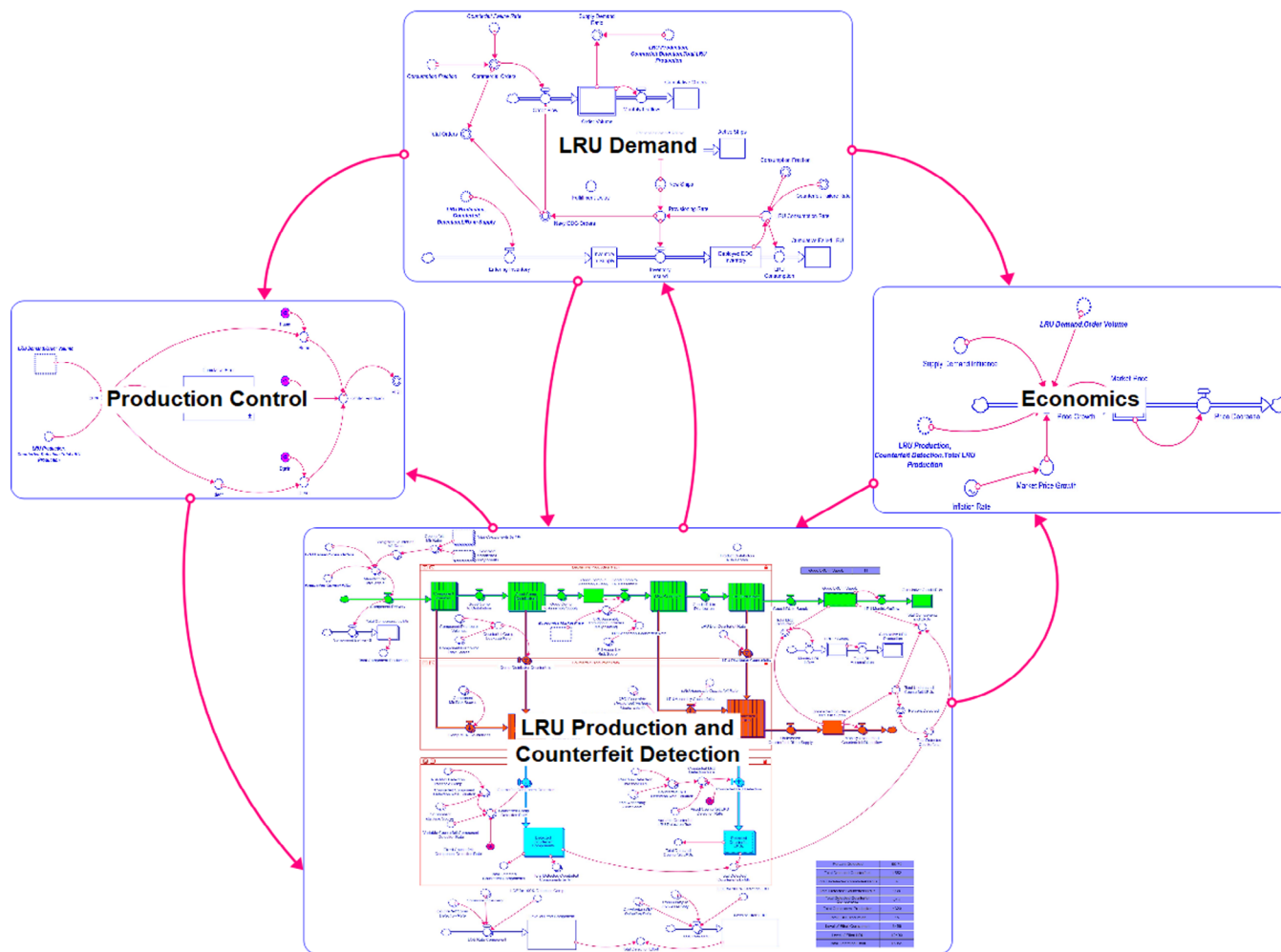
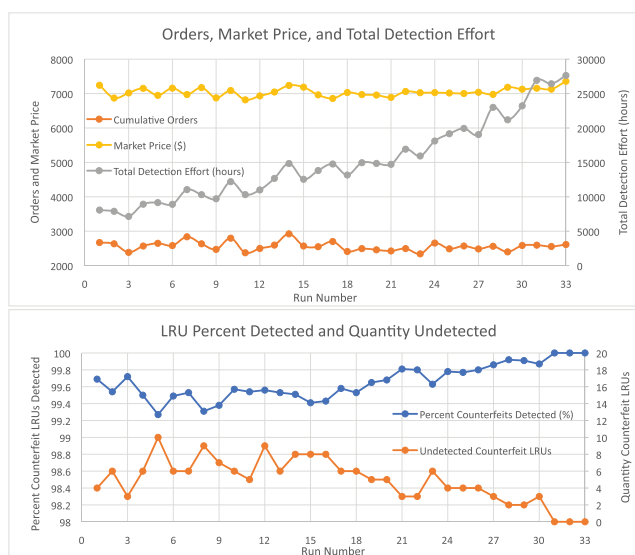


FIGURE 2 Overall module relationship structure with additional detail shown for each module.

TABLE 1 Selected runs exploring the effect of component and LRU detection levels on total undetected counterfeit LRUs entering the market.

Counterfeit Component Detection Rate (%)	Counterfeit LRU Detection Rate (%)	Percent Counterfeits Detected (%)	Cumulative Orders	Total Detection Effort (hours)	Market Price (\$)	Undetected Counterfeit LRUs
100	0	99.69	2672	8074	\$ 7,243	4
100	0	99.54	2634	7893	\$ 6,871	6
100	0	99.72	2386	7152	\$ 7,019	3
90	10	99.5	2570	8925	\$ 7,152	6
90	10	99.27	2649	9157	\$ 6,949	10
90	10	99.49	2583	8910	\$ 7,158	6
80	20	99.53	2838	11045	\$ 6,972	6
80	20	99.31	2634	10313	\$ 7,174	9
80	20	99.38	2472	9713	\$ 6,875	7
70	30	99.57	2798	12201	\$ 7,089	6
70	30	99.54	2374	10324	\$ 6,818	5
70	30	99.56	2499	11004	\$ 6,933	9
60	40	99.53	2597	12675	\$ 7,046	6
60	40	99.51	2923	14842	\$ 7,238	8
60	40	99.41	2571	12549	\$ 7,187	8
50	50	99.43	2549	13818	\$ 6,962	8
50	50	99.58	2701	14768	\$ 6,859	6
50	50	99.53	2411	13165	\$ 7,031	6
40	60	99.65	2494	14957	\$ 6,971	5
40	60	99.68	2459	14851	\$ 6,957	5
40	60	99.81	2426	14719	\$ 6,890	3
30	70	99.80	2495	16921	\$ 7,062	3
30	70	99.63	2342	15935	\$ 7,026	6
30	70	99.78	2656	18110	\$ 7,028	4
20	80	99.77	2488	19163	\$ 7,017	4
20	80	99.8	2571	19942	\$ 7,003	4
20	80	99.86	2485	19046	\$ 7,039	3
10	90	99.92	2563	23002	\$ 6,977	2
10	90	99.91	2400	21189	\$ 7,184	2
10	90	99.87	2586	23219	\$ 7,128	3
0	100	100	2595	26932	\$ 7,156	0
0	100	100	2556	26426	\$ 7,129	0
0	100	100	2613	27629	\$ 7,359	0



detection effort) to target detection efforts at the component level. This makes sense because counterfeit LRU detection will effectively catch both counterfeited LRUs and counterfeit components within otherwise legitimate LRUs. Two notable observations that may be drawn from this are that inspection at the LRU level is more labor intensive, as there are more components to inspect when aggregated into an LRU. This also drives the market price of the LRU to increase with the increased percentage of detection. This also makes sense because the price is affected by supply and demand via the ratio of LRU orders to LRU production. When more counterfeit LRUs are removed from the market, production is effectively lowered and will fall short of orders, driving the price up for the items available on the market (i.e., demand outstrips supply.)

5 | DISCUSSION

As stated earlier, this article was intended to demonstrate the value of using system dynamics modeling to explore the timing of counterfeit detection efforts in the microelectronics supply chain, and to address the question: Is it more effective to target detection efforts at the component level or at the LRU level? This approach can support Navy, DoD, other US Government and partner nation agencies, industry efforts, and professional standards organizations to better understand and more effectively counter the introduction and detection of both ersatz and malign counterfeits. Based on the study results, the defense industry should focus counterfeit detection efforts later in the supply chain to preclude the opportunity for additional counterfeit parts insertion after detection efforts have been performed. In addition, this approach and the results from this study can guide research and development in microelectronics inspection technologies. The defense industry would benefit from detection systems capable of employment at the tail end of the supply chain that are capable of rapidly, nondestructively, and effectively assaying LRUs and other microelectronics assemblies.

While the case study focused on a Naval defense application, the conclusions may be useful for all 16 critical infrastructure segments. For instance, hospitals and medical facilities often have backup generators and power management systems, which rely on several microelectronics LRUs. Counterfeit components could cause backup generators to fail during times of crisis and could lead to negative patient outcomes. Similarly, many nuclear and hydroelectric power plants have large backup generators to support plant operations during times of off-site power loss, and counterfeits reduce the reliability and availability of these backup power systems. More broadly, microelectronics are not exclusive to engines and generators and are found across almost all critical infrastructure sectors from banking and finance to agriculture.

From a systems engineering perspective, system dynamics modeling offers practitioners an opportunity to explore a variety of lifecycle management problems associated with counterfeit parts and to compare the benefit of different policies to address these. System of systems and complex systems engineering is proving to be a critical aspect of supply chain design and management. As part of a MBSE approach to systems engineering, system dynamics is a valuable tool for both planning and analysis.⁴⁸

It should be noted that the value of any modeling and simulation is largely dependent on the availability and validity of relevant data. When dealing with the extent to which counterfeiting is being introduced into products deliberately or by upstream sources, suppliers are often reluctant or unable to provide this data. Given this reality, practitioners should be careful to populate their models with data from reliable sources that is verifiable, and appropriately caveat the data and assumptions used. Despite the fact the model developed for this study was notional due to the lack of publicly available counterfeit data for the system under investigation, the approach illustrates the potential of SD modeling in a systems engineering context, for supply chain applications and stakeholders.

6 | CONCLUSION

Government and industry stakeholders are making progress toward increasing the resilience of the microelectronics supply chain; however, significant gaps persist in the identification and mitigation of ersatz and malign counterfeit components and LRUs introduced by suppliers. Efforts to expand the capability and capacity of the DIB and US fabrication laboratories primarily focus on microelectronics design and fabrication technologies and advances in STEM education. While this includes methods to identify and protect against the introduction of counterfeit items, the lack of transparency provided by suppliers represents a significant challenge in the modeling and analysis of the microelectronics supply chain.

The modeling done in this research was notional due to the lack of available data from suppliers and the defense industry related to the extent of counterfeits being introduced into Navy systems. As such, a goal of this modeling was to demonstrate the potential value of understanding the system dynamics associated with a small segment of the U.S. Navy's microelectronics supply chain; specifically, the timing of counterfeit detection efforts, and the impact of counterfeit components and LRUs on market cost. While system dynamics modeling is not intended to be predictive in nature, it may enhance the awareness of underlying non-linear relationships that result in problematic supply chain behavioral outcomes. All critical industries including the defense industry may benefit from a better understanding of counterfeit detection as shown in this study.

In addition, this research informs future related work in detection means and methods. The results of the simulation indicate the need for nondestructive assay methods that can be applied as late in the supply chain as possible, with the capability to assess integrated components at the LRU level (versus at the individual chip level.) Logically, the later in the supply chain that detection methods can be applied, the fewer chances there are for additional insertion of counterfeits, and the more important it is not to destroy the item under investigation.

6.1 | Future work

In its current form, this model has the utility to explore a variety of counterfeit detection decisions and outcomes. This makes it a valuable

tool for stakeholders who are looking for a mathematical basis to develop qualitative comparisons between strategies. While there is value in the current state of the model, there are several areas where the model could be refined, extended, or otherwise improved to support future research and analysis.

The current model does not incorporate real world data on LM2500 production. In fact, very little actual data is publicly available regarding the introduction of counterfeit components and LRUs in defense systems. To better develop and validate the model, better LM2500 production history data from General Electric is needed, as is microelectronics counterfeiting data in general. To achieve better model performance, it will be necessary to integrate real world data into the model and tune the variables and algorithms so that it can provide more accurate behavioral trend analysis over an extended time horizon. This is a challenge for two reasons. First, there is limited public data on counterfeit detection rates, which makes validation of a broadly applicable model and generalizable conclusions difficult. Second, from the defense context, data related to counterfeit components and LRUs, and aggregation of counterfeiting rates and detection, is sensitive and often classified, which challenges academic utility. This shows the need to collect such data to facilitate analyses in this domain. It is hoped that future modelers will have access to real-world data that provides the fidelity necessary to support ongoing efforts to better identify, track, and reduce the introduction of counterfeit microelectronic components in supply chains. Alternatively, the model developed in this article can be adapted with proprietary or non-public data for further analysis within a secure environment.

The model used for this study was fit for purpose at a certain level of analysis to demonstrate the value of a system dynamics approach in pursuing a design solution through systems engineering. Currently, the model follows the sequential flow of production: components are produced and assembled into LRUs which are then distributed into the supply system. From an economic perspective, demand for LRUs drives demand for components. If stakeholders want this model to better reflect the economics of manufacturing, the model should be updated to reflect real supply chain dynamics by having the demand for LRUs feed the LRU distributors, which should in turn drive demand on LRU producers, which should sequentially cascade the demand signal down each step of the production flow process. While the current model follows the sequential flow of production, increased fidelity can be introduced through economic considerations associated with each step of the production flow such as profit margin for each entity (producer/distributor); go/no-go, or stop/slow/hold/accelerate decision logic for each entity based on profitability; and, capacity objectives and limits for each entity (e.g., maximum production capacity).

The current model allows users to enter a limited number of specific counterfeit detection rates. A more automated and adaptive model would incorporate economics into the counterfeit detection flow (e.g., cost and benefit to inspect at each point in time, which can drive adaptive strategies). Since the current model does not specify whether it is "cleared" workers or unvetted workers performing screening at the various links in a supply chain, further model development could incorporate multi-stage/multi-entity counterfeit detection.

The utility of the model can be expanded by allowing the user to adjust the number of LRUs to reflect other shipboard systems, though they would also need to adjust the production history and commercial demand (if applicable) for the corresponding system. Further, since the current model traces a single counterfeit component that is inserted into a single LRU, model fidelity can be increased by adding the ability to import a system hierarchy of components with multiple components per LRU.

To ensure that this work adds value, the authors plan to socialize this work with a variety of potentially interested stakeholders including various DoD program managers, standards organization committees, and organizations such as the Defense Microelectronics Activity (DMEA). DMEA works on production of trusted microelectronics, provides radiation effects testing, develops microelectronics acquisition strategies, and conducts specialized engineering/re-engineering for critical military applications or systems with DMSMS issues.

ACKNOWLEDGMENTS

The views presented are those of the authors and do not necessarily represent the views of the Navy, DOD, or the US Government. Approved for Public Release; distribution is unlimited.

DATA AVAILABILITY STATEMENT

The data that support the findings of this study are available from the corresponding author upon reasonable request.

ORCID

Douglas L. Van Bossuyt  <https://orcid.org/0000-0001-9910-371X>

REFERENCES

1. United States Senate. The Committee's Investigation into Counterfeit Electronic Parts in the Department of Defense Supply Chain—Hearing before the Committee on Armed Services, 8 Nov 2011, S. HRG. 112-340. US Senate; 2011.
2. US Congress. H.R.1540 – National Defense Authorization Act for Fiscal Year 2012. 112th US Congress; 2012.
3. Dyatkin B. While transistors slim down, microchip manufacturing challenges expand. *MRS Bull.* 2021;46:16-18. Accessed July 7, 2023. <https://link.springer.com/article/10.1557/s43577-020-00001-3/>
4. Clark B, Patt D. *Regaining the Digital Advantage: A Demand-Focused Strategy for US Microelectronic Competitiveness*. Hudson Institute; 2021. Accessed July 7, 2023. <https://www.hudson.org/national-security-defense/regaining-the-digital-advantage-a-demand-focused-strategy-for-us-microelectronics-competitiveness/>
5. Guin U, Huang K, DiMase D, Carulli JM, Tehranipoor MM, Makris Y. Counterfeit integrated circuits: a rising threat in the global semiconductor supply chain. *Proc. IEEE.* 2014;102(8):1207-1228.
6. Caswell G. Counterfeit detection strategies: when to do it /how to do it. *International Symposium on Microelectronics.* 2010;2010:000227-000233. doi:10.4071/isom-2010-TP2-Paper5
7. SAE International. *Counterfeit Electrical, Electronic, and Electromechanical (EEE) Parts; Avoidance, Detection, Mitigation, and Disposition*. AS5553D. SAE International; 2022.
8. Ersatz. Merriam-Webster. Accessed December 19 <https://www.merriam-webster.com/dictionary/ersatz/>, 2022.
9. Malign. Merriam-Webster. Accessed December 19. <https://www.merriam-webster.com/dictionary/malign/>, 2022.
10. Blanchard BS, Fabrycky WJ. *Systems Engineering and Analysis*. 5th ed. Prentice Hall; 2011.

11. Cybersecurity and Infrastructure Security Agency. Critical Infrastructure Sectors. Accessed July 4, <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/>. 2024.
12. US Executive Office of the President. *Executive Order 13806 of July 21, 2017*. US Executive Office of the President; 2017.
13. US Government Interagency Task Force. *Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States*. US Government Executive Branch; 2018.
14. National Archives and Records Administration. Federal Register Notice of Request for Written Comments in Support of the Department of Defense's One-Year Response to Executive Order 14017, "America's Supply Chains. *Federal Register*. 86(185). National Archives and Records Administration; 2021.
15. US Department of Defense. *Securing Defense-Critical Supply Chains: An Action Plan Developed in Response to President Biden's Executive Order 14017*. US Department of Defense; 2022.
16. Semiconductor Industry Association. *2022 State of the U.S. Semiconductor Industry*. Semiconductor Industry Association; 2022.
17. Meshel D. Counterfeit Parts Prevention Strategy Guide Product Overview. Aerospace Report No. TOR-2014-02161, Accessed April 8, <https://aerospace.org/sites/default/files/maiw/TOR-2014-02161.pdf/>. 2024.
18. SAE International. *Counterfeit Electrical, Electronic, and Electromechanical (EEE) Parts: Avoidance, Detection, Mitigation, and Disposition—Aerospace Standard AS5553*. SAE International; 2022.
19. SAE International. *Counterfeit Electrical, Electronic, and Electromechanical (EEE) Parts: tools for Risk Assessment of Other than an Authorized Source (e.g., Independent Distributors)—Aerospace Recommended Practice ARP6178A*. SAE International; 2023.
20. SAE International. *Counterfeit Electrical, Electronic, and Electromechanical (EEE) Parts: Avoidance, Detection, Mitigation, and Disposition—Independent Distribution—Aerospace Standard AS6081*. SAE International; 2023.
21. SAE International. *Test Methods Standard; General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts—Aerospace Standard AS6171*. SAE International; 2018.
22. Lockheed Martin. FAQs—Counterfeits. Accessed April 8, <https://www.lockheedmartin.com/en-us/suppliers/faqs/counterfeits.html/>. 2024.
23. Boeing. Clause Number: Q132 – Counterfeit Parts Detection and Avoidance System Requirements. 2024. https://www.boeing.com/clauses/docs/Q132_20230523.pdf/
24. Teledyne FLIR. Does FLIR have a counterfeit protection plan?. Accessed April 8, <https://www.flir.com/support-center/oem/does-flir-have-a-counterfeit-protection-plan/>. 2024.
25. Actestlab. Advanced Component Testing. Accessed June 28, <https://actestlab.com/services/authenticity-inspection/>. 2024.
26. SMTcorp. The Industry Leader in Counterfeit Electronics Mitigation. Accessed June 28, <https://actestlab.com/services/authenticity-inspection/>. 2024.
27. Integra Technologies. Counterfeit Detection. Accessed June 28, <https://www.integra-tech.com/counterfeit-detection/>. 2024.
28. AERI. Counterfeit Electronic Component Detection. Accessed June 28, <https://www.aeri.com/counterfeit-electronic-component-detection/>. 2024.
29. Purdue University. Scalable Asymmetric Lifecycle Engagement (SCALE). Accessed July 7, <https://research.purdue.edu/scale/>. 2023.
30. US Congress. *H.R.4346 - Chips and Science Act*. 117th US Congress; 2022.
31. Mondschein J, Welburn JW, Gonzales D. *Securing the Microelectronics Supply Chain—Four Policy Issues for the U.S. Department of Defense to Consider*. Rand Corporation; 2022.
32. Simakhin EA, Shirin AO, Kessarinskiy LN, et al. X-ray Based Electronic Components Authentication Methods to Counterfeit Detection. 2021 IEEE 32nd International Conference on Microelectronics (MIEL). Nis, Serbia. 2021; 119–121. doi:10.1109/MIEL52794.2021.9569042
33. Oriero E, Hasan SR. Survey on recent counterfeit IC detection techniques and future research directions. *Integration*. 2019;66:135–152. doi:10.1016/j.vlsi.2019.02.006
34. Hoveida P, Phoulady A, Choi H, May N, Shahbazmohamadi S, Tavousi P. Terahertz-readable laser engraved marks as a novel solution for product traceability. *Sci Rep*. 2023;13. doi:10.1038/s41598-023-39586-5
35. Sterman J. *Business Dynamics: Systems Thinking and Modeling for a Complex World*. Irwin/McGraw-Hill; 2000.
36. Porter NW. The value of system dynamics modeling in policy analytics and planning. *Policy Anal Model Inform*. 2018;25:123–150. doi:10.1007/978-3-319-61762-6_6
37. Nuerk J, Dařena F. Activating supply chain business models' value potentials through systems engineering. *Syst Eng*. 2023;1–15. doi:10.1002/sys.21676
38. Kasperek D, Schenk D, Kreimeyer M, Maurer M, Lindemann U. Structure-based system dynamics analysis of engineering design processes. *Syst Eng*. 2016;19(3):278–298.
39. Walworth T, Yearworth M, Shrieves L, Sillitto H. Estimating project performance through a system dynamics learning model. *Syst Eng*. 2016;19(4):334–350.
40. Liu T, Zhang M-G, Song J, Zhao Y. Multi-agent evolutionary game of process safety culture in Chinese chemical industry based on system dynamics. *Syst Eng*. 2022;25:107–114. doi:10.1002/sys.21604
41. Alfari A, Khiyami A, Alawad A, Alsaati A, Hadhrawi M. The integrated energy decision support system. *Syst Eng*. 2015;18(5):511–529. doi:10.1002/sys.21326
42. Coyle RG. The use of optimization methods for policy design in a system dynamics model. *Syst Dynamics Rev*. 1985;1:81–91. doi:10.1002/sdr.4260010107
43. Chen JH, Jan TS. A system dynamics model of the semiconductor industry development in Taiwan. *J. Oper. Res. Soc*. 2005;56(10):1141–1150.
44. Chen S, Pan Y, Chen L, Wu DD. A system dynamics model for capacity planning of component supply in complex product manufacturing. *IEEE Syst. J*. 2021;15(1):8–16. doi:10.1109/JSYST.2019.2950627
45. DDG: GUIDED MISSILE DESTROYER. Naval Vessel Register. Accessed November 1, https://www.nvr.navy.mil/NVRSHIPS/HULL_SHIPS_BY_CATEGORY_DDG_99.HTML. 2022.
46. Reichelt Sing a New Standard: GE's LM2500 Gas Turbine Achieves 75 Million Combined Operating Hours. General Electric Press Release; 2015. <https://www.ge.com/news/press-releases/setting-new-standard-ges-lm2500-gas-turbine-achieves-75-million-combined-operating>
47. General Electric. *GE and U.S. Navy Celebrate 40th Operating Anniversary of LM2500 Gas Turbine*. General Electric Press Release. 2009. <https://www.geaerospace.com/press-release/marine-industrial-engines/ge-and-us-navy-celebrate-40th-operating-anniversary-lm2500>
48. Chavy-Macdonald MA, Oizumi K, Kishita Y, Aoyama KA. System dynamics and scenarios framework for architecting product design goals for changeability. *IEEE Syst. J*. 2019;13(2):1957–1968. doi:10.1109/JSYST.2018.2886565

How to cite this article: Porter W, Reese C, Bickford J, Bourn S, Van Bossuyt DL. The impact of counterfeit components and LRUs in the navy surface warfare supply chain: A systems dynamics approach. *Systems Engineering*. 2025;28:157–174. <https://doi.org/10.1002/sys.21785>

APPENDIX A

This appendix provides a detailed description of the stock and flow model used in this article. To increase readability, the following sections apply a consistent style format to the written description of **Modules**, **Converters**, **Flows**, and **Stocks**.

A.1 | LRU DEMAND MODULE

The **LRU Demand** module simulates the demand for LM2500 engine control LRUs over the ten-year simulation period. The LRU Demand stock and flow model (shown below in Figure A1) consists of three main flow paths: one for Navy DDG LM2500 LRU demand (the flow path at the bottom of the figure), one to track the number of active DDG ships (the flow path in the middle of the figure), and one to aggregate the Navy and Commercial LRU orders into a combined order volume stock (the flow path at the top of the figure).

The demand for LM2500 engine control LRUs is driven by both Navy DDG and Commercial industry. The demand is based on the need to support new platform production and to replace failed parts. The Navy DDG demand is based on the actual number of fielded ships at the model's start time as well as the real production numbers of DDGs for the 10-year simulated run of the model.⁴⁴ The **Active Ships** stock is the number of DDGs in service at the start time of the simulation, and grows by the value of new ships commissioned per month over the period of the simulation.

The bottom-most flow path of the Demand Module (Figure A1) depicts the Navy demand for LRUs from the overall LRU inventory. The **Inventory in Supply** stock is initialized at 50 as an estimate of total avail-

able inventory at the simulation start time. The **Deployed DDG Inventory** stock is initialized at 496 to represent 62 DDGs each with 4 engines with 2 LRUs per engine. The **Cumulative Failed LRU** stock tracks aggregate LRU failures over the simulation period based on the authors' estimated failure rate distribution for the blended inventory of genuine and counterfeit LRUs.

The top-most flow in Figure A1 represents the aggregate demand for LRUs from both Navy DDG and commercial needs. The commercial demand for new production is based on an average monthly production of LM2500 engines and an estimated value of engines at model initiation based on the historical production values previously cited.

The **Order Volume** stock is initialized at 60 to match the 10 active orders for the Navy plus a 1% spares level (~50) for commercial industry. The **Monthly Outflow** completely drains the **Order Volume** stock each cycle into the **Cumulative Orders** stock that tracks the aggregate orders over the period of the simulation. The **Order Volume** stock is used to calculate the order volume divided by the **Total LRU Production**. A graph showing the results for Commercial Orders and Navy DDG Orders from a sample simulation run is shown in Figure A2. Note the left axis for commercial order quantities and the right axis for Navy order quantities. The spikes in the graph represent the total demand at that point in time for LRUs to support engine production and replace failed units.

A.2 | LRU Production and Counterfeit Detection Module

The LRU Production and Counterfeit Detection module, shown in Figure A3, consists of a series of arrayed conveyors that represent the production and distribution of components and LRUs. The model is

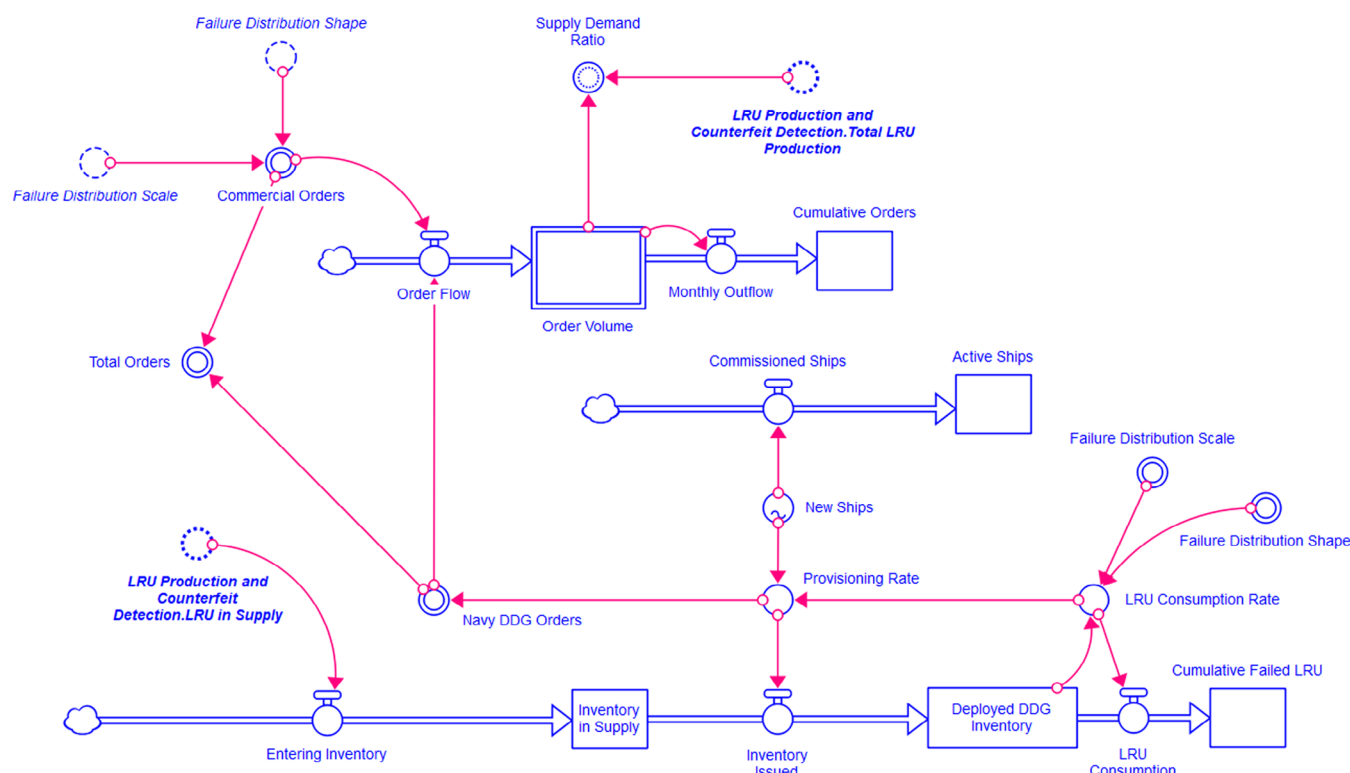


FIGURE A1 LRU demand module.

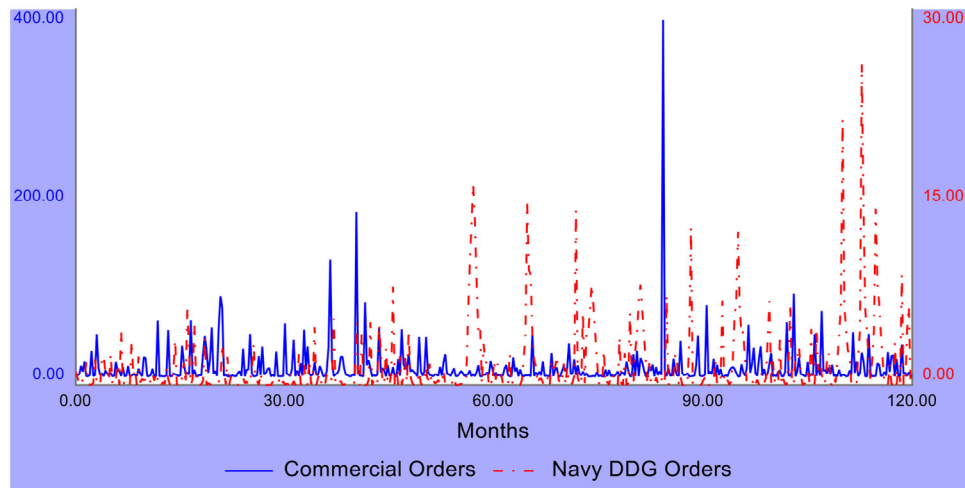


FIGURE A2 LM2500 engine demand for LRUs (sample simulation run).

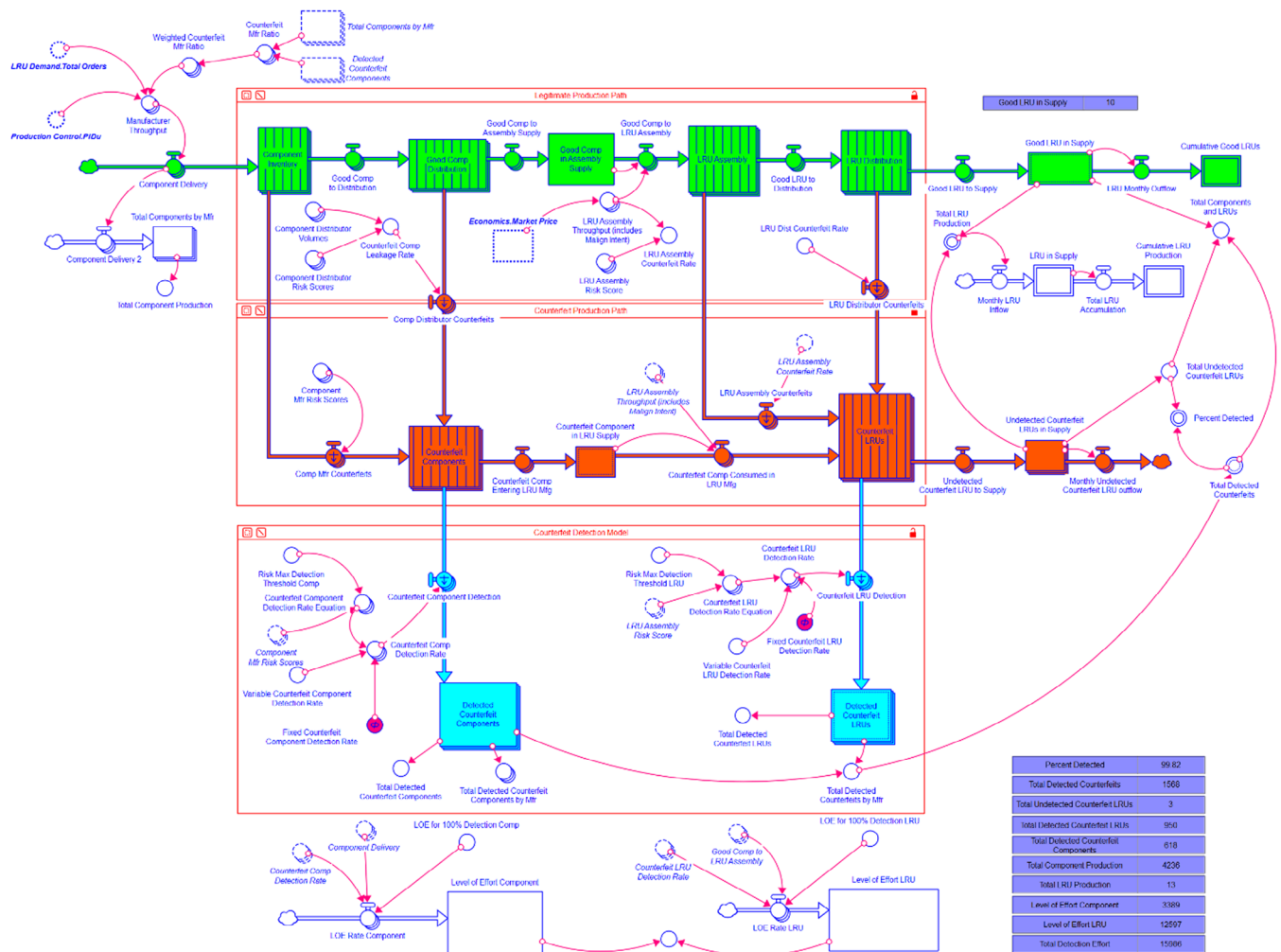


FIGURE A3 Counterfeit production and detection module.

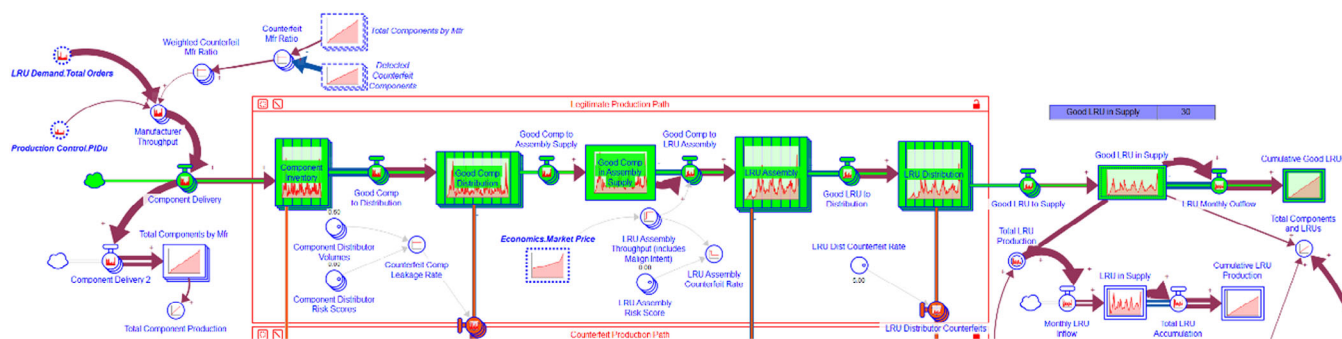


FIGURE A4 Legitimate production flow path.

arrayed to represent multiple entities (i.e., suppliers, distributors, etc.) at each step of the process, each with a different ratio of counterfeit to legitimate part throughput.

In this model, there are two separate logical flow paths for micro-electronics production—one representing legitimate production (the green flow path at top), and the other representing counterfeit production (the red flow path in the middle). All production begins on the legitimate path, but each step of the process presents an opportunity for compromised items to leak from the legitimate path (green) to the counterfeit path (red). Note, in the real supply chain, legitimate parts and undetected counterfeit parts are comingled in the same physical flow; the flow paths are separated in this model as a means to facilitate the math and support the quantification of each type of item. Counterfeit items that are detected are removed from the process and quarantined (the blue stocks at the bottom of the model). Stocks representing process steps along the legitimate path are modeled as arrayed conveyors with leakage rates representing the transfer of items to the counterfeit path. Stocks on the counterfeit path are also modeled as arrayed conveyors, with leakage rates that represent counterfeit item detection and removal from the supply chain (i.e., from the red path into the blue stocks). All products that make it through the green and red flow paths enter the supply system, and the quantity of parts in the blue stocks represents the detected counterfeits that are removed from the supply chain.

A.2.1 | LRU Production

The production section of the model (i.e., the top two flow paths as seen in Figure A3) is split into two paths including a legitimate production path (colored green in Figures A3 and A4) and a counterfeit production path (colored red in Figures A3 and A5). The process entails four major steps: component production, component distribution, LRU production, and LRU distribution. Each of these steps is represented as an arrayed-converter stock to accommodate multiple business entities (i.e., producers/distributors). The production model includes five component manufacturers, three component distributors, and three entities that manufacture and distribute LRUs. At each major step of the process, a percentage of parts is redirected as counterfeits via a leakage flow from the associated array, where they then flow into the counterfeit path of the production model. A counterfeit can be generated at the component level or the LRU level via intentional coun-

terfeiting (whether malign or ersatz) or unintentional inclusion of a counterfeit item from earlier in the production process.

A.2.2 | Counterfeit LRU Production

As described, counterfeits exit the legitimate production flow at each step of the process and enter a parallel (red) flow path for counterfeit production and distribution, as shown in Figure A5.

The counterfeit production process begins with the *Comp Mfr Counterfeits* and the *Comp Distributor Counterfeits* outflows that feed into the **Counterfeit Components** arrayed conveyor stock that represents the total number of counterfeit components in the supply chain. Counterfeit Components leave the **Counterfeit Components** stock via the *Counterfeit Comp Entering LRU Mfg* flow that feeds into the **Counterfeit Component in LRU Supply** stock, or are detected and removed from the **Counterfeit Components** stock via a *Counterfeit Component Detection* outflow. Counterfeit components flow out of the **Counterfeit Component in LRU Supply** stock via a *Counterfeit Comp Consumed in LRU Mfg* flow. This arrayed flow represents the LRU production by the same three LRU production and distribution agents and represents unintentional production of counterfeit LRUs via the inclusion of undetected counterfeit components.

A.2.3 | Counterfeit Detection

There are two points of counterfeit detection and removal from the supply chain including one at the component-level (the *Counterfeit Component Detection* leakage flow), and one at the LRU-level (the *Counterfeit LRU detection* leakage flow). The counterfeit detection and removal outflows are shown colored blue in Figures A3 and A6.

The *Counterfeit Component Detection* leakage flow removes components from the **Counterfeit Components** arrayed conveyor stock. The leakage rate is set by the *Counterfeit Comp Detection Rate* arrayed converter that is structured to allow for user selection of either a fixed or variable detection rate. A fixed detection rate would be used in instances where stakeholders want to implement a standard policy of inspection for all components from all suppliers. A variable detection rate allows stakeholders to adjust their level of inspection based on the perceived risk of counterfeit components from specific suppliers. To develop this value, a notional curve (shown in Figure A7) was established relating a perceived manufacturer risk score to a desired counterfeit detection rate with values, based on discussion

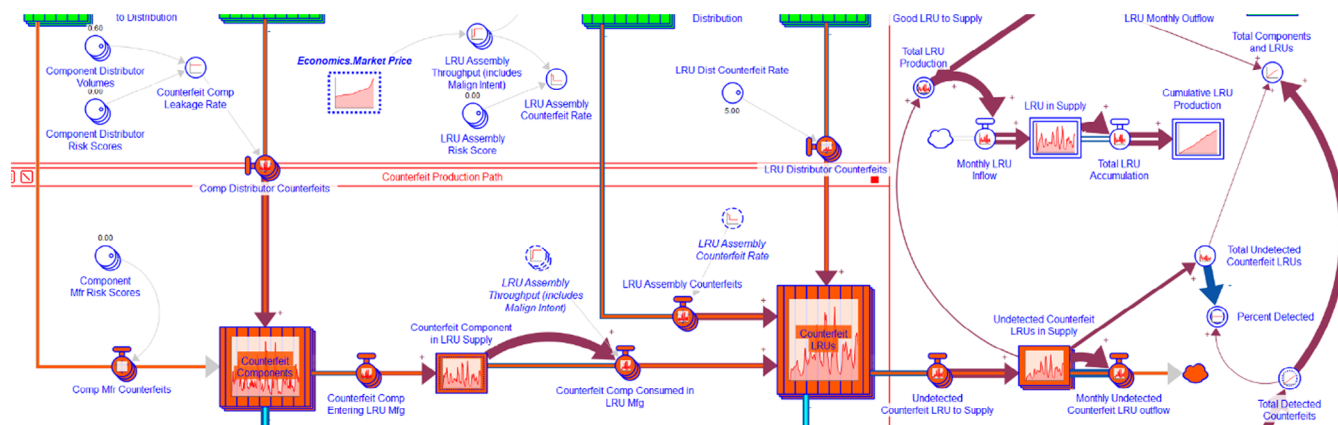


FIGURE A5 Counterfeit production flow path.

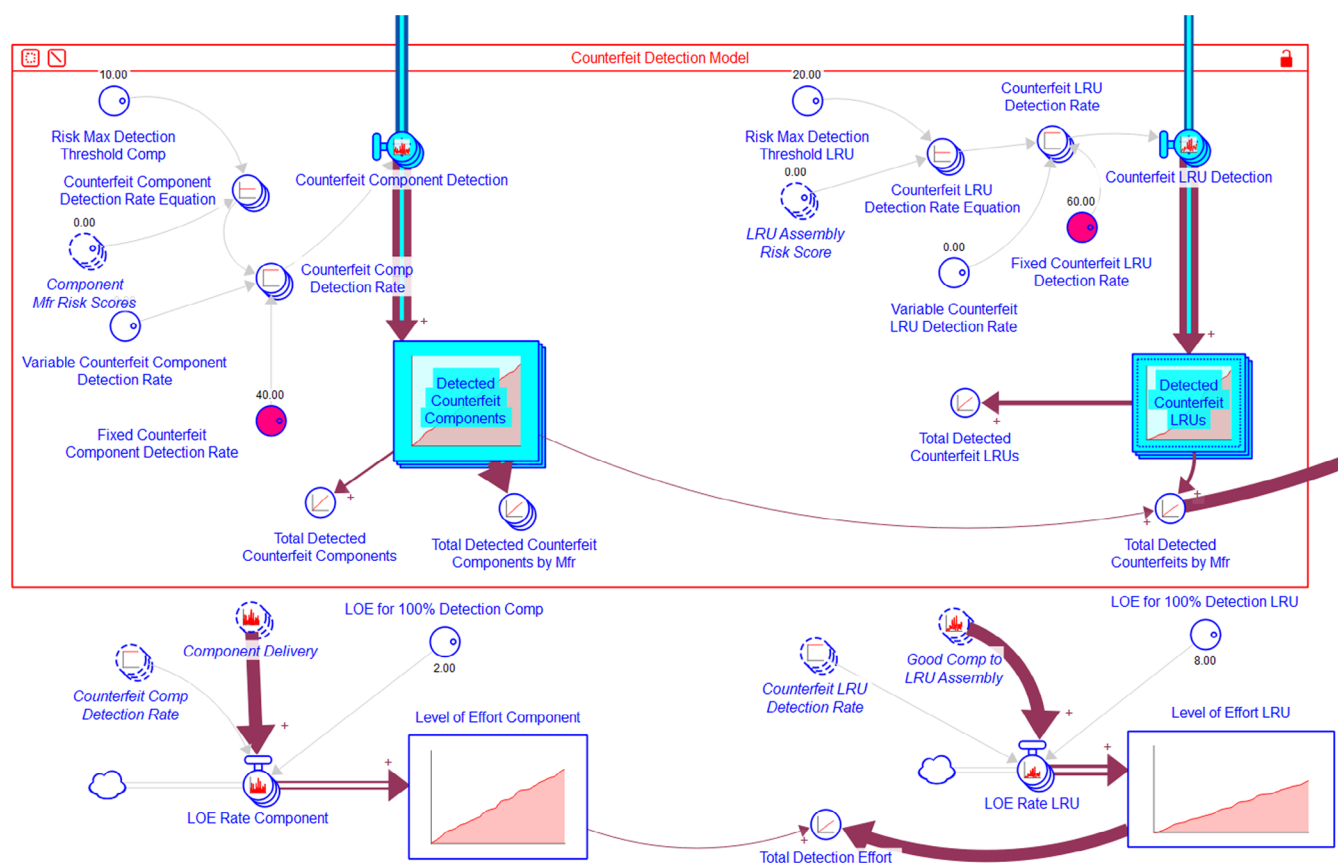


FIGURE A6 Counterfeit detection flow path.

with Navy counterfeit detection experts. The curve represents the scenario where there is a desire (objective value) to capture 95% of counterfeits if 25% or more of items from a supplier are counterfeit, but the stakeholders are okay capturing 80% of counterfeits if only 15% of items from a supplier are counterfeit (threshold value).

The Counterfeit Component Detection outflow feeds into a **Detected Counterfeit Components** stock array. The **Detected Counterfeit Components** stock array feeds several converters used for calculation purposes, including the Total Detected Counterfeit Compo-

nents converter, the Total Detected Counterfeit Components by Mfr converter, and the Total Detected Counterfeits by Mfr converter.

Counterfeit LRU detection is modeled in the same way as counterfeit component detection. A Counterfeit LRU Detection outflow removes counterfeit LRUs from the **Counterfeit LRUs** arrayed conveyor stock set by a Counterfeit LRU Detection Rate converter. Like the component detection rate, the Counterfeit LRU Detection Rate converter is user-selectable as a fixed or variable detection rate. If a fixed rate is selected, the Counterfeit LRU Detection Rate converter is set to the value

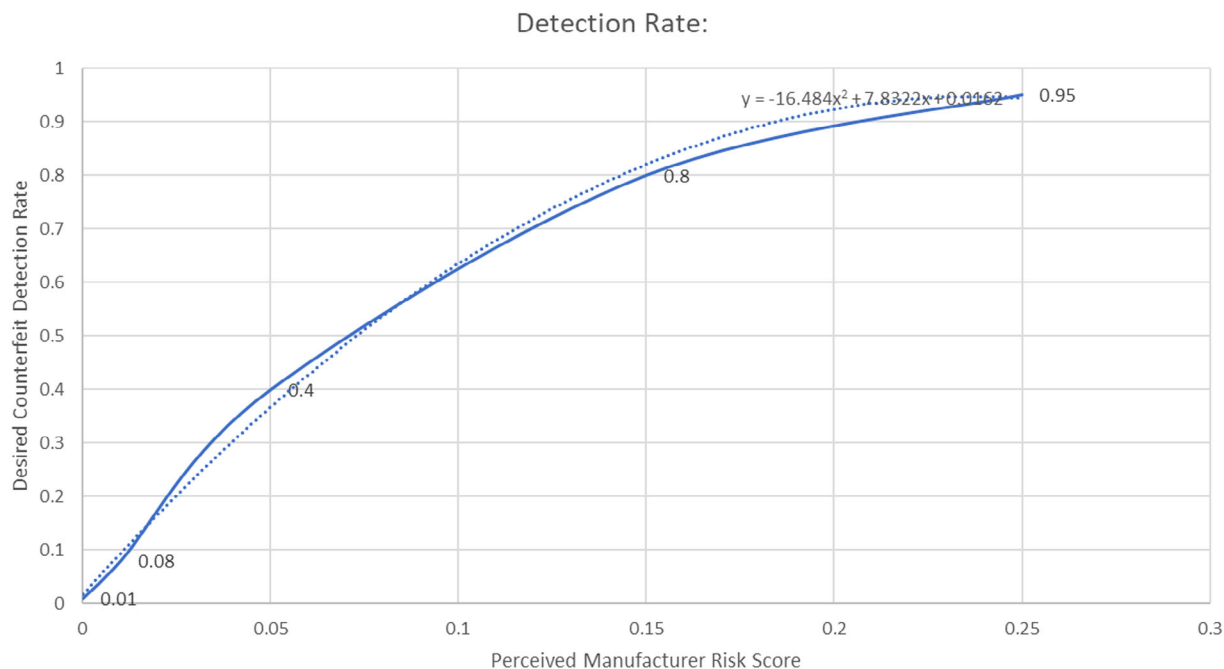


FIGURE A7 Empirically determined variable counterfeit detection rate.

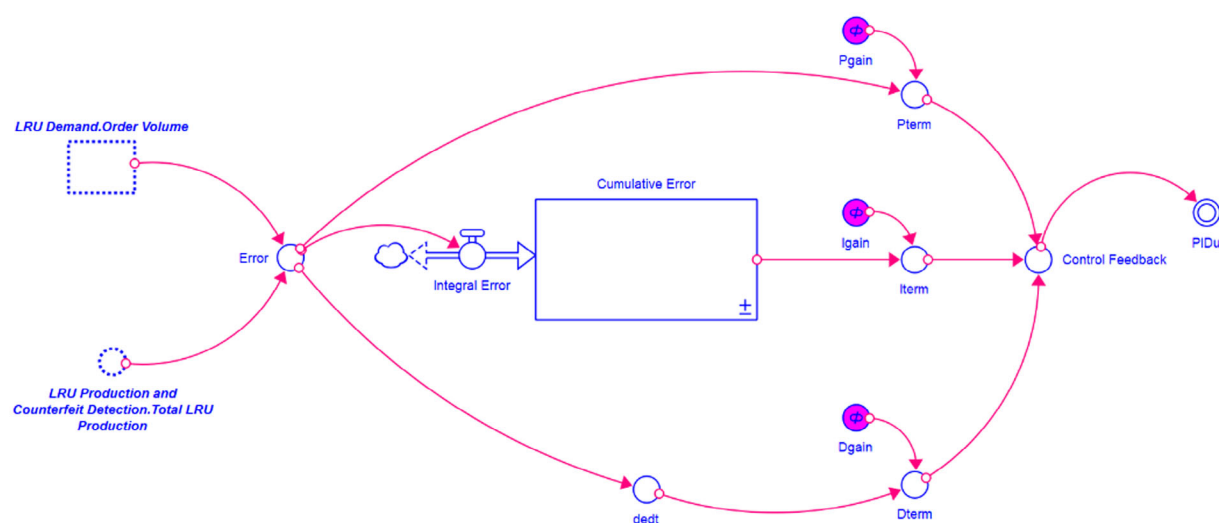


FIGURE A8 The Production Control module implemented as a PID controller.

of the *Fixed Counterfeit LRU Detection Rate* which is adjustable in the user interface panel (and shown as a pink converter in Figure A6). If a variable rate is selected, the *Counterfeit LRU Detection Rate* converter is set by an arrayed *Counterfeit LRU Detection Rate Equation* converter.

A.3 | Production Control Module

The Production Control module (Figure A8) ensures that production tracks demand as the simulation evolves so that the market price is not driven to extremes by significant misalignments between supply and

demand. As the model does not attempt to replicate complex supply chain dynamics (cascading orders, etc.), this method of manually adjusting production was chosen as a simple way to replicate a normally functioning supply chain.

The module receives two inputs including the *Order Volume* stock from the LRU Demand module, and the *Total LRU Production* converter from the LRU Production and Counterfeit Detection module. These elements are used to calculate the simple difference via $\text{Error} = \text{Order Volume} - \text{Total LRU Production}$. The *Error* value converter feeds three calculation paths including a proportional term calculation (based on

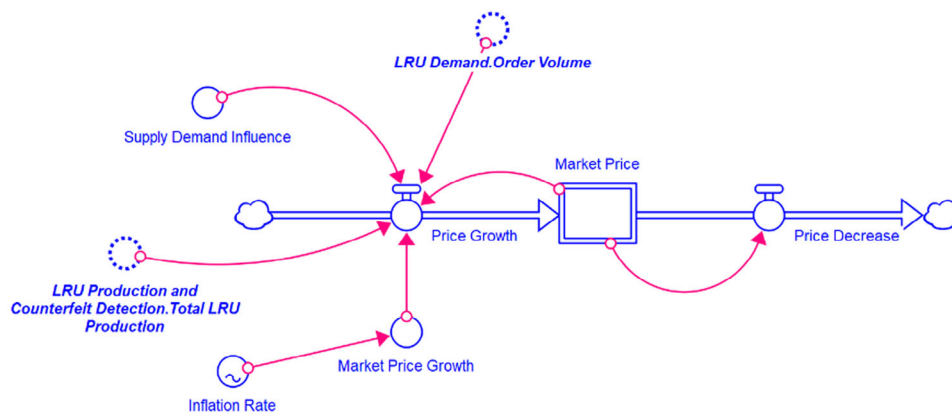


FIGURE A9 Graphical representation of the economics module.

the instantaneous error), an integral term calculation (based on the cumulative error), and a derivative term calculation (based on the rate of change of the error). Each calculation includes an error term multiplied by a user-adjustable gain value (*Pgain*, *Igain*, and *Dgain* converters, highlighted pink in Figure A8). These terms are aggregated into a single value (*PIDu*) that is applied as a multiplier to manufacturer throughput at the component stage of the **LRU Production and Counterfeit Detection** module. In this model, *PIDu* must be constrained as non-negative because applying a negative multiplier to the production rate would imply reversing flow in the production process, and this is not representative of real-world supply chains.

A.4 | Economics Module

The Economics module conveys the aggregate market forces that drive the market price of the LM2500 engine control module. An increase in the demand for additional units above and beyond the supply on hand results in an increase in the market price.

The Economics module is relatively straightforward, as shown in Figure A9. A single stock **Market Price** describes the anticipated price per unit at the given time step, with one inflow (*Price Growth*) and one outflow (*Price Decrease*). Furthermore, the increase in the market price for the LM2500 engine control LRU is influenced by the *Inflation Rate*, which is provided as a discrete input of the actual US inflation rate during each month of the period of the simulation.

Due to lack of available information (e.g., actual counterfeit detection levels of effort and efficacy at each step of the supply chain, actual counterfeit insertion costs, profit margins, incentive thresholds, etc.) the overall model is based on several assumptions that preclude detailed incorporation of market price as a driver in the LRU Production and Counterfeit Detection module. However, the SD model does incorporate market price influences in the *LRU Assembly Throughput (includes Malign intent)* calculation, previously described, wherein a market price of less than \$3,000 drives an intentional increase in ersatz counterfeit LRU production to flood the market with counterfeits and thereby drive up the market price (Figure A10). This approach represents a subversive way that global actors with substantial microelectronics supply chain influence can achieve malign outcomes without direct involvement in malign counterfeiting opera-

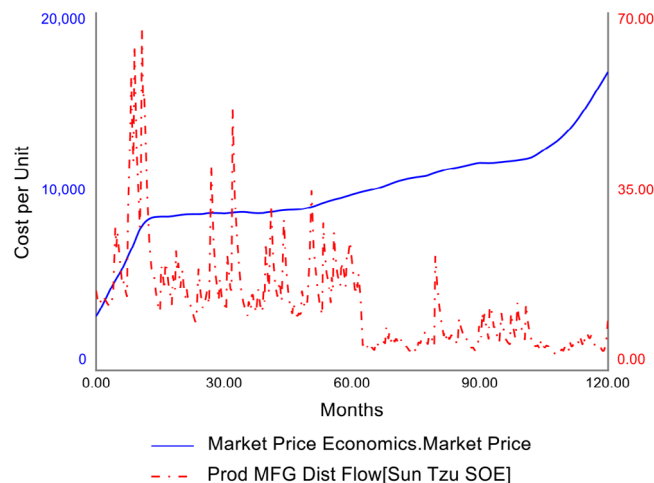


FIGURE A10 Impact of artificially increased production when market price is less than \$3000.

tions (i.e., driving market conditions to incentivize ersatz counterfeiting with a malign intent.)

APPENDIX B: INTERFACE PANELS

The interface panel for the model is intended to provide the user with a simplified means to adjust key variables, run the simulation, and visualize the effect on key parameters. The interface panel (Figures B1 and B2) allows the user to explore the specific question, “Is it more effective to target detection efforts at the component level or at the LRU level?” as described in the main body of the article.

The main panel contains two user-adjustable variables that correspond to previously described converters including *Counterfeit Component Detection Rate* and *Counterfeit LRU Detection Rate*, presented as sliders with green text, positioned at the top left. After setting the desired values, the user then executes the simulation. The graphs include a plot of Order Volume (at mid left); a plot of Market Price (at bottom left); a plot showing total Component and LRU production and total Undetected Counterfeit LRUs (at top right); and a plot showing the level of effort (LOE) on component detection, LOE on LRU detection, and total detection LOE (at bottom right). The panel also displays

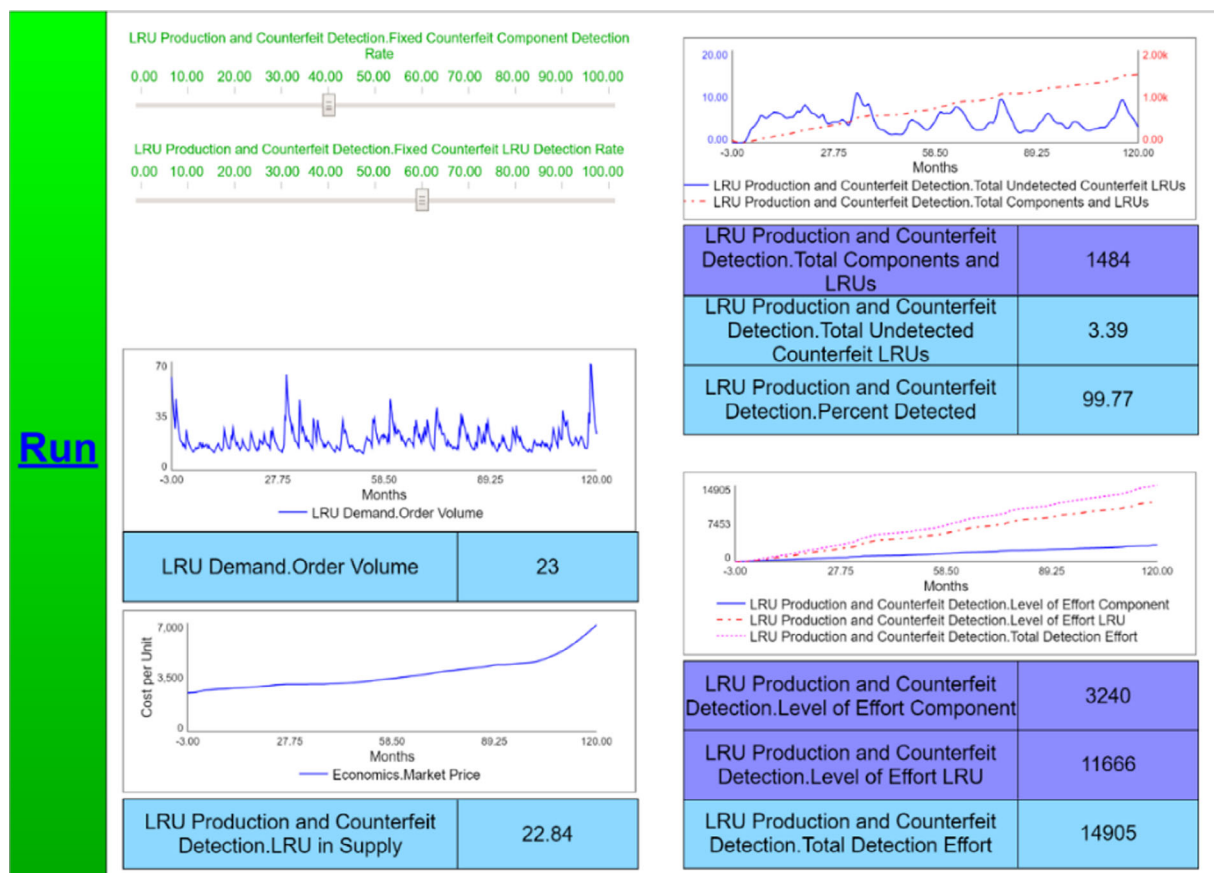


FIGURE B1 Main interface panel.

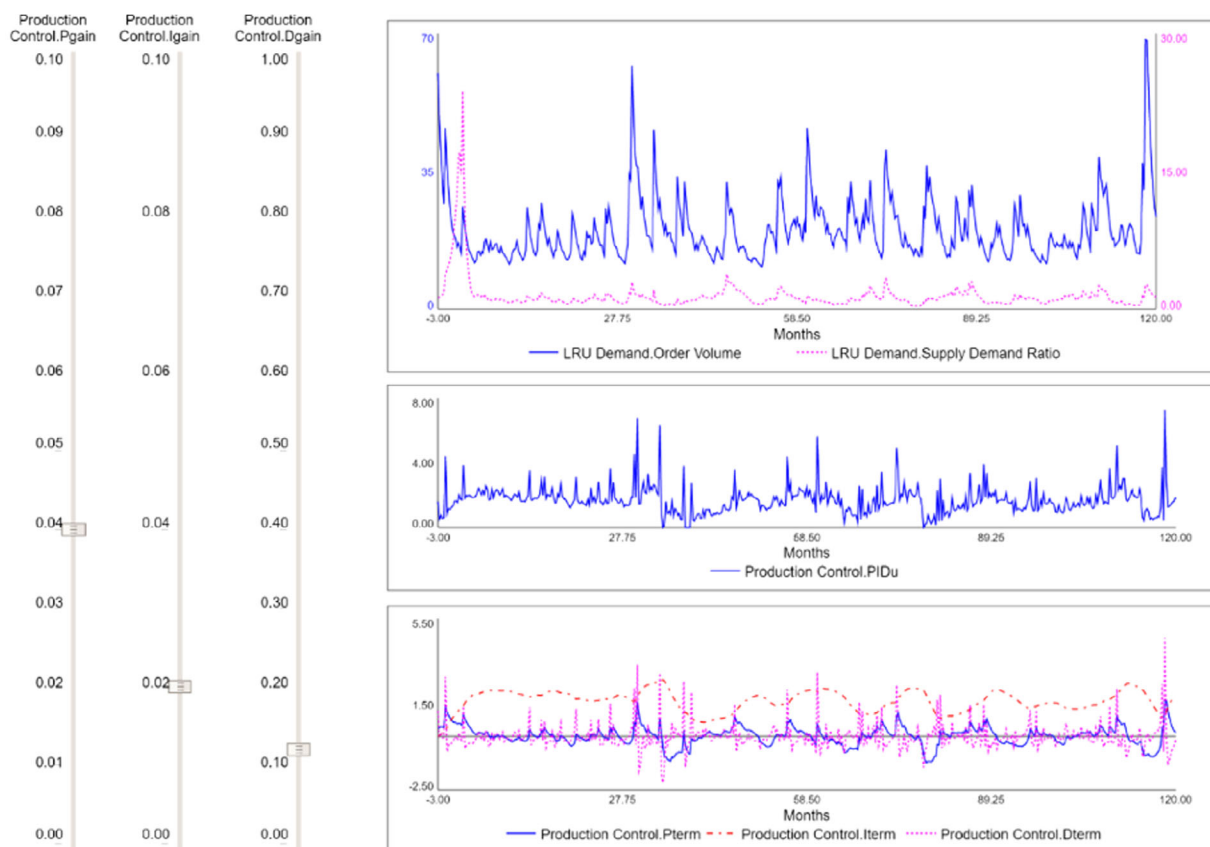


FIGURE B2 Interface panel with user-adjustable PID gain parameters.

eight numerical data fields including the current value of order volume, current quantity of LRUs in supply, total production of components and LRUs, the total quantity of undetected counterfeit LRUs, the percent of counterfeits detected, total LOE spent on component detection, total LOE spent on LRU detection, and overall total LOE spent on counterfeit detection.

Page 2 of the user interface panel (Figure B2) includes three vertical sliders where the user can adjust the gain parameters on the PID control that drives the production rate. The plots on the right side of the panel show Order Volume and Supply Demand Ratio (top right), the $PIDu$ value (middle right), and the individual $Pterm$, $Iterm$, and $Dterm$ values (bottom right), to assist the user in tuning the gain values.