Risk Analysis DOI: 10.1111/risa.12536

Perspective

Traceability and Risk Analysis Strategies for Addressing Counterfeit Electronics in Supply Chains for Complex Systems

Daniel DiMase,[1] Zachary A. Collier,[2] Jinae Carlson,[1] Robin B. Gray Jr.,[3] and Igor Linkov[2,*]

Within the microelectronics industry, there is a growing concern regarding the introduction of counterfeit electronic parts into the supply chain. Even though this problem is widespread, there have been limited attempts to implement risk-based approaches for testing and supply chain management. Supply chain risk management tends to focus on the highly visible disruptions of the supply chain instead of the covert entrance of counterfeits; thus counterfeit risk is difficult to mitigate. This article provides an overview of the complexities of the electronics supply chain, and highlights some gaps in risk assessment practices. In particular, this article calls for enhanced traceability capabilities to track and trace parts at risk through various stages of the supply chain. Placing the focus on risk-informed decision making through the following strategies is needed, including prioritization of high-risk parts, moving beyond certificates of conformance, incentivizing best supply chain management practices, adoption of industry standards, and design and management for supply chain resilience.

KEY WORDS: Counterfeit; semiconductors; supply chain risk management; traceability

1. INTRODUCTION

As supply chains become more globally interconnected and complex, they become increasingly vulnerable to exploitation by counterfeiters. It is estimated that the total impact of counterfeit and pirated products for G20 nations was between $455 to $650 billion in 2008, and is projected to grow to $1.2 to $1.7 trillion in 2015.[1] For example, in 2013, E.U. customs officials detained approximately 36 million individual counterfeit items, and the United States made over 28,000 seizures of counterfeit shipments, 24% of which were consumer electronics, computers, or related accessories.[2,3]

While certain counterfeit products such as pharmaceuticals have gained world-wide attention, counterfeit electronics have remained relatively ignored until recently, despite the grave risks that these counterfeits pose. The U.S. Government Accountability Office (GAO) outlined potential risks to include economic losses and health and safety risks.[4] Due to the large scope of the electronics industry, and the increasing interconnectedness of the global supply chain, there are many different economic sectors and stakeholders that have the potential to be harmed. For instance, if a microprocessor is corrupted, then any number of economic sectors could be at risk, including energy, retail, or finance.[5]

Most critically, counterfeit electronics carry national security implications.[4] In fact, it has been found that counterfeit electronic parts misrepresented as military grade can be easily purchased on

[1]Honeywell, Phoenix, AZ, USA.
[2]U.S. Army Engineer Research & Development Center, Concord, MA, USA.
[3]ECIA - Electronic Components Industry Association, Alpharetta, GA, USA.
[*]Address correspondence to Igor Linkov, U.S. Army Engineer Research & Development Center, Concord, MA, USA; Igor.Linkov@usace.army.mil.

the Internet[6] and that counterfeits have been found in U.S. Department of Defense (DoD) supply chains, including counterfeit memory devices in the mission computers of missile systems.[7] Products in DoD supply chains are usually designed to have a long service length and some frequently exceed the service length, and in practice, most of the counterfeit parts are from products that are nearing or have passed obsolescence.[8,9] The longer these products are in service the more susceptible they become to counterfeits. This is due to the increased difficulty in obtaining parts; other, less than optimal, sources are used for acquisition instead that have a higher probability of supplying counterfeit parts. Implications of counterfeits in military supply chains include degraded functionality of weapon systems and infrastructure, physical harm to troops, and the interception of sensitive data via Trojans and malware.[10]

In January 2012, President Barack Obama signed the National Strategy for Global Supply Chain Security,[11] which aims to promote the secure and efficient movement of goods, and to foster a resilient supply chain. The National Strategy calls for a robust risk management strategy, including the identification and prioritization of risks, implementation of a layered defense, and formulation of an adaptive approach to respond to evolving threats. Recently, an Executive Order related to critical infrastructure cybersecurity was released, again calling for the development and implementation of risk-based standards.[12]

Counterfeit detection methods have made great improvements in their effectiveness, but in order to keep up with the increasing sophistication of today's counterfeits, further improvements in assessing risk and building resilience are necessary. Past and current efforts in the anti-counterfeiting arena include advances in the field of circuit design, such as DNA marking,[13] physical unclonable functions (PUFs),[14] and various on-chip sensors.[15] For instance, similarly to how DNA is used as forensic evidence in criminal proceedings, DNA marking technologies involve tagging a label or the part itself with a unique botanical DNA compound, which can then be later authenticated via a secure server, and is virtually impossible to duplicate.[13] Advances have also been made in testing technologies ranging from visual inspections to microscopy, X-ray inspection, and die inspection, although some of these methods can be destructive.[16] The Society of Automotive Engineers (SAE) has a test laboratory standards development committee (G-19A) that has been developing a test methods standard specific to electrical, electronic, and electromechanical (EEE) parts that has incorporated guidance for conducting a risk assessment and mitigating actions commensurate with the identified risk. It is anticipated that the standard will be published before the end of 2015. In parallel, best practices in supply chain management have been discussed, including traceability documentation, distributor selection, obsolescence management, incident reporting and information sharing, and electronic waste disposal methods.[17,18] Critically, research gaps still remain, primarily in the area of risk analysis[19,20] and technology solutions that enable more cost-effective solutions to counterfeit avoidance and detection. Research gaps in risk analysis are partially due to the difficulty in quantifying the impacts and consequences of counterfeits, necessitating the use of semi-quantitative methods.[21] Moreover, counterfeiting is an ever evolving threat; as new technologies and policies are established, counterfeiters devise novel methods for escaping detection. In addition, solutions that provide track and trace and anti-tamper capabilities in the supply chain can aid in the establishment of supply chain trust by pinpointing the origins of authentic material that has not been counterfeited or modified. Therefore, to meet the calls for resiliency and security from the White House, there is a critical need for analytical methods to aid in making credible decisions in the absence of certainty, risk-based test analysis that leads to detection of counterfeit items with higher confidence and at lower cost, and strategic risk mitigation efforts.[19]

2. THE ELECTRONIC, ELECTROMECHANICAL, AND ELECTRIC PARTS SUPPLY CHAIN

2.1. Supply Chain Overview

Supply chain management is a fundamental part of an organization's strategy and can be very complex.[22] In an ideal state, the EEE supply chain is composed of five major segments—original component manufacturers (OCMs), authorized distributors, circuit board assemblers, prime line replaceable unit (LRU) contractors and subcontractors, and the systems producers (Fig. 1). Although this is the ideal model, it is not always a viable option for meeting customer delivery requirements. Original equipment manufacturers (OEMs) have the ability to purchase components directly from OCMs along with contract manufactures, master distributors,

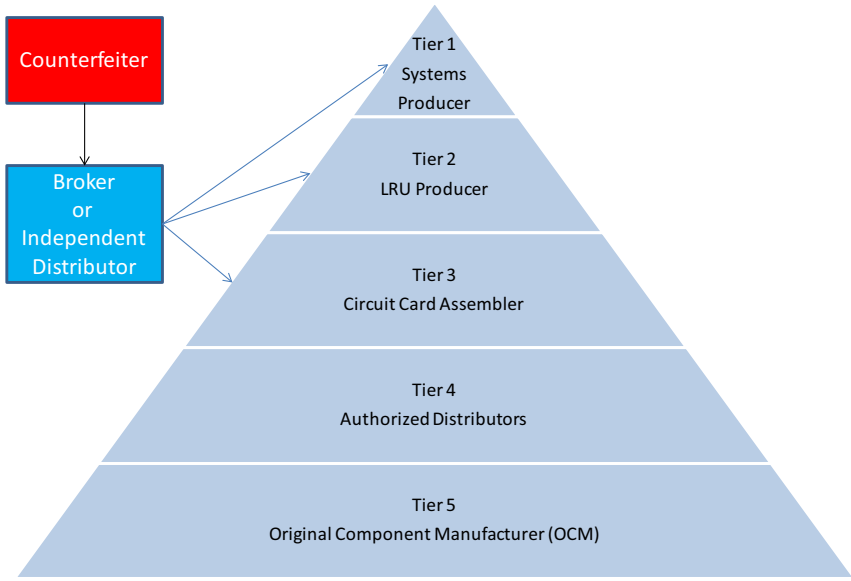

Fig. 1. Supply chain pyramid.

authorized distributors, brokers, and independent distributors (Fig. 2). Once material is purchased and received at any of these supply chain channels, it is not unusual for inventory to be redistributed interdivisionally or resold back into the market. As components are transferred and/or resold numerous times, the ability to trace the material to its origin becomes increasingly more difficult. The ability to maintain traceability from even the most reputable authorized/franchised distributors does not always exist and increases the likelihood of introducing counterfeit material into an organization's supply chain. It has been determined that the highest risk for counterfeit materials entering the supply chain is through the broker and independent distributor marketplace.

When reviewing the supply chain pyramid (Fig. 1), it is the third tier (circuit card assembler) that typically integrates EEE components; however, it is not uncommon for large OEMs and contract manufacturers to procure EEE components also. Maintaining traceability within an organization is also vital for counterfeit prevention as it is common practice for inventory to be transferred both interdivisionally or between the OEMs and contract manufacturers who are assembling the circuit cards on behalf of the OEMs. Lack of capabilities to trace material within an organization can harm multiple product lines within an organization if counterfeit material is transferred and consumed.

For the aerospace industry at large, once inventory is received and passes inspection, it is typically considered acceptable under the organization's quality system. Current supply chain practices do not require traceability/documentation above and beyond current documentation practices such as purchase order history along with lot/batch and date code information for such purchases. Additionally, paper documentation (e.g., certificates of conformance, packing lists, and test documentation) are typically filed in the archives and stored in accordance with the organization's records information management policy. The paperwork is not typically linked with the physical batch/shipment of parts and has a retention period associated with the receipt of goods versus the consumption, when the products may be used many years after the organization's record retention period. After the record retention period has elapsed, the paperwork is typically destroyed. Critically, this paperwork is increasingly subject to counterfeit along with the parts themselves, and cannot be taken as a sole guarantee of authenticity.

If purchases are fulfilled and documented through the OEM or authorized distributor, the acquired material is considered low risk to an organization. Outside of space-grade manufacturing, the majority of organizations only track material to stores unless traceability to the assembly is required. If traceability requirements to the end-item assembly are contractually flowed down to an organization,

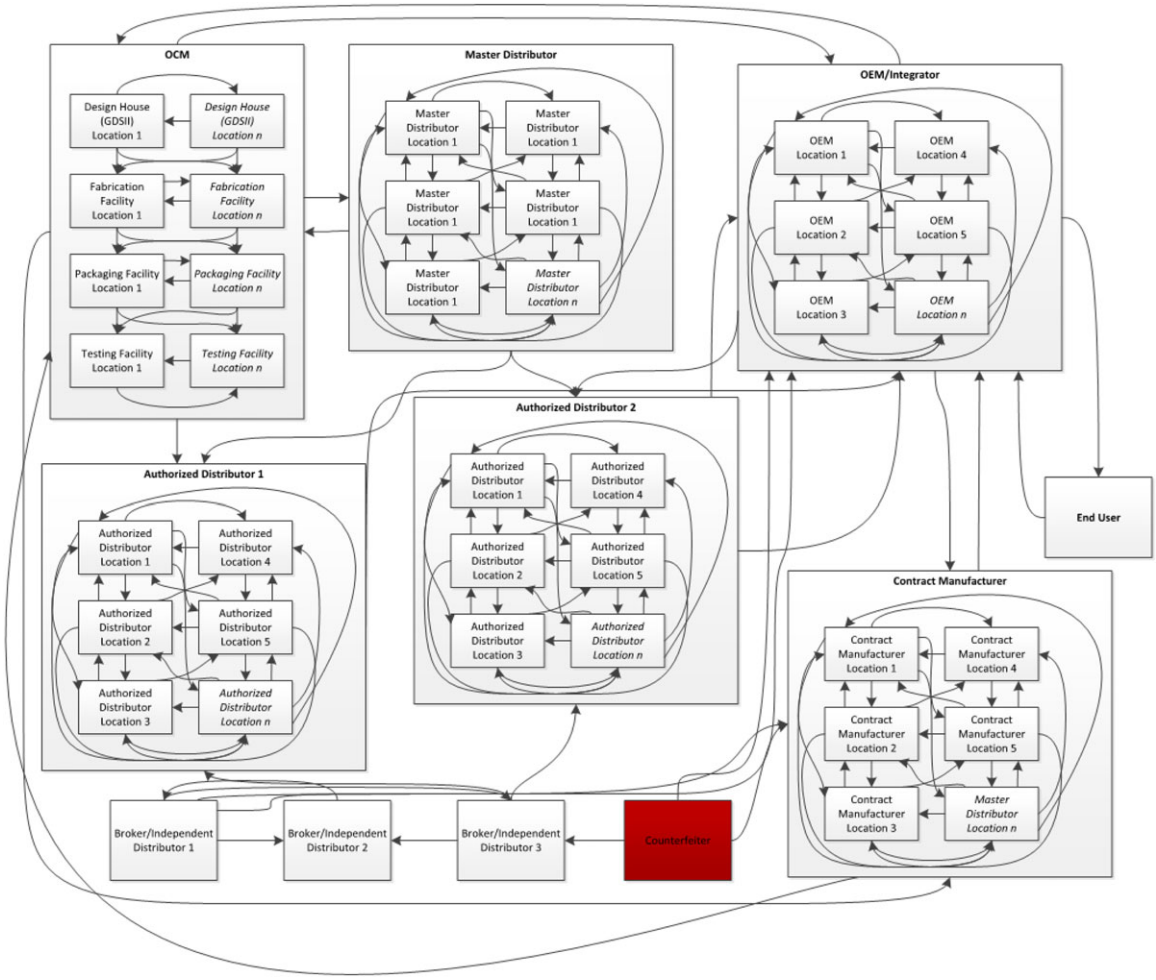

Fig. 2. Conceptual model of the electronics supply chain.

additional tracking may be needed. One identified path for meeting this requirement is the use of batch management with configuration controls that track work-in-progress (WIP) inventory on the factory floor to the lowest level serialized assembly. The infrastructure needed for this requires significant data storage and physical intervention to ensure appropriate recording points in the manufacturing process. Capital equipment changes may be necessary on the factory floor to automate recording of lot/date codes into data systems as material is consumed. All of this can be extremely labor intensive and costly, ranging from approximately 3x to 10x the original part cost.

2.2. Sources of Counterfeit Risk

EEE counterfeit part prevention typically consists of supply chain risk management down to the piece part provider. Industry- and government-accepted standards on counterfeit avoidance require use of authorized sources, and when authorized sources are not available, sources of supply that have verifiable traceability to the original manufacturer.[23–25]

A significant source of counterfeit EEE parts is the disposal of electronic waste, often called "e-waste," which is generated from discarded electronic assemblies from businesses and consumers and harvested from these assemblies in developing countries.[26] Even if developed countries were to regulate and attempt to control e-waste, developing countries where the material is harvested have enough of their own supply of e-waste due to their own consumption and disposal of material.

One of the most advanced threats of EEE counterfeits are those that are considered "tampered."

The SAE G-19A committee defines a tampered counterfeit part as "a part which has been modified for sabotage or malfunction." Parts of this category would likely be state sponsored by adversary countries and could have dangerous or catastrophic consequences for systems that incorporate them. Consequences include but are not limited to denial of service of a critical function of the system, side-channel attacks that enable loss of sensitive or critical information, premature or latent failure, or unauthorized access to proprietary data or system functionality. This category of counterfeit devices is of particular concern for applications affecting national security, such as weapon systems, communications systems, or the systems impacting the critical infrastructure, including power utilities, mass transportation, and banking.[26]

From the 387 companies and organizations surveyed by the U.S. Department of Commerce in a defense industrial base assessment of counterfeit electronics, the largest percentage of counterfeits were sold by brokers and independent distributors where pedigree and traceability to the original manufacturer are often unavailable.[7] One reason for the lack of traceability is because independent distributors often receive their inventory from OEM surplus material that is no longer needed for production or maintenance and repair operations. OEMs sell the surplus to recover costs of their excess inventory or the material is consigned to an independent distributor. Other sources include excess inventory from contract manufacturers. Contract manufacturers and OEMs often order components from multiple sources and commingle the inventory and then sell this commingled inventory into the open market. As a result, traceability of this inventory is often difficult to document and prove.

In addition, selling excess inventory is typically not the OEM's or contract manufacturer's core business model and done at a loss, which increases the likelihood of not receiving the necessary information for traceability and pedigree to the original manufacturer. Once the surplus is sold, the independent distributor is unlikely to receive additional surplus of the same item to support ongoing sales. Many independent distributors will also broker parts to support their customers and business model for additional revenue, since inventory sales are unpredictable. Brokers will shop for parts required to support their customers from other independent distributors who are showing stock on the parts they need. While brokers locate inventory per customer demand and buy and sell on short order, independent distributors speculate on inventory. Many independent distributors also broker parts.

Independent distributors and brokers choose not to share their source of supply for two reasons. One, they don't want to lose competitive advantage by giving up their source and be cut out of the transaction as a middleman. They also do not want to risk losing a future source of ongoing surplus and sales revenue. Two, they may be restricted by contract from disclosing the source of the surplus. OEMs and contract manufacturers may not want their name associated with the sale of parts from surplus, which could impact their relationship and future agreements with their ongoing supplier base. Since brokers are buying parts without verifiable traceability and pedigree, the market is ripe for fraudulent actors to introduce counterfeit parts into the supply chain through brokers. In addition, independent distributors may not have the appropriate inventory control systems to segregate material that has pedigree and traceability from material that does not. In addition, independent distributors may not have adequate inspection and test capabilities to detect today's advanced counterfeits. Even the most advanced test capabilities cannot authenticate parts and can be extremely costly and time consuming. Since their primary business is brokering parts and selling excess inventory, there is significant risk of commingled material from multiple sources with unknown verification, traceability, and pedigree.

The actor that is generally the most susceptible to counterfeits is the broker. A supply chain can only be as strong as its weakest link. As such, all of the brokers in the supply chain might be very trustworthy, but if one link in the supply chain is more susceptible to counterfeits, then the whole system now becomes susceptible to counterfeits. Some of the more "trustworthy" brokers utilize testing laboratories to verify the authenticity of their products; however, many have little or no screening and verification.

From a risk-based perspective, the most likely source for receiving counterfeit parts is open market material acquired from independent distributors and brokers without verifiable traceability and pedigree to the original manufacturer. There is still a risk of receiving counterfeit parts from authorized sources if they do not have adequate controls to validate when returned material is not what was originally sold to the OEM or contract manufacturer. There is also a risk when the authorized source acquires any

material from the open market and commingles these parts without traceability and pedigree in their inventory. However, for authorized sources whose core business model is to acquire parts only from original manufacturers that have appropriate inventory controls, the risk is very small. Furthermore, the risk can mitigated through appropriate industry standards.

3. SUPPLY CHAIN NEEDS

3.1. Enhanced Risk Assessment Models

To be able to effectively manage supply chain risks arising from counterfeit electronics, it is necessary to first be able to assess the supply chain risk. However, a majority of the literature on supply chain risk is related to disruptions (e.g., natural and man-made disasters, trucking accidents) or external market uncertainties (e.g., coordination of supply and demand).[27–30] Traditional approaches to disruption risk management attempt to balance the costs of risk mitigation alternatives with expected losses from a disruption event, with an objective of minimizing total costs,[29] and a number of supply chain modeling efforts have arisen to include deterministic, stochastic, economic, and simulation-based models.[31]

However, comparatively few supply chain risk models have dealt with the issue of assessing counterfeit risks—where instead of disruptions, adulterated products are inserted into the supply chain. Conrad *et al.*[32] developed a stochastic mapping approach for assessing the risks of contaminated food supply. Lehtonen *et al.*[33] used a hidden Markov model for location-based authentication in the pharmaceutical supply chain. However, these approaches can be quite data-intensive and require numerous assumptions from subject matter experts regarding the probabilities of goods transferring from one actor in the supply chain to another, which in a complex supply chain may become burdensome. Moreover, a purely quantitative risk assessment may miss out on the weights that decisionmakers place on different (e.g., everyday vs. catastrophic) risks.[34] Collier *et al.*[21] developed a semi-quantitative risk assessment method for suspect counterfeit electronics based on knowledge of the system criticality and vendor history in an attempt to aid the selection of appropriate authentication testing protocols. Schaffer[35] developed a set of semi-quantitative spreadsheet tools that assess the risk of counterfeits based on part type, features of the untrusted supplier, and anticipated costs resulting from counterfeit use. However, the likelihood of receiving a counterfeit is assessed by proxy through knowledge of the vendor (e.g., quality certifications, open incident reports) instead of information about the supply chain route itself. Thus, while these tools[21,35] are a useful starting point, there is a need to develop a supply chain risk assessment model specifically tailored to counterfeit electronics risks, informed by the route that the parts have gone through before reaching an end user.

3.2. Traceability Considerations

In order to utilize enhanced risk assessment models, there is a need to know through what points the products are being shipped. The ability to effectively trace products through the supply chain is critical to understanding the risks involved, especially when supply chains topologies are complex, such as in food[32] and pharmaceuticals.[36]

In May 2014, defenses regulations were introduced to address counterfeit electronic part traceability. DFARS clause 252.246-7007,[37] specific to counterfeit avoidance and detection of electronic parts, addressees traceability by requiring systems criteria for a counterfeit electronic part detection and avoidance system that

> *shall include risk-based policies and procedures that address, at a minimum, the following areas . . . : Processes for maintaining electronic part traceability (e.g., item unique identification) that enable tracking of the supply chain back to the original manufacturer, whether the electronic parts are supplied as discrete electronic parts or are contained in assemblies. This traceability process shall include certification and traceability documentation developed by manufacturers in accordance with Government and industry standards; clear identification of the name and location of supply chain intermediaries from the manufacturer to the direct source of the product for the seller; and where available, the manufacturer's batch identification for the electronic part(s), such as date codes, lot codes, or serial numbers. If IUID marking is selected as a traceability mechanism, its usage shall comply with the item marking requirements of 252.211-7003, Item Unique Identification and Valuation.*

One could interpret this requirement in the most rigorous way as having a system that identifies the name and location of all supply chain intermediaries from the original manufacturer once the parts are produced to the system (e.g., an airplane or weapons system), and each intermediary and location in between. However, the costs of this level of traceability may outweigh the benefits. From an industry perspective, there is a critical need to understand

what the optimal level of traceability within the supply chain is to support and address counterfeit prevention and ensure pedigree to the original manufacturer. There are only a few families of electronic parts that offer the name and location of the supply chain intermediary from the original manufacturer (MIL-PRF-38535 and MIL-PRF-19500). Even for these military specifications, traceability requirements are only applicable to supply chain transactions prior to the integration of these parts into circuit cards, and do not specify traceability requirements to the final delivered system. There are well over 100 different military federal supply classes of electronic parts, many of which do not require identifying and naming all known intermediaries in the military specification. In addition, commercial devices do not require or provide this information. Electronic systems supporting the Warfighter could not be produced on the limited number of MIL-Spec parts that identify the name and location of all known intermediaries, requiring the use of parts with limited traceability. Thus, there is a need for thoughtful approaches to traceability that balance the costs of increased traceability with the risks posed to different systems. The following are some considerations for designing and implementing a traceability program.

3.2.1. Prioritize High-Risk Parts

In support of U.S. DoD's better buying power initiatives, which encompass a set of fundamental acquisition principles to achieve greater efficiencies through affordability, cost control, elimination of unproductive processes and bureaucracy, and promotion of competition,[38] there are less costly alternatives than space grade traceability to achieve the intent of the regulations specified above for counterfeit electronic part detection and avoidance. One less costly alternative is to implement "risk-based policies and procedures" as specified in the regulations, focusing on acquiring material from authorized sources, such as the original manufacturer or its authorized/franchised distributor or after-market manufacturer. When these sources of supply are not available, the policy should require a risk assessment that may require more stringent test and inspection requirements on material acquired from independent distributors and brokers, where the likelihood of receiving a counterfeit part is more probable than from other trusted sources, and the traceability to the original manufacturer is limited or impossible to achieve. When material is acquired from brokers and independent distributors in critical applications, the forward traceability may need to link the risk analysis and testing performed to mitigate counterfeiting to the lot of parts received. This is because no amount of testing can truly authenticate an electronic part. The best testing can do is increase the confidence that parts do not show evidence of counterfeiting based on testing performed. Parts that could impact mission criticality and safety should have more testing performed to increase confidence for those applications. From a "risk-based" perspective, traceability of electronic parts should be focused on material acquired from other than authorized sources since these parts are most at risk for counterfeiting. From a technical perspective, tracking parts without verifiable traceability and pedigree makes sense since we can determine if appropriate testing was performed on critical systems and components throughout the expected lifecycle of the system. Even if new counterfeit methods are discovered, organizations that are tracking these parts could evaluate the potential consequences and make a determination of how to mitigate discovered problems.

3.2.2. Move Beyond Certificates of Conformance

Organizations also need to be careful not to trust the paper certificate of conformance (CoC) as a means to verify whether parts are authentic. These documents are easily counterfeited and are not tethered to the part. An organization could acquire a small quantity of known good parts specifically to acquire the CoC. As a result, the valid CoC can be fraudulently associated with the parts that were acquired from the open market without pedigree and traceability to the original manufacturer. There are numerous examples of false CoCs that have been provided by suppliers reported for selling counterfeit parts by ERAI, an organization that monitors, mediates, and reports issues impacting the electronics supply chain. Additional research and development is needed in promising areas that can help mitigate the threat of counterfeiting, such as QR codes capable of authenticating parts on location, which include data documentation, embedded systems on chips that include security features, and covert features embedded in parts to assist in identifying authentic and counterfeit parts.

3.2.3. Incentivize Best Practices

To be fair and equitable, government should not punish organizations that are victims of unknown counterfeit methods. Safe harbor should be established for organizations that stay current with detection techniques and report known problems of fielded issues to their customers. After all, industry can only address the "known risks" and should not be held accountable for problems that have yet to be discovered. A risk-based solution to implement the appropriate level of traceability, such as tracing parts on critical systems acquired from independent distributors and brokers, and the testing performed to authenticate the material, will be an added cost to execute, but should be a fraction of the cost to implement full traceability from origin to destination for all parts. In this example, if batch management with configuration control and associated testing is implemented and limited to the parts that have no verifiable traceability and pedigree, then the cost increase should be contained to the support necessary to track the limited number of parts on the assembly that do not have verifiable traceability and pedigree to the original manufacturer.

3.2.4. Adoption of Standards

After months of cross-industry deliberation that included collaboration from government on the traceability topic on SAE's G-19CI, the technical subject matter experts from the committee recommended that EEE parts verified from authorized sources maintain electronic part traceability during the procurement and receiving process that enables tracking of the supply chain back to the OCM or the OCM's authorized distributors, whether the electronic parts are supplied as discrete electronic parts or contained in assemblies. The group also recommended that EEE parts from sources other than authorized suppliers pursue clear identification of the name and location of supply chain intermediaries from OCM or authorized suppliers, and in the absence of this level of backwards traceability to the original manufacturer, that inspections, tests, and other risk mitigation methods should be applied. SAE published a standard, AS6496 "Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition—Authorized/Franchised Distribution," that addresses concerns from authorized distributor sources.[25] Organizations may want to invoke AS6496 on their authorized distributors to ensure that appropriate controls are in place to mitigate the risk of receiving counterfeit EEE parts and ensure that material acquired has traceability and pedigree to the original manufacturer. The Joint Electron Device Engineering Council (JEDEC) is currently developing a standard for original manufacturers to address the risk of counterfeit parts. Other available standards include SEMI T20-0710[39] and ISO/IEC JTC 1/SC 27, which is currently in development.[40] The ISO 31000 standard[41] also provides general risk management guidelines from an enterprise level and can be used to tailor anti-counterfeit and other risk management plans and activities for alignment with organizational goals and objectives.

3.2.5. Designing and Managing for Supply Chain Resilience

Supply chain resilience should be considered in addition to supply chain risk management. The central theme of supply chain resilience is that the supply chain should have the ability to recover to its original functional state after a disruption.[42–45]

Similarly to how organizations can design their supply chains to be resilient against disruptions such as natural and manmade disasters, supply chains must also be resilient to the introduction of counterfeits. While redundancy, flexibility, and corporate culture can be important factors that determine supply chain resilience,[44] recent research is focused on considering resilience as a system property; supply chain trust can act as an enabler of system-wide resilience.[45]

4. CONCLUSIONS

As the quality of counterfeit products increases, so does the effectiveness of the detection methods, as well as that of countermeasures. In years past, it was sufficient to simply conduct a visual inspection of the part(s) in question, but as time has progressed, more effective and reliable inspection methods have become required in order to maintain an appropriate level of security. And while new authentication methods such as DNA marking technology are becoming available, in a resource-constrained environment, the risk-based prioritization of countermeasures becomes critical. Risk analysis methods must be developed and implemented in parallel to complement these novel technologies.

Traceability does not provide any assurance with regard to quality and performance once the component leaves the authorized supply chain with appropriate material controls, regardless of the effectiveness of methodologies and procedures used. While traceability may show the chain of custody, it does not indicate whether the part has been properly packaged, stored, or handled or whether it has been tampered with along the way. Trusted sources throughout the supply chain need to maintain effective material controls to ensure appropriate material handling and storage, and to ensure material with traceability is not comingled with material without traceability. Future research is needed to build security and traceability upfront, in the design of electronic parts, that enables security and traceability throughout the components' lifecycle. This traceability, in conjunction with other good supply chain risk management practices, is critical for military acquisition risk management[46] and cyber-physical security.[47]

Though it is impossible to prevent counterfeits from entering a supply chain completely, it is entirely possible to reduce the frequency of their occurrence. Effectively securing the electronics supply chain against harmful counterfeits requires a wide-reaching, coordinated effort. Advances must be made in technological design, supply chain management, and risk analytics. Like three legs of a stool, without one, the others cannot stand. However, together, these fields can contribute to truly risk-informed decision making regarding strategies for counterfeit avoidance and supply chain resilience, thereby ensuring global economic prosperity and national security.

ACKNOWLEDGMENTS

The authors would like to thank Steve Walters and Joel Heebink for comments on the article. Permission was granted by the USACE Chief of Engineers to publish this material. The views and opinions expressed in this article are those of the individual authors and not those of the U.S. Army or other sponsor organizations.

REFERENCES

1. Frontier Economics. Estimating the Global Economic and Social Impacts of Counterfeiting and Piracy. London: Frontier Economics Ltd, 2011.
2. European Commission. Protecting Intellectual Property Rights: Customs Authorities Detain Nearly 36 Million Fake Goods at EU Borders in 2013. Brussels: European Commission, 2014. Available at: http://europa.eu/rapid/press-release_IP-14-890_en.htm.
3. US Department of Homeland Security. Intellectual Property Rights Seizures Statistics, Fiscal Year 2013. Washington, DC: Department of Homeland Security, 2013. Available at: http://www.cbp.gov/sites/default/files/documents/2013%20IPR%20Stats.pdf.
4. GAO. Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods. GAO-10-423. Washington, DC: Government Accountability Office, 2010.
5. Kelic A, Collier ZA, Brown C, Beyeler WE, Outkin AV, Vargas VN, Ehlen MA, Judson C, Zaidi A, Leung B, Linkov I. Decision framework for evaluating the macroeconomic risks and policy impacts of cyber attacks. Environment Systems and Decisions, 2013; 33(4):544–560.
6. GAO. Suspect Counterfeit Electronic Parts Can Be Found on Internet Purchasing Platforms. GAO-12-375. Washington, DC: Government Accountability Office, 2012.
7. Department of Commerce. Defense Industrial Base Assessment: Counterfeit Electronics. Washington, DC: Bureau of Industry and Security, Office of Technology Evaluation, 2010. Available at: http://www.bis.doc.gov/index.php/other-areas/office-of-technology-evaluation-ote/industrial-base-assessments.
8. Pecht M, Tiku S. Bogus: Electronic manufacturing and consumers confront a rising tide of counterfeit electronics. IEEE Spectrum, 2006; 43(5):37–46.
9. Rojo FJR, Roy R, Shehab E. Obsolescence management for long-life contracts: State of the art and future trends. International Journal of Advanced Manufacturing Technology, 2010; 49:1235–1250.
10. Guin U, Huang K, DiMase D, Carulli JM, Jr., Tehranipoor M, Makris Y. Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain. Proceedings of the IEEE, 2014; 102(8):1207–1228.
11. US White House. National Strategy for Global Supply Chain Security. Washington, DC: US White House, 2012. Available at: http://www.whitehouse.gov/sites/default/files/national_strategy_for_global_supply_chain_security.pdf.
12. Improving Critical Infrastructure Cybersecurity. Executive Order 13636, 2013. Available at: http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.
13. Hayward JA, Meraglia J. DNA to safeguard electrical components and protect against counterfeiting and diversion. In Proceedings from the 37th International Symposium for Testing and Failure Analysis, November 13–17, 2011, San Jose, CA, USA.
14. Ruhrmair U, Devadas S, Koushanfar F. Security based on physical unclonability and disorder. Pp. 65–102 in Tehranipoor M, Wang C (eds). Introduction to Hardware Security and Trust. New York: Springer, 2011.
15. Tehranipoor M, Wang C. Introduction to Hardware Security and Trust. New York: Springer, 2011.
16. Sood B, Das D, Pecht M. Screening for counterfeit electronic parts. Journal of Material Science: Materials in Electronics, 2011; 22(10):1511–1522.
17. Livingston H. Avoiding counterfeit electronic components. IEEE Transactions on Components and Packaging Technologies, 2007; 30(1):187–189.
18. Villasenor J. Compromised by Design? Securing the Defense Electronics Supply Chain. Washington, DC: Brookings Institution, 2013.
19. Collier ZA, Linkov I, DiMase D, Walters S, Tehranipoor M, Lambert JH. Cybersecurity standards: Managing risk and creating resilience. Computer, 2014; 47(9):70–76.
20. Linkov I, Anklam E, Collier ZA, DiMase D, Renn O. Risk-based standards: Integrating top-down and bottom-up

approaches. Environ Systems and Decisions, 2014; 34(1): 134–137.
21. Collier ZA, Walters S, DiMase D, Keisler JM, Linkov I. A semi-quantitative risk assessment standard for counterfeit electronics detection. SAE International Journal of Aerospace, 2014; 7(1):171–181.
22. Spekman RE, Kamauff JW, Jr., Myhr N. An empirical investigation into supply chain management: A perspective on partnerships. International Journal of Physical Distribution & Logistics Management, 1998; 28(8):630–650.
23. SAE. Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition. Society of Automotive Engineers, 2013. SAE AS5553A. Available at: http://standards.sae.org/as5553a/.
24. SAE. Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition—Distributors. Counterfeit Electronic Parts: Avoidance Protocol, Distributors. Society of Automotive Engineers, 2012. SAE AS6081. Available at: http://standards.sae.org/as6081/.
25. SAE. Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition—Authorized/Franchised Distribution. Society of Automotive Engineers, 2015. SAE AS6496. Available at: http://standards.sae.org/wip/as6496/.
26. Guin U, DiMase D, Tehranipoor M. Counterfeit integrated circuits: Detection, avoidance, and the challenges ahead. Journal of Electronic Testing, 2014; 30(1):9–23.
27. Vanany I, Zailani S, Pujawan N. Supply chain risk management: Literature review and future research. International Journal of Information Systems and Supply Chain Management, 2009; 2(1):16–33.
28. Tang CS. Perspectives in supply chain risk management. International Journal of Production Economics, 2006; 103(2):451–488.
29. Kleindorfer PR, Saad GH. Managing disruption risks in supply chains. Production and Operations Management, 2005; 14(1):53–68.
30. Norrman A, Lindroth R. Categorization of supply chain risk and risk management. Pp. 17–24 in Brindley C (ed). Supply Chain Risk. Hampshire: Ashgate Publishing Limited, 2004.
31. Beamon BM. Supply chain design and analysis: Models and methods. International Journal of Production Economics, 1998; 55(3):281–294.
32. Conrad SH, Beyeler WE, Brown TJ. The value of utilising stochastic mapping of food distribution networks for understanding risks and tracing contaminant pathways. International Journal of Critical Infrastructures, 2012; 8(2/3):216–224.
33. Lehtonen M, Michahelles F, Fleisch E. Probabilistic Approach for Location-Based Authentication. Auto-ID LabsWhite Paper WP-SWNET-020. Zurich: Swiss Federal Institute of Technology (ETH) Zurich Department of Management, Technology and Economics, 2007.
34. Franck C. Framework for supply chain risk management. Supply Chain Forum, 2007; 8(2):2–13.
35. Schaffer M. Development of a Methodology to Determine Risk of Counterfeit Use. Hendron, VA: International Electronics Manufacturing Initiative, 2013. Available at: http://thor.inemi.org/webdownload/projects/Miniaturization/Counterfeit_WhitePaper_110513.pdf.
36. Enyinda CI, Szmerekovsky J. Sense and respond supply chain: A prescription for mitigating vulnerability in the U.S. pharmaceutical value chain. Journal of Global Business Issues, 2008; 2(2):95–103.
37. Contractor Counterfeit Electronic Part Detection and Avoidance System. Washington, DC: Defense Federal Acquisition Regulation Supplement 252.246-7007, 2014. Available at: http://www.acq.osd.mil/dpap/dars/dfars/html/current/252246.htm.
38. Carter AB. Better Buying Power: Mandate for Restoring Affordability and Productivity in Defense Spending. Washington, DC: Office of the Under Secretary of Defense, Acquisition Technology and Logistics, 2010. Available at: http://bbp.dau.mil/docs/Better%20Buying%20Power–Mandate%20for%20Restoring%20Affordability%20and%20Productivity%20in%20Defense%20Spending.pdf.
39. SEMI. Specification for Authentication of Semiconductors and Related Products. SEMI International Standards, 2009. SEMI T20-0710. Available at: http://ams.semi.org/ebusiness/standards/SEMIStandardDetail.aspx?ProductID=211&DownloadID=1685.
40. ISO. ISO/IEC JTC 1/SC 27 —IT Security Techniques. International Organization for Standardization, 2014. Available at: http://www.jtc1sc27.din.de/cmd?level=tpl-home&contextid=jtc1sc27&languageid=en.
41. ISO. ISO 31000—Risk Management. International Organization for Standardization, 2009. Available at: http://www.iso.org/iso/home/standards/iso31000.htm.
42. Christopher M, Peck H. Building the resilient supply chain. International Journal of Logistics Management, 2004; 15(2):1–13.
43. Fiksel J, Polyviou M, Croxton KL, Petit TJ. From risk to resilience: Learning to deal with disruption. MIT Sloan Management Review, 2015; 56(2):1–8.
44. Sheffi Y. Building a resilient supply chain. Harvard Business Review, 2005; 1(8):1–4.
45. Collier ZA, DiMase D, Heffner K, Linkov I. Building a trusted and agile supply chain network for electronic hardware. Proceedings from the 20th International Command and Control Research and Technology Symposium, June 16–19, 2015, Annapolis, MD, USA.
46. Linkov I, Trump BD, Pabon N, Collier ZA, Keisler JM, Scriven J. A decision analytic approach to Department of Defense acquisition risk management. Military Operations Research, 2012; 17(2):53–70.
47. DiMase D, Collier ZA, Heffner K, Linkov I. Systems engineering framework for cyber physical security and resilience. Environment Systems and Decisions, 35(2):291–300.