IPIC 2016
3rd International Physical Internet Conference
June 29-July 1, 2016 | Atlanta, GA USA

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

Douglas A. Bodner[1]
1. Tennenbaum Institute, Georgia Institute of Technology, Atlanta, Georgia, USA
Corresponding author: doug.bodner@gatech.edu

Abstract: *Recent years have seen counterfeit part intrusions into the defense supply chain. Previous work has studied this problem using enterprise simulation to determine effective combinations of policies to mitigate the effects of counterfeits. This paper considers a transformed version of the enterprise and its supply chain as a means of combating the counterfeiting problem. Elements of this transformation are consistent with the Physical Internet paradigm. This paper presents the transformed enterprise and supply chain, as well as an enterprise simulation model that can be used to evaluate the transformed enterprise, as well as different pathways of transformation.*

Keywords: *Counterfeit parts, enterprise simulation, open collaborative supply chain, enterprise transformation*

1 Introduction

Supply chains are increasingly subject to intrusions from counterfeit parts. For instance, the past fifteen to twenty years have seen the issue of counterfeits parts manifest in the defense supply chain (Government Accountability Office, 2012; Pecht and Tiku, 2006; Senate Armed Services Committee, 2012; Stradley and Karraker, 2006). For the most part, counterfeits have been electronic components such as integrated circuits and field-programmable gate arrays (Guin et al., 2014). These parts are used primarily as replacement parts in sub-systems for submarines, aircraft and other military platforms. Counterfeit parts pose safety and reliability risks for these platforms. They also pose cybersecurity risks, as electronic components may contain back-doors and other security threats.

We can look at two perspectives for the rise of counterfeiting. First, there are global trends driving this phenomenon. Electronics manufacturing has been mostly off-shored from the United States. Most discovered counterfeiting incidents are traced back to foreign sources. Sub-systems are increasingly complex. Thus, it is difficult to detect counterfeit components that are constituents in these sub-systems. Military systems are deployed in service for longer periods of time, driving obsolescence of sub-systems and components. It becomes more difficult to source genuine replacement components for obsolete sub-systems (Livingston, 2007). Finally, electronic waste has become a significant problem for developed countries. While responsible recycling exists, large quantities of waste are shipped to third-world nations, and some electronic components return to the supply chain as recycled or defective components that are re-marked as new (Senate Armed Services Committee, 2012).

For a second perspective, we can also look at the characteristics of the supply chain. The defense supply chain is a multi-tiered, complex network of suppliers. Lead systems integrators have traditionally not had visibility to suppliers that are more than one or two times removed from them. The defense supply base has experienced the phenomena of sole-sourcing and diminishing suppliers, both of which pose original supplier sourcing risks that may lead to sourcing from counterfeiters. Finally, the supply chain operates as an extended enterprise (Rouse, 2005a) consisting of government agencies and private firms. The Department of Defense can set policies for acquisition and sustainment supply chains. Customs and Border Patrol inspects incoming goods for counterfeits, and the Department of Justice investigates and prosecutes counterfeiting crimes. Yet, there is no locus of control, and counterfeiters and legitimate suppliers may exhibit adaptive behavior that undermines the effectiveness of policy intents. The enterprise can be considered as a complex adaptive system (Miller and Page, 2007).

Our previous research has investigated the problem of counterfeit parts in the defense supply chain using enterprise simulation (Bodner, 2015). This approach has allowed testing of different anti-counterfeiting policies in this extended enterprise in which adaptive behavior can cause unintended secondary effects. Policies include supplier qualification, increased test and evaluation, planned sub-system design refreshes, lifetime buys of obsolete components, system design considerations for selection of reliable suppliers, and restrictions on export of electronic waste. In this paper, we extend this model to consider the threat from counterfeit parts in the context of a transformed enterprise using an open and collaborative supply chain that can enable new protocols for addressing counterfeits, similar to a Physical Internet supply chain (Montreuil, 2011). Such protocols include supplier reliability ratings, supplier visibility through tiers, and lifecycle part tracking.

The paper addresses how this open and collaborative supply chain is modeled using enterprise simulation. Section 2 describes the relatively new field of enterprise simulation and the existing enterprise model for counterfeit parts. Section 3 discusses transformation of the supply chain enterprise to a collaborative supply chain with policies and protocols for counterfeit mitigation. Section 4 presents an enterprise simulation model for this transformed enterprise with example of policies and their effectiveness. Finally, Section 5 concludes with discussion on potential obstacles to the transformation from the current supply chain to the open and collaborative supply chain enterprise.

2 Enterprise Simulation

There has been an increasing interest in the research community in the study of enterprises from several perspectives. These range from network analysis (Basole et al., 2011), to operational improvement (Wirthlin, 2009), to multi-actor policy analysis (Park et al., 2012), to enterprise transformation (Glazner, 2011). Enterprises consist of a complex set of phenomena that combine technical aspects and socio-behavioral aspects of organizations. For instance, technical behavior consists of organizational processes and work products. Socio-behavior emerges from how multiple individuals and organization react to information and incentives.

Simulation is a useful method to study complex systems with uncertain and emergent behavior. However, due to the complex nature of enterprises, we have found that no single simulation paradigm captures complete set of the structure and behavior. Discrete-event simulation best addresses those types of enterprise problems that are heavily process-focused (Barijis, 2011; Pennock and Rouse, 2008; Wirthlin, 2009). Agent-based simulation is useful in multi-actor enterprises where actors act and react to information and incentives (Hakimi et al., 2010; Hakimi et al., 2012; Park et al., 2012). System dynamics models can represent lags and feedback loops in enterprise behaviors such as funding, research and development, and product introduction and lifecycles (Affeldt, 1999; Rabelo et al., 2005).

We have developed an enterprise simulation modeling framework that combines these three simulation paradigms so that each can be used to model aspects of the enterprise for which it is best suited. This framework is based on a modified version of an enterprise modeling methodology described in Pennock et al. (2016):

1. After the question of interest is defined, the relevant layers of phenomena in the enterprise are conceptually modeled. This often occurs at four levels – the eco-system level, the enterprise network structure level, the delivery operations level, and the work practices level.
2. A core model of phenomena is identified, designed and implemented.
3. Peripheral models are identified and developed consistent with the core model. Then these are integrated into the overall model as needed.
4. Experimentation is conducted with the core model and various peripheral models to identify the effects and interactions of enterprise and individual actor policies.

This framework is implemented using AnyLogic® 7, a simulation software package that allows the three simulation paradigms to be integrated into a single model. It also provides Java™ class extensions for modeling specialized aspects of enterprises. For the problem of counterfeit parts in the supply chain, the following sub-models have been identified and developed (Bodner, 2015).

- *Systems and constituents*. The enterprise produces and sustains systems (i.e., weapons systems, planes, ships, unmanned aerial vehicles, etc.). These have constituent parts in the form of sub-systems and components. A sub-model is used to represent these systems and their constituents, plus the bill-of-materials that relates the systems to their constituents. This is implemented using agent-based modeling, with the different constituents having state transitions representing failures and repairs.
- *Supply chain operations*. A supply chain sub-model contains the factories and inventories for each component and sub-system. Fabrication factories manufacture components, and then a series of assembly factories assemble minor sub-systems, then major sub-systems, and finally the overall system. In addition, components and sub-systems are shipped from the factory to various field locations for use in maintenance and repair. This is also represented using agent-based models. Factory and inventory agents communicate with one another in ordering and shipping parts through the supply chain. Components can be inspected at various places, including at customs stations and entry points to the DoD supply chain.
- *Enterprise actors and relationship network*. Suppliers that own factories and other locations in the supply chain model are represented in an agent-based enterprise actor sub-model. Counterfeiters are represented as enterprise actors, as well. Suppliers contract with other suppliers, and they react to changing market conditions and policies. For instance, a supplier may decide to leave the market for a particular type of sub-system due to lowered profit margins. The firms to which it supplies would then need to find another supplier for that sub-system.
- *Policy actors*. A policy actor model represents the various agencies and other organizations that enact policies affecting counterfeit parts. Policy actors include the Department of Defense, Customs and Border Patrol, and the Department of Justice. Their policy decisions affect the behavior of the enterprise actors and also may affect activities in the supply chain. For instance, policies that increase the cost of doing business may result in supplier diminishment. Policies may also affect supply chain operations such as increased testing and inspection.
- *Exogenous environment*. An exogenous environment sub-model represents the external world and its effect on counterfeiting and anti-counterfeiting policies. Currently,

technology progression and electronic waste disposal are modeled. These are peripheral models that can be used for particular analyses.

The relationships of these sub-models to one another are shown in Figure 1.

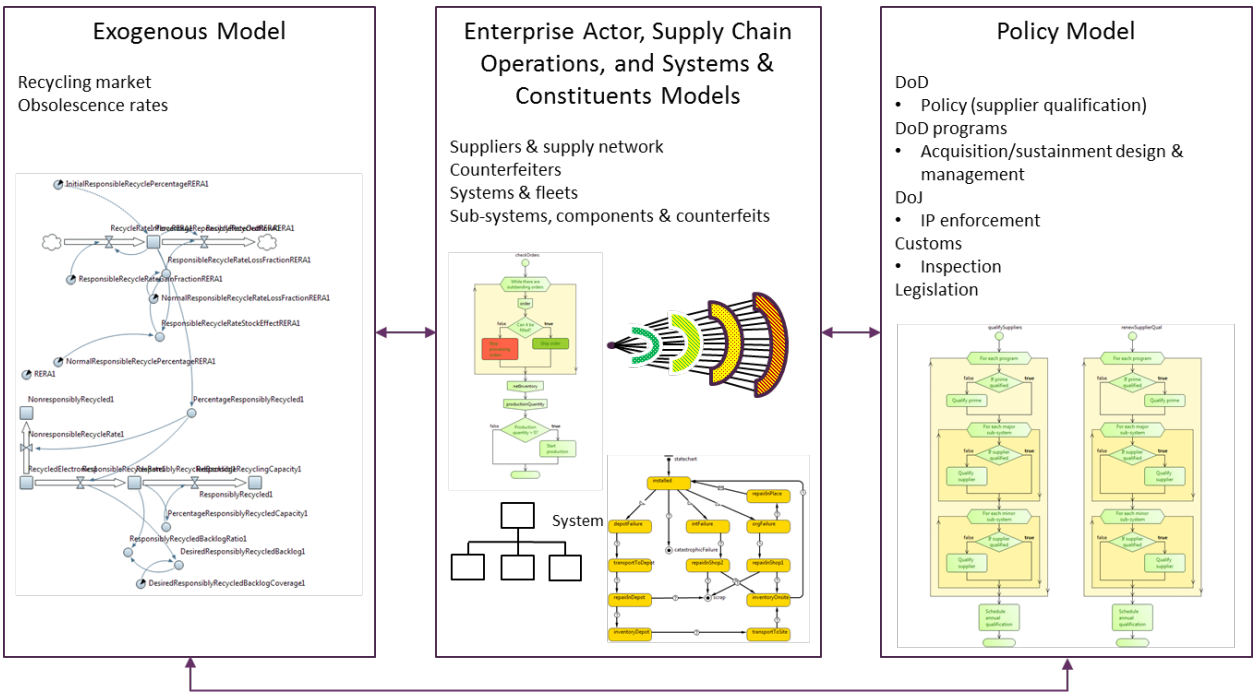

Figure 1: Enterprise simulation sub-models

This model has been used to study the effectiveness of different policies such as supplier qualification, increased component testing, and resources devoted to investigation and prosecution on different enterprise performance measures, including

- Cost,
- Availability of fielded systems,
- Number of counterfeit suspects interdicted and counterfeit escapes allowed.

The model has an interface with policy controls and an enterprise status dashboard. This allows the analyst to experiment with different policy options and see the resulting enterprise performance over time.

3 Transformation to Address Counterfeit Parts

In this section, we discuss transforming the supply chain enterprise to be consistent with selected precepts of the Physical Internet paradigm that could aid in mitigation of counterfeit parts.

3.1 Transformation framework

Enterprise transformation is a purposeful effort at substantial change in an enterprise within a relatively short timeframe. Transformation typically is driven by some sort of value deficiency, which could be unrealized potential value or a threat to current value (Rouse, 2005b). Transformation is the process of moving from an as-is enterprise to a to-be enterprise. Since transformation is a substantial undertaking, it is important to plan the pathway or set of steps that comprise the transformation. Since alternate pathways and alternate to-be enterprises exist in any

transformation effort, enterprise simulation can be a useful tool in assessing pathways and potential to-be enterprises. This concept is illustrated in Figure 2.

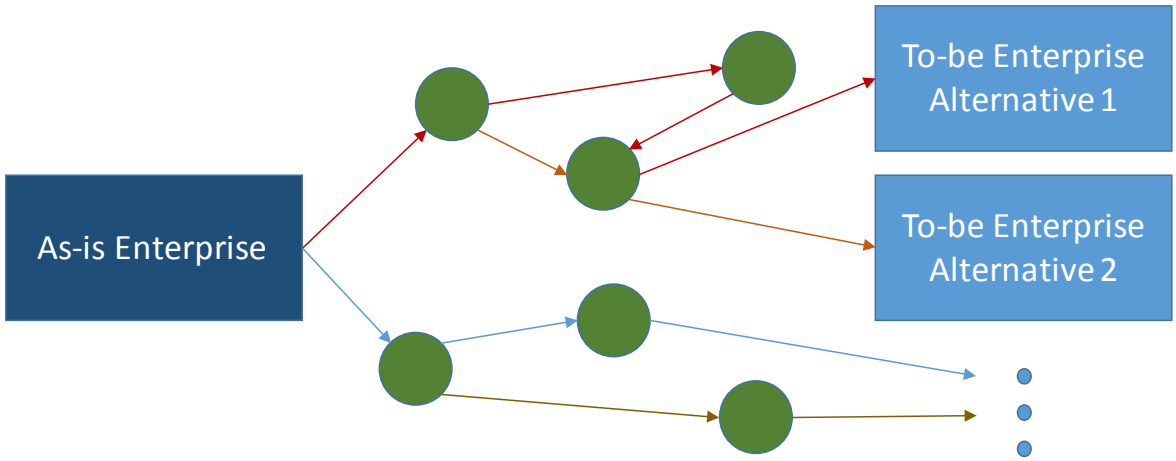

Figure 2: Transformation framework

3.2 Description of to-be enterprise

Clearly, counterfeit parts pose a threat to value in terms of reliability, safety and security. The problem of counterfeiting may not provide enough justification to pursue a full-scale enterprise transformation, though. Therefore, we also align it with recent DoD initiatives in acquisition reform, most particularly the Better Buying Power initiative that seeks to reduce costs associated with acquiring weapons systems and other items (Department of Defense, 2016). This is a large-scale effort aimed at improving value through reduced cost, and it would most likely justify a transformation. Some of its tenets include increased competition, use of commercial technology and open system architectures.

The current enterprise is addressing the counterfeit parts problem via application of selected policies to the existing enterprise and supply chain. We envision a to-be enterprise that is transformed to a collaborative supply chain enterprise with certain elements that are related to the Physical Internet paradigm as well as the Better Buying Power initiative. The notion of a collaborative enterprise for the defense supply chain enterprises has been a trend in recent years (Kessler et al., 2012). The to-be enterprise considered here is characterized by transformation elements shown in Table 1. These are linked to relevant Physical Internet principles as described by Montreuil (2011). It should be noted that the Physical Internet principles relate to sourcing rather than transportation, since sourcing is more relevant to counterfeit mitigation. However, the transportation-related Physical Internet principles could be considered in efforts to make the supply chain more efficient and sustainable.

Taken together, these transformation elements facilitate moving the DoD supply chain enterprise to a new to-be state of an open collaborative enterprise. Many parts require controlled environments, and transport/storage in these environments must be verified and documented for the part to be considered genuine. Thus, it would be important to have containers and packaging that keep sensitive parts in controlled environments with automatic verification, to increase trust that environmental conditions have been met. Supplier reliability ratings would be based on counterfeit-free supplies, in addition to other metrics such as lead times. It should be noted that there is a reporting system for counterfeit suspects and other part issues (GIDEP, 2016), so supplier reliability ratings would expand on this reporting system. Lifecycle tracking of parts has been proposed, but is difficult to implement due to technology limitations. Research into such technologies as plant DNA is being conducted to overcome this problem (Harbert, 2012). This would facilitate trust in part genuineness. A trusted foundry currently exists and is a set of suppliers that can produce

discontinued electronics based on reverse engineered processes (Trusted Foundry, 2016). Expanded use of this concept involves improved digitization of part designs and processes so that obsolete and discontinued parts can be brought into production again in a cost-efficient and timely manner.

Table 1: Transformation elements of to-be enterprise

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

4 Model of Transformed Enterprise and Supply Chain

Here, we discuss the modeling of the above elements in the enterprise simulation model for purposes of studying potential transformations.

4.1 Systems and constituents

The systems and constituents sub-model addresses components, sub-systems and systems. It originally did not track parts through their lifecycles, but this tracking is now enabled by a log that is kept for each part. Also, the sub-model originally had a basic shipment object that functions as a collection of material objects (e.g., components or sub-systems) for purposes of transporting multiple material objects together. A new container object is introduced to model the smart containers that are envisioned for use in tracking components through their lifecycles and for documenting and providing verification of required environmental conditions for sensitive parts. For instance, many electronic components should be stored in electro-static bags. A component can be considered as counterfeit if it is not stored properly and then passed with forged documentation stating that it has been stored properly.

A shipment object is modified to consist of a collection of container objects. A container object has the following attributes:

- Capacity

- Environmental state (temperature, whether parts are in sealed packages, etc.)
- Log of locations traversed (chain of custody) and environmental state history

In addition to its own log, the container has methods to log the history of each part in terms of chain of custody and environmental conditions for the part while it is in the container object.

4.2 Supply chain

A reliability rating is added for each facility in the supply chain. Currently, this rating addresses only whether a counterfeit suspect has been identified as having passed through the facility without being identified. It is in the form of a percentage currently. This could be extended in the future to include additional information such as lead time performance, reliability of parts produced, etc. When a counterfeit suspect is identified, its log is referenced to determine facilities that are in its chain of custody so that the reliability of those facilities can be adjusted.

In addition, when a component or sub-system is assembled into another constituent in a factory or in the field as a replacement, its log is updated to show that it has been used. As it undergoes maintenance and repairs operations in the field, these are updated in the log as well.

4.3 Enterprise actors

Based on facilities owned by each supplier, a reliability for the supplier is computed. Currently, this averages the reliability over all the supplier's facilities. However, it could be weighted by part criticality. When a firm is looking for a supplier for a particular part, it can use the reliability rating as well as cost for decision-making. The more critical a part is to the functionality and safety of the system in which it is to be placed, the more sensitive the firm can be to reducing risk by selecting a reliable supplier.

Due to the network of agents, the original enterprise simulation provided capability for full visibility of supplier through the various tiers. Methods have been added to the supplier agents to take advantage of the network structure so that a lead system integrator, for instance, can query on one of its direct suppliers and receive information on all suppliers used by that supplier in its supply chain network. Thus, a supplier can access the reliability of all suppliers used by a potential supplier in making sourcing decisions. In addition, analytics can be performed on the supplier network to determine risks such as sole-sourcing.

Finally, the use of the trusted foundry is expanded in the model. In the original model, only a pre-specified set of components are manufactured by the trusted foundry. Now, when a supplier leaves the market for a particular component, the program that uses the component can request that the trusted foundry produce the component. We assume that this is enabled by transfer of digital design data plus permission of the original IP holder.

4.4 Policy actors

We keep the original set of policy options and actors in the model, but for purposes of studying transformation, we develop a new transformation agent that enables the various transformation elements according to a pre-specified transformation pathway. The idea is to provide capability to study potential to-be enterprises as well as pathways to them. This will require substantial enhancement of the user interface for the model so that the user can specify a particular pathway with timing and also dependency relations. This interface represents future work. In addition, the open system architecture and use of commercial parts are not yet modeled

5 Conclusion and Future Research

This paper has described transformation of the defense supply chain enterprise along precepts found in the Physical Internet to help address the problem of counterfeit part intrusions. An existing policy simulation is adapted so that it can be used to study the transformation from the as-is enterprise to a

potential to-be enterprise. Various transformation elements are proposed to comprise the to-be enterprise.

It should be noted that the enterprise simulation model does not address several potential barriers to a transformation effort. First, it does not address the culture change that needs to occur in the enterprise to enable the transformation. Second, most actors in the defense sector guard their intellectual property and may be reluctant to participate in an open enterprise unless there are IP safeguards. Related to this, some components and sub-systems are sensitive in terms of mission-critical value, and there would be reluctance to operate those in an open enterprise without some type of safeguards. Finally, counterfeiting is a sensitive issue, and firms are reluctant to admit that they have passed potential counterfeits, and they may also be reluctant to report incidents involving business partners. In this regard, there is substantial education needed in the industry on proper reporting.

Future work involves using the enterprise simulation model to study different potential transformation scenarios. Part of this work involves obtaining data in the form of cost estimates and durations for the various transformation elements. The overall goal would be to use the simulation model as a platform to study trade-offs between cost, deployed system availability, and counterfeit intrusions.

Acknowledgments

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

References

Affeldt, J.F. (1999): *The Application of System Dynamics (SD) Simulation to Enterprise Management*, Proceedings of the 1999 Winter Simulation Conference, 1496-1500.

Barjis. J. (2011): *Enterprise Modeling and Simulation within Enterprise Engineering*, Journal of Enterprise Transformation, v1, 185-207.

Basole, R.C., W.B. Rouse, L.F. McGinnis, D.A. Bodner, W.C.Kessler (2011): *Models of Complex Enterprise Networks*, Journal of Enterprise Transformation.

Bodner, D.A. (2015): *Mitigating Counterfeit Part Intrusions with Enterprise Simulation*, Procedia Computer Science, v61, 233-239.

Department of Defense (2016). Better Buying Power, http://bbp.dau.mil.

GIDEP (2016). Governemnt-Industry Data Exchange Program, http://www.gidep.org.

Glazner C. (2011). *Enterprise Transformation Using a Simulation of Enterprise Architecture*, Journal of Enterprise Transformation, v1, 231-60.

Government Accountability Office (2012): Suspect Counterfeit Electronic Parts Can Be Found on Internet Purchasing Platforms, Report GAO-12-375. Washington, DC.

Guin U., D. Dimase, M. Tehranipoor (2014): *Counterfeit Integrated Circuits: Detection, Avoidance, and the Challenges Ahead*, Journal of Electronic Test.

Hakimi D., B. Montreuil, O. Labarthe (2010): *Supply Web Agent-Based Simulation Platform*, Proceedings of the 2010 International Conference on Information Systems, Logistics and Supply Chain, Casablanca, Morocco.

Hakimi, D., B. Montreuil, R. Sarraj, E. Ballot, S. Pan (2012): *Simulating a Physical Internet Enabled Mobility Web: The Case of Mass Distribution in France*, Proceedings of the 2012 International Conference of Modeling, Optimization and Simulation, Bordeaux, France.

Harbert, T. (2012). *Plant DNA vs. Counterfeit Chips*, IEEE Spectrum, http://spectrum.ieee.org/semiconductors/devices/plant-dna-vs-counterfeit-chips.

Kessler, W.C., L.F. McGinnis, N. Bennett, eds. (2012). Enterprise Transformation: Manufacturing in a Global Enterprise, IOS Press.

Livingston H. (2007): *Avoiding Counterfeit Electronic Components*, IEEE Transactions on Components, Packaging, and Manufacturing Technology, v30, 187-189.
Miller J.H., S.E. Page (2007): Complex Adaptive Systems: An Introduction to Computational Models of Social Life. Princeton University Press, U.S.A.
Montreuil B. (2011): *Towards a Physical Internet: Meeting the Global Logistics Sustainability Grand Challenge,* Logistics Research, v3, no2-3, 71-87.
Park, H., T. Clear, W.B. Rouse, et al. (2012): *Multi-level Simulation of Health Delivery Systems: A Prospective Tool for Policy, Strategy, Planning, and Management*, Service Science, v4, 253-268.
Pecht M, S. Tiku (2006): *Bogus: Electronic Manufacturing and Consumers Confront a Rising Tide of Counterfeit Electronics*, IEEE Spectrum, v43, 37-46.
Pennock, M.J., W.B. Rouse (2008): *The Costs and Risks of Maturing Technologies, Traditional vs. Evolutionary Approaches*, Proceedings of the 2008 Acquisition Research Symnposium, Monterey, CA, 106-126.
Pennock, M.J., W.B. Rouse, D.A. Bodner, C. Gaffney, J. Hinkel, C. Klesges, M. Oghbaie (2016). *Enterprise Systems Analysis*, Technical Report SERC-2016-TR-103, Systems Engineering Research Center, Hoboken, NJ.
Rabelo, L., M. Helal, A. Jones, H.-S. Min (2005): *Enterprise Simulation: A Hybrid System Approach*, International Journal of Computer Integrated Manufacturing, v18, no6, 498-508.
Rouse, W.B. (2005a): *Enterprises as Systems: Essential Challenges and Approaches to Transformation*, Systems Engineering, v8, no2, 138-50.
Rouse, W.B. (2005b) *A Thoery of Enterprise Transformation*, Systems Engineering, v8, no4, 279-295.
Senate Armed Services Committee (2012): Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain, Washington, DC.
Stradley J., D. Karraker (2006): *The Electronic Part Supply Chain and Risks of Counterfeit Parts in Defense Applications*, IEEE Transactions on Components, Packaging, and Manufacturing Technology, v29, 703-705.
Trusted Foundry (2016). Trusted Foundry Program, https://dodtechspace.dtic.mil/groups/trusted-microelectronics.
Wirthlin, J.R. (2009): Identifying Enterprise Leverage Points in Defense Acquisition Program Performance, Doctoral Dissertation, Massachusetts Institute of Technology, U.S.A.