20th ICCRTS

Title of Paper:

Building a Trusted and Agile Supply Chain Network for Electronic Hardware

---

Authors:

Zachary A. Collier
US Army Engineer Research & Development Center
3909 Halls Ferry Road, Vicksburg, MS 39180
601-634-7570
Zachary.A.Collier@usace.army.mil

Daniel DiMase
SAE G19 Standards Development Committee
400 Commonwealth Drive, Warrendale, PA 15096
480-707-0656
Daniel.DiMase@Honeywell.com

Kenneth Heffner
SAE G19 Standards Development Committee
400 Commonwealth Drive, Warrendale, PA 15096
727-539-4205
kenneth.h.heffner@honeywell.com

Igor Linkov
US Army Engineer Research & Development Center
696 Virginia Road, Concord, MA 01742
978-318-8197
Igor.Linkov@usace.army.mil

Point of Contact: Igor Linkov

Topics:

6) Cyberspace, Communications, and Information Networks
1) Concepts, Theory, and Policy
11) Agile C2 Security

Building a Trusted and Agile Supply Chain Network for Electronic Hardware

Zachary A. Collier[1], Daniel DiMase[2], Kenneth Heffner[2], Igor Linkov[1]

[1]US Army Engineer Research & Development Center
[2]SAE G19 Standards Development Committee

Abstract: Modern military and industrial activities are characterized by global connectivity, including material and information flows through highly interconnected networks. This is especially true of the cyber physical systems domain, where the systems are vulnerable to a number of concerns impacting quality, safety, and security. For example, the supply chain is no longer vertical, and outsourcing occurs on a number of fronts, including the electronics hardware acquired. Malicious Trojans and tampering are potential threats that may originate from untrusted sources, and pose a substantial threat to the security of information and the reliability of mission critical systems. Certification programs exist, such as the DoD's Trusted Foundry Program, which accredits certain suppliers. However it is not always possible to purchase items through trusted suppliers due to obsolescence and other market dynamics. In this paper, we outline some current efforts related to hardware security and trust, and apply the principles of C2 Agility to the hardware supply chain. We explore the link between agility, resilience (defined by some as an enabler of agility), and trust. In addition, we will suggest future efforts by which to embed and promote trust throughout the supply chain network in order to enhance agility.

1. Introduction

Changes in the electronics manufacturing industry, including increasing costs of building fabrication facilities and the quickened pace of technological innovation, have given rise to contract manufacturing (Mason et al., 2002). This trend towards outsourcing of manufacturing, coupled with rapid obsolescence, has increased the necessity to purchase parts from potentially *untrusted* sources, increasing the likelihood of counterfeit parts being introduced into the supply chain (Pecht & Tiku, 2006; Rojo et al., 2010; Villasenor, 2013). Villasenor (2013) concludes that in the electronics supply chain, "Trust should not be assumed", and for good reason - these counterfeit electrical, electronic, and electromechanical (EEE) parts may be relabeled, refurbished, or repackaged to misrepresent the component's authenticity (Sood et al., 2011). The supply chain and associated systems in which the electronic parts service are highly networked, and this "ubiquitous connectivity" (Alberts, 2010) means that a compromised system can trigger failures that cascade throughout multiple critical infrastructure systems and economic sectors (Rinaldi et al., 2001; Kelic et al., 2013).

Of particular concern is the introduction of counterfeits into the Department of Defense (DoD) supply chain. The U.S. Department of Commerce found over 8,000 reported occurrences of counterfeits in one year within the defense industrial base (Department of Commerce, 2010). A report from the U.S. Senate Armed Services Committee (2012) concluded that the "reliance on unvetted independent distributors to supply electronic parts for critical military applications results in unacceptable risks to national security and the safety of U.S. military personnel."

In response to these concerns, the U.S. White House (2009) identified supply chain security as a priority in their Cyberspace Policy Review, and the 2012 National Defense Authorization Act sets forth a "risk-based approach" for counterfeit avoidance (2011). More generally, Executive Order 13636 (2013) and Presidential Policy Directive 21 (2013) call for similar risk-based protections against a wide array of cyber threats.

Despite calls for risk-based approaches, it has been argued elsewhere that the situation of hardware security is too complex and highly uncertain for the traditional risk assessment paradigm (Collier et al.,

2014a; Linkov et al. 2014a; Fiksel et al. 2015), and that a shift in thinking towards *resilience* is more appropriate (Linkov et al. 2014b). A resilience-oriented approach does not focus exclusively on prevention, an approach that incurs an unavoidable failure rate. Adding a focus on resilience, while still seeking to minimize failures, seeks to mitigate the consequences of these failures where they inevitably occur. Moreover, since semiconductor production and design are increasingly conducted outside of the U.S., the issue of *trust* in the supply chain is becoming especially critical (Villasenor, 2013). However, resilience, trust, and related terms such as agility, are often difficult to define and may have different nuances depending on the application area.

In this paper, we first examine how the terms resilience, agility, and trust can be defined in terms of supply chains. Then, based on these definitions, we place the supply chain into a command and control (C2) context, based on the work of Alberts (2011), and explore how the concepts relate to one another. Finally, we describe some ongoing efforts related to trust in the electronics supply chain, and outline areas for future research necessary to build a trusted and agile supply chain.

2. Background and Definitions

2.1. Resilience

Traditional supply chain risk management (SCRM) research has focused on cost minimization, balancing expected losses with risk management controls (Kleindorfer & Saad, 2005; Carvalho & Cruz-Machado, 2011). Moreover, much of the literature is based on disruptions such as catastrophies or uncertainties in external market conditions (Vanany et al., 2009; Tang, 2006; Kleindorfer & Saad, 2005; Norman & Lindroth, 2004). However, the practices that organizations use for cost minimization (e.g., just-in-time inventory management) can also make supply chains vulnerable to disruptions (Fiksel et al., 2015). Given the inherent unpredictability in the factors that relate to supply chain vulnerability, (Fiksel et al. (2015) define six vulnerability factors: turbulence, deliberate threats, external pressures, resource limits, sensitivity, and connectivity), a shift away from risk management and towards resilience management is necessary.

Table 1 lists some selected definitions of supply chain resilience. Common among them is the theme of "bouncing back" from a catastrophic disruption to an original state of functionality, or potentially a different but more desirable state. Sheffi (2005) similarly claims that supply chain resilience implies the ability to not only manage disruptions, but to derive advantage from them.

Table 1: Definitions and Factors of Supply Chain Resilience

Definition	Factors	Source
"The ability of a system to return to its original state or move to a new, more desirable state after being disturbed"	Supply chain re-engineering, Supply chain collaboration, Supply chain risk management culture, Agility	Christopher & Peck, 2004
"The ability of a company to bounce back from a large disruption – this includes, for instance, the speed with which it returns to normal performance levels"	Redundancy, Flexibility, Corporate culture	Sheffi, 2005
"The ability of a supply chain system to reduce the probabilities of a disruption, to reduce the consequences of those disruptions once they occur, and to reduce the time to recover normal performance"	Supply chain density, Supply chain complexity, Node criticality	Falasca et al., 2008
"Resilience refers to the ability of the supply chain to cope with unexpected disturbances. It is concerned with the system ability to return to its	Capacity buffers, Risk sharing, Responsiveness, Strategic inventory, Small batch sizes, Flexible	Carvalho & Cruz-Machado, 2011

original state or to a new one, more desirable, after experiencing a disturbance, and avoiding the occurrence of failure modes"	transportation, Demand visibility	
"The capacity of an enterprise to survive, adapt and grow in the face of turbulent change"	Flexibility in sourcing, Flexibility in manufacturing, Flexibility in order fulfillment, Production capacity, Efficiency, Visibility, Adaptability, Anticipation, Recovery, Dispersion, Collaboration, Organization, Market position, Security, Financial strength, Product stewardship	Fiksel et al., 2015

There is no consensus in the literature about what factors mediate supply chain resilience. For instance, Sheffi (2005) lists three qualitative factors: redundancy, flexibility, and culture. Fascala et al. (2008) list three measurable, network-based factors, including density (geographic spacing of nodes), complexity (number of connections between nodes), and node criticality (importance of nodes within the system). Fiksel et al. (2015) developed 16 factors that influence resilience. While the lists of factors vary, similar themes reoccur, such as flexibility, adaptability, the ability to map out the supply chain process, and a supportive organizational culture.

2.2. Agility

In contrast to supply chain resilience which was focused on bouncing back from disruptions, supply chain agility places a greater emphasis on the speed of meeting customer demands (responsiveness) in a turbulent and uncertain environment, as shown in Table 2. It is important to note that agility, as the term is used here, is not to be confused with *leanness*, which is focused on reducing waste in the supply chain and is often associated with low-inventory processes, such as those popularized by Toyota (Christopher & Towill, 2001; Christopher, 2000). Christopher (2000) shows that agility, rather than leanness, is particularly necessary in environments when demand is volatile and variety is high.

Table 2: Definitions and Factors of Supply Chain Agility

Definition	**Factors**	**Source**
"The ability to respond rapidly to unpredictable changes in demand or supply"	Market sensitivity, Virtual data sharing, Process integration, Networks	Christopher & Peck, 2004; Christopher, 2000
"The ability of a supply chain to rapidly respond to changes in market and customer demands"	Responsiveness, Competancy, Flexibility/adaptability, Quickness/speed	Sharp et al., 1999; Lin et al., 2006
"An agile supply chain is an integration of business partners to enable new competencies in order to respond to rapidly changing, continually fragmenting markets"	Speed, Quality, Flexibility, Responsiveness	Baramichai et al., 2007

In contrast with resilience, which typically is defined in terms of a catastrophic disruption, agility is focused on relatively minor fluctuations, typically in supply or demand (Collin & Lorenzin, 2006). However, similar to resilience, a critical component of agility is the speed at which the system responds to the fluctuations (Lin et al., 2006). However, speed alone is not agility, but rather the ability to quickly "realize enterprise objectives" (Lin et al., 2006). This meeting of goals also requires the ability to sense and respond to changes, which Lin et al., (2006) refer to as "responsiveness", and Christopher (2000) refers to as "market sensitivity". On the other hand, according to Lin et al. (2006), "flexibility" is the ability to creatively leverage different processes and tools to achieve the same result. According to

Christopher (2000), relationships are critical to the sharing of information and cooperation between a network of coordinated actors pursuing the same goals.

2.3. Trust

Within the supply chain literature, trust has been a difficult concept to define. Speckman et al. (1998) define trust as a belief, held by an actor in the supply chain, that another actor will act consistently and do what they claim that they will do. Belief that a partner will act consistently, with honesty, integrity, reliability, and justice are all listed as important features of trust, especially in that this belief will decrease behavioral uncertainty between partners (Akkermans et al. 2004; Chan, 2003; Kwon & Suh, 2004). Importantly, the trust relationship is a calculative, risk-based arrangement benefitting the rational self interest of the parties involved (Kwon & Suh, 2004; Suh & Kwon, 2006). In particular, Kwon & Suh (2004) state that trust is economically beneficial in that it decreases transaction costs incurred from verification of the supplier's credibility and reliability.

A trust relationship can only be sustained through commitment from all of the individual actors (Spekman et al., 1998; Kwon & Suh, 2004). However, several factors can aid in building and sustaining trust. This focus on sustaining relationships is consistent with the conclusion that relationships between members of the supply chain network are critical to enable supply chain agility (Christopher, 2000; Lin et al., 2006; Baramichai et al. 2007). Akkermans et al. (2004) present a conceptual causal mapping of supply chain trust, in which a history of successful collaboration, familiarity between partners, and information sharing create a positive feedback loop.

These results are generally consistent with discussions of trust from the psychological literature. For instance, Colquitt et al. (2007) define trust in terms of an intention to *accept vulnerability* by the trustor to the trustee based on *positive expectations* about the trustee's actions. This conception of trust echoes the notions of collaborative risk sharing and the rational cost-benefit calculus mentioned above. Trust in the trustor-trustee framework is a function of the *trustworthiness* of the trustee (i.e., their ability, integrity) and the *trust propensity* of the trustor (i.e., a disposition to be willing to rely upon others) (Glaeser et al., 2000; Colquitt et al., 2007). Figure 1, based on Conquitt et al. (2007), depicts this relationship. In it, trust is a function of trustworthiness and trust propensity, and in turn, trust modulates some type of behavior (either positively or negatively).

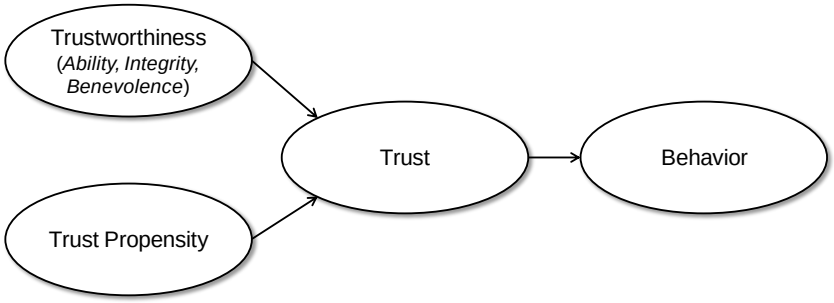

Figure 1: A conceptual model of trust (adapted from Colquitt et al., 2007)

According to Handfield & Bechtel (2002), the primary "behavior" of interest in the supply chain context is the reduction of cycle times within the supply chain, which they term "responsiveness". In their formulation, organizational arrangements that foster trust are ultimately beneficial because they increase the speed of transactions within the supply chain. Not only is time to fulfill orders critical, but low-trust relationships result in opportunity costs – time spent verifying the trustworthiness of a partner could be better spent optimizing other features of the organization's operations (Kwon & Suh, 2004). This trust-

speed relationship is reinforced in the popular literature as well – Covey (2006) devotes an entire book to the subject. In it, the following notional equation is presented:

$$(S*E)T = R \quad (1)$$

where S is strategy, E is execution, T is trust, and R is results (Covey, 2006). In this simple model, trust is shown to be a multiplier, where high trust can greatly facilitate results (e.g., cost and speed at which operations are conducted), but low trust can severely dampen them.

3. A C2 Perspective on Resilience, Agility, and Trust

The international C2 community has adopted an encompassing view of the term Agility defining it in terms of task or mission success (e.g. acceptable performance at an acceptable costs with an acceptable risk) rather than one or more aspects of success (e.g. responsiveness and/or resilience). In this community, agility is defined as "*the ability to successfully effect, cope with, and/or exploit changes in circumstances*" (Alberts, 2011). In this theoretic construct, resilience is one of six interrelated components or enablers of agility, along with responsiveness, versatility (i.e., robustness), innovativeness, and adaptability. In the supply chain literature, resilience (to large disruptions) was thought of as a special case of agility (to disruptions of small or large size, or external pressures more generally). Similarly, in the C2 context, resilience is but one factor affecting the overall agility of a system (Alberts, 2011). Similarly to others (Sheffi, 2005; Conboy & Fitzgerald, 2004), Alberts (2011) also notes that simply adapting to changes is insufficient for agility, and instead proposes that "embracing" changes can not only return a system to its original position, but to a new, better state.

Of particular importance to agility is responsiveness, which in the C2 literature is "*related to the time it takes to recognize and respond to a change or anticipated change in circumstances*" (Alberts, 2011). In particular, responsiveness is defined in terms of some system performance or critical functionality. Figure 2 depicts a generic picture of system functionality plotted against time, in which the functionality drops in response to an adverse event, and then gradually recovers back to the baseline level. This model is also depicted in terms of supply chain resilience by Sheffi & Rice (2005) and Falasca et al., (2008). Along the x-axis are listed the steps of the event management cycle defined by the National Academy of Sciences (2012). Linkov et al. (2013, 2014b) show that it is both the magnitude of the "dip" in critical functionality and the time it takes to absorb and recover functionality that define a system's resilience profile.

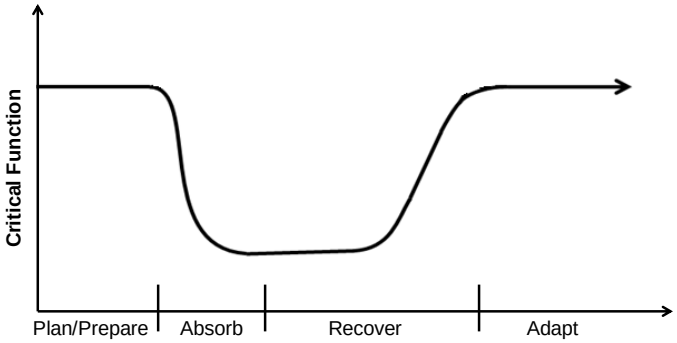

Figure 2: A generic resilience profile

Stated in terms of C2, resilience only makes sense with respect to time – when resilience (and the other components of agility) is coupled with responsiveness (Collier & Linkov, 2014) and in the context of a determination of a range of "acceptable" performance values (y axis). This enables one to consider some

degradations as tolerable and does not require a return to a pre-existing levels of performance but rather to a level deemed minimally acceptable.

Given the trust-speed relationship, then it becomes evident that higher levels of trust between partners in a system can serve to boost responsiveness, and by association, resilience and agility (Figure 3a). All else being equal, a more responsive system will be able to more quickly detect a change, decide on the corrective course of action, execute the action, and reach the desired effect (in Figure 3b, shifting the upward part of the curve to the left).This leads us to conclude that in a supply chain, this increase in speed of absorption and recovery can be facilitated by increased trust. In other words: *Trust enables Responsiveness, and Responsiveness enables Agility.*

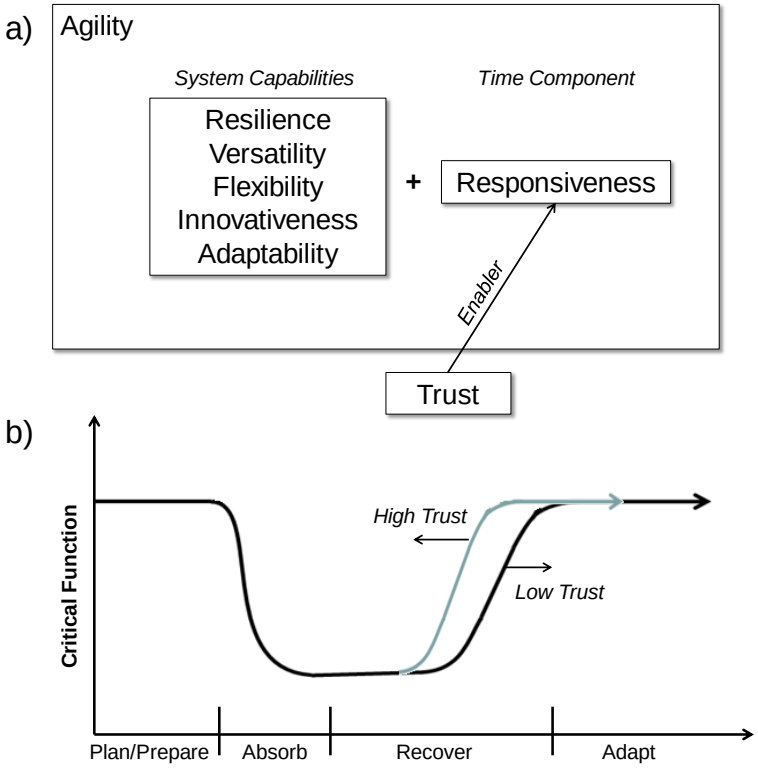

Figure 3: A) The relationship between trust and agility; B) The effect of trust on resilience, where as trust increases, the time to absorb and recover decreases

Of particular importance from a C2 standpoint is determining the critical function of a supply chain (the y-axis in Figure 3b). In terms of trust, this is the "behavior" (from Figure 1) that trust enables through responsiveness. This measure of "success" is highly mission-specific and dependent on particular circumstances. In terms of supply chains, key critical functionalities may relate to order fulfillment, response times, and cost management (see e.g., Klapper et al., 1999; Gunasekaran et al., 2004). While the choice of metrics is context-specific, good performance metrics should always be aligned with the strategic goals of the enterprise (Beasley et al. 2010).

Investments in physical and human assets, information sharing, and contract mechanisms are important enablers of trust, and thus speed (Handfield & Bectel, 2002; Kwon & Suh, 2004; Chan, 2003). For instance, physical and human assets, which might include investment in equipment, tools, systems, personnel, or training, may increase speed by reducing setup times, improving demand forecasts, and improving understanding of supply chain requirement and capacity (Handfield & Bechtel, 2002). Information sharing is critical to early detection and decision making regarding changes in circumstances.

Contract mechanisms can also increase speed by reinforcing and incentivizing the partners in the supply chain through clear communication of expectations and conflict resolution procedures (Handfield & Bechtel, 2002).

4. The Present and Future of Trust

4.1. Current Efforts in Supply Chain Trust

There are a number of initiatives addressing supply chain trust. DoDI 5200.44 specifies requirements to procure DoD-specific integrated circuit-related products and services from a trusted supplier accredited by the Defense Microelectronics Activity (DMEA) (DoD, 2012). DMEA and the National Security Agency (NSA) co-fund the Trusted Foundry Program with the goal of facilitating the US Government's unique needs associated with securing trusted, low-volume use electronics through suppliers that meet certain criteria (DMEA, 2002). DMEA defines trusted as "*the confidence in one's ability to secure national security systems by assessing the integrity of the people and processes used to design, generate, manufacture and distribute national security critical components (i.e. microelectronics)*" (DMEA, 2002). Furthermore, DMEA specifies that trusted sources will provide an assured chain of custody for integrated circuits, ensure against supply chain disruptions, prevent the modification and/or tampering of integrated circuits, and protect against reverse engineering (DMEA, 2002).

A research effort originating in DARPA is aimed at developing tools to nondestructively verify the trustworthiness of an electronic component. The DARPA Supply Chain Hardware Integrity for Electronics Defense (SHIELD) program focuses on small (100 x 100 micron) components, called dielets. The program seeks to develop low-cost dielets including encryption and sensor functionalities to affix to microchips which could provide assurance against a host of threats including counterfeit and sub-standard components. These dielets could send challenge-response information back and forth between a centralized server to determine authentication (DARPA, 2014).

There are a number of industry standards addressing counterfeit prevention that incorporate requirements for supply chain management to establish supply chain trust. The Society of Automotive Engineers (SAE) has a suite of standards addressing counterfeit avoidance and detection. Two of the core standards from the suite, SAE Aerospace Standard AS5553, *Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition* and AS6174, *Counterfeit Materiel; Assuring Acquisition of Authentic and Conforming Materiel* specify requirements to use original manufacturers or trusted suppliers with traceability to the original manufacturer whenever possible. When material is not available from trusted sources, then the industry standards require performing a risk assessment and mitigation that includes testing and verification requirements for items and suppliers identified as having high risk for counterfeiting. SAE has additional standards published in the suite specific to the Electrical, Electronic, and Electromechanical (EEE) family of devices that includes AS6496, *Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition - Authorized/Franchised Distribution,* and ARP6178, *Fraudulent/Counterfeit Electronic Parts; Tool for Risk Assessment of Distributors.* AS6496 is intended to enhance the effectiveness of existing practices and procedures within the Authorized Distribution Channel to mitigate the risk of counterfeit electronic parts entering the supply chain. ARP6178 is a recommended process document to evaluate distributors that procure electronic components without traceability to the original manufacturer. In addition, SAE has a draft work-in-process, AS6171, *Test Methods Standard; General Requirements, Suspect/Counterfeit Electrical, Electronic, and Electromechanical Parts* that is intended to provide guidance and requirements for the Test Laboratory to detect suspect counterfeit and counterfeit EEE parts in the supply chain. The SAE suite of standards is intended to be applied to the appropriate sectors of the supply chain which the specific standard applies in an effort to mitigate counterfeiting across the diverse supply chain.

Another accreditation standard, The Open Trusted Technology Provider Standard (O-TTPS), published by The Open Group, is focused on establishing a set of guidelines to address trust for commercial off-the-shelf (COTS) hardware and software technologies. The best practices and guidelines are designed to address the entire product lifecycle, from design through disposal. Version 1.0 of the standard has been released and is concerned with maliciously tainted and counterfeit products, as well as overall supply chain security. Similar to the DoD Trusted Foundry Program, suppliers have the opportunity to be accredited as "Open Trusted Technology Providers" through adherence to these requirements (The Open Group, 2014).

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) have created a multi-part standard offering guidance on risk assessment of goods and services acquired from outside suppliers (ISO/IEC, 2015). The scope of products and services covered by the ISO/IEC 27036 standards include IT outsourcing and cloud computing services, professional services, telecommunication and Internet services, custom products and services built to the acquirer's specification, and utilities (e.g. electric power and water). The standards provide guidance on assessing security risks and implementing controls when acquiring information technology products and services in business-to-business relationships (ISO/IEC, 2015).

U.S. Defense Logistics Agency (DLA) has established qualification programs in an effort to establish trust in their supply chain. Two key programs are the Qualified Suppliers List of Distributors (QSLD) and the Qualified Testing Suppliers List (QTSL). The QSLD program establishes and maintains a list of pre-qualified sources of EEE components and establishes a set of performance criteria for distributors to meet before qualifying, including accepted commercial practices, quality assurance procedures, and traceability requirements. QSLD applies to semiconductors and electronic microcircuits (DLA, 2015a). The QTSL is a similar program which establishes and maintains a list of pre-qualified testing suppliers. These suppliers must also comply with a set of performance criteria regarding counterfeit mitigation and quality assurance practices (DLA, 2015b).The terms of qualification for QSLD and QTSL are valid for three years and the accepted suppliers are subject to audit by DLA.

4.2. Future Work and Research Needs

Future work should include research and applications for closing the gaps in the User assessment toolset necessary to sustain trust and agility in a resilient supply chain. Applying C2 principles to agility and trust for a resilient supply chain is possible through a systems engineering baseline that incorporates a review and assesses the critical system not only for resiliency, but for robustness and reliability as well (Larson et al., 2005). Research leading to the modeling and consolidation of these three critical supply chain elements is essential to address gaps in the means for affordable and practical C2 sustainment of a trusted supply chain. The means to bound and direct research begins with standard work for defining the systems engineering baseline of a target cyber physical system (CPS) relying on a trusted supply chain (Zhu & Basar, 2011) that designs-in quality, safety, and security. A systems engineering baseline includes design for reliability with quality metrics that ensures the system will work the way the User expects it to work. Design for robustness ensures that the system operates safely under a given range of stressful or adverse conditions anticipated in the operational requirements defined by the User at the onset of the systems design. Through design for resiliency, a system subjected to an unexpected perturbation, such as security attacks, restores itself to a reliable and robust condition.

Systems design for resiliency and security optimizes command and control sustainment. The systems design architectural requirements supporting the operational requirements of the CPS define the performance expected of the components (e.g. microelectronics) selected to achieve robustness and reliability that must now include cyber physical systems security (CPSS) (DiMase et al., 2015). Research in modeling resiliency and CPSS while maintaining systems robustness and reliability will fill a

gap where there is no means to achieve optimum C2 for hardware assurance. The existing Federal Logistics Information System does not currently have criticality code definitions for electronic parts that include resiliency and security through hardware assurance (DoD, 2010). Modeling research should extend to the electronic parts wherein the part can be profiled for its ability to create a meaningful and significant disturbance to the reliability and robustness of the CPS functional design. In the selection of robust electronic parts, the systems design engineer must consider the environmental and operational extremes of the system. In this manner, the threat of intended mission conditions to the performance of the CPS can be aligned to the performance specification of the electronic part. The research and science supporting the robust electronic device for safety and quality has been established for many years (Tummala et al., 1997). Systems engineering design for robustness to maintain reliability can thereby be modeled to the CPS and the best design path for reliability can be pursued. A similar approach and toolset to modeling and characterizing electronic parts for resiliency and security is needed.

In attempting an analogous approach for resiliency, designing CPS electronic parts for the ability to work through unexpected perturbations through malicious, embedded software and firmware lacks the benefit of years of scientific research and application experience. At the electronic part level, the limited knowledge of resiliency and security can be attributed directly to a lack of trust and agility in the supply chain. The U.S. government recently passed DFARS 79 Federal Regulation 26001, 'Detection and Avoidance of Counterfeit Electronic Parts (Effective: May 6th, 2014)' to drive for accountability in ensuring trust in U.S.-procured CPS. Industry is now challenged to establish methods for showing compliance to the goals of the DFARS guidance to secure supply chain agility and trust.

Advancements in test techniques with standard work for hardware, firmware, and software validation are needed. Current standard test methods for microelectronics are limited in addressing attack vectors associated with tampered counterfeit part types. This classification of counterfeit types includes electronic parts with embedded malware and hardware Trojans that introduce a number of vulnerabilities that can lead to loss of functionality, loss of intellectual property, or dangerous exploitations of a part in a system during its lifecycle. The SAE G-19A Test Laboratory Standards Development Committee has formed a subgroup specific to tampered microelectronics whose scope and charter includes development of a taxonomy of vulnerabilities, categorization of attack vectors, and standardized test methods to detect vulnerabilities. This subgroup has drafted their first test method for the detection of altered electronics using unintended emissions. Additional technologies and test methods are under review by the subgroup. Additional support for the subgroup is needed to establish and expedite methods for detecting the presence of malicious features in electronic parts.

Vulnerabilities of systems due to the complexities and integration of hardware, firmware, and software cannot be addressed through software and information assurance alone. A solution that includes a holistic approach to cyber physical systems security that includes metrics and a common understanding of system evaluation is needed. SAE currently has announced a call to action for a systems engineering committee to advance the knowledge of how vulnerabilities are introduced in cyber physical systems, identifying best practices for addressing different areas of concern, establishing and standardizing methods for identifying vulnerabilities in cyber physical systems, and developing cost effective design and evaluation methods for cyber physical systems security that includes assessing effectiveness of solutions. Support is needed to expedite the development of the cyber physical systems security effort from the SAE systems engineering committee.

Some notable resiliency modeling efforts have been made to initiate the topographical analysis of a CPS to identify nodes of vulnerability to the host system instantiated by a counterfeit or tampered electronic part (McDonald, et al., 2010). However, research is needed to design and build real-world models and ranges supporting scientific experimentation to validate the model. Currently, there is limited published research on the categorization of the threats attributable to trust in electronic parts (Beaumont et al.,

2011). However, many of the detection and prevention methods are in early stages of development and require research for demonstrating adaptability to evolving, dynamic malware and embedded hardware threats.

Using trusted suppliers and foundries is an alternative for ensuring supply chain trust. Trusted suppliers are challenged to stay ahead of the evolving threat environment for hardware assurance while remaining an agile and resilient supplier for their customers. A combination of research for detection tools for embedded malware, invasive design (3-D) and advanced manufacturing and packaging technologies can be applied to prevent introduction of malware at points in the life cycle beyond the CPS hardware OEMs (Chakraborty et al., 2009). Finally, additional research is needed to build fidelity models that will allow the connection between the embedded hardware threat and the nodal topographical map that provides the basis for optimum C2 design for resiliency (Ford et al., 2012) and security while maintaining quality and safety. Complementary research is needed that defines a risk-based approach to cyber resiliency that assesses and manages risk across dynamic cyber physical systems (DiMase et al., 2015). Additional research and technology solutions are needed that advance our knowledge on how to detect counterfeiting and track and trace authentic devices and parts that have been validated for counterfeit avoidance and detection to cost effectively address the problem.

As a practical matter, several authors note that managing for resilience may be in conflict with other business goals (e.g., cost minimization or operational efficiency) (Falasca et al., 2008; Carvalho & Cruz-Machado, 2011). Pettit et al. (2008) define a "resilience gap", where excessive capabilities (in this case, resilience controls or attributes) unnecessarily diminish profits, or inadequate capabilities leave the supply chain unacceptably vulnerable. When capabilities are balanced with vulnerabilities, resilience is optimized (Pettit et al., 2008; Fiksel et al. 2015). This is consistent with the C2 concept of "requisite agility" which, based on the law of "requisite variety" from the field of Cybernetics (Ashby, 1956), states that a system only needs to be as agile as the set of circumstances that it faces (Alberts, 2011). Moreover, there may be tradeoffs associated with measures taken to increase trust (e.g., increased costs for verification and tracking, reduced flexibility in supplier selection). These tradeoffs allude to the need for further research and development of multiple-criteria decision support tools to aid in evaluating the design tradespace (Linkov et al., 2012). However, improved trust metrics will need to be developed before an evidence-based model can be used to explore decision tradeoffs and trust dynamics.

Ultimately, future work through these suggested research areas should lead to tools that enable profile modeling for parts in the supply chain by combining research artifacts derived from the CPS topographical mapping tools and device detection and prevention methods. The resultant toolset should allow Users agility to bound part assessment of embedded malware and hardware Trojans with the tampered part influence on the CPS as nodes of vulnerability. Electronic part profiling will enhance agility while achieving trust for the part through its application in the supply chain life cycle. Finally, support to emerging system-on-chip architectures is needed for designed-in cyber resiliency.

Future work to render models for supply chain resiliency will enable command and control through standard work toolsets for systems security engineering design supported by research and application demonstration. A foundation for building evidence-based cyber resiliency modeling exists in early work in threat topography and data flow analysis. Actuarial Science provides a path to metrics for the single point and cumulative risk of loss (Kaas et al., 2009). The application of these metrics depends on empirical observations of known threats and the severity of risk posed by these threats based on the exposure provided by the systems design. The empirical data on threats to cyber resiliency is collected and accumulated through initiatives like the U.S. Cyber Security Framework where collaboration in reporting attacks and the associated etiology will allow for actuarial analysis of the CPS. The results will permit future work in the development of R-based modeling tools that can be applied globally through collaborative sites like Comprehensive R Archive Network (CRAN, 2015).

5. Acknowledgements: The authors would like to thank Dave Alberts for his comments on this manuscript. Permission was granted by the USACE Chief of Engineers to publish this material. The views and opinions expressed in this paper are those of the individual authors and not those of the US Army, or other sponsor organizations.

6. References

1. Akkermans H, Bogerd P, van Doremalen J (2004) Travail, transparency and trust: A case study of computer-supported collaborative supply chain planning in high-tech electronics. *European Journal of Operational Research* 153: 445–456
2. Alberts DS (2010) The Agility Imperative: Précis. DOD Command and Control Research Program: Washington, DC. http://www.dodccrp.org/files/Alberts_Agility_Imperative_Precis.pdf
3. Alberts DS (2011) *The Agility Advantage: A Survival Guide for Complex Enterprises and Endeavors*. DOD Command and Control Research Program: Washington, DC.
4. Ashby WR (1956) *An Introduction to Cybernetics (Vol. 2)*. Chapman & Hall: London.
5. Baramichai M, Zimmers Jr. EW, Marangos CA (2007) Agile supply chain transformation matrix: an integrated tool for creating an agile enterprise. *Supply Chain Management* 12(5):334-348.
6. Beasley MS, Branson BC, Hancock BV (2010) Developing key risk indicators to strengthen enterprise risk management. Committee of Sponsoring Organizations of the Treadway Commission (COSO).
7. Beaumont M, Hopkins B, Newby T (2011) Hardware Trojans – Prevention, Detection, Countermeasures (A Literature Review). Australian Government Department of Defence, Defense Science and Technology Organisation; Publication No. DSTO –TN -1012.
8. Carvalho H, Cruz-Machado V (2011) Integrating Lean, Agile, Resilience and Green Paradigms in Supply Chain Management (LARG_SCM). In: Li P (Ed.), *Supply Chain Management.* InTech: Rijeka, Croatia, pp. 27-48.
9. Chakraborty RS, Narasimhan S, Bhunia S (2009) Hardware Trojan: Threats and Emerging Solutions. *IEEE International High Level Design Validation and Test Workshop (HLDVT)*, San Francisco, CA, November 4-6, 2009. pp. 166-171.
10. Chan FTS (2003) Performance measurement in a supply chain. *Int J Adv Manuf Technol* 21:534–548.
11. Christopher M (2000) The agile supply chain: competing in volatile markets. *Industrial Marketing Management*, 29(1): 37-44.
12. Christopher M, Towill D (2001) An integrated model for the design of agile supply chains. *International Journal of Physical Distribution and Logistics Management*, 31(4): 235-24.
13. Christopher M, Peck H (2004) Building the Resilient Supply Chain. *International Journal of Logistics Management*, 15(2): 1-13.
14. Collier ZA, Linkov I (2014) Decision making for resilience within the context of network centric operations. *Paper presented at 19th International Command and Control Research and Technology Symposium (ICCRTS)*, Alexandria, VA, 16-19 June, 2014.
15. Collier ZA, Linkov I, DiMase D, Walters S, Tehranipoor M, Lambert JH (2014a) Cybersecurity standards: managing risk and creating resilience. *Computer* 47(9):70-76.
16. Collier ZA, Walters S, DiMase D, Keisler JM, Linkov I (2014b) A semi-quantitative risk assessment standard for counterfeit electronics detection. *SAE International Journal of Aerospace* 7(1):171-181.
17. Collin J, Lorenzin D (2006) Plan for supply chain agility at Nokia: lessons from the mobile infrastructure industry. *International Journal of Physical Distribution & Logistics Management*, 36(6): 418-430.
18. Colquit JA, Scott BA, LePine JA (2007) Trust, Trustworthiness, and Trust Propensity: A Meta-Analytic Test of Their Unique Relationships with Risk Taking and Job Performance. *Journal of Applied Psychology* 92(4):909-927.

19. Conboy K, Fitzgerald B (2004) Toward a conceptual framework of agile methods: a study of agility in different disciplines. *WISER'04*, November 5, 2004, Newport Beach, California, USA.
20. Covey SMR (2006) *The Speed of Trust: The One Thing that Changes Everything*. Simon and Schuster: New York.
21. CRAN (2015) The Comprehensive R Archive Network. http://cran.r-project.org/
22. DARPA (2014) Tiny, Cheap, Foolproof: Seeking New Component to Counter Counterfeit Electronics. http://www.darpa.mil/newsevents/releases/2014/02/24.aspx
23. DiMase D, Collier ZA, Heffner K, Linkov I (2015, submitted) Systems engineering framework for cyber physical security and resilience. *Environment Systems & Decisions* DOI: 10.1007/s10669-015-9540-y.
24. DLA (2015a) QSLD Program (Qualified Suppliers List of Distributors). http://www.landandmaritime.dla.mil/offices/sourcing_and_qualification/offices.aspx?Section=QSL
25. DLA (2015b) QTSL Program (Qualified Testing Suppliers List). http://www.landandmaritime.dla.mil/offices/sourcing_and_qualification/offices.aspx?Section=QTS
26. DMEA (2002) Trusted Foundry Program. http://www.dmea.osd.mil/trustedic.html
27. DoD (2002) Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN). Department of Defense Instruction Number 5200.44. http://www.dtic.mil/whs/directives/corres/pdf/520044p.pdf
28. DoD (2010) Federal Logistics Information System. DoD 4100.39-M, Volume 10. http://www.dtic.mil/whs/directives/corres/pdf/410039m/410039m_vol10.pdf
29. Executive Order 13636 (2013)—Improving Critical Infrastructure Cybersecurity. http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf
30. Falasca M, Zobel CW, Cook D (2008) A Decision Support Framework to Assess Supply Chain Resilience. In: Fiedrich F, Van de Walle B (Eds.), *Proceedings of the 5th International ISCRAM Conference*, Washington, DC, USA, May 2008, pp. 596-605.
31. Fiksel J, Polyviou M, Croxton KL, Pettit TJ (2015) From Risk to Resilience: Learning to Deal with Disruption. *MIT Sloan Management Review* 56(2):1-8.
32. Ford R, Carvalho M, Mayron L, Bishop M (2012) Towards Metrics for Cyber Security. *21st EICAR Annual Conference Proceedings.* pp. 151–159.
33. Glaeser EL, Laibson DI, Scheinkman JA, Soutter CL (2000) Measuring Trust. *The Quarterly Journal of Economics*, 811-846.
34. Gunasekaran A, Patel C, McGaughey RE (2004) A framework for supply chain performance measurement. *International Journal of Production Economics* 87: 333-347.
35. Handfield RB, Bechtel C (2002) The role of trust and relationship structure in improving supply chain responsiveness. *Industrial Marketing Management* 31: 367– 382.
36. ISO/IEC (2015) ISO/IEC 27036:2013+ - IT Security – Security Techniques – Information Security for Supplier Relationships. http://www.iso27001security.com/html/27036.html
37. Kaas R, Goovaerts M, Dhaene J, Denuit M (2009) *Modern Actuarial Risk Theory: Using R.* Springer: Heidelberg.
38. Kelic A, Collier ZA, Brown C, Beyeler WE, Outkin AV, Vargas VN, Ehlen MA, Judson C, Zaidi A, Leung B, Linkov I (2013) Decision Framework for Evaluating the Macroeconomic Risks and Policy Impacts of Cyber Attacks. *Environment Systems & Decisions* 33(4): 544-560.
39. Klapper LS, Hamblin N, Hutchinson L, Novak L, Vivar J (1999) Supply Chain Management: A Recommended Performance Measurement Scorecard. LG803R1. Logistics Management Institute.
40. Kleindorfer PR, Saad GH (2005) Managing Disruption Risks in Supply Chains. *Production and Operations Management* 14(1): 53-68.
41. Kwon I-W G, Suh T (2004) Factors Affecting the Level of Trust and Commitment in Supply Chain Relationships. *The Journal of Supply Chain Management* 40(1):4-14.
42. Larson R, Marks D, Dahlel M, Ilic M (2005) The 3 R's of Critical Energy Networks: Reliability, Robustness and Resiliency. White paper submitted to the MIT Energy Research Council;

Massachusetts Institute of Technology - Center for Engineering Systems Fundamentals; October 30, 2005; http://cesf.mit.edu/abstracts/103005.html.
43. Lin C-T, Chiu H, Chu P-Y (2006) Agility index in the supply chain. *International Journal of Production Economics* 100:285-299.
44. Linkov I, Anklam E, Collier ZA, DiMase D, Renn O (2014a) Risk-based standards: integrating top-down and bottom-up approaches. *Environment Systems & Decisions* 34(1):134-137.
45. Linkov I, Bridges T, Creutzig F, Decker J, et al. (2014b) Changing the Resilience Paradigm. *Nature Climate Change*, 4, 407– 409.
46. Linkov I, Eisenberg DA, Bates ME, Chang D, Convertino M, Allen JH, Flynn SE, Seager TP (2013) Measurable resilience for actionable policy. *Environmental Science & Technology* 47(18):10108–10110.
47. Linkov I, Trump BD, Pabon N, Collier ZA, Keisler JM, Scriven J (2012) A decision analytic approach for Department of Defense acquisition risk management. *Military Operations Research* 17(2):53-70.
48. Mason SJ, Cole MH, Ulrey BT, Yan L (2002) Improving electronics manufacturing supply chain agility through outsourcing. *International Journal of Physical Distribution & Logistics Management* 32(7): 610-620.
49. McDonald MJ, Mulder J, Richardson BT, Cassidy RH, et al. (2010) Modeling and Simulation for Cyber-Physical System Security Research, Development and Applications. Sandia National Laboratories: Albuquerque, New Mexico, Report SAND 2010-0568.
50. National Academy of Sciences (2012) Disaster Resilience: a National Imperative. National Academic Press: Washington, DC. http://www.nap.edu/catalog.php?record_id=13457
51. Norrman A, Lindroth R (2004). Categorization of supply chain risk and risk management. In: Brindley C (Ed.), *Supply Chain Risk*. Ashgate Publishing Limited.
52. Pecht M, Tiku S (2006) Bogus: electronic manufacturing and consumers confront a rising tide of counterfeit electronics. *IEEE Spectrum* 43(5): 37-46.
53. Pettit T, Fiskel J, Croxton K (2008) Can you measure your supply chain resilience? *Supply Chain and Logistics Journal*, 10(1): 21-22.
54. Presidential Policy Directive 21 (2013) Critical Infrastructure Security and Resilience. http://www.whitehouse.gov/the-pressoffice/2013/02/12/presidential-policy-directive-critical-infrastructuresecurity-and-resil.
55. Rinaldi S, Peerenboom J, Kelly T (2001) Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine* 21(6):11–25.
56. Rojo FJR, Roy R, Shehab E (2010) Obsolescence management for long-life contracts: state of the art and future trends. *Int J Adv Manuf Technol* 49:1235–1250.
57. Sharp JM, Irani Z, Desai S (1999) Working towards agile manufacturing in the UK industry. *International Journal of Production Economics* 62, 155–169.
58. Sheffi Y (2005) Building a resilient supply chain. *Harvard Business Review* 1(8): 1-4.
59. Sheffi Y, Rice JB Jr. (2005) A supply chain view of the resilient enterprise. *MIT Sloan Management Review*, 47(1):41-48.
60. Sood B, Das D, Pecht M (2011) Screening for counterfeit electronic parts. *Journal of Materials Science: Materials in Electronics* 22(10): 1511-1522.
61. Spekman RE, Kamauff JW Jr., Myhr N (1998) An empirical investigation into supply chain management: A perspective on partnerships. *International Journal of Physical Distribution & Logistics Management*, 28(8): 630-650.
62. Suh T, Kwon I-W G (2006) Matter over mind: When specific asset investment affects calculative trust in supply chain partnership. *Industrial Marketing Management* 35: 191 – 201.
63. Tang CS (2006) Perspectives in supply chain risk management. *International Journal of Production Economics*, 103(2), 451-488.
64. The Open Group (2104) The Open Trusted Technology Provider™ Standard (O-TTPS) Accreditation Program. http://www.opengroup.org/accreditation/o-ttps

65. Tummala RR, Rymaszewski EJ, Klopfenstein AG (1997) *Microelectronics Packaging Handbook, Part II*. Springer: Dordrecht.
66. U.S. Department of Commerce (2012) Defense Industrial Base Assessment: Counterfeit Electronics. http://www.bis.doc.gov/index.php/forms-documents/doc_view/37-defense-industrial-base-assessment-of-counterfeit-electronics-2010
67. U.S. Senate Armed Services Committee (2012) Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain. Senate Report 112-167.
68. U.S. White House (2009) Cyberspace policy review: assuring a trusted and resilient information and communications infrastructure. http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.
69. Vanany I, Zailani S, Pujawan N (2009) Supply Chain Risk Management: Literature Review and Future Research. *International Journal of Information Systems and Supply Chain Management* 2(1):16-33.
70. Villasenor J (2013) Compromised by Design? Securing the Defense Electronics Supply Chain. Brookings Institution.
71. Zhu Q, Basar T (2011) Robust and Resilient Control Design for Cyber-Physical Systems with an Application to Power Systems. *50th IEEE Conference on Decision and Control and European Control Conference (CDC-ECC)*, Orlando, FL, USA, December 12-15, 2011; pp. 4066-4071.