In press, accepted to *Benchmarking: An International Journal*

Decision Model with Quantification of Buyer-Supplier Trust in Advanced Technology Enterprises

Zachary A. Collier[1], Ujjwal Guin[2], Joseph Sarkis[3], James H. Lambert[4]

[1] Department of Management, Radford University, Radford, VA
[2] Department of Electrical and Computer Engineering, Auburn University, Auburn, AL
[3] Robert A. Foisie School of Business, Worcester Polytechnic Institute, Worcester, MA, and Hanken School of Economics, Humlog Institute, Helsinki, Finland.
[4] Department of Engineering Systems and Environment, University of Virginia, Charlottesville, VA

Abstract: *Purpose:* In the buyer-supplier relationship of a high-technology enterprise, the concepts of trust and risk are closely intertwined. Entering into a buyer-supplier relationship inherently involves a degree of risk, since there is always an opportunity for one of the parties to act opportunistically. Purchasing and supply managers play an important role in reducing the firm's risk profile, and must make decisions about whether or not to enter into, or remain in, a relationship with a supplier based on a subjective assessment of trust and risk. *Methodology:* In this paper, we seek to explore how trust in the buyer-supplier relationship can be quantitatively modeled in the presence of risk. We develop a model of trust between a buyer and supplier as a risk-based decision, in which a buyer decides to place trust in a supplier, who may either act cooperatively or opportunistically. We use a case study of intellectual property (IP) piracy in the electronics industry to illustrate the conceptual discussion and model development. *Findings:* We produce a generalizable model that can be used to aid in decision making and risk analysis for potential supply-chain partnerships, and is both a theoretical and practical innovation. However, the model can benefit a variety of high-technology enterprises. *Originality:* While the topic of trust is widely discussed, few studies have attempted to derive a quantitative model to support trust-based decision making. This paper advances the field of supply chain management by developing a model which relates risk and trust in the buyer-supplier relationship.

Keywords: Supplier Management, Supplier Risk, Value of Information, Intellectual Property, Zero Trust, Overproduction

1. Introduction

Supplier management is a strategically important business function, described by Large (2005) as "the external part of the purchasing management process that plans, implements and controls the business relationships with suppliers," and has a direct impact on a firm's operations and profitability (Chen *et al*., 2016; Kraljic, 1983). While the buyer-supplier relationship can represent an *asset* to a firm, it can also be a source of *risk.* Supplier failures may result in the purchasing firm being unable to fill orders, or in other negative impacts to product quality, production, transportation, inventory, payments, IT systems, and project success, among others (Collier & Lambert, 2021; Grudinschi *et al*., 2014; Costantino & Pellegrino, 2010; Hallikas *et al*., 2005; Pavlou, 2003). A further source of risk in the buyer-supplier relationship is the opportunistic, unethical behavior of one of the parties (Gullett *et al*., 2009; Hill *et al*., 2009). This *relational risk* arises from a misalignment of partner interests, where one of the partners seeks to accrue maximum benefits for themselves at the expense of their partner (Gelderman *et al*., 2020; Inkpen & Currall, 2004; Das & Teng, 2003). Since in buyer-seller relationships there is always a chance that one party may engage in opportunistic behavior (Gelderman *et al*., 2020; Chen *et al*., 2016), the tasks of supplier selection and supplier relationship management involve risk-based decision making about whether the buyer can *trust* the supplier (Hallikas *et al*., 2005). Trust and risk are generally assumed to be inversely related – as trust in one's supply chain partners increases, risk decreases (Fawcett *et al*., 2012).

Recently, the concept of *Zero Trust* has emerged within the supply chain field which inverts this assumption about the relationship between risk and trust, asserting that less trust is associated with less risk (Collier & Sarkis, 2021). Zero Trust is a philosophy and set of guiding principles originating in the information technology field exploring the idea of how one might manage security if it was assumed that attackers were already present on the network (Kindervag, 2010). Rather than using firewalls and other means to keep attackers outside of the network's perimeter, Zero Trust established a set of principles and tenets for making per-request, risk-based authentication and authorization decisions (NIST, 2020). Zero Trust requires a "trust algorithm" to process multiple data inputs on the access request, the subject making the request, the asset being accessed, resource policy requirements, and threat intelligence (NIST, 2020). Before granting access to a network resource, a quantifiable assurance case must be made regarding the trustworthiness of the agent requesting access, taking a "guilty until proven innocent" security posture.

While this set of ideas was originally narrowly confined to the information technology field, efforts to extend the principles to other domains have begun to gain traction. For example, the U.S. Department of Defense has expressed interest in leveraging the foundational principles of Zero Trust throughout the defense supply chain for procurement of microelectronics (Lopez, 2020). This involves assuming that no device or source of supply is secure prior to being validated, as well as obtaining quantifiable assurance, based on Zero Trust principles, that all microelectronics are safe to deploy (Leopold, 2020). However, this requires translating the principles of Zero Trust from its original domain, i.e., information technology systems, to a new domain, i.e., the supply chain, where there may not be a clear one-to-one mapping of concepts (Collier & Sarkis, 2021).

Supplier trust and risk are interrelated concepts; however, their relationship is often difficult to operationalize and quantify. In particular, there exists a research gap, as well as a practical need, for a quantitative model which can support risk-based trust decisions for supplier selection, especially in low-trust, high-risk environments. The foundations, gaps, and opportunities for the present paper are as follows:

1. Specifically, in this paper we explore how trust in the buyer-supplier relationship can be modeled as a risky decision problem. This paper seeks to cast a new perspective on supplier trust as a risk-based decision.
2. This paper contributes to the supply chain management literature by developing a generalizable model that relates supplier trust and risk, which can be used to aid in decision making about

potential risky supply chain partnerships. The model is not industry-specific, and therefore represents a valuable perspective for supplier management theory and practice.

2. Background

2.1. Trust in the Buyer-Supplier Relationship

In a widely-cited definition provided by Mayer *et al*. (1995), trust is "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party." Trust is framed as a dyadic relationship between a trustor and a trustee, relative to a domain of action (Nickel & Vaesen, 2102; Holma, 2012). It is conceptualized as a "subjective state of positive expectations" held by a trustor (Das & Teng, 2001) that the trustee will act in a way that is in alignment with the best interests of the trustor, instead of acting in a self-serving, opportunistic way (Spekman *et al*., 1996). Moreover, scholars distinguish between trust itself, which is conceived as a willingness to take the risk or make oneself vulnerable to the trustee, and the subsequent risk-taking behavior based on that willingness (Nickel & Vaesen, 2012; Das & Teng, 2004; Mayer *et al*., 1995). Huang and Nicol (2009) summarize trust as a psychological state containing the following elements:

1. An *expectancy* that the trustee will perform specific actions,
2. A *belief* that the trustee will perform the actions based on an assessment of the trustee's competence and goodwill,
3. A *willingness to be vulnerable* in the belief that the trustee will perform the expected actions.

In the theoretical literature on trust, a trustor (in our case, a buyer) is characterized by a trust propensity, while the trustee (in our case, a supplier) is characterized by trustworthiness. The trust propensity is a stable, dispositional attitude of the trustor related to the likelihood of trusting others. The trustworthiness of a trustee is judged by the trustor along a number of perceived attributes (Mayer *et al*., 1995). While various authors have proposed a number of variables affecting trustworthiness (e.g., Hurley, 2006), a common framework is to use the three variables of ability, benevolence, and integrity. Ability refers to a trustee's competence in performing a specific task, while benevolence refers to the trustee's inclination to do what is in the best interest of the trustor, and integrity is the trustee's adherence to moral norms (Colquitt *et al*., 2007; Mayer *et al*., 1995). Sometimes the latter two considerations are combined into one (e.g., Das & Teng, 2001). For example, in a buyer-seller relationship, the buyer must believe that the seller has both the ability and motivation (where motivation is comprised of benevolence and integrity) to provide the items being purchased (Jarvenpaa *et al*., 2000).

In supplier management, trust is an important tool to reduce risk (Huang & Chiu, 2018; Ghosh & Fedorowicz, 2008). Purchasing and supply managers play an important role in reducing the firm's supplier risk profile by managing supplier relationships (Tate, 2010). Buyers are able to manage their supplier risk profile by evaluating potential suppliers through a process of decision making and risk analysis and negotiation (Hallikas *et al*., 2013).

These trust decisions involve whether or not to enter into, and remain in, specific buyer-supplier relationships. Successful relationships involve, at a minimum, the mutual forbearance of opportunistic behavior between partners (Inkpen & Currall, 2004), while high-trust relationships are characterized by open communication, cooperative problem solving, and mutually-shared goals (Kleemann & Essig, 2013; Fawcett *et al*., 2012). Buyers and suppliers in high-trust relationships often develop a sense of deep interdependence and co-prosperity. Trust in buyer-supplier relationships has been shown to foster long-term cooperation, innovation, and relationship satisfaction (van der Valk *et al*., 2016; Tangpong *et al*., 2008; Sarkar & Mohapatra, 2006; Möllering, 2003). Trust is a relational control based on shared norms and

expectations, as contrasted with contractual controls which involve written policies and procedures (Gelderman *et al*., 2020; Huang & Chiu, 2018; Chen *et al*., 2016).

2.2. Theory Building

Poppo *et al*. (2016) distinguish between different ways to frame trust in the buyer-supplier relationship. One of those frames is "calculative trust". From the calculative perspective, based on theories from Transaction Cost Economics, buyers make a risk-based calculation in which it is warranted to trust a counterparty when the expected gain from trusting outweighs the alternative of not trusting (Wang et al., 2020; Suh & Kwon, 2006; Gambetta, 2000; Williamson, 1993).

Based on this observation that trust can be framed as a quantitative, calculative, risk-based assessment, Gambetta (2000) operationalized trust as an assessment of subjective probability: "Trust (or, symmetrically, distrust) is a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action." Inkpen and Currall (2004) describe that when partnerships are formed, the partners assess a subjective probability that the partner will cooperate. This calculative, risk-based theory of trust implies that trust is warranted when the trustor assesses the expected gain of placing oneself at risk to be greater than the expected gain of not placing oneself at risk (Wang et al., 2020; Fawcett et al., 2017; Suh & Kwon, 2006). Stated differently, placing trust in another implies that the probability that one's counterparty will act in a way that is beneficial is high enough to justify engaging in cooperation (Sears et al., 2020).

Williamson (1993) defined four theoretical assumptions about the calculative theory of trust. First, the parties must be aware of the possible outcomes and the associated probabilities of those outcomes. Second, the parties can take actions to mitigate their losses and enhance their gains. Third, the parties proceed with a transaction only if they project expected net gains from the exchange. Finally, in a situation with multiple trustees with which to transact, the transactions will be completed with the trustee that maximizes the trustor's expected net gain. Therefore, calculative trust assumes that agents are rational decision makers who make forward-looking trust decisions, maximizing their economic self-interest based on a calculation of expected costs and benefits (Wang et al., 2020; Poppo et al., 2016; Suh & Kwon, 2006). The calculative theory of trust focuses on establishing contractual governance mechanisms to control the risks within a transaction through incentivizing certain partner behavior (Bonatto et al., 2021; Williamson, 1993).

When a firm makes the decision to engage in a trusting action, they perform a risk assessment, weighting the expected benefits and costs (Inkpen & Currall, 2004). Such a risk assessment is based on the consequences of possible outcomes and their associated probabilities (such as partner cooperation or betrayal), in accordance with the first theoretical assumption identified by Williamson (1993). This is consistent with the literature on risk, where risk is a measure of the likelihood and severity of an adverse event (Lowrance, 1976), or as a triplet of answers to the questions "what can go wrong?", "how likely is it?", and "what are the consequences?" as defined by Kaplan and Garrick (1981). Trust, defined as a probability assessment, is therefore a critical element in the calculative, risk-based, decision-making process.

One methodological approach for risk-based decision making is the decision tree. Decision trees frame decisions in terms of uncertainties about future states or events, future payoffs, and multiple alternatives from which an agent can select, with the goal of maximizing the agent's expected value or expected utility. For an overview of decision trees, see Ragsdale (2017). Huang and Fox (2005) frame trust decisions (in an information technology context) using decision trees, and Tallman and Shenkar (1997) describe a decision tree for international joint venture formation. Decision trees can be extended to account for risk aversion through the use of utility functions, and to determine the value of information (VOI). Value of information (VOI) is a tool from decision analysis that allows one to quantify the economic value of reducing

uncertainty around a particular decision problem (Howard, 1966, Keisler *et al*., 2013). The concept of VOI is that with additional information, one can reduce the uncertainty surrounding a decision, and therefore make a better decision with a better expected payoff. VOI can be mathematically expressed as the expected value gained from making a decision *with* the information minus the expected value gained from making the decision *without* the information. That difference can be interpreted as the maximum one would be willing to pay to acquire such information. A further distinction is that information can be perfect or imperfect (also referred to as sample information). Perfect information is a theoretical upper bound for the value of information, in which the decision-maker is able to know the actual future state of nature with certainty, whereas sample information reduces the uncertainty only somewhat (Keisler *et al*., 2013).

3. Methodology

Taking a decision-oriented view, we will utilize decision trees as a generic, quantitative framework in which to analyze supplier trust and risk. We adopt the definition of Gambetta (2000) mentioned above, where trust is described as a level of subjective probability that a trustee will perform a particular action.

We first consider the simplest case of trust decision. This can be represented as a simple lottery, in which the trustor can either trust a given trustee or not trust the trustee. If the trustor decides not to trust the trustee in question, they receive a sure-thing payoff of *Z*. However, the trustor can decide to trust (e.g., share valuable IP), and the trustee can either cooperate and deliver a payoff of *X*, or betray the trustor and deliver a loss of *Y*, where $X > Z > Y$. Further, the trustor, in the absence of any additional information, makes a subjective probability assessment about whether the trustee will cooperate, p, as described by Gambetta (2000). Therefore the probability that the trustee will betray the trustor is $1\text{-}p$. This is summarized in Figure 1, where a square node represents a decision, and a circular node represents an uncertainty.

A risk-neutral decision-maker would decide to trust when the expected value of trusting was greater than the expected value of not trusting, i.e., when $pX + (1\text{-}p)Y > Z$, and would be indifferent between the two alternatives when $p = \frac{Z-Y}{X-Y}$. Further, the risk of trusting can be quantified as the expected downside:

$$Risk = (1 - p)Y \tag{1}$$

This definition of risk is directly linked to trust, where trust is the subjective probability estimate that the trustee will cooperate, p, and therefore the risk that they will not cooperate is the complement of p multiplied by the loss, *Y*. This definition of risk is consistent with various definitions put forward, such as the one by Lowrance (1976) mentioned above, where risk is a measure of the likelihood ($1\text{-}p$) and severity (Y) of an adverse event.

Of course, to blindly trust a trustee of unknown trustworthiness is a risky strategy, and ideally in an uncertain situation with potentially large consequences, one would like to take certain precautions that reduce uncertainty. Gathering additional information about the trustee before making the trust decision is one such strategy. Information such as background checks, references, and other due diligence may reduce the trustor's uncertainty about whether the trustee will cooperate or betray, and so it may have positive value. Calculating the VOI is a way to quantify the value of this additional information with respect to the decision.

In the case of perfect information (Figure 2), we see that the chance node comes first, followed by the decision node, representing the case where the uncertainty about the future is revealed *before* the trustor makes the decision. Therefore in the case where we know that the trustee is going to cooperate, the choice would be to trust, while in the case where we know that the trustee is going to betray, we would choose not

to trust. Since the VOI is equal to the expected payoff of the decision with the information minus the expected payoff of the decision without the information, the VOI, in this case, would be:

$$VOI = [pX + (1-p)Z] - \max(pX + (1-p)Y, Z) \quad (2)$$

4. Numerical Example of the Microelectronics Supply Chain

4.1. Background and Motivation

The preceding discussions of trust and risk in the buyer-supplier relationship have been general, and can broadly apply across any specific industry sector. However, to concretize the concepts, we have selected one particular industry where trust plays a prominent role – the microelectronics industry. In the following section, we provide a brief background to some of the issues of risk and trust associated with the supply chains for electronic hardware and embedded systems, which frames the case study which follows.

The complexity of the electronics supply chain has grown significantly due to the expansion of globalization in the 21st century, coupled with the pressures of obsolescence (Collier & Lambert, 2020). Unfortunately, the electronics supply chain has been infiltrated by counterfeit integrated circuits (ICs), which pose serious threats to critical infrastructure due to their inferior quality. Counterfeit electrical, electronic, and electromechanical (EEE) parts have been either relabeled, refurbished, or repackaged to misrepresent their authenticity (Sood *et al*., 2011). Guin *et al*. (2014a) developed a taxonomy of counterfeit types, including recycling, remarking, overproduction, out of specification/defective, cloning, forging of documentation, and tampering. These counterfeits cost the United States semiconductor industry approximately $7.5 billion due to replacement and repair costs (Wood, 2016). Collier *et al*. (2014) defined several tiers of supplier risk of suspect counterfeit parts, based on a number of verifiable factors like whether a supplier was certified to one or more quality management standards, if there were non-compliance notices or other alerts issued for the supplier within given time frames, and the buyer's prior history with the supplier. These qualitative indicators could be used as a proxy for supplier trustworthiness.

Another driver of supplier risk in the microelectronics industry is intellectual property (IP) infringement (Hallikas *et al*., 2005). The theft of IP contained in ICs is an emerging threat, arising due to the changing nature of the global supply chain. The supply chain for electronic parts is extremely complex, with many players, including original equipment manufacturers (OEMs), original component manufacturers (OCMs), contract manufacturers, distributors, and brokers (DiMase *et al*., 2016). The exorbitant costs associated with building and operating highly-specialized fabrication facilities have promoted the practice of contract manufacturing, and the shift from vertical supply chains to horizontal ones (Guin *et al*., 2014a; Lambert *et al*., 2013; Mason *et al*., 2002). Outsourcing and globalization, while effective in terms of cost reduction, come with risks in terms of IP piracy, and poses a unique supplier management challenge.

The vulnerability arises when a design is outsourced to an untrusted supplier (i.e., an untrusted foundry, or "fab") for fabrication. As an untrusted fab possesses all the relevant information regarding the buyer's design, it can easily engage in a practice known as *overproduction,* in which they produce more chips than the contracted amount and sell the extra units at a deep discount without the knowledge of a design house (Jin, 2015; Guin *et al*., 2014a; Actel, 2002). In the globalized supply chain of semiconductor manufacturing, test and distribution, design houses have little control over the protection of their designs. Additionally, the threat of IP piracy arises from physical reverse engineering of the IC or pirating the design for manufacturing – effectively creating clones of the authentic parts for a fraction of the cost. A clone is an unauthorized production of a part without the producers having the legal IP rights (Guin *et al*. 2014a). The layer-by-layer reverse engineering of the IC by an untrustworthy supplier can lead to the extraction of the IP, exposing the complete or targeted part of the design. The development and verification of IP requires

significant time and effort, and as a result, the unauthorized copying or modifying of the IP for illegal redistribution or reuse leads to economic losses for the firm and security risks to end users. IP infringement has emerged as a costly threat as restricting an adversary from obtaining the design information has become very difficult.

From a purchasing and supply perspective, while it is always ideal to purchase from a *trusted* supplier or manufacturer, it is not always a feasible option. The resulting questions are "who can be trusted?" and "if they cannot be trusted, how can we mitigate our risks?" (Chesebrough, 2017). Indeed, in the electronics supply chain, Villasenor (2013) warns, "trust should not be assumed."

So, what are some approaches currently being investigated within the microelectronics supply chain to ensure trust? One strategy is through industry standardization. Among different standards, SAE International Aerospace Standard AS6171 has gained popularity among various test agencies, which recommends different physical and electrical tests for authentication (SAE International, 2016). The goal of these tests is to identify defects and anomalies present in suspect counterfeit chips. Guin *et al* (2014a, 2014b) introduced counterfeit defect coverage (CDC) and counterfeit Type Coverage (CTC) as test metrics to evaluate the effectiveness of these test methods. The defects taxonomy consists of 69 defects (SAE International, 2016). They also developed an algorithm, known as the CDC algorithm, to determine an optimum set of test methods to maximize CDC. Later, SAE International adopted this methodology in Aerospace Standard AS6171 for the basis of test method selection and evaluation of test effectiveness. The currently-used assessment framework is shown in Figure 3. This framework works in two different modes. In "Custom Assessment", the effectiveness of the user/requester test plan is evaluated. The test metrics, CDC, CTC, Under-Covered Defects (UCDs), and Not-Covered Defects (NCDs), are reported. In the "Dynamic Assessment", the framework receives the user-specified test time and cost as the input and recommends a set of test methods that provide maximum coverage with/without considering test time, cost budget and risk level. Then the assessment is done based on the same test metrics. The inputs of the framework, i.e., confidence level matrix (the detection confidence of a defect by a test method), defects mapping, and decision index are developed from the inputs of the subject matter experts (SMEs).

Another strategy is to employ a radio-frequency identification (RFID) tag with a small non-volatile memory (NVM) which can be placed on the package to enable the traceability of electronic parts, particularly, microcircuits. Alam *et al*. (2018) proposed to store the frequency of a ring oscillator (RO) and an electronic chip ID (*ECID*) into a passive RFID tag, which can be accessed through a commercial RFID reader. The content of the tag is protected using a digital signature. An improved solution proposed by Zhang & Guin (2019) builds a chain of trust amongst the manufacturer, distributors, and the system integrator (end-user) by enabling end-to-end traceability from manufacturing to system integration and provides robust protection against IC recycling. A hash-chain-like structure is exploited to enable the traceability that records all the stages involved in the entire supply chain. The integrity of the chain is ensured by adding the authentic public key from the following stage into the digital signature. A distributor can verify the RFID content without powering the chip up. Note that any modification or tampering of the RFID tag data can be easily detected as digital signatures protect the content. Recycled parts can be detected by comparing the verified RO frequencies stored in the RFID tag memory with measured values from the chip by the end-user only.

Further, blockchain technology has been discussed as a candidate to ensure the security and integrity of the supply chain. Blockchain is a distributed and shared digital ledger, where all the transactions and records are hashed and stored to provide both integrity and transparency. The inherent properties and features of blockchain (near-real time, disintermediation, distributed, irreversibility, and immutability) could significantly enhance the traceability, transparency, and reliability of the supply chain (Cui *et al*., 2019a; Xu *et al*., 2019; Islam & Kundu, 2019). A low-cost blockchain instance has been proposed by Cui *et al*. (2019b) for providing traceability of electronic parts. The prototype system is implemented using a

permissioned blockchain instance (e.g., Hyperledger Fabric, Androulaki *et al*., (2018)). A unique device ID is embedded into the device using one-time programmable memory (e.g., ECID) or a unique identification obtained for a physically unclonable function (PUF), which will be stored in the blockchain for future authentication. The blockchain-based framework can comprehensively address in-transit thefts, human errors, delivery and management failures, and dishonest entities in the supply chain by enabling device ownership transfer, which can be triggered and controlled by device owners.

Finally, a number of novel technological solutions at the hardware level have been proposed to prevent IP piracy by limiting the attacker's capability of accessing the inner details of ICs, briefly described here:

- *Logic Locking:* The underlying principle in logic locking is to incorporate additional key gates in the original netlist to obtain a key-dependent circuit, where only the design house knows the correct secret key. This key needs to be stored in tamper-proof memory once a chip passes manufacturing tests at a secure location (Guin *et al*., 2018, 2017, 2016). Despite many solutions to resist attacks, logic locking techniques have not achieved complete security against physical attacks as previously thought due to the possibility of the key extraction (Subramanyan *et al*., 2015). As a result, currently none of the logic locking techniques can be categorized to provide absolute defense against IP piracy.
- *IC Camouflaging:* The camouflaging of IC designs provides deceptive information to an adversary exploiting the design using physical reverse engineering techniques. The notion of IC camouflaging is based on the fabrication level steps, which typically require creating a layout from camouflaged cells/gates whose functionality or gate type cannot be deduced under reverse engineering. However, the camouflaged cells still perform the same function as intended by the IC designer to correctly depict the functionality of the IP in place (Shakya *et al*., 2019; Li *et al*, 2017a; Yasin *et al*., 2016). Note that a foundry is treated as trusted, and camouflaging cannot be used to address IP piracy at an untrusted foundry.
- *Split Manufacturing:* The production of ICs is carried out in two different foundries when split manufacturing is implemented. The design of an SoC needs to be divided into two parts - front end of the line (FEOL) and back end of the line (BEOL). An untrusted foundry is provided with the FEOL design, which contains partial information regarding the SoC that requires complex steps for fabricating and involves higher cost. Fabrication of BEOL does not incorporate complex fabrication steps and can be done at a trusted foundry. The untrusted foundry sends the fabricated wafers directly to the trusted foundry for the complete fabrication. An untrusted foundry cannot reconstruct the complete SoC as it does not have layout or connection details for the upper metal layers (Yang *et al*., 2020; Wang *et al*., 2018; Vaidyanathan *et al*., 2014).
- *Watermarking:* The process of IP watermarking is based on embedding secret information inside an IP design. Watermarking can be used to authenticate and identify the IP owner if required. Practically, the watermark should be robust enough to prevent any external modification to it, and it should not adversely impact the IP functionality. It should be disseminated throughout the design but with lower overhead. The main challenge is to avoid very expensive redesign steps and to eliminate or at least reduce the number of required unique masks (Cui *et al*., 2011; Abdel-Hamid *et al*., 2005).

4.2. Numerical Example

The following is a numerical example of overproduction to demonstrate the general principles and methods described above. Given the covert nature of overproduction, it is difficult to trace specific details (Polczynski, 2004) and therefore the specific values are illustrative.

Suppose an original component manufacturer (OCM) designs an IC with proprietary IP, and seeks to contract the manufacturing of the IC to a foundry for a price of $75,000. Suppose the OCM holds a contract

to sell the manufactured parts for $150,000 to an OEM, and therefore if they decide to place their trust in the untrusted foundry, and the foundry cooperates (i.e., does not steal the OCM's IP), the OCM's payoff will be $75,000 (the $150,000 sale less the $75,000 payment to the foundry). On the other hand, if the foundry steals the IP, the OCM incurs a total loss of $500,000, which includes loss of future profit of the ICs ($425,000), which have flooded the market at a lower price. Finally, if the OCM decides not to trust the foundry, the OCM incurs a certain loss of $75,000, i.e., the lost profit from not filling the contract.

Further, assume that the subjective probability estimation that the OCM places on the foundry cooperating is *p,* and therefore the subjective probability estimate that the foundry does not cooperate (i.e., steals the IP), is *1-p.* This is summarized in Figure 4.

We conduct a sensitivity analysis by varying the value of *p* between 0 (assuming the foundry definitely will not cooperate) and 1 (assuming the foundry definitely will cooperate). We plot the expected payoff from trusting the foundry with the valuable IP. Moreover, we calculate the risk incurred by the OCM in this uncertain trust relationship from (1), which is simply the estimated probability that the foundry steals the IP multiplied by the losses associated with that outcome. Finally, we assume the OCM somehow had perfect information about whether the foundry would or would not cooperate. As mentioned above, perfect information is a theoretical abstraction, but provides a helpful upper bound on the willingness to pay for additional uncertainty reduction. From (2), we calculate the value of the perfect information as we vary the subjective probability estimate *p.*

What does the decision look like from the perspective of the foundry? The foundry has two alternatives, namely to overproduce (betrayal) and to not overproduce (cooperation). Assume that if the foundry does not overproduce, i.e., they manufacture the contracted quantity of units as promised, then they make a payoff of $75,000 (i.e., their payment from the OCM). If they decide to overproduce, they still receive the payment, as well as some additional payoff, $425,000 (the amount that the OCM lost). However, assume there is a probability *q* that the foundry gets caught and has to pay a fine of $1,000,000. The resulting decision tree is shown in Figure 5.

4.3. Results, Discussion, and Extensions

The results from the trustor's perspective are plotted in Figure 6. Note that the x-axis in Figure 6 is *p,* the probability that the trustor estimates that the trustee will cooperate, which is the definition of trust given by Gambetta (2000). In other words, we can view Figure 6 as plotting the expected payoff of the trustor as a function of trust in the trustee.

A noteworthy feature of Figure 6 is that the VoI is maximized at a probability *p* around 0.739. This is the probability at which the OCM would be indifferent between trusting and not trusting the foundry. As a general feature of VoI, in order for information to have value, the information must change a future decision (Coopersmith & Cunningham, 2002). In other words, ability to make a different decision in light of new information is the source of the value. Since being exactly indifferent implies that a small change in some relevant variable such as a payoff or a probability would change one's decision to one alternative or the other, marginal information has a great deal of value. Similarly, we see that VoI is worthless when *p* equals 0 and 1. The same reasoning applies – when a decision maker has certainty, additional information has no value since nothing new was learned and so no different decision was made.

In Figure 7, we set the x-axis to the probability that the trustee gets caught if they decide to overproduce, *q*. Two interesting points are worth noting in Figure 7. First, the point where the payoff of betrayal (overproducing) is equal to the payoff of cooperation (not overproducing) is at approximately q=0.298. In other words, if there is a greater than 0.298 probability of getting caught overproducing, the foundry is better off cooperating instead. Another interesting intersection point is where the expected payoff of

betrayal is equal to $0, corresponding to a probability of getting caught of around 0.35. This means that the foundry would never decide to overproduce if the probability of getting caught was greater than 0.35, since the expected payoff would be negative.

How does this relate back to the trustor's decision? If the foundry believes that their probability of getting caught is less than 0.298, they will choose to overproduce. While the probability of the foundry getting caught if they overproduce is distinct than the probability that they will actually overproduce, it is a reasonable first pass assumption from the trustor's point of view to estimate the probability of trustee cooperation (i.e., p) as $1-q$, i.e., the probability of the trustee getting away with overproduction. If the foundry cooperates if $q > 0.298$, this implies that they cooperate if $1-q > 0.702$ (i.e., if their probability of not getting caught is greater than 0.702, they will not overproduce). If the OCM lets $p \geq 0.702$, then their payoff of trusting (between -$96,350 and $75,000 over the range $p=[0.702,1]$) is sometimes greater and sometimes less than the payoff of not trusting (they would be indifferent when $p=0.739$), and the maximum VOI is equal to $105,300 (when $p=0.702$), setting an upper bound for the amount of money they would be willing to expend to learn about the foundry's trustworthiness.

4.3.1. Extension: Value of Imperfect Information

One rarely, if ever, can acquire perfect information, and so instead, we often rely on sample, or imperfect, information. Sample information can come from the results of some type of test or expert elicitation, in which there is some uncertainty remaining. For instance, Coopersmith and Burkholder (2013) described the use of sample information in deciding where to drill for oil. In their example, seismic tests were conducted to give a better, although imperfect, understanding of whether an underground reservoir will produce oil. Whereas perfect information gives the decision maker the ability to know the future states of nature with certainty, sample information reduces the uncertainty only somewhat (Keisler et al., 2013).

One potential way to gather information about a potential supply chain partner would be to ask for references. Aamdot (2006) defined a reference as an "expression of an opinion, either orally or through a written checklist, regarding an applicant's ability, previous performance, work habits, character, or potential for future success." The purpose of soliciting such references, which may be an element of a larger background check or due diligence effort, is to uncover "counterproductive work behaviors" which include illegal, immoral, and/or deviant behavior which may be impactful to the organization (Brody et al., 2015). References are not highly accurate predictors of behavior, however, and are prone to two failure modes – falsely identifying bad partners as good, and falsely identifying good partners as bad (Brody et al., 2015). Aamdot and Williams (2005) found the predictive validity of references to be around 0.29, while McCarthy and Goffin (2001) reported values from the literature between 0.01 and 0.38. Such low predictive validity could be due to leniency (a bias toward only reporting the positives while withholding the negatives) and a lack of knowledge about the subject of the reference (Aamdot, 2006).

With this in mind, consider that the foundry will either *Cooperate (C)* or *Betray (C'),* once a formal buyer-supplier relationship has been established. Further, assume that the OCM can gather some sample information (e.g., by soliciting some references) on the foundry, resulting in an impression in which the foundry *Appears Trustworthy (T)* or *Appears Untrustworthy (T').* If the foundry is actually going to cooperate (with probability $P(C)=p$), the reference returns an impression of "appears trustworthy" with conditional probability $P(T|C)$. Similarly, if the foundry is actually going to betray (with probability $P(C')$), then the reference will return an impression of "appears untrustworthy" with probability $P(T'|C')$. However, if there are non-zero probabilities of returning incorrect results, i.e., the reference could say the foundry appears untrustworthy when they actually will cooperate, and the reference could say that the foundry appears trustworthy when they in fact will betray, then the information gathered is imperfect.

However, what the OCM would really like to know is: based on the result gained from the reference, what is the probability that the foundry will cooperate or betray. Using Bayes Theorem, we obtain:

$$P(C|T) = \frac{P(T|C)P(C)}{P(T)} = \frac{P(T|C)P(C)}{P(T|C)P(C) + P(T|C')P(C')} \tag{3}$$

In terms of the decision tree, this can be visualized by "flipping the tree", as shown in Figure 8a, where we remove the decision nodes for clarity. The resulting decision tree with imperfect information is shown in Figure 8b. As with the value of perfect information, the value of sample information is equal to the expected payoff of the decision with the sample information minus the expected payoff of the decision without the information.

Since given the prevalence of leniency, references are not necessarily the most predictive indicators of behavior, we will let the probability that a partner will cooperate, given a good reference, P(C|T), be relatively low, 0.65. However, we will assume that the probability of partner betrayal, given a bad reference, P(C'|T') is very high, 0.99. The resulting graph (Figure 9) shows the value of sample information plotted against the value of perfect information. We see that the value of sample information is less than the value of perfect information. The value of perfect information provides an upper bound of the value of sample information.

4.3.2. Extension: Loss Aversion

Another extension to the model described above is the incorporation of attitude about risk and loss. In the preceding examples, we have assumed that the decision makers are risk neutral. However, in reality, decision makers may approach trust decisions based on some level of risk aversion (Arai, 2009). Specifically, we consider the case of loss aversion, in which decision makers interpret the impact of losses as greater than the impact of the same amount of gains. Tversky and Kahneman (1992) defined a value function for some monetary gain or loss *x,* as:

$$v(x) = \begin{cases} x^{\alpha} & if\ x \geq 0 \\ -\lambda(-x)^{\beta} & if\ x < 0 \end{cases} \tag{4}$$

where α and β are parameters related to risk aversion, and λ is a coefficient denoting the aversion to losses.

Following Tversky and Kahneman (1992), we use $\alpha=\beta=0.88$, and $\lambda=2.25$. The resulting graph (Figure 10) shows the value of trusting and not trusting, as well as the risk of trusting. The discontinuity in the value for trusting occurring around $p=0.87$, which is where the value of trusting is equal to 0. This is the point, as we increase in *p,* that the loss aversion no longer applies.

5. Theoretical and Managerial Implications

As supply chains evolve, becoming more complex, global, and interconnected, the importance of considering trust increases for personnel responsible for purchasing and supply management. Important theoretical and practical implications exist for both buyers and suppliers.

5.1. Theoretical Implications

From a theoretical perspective, while the theory of trust recognizes the distinction between calculative and relational trust (Poppo *et al*., 2016), we have framed and operationalized trust in a calculative manner, most closely associated with the theory of Transaction Cost Economics. In part, the calculative notion of trust lends itself more naturally to the type of decision modeling employed in this paper. While there is a calculative aspect to trust, focusing strictly on calculative trust at the expense of relational trust can overlook the importance of the social embeddedness of the buyer-supplier relationship (Granovetter, 1985). Moreover, the calculative perspective focuses more on a one-shot transaction, where the relational perspective is more suited to view the trust relationship as it evolves over time through repeated interactions. Such repeated interactions may lend themselves to being modeled using game theory. Therefore, conceptualizing and synthesizing trust in both calculative and relational terms is an important next step for theoretical development.

Proposition 1: *Buyer-supplier trust decision making is typically a repeated, socially embedded relationship, rather than a one-shot transaction. Tools from game theory may be appropriate for modeling such iterated transactions, combining insights from both calculative trust and relational trust.*

Another theoretical aspect is that we have only considered the buyer-supplier relationship in isolation; that is to say that this discussion has ignored the possibility that the buyer may be pursuing a multiple sourcing strategy or that the buyer could switch sourcing to a different supplier (Bygballe, 2017; Costantino *et al*., 2010). Such industry-related dynamics, such as power-dependence, adversarial or cooperative posture, and degree to which the buyer and supplier's operations are interlinked, may play into both the calculative and relational aspects of trust in the buyer-supplier relationship (Tangpong *et al*., 2008).

Proposition 2: *Organizations may pursue risk management strategies such as multiple sourcing. The buyer may view and model themselves as holding a portfolio of supplier relationships, and therefore portfolio analysis tools may be used to optimize the risk and return of engaging in various trust relationships.*

Discussions of trust generally focus on interpersonal or interfirm trust. However, trust can take a wider scope, where researchers have proposed theories where the trustor can place their trust in the products being purchased (Hawlitschek *et al*., 2016), as well as the information technology (IT) artifacts and systems (Vance *et al*., 2008), software code (Thompson, 1984), and e-commerce platforms (Pavlou, 2003; Jarvenpaa *et al*., 2000) which facilitate the transaction. For instance, Hawlitschek *et al*. (2016) extend the trustor-trustee model of Mayer *et al*. (1995) to explore trust in consumer-to-consumer (C2C) markets. From the perspective of the consumer, the intention to consume is driven by the perceived trustworthiness (based on ability, integrity, and benevolence) of the supplying partner, the platform, and the product. Importantly, the product's trustworthiness is considered only in terms of its perceived ability (i.e., functionality or performance), since it is an inanimate object and so cannot act with benevolence or integrity (Hawlitschek *et al*., 2016).

Proposition 3: *The risk associated with trusting changes depending on the trustees. Trustees within a supply chain could refer to a supplier, the product being supplied, or the platform over which the transaction is taking place. Therefore, quantitative analyses of supply chain trust should consider multiple referents.*

5.2. Managerial Implications

From the practical managerial perspective of a buyer (the trustor), trust inherently involves some degree of uncertainty and vulnerability. As a trustor, there are dangers in trusting too much, as well as trusting too little – the virtue lies somewhere in the mean, where the buyer's subjective assessment of trust is close to the actual trustworthiness of the supplier (Butler *et al*., 2009; Solhaug *et al*., 2007). Therefore, during

supplier selection, there is practical value in carrying out uncertainty-reducing actions before entering into a trust relationship with a trustee.

However, it may not always be clear what criteria one would want to investigate before making that decision. In terms of defense microelectronics, as an example, §224 of the 2020 National Defense Authorization Act (2019) defines several criteria for ensuring a trusted supply chain and operational security standards, including: "*(I) manufacturing location; (II) company ownership; (III) workforce composition; (IV) access during manufacturing, suppliers' design, sourcing, manufacturing, packaging, and distribution processes; (V) reliability of the supply chain; and (VI) other matters germane to supply chain and operational security".* However, there is a need for generalized criteria which can be used as guides to information gathering when making quantifiable trust decisions. Relatedly, the literature on supply chain trust identifies numerous possible antecedents to trust. Paluri and Mishal (2020) identified 40 different antecedents, such as communication, information sharing, power, shared values, competence, and others. Wang et al. (2020) presented a table with 27 studies on trust in interfirm relationships, similarly listing the multiple antecedents identified in each study. Each of these antecedents could be a criterion to consider by a trustor when entering into a trust relationship with a trustee. With such a vast quantity of criteria by which to assess trustees, there is a need for a taxonomy, checklist, or similar aid for structuring, collecting, and synthesizing information about different trustees to aid in the decision making process.

Proposition 4: *There is a need for managerial guidance and tools on generalizable criteria which should be considered about a potential supplier when entering into a risky buyer-supplier relationship to aid in the information gathering process.*

From the practical perspective of the supplier, trust is equally important. Risk arises for a supplier based on the possibility of the buyer ending the relationship by switching to another supplier, or not entering into the proposed relationship (Bygballe, 2017; Grudinschi *et al*., 2014). To continue a profitable business relationship, the seller must signal their trustworthiness, in effect adjusting the buyer's subjective probability assessment, *p,* upward, and therefore lowering the buyer's perceived risk. Insights from Signaling Theory (Spence 1973; Ross 1977) can be used by the supplier to communicate particular information about their trustworthiness to the buyer. For example, relationship competencies valued by buyers include a willingness to collaborate and share information, a commitment to the relationship, and shared goals (Grudinschi *et al*., 2014). Selnes (1998) proposes four aspects of trustworthiness and satisfaction: competence, communication, commitment, and conflict handling. Gullett *et al*. (2009) propose six factors: honest communication, task competence, quality assurance, interactional courtesy, legal compliance, and financial balance.

Proposition 5: *Trustworthiness is an important signal. Signaling Theory can be used as a lens to explore how suppliers can strategically signal their competencies with the goal to either enter into a new relationship with a buyer or maintain and improve a current relationship.*

Finally, in terms of practical managerial implications, while it is ideal to buy from a trusted, accredited supplier, in some cases, it is just not feasible. When trust cannot be utilized as a risk management strategy, other tools must be used instead, including contractual mechanisms (Ghosh & Fedorowicz, 2008). Controls that can be used include governance structures, contractual requirements, sanctions for violating one's end of the bargain, holding collateral to protect against the loss, and strict quality standards (Das & Teng, 2001; Molm *et al*., 2000). Finally, if the risk is too high to be acceptable, the best risk management strategy may be *avoidance,* i.e., not to enter into the trust relationship in the first place.

6. Conclusions

This paper explored trust and risk from the perspective of buyer-supplier relationships, and concretized the theoretical discussion through the example of the supply chain for electronics. Using the perspective of decision analysis, we framed the problem as a decision of a buyer whether or not to place trust in a supplier. Using concepts of trust from a number of fields, we were able to model the buyer-supplier trust relationship and estimate the risk associated with a trustee acting against the interests of the trustor. This research builds upon and extends the literature on trust and risk in buyer-supplier relationships by formalizing and relating concepts of risk and trust.

Specifically, we have shown how trust can be modeled in the buyer-supplier relationship in the presence of risk, and how in equation (1) trust and risk are related. Namely, by conceptualizing trust as a subjective probability assessment that the trustee will act in alignment with the interests of the trustor (Gambetta, 2000), the risk can be expressed as a function of that probability and the adverse losses associated with betrayal. This risk-based framing and decision analytic modeling perspective is a novel contribution to the literature on the buyer-supplier relationship.

More research is needed to gather and report data, which can be used to parameterize such models. Currently, parameterization of risk-based models often relies on the inputs from the subject matter experts (SMEs), rather than actual empirical data. The input to such models may be overly optimistic and may provide a false sense of security and confidence, or they could be overly pessimistic and lead to overspending on unnecessary security measures. SME-based models need to be updated, where possible, by utilizing actual data from the current market. Methodological approaches for tracking, monitoring, and reporting uncertainties and risk data represent an area of application for vulnerable supply chains (Lambert *et al*. 2016, 2008).

Finally, regarding the electronics industry, anti-counterfeit and supply chain risk management is only one area of concern for purchasers among many as it relates to a comprehensive, systems-oriented perspective for cyber-physical systems security (DiMase *et al*., 2015). The methodological framework described in this paper could be utilized to investigate other trust relationships within various areas of concern, including track and trace, life cycle and obsolescence management, software assurance and application security, and others.

Acknowledgements: This work was supported in part by the National Science Foundation under Grant 1916760 "Phase I IUCRC University of Virginia: Center for Hardware and Embedded System Security and Trust (CHEST)", and in part by the Commonwealth Center for Advanced Logistics Systems (CCALS) and by Systems Planning & Analysis Inc. (SPA).

REFERENCES

Aamdot, M. (2006), "Validity of recommendations and references", *Assessment Council News: Newsletter of the IPMA-HR Assessment Council,* February 2006, pp. 4-6.

Aamdot, M., and Williams, F. (2005), "Reliability, validity, and adverse impact of references and letters of recommendation", In *20th Annual Conference of the Society for Industrial and Organizational Psychology,*

Abdel-Hamid, A.T., Tahar, S., and Aboulhamid, E.M. (2005), "A public-key watermarking technique for IP designs", In *Design, Automation and Test in Europe,* pp. 330-335.

Actel (2020), "Design security in nonvolatile flash and antifuse FPGAs: security backgrounder", Actel Corporation, Sunnyvale, CA, USA.

Alam, M., Chowdhury, S., Tehranipoor, M.M., and Guin, U. (2018), "Robust, low-cost, and accurate detection of recycled ICs using digital signatures. In *2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pp. 209-214.

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., *et al*. (2018), "Hyperledger fabric: a distributed operating system for permissioned blockchains", In *Proceedings of the Thirteenth EuroSys Conference*, pp. 1-15.

Arai, K. (2009), "Defining trust using expected utility theory", *Hitotsubashi Journal of Economics*, Vol. 50, pp. 205-224.

Bonatto, F., Martins de Resende, L.M., and Pontes, J. (2021), "Supply chain governance: a conceptual model", *Journal of Business & Industrial Marketing,* DOI: 10.1108/JBIM-09-2019-0418.

Brody, R.G., Perri, F.S., and Van Buren, H.J. (2015), "Further beyond the basic background check: predicting future unethical behavior", *Business and Society Review,* Vol. 120 No. 4, pp. 549-576.

Butler, J., Giuliano, P., and Guiso, L. (2009), "The right amount of trust", Working Paper 15344, NBER Working Paper Series, National Bureau of Economic Research, Cambridge, MA.

Bygballe, L.E. (2017), "Toward a conceptualization of supplier-switching processes in business relationships", *Journal of Purchasing & Supply Management,* Vol. 23, pp. 40-53.

Chen, Y.S., Su, H.C., and Ro, Y.K. (2016), "Can I read your mind? Perception gaps in supply chain relationships", *Journal of Purchasing & Supply Management,* Vol. 22, pp. 311-324.

Chesebrough, D. (2017), "Trusted microelectronics: a critical defense need", *National Defense Magazine*, available at: https://www.nationaldefensemagazine.org/articles/2017/10/31/trusted-microelectronics-a-critical-defense-need (accessed 08 April 2020)

Collier, Z.A., and Sarkis, J. (2021), "The zero trust supply chain: managing supply chain risk in the absence of trust", *International Journal of Production Research,* Vol. 59 No. 11, pp. 3430-3445.

Collier, Z.A., and Lambert, J.H. (2021), "Measurement and tracking of project activity quality based on time and cost indicators", In *Proceedings of the Appalachian Research in Business Symposium*, Richmond, KY, USA, pp. 32-37.

Collier, Z.A., and Lambert, J.H. (2020), "Managing obsolescence of embedded hardware and software in secure and trusted systems", *Frontiers of Engineering Management,* Vol. 7 No. 2, pp. 172-181.

Collier, Z.A., DiMase, D., Heffner, K., and Linkov, I. (2015), "Building a trusted and agile supply chain network for electronic hardware", In *20th International Command and Control Research and Technology Symposium (ICCRTS)*, Annapolis, MD, USA.

Collier, Z.A., Walters, S., DiMase, D., Keisler, J.M., and Linkov, I. (2014), "A semi-quantitative risk assessment standard for counterfeit electronics detection", *SAE International Journal of Aerospace*, Vol. 7 No. 1, pp. 171-181.

Colquitt, J.A., Scott, B.A., and LePine, J.A. (2007), "Trust, trustworthiness, and trust propensity: a meta-analytic test of their unique relationships with risk taking and job performance", *Journal of Applied Psychology*, Vol. 92 No. 4, pp. 909-927.

Coopersmith, E., and Burkholder, K. (2013), "Valuing seismic at the drilling program level for sweet spot identification in unconventional resource", In *Unconventional Resources Technology Conference*, Denver, Colorado, USA, 12-14 August 2013.

Coopersmith, E.M., and Cunningham, P.C. (2002), "A practical approach to evaluating the value-of-information and real option decisions in the upstream petroleum industry", In *SPE Annual Technical Conference and Exhibition*, San Antonio, 29 September–2 October, Paper SPE 77421.

Costantino, N., and Pellegrino, R. (2010), "Choosing between single and multiple sourcing based on supplier default risk: a real options approach", *Journal of Purchasing & Supply Management,* Vol. 16, pp. 27-40.

Cui, P., Guin, U., Skjellum, A., and Umphress, D. (2019a), "Blockchain in IoT: current trends, challenges, and future roadmap", *Journal of Hardware and Systems Security*, Vol. 3 No. 4, pp. 338-364.

Cui, P., Dixon, J., Guin, U., and Dimase, D. (2019b), "A blockchain-based framework for supply chain provenance", *IEEE Access*, Vol. 7, pp. 157113-157125.

Cui, A., Chang, C.H., Tahar, S., and Abdel-Hamid, A.T. (2011), "A robust FSM watermarking scheme for IP protection of sequential circuit design", *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, Vol. 30 No. 5, pp. 678-690.

Das, T.K., and Teng, B.S. (2004), "The risk-based view of trust: a conceptual rramework", *Journal of Business and Psychology*, Vol, 19 No. 1, pp. 85-116.

Das, T.K., and Teng, B.S. (2003), "Partner analysis and alliance performance", *Scandinavian Journal of Management,* Vol. 19, pp. 279-308.

Das, T.K., and Teng, B.S. (2001), "Trust, control, and risk in strategic alliances: an integrated framework", *Organization Studies*, Vol. 22 No. 2, pp. 251-283.

DiMase, D., Collier, Z.A., Carlson, J., Gray, R.B., and Linkov, I. (2016), "Traceability and risk analysis strategies for addressing counterfeit electronics in supply chains for complex systems", *Risk Analysis*, Vol. 36 No. 10, pp. 1834–1843.

DiMase, D., Collier, Z.A., Heffner, K., and Linkov, I. (2015), "Systems engineering framework for cyber physical security and resilience", *Environment Systems & Decisions*, Vol. 35 No. 2, pp. 291-300.

Fawcett, S.E., Jin, Y.H., Fawcett, A., and Magnan, G. (2017), "I know it when I see it: the nature of trust, trustworthiness signals, and strategic trust construction," *The International Journal of Logistics Management,* Vol. 28 No. 4, pp. 914-938.

Fawcett, S.E., Jones, S.L., and Fawcett, A.M. (2012), "Supply chain trust: the catalyst for collaborative innovation", *Business Horizons,* Vol. 55, pp. 163-178.

Gambetta, D. (2000). "Can we trust trust?", Gambetta, D. (Ed.), *Trust: Making and Breaking Cooperative Relations*, electronic edition, Department of Sociology, University of Oxford, pp. 213-237.

Gelderman, C.J., Semejin, J., and Verhappen, M. (2020), "Buyer opportunism in strategic supplier relationships: triggers, manifestations, and consequences", *Journal of Purchasing & Supply Management,* Vol. 26 No. 2, article 100581.

Ghosh, A., and Fedorowicz, J. (2008), "The role of trust in supply chain governance", *Business Process Management Journal*, Vol. 14 No. 4, pp. 453-470.

Granovetter, M. (1985), "Economic action and social structure: the problem of embeddedness", *The Americal Journal of Sociology,* Vol. 91 No. 3, pp. 481-510.

Grudinschi, D., Sintonen, S., and Hallikas, J. (2014), "Relationship risk perception and determinants of the collaboration fluency of buyer-supplier relationships in public service procurement", *Journal of Purchasing & Supply Management,* Vol. 20, pp. 82-91.

Guin, U., Zhou, Z., and Singh, A. (2018), "Robust design-for-security architecture for enabling trust in IC manufacturing and test", *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, Vol. 26 No. 5, pp. 818-830.

Guin, U., Zhou, Z., and Singh, A. (2017), "A novel design-for-security (DFS) architecture to prevent unauthorized IC overproduction", In *2017 IEEE 35th VLSI Test Symposium (VTS)*, pp. 1-6.

Guin, U., Shi, Q., Forte, D., and Tehranipoor, M.M. (2016), "FORTIS: a comprehensive solution for establishing forward trust for protecting IPs and ICs." *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, Vol. 21 No. 4, pp. 1-20.

Guin, U., DiMase, D., and Tehranipoor, M. (2014a), "Counterfeit integrated circuits: detection, avoidance, and the challenges ahead," *Journal of Electronic Testing*, Vol. 30 No. 1, pp. 9-23.

Guin, U., DiMase, D., and Tehranipoor, M. (2014b), "A comprehensive framework for counterfeit defect coverage analysis and detection assessment", *Journal of Electronic Testing*, Vol. 30, No. 1, pp. 25-40.

Gullett, J., Do, L., Canuto-Carranco, M., Brister, M., Turner, S., and Caldwell, C. (2009)" "The buyer-supplier relationship: an integrative model of ethics and trust", *Journal of Business Ethics,* Vol. 90, pp. 329-341.

Hallikas, J., Puumalainen, K., Vesterinen, T., and Virolainen, V.M. (2005), "Risk-based classification of supplier relationships:, *Journal of Purchasing & Supply Management,* Vol. 11, pp. 72-82.

Hawlitschek, F., Teubner, T., and Weinhardt, C. (2016), "Trust in the sharing economy", *Swiss Journal of Business Research and Practice*, Vol. 70 No. 1, pp. 26-44.

Hill, J.A., Eckerd, S., Wilson, D., and Greer, B. (2009), "The effect of unethical behavior on trust in a buyer-supplier relationship: the mediating role of a psychological contract violation", *Journal of Operations Management,* Vol. 27, pp. 281-293.

Holma, A.M. (2012), "Interpersonal interaction in business triads – case studies in corporate travel purchasing", *Journal of Purchasing & Supply Management,* Vol. 18, pp. 101-112.

Howard, R.A. (1966), "Information Value Theory", *IEEE Transactions on Systems Science and Cybernetics*, Vol. 2 No. SSC1, pp. 22-26.

Huang, J., and Nicol, D. (2009), "A calculus of trust and its application to PKI and identity management", In *IDTrust '09*, Gaithersburg, MD, USA.

Huang, J., and Fox, M.S. (2005), "Trust judgement in knowledge provenance", Proceedings of the 16th International Workshop on Database and Expert Systems Applications (DEXA'05).

Hurley, R.F. (2006), "The decision to trust", *Harvard Business Review*, Vol. 84 No. 9, pp. 55-62.

Inkpen, A.C., and Currall, S.C. (2004), "The coevolution of trust, control, and learning in joint ventures", *Organization Science,* Vol. 15 No. 5, pp. 586-599.

Islam, M. N., and Kundu, S. (2019), "Enabling IC traceability via blockchain pegged to embedded PUF", *ACM Transactions on Design Automation of Electronic Systems (TODAES),* Vol. 24 No. 3, pp. 1-23.

Jarvenpaa, S.L., Tractinsky, N., and Vitale, M. (2000), "Consumer trust in an internet store", *Information technology and management*, Vol. 1 No. 1-2, pp. 45-71.

Jin, Y. (2015), "Introduction to hardware security", *Electronics,* Vol. 4, pp. 763-784.

Kaplan, S., and Garrick, B.J. (1981), "On the quantitative definition of risk", *Risk Analysis,* Vol. 1 No. 1, pp. 11-27.

Keisler, J.M., Collier, Z.A., Chu, E.J., Sinatra, N., and Linkov, I. (2014), "Value of information analysis: state of the application", *Environment Systems & Decisions*, Vol. 34 No. 1, pp. 3-23.

Kindervag, J. (2010), "Build security into your network's DNA: the zero trust network architecture", Cambridge, MA: Forrester Research, Inc.

Kleemann, F.C., and Essig, M. (2013), "A providers' perspective on supplier relationships in performance-based contracting", *Journal of Purchasing & Supply Management,* Vol. 19, pp. 185-198.

Kraljic, P. (1983), "Purchasing must become supply management", *Harvard Business Review,* Vol. 61 No. 5, pp. 109-117.

Lambert, J.H., N.N. Joshi, and S.A. Thekdi (2016), "Multi-dimensional data and model uncertainties in comparing heterogeneous benefits of distributed transportation projects", *ASCE Journal of Infrastructure Systems.* Vol. 22 No. 2, article 04015020.

Lambert, J.H., J.M. Keisler, W.E. Wheeler, Z.A. Collier, and I. Linkov (2013), "Multiscale approach to the security of hardware supply chains for energy systems", *Environment Systems & Decisions*, Vol. 33 No. 3, pp. 326-334.

Lambert, J.H., B.L. Schulte, and N.N. Joshi (2008), "Multiple criteria intelligence tracking for detecting extremes from sequences of risk incidents", *Journal of Industrial and Management Optimization*, Vol. 4 No. 3, pp. 511-533.

Large, R.O. (2005), "External communication behaviour of purchasers – effects on supplier management performance", *Journal of Purchasing & Supply Management,* Vol. 11, pp. 28-41.

Leopold, D. (2020), "DARPA chip effort pivots to securing US supply chain", Enterprise AI, available at: https://www.enterpriseai.news/2020/08/20/darpa-chip-effort-pivots-to-securing-us-supply-chain/ (accessed 24 May 2021).

Li, M., Shamsi, K., Meade, T., Zhao, Z., Yu, B., Jin, Y., and Pan, D.Z. (2017), "Provably secure camouflaging strategy for IC protection", *IEEE transactions on computer-aided design of integrated circuits and systems*, Vol. 38 No. 8, pp. 1399-1412.

Lopez, C.T. (2020), "DOD adopts zero trust approach to buying microelectronics", DOD News, available at: https://www.defense.gov/Explore/News/Article/Article/2192120/in-microelectronics-dod-moves-from-trusted-foundry-model-to-zerotrust/ (accessed 24 May 2021)

Lowrance, W.W. (1976), *Of Acceptable Risk: Science and the Determination of Safety*, William Kaufman Inc.

Mason, S.J., Cole, M.H., Ulrey, B.T., and Yan, L. (2002), "Improving electronics manufacturing supply chain agility through outsourcing", *International Journal of Physical Distribution & Logistics Management*, Vol. 32 No. 7, pp. 610–620.

Mayer, R.C., Davis, J.H., and Schoorman, F.D. (1995), "An integrative model of organizational trust", *Academy of Management Review,* Vol. 20 No. 3, pp. 709-734.

McCarthy, J.M., and Goffin, R.D. (2001), "Improving the validity of letters of recommendation: an investigation of three standardized reference forms", *Military Psychology,* Vol. 13 No. 4, pp. 199-222.

Möllering, G. (2003), "A typology of supplier relations: from determinism to pluralism in inter-firm empirical research", *Journal of Purchasing & Supply Management,* Vol. 9, pp. 31-41.

Molm, L.D., Takahashi, N., and Peterson, G. (2000), "Risk and trust in social exchange: an experimental test of a classical proposition", *The American Journal of Sociology*, Vol. 105 No. 5, pp. 1396-1427.

National Defense Authorization Act for Fiscal Year 2020, Public Law 116-92 § 224 (2019), available at: https://congress.gov/116/plaws/publ92/PLAW-116publ92.pdf (accessed 24 May 2021)

Nickel, P.J., and Vaesen, K. (2012), "Risk and trust", Roeser, S., Hillebrand, R., Sandin, P., Peterson, M., (Ed.s.), *Handbook of Risk Theory: Epistemology, Decision Theory, Ethics and Social Implications of Risk*. Springer: Berlin, pp. 857-876.

NIST (2020). "Zero Trust Architecture", NIST Special Publication 800-207. Gaithersburg, MD: National Institute of Standards and Technology.

Paluri, R.A., and Michal, A. (2020), "Trust and commitment in supply chain management: a systemic review of literature", *Benchmarking: An International Journal,* Vol. 27 No. 10, pp. 2831-2862.

Pavlou, P.A. (2003), "Consumer acceptance of electronic commerce: integrating trust and risk with the technology acceptance model", *International Journal of Electronic Commerce*, Vol. 7 No. 3, pp. 69-103.

Polczynski, M.H. (2004), "Protecting intellectual property in a global environment", *Intellectual Property Journal,* Vol. 18, pp. 83-95.

Poppo, L., Zhou, K.Z., and Li, J.J. (2016), "When can you trust "trust"? Calculative trust, relational trust, and supplier performance", *Strategic Management Journal,* Vol. 37, pp. 724-741.

Ragsdale, C.T. (2107). *Spreadsheet Modeling and Decision Analysis: A Practical Introduction to Business Analytics.* 8th Edition. Cengage: Boston.

Ross, S.A. (1977), "The determination of financial structure: the incentive signaling structure", *Bell Journal of Economics*, Vol. 8, pp. 23–40.

SAE International (2016), "Test methods standard; general requirements, suspect/counterfeit, electrical, electronic, and electromechanical parts", available at: https://www.sae.org/standards/content/as6171a/ (accessed 08 April 2020)

Sarkar, A., and Mohapatra, P.K.J. (2006), "Evaluation of supplier capability and performance: a method for supply base reduction", *Journal of Purchasing & Supply Management,* Vol. 12, pp. 148-163.

Sears, J.B, McLoed, M.S., Evert, R.E., Payne, G.T. (2020), "Alleviating concerns of misappropriation in corporate venture capital: creating credible commitments and calculative trust", *Strategic Organization,* DOI: 10.1177/1476127020926174

Selnes, F. (1998), "Antecedents and consequences of trust and satisfaction in buyer-seller relationships", *European Journal of Marketing,* Vol. 32 No. 3, pp. 305-322.

Shakya, B., Shen, H., Tehranipoor, M., and Forte, D. (2019), "Covert gates: protecting integrated circuits with undetectable camouflaging", *IACR Transactions on Cryptographic Hardware and Embedded Systems*, Vol. 3, pp. 86-118.

Solhaug, B., Elgesem, D., and Stølen, K. (2007), "Why trust is not proportional to risk", In *Second International Conference on Availability, Reliability and Security (ARES'07)*.

Sood, B., Das, D., and Pecht, M. (2011), "Screening for counterfeit electronic parts", *Journal of Materials Science: Materials in Electronics,* Vol. 22 No. 10, pp. 1511–1522.

Spekman, R.E., Kamauff Jr., J.W., and Myhr, N. (1998), "An empirical investigation into supply chain management: a perspective on partnerships", *International Journal of Physical Distribution & Logistics Management*, Vol. 28 No. 8, pp. 630-650.

Spence, M. (1973), "Job market signaling", *Quarterly Journal of Economics,* Vol. 87, pp. 355–374.

Subramanyan, P., Ray, S., and Malik, S. (2015), "Evaluating the security of logic encryption algorithms", In *2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pp. 137-143.

Suh, T., and Kwon, I.W.G. (2006), "Matter over mind: when specific asset investment affects calculative trust in supply chain partnership", *Industrial Marketing Management*, Vol. 35, pp. 191-201.

Tallman, S.B., and Shenkar, O. (1997), "A managerial decision model of international cooperative venture formation", *Journal of International Business Studies*, Vol. 25 No. 1, pp. 91-113.

Tangpong, C., Michalisin, M.D., and Melcher, A.J. (2008), "Toward a typology of buyer-supplier relationships: a study of the computer industry", *Decision Sciences,* Vol. 39 No. 3, pp. 571-593.

Tate, W. (2010), "A primer on sourcing and procurement in an integrated supply chain", *Supply Chain Management Review,* available at: https://www.scmr.com/article/a_primer_on_sourcing_and_procurement_in_an_integrated_supply_chain (accessed 15 July 2020)

Thompson, K. (1984), "Reflections on trusting trust", *Communications of the ACM,* Vol. 27 No. 8, pp. 761-763.

Tversky, A., and Kahneman, D. (1992), "Advances in prospect theory: cumulative representation of uncertainty", *Journal of Risk and Uncertainty,* Vol. 5, pp. 297-323.

Vaidyanathan, K., Liu, R., Sumbul, E., Zhu, Q., Franchetti, F., and Pileggi, L. (2014), "Efficient and secure intellectual property (IP) design with split fabrication", In *2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST),* pp. 13-18.

van der Valk, W., Sumo, R., Dul, J., and Schroeder, R.G. (2016), "When are contracts and trust necessary for innovation in buyer-supplier relationships? A necessary condition analysis", *Journal of Purchasing & Supply Management,* Vol. 22, pp. 266-277.

Vance, A., Elie-Dit-Cosaque, C., and Straub, D.W. (2008), "Examining trust in information technology artifacts: the effects of system quality and culture", *Journal of Management Information Systems*, Vol. 24 No. 4, pp. 73–100.

Villasenor, J. (2013), "Compromised by design? Securing the defense electronics supply chain", Center for Technology Innovation at Brookings Institute. Washington, DC.

Wang, M., Zhang, Q., Zhou, K.Z. (2020), "The origins of trust asymmetry in international relationships: an institutional view", *Journal of International Marketing,* Vol. 28 No. 2, pp. 81-101.

Wang, Y., Chen, P., Hu, J., Li, G., and Rajendran, J. (2018), "The cat and mouse in split manufacturing", *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, Vol. 26 No. 5, pp. 805-817.

Williamson, O.E. (1993), "Calculativeness, trust, and economic organization", *Journal of Law and Economics,* Vol. 36 No. 1, pp. 453-486.

Wood, G. (2016), "Costly counterfeit electronic components in the supply chain can also be a safety concern. IHS Markit", available at: http://blog.ihs.com/costly-counterfeit-electronic-components-in-the-supply-chain-can-also-be-a-safety-concern (accessed 08 April 2020).

Xu, X., Rahman, F., Shakya, B., Vassilev, A., Forte, D., and Tehranipoor, M. (2019), "Electronics supply chain integrity enabled by blockchain", *ACM Transactions on Design Automation of Electronic Systems (TODAES),* Vol. 24 No. 3, pp. 1-25.

Yang, Y., Chen, Z., Liu, Y., Ho, T. Y., Jin, Y., and Zhou, P. (2020), "How secure is split manufacturing in preventing hardware trojan?", *ACM Transactions on Design Automation of Electronic Systems (TODAES),* Vol. 25 No. 2, pp. 1-23.

Yasin, M., Mazumdar, B., Sinanoglu, O., and Rajendran, J. (2016), "CamoPerturb: secure IC camouflaging for minterm protection", In *2016 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, pp. 1-8.

Zhang, Y., and Guin, U. (2019), "End-to-end traceability of ICs in component supply chain for fighting against recycling", *IEEE Transactions on Information Forensics and Security*, Vol. 15, pp. 767-775.

Figure Captions

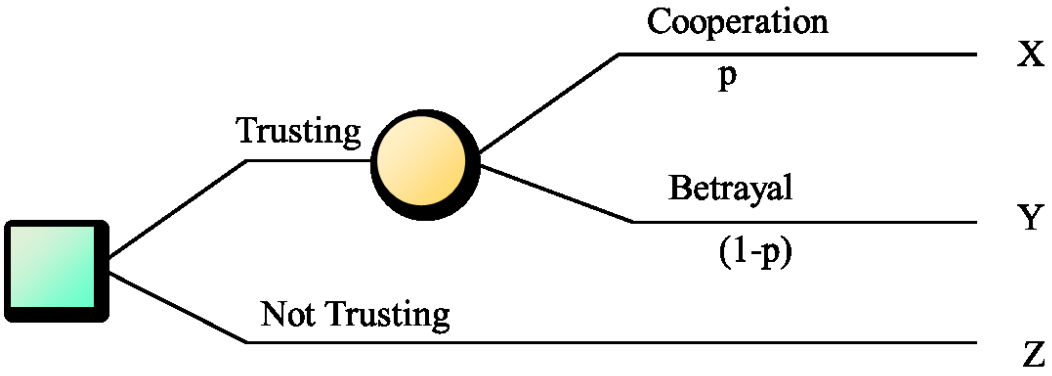

Figure 1: Simple Trust Decision

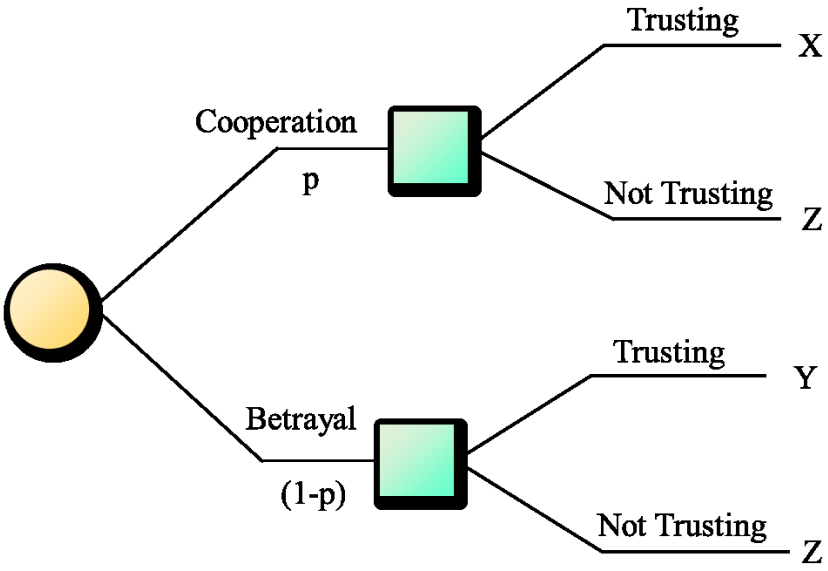

Figure 2: Trust Decision with Perfect Information

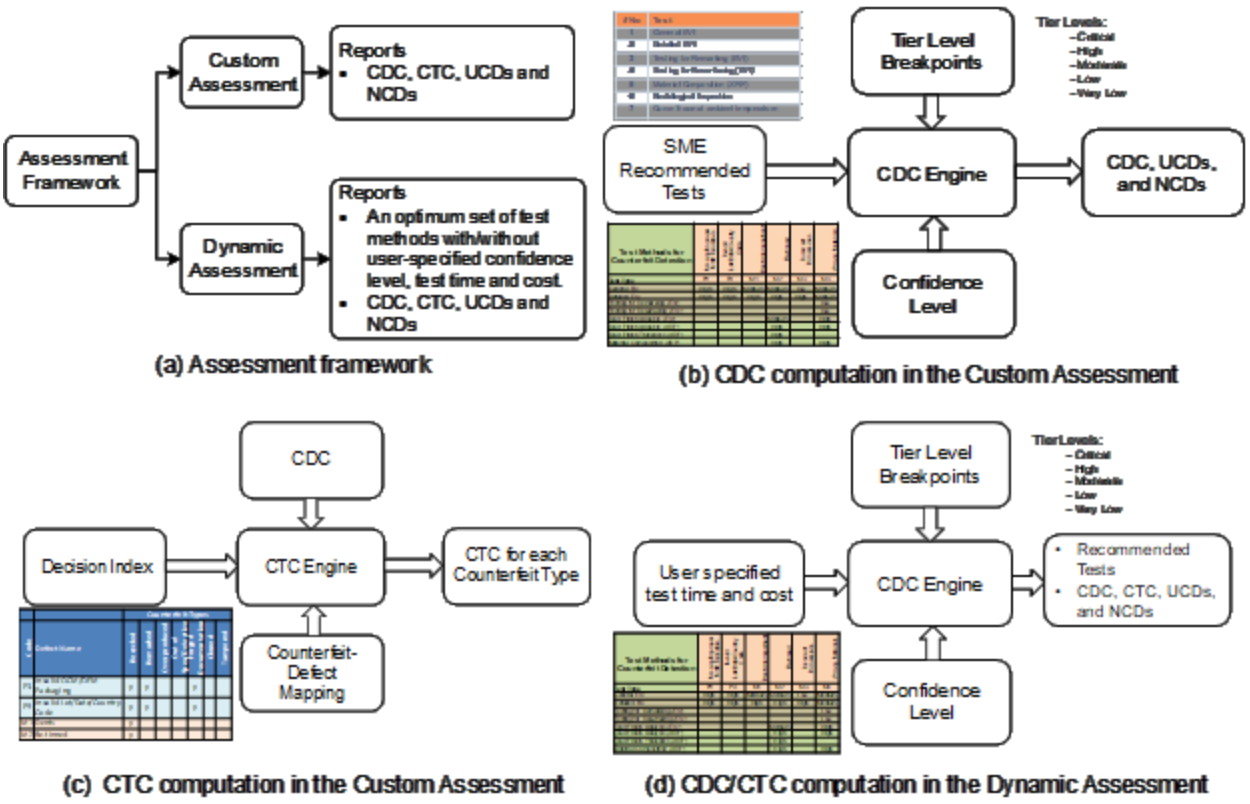

Figure 3: Evaluation of the effectiveness of the test methods based on CDC/CTC metrics.

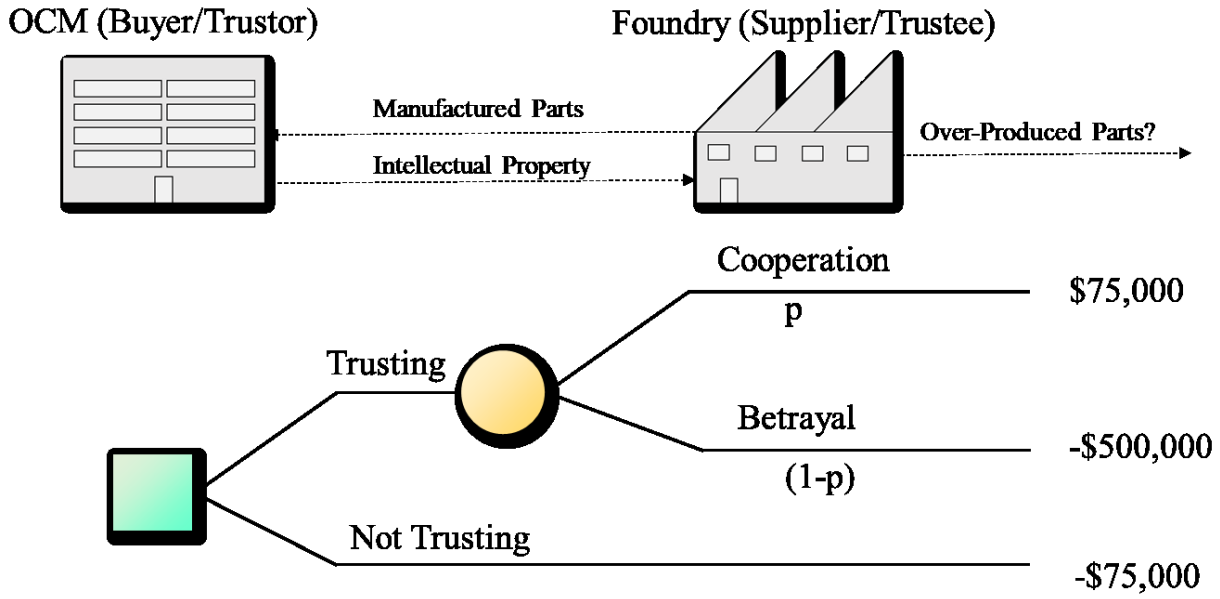

Figure 4: Case Study between an OCM (Trustor) and Foundry (Trustee)

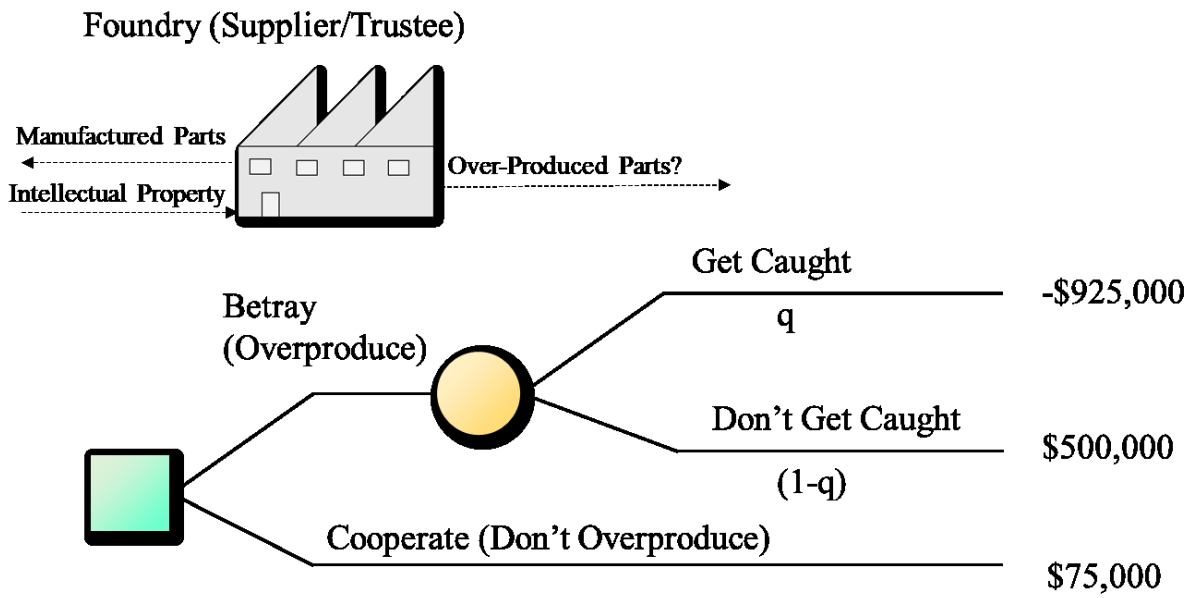

Figure 5: The decision to overproduce or not from the trustee's perspective

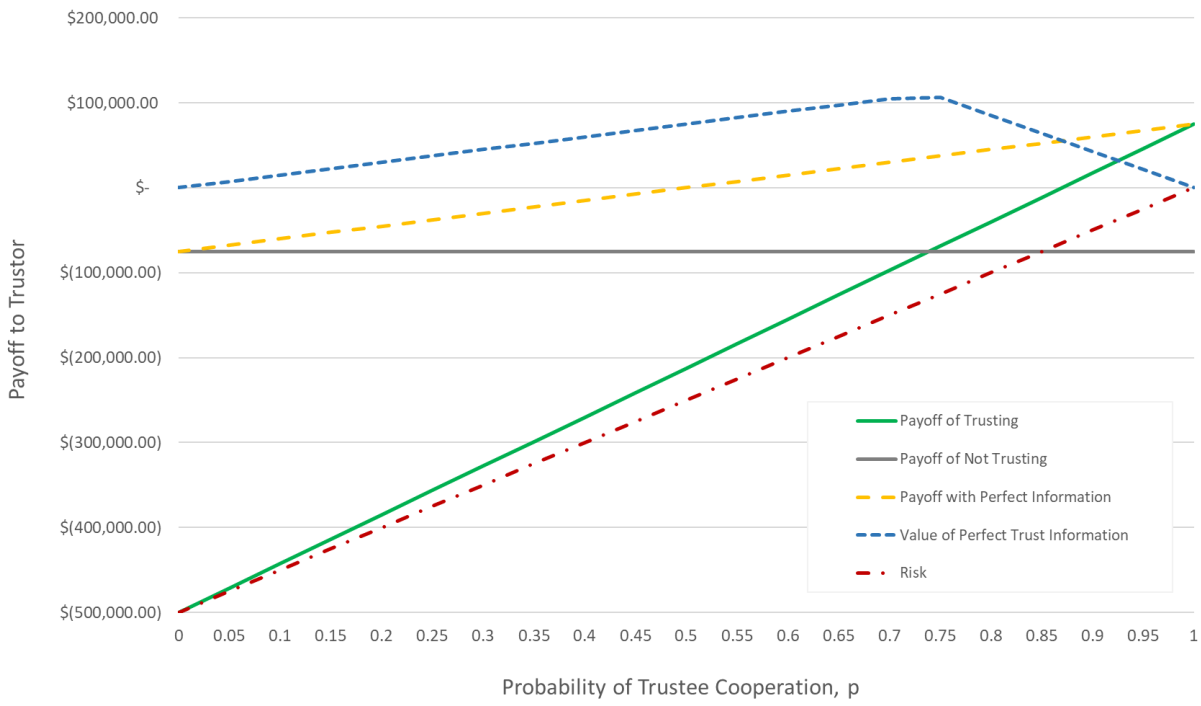

Figure 6: Payoffs and value of information associated with the decision of an OCM to trust a foundry

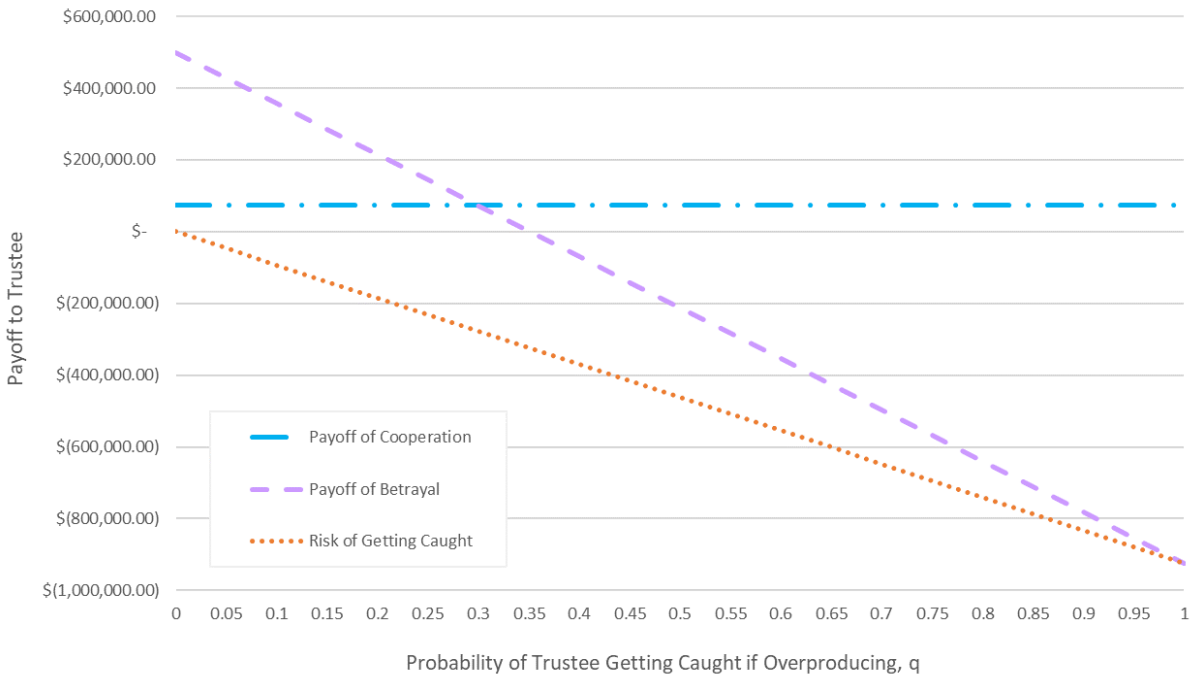

Figure 7: Payoffs associated with the decision of a foundry to overproduce or not overproduce

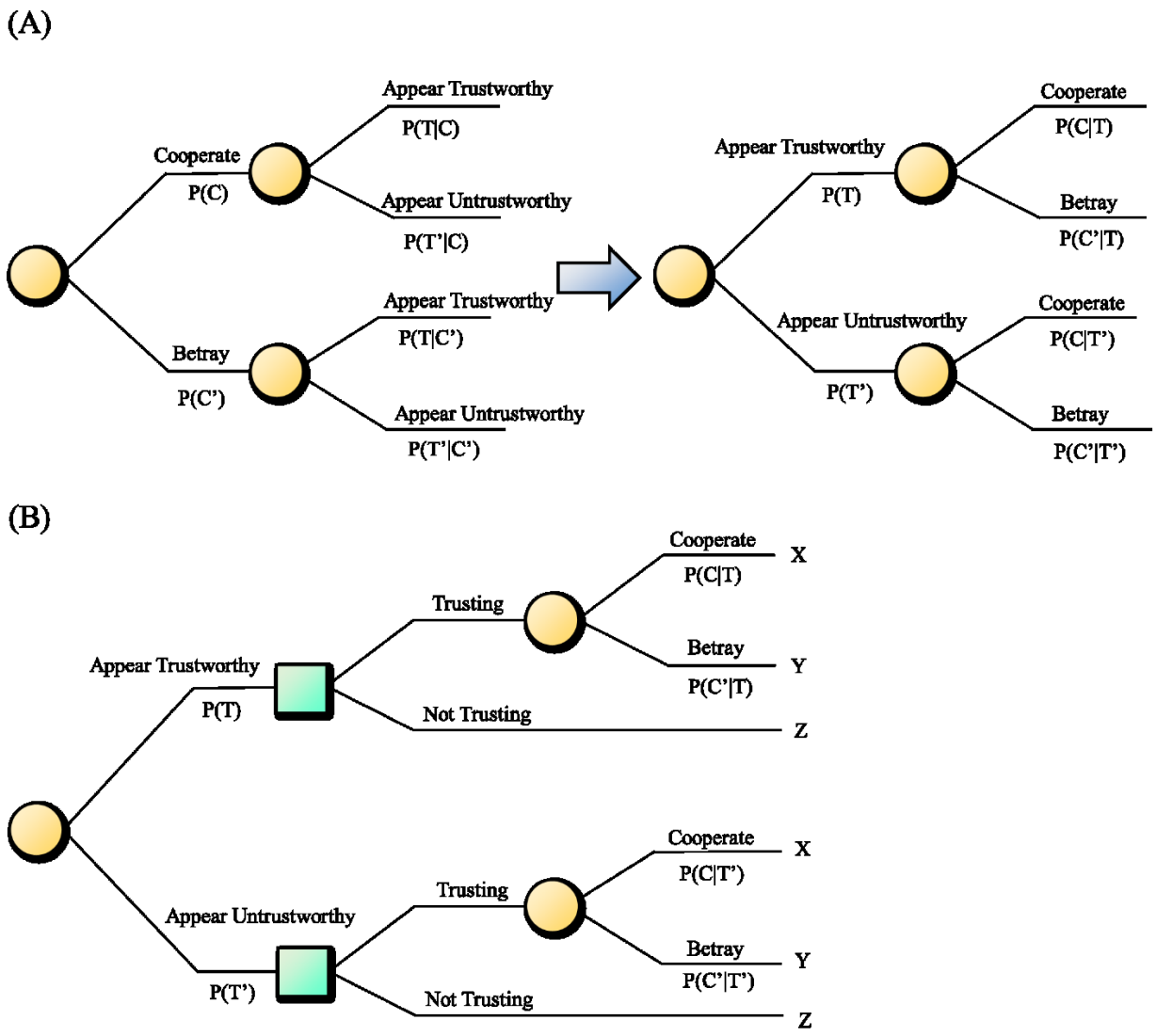

Figure 8: Trust Decision with Sample Information

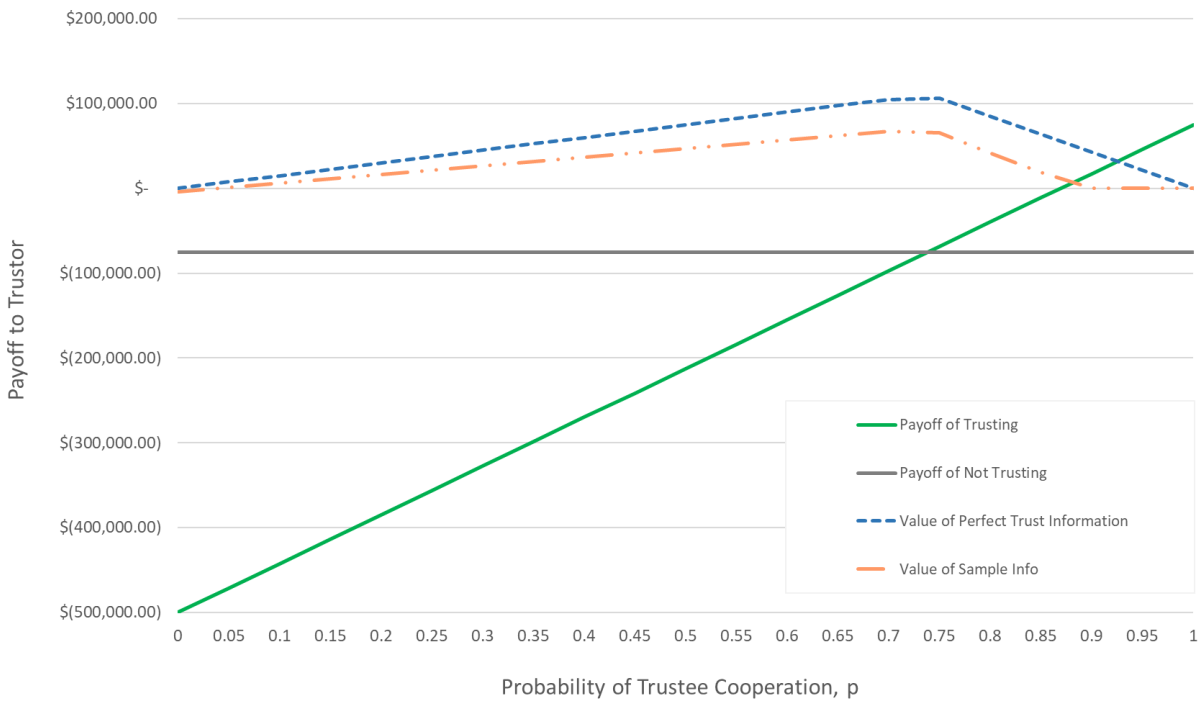

Figure 9: Payoffs and value of sample information associated with the trust decision

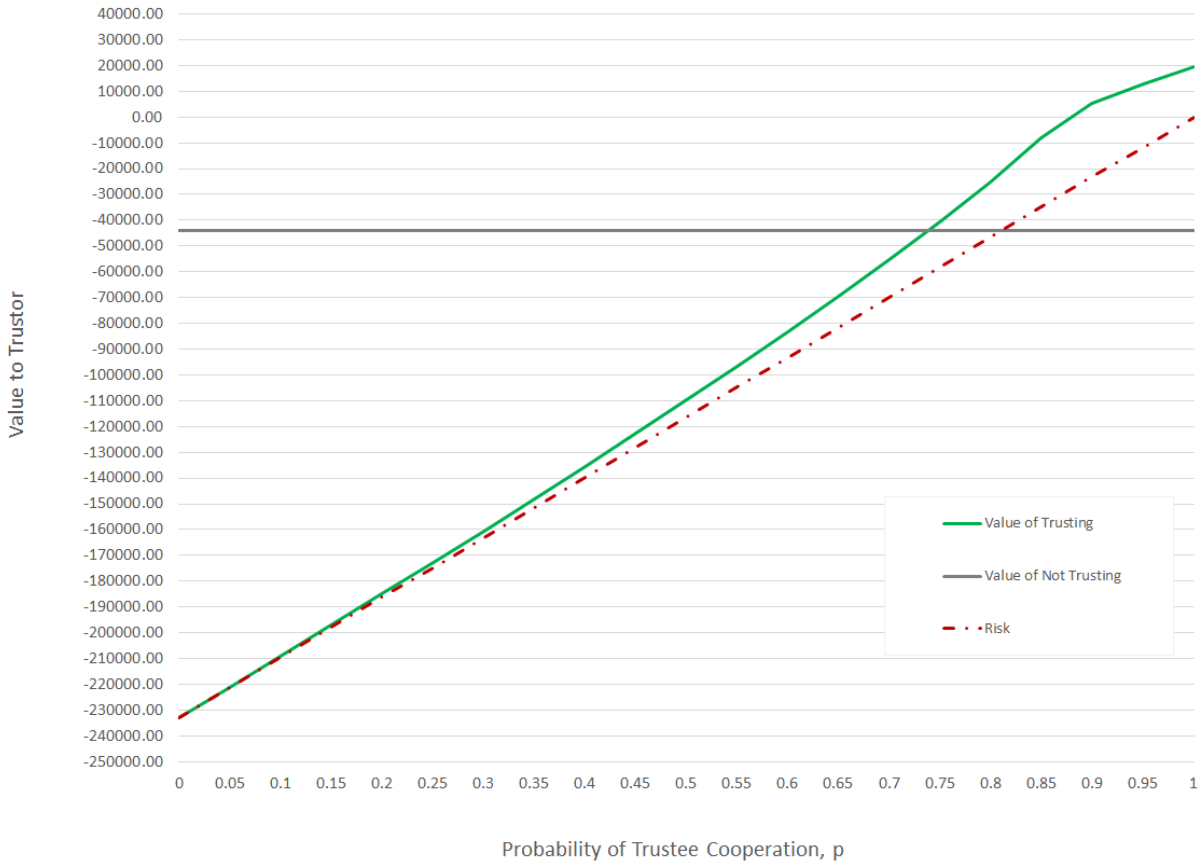

Figure 10: Value function associated with trust decision when accounting for loss aversion