Zero Trust for Hardware Supply Chains: Challenges in Application of Zero Trust Principles to Hardware

White Paper

Electronics Division
October 2021

A discussion of the Zero Trust and Quantifiable Assurance concepts as related to microelectronics to promote broader dialog on the complexities facing the Defense Industrial Base regarding these controversial topics.

[This Page Intentionally Blank]

Foreword

This white paper facilitates a broader understanding of Zero Trust and the challenges for application to hardware and supply chain assurance. Its purpose is to facilitate a high-level understanding of zero trust principles, to foster necessary dialog for understanding what it will take to apply these principles to the microelectronics domain, including the need to demonstrate and prove techniques, prior to implementing specific guidance in acquisition policy. The Zero Trust security model was originally designed as an assurance framework for information technology systems (i.e., networks). It has emerged as a strategy in the electronic hardware domain to manage the risk of counterfeiting, malicious modification and exploitation anywhere in the supply chain. The core design principle of Zero Trust is that no component or actor in the system should be assumed to be trusted by default or in isolation, which results in a focus on verification, detection, and response. In this paper, we discuss what "Zero Trust" means in the context of hardware and supply chain assurance, and systems engineering.

Assurance of microelectronics hardware and its attendant supply chain present significant challenges and difficulties in the application of Zero Trust principles. Zero Trust does not mean that there is no trust in the system. Rather Zero Trust is a set of principles about how to make risk-based decisions to grant limited access and integration in a system based on continuous monitoring and layered security. This requires a methodology and economic motivation to quantify assurance through risk-based assessments and controls that drive design, manufacturing, testing, maintenance and sustainment, and the requisite supply chain decisions. The implementation of Zero Trust for hardware assurance will require a clear understanding of the challenges involved and significant investment and incentive structures to motivate the robust application and adoption of quantifiable assurance. This paper shows the need by industry and government across the entire supply chain, from design to manufacturing to test to system integration to operations and maintenance to disposal. While some argue that Zero Trust is essential based on the rapidly increasing threat landscape and evolution of manufacturing capacity, Zero Trust is not a binary solution, but rather, one potential tool in a range of security solutions.

Paper Disposition

This paper will be made available on the National Defense Industrial Association website as a reference resource: https://www.ndia.org/divisions/electronics/resources. Permission is granted to widely distribute and quote this paper with proper attribution.

Principal Authors

Below is a list of the principal authors of this paper:

Daniel DiMase, President and CEO, Aerocyonics, Inc.
Zachary A. Collier, Assistant Professor, Dept. of Management, Radford University
Jeremy Muldavin, DMTS Program Management, GlobalFoundries
John A. Chandy, Professor, Dept. of Electrical and Computer Engineering, University of Connecticut
Donald Davidson, Director, Cyber-SCRM Programs, Synopsys
Derek Doran, Director of Research and Development, Tenet3, LLC
Ujjwal Guin, Assistant Professor, Dept. of Electrical and Computer Engineering, Auburn University
John Hallman, Product Manager, OneSpin Solutions
Joel Heebink, Project Engineer, Aerocyonics, Inc.
Ezra Hall, Senior Director Aerospace and Defense Business Line, GlobalFoundries
Honorable Alan R. Shaffer, Member Board of Regents, Potomac Institute for Policy Studies

Members of the Electronics Division reviewed this paper prior to its publication. For more information about the Electronics Division, including a list of upcoming events, please visit NDIA.org/Divisions/Electronics.

Table of Contents

Executive Summary

Overview

Microelectronics are the foundation of our connected economy and infrastructure upon which our lives depend. Microelectronic hardware, and their supporting supply chains, face unprecedented security[1] risks that threaten national security, global commerce, and the continuity of our daily lives. The confidence (trust) that the components and system will behave as intended, free of defects and vulnerabilities, over the lifetime of the system is critical. Assurance strategies define the set of actions, evidence, and risk mitigation processes to ensure and demonstrate the confidence (trust) in a system to perform its mission. "Zero Trust" is a recent assurance strategy that aims to deliver more confidence (trust) in our microelectronics systems. Originating in the information technology (IT) security field, its analogous application to the hardware domain is immature and not completely applicable. Microelectronics supply chains differ from IT systems where many redundancies and pathways for delivering services are common. Properly aligned with existing measures to establish trust, assured availability[2] and access, clear definitions of Zero Trust principles for microelectronics can further strengthen our confidence in critical microelectronics and their supply chain. Confusion about, and improper implementation of Zero Trust, may lead to wasted resources, significant residual risks to our systems and supply chains, and a false sense of security that the hardware, and supply chains that deliver it, are protected.

Zero Trust - no implicit trust in any one component of a system, where trust is built through continual fine-grained multi-factor monitoring and authentication of the quantified risk[3] before access and integration to the larger system is permitted.

Major Findings

Zero Trust principles require the use of quantifiable assurance where evidence-based and risk-informed assessments of confidentiality, integrity, availability, provenance, and nonrepudiation (see Appendix 3 for definitions of these terms) are the basis for making access and integration decisions. The principles can be applied in the domains of hardware, firmware, software, systems, and systems of systems, as well as in the attendant global supply chain. Critical Zero Trust principles include:

- Assume the adversary is already in the system over its life cycle and its supply chain. The application of least-privileged access and continuous monitoring measures are able to increase and measure security[4] respectively.
- Apply layered security including the application of tools for observability, risk assessment, and control. Such tools may include those that provide fine-grained, multi-factor monitoring and authentication, observability, traceability, authentication, provenance, verification, and validation.
- Make risk-based decisions with trade-offs between costs and benefits tailored to system and organizational risk constraints.
- Economic and market forces are necessary to ensure adoption and proliferation across the supply chain.
- Provenance and traceability are necessary over the lifecycle to form assurance cases that the hardware remains secure and continues to function as intended.
- Multi-factor authentication should show that the article's origin is undisputed and tied to provenance to provide a risk-based assurance claim.
- Multi-factor monitoring should include a series of observations and checks to build provenance over a period of time based on the risk of the perceived threats.
- Apply the assurance process iteratively across the lifecycle with continuous monitoring to address the evolving threat(s).

Major Recommendations

We envision a future where Zero Trust as a concept is better understood as applied to hardware and the global distributed supply chain. It is important to remember that Zero Trust as applied to hardware and supply chains remains an unproven concept, and must be matured and validated before being broadly applied. Improved understanding leads to the selective deployment of Zero Trust principles as part of a greater suite of comprehensive assurance activities and market incentives (e.g. Trusted Foundry Accreditation, availability and capacity incentives, access contracts, Foreign Ownership, Control or Influence (FOCI) mitigations, Committee on Foreign Investment in the United States (CFIUS), etc.). Understanding and accounting for the limits of Zero Trust principles and implementation constraints is critical for effective assurance. Zero Trust can be researched and implemented along with current policies, protections, and accreditations for maintaining trusted supplier relationships and business models. Zero Trust principles of fine-grained, multi-factor continual authentication and monitoring of the microelectronics production and supply chain can deliver traceability and limit access to critical Intellectual Property (IP). Application to processing steps can further ensure that microelectronics hardware integrity, confidentiality, availability, and provenance can be quantifiably assured. We anticipate follow on implementation, studies, and/or playbooks.

Zero Trust may face challenges in implementation and adoption. Zero Trust, including fine-grained, multi-factor monitoring and authentication, and other activities across the lifecycle of microelectronics parts, could effectively guide risk-based investment and innovation in activities that contribute to supply chain security and trust. The global nature of the microelectronics supply chain makes properly understanding and implementing Zero Trust, as part of a set of risk-based, data-driven solutions, a critical imperative to secure the future economy and maintain U.S. leadership in all domains related to microelectronics.

The goal of this paper is to lay out a foundation for understanding Zero Trust concepts for hardware assurance and the production ecosystem, and to highlight the current gaps in implementation for hardware systems and their attendant supply chains. The challenges described in this paper apply to all microelectronic parts (e.g., ASICs, FPGAs, GPUs, CPUs). Quantifiiable hardware assurance is a framework for implementing and monitoring the Zero Trust security model for microelectronic hardware. The implementation of this framework will require a clear understanding of the challenges and significant investment and incentive structures to motivate robust application of quantifiable assurance and principles like Zero Trust. There are other ways to get to the same assurance state, and the cost and speed of implementation are critical factors when deciding which method to implement. Many assurance methods today place the burden on the designers and customers rather than the foundries and manufacturers to also create mitigations to also protect the devices and production environment. Zero Trust as it is proposed today is immature, with unknown costs of implementation and efficacy. Quantifiable assurance is an attempt to quantify risk to implement and monitor the Zero Trust security model. Adoption by industry and government, and integration with other proven and quantifiable assurance mitigations will be needed to build and maintain good cyber supply chain risk management (C-SCRM) strategies for both hardware and software assurance.

Section 1: Introduction

Section 1a: The Zero Trust Concept

There is a common adage that “driving is a privilege, not a right.” It illustrates the concept that before a parent hands over the car keys, a certain level of confidence (trust[5]) in the child must be established. Before access to the car can be granted, a baseline level of competence in driving must be established, authenticated by a valid driver’s license, and a number of confidence-building actions (assurance[6]) must be demonstrated by the child. Parents observe and build trust through activities like the child demonstrating responsibility through successfully completing a driver’s safety course and an accident- or citation-free history. Other behaviors like doing their homework, chores, showing up on time, and getting along with their siblings may be secondary indicators of trustworthiness. When a child breaks their parents’ trust, they typically get grounded from going out of a confined and controlled area (their room, the house, etc.) and are given limited access to their cell phone, computers, social networks, the car keys, etc. They are often closely watched, must report on their location and activities frequently, and so on, until the trust is re-established. These are not just punishments, designed to change the child's behavior or limit the damage of poor behavior. They are measured assurance observations and restrictions designed to help rebuild (assure) the parent’s confidence (trust) that their child is going to behave as expected and eventually restore the privileges (access) and roles within the family. The child earns trust and establishes the parents' confidence through monitored behavior until the child demonstrates the behavior that will result in authorization to drive again. Taking the keys away forever would make the family less efficient and ultimately destroy trust within the family. In this case, access to specific resources (i.e., car keys) is based on an assessment (at least in theory able to be calculated and quantified) that the trustee (i.e., the child) will behave in a way that is aligned with the interests of the family as a system. This view assumes that building trust within the system can enable the system to function smoothly and efficiently. This analogy demonstrates that monitoring every single behavior leads to inefficiencies that must be weighed against the risks.

The confidence (trust) that the components and system will behave as intended, free of defects and vulnerabilities, over the lifetime of the system is critical. Assurance is the set of actions, evidence, and risk mitigation processes to ensure and demonstrate the confidence (trust) in a system to perform its mission. A new assurance strategy has recently emerged for building trust in IT systems and is being explored for hardware and supply chain applications – “Zero Trust.”

We define Zero Trust as:

Zero Trust - no implicit trust in any one component of a system, where trust is built through continual fine-grained[7] multi-factor[8] monitoring and authentication[9] of the quantified risk before access[10] and integration to the larger system is permitted.

Zero Trust is an assurance strategy that aims to deliver measured confidence (trust) in our microelectronics systems. Originating in the information technology security field, its analogous application to the hardware domain has not yet been fully matured. Furthermore, the term Zero Trust is somewhat misleading, in that it might imply that trust is never granted within the system. As defined in Executive Order 14028:

> *“the term “Zero Trust Architecture” means a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. The*

Zero Trust security model eliminates implicit trust in any one element, node, or service and instead requires continuous verification of the operational picture via real-time information from multiple sources to determine access and other system responses. In essence, a Zero Trust Architecture allows users full access but only to the bare minimum they need to perform their jobs. If a device is compromised, zero trust can ensure that the damage is contained. The Zero Trust Architecture security model assumes that a breach is inevitable or has likely already occurred, so it constantly limits access to only what is needed and looks for anomalous or malicious activity. Zero Trust Architecture embeds comprehensive security monitoring; granular risk-based access controls; and system security automation in a coordinated manner throughout all aspects of the infrastructure in order to focus on protecting data in real-time within a dynamic threat environment. This data-centric security model allows the concept of least-privileged access to be applied for every access decision, where the answers to the questions of who, what, when, where, and how are critical for appropriately allowing or denying access to resources based on the combination of sever[ity and cost.]"

Zero Trust may thus be seen as a security posture that states that no implicit trust will be granted to any one person or component within a system or will grant access for any one component to all domains of the system. Starting from the assumption that all actors are untrustworthy by default, decisions to provide access are on a per-request basis with trust and access built through multi-factor, fine-grained, continual observation.

Zero Trust is an application of an observe, orient, decide, and act (OODA) loop (Boyd, 1995). How would Zero Trust apply to the example of child driving privileges? We *observe* the childs' behavior, define a set of rules and expected behaviours (*orient*), *decide* if they reached those goals to rebuild confidence, *act* to restrict or enable access when the behavior meets the thresholds, and then repeat the loop until, and even after, full confidence is re-established (Figure 1). Note, quantifiable assurance is not a "one and done" data collection effort. Less visibility into supply chains may mean more continuous diagnostics and mitigations (CDM) may be required. This goes hand-in-hand with the Zero Trust/Quantifiable Assurance concept - one gains (or loses) "trust" with more data, and risk can be mitigated through CDM, more compartmentalization and segmentation, and identification of critical dependencies.

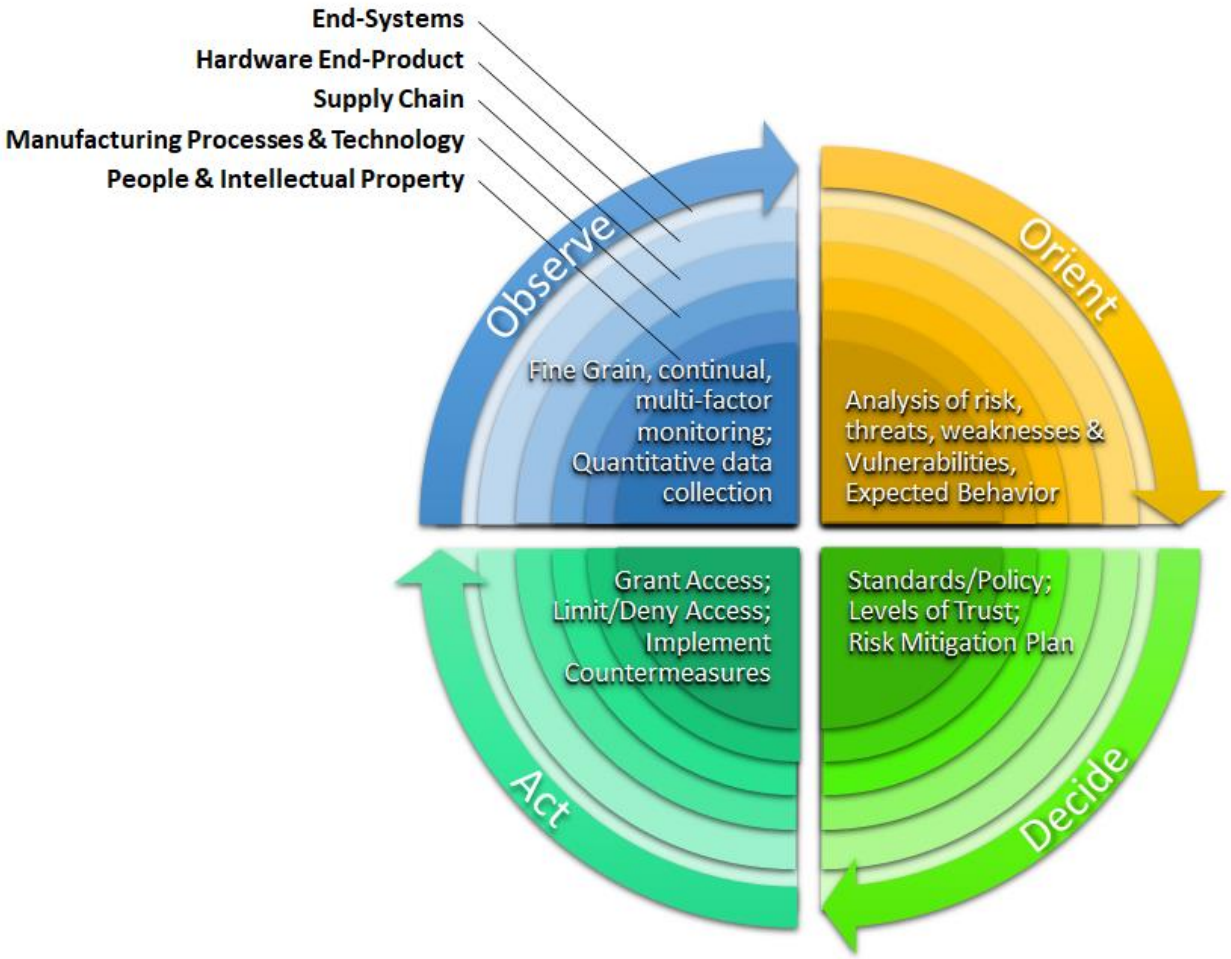

Figure 1: Zero Trust for Hardware Assurance

The rest of this paper will examine how this process may apply to building trust in our microelectronics hardware and supply chains through continual observation, orientation, decisions, and actions based on Zero Trust principles (as outlined in the executive summary).

Section 1b: Zero Trust for Hardware

The recent interest in Zero Trust for hardware and supply chains has been prompted by various technological, economic, geopolitical, and social trends. We rely upon technology in virtually every aspect of our modern lives - and this technology is grounded upon microelectronics and their supporting supply chain. Innovations that have transformed our society through mobile computing and connectivity are beginning to transform cyber-physical systems (self-driving cars, drones, autopilot systems, etc.) and critical infrastructure (banking, commerce, communication, automated trading, etc.). The ability to transform ideas into capabilities through microelectronics and it's supply chain faster, more efficiently, and with the highest performance and assurance in a domestic ecosystem is critical to leadership in national security and economic competitiveness. If the supply of microelectronics is exploited or shut off in terms of availability or access, modern life as we know it will be fundamentally impacted.

The global microelectronics supply chain, as a means to supporting our modern way of life, supports an array of functions across critical industry sectors such as communications, defense, healthcare,

transportation, the electric grid, and finance. Untrustworthy hardware components that are inserted into critical civilian and military systems across their lifecycle can result in compromised performance, safety risks, loss of sensitive data, and mission failure including loss of life (Figures 2 and 3). Supply chain attacks occur when an actor gains access to a critical asset or system somewhere within the system's chain of suppliers. For example, concerns over the trustworthiness of hardware components comprising 5G communications network infrastructure have already raised national security concerns (Donahue, 2020). While more of a software-related incident than hardware, the recent hack of the Oldsmar, Florida water treatment facility through a remote desktop application, resulting in dangerous levels of sodium hydroxide in the water supply, serves as a "wake up call" that modern supply chains include enormous attack surfaces, including third-party vendors such as software providers (Bezanson et al., 2021). "Half-Double" is an example of a hardware attack that flips the memory bits in certain varieties of dynamic random-access memory (DRAM) devices. By exploiting weaknesses in the microelectronics design, hackers can obtain higher kernel privileges on a targeted system that contains those DRAM devices (Paganini, 2021).

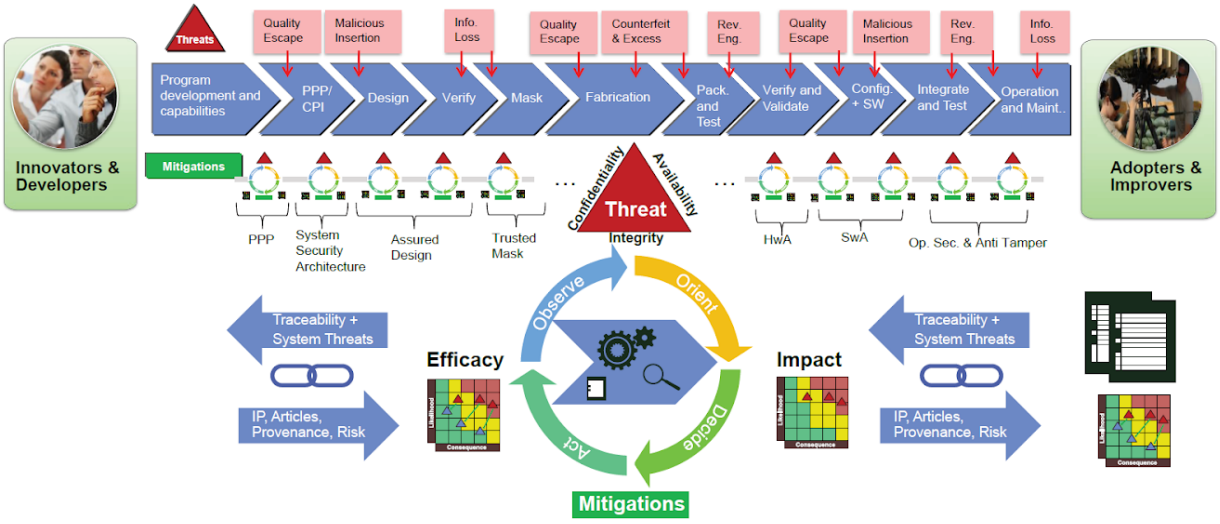

Figure 2: The Microelectronics Threat Landscape - An Enormous Attack Surface

As evidenced above, the things we take for granted, such as safe, clean water, and secure communications, can be compromised through hardware vulnerabilities.

There is an opportunity to develop systems with a higher trust in a domestic ecosystem, especially since US-based companies are subject to US laws and regulations. As shown in Figure 2, innovators and developers originate their ideas in the form of system requirements, intellectual property, and architectures. These are then transformed into integrated circuit designs and mask files where the billions of transistors and wires are written onto photo-lithographic masks. These masks contain the blue-print for the design, when coupled with the process design kit (PDK) and a production process recipe, allow the raw materials (silicon, gasses, metals, and rare-earth metals, etc.) to be transformed through thousands of steps performed in an automated flow through the world's most complicated production equipment. Each step takes the relevant recipe from the IP with the process design kit and adds or removes a feature to the starting materials to eventually produce the finished wafers, chips, circuit boards, assemblies, and software-enabled systems that deliver the capability intended by the original designers. At each stage there is an opportunity for an adversary or quality escape to compromise the product or production

capability. At each stage there is also an opportunity to observe, orient, decide, and act to assure confidentiality, availability, and integrity in the production process, supply chain, and products. Through this process, the threats and vulnerabilities are assessed to determine the risk of impact, and mitigations are selected to reduce the risk by deterring attacks and fixing vulnerabilities. The efficacy of the mitigations in reducing the risks of attack and minimizing the impact to production or product performance can be quantified through metrics. The assurance process is continual, with each stage feeding a risk profile to the next and back to the originators of the IP for continual improvement. Provenance and traceability associated with the articles and production processes can establish confidence in authenticity and integrity throughout the supply chain that is non-reputable. System risks and newly discovered vulnerabilities must be communicated across the critical elements of the supply chain, from end users to IP originators and the production and distribution ecosystem in between. The concept of the framework needs to be matured through industry standard work. The work needs to include risk-based perspectives through the verticals of the supply chain chevron and horizontally across the lifecycle, captured through traceability, non-repudiation, and provenance.

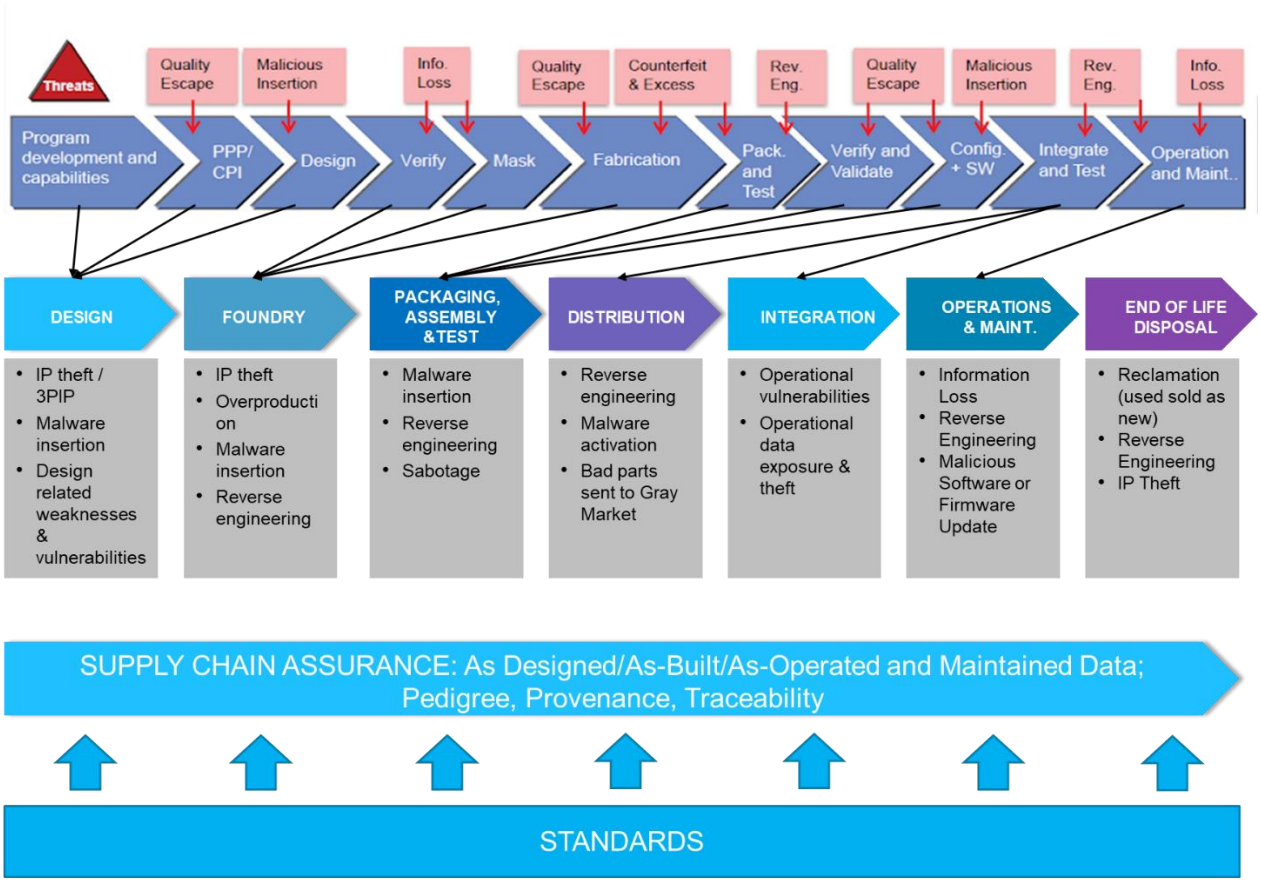

Figure 3: Threats associated with various life cycle stages

The problem of hardware trust is compounded by multiple factors, including its global nature, geopolitical issues, complexity, lack of transparency, and horizontal integration of the microelectronics supply chain (DiMase et al., 2016). Complicating the issue is the fact that malicious activity in microelectronics hardware or software is very difficult to detect, and can be left in a dormant state until activated. Ideally, one would always purchase components from trusted suppliers, but there is not an unlimited supply of these suppliers and the components they supply represent a small subset of the functions needed in a system. This means that risk tradeoffs must sometimes be made in acquisition decisions. Unfortunately,

"every part of the supply chain can be attacked" (Schneier, 2019), leading to a significant lack of trust in our hardware, systems, and production capability. Consequently, a risk-based approach must be adopted, where more "critical components" warrant more supply chain risk management (SCRM) and supply chain security (SCS) due diligence, and less critical components warrants accepting more risk.

Aside from the U.S. government and military, several industry sectors have a vested interest in securing the microelectronics supply chain:

- Automotive/Aerospace companies care about the integrity of their electronic parts, systems, and supply chains, and want to understand and evaluate the risks and mitigations around microelectronics integrity and supply, impacting quality, reliability, security, and safety (Brewster 2018; Careless 2019; Kumar 2018a; Solon 2016).
- The insurance industry is evaluating and underwriting risk from companies, including suppliers and integrators looking to be insured, and will benefit from fine-grained observability and other mitigations to minimize risk and financial exposure.
- Microelectronics manufacturers and their customers desire an assured supply of secure microelectronics.
- Designers of Analog & RF components such as microwave and mixed-signal, photonics, and biomedical microelectronics cannot use design and validation-only protections to ensure trust in their systems.
- Critical Infrastructure industries and organizations falling into any of the 16 critical infrastructure sectors, as defined by the US Cybersecurity and Infrastructure Safety Agency (2020), or adjacent industry sectors, are interested in the security of their hardware. These include water treatment and distribution, transportation networks including the highway system, communications networks (5G, 6G, …), energy distribution (electricity, fuel, ...), railways, pipelines, etc.
- In the healthcare industry, privacy of personal health data and safety are a critical concern to providers and definitely to the recipients of life-sustaining care.

Section 1c: A Common Understanding of Zero Trust for Hardware

The goal of this paper, as stated in the major recommendations, is to explore the applicability and gaps of Zero Trust concepts to solve the problem of hardware assurance. This is a priority to maintain our technology leadership, assure supply, and secure the systems that rely on microelectronics hardware to deliver the modern life and the economic infrastructure that is fueling our nation's current and future growth. The high stakes associated with security and trust in the microelectronics supply chain means that the cost of not taking action, and/or pursuing Zero Trust without a clear understanding of the requirements, is potentially significant. The original concept of Zero Trust is based upon the context of IT networks - highly distributed and redundant systems, whereas hardware (microelectronics) and supporting supply chains are structurally different (typically not distributed, redundant, or fungible), resulting in a murky analogy between the two domains. Confusion and a lack of consensus around the notion of Zero Trust will, ***at a minimum***, result in wasted money and the continued delivery of IT-enabled products and cyber-physical systems with unknown provenance and pedigree that result in unacceptable risk to their users and stakeholders. ***At the worst***, it will result in a supply dominated by our foreign adversaries, exposing the nation to a loss of technological leadership and putting the nation and its citizens at risk. The global nature of the microelectronics supply chain makes properly understanding and implementing Zero Trust as part of a set of risk-based, data-driven solutions a critical imperative to secure the future economy and maintain US and Allied leadership on the international stage.

The future we envision is one where Zero Trust as a concept is understood as it relates to hardware and the supply chain, and can be selectively deployed as part of a larger quantifiable assurance mitigation

and incentive toolset. This will ultimately involve ranges of risk mitigations, including the application of fine-grained, multi-factor monitoring and authentication, observability, traceability, provenance, verification and validation, applied across the lifecycle of microelectronics parts. The evidence offered by data collection under a quantifiable assurance methodology supporting Zero Trust can be used to promote assurance activities, robust systems, and supply chains. To support these goals, government policy, regulations, and industry standards should provide Zero Trust/quantifiable assurance for microelectronic parts from cradle to grave, and capture relevant information for assurance from the supply chains necessary to deliver them that are valued by both government, industry, and consumers alike.

Properly framed, Zero Trust can guide risk-based investment and innovation in activities that contribute to trust, including fine-grained, multi-factor monitoring and authentication, and other activities across the lifecycle of microelectronics parts that will improve security, safety, reliability, and quality of systems. Simply “putting up walls” around untrusted components limits the overall performance and trust in the system and supply chain. Similarly, you can't just lock your Intellectual Property (IP) inside the design. A synthesis and application of Zero Trust principles for hardware should be used to inform agreed-upon, commercially-acceptable global sourcing standards developed for IT products, services, and manufacturing capability, including criteria for measuring risk in systems, components, and sub-components - not just in information systems, but also IoT and cyber-physical systems (all IT-enabled capabilities). Acceptance and implementation of the concepts related to Zero Trust can inform both the demand side (e.g., users of products and systems who demand data/knowledge on the risk they are assuming in their ecosystem, based on products and services they are utilizing) and the supply side (e.g., developers/providers for both initial acquisition and life cycle sustainment who deliver products and services with some degree of trust/confidence).

Specifically, our main assertions are as follows:

1. Zero Trust is a potentially misleading term. Zero Trust does not mean that trust is never granted within the system or within the supply chain, but rather that no component or actor in the system or supply chain should be assumed to be trusted by default or in isolation, which results in a focus on verification, detection, and response. It involves a set of concepts related to granting privileged access to resources, using continuous monitoring to inform trust decisions.
2. The OODA (observe, orient, decide, act) loop can be a useful guiding framework for Zero Trust, helping connect observed data with potential risks and implementation of appropriate countermeasures. The OODA loop is a four-step repeating approach for decision making that focuses on monitoring and examining available information, putting it into a situational context, quickly selecting the appropriate course of action, and implementing the decision while also understanding that changes can be made as more data becomes available (See Figure 1).
3. Quantifiable Assurance is a more descriptive and informative term and forms the basis for Zero Trust implementations. It involves risk-based assessments of confidentiality, integrity, availability, and non-repudiation in the global supply chain, hardware, firmware, software, systems, and systems of systems. There are two main lines of evidence: documentation and the testing. One can validate and document the process or do exhaustive testing, and there are pros and cons to each approach.
4. A Zero Trust ecosystem applied to the semiconductor industry should assume that the adversaries and malicious insiders are already in the supply chain. Additional measures that include least privilege access and continuous monitoring can provide a layer of measurable security that is currently missing from today's supply chain. Asking suppliers to continually demonstrate that they are not stealing IP, over-producing, and faithfully producing microelectronics before giving them preferred access to critical markets is an example of least privilege access. These measures alone do not guarantee availability and access to production.

Policy and incentives must be combined with investments and protections of the microelectronics supply chain to enable availability and access and still prevent adversarial nation state-level intervention or natural disasters from significantly impacting critical supply.

5. Applying Zero Trust in practice requires making tradeoffs between costs and benefits within the system, and there must be systems-level optimization tailored to the specific applications and based on levels of risk (tolerance). Blindly applying Zero Trust to the global supply chain will result in a fragmented implementation, even with incentives and adoption by some suppliers and components. Zero Trust is not appropriate for everything and must be carefully applied alongside many other supply chain and hardware assurance actions. Section 2 explores the role of systems engineering in supporting design and supply chain tradeoffs.

The remainder of this paper lays out the theoretical foundations of Zero Trust as it can be applied to the microelectronics supply chain and sets forth an agenda for practical and theoretical research.

Section 2: Systems Engineering View of Zero Trust for Hardware

Recently, the idea of a Zero Trust strategy for hardware security and assurance has gained traction (e.g., Lopez, 2020; Paulsen, 2020). However, there has yet to emerge an agreed-upon definition for Zero Trust for hardware, and the methodology for measuring trust, assurance, and risk is not transparent in the hardware space. As mentioned earlier, the concepts and principles of Zero Trust for information systems do not neatly map onto the hardware supply chain, which includes design, manufacturing, test, procurement, distribution, integration into systems, and maintenance, throughout the entire life cycle and across many suppliers located in many world-wide locations. There is also a lack of established risk-based criteria to guide decision-making regarding what levels of trust and assurance are needed, how to define tiers of trust for parts and suppliers, and how to mitigate risk to agreed-upon acceptable levels. Furthermore, without both incentives and standards for efficient implementation by suppliers, successful business models for adoption will be fleeting and difficult to achieve broadly. Finally, the rapid automated response, quarantine, and remediation capabilities of IT software and incident response teams is difficult to replicate in a hardware supply chain. See Appendix 2 for more information about the origin of Zero Trust.

Hardware Assurance (HwA) quantifications must include the impact of the supply chain and cyber-supply chain risk management (C-SCRM) in mitigating vulnerabilities. Cybersecurity traditionally references the **"C-I-A Triad"**, which consists of **Confidentiality, Integrity,** and **Availability**. This traditional triad concept overly simplifies hardware security concerns, and we should consider adding **nonrepudiation**, **provenance**, **traceability**, and **pedigree** as areas to be addressed (See Appendix 3). For HwA of integrated circuits (ICs) and cyber-physical systems security (CPSS), the C-I-A Triad should also include provenance, traceability, and nonrepudiation of Intellectual Property (IP) mapped into the IC, starting with the design and different IP blocks[11], through fabrication, packaging, and integration into the end-use product/system in which the IP will be used. For each of the IP blocks, one should take a risk-based approach of evaluating critical program information and functionality against threats impacting the CIA Triad.

As systems become more complex through the integration of hardware, software, and firmware, a Systems Engineering view becomes increasingly more important to address the risks that could impact the system's security, reliability, quality, and safety. Hardware should be be perceived as a hard-wired path of execution logic performing instructions, often combined with analog, radio frequency, electro-optical, and other non-logic type input, output and/or functionality. Hardware is 'hard' coded (meaning it can't be changed after manufacturing), software is 'soft' (meaning we can more easily perform updates in the field), and firmware is 'firm' (in between hard and soft from an update perspective). If the hardware, software, or firmware is altered, then the desired system output will also be altered by the attack. Moreover, systems have many other performance attributes which must be considered, such as maintainability, repairability, flexibility, resilience, etc., and of course programmatic concerns such as budget and schedule. While the idea of absolute Zero Trust sounds appealing at first glance, locking the system down too much can have detrimental effects on the performance and cost. There is a complex, multi-dimensional tradespace between security and the other *"-ilities"* of the system. System designers and owners must make risk-informed trades.

Unfortunately, the complexity of systems and supply chains, coupled with a lack of supply chain visibility, results in systems which are so complex that we cannot fully understand them. To address these threats,

a balanced Systems Engineering approach that addresses the security of the system from a risk-based perspective is needed. The approach needs to start with the mission and business objectives of the system that observes, analyses, and quantifies the risk to the system that includes consideration of the lowest level of parts that will be incorporated into the system, and the systems operating environment. Increased diligence is required to better gain insights into the weaknesses and vulnerabilities in the system, because, you can't understand what you can't observe. Assurance measures need to include an assessment of the supply chain risk and other considerations such as hardware assurance, software assurance, systems engineering, and risk management.

Moreover, the tradeoffs are not just confined to the end system - but also involve the system of supply. This involves thinking about the lifecycle of the system and the microelectronics which enable the system to perform its intended functions, and the potential attacks that could occur across the lifecycle. Weaknesses and vulnerabilities originate at the component (and sub-component) level, which include concerns of the supply chain that could have an impact on the systems into which these components have been integrated. Today's modern microelectronic parts have become increasingly complex, with billions of transistors and core logic that in itself is considered a system-on-chip (SOC). The design, manufacturing, packaging, distribution, integration, maintenance, and even disposal of these SOCs all have points of attacks that could be exploited (see Figure 3). The supply chain of these SOCs is incredibly complex and spans a horizontal, global territory. The origin of these SOCs is Intellectual property (IP) which comprise these complex parts and the IP is designed by hundreds of engineers and multiple organizations spanning the globe. IP may be acquired on cloud platforms and integrated into the core of an SOC. Organizations utilizing the IP may not have access to the design information that is necessary to observe potential Trojans that could have been integrated into the design files. Beyond the design, a rogue actor or state-sponsored entity could carefully plan a variety of attacks intended to exploit weaknesses and vulnerabilities that impact the confidentiality, integrity, and/or availability of targeted systems and critical information. In addition, the longer a system is active in the field, more weaknesses and vulnerabilities are discovered that can be exploited, requiring continual monitoring to address newly discovered risks that require attention.

Hardware assurance and these domains of consideration can become quite complex. The SAE G-32 "Cyber Physical Systems Security Committee" sub-group for Hardware Assurance has been working to create standard work to address the HwA topic (Figure 4), and is focused on the microelectronic component level. A few observations to note from the ongoing work in the committee are:

- Security needs to be a consideration early in the design phase. It will be much less costly if security is built into the design on the front-end. Otherwise sustainment may cost more than designing new systems.
- Security is a moving target. Given enough time over a broad attack surface of the lifecycle of microelectronic parts integrated into systems, an adversary can find new weaknesses or vulnerabilities we haven't considered to exploit. Further, the threat surface is continually expanding. A "trusted" chip today may not be equally trusted tomorrow.
- Supply chain risk management is a major element in our HwA process. Attacks can occur anywhere in the supply chain.
- Systems Engineering and Systems Security Engineering needs to be included in the decision making. Mitigations to vulnerabilities are often system-specific and may require different disciplines to resolve. For instance, in one example, a NAS Drive for storage was impacted by Spectre. The resolution wasn't a recall to replace the microelectronic component impacting the system. The fix was a software patch that initially slowed the performance of the drive. A more sustainable solution that didn't impact the performance of the system was resolved through

another software patch to the operating system. This also emphasizes the point that engagement with a broader cross-functional team will be necessary to facilitate appropriate risk mitigation and decision making.

- Provenance, traceability, observability, and authentication will be needed to address potential issues in the field during operations and sustainment. Zero day[12] vulnerabilities are discovered every day. We will need appropriate tools to respond to those vulnerabilities on critical systems.
- Assurance must be quantified and valued by programs and markets if we are to be successful. Incentives based on data-driven quantitative risk are needed to motivate acquisition, suppliers, and consumer behavior.

While the topic appears complex, the work of the standards committees will help codify the appropriate actions necessary to address the unacceptable risk on our critical systems. Governments and markets must find ways to remunerate the value of the industry standards for sustained application of assurance and an assured supply chain.

Figure 4: SAE G32 Has Subcommittees Dedicated to Cyber Physical Systems Security and Engineering

One of the key questions related to hardware security and trust is: “Can we determine if something functions as intended and only as intended?”. Being able to answer this, and therefore to have trust in the components being used in critical systems, involves building and maintaining good cyber supply chain risk management strategies, including hardware assurance, software assurance, and assured services. A risk-based approach requires the ability to observe salient risk data, and use that to assess the risk to performance in terms of the C-I-A Triad (or C-A-I-N, where N stands for nonrepudiation). From there, one must make risk-informed trust decisions based on the criticality of the system, level of risk tolerance, and other relevant factors which inform the mitigations applied to the system to reduce the residual risk to an acceptable level. Open communications will be necessary with stakeholders to determine whether residual risk is acceptable given the mission requirements of the organization or program of record. Verifying that intended functions of microelectronics occur as intended is itself a significant industry challenge requiring many simulation and testing cycles. It is not possible to test ALL possible unintended

functions of microelectronic components that attackers may utilize or derive to compromise components or systems. Hence, trust (or Zero Trust) needs to be founded upon a predictive model based on assessed risk, observed trustworthiness, and level of risk tolerance to make investments in areas that will provide the most return (increased trust).

It is increasingly clear that more research into ways to measure, or quantify, the probability that a microelectronic component will operate as designed has to be a high priority to advance Zero Trust. This is true for all classes of microelectronics. Certainly, logic chips are easily understood. But the verification needs to extend to microelectronics like memory devices. Think of the havoc that could ensue if false data were injected into memory devices. Loss of "trust" in microelectronics compromises the entire system.

System security is not just about "not trusting anybody, ever" but instead is about establishing a quantifiable assurance case about whether, and to what extent, trust is granted to different entities, and risk mitigation actions occur based on measured data and assessment activities.

In December 2020, DoD published DODI 5000.90 specifying four risk tolerance (assurance levels) for cybersecurity risk tolerance in DoD weapon systems (DOD, 2020b), see Table A2 (in Appendix 4). Note that the takeaway is that mitigation decisions should be commensurate with the risk. Not only DoD, but also US Government and other enterprises like Critical Infrastructure (domestic and foreign) may want to consider adopting a similar Risk Tolerance/Assurance Level construct – enabling developers/providers to build assurance cases for the hardware (HW) & software (SW) components provided, and acquirers/users to develop assurance level requirements for their systems and consequently requirements/specifications for that system's embedded HW & SW components/subcomponents. We are unlikely to ever be able to fully verify or test our way out of this dilemma, which is why we need a risk-based process.

Consideration should also be given to the people/organizations in the design, development, manufacture and delivery supply chain, who touch the products' lifecycle and supply chain; what skills do they have, what is their past performance, what allegiances do they have (possible criminal elements and adversarial nation states) and what processes do they use (documented best practices, adherence to standards, and use of certifications).

All-in-all, in a Zero Trust environment, an organization has to pay careful attention to, and perform the necessary due diligence across the lifecycle of the parts and their supply chains. This includes determining the transparency of the supply chains, the efficacy of mitigations to address discovered weaknesses and vulnerabilities, sustainment of the assurance processes (this is not a find and fix one-time issue), and continued monitoring of ecosystems and the HW and SW that enable and support them. Monitoring supply chains alone is insufficient. Availability and access are not guaranteed by monitoring, and must be assured through investment, incentives, market forces, and national and international policies.

Taking a Zero Trust posture does not mean that an organization has to start from scratch – layering existing security measures can be a first step in the Zero Trust journey. Many technologies and approaches already exist for hardware security and trust which can be leveraged within an overarching Zero Trust philosophy. See Appendix 5 for examples of current practices and gaps.

However, no security strategy is 100% effective, and even trusted suppliers could become victims to sophisticated adversaries and criminal actors who have had time to evaluate means of exploiting weakness and vulnerabilities, and through supply chain attacks. A trusted supplier may even be a target

for adversaries. As a non-hardware analogy related to how a trusted supply chain partner could lead to downstream vulnerabilities, take for example the recent SolarWinds attack, where alleged Russian adversaries targeted a major software company that provides management tools for network and infrastructure monitoring to hundreds of thousands of organizations around the world. Malware installed in their software penetrated large parts of the U.S. Federal Government and numerous companies and their information technology systems. A Zero Trust security posture provides a better chance of fending off sophisticated attackers, when coupled with other layered defenses, such as a trusted supplier program. Appendix 6 explores the role of trusted suppliers within a Zero Trust framework.

Zero Trust is not a one-size-fits-all solution, and does not preclude the need for maintaining a monitored and trusted supply base.

Section 3: Enabling Quantifiable Assurance

Fine-grained systems monitoring and risk-based decision making are important aspects of the Zero Trust concept. SMEs need tools that minimize sources of bias, and synthesize system facts and observations, into quantitative tools. The systems engineering view of Zero Trust motivates *data-driven, quantitative* tools for this purpose. This is because a Systems Engineering view hierarchically decomposes a system's complex structure to understand how the lowest level parts of a system are related to higher level capabilities or process steps. This view, put simply, captures all of the constituent parts or entities of a system (at whatever level of resolution is desired), how they are related to each other, and how they collectively compose larger components. The entities, their associations and compositions constitute *facts* about what a system is and does that can be stored in a *knowledge base*. Knowledge bases can then be analyzed algorithmically and quantitatively. Entities, relations, and components in the system knowledge base can be endowed with metadata describing its properties (enhancing knowledge about system components) and even datasets of measurements, unstructured documents, and other observational data.

The knowledge-base of a system captures a "common operating picture" that analysts can reference and agree upon as a single source of facts about the system. This enables evaluators to make recommendations based on encoded, queryable facts (i.e. that can be queried) to assess Zero Trust constructs in a system. This quantitative, algorithmic approach significantly reduces individual biases present in a qualitative analysis of whether a system satisfies Zero Trust principles sufficiently. Metrics over this knowledge base further establish a common definition of what aspects of a system are "important", and how multiple system properties should be integrated to evaluate some aspect of assurance. While the interpretation of the metric may vary among SMEs, it at least is an interpretation based on a common base of system facts and data that codify assurance aspects.

All assurance metrics should be developed from a knowledge base of system facts and data observations. One example of a knowledge base may be a digital thread of a system, captured as:

> *"The Digital Thread concept, conceived in the lab in 2007 and increasingly permeating industry, is a technological framework that helps organize data across the lifespan of a product--from initial design to manufacturing, operation and maintenance -- interconnecting data, modeling, and analysis to enable better decisions at all product life stages. It's a new way of organizing the traditional "paper trail" of data typical of each phase of the acquisition process and is revolutionizing the way engineers think about design, manufacturing, supply chains and sustainment, moving to model-centric processes and beyond."* (Alia-Novobilski, 2017)

The digital thread is defined by an NDIA 2017 White Paper:

> *"The digital thread is the set of digitally created, stored and exchanged information that supports the manufacturing and sustainment processes of modern products. The digital thread exists throughout the product lifecycle."* (NDIA, 2017)

The digital thread of a system for data-driven quantifiable assurance must capture *knowledge* about the system *as designed, as built*, and *as operated and maintained*. *As-designed* knowledge captures information about the process, assumptions, intended components, and actors involved in the development of the system. Such knowledge is fundamental for assessing the basic assurance of a system: a low-assurance design will never yield a high-assurance system. *As built* captures knowledge

about the completed, factual construction of a system. There are inevitable deviations between its design and its construction, whether intentional or otherwise, and capturing the system *as built* affords an opportunity to compare. *As-built* models form the baseline knowledge base for data driven, practical quantifiable assurance analysis. Finally, *as-operated and maintained* models incorporate knowledge about the actors, environment, and conditions of the system's operation.

Armed with knowledge encoded about a system and associated datasets, models quantifying an aspect of assurance can be developed. A knowledge metric is a quantity inferred directly by facts in the knowledge base. Such a metric can be as simple as a frequency count of how much is known (the number of facts) about a system entity, or a measure of information completeness (of all entities expected to have some fact). Knowledge metrics can even be based on types of knowledge captured. For example, knowledge about the protocols and inbound/outbound traffic flows along a digital communication line between components, leading to a quantitative profile of the most reliant protocols on which the system relies, may be indicative of its susceptibilities.

The design space of quantitative models for assurance is large. Model development should start by understanding how "assurance" is interpreted for a system. One understanding may relate assurance to reliability, in the sense that a system is operating with assurance if all its constituent components are operating with assurance. Models and methods from systems reliability theory can then relate component-wise assurance (reliability) to total system assurance. Another understanding may consider assurance to be associated with system behaviors that are both consistent and expected. Then knowledge metrics and system data can be monitored over time, and statistical anomaly detection methods could identify deviations from expectation, and hence the transition of a system into low assurance states. No matter the modeling approach however, it is important to consider the fact that assurance about a system is never definitive or certain; to suggest otherwise would mean there is complete trust in a system to operate as expected. Quantitative models therefore need to provide not only a single assurance assessment "value", but a likely range of values with some probability. A model that emits a probability density function over the range of assurance scores (e.g., 0 to 1), for example can be used to compute a band of scores the true assurance of the system falls within some confidence (e.g., 95% probability).

The systems engineering view of Zero Trust motivates data-driven, quantitative tools for the purpose of making a quantifiable assurance case.

Concluding Comments: Vision for the Future of Trust

Zero Trust for hardware assurance means there is no implicit trust in any one component of a system, where trust is built through continual fine-grained, multi-factor monitoring and authentication and quantified risk before access and integration into the larger system is permitted. The problem of extending Zero Trust principles to hardware and it's supply chain requires a call to action emphasizing solutions using a holistic, risk-based Systems Engineering perspective and market incentives to supply the necessary transformation of IP into hardware systems. The solution should include developing a common lexicon of terms and metrics for assessing weaknesses and vulnerabilities and areas of concern with the goal of more robust and resilient systems that include assured microelectronics and their supply chain.

The problem of availability and access to microelectronics will not be resolved through design for security alone, especially when supply for microelectronics hardware is currently centralized in Asia. This geographic centralization can lead to supply disruptions due to natural disasters or adversarial nation state peer conflict. Incentives to diversify and develop the supply chain can address risk of these types of disruptions, and can also provide sourcing alternatives that reduce reliance on suppliers that may be easy targets for cyber criminals or adversarial nation state actors who have the advantage of time to study systems, supply chains, and components to identify weaknesses and discover latent vulnerabilities they can and will exploit.

Standardization and implementation of market-based incentives is needed to codify the cyber physical systems security framework and hardware assurance practices that provide requirements and guidance for implementation in a scalable manner. The path for designing standardized metrics for effectiveness should include a risk-based mindset across the life-cycle and supply chain that are tied to market incentives and business cases for suppliers to enable access. The incentives and market access should motivate observability and controls across the attack surface to limit cyber criminals and adversarial nation state actors' influence on the complex, global supply chains.

Policy makers, regulators, and standards development organizations will need to provide standards and incentives that encourage appropriate action and participation from suppliers. Incentives should encourage more domestic and allied country manufacturing of microelectronics for not only defense applications, but also to secure our nation's critical infrastructure including 5G/6G. Government contracting officers and program managers should have criteria and requirements for awarding contracts and purchase orders that consider program and product criticality and supply chain risk. Quantifiable metrics of assurance and security will be needed to provide a common understanding (standard) that could be meaningful to government, industry, and consumers alike when they are making acquisition decisions that could impact their privacy, safety, and security.

Therefore, collaboration and incentives are proposed that includes government, industry, and academia recognizing a need for action in developing a risk-based systems security engineering approach. Standardization of cyber physical systems security and hardware assurance is a necessary step toward characterizing the risk. We hope this paper provides a vision and shared understanding to put the nation on a path toward more secure and trustworthy systems.

Endnotes

1. Security (n): Quality or state of being secure: freedom from danger, freedom from anxiety, freedom from loss of information, materials, financial value, or capability.

2. Availability: Existence or usability of an item or capability.

3. Quantified Risk: Measures of authenticity, provenance, traceability, observability, validation and verification, availability, access control, affordability, implementation costs, and functional performance, etc., that result in mission goals such as confidentiality, integrity, and availability.

4. Security (v): Measures taken to guard against espionage, sabotage, crime, attack, or escape.

5. Trust: The confidence that the components and system will behave as intended, free of defects and vulnerabilities, over the lifetime of the system.

5a. “The confidence one element has in another, that the second element will behave as expected”. (NIST SP 800-161)

5b. “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.” (DoD AT&L Memorandum)

5c. “The terms ‘‘trust’’ and ‘‘trusted’’ refer, with respect to microelectronics, to the ability of the Department of Defense to have confidence that the microelectronics function as intended and are free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system at any time during its life cycle.” (NDAA FY2017, Sec. 231)

6. Assurance: Actions, evidence, and risk mitigation processes to ensure and demonstrate the confidence (trust) in a system to perform its mission.

6a. “Grounds for justified confidence that a claim has been or will be achieved. Note 1: Assurance is typically obtained relative to a set of specific claims. The scope and focus of such claims may vary (e.g., security claims, safety claims) and the claims themselves may be interrelated. Note 2: Assurance is obtained through techniques and methods that generate credible evidence to substantiate claims.” (NIST SP 800-160 Vol. 1; ISO/IEC 15026)

6b. “Assuance Case: A reasoned, auditable artifact created that supports the contention that its top-level claim (or set of claims), is satisfied, including systematic argumentation and its underlying evidence and explicit assumptions that support the claim(s).” (NIST SP 800-160 Vol. 1 from ISO/IEC 15026)

7. Fine-grained: detailed analysis resulting in data elements, which may include temporal, spatial features.

8. Multi-factor: A characteristic of an authentication or monitoring system that requires more than one distinct factor (multiple temporal and spatial variables or measurements) for successful authentication and monitoring. Multi-factor authentication can be performed using a single authenticator that provides more

than one factor or by a combination of authenticators that provide different factors. The three authentication factors are something you know, something you have, and something you are.

9. Authentication: Verifying the genuine property, undisputed origin, or identity of a user, process, or device, often as a prerequisite to allowing access to resources.

10. Access: The right or opportunity to use or benefit from something.

11. IP blocks, or IP cores, are “discrete design units that can be incorporated in individual chip designs”. They are “discrete functional unit[s] of an integrated circuit”. Examples include designs for microprocessor cores, embedded memory, USB implementation, or Ethernet connectivity. The practice of licensing ready-made IP blocks is done to reduce development time and costs (Greenbaum, 2011)

12. A Zero-Day is a vulnerability discovered that may not have a mitigation. Until the vulnerability is mitigated, criminal hackers or adversaries could exploit the vulnerability to adversely affect programs, data, or impacted systems. The term “zero-day” refers to the number of days a new vulnerability is discovered, and the number of days an organization has to mitigate the disclosed vulnerability.

References

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

Alia-Novobilski, M. (2017). Digital Thread laces decision-making, data for Air Force acquisition. Wright Patterson Air Force Base. https://www.wpafb.af.mil/News/Article-Display/Article/1087681/digital-thread-laces-decision-making-data-for-air-force-acquisition/

Asadizanjani, N., Tehranipoor, M., & Forte, D. (2017). Counterfeit electronics detection using image processing and machine learning. In *Journal of physics: conference series* (Vol. 787, No. 1, p. 012023). IOP Publishing.

Banga, M., & Hsiao, M. S. (2011, June). Odette: A non-scan design-for-test methodology for trojan detection in ics. In *2011 IEEE International Symposium on Hardware-Oriented Security and Trust* (pp. 18-23). IEEE.

Beck, P., Hofmann, E., & Stölzle, W. (2012). One size does not fit all: An approach for differentiated supply chain management. *International Journal of Services Sciences*, *4*(3-4), 213-239.

Becker, G. T., Regazzoni, F., Paar, C., & Burleson, W. P. (2013, August). Stealthy dopant-level hardware trojans. In *International Conference on Cryptographic Hardware and Embedded Systems* (pp. 197-214). Springer, Berlin, Heidelberg.

Bezanson, P.J., Morgan, V.E., Springer, D., Cahoon, C.E. (2021). Florida Water System Hack Highlights Challenges for Public Utility Cybersecurity. *The National Law Review*, https://www.natlawreview.com/article/florida-water-system-hack-highlights-challenges-public-utility-cybersecurity

Boyd, J.R. (1995). The Essence of Winning and Losing, A five slide set by John R. Boyd. https://danford.net/boyd/essence.htm

Brewster, T. (2018). This guy hacked hundreds of planes from the ground. *Forbes*, https://www.forbes.com/sites/thomasbrewster/2018/08/09/this-guy-hacked-hundreds-of-planes-from-the-ground/#6d8d323046f2

Bu, L., & Kinsy, M. A. (2018, May). Hardening AES Hardware Implementations Against Fault and Error Inject Attacks. In *Proceedings of the 2018 on Great Lakes Symposium on VLSI* (pp. 499-502).

Careless, J. (2019) Putting the CAN Bus Hack into Context. *AIN Online*, https://www.ainonline.com/aviation-news/general-aviation/2019-08-28/putting-can-bus-hack-context

Čisar, P., & Čisar, S. M. (2016, November). The framework of runtime application self-protection technology. In *2016 IEEE 17th International Symposium on Computational Intelligence and Informatics (CINTI)* (pp. 000081-000086). IEEE.

Collier, Z. A., & Sarkis, J. (2021). The zero trust supply chain: Managing supply chain risk in the absence of trust. *International Journal of Production Research*, 59(11), 3430-3445.

Crawford, A., Dillard, J., Fouquet, H., Reynolds, I. (2021). The World is Dangerously Dependent on Taiwan for Semiconductors. *Bloomberg*, https://www.bloomberg.com/news/features/2021-01-25/the-world-is-dangerously-dependent-on-taiwan-for-semiconductors

Cui, A., Chang, C. H., Tahar, S., & 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*, *30*(5), 678-690.

Daniel, B. (2020). Counterfeit Electronic Parts: A Multibillion-Dollar Black Market. Trenton Systems Blog, https://www.trentonsystems.com/blog/counterfeit-electronic-parts

Das, D., Danial, J., Golder, A., Ghosh, S., Wdhury, A. R., & Sen, S. (2020, March). Deep learning side-channel attack resilient AES-256 using current domain signature attenuation in 65nm CMOS. In *2020 IEEE Custom Integrated Circuits Conference (CICC)* (pp. 1-4). IEEE.

DiMase, D., Collier, Z. A., Carlson, J., Gray Jr, R. B., & Linkov, I. (2016). Traceability and risk analysis strategies for addressing counterfeit electronics in supply chains for complex systems. *Risk Analysis*, *36*(10), 1834-1843.

DMEA (2021). Trusted Foundry Program. https://www.dmea.osd.mil/TrustedIC.aspx

DOD (2020a). DODI 5000.02T: Operation of the Defense Acquisition System. US Department of Defense. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500002tp.PDF?ver=6KTtyfGjzLqbnGyWBNDnAQ%3d%3d

DOD (2020b). DODI 5000.90: Cybersecurity for Acquisition Decision Authorities and Program Managers. US Department of Defense. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500090p.PDF?ver=MIG3uLnzXl31QcvXJTZ5uA%3D%3D

Donahue, T. (2019). The Worst Possible Day: U.S. Telecommunications and Huawei. *PRISM*, *8*(3), 14-35.

Doulcier-Verdier, M., Dutertre, J. M., Fournier, J., Rigaud, J. B., Robisson, B., & Tria, A. (2011, February). A side-channel and fault-attack resistant AES circuit working on duplicated complemented values. In *2011 IEEE International Solid-State Circuits Conference* (pp. 274-276). IEEE.

Gartner (2021). IT Glossary. Runtime Application Self-Protection (RASP). https://www.gartner.com/en/information-technology/glossary/runtime-application-self-protection-rasp

Gentner, D. (1983). Structure-mapping: A theoretical framework for analogy. *Cognitive Science*, *7*(2), 155-170.

Goodin, D. (2015). Cutting-Edge Hack Gives Super User Status by Exploiting DRAM Weakness. *Ars Technica*, https://arstechnica.com/information-technology/2015/03/cutting-edge-hack-gives-super-user-status-by-exploiting-dram-weakness/

Gordin, I., Graur, A., & Potorac, A. (2019, October). Two-factor authentication framework for private cloud. In *2019 23rd International Conference on System Theory, Control and Computing (ICSTCC)* (pp. 255-259). IEEE.

Greenbaum, E. (2011). Open source semiconductor core licensing. *Harvard Journal of Law & Technology*, *25*(1), 131-157.

Guin, U., Wang, W., Harper, C., & Singh, A. D. (2019, May). Detecting recycled socs by exploiting aging induced biases in memory cells. In *2019 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)* (pp. 72-80). IEEE.

Guin, U., DiMase, D., & Tehranipoor, M. (2014). Counterfeit integrated circuits: Detection, avoidance, and the challenges ahead. *Journal of Electronic Testing*, *30*(1), 9-23.

Guin, U., Huang, K., DiMase, D., Carulli, J. M., Tehranipoor, M., & Makris, Y. (2014). Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain. *Proceedings of the IEEE*, *102*(8), 1207-1228.

Humphries, M. (2021). Chipmakers Asked to Reduce Usage as Taiwan Prepares for Serious Water Shortages. *PC Magazine*, https://uk.pcmag.com/processors/131899/chipmakers-asked-to-reduce-usage-as-taiwan-prepares-for-serious-water-shortages

ISO (2018). ISO 26262-1:2018. Road Vehicles - Functional Safety - Part 1: Vocabulary. https://www.iso.org/standard/68383.html

ISO/IEC (2018). ISO/IEC 20243-1:2018. Information technology — Open Trusted Technology ProviderTM Standard (O-TTPS) — Mitigating maliciously tainted and counterfeit products — Part 1: Requirements and recommendations. https://www.iso.org/standard/74399.html

ISO/IEC (2013). ISO/IEC 27036-3:2013. Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for information and communication technology supply chain security. https://www.iso.org/standard/59688.html

ISO/IEC (2011). ISO/IEC 15026-2:2011. Systems and Software Engineering - Systems and Software Assurance - Part 2: Assurance Case. https://www.iso.org/standard/52926.html

ISO/IEC/IEEE (2015). ISO/IEC/IEEE 15288:2015. Systems and Software Engineering - System Life Cycle Processes. https://www.iso.org/standard/63711.html

Jain, A., Zhou, Z., & Guin, U. (2021). TAAL: tampering attack on any key-based logic locked circuits. *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, *26*(4), 1-22.

Kim, T. H., Persaud, R., & Kim, C. H. (2008). Silicon odometer: An on-chip reliability monitor for measuring frequency degradation of digital circuits. *IEEE Journal of Solid-State Circuits*, *43*(4), 874-880.

Kim, C. H., & Quisquater, J. J. (2007). Faults, injection methods, and fault attacks. *IEEE Design & Test of Computers*, *24*(6), 544-545.

Kim, Y., Daly, R., Kim, J., Fallin, C., Lee, J. H., Lee, D., et al. (2014). Flipping bits in memory without accessing them: An experimental study of DRAM disturbance errors. *ACM SIGARCH Computer Architecture News*, *42*(3), 361-372.

Kindervag, J. (2011). Applying Zero Trust to the Extended Enterprise: Preparing Your Network for Any Device, Anywhere, Any Time. Cambridge, MA: Forrester Research, Inc.

Kindervag, J. (2010a). Build Security into Your Network's DNA: The Zero Trust Network Architecture. Cambridge, MA: Forrester Research, Inc.

Kindervag, J. (2010b). No More Chewy Centers: Introducing the Zero Trust Model of Information Security. Cambridge, MA: Forrester Research, Inc.

Kumar, M. (2018a). Chinese Hackers Find Over a Dozen Vulnerabilities in BMW Cars. *The Hacker News*, https://thehackernews.com/2018/05/bmw-smart-car-hacking.html

Kumar, M. (2018b). New Rowhammer Attack Can Hijack Computers Remotely Over the Network. *The Hacker News*, https://thehackernews.com/2018/05/rowhammer-attack-exploit.html

Lapedus, M. (2020). China Speeds Up Advanced Chip Development. *Semiconductor Engineering,* https://semiengineering.com/china-speeds-up-advanced-chip-development/

Li, Y., Hatano, R., Tada, S., Matsuda, K., Miura, N., Sugawara, T., & Sakiyama, K. (2019, December). Side-channel leakage of alarm signal for a bulk-current-based laser sensor. In *International Conference on Information Security and Cryptology* (pp. 346-361). Springer, Cham.

Li, M., Shamsi, K., Meade, T., Zhao, Z., Yu, B., Jin, Y., & Pan, D. Z. (2017). Provably secure camouflaging strategy for IC protection. *IEEE transactions on computer-aided design of integrated circuits and systems*, *38*(8), 1399-1412.

Livingston, H. (2007). Avoiding counterfeit electronic components. *IEEE Transactions on Components and Packaging Technologies*, *30*(1), 187-189.

Lopez, C.T. (2020). DOD Adopts Zero Trust Approach to Buying Microelectronics. *DOD News*, https://www.defense.gov/Explore/News/Article/Article/2192120/in-microelectronics-dod-moves-from-trusted-foundry-model-to-zero-trust/

Luszcz, J. (2018). Apache Struts 2: how technical and development gaps caused the Equifax Breach. *Network Security*, *2018*(1), 5-8.

Matsuda, K., Fujii, T., Shoji, N., Sugawara, T., Sakiyama, K., Hayashi, Y. I., ... & Miura, N. (2018). A 286 f 2/cell distributed bulk-current sensor and secure flush code eraser against laser fault injection attack on cryptographic processor. *IEEE Journal of Solid-State Circuits*, *53*(11), 3174-3182.

Matsuda, K., Miura, N., Nagata, M., Hayashi, Y. I., Fujii, T., & Sakiyama, K. (2016, December). On-chip substrate-bounce monitoring for laser-fault countermeasure. In *2016 IEEE Asian Hardware-Oriented Security and Trust (AsianHOST)* (pp. 1-6). IEEE.

Microsoft Security Response Center (2020). Customer Guidance on Recent Nation-State Cyber Attacks. Microsoft Security Response Center. https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/

NDIA. (2017). Cybersecurity for Manufacturing Networks. A white paper prepared by NDIA Cybersecurity for Advanced Manufacturing Joint Working Group (CFAM JWG). https://www.ndia.org/-/media/sites/ndia/divisions/working-groups/cfam/ndia-cfam-2017-white-paper-20171023.ashx?la=en

NIST. (2021). Key Practices in Cyber Supply Chain Risk Management: Observations from Industry. NISTR 8276. Gaithersburg, MD: National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8276.pdf

NIST. (2020a). Zero Trust Architecture. NIST Special Publication 800-207. Gaithersburg, MD: National Institute of Standards and Technology. https://csrc.nist.gov/publications/detail/sp/800-207/final

NIST. (2020b). Security and Privacy Controls for Information Systems and Organizations. NIST Special Publication 800-53, Revision 5. Gaithersburg, MD: National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

NIST. (2020c). Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. NIST Special Publication 800-171. Gaithersburg, MD: National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

NIST. (2018). Risk Management Framework for Information Systems and Organizations. NIST Special Publication 800-37, Revision 2. Gaithersburg, MD: National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

NIST. (2015). Supply Chain Risk Management Practices for Federal Information Systems and Organizations. NIST Special Publication 800-161. Gaithersburg, MD: National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf

Paganini, P. (2021). Google discovered a new variant of Rowhammer attack dubbed Half-Double. *Security Affairs*, https://securityaffairs.co/wordpress/118284/hacking/rowhammer-variant-dubbed-half-double.html

Paulsen, C. (2020). The Future of IT Operational Technology Supply Chains. *Computer*, *53*(1), 30-36.

Pierson, D., Yun, M. (2020). The most important company you've never heard of is being dragged into the U.S.-China rivalry. *Los Angeles Times*, https://www.latimes.com/world-nation/story/2020-12-17/taiwan-chips-tsmc-china-us

Prouff, E., Rivain, M., & Bevan, R. (2009). Statistical analysis of second order differential power analysis. *IEEE Transactions on computers*, *58*(6), 799-811.

Quadir, S. E., Chen, J., Forte, D., Asadizanjani, N., Shahbazmohamadi, S., Wang, L., et al. (2016). A survey on chip to system reverse engineering. *ACM journal on emerging technologies in computing systems (JETC)*, *13*(1), 1-34.

Rahman, M. T., Tajik, S., Rahman, M. S., Tehranipoor, M., & Asadizanjani, N. (2020, December). The key is left under the mat: On the inappropriate security assumption of logic locking schemes. In *2020 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)* (pp. 262-272). IEEE.

Robertson, J., & Riley, M. (2018). The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies. *Bloomberg Businessweek*: https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

SAE. (2016). Test Methods Standard; General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts. https://saemobilus.sae.org/content/as6171

Schneier, B. (2019). Every Part of the Supply Chain Can be Attacked. *New York Times*, https://www.nytimes.com/2019/09/25/opinion/huawei-internet-security.html

Schramm, K., & Paar, C. (2006, February). Higher order masking of the AES. In *Cryptographers' track at the RSA conference* (pp. 208-225). Springer, Berlin, Heidelberg.

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

Semiconductor Industry Association. (2021). Broad Coalition of Tech, Medical, Auto, Other Business Leaders Urge President Biden to Fund Domestic Semiconductor Manufacturing, Research in Infrastructure Plan. https://www.semiconductors.org/broad-coalition-of-tech-medical-auto-other-business-leaders-urge-president-biden-to-fund-domestic-semiconductor-manufacturing-research-in-infrastructure-plan/

Simchi-Levi, D., Clayton, A., & Raven, B. (2013). When one size does not fit all. *MIT Sloan Management Review*, *54*(2), 15.

Smith, B. (2020). A moment of reckoning: the need for a strong and global cybersecurity response. *Microsoft On the Issues Blog*, https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/

Solon, O. (2016). Team of Hackers Take Remote Control of Tesla Model S from 12 Miles Away. *The Guardian*, https://www.theguardian.com/technology/2016/sep/20/tesla-model-s-chinese-hack-remote-control-brakes

Stern, A., Mehta, D., Tajik, S., Guin, U., Farahmandi, F., & Tehranipoor, M. (2020, December). SPARTA-COTS: A Laser Probing Approach for Sequential Trojan Detection in COTS Integrated Circuits. In *2020 IEEE Physical Assurance and Inspection of Electronics (PAINE)* (pp. 1-6). IEEE.

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

Sugawara, T., Shoji, N., Sakiyama, K., Matsuda, K., Miura, N., & Nagata, M. (2019). Side-channel leakage from sensor-based countermeasures against fault injection attack. *Microelectronics Journal*, *90*, 63-71.

Tehranipoor, M. M., Guin, U., & Forte, D. (2015). Counterfeit integrated circuits. In *Counterfeit Integrated Circuits* (pp. 15-36). Springer, Cham.

The Jericho Forum. (2007). Jericho Forum Commandments, version 1.2. Available at: https://collaboration.opengroup.org/jericho/commandments_v1.2.pdf

Thompson, K. (1983). Reflections on trusting trust. *Communications of the ACM*, 27(8), 781-783.

Tiri, K., & Verbauwhede, I. (2004, February). A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation. In *Proceedings Design, Automation and Test in Europe Conference and Exhibition* (Vol. 1, pp. 246-251). IEEE.

US Cybersecurity and Infrastructure Safety Agency. (2020). Critical Infrastructure Sectors. https://www.cisa.gov/critical-infrastructure-sectors

Vaidyanathan, K., Liu, R., Sumbul, E., Zhu, Q., Franchetti, F., & Pileggi, L. (2014, May). 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). IEEE.

Wang, P., & Johnson, C. (2018). Cybersecurity incident handling: a case study of the Equifax data breach. *Issues in Information Systems*, *19*(3).

Wickens, K. (2021). World-Leading Chip Makers TSMC Threatened by Taiwan Water Crisis. *PC Gamer,* https://www.pcgamer.com/tsmc-threatened-by-taiwan-water-crisis/

Yang, Y., Chen, Z., Liu, Y., Ho, T. Y., Jin, Y., & Zhou, P. (2020). How Secure Is Split Manufacturing in Preventing Hardware Trojan?. *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, *25*(2), 1-23.

Zetter, K. (2016). Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. *Wired*, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

Zhang, Y., Jain, A., Cui, P., Zhou, Z., & Guin, U. (2020). A novel topology-guided attack and its countermeasure towards secure logic locking. *Journal of Cryptographic Engineering*, 1-14.

Zhou, Z., Guin, U., & Agrawal, V. D. (2018, April). Modeling and test generation for combinational hardware Trojans. In *2018 IEEE 36th VLSI Test Symposium (VTS)* (pp. 1-6). IEEE.

Appendix 1: Developing the Right Strategy

The move to a quantifiable assurance model for trust is not insignificant. As such, various options, some interim, are likely to be used depending on the nature of the supply chain and risk tolerance involved. Below are three examples of options, some elements of which may be in place today. Options on the spectrum of trusted assurance include Government Owned, Commercially Operated (GOCO) with trust principles, an expanded trusted supplier program, and purely quantifiable assurance with commercial industry (see Table A1). Each of these must solve availability, access, and assurance of the supply chain, and each has advantages and disadvantages. Any of these options, by themselves, may not meet the DoD goals for procured systems and hardware and long-term US goals for a robust, expanding onshore microelectronics ecosystem. Quantifiable assurance must be coupled with availability, access contracts, and market incentives to be successful. Government, industry, and academia will need to continute to support and fund the initiatives under DARPA, NSF, NIST, DOE, and other programs to continue to advance the capabilities and capacity of these options.

Table A1: Comparisons of Trust Strategies

<table>
<tr><th colspan="2">Option 1: Government Owned, Commercially Operated Split Fab (GOCO)</th></tr>
<tr><td rowspan="2">Government Owned, Commercially Operated, trusted design, split fab back-end production and packaging. Customers work with just one or two microelectronics designers and fabricators, and buy some critical microelectronics circuits (ASIC and FPGA) through these organizations. Could be useful for research and development capture into production.

Recommendations:
Ensure that a business and value proposition is well established
Push towards majority commercial operations to achieve volume and therefore yield
Encourage government embedment and research capture and transition</td><td>Advantages
Can address design, split-fab manufacturing, & packaging in a trusted/classified environment
Focus on a few key technologies and products with one or two suppliers
R&D capture into a production environment could be implemented
Could be used as leverage to benchmark/prototype for other options</td></tr>
<tr><td>Disadvantages
Limited scalability and recovery options due limited supplier choice, IP choice, production capacity, etc.
Doesn’t achieve self sustaining business case, resulting in annual high cost to implement and maintain (especially true for state-of-the-art lithography)
Only addresses a small subset of critical (ASIC, FPGA, GOTS) parts at increased costs. Does not address COTS parts without participation from large commercial customers
Only addresses sponsoring customer requirements, consumer markets unprotected (electrical grid, IoT, medical, appliances, 5/6G, autonomous vehicles, etc.)
Limited technology refresh, requires continual reinvestment
Can’t do modifications (e.g. RAD-Hard) on front-end due to split-fab</td></tr>
</table>

<table>
<tr><td colspan="2">Option 2: Trusted Supplier</td></tr>
<tr><td rowspan="2">Major customers continue using the existing model and procure microelectronics/integrated circuits (ASIC) to the greatest extent possible from “trusted suppliers” certified and approved through that customer’s approach for “trusted suppliers” or the government’s Trusted Access Program Office (TAPO) for fabricating integrated circuits.

Recommendations:
Continued support by USG
Adopt quantifiable assurance option 3 to strengthen and expand Trusted supplier services
Accelerate use and expand offered processes currently available
Develop improved guidebooks for program managers and contracting officers for appropriate use of Trusted suppliers</td><td>Advantages
Existing approach already implemented and can leverage assurances from Option 3
Satisfies ITAR/EAR requirements and is used for production of critical defense systems
Guaranteed access and preferred supply for USG (DPAS, etc.)</td></tr>
<tr><td>Disadvantages
Additional costs over pure commercial access
Limited number of suppliers
Limited standards, policy, enforcement, or incentives for the use of trusted suppliers and parts in USG systems and commercial systems</td></tr>
<tr><td colspan="2">Option 3: Quantifiable Assurance</td></tr>
<tr><td>Joint Government/DoD/industry effort to implement comprehensive, risk-based, quantifiable microelectronics supply chain hardware assurance (HwA) and cyber physical system security (CPSS) mechanisms and protocols to protect all categories of microelectronics/integrated circuits (ASIC, FPGA, COTS, etc.) such that safe/protected dual-use microelectronics are available and market incentives for domestic production tied to assurance for both DoD and consumer use.

Recommendations:
Continue efforts to update/develop applicable industry and government standards to implement comprehensive, risk-based, quantifiable microelectronics supply chain HwA and CPSS mechanisms and protocols to achieve safe and fully protected dual-use microelectronics of every category (ASIC, FPGA, COTS, etc.)</td><td>Advantages
Addresses all categories of microelectronics/integrated circuits (ASIC, FPGA, COTS, RF, analog, optoelectronic, etc.)
Addresses design through manufacture through integration into a system, across entire lifecycle (cradle to grave)
Addresses government/DoD/critical infrastructure and consumer markets
Infrastructure and automated processes in the development and testing of microelectronics to support many quantifiable assurance mechanisms already exist
Quantifiable assurance can be tied to incentives & market access to build domestic capability
Adds layers of defense for preventing HwA and CPSS attacks and damage
Quantifiable metrics could be relevant government/industry/consumers alike</td></tr>
</table>

• Quantifiable Assurance complements the current Trusted Supplier program and may provide access to fab, vendors, and services that are currently not accredited. • Provide means and measures of vetting suppliers including an evaluation of the security architecture within the supplier's facilities (e.g., CMMC). • Advocate for dedicated programs to develop and validate near-term quantifiable assurance solutions utilizing existing data infrastructure and processes, as well as longer term innovations to advance the state of the art.	Disadvantages • Greatest effort required to accomplish • Requires significant standards development/update • Requires supply chain top to bottom implementation from willing industry partners • Requires broad commercial, government, and academic support • Requires transparent disclosure of vulnerabilities and TTPs between mutually trusted government and industry partners

Better identification and reporting of weaknesses and vulnerabilities in hardware are needed. History has proven that industry and the lawyers that advise them are resistant to reporting problems they think will incriminate themselves or harm market reputation. However, researchers in academia are publishing new articles every day that identify novel weaknesses and vulnerabilities. Databases and reporting tools, such as the ITU-T Cybersecurity Information Exchange (CYBEX) 1500 Series Weaknesses and Vulnerabilities Database, will need to establish a cadence to troll for new research publications and identify new findings from bug bounty hunters, and quickly capture them in the database so that industry and government can take appropriate mitigating actions when warranted. The concepts of liability transfer from the insurance industry and well-tuned market incentives could motivate more reporting. Mandatory reporting and protection of those who report could also help reduce the current stigma of "blaming the victim".

Full post-deployment security lifecycle management must be adopted. The truism "Attacks only get better" applies to hardware just as equally as software and the IT infrastructure. Systems must be designed with identification, detection, response, and remediation functions for the inevitability that attackers will innovate and latent vulnerabilities will be discovered and exploited after hardware has been created and deployed.

Research and development in the verification science of hardware assurance is needed to mature the readiness and efficacy of risk calculations across the lifecycle and supply chain. Cost-effective methods that identify the weaknesses and vulnerabilities of microelectronic parts are needed as well. The cost and efficacy of attacks versus the cost and efficacy of solutions needs to be studied and carefully considered in our framework. The node size of microelectronic parts continues to shrink, with work already in development for 1 to 3 nanometers, which is near atom size (a typical atom is 0.1 to 0.5 nanometers). Packaging is also becoming more complex with the introduction of 2.5D, 3D, and interposer technology. With advancement in science in microelectronics, new tools and methods will be necessary to conduct the analysis.

Solutions are immediately needed to address the unacceptable risk of threats to hardware that impact system security, safety, reliability, and quality. There is a need for industry standards that are applicable to multiple sectors, with a focus on the critical infrastructure. There is no need to reinvent the wheel. Solutions should leverage existing best practices and standards with a focus on closing identified gaps. A holistic approach that integrates existing practices that are effective toward resolving the problem is needed. We should leverage existing programs, such as the DMEA Trusted Supplier Program to address risk in the supply chain and to guarantee access to trusted microelectronics within our ecosystem for our

most critical systems while the science of risk calculation for microelectronics matures. Investments by and in the Trusted Supplier Program should be capitalized upon with careful risk analysis and layering of evolving approaches to this network of US and allied Nation suppliers. Outreach and training to provide awareness of the issue will be an important factor to engage the sectors that may not be aware of the severity of the threat or the needed sense of urgency to take action. Sectors such as Aerospace & Defense, Automotive, Industrial Control Systems, Medical Devices, Industrial Internet of Things (IIoT), Energy, Communication, and Banking and Finance are just a few sectors that should have grave concern, where the cost of inaction could have a significant and grave national security impact to defense and commerce.

The problem won't be resolved in a silo and there are no silver bullets. Hardware Assurance requires cross-functional support beyond component engineers to properly identify threats and unacceptable risks that impact the systems into which the parts are integrated, design for response and remediation, and to properly take action to mitigate concerns. Functions such as systems engineering, systems security engineering, and software engineering need to be integrated into the decision making to manage the risk. Organizationally, the engineering functions and security functions must interface with the business functions, including supply chain and operations management, insurance/risk management, and C-suite executives. Other Stakeholders, such as integrators, end-users, suppliers, and customers will also need to be included in relevant risk-analysis and decision-making conversations.

Therefore, collaboration is proposed that includes government, industry, and academia recognizing a need for action in developing a risk-based systems security engineering approach to standardization of cyber physical systems security and hardware assurance, including the following:

- **Characterize Risk:** of the Cyber-Physical System (CPS), assess weaknesses and vulnerabilities of the system and the supply chain and recommend mitigating actions.
    - Develop technologies that provide transparency for provenance and traceability of hardware that is interoperable across the entire supply chain to address and quantify risk, while protecting intellectual property and supply chain integrity.
    - Advance the knowledge of how weaknesses and vulnerabilities are introduced and exploited in cyber physical systems and in microelectronic products and services and supply chains.
    - Research and develop quantified metrics for HwA. A semi-quantitative approach that includes quantitative and qualitative measures may be necessary due to the complexity of matter.
- **Systems Engineering Approach:** Identify best practices for addressing different areas of concern, utilizing existing processes, procedures, and standards when possible.
    - Close gaps in Hardware and Software Assurance (HwA/SwA) and integrate a holistic approach through the Cyber Physical System Security (CPSS) Systems Engineering Effort.
    - Develop cost-effective design and evaluation methods for mitigation of risk in cyber physical systems security design and HwA that includes assessing effectiveness of solutions, and improvements to the verification science of integrated circuits.
    - Develop a detailed taxonomy for CPSS that includes HwA and supply chain assurance.
    - Integrate a whole-system lifecycle approach to hardware security to include resiliency and recovery planning.

- **Standardize & Incentivize:** for identifying weaknesses and vulnerabilities in cyber physical systems and microelectronics products and services that could be introduced at any point in the CPS life cycle.
    - Standardize a systems engineering approach to address cyber physical systems security and HwA with a goal of designing resilient systems that can survive an attack.
    - Individuals responsible for implementation will need training. This includes awareness training for executives and policy makers, and procedural training for cross-functional team members who need to perform their job in accordance with the new normal.
    - USG and industry incentives to deliver observability, risk reporting, and supply chain risk management for critical infrastructure (5-6G, automotive, energy, etc.) and the hardware upon which they rely.
    - Assure availability and access to microelectronics through targeted incentives, contractual agreements, capability and capacity building, and alignment of USG and commercial market-based forces.

Appendix 2: Origins of Zero Trust

The concept of Zero Trust was originally developed in the IT security research literature, motivated by concerns that it was becoming increasingly difficult to protect the perimeter of an information system from malicious attacks and intrusions (Kindervag 2010a, 2010b, 2011; The Jericho Forum, 2004). With the advent of the cloud and as borders of the IT systems became less clear, it became almost impossible to decide which users should be granted trusted access to the various IT assets and resources (Kindervag, 2011). The prevailing notion of trusted and untrusted networks was supplanted by the idea of Zero Trust, where "in zero trust, all network traffic is untrusted" (Kindervag, 2010a). The US National Institute of Standards and Technology (NIST) provided guidance in NIST Special Publication 800-207, "Zero Trust Architecture", providing the following working definitions:

> *"Zero trust (ZT) provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised. Zero trust architecture (ZTA) is an enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a zero trust architecture plan."* (NIST, 2020)

The key element of a Zero Trust strategy is that, instead of focusing on keeping attackers out of the network, we assume that an attacker is already present on the IT network and the focus is on limiting the attacker's ability to move inside the system. The effort then shifts to figuring out how to grant access to users on a per-request basis (NIST, 2020). Zero Trust is not a technology but rather a set of concepts and principles which form a new philosophy for thinking about trust. Kindervag (2010a) lays out three key elements of this new philosophy: first, information systems administrators need to assume that all network traffic poses a threat until it has been authorized and secured; second, a least-privilege strategy should be enforced for those granted network access; and third, all network traffic should be inspected and logged in real-time. Thus, Zero Trust serves as a set of guiding principles for making trust-based, data-driven authentication and authorization decisions.

However, this understanding of Zero Trust is based upon the context of IT networks - highly distributed and redundant systems. Applying the principles of Zero Trust to the microelectronics supply chain is an entirely different story. Instead of highly distributed and redundant systems, there may only be a small number of suppliers - and therefore concerns about the availability of supply are more relevant. For example, current water shortages in Taiwan, where many chips are manufactured, have caused reservoirs to fall below 20% of their capacity, and as a result, chipmakers have been asked to scale back production (Humphries, 2021).

Correctly applying the concepts of Zero Trust to microelectronics will therefore involve, not a simple one-to-one mapping of concepts, but rather *reasoning by analogy*, in which the principles and tenets are adapted from one domain to another (Gentner, 1983). Concepts and implementations, and the structural relationships between them, may need to be abstracted, broadened, or otherwise adapted for the context of hardware. There is risk involved in not mapping concepts appropriately - an incomplete or inappropriate mapping of concepts may be worse than no mapping at all.

Appendix 3: C-I-A Triad Examples for Hardware and Other Relevant Concepts

Protecting **confidentiality** in HwA is dependent on being able to define and enforce certain access levels of information and data. Sensitive information and data may need to be organized by who needs access and the need to protect the information and data from unauthorized access. Information that may need to be protected could include design data or data from the use of the device that is proprietary or subject to Export Administration Rules (EAR) and/or International Trafficking in Arms Regulations (ITAR) and/or Classified. ITAR is a United States regulatory requirement to restrict and control the export of defense and military-related technologies to safeguard U.S. national security and further U.S. foreign policy objectives. An example of critical data used by a device could be a missile system with critical flight data that a device uses to navigate the missile. IP blocks within the device may also need confidentiality protection. An example could be the controls of a radar system used for a defense program. Organizations outside of defense consider their design data and information proprietary, needing protection. Additional information, such as individuals performing work in the supply chain may need to be protected due to privacy concerns. Files may be encrypted to protect the information, both in transit and at rest. Entities with access to confidential information and data will need the appropriate controls to protect the information, and to manage and mitigate threats from bad actors seeking access at any point in the supply chain throughout the lifecycle of the part. Bad actors can greatly reduce the time to successful exploits with access to confidential information. To better understand the concept, *Bloomberg Businessweek* reported an example of a state sponsored attack on confidentiality accomplished through the insertion of a tiny microchip, not much bigger than a grain of rice, that was not part of the boards' original design (Robertson & Riley, 2018). According to the article, investigators determined that the chips allowed the attackers to create a stealth doorway into any network that included the altered machines. Multiple people familiar with the matter say investigators found that the chips had been inserted at factories run by manufacturing subcontractors in China. Although there are multiple areas in the supply chain that a bad actor could exploit a vulnerability to alter the integrity of the device or the data which the device utilizes, this example highlights that additional assurance measures may be appropriate based on the provenance of the device and the user's risk tolerance level.

Integrity is an essential component of the CIA Triad that is intended to ensure that the design and the data being used by the device are free of modification and known vulnerabilities that could alter the functionality of the device or modify or delete the data which the device utilizes to perform its intended function. Today's microelectronic devices typically contain billions of transistors that construct a complex system-on-chip architecture. The device could contain hardware Trojans meant to perform similar attacks to the one which *Bloomberg Businessweek* published. The attack on the City of Oldsmar, Florida water treatment facility is a good example of an attack on integrity. The attack increased the amount of chemicals used to treat the water that could have made the water poisonous. If the attack were successful, it could have resulted in a potential disaster, particularly with the region hosting visitors for Super Bowl LV at the time of the attack. The integrity of the water supply would have been impacted if the anomaly was not spotted by an operator at the plant. An example of an attack on integrity for an integrated circuit was demonstrated through a paper published by researchers at UMass Amherst. The paper demonstrated how a gate of the original design was modified by applying a different dopant polarity to specific parts of the gate's active areas to remove the functionality of the random number generator that empowers encryption of the IC. Through this approach, the attacker is able to predict the output of the random number generator to get the key in order to break the encryption, thereby impacting the

integrity of the device (Becker et al., 2013). This example also demonstrates an attack on confidentiality of data thought to be encrypted by the device.

Counterfeiting of ICs also impacts integrity. According to SAE AS6171 *Test Methods Standard; General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts* (EEE), there are seven counterfeit part types: recycled, remarked, overproduced, out-of-specification/defective, cloned, forged documentation/part substitution, and tampered. Integration of any one of these types of counterfeit EEE parts could impact the mission or business objectives, as end-product organizations face the challenge of ensuring the quality, reliability, safety, and security of products purchased from suppliers throughout the world and at all levels within the supply chain. When a counterfeit product is integrated into a system, one cannot make predictions about product integrity since nothing is known about the counterfeit product. Counterfeiting has become prevalent and has significant financial impact on the organizations who have invested in the development of their intellectual property. According to the Semiconductor Industry Association (SIA), counterfeit electronics parts cost manufacturers more than $7.5 billion annually and translates into nearly 11,000 lost jobs just in the United States alone (Daniel, 2020). There is also an impact to organizations that is not fully captured in these estimates, for example, the cost of remediation and reputation. Extreme effort, expense, and often destructive testing are necessary to provide with a high confidence that a part is authentic. Without provenance and traceability, no amount of testing can 100% authenticate a part. Testing can only provide a hypothesis that there was no evidence of defects found associated with counterfeit products. The persistent threat of counterfeiting only proves that supply chain integrity matters, and brand owners will need to be diligent in overseeing their supply chain and protecting their brand.

An example of an attack on the confidentiality and integrity of data processed on integrated circuits is demonstrated through the rowhammer security exploit. This attack changes the state of the memory cells (from “0” to “1” or vice versa) impacting the availability and integrity of the data (Kim et al., 2014). The rowhammer attack has also been used in some privilege escalation security exploits to gain access to network resources that were otherwise unavailable (Kumar, 2018b; Goodin, 2015).

Availability is the final component of the C-I-A Triad that refers to the availability of the device or the data needed for the device. Availability includes access to design data and manufacturing of the device, which could be interrupted for various reasons. C-SCRM is essential to mitigate the threats posed to availability. Denial of service is an example of an availability attack. An example of denial of service includes the December 2015 cyberattack on the Ukraine power grid, which temporarily disrupted the electricity supply to consumers. Availability also relates to physical access to product and material within the supply chain. The coronavirus pandemic revealed the reliance for supplies from countries like China, such as on personal protective equipment. The global semiconductor manufacturing capacity in the U.S. has decreased from 37 percent in 1990 to 12 percent today. This decline is largely due to substantial subsidies offered by the governments of our global competitors, which have put the U.S. at a competitive disadvantage for new fabrication construction (Semiconductor Industry Association, 2021). China is backed by their government with over $150 billion in funding and plans to make more of their own ICs (Lapedus, 2020). The world is dangerously dependent on Taiwan for semiconductors. A disruption in semiconductor supply and availability could have a significant impact. The current shortage of automotive chips during the pandemic could cost $50 to $60 billion in losses just for automotive manufacturers (Crawford et al., 2021). Taiwan Semiconductor Manufacturing Co. (TSMC) makes more than half of the world’s contracted semiconductor ICs and could impact the availability of supply for a number of industries. TSMC makes ICs for iPhones, Amazon cloud computers, and for fighter jets like the F-35 (Pierson & Yun, 2020). Beijing considers Taiwan a part of China, and in the event of a geopolitical dispute, the impact to industry’s ability to deliver technology using ICs, and the ability for the U.S. and

their allies to maintain a technological advantage could be thwarted, as semiconductors are vital to national security assets in the global race for technology supremacy. Even setting geopolitics aside, dependence of the supply chain on a single point of failure is dangerous. Take for example, the water shortage that impacted TSMC and threatened their production capability, potentially impacting some of their top customers such as Intel, AMD, Apple, Samsung, and Nvidia to name a few. The water shortage demonstrates the limited and potentially restrictive availability of resources needed to produce EEE parts (Wickens, 2021).

Provenance, traceability, and **nonrepudiation** have an important role in establishing trust and assurance in microelectronic devices for the systems and people that depend on them. **Nonrepudiation** is the assurance that someone cannot deny the validity of something, or more specifically, refute responsibility. As an example, when you sign a legal contract in ink, your signature is a nonrepudiation mechanism. You cannot later disagree to the contract terms or refute ever taking part in the agreement. Provenance and traceability are often used interchangeably, but the terms have distinct meanings that complement each other relative to transparency and establishing trust. **Provenance** is the "chronology of the origin, development, ownership, location, and changes to a system or system component and associated data. It may also include personnel and processes used to interact with or make modifications to the system, component, or associated data" (NIST, 2021). SAE AS5553 defines counterfeiting and lays out the elements of a counterfeit prevention plan that mitigates the risk of using counterfeit items; including the step of always purchasing parts from authorized sources, thereby maximizing the likelihood of traceability to the original manufacturer. Providing provenance significantly extends this idea and greatly improves this mitigation. A good example to describe the differences is in the food supply chain where consumers have a need to know more about how the food was processed that includes the source and origin. Food allergies such as peanut and gluten allergies, and dietary preferences such as vegetarian, vegan, kosher, halal, etc., create the need for more information about the food and how it was processed. For instance, some snacks that do not contain peanuts must still disclose if their facility processes other snacks that contain peanuts in the event there is contamination. Provenance can be viewed as the outcome of scientific verification and validation of the food source (such as no peanut products processed at the origin, vegan, organic, Non-GMO) and the food origin (such as geographic location), so you can select your wild-caught Norwegian salmon vs. farm-grown Atlantic salmon at the supermarket or restaurant. The food industry has a complex supply chain of farmers, producers, and distributors. **Traceability** identifies the intermediaries from the origin to destination. Like every other sector, the food industry contains deceptive organizations and individuals looking to make money based on fraud, adulteration, and deception regarding the food they sell, establishing the need for provenance, traceability, and nonrepudiation. In the microelectronics sector, provenance, traceability, and nonrepudiation also play a critical role in establishing hardware assurance, quantified trust, and risk-based cybersecurity for the systems in which the ICs are integrated. Today's complex system-on-chip (SOC) designs may contain billions of transistors and gates that could contain weaknesses and vulnerabilities that could be exploited by an attacker. Hardware designers and organizations may design the entire SOC or selectively acquire Intellectual Property (IP) cores from other designers that may not be verified and validated against known weaknesses and vulnerabilities that could be exploited by an attacker.

Finally, **pedigree** validates the composition and provenance of technologies, products, and services. A common example of pedigree is represented in biological representation of animals, such as dogs and horses. For example, the American Kennel Club certifies the pedigree of dogs. A certificate of pedigree, for example, will certify a dog as a Female Labrador Retriever that includes the lineage of the dog's parents and grandparents, proving that the dog is a purebred Labrador. For hardware, pedigree includes material composition of components in accordance with claimed performance characteristics from

hardware manufacturers. For example, a MIL-Spec part has claims that the component has undergone certain performance qualification and testing criteria in accordance with a military specification (e.g. MIL-PRF-38535 for Integrated Circuits (Microcircuits) Manufacturing). A MIL-Spec part would need pedigree to a qualified manufacturer who has been certified to build components in accordance with the military specification. Pedigree is also an important concept in counterfeit components. For example, counterfeit clones and overproduced parts may not have the same material composition or qualification testing impacting the potential performance of such devices. While one may think they operate the same as an authentic device, the component may not operate as expected due to changes in materials, construction and/or lack of screening normally performed through required verification testing.

Appendix 4: Guidance on Risk and Assurance

Risk management is not a “one-shot” process of populating a risk matrix and then storing it on a shelf - it involves continual monitoring and reassessment of residual risk to ensure that the risk is acceptable at any given time. Luckily a number of guidance documents and standards have been published which can aid in risk-based decision making within a Zero Trust environment. As summarized by DODI 5000.02T:

> *“ACTIVITIES TO MITIGATE CYBERSECURITY RISKS. DoD Program Managers will rely on existing cybersecurity standards tailored to reflect analysis of specific program risks and opportunities to determine the level of cyber protections needed for their program information, the system, enabling and support systems, and information types that reside in or transit the fielded system. Appropriate cyber threat protection measures include information safeguarding, designed in system protections, supply chain risk management (SCRM), software assurance, hardware assurance, anti-counterfeit practices, anti-tamper (AT), and program security related activities such as information security, operations security (OPSEC), personnel security, physical security, and industrial security.”* (DoD, 2020a)

In February 2021, NIST published NISTIR 8276 “Key Practices in Cyber Supply Chain Risk Management: Observations from Industry”. Regarding SCRM for Information and Communications Technologies (ICT):

> *“ICT SCRM is an organization-wide activity that should be directed under the overall agency governance, regardless of the specific organizational structure. At the organization level, ICT SCRM activities should be led by the risk executive function, described in [NIST SP 800-39], and implemented throughout the organization by a variety of individuals in different roles. The audience for this publication is federal agency personnel involved in engineering/developing, testing, deploying, acquiring, maintaining, and retiring ICT components and systems. These functions may include, but are not limited to, information technology, information security, contracting, risk executive, program management, legal, supply chain and logistics, acquisition and procurement, other related functions, and system owner. Other personnel or entities are free to make use of the guidance as appropriate to their situation.”* (NIST, 2021)

Similarly, NIST Special Publication 800-161, while written for US Government organizations, presents best practices that can translate to the commercial sector. NIST takes a lifecycle perspective, where “ICT SCRM encompasses activities in the system development life cycle, including research and development (R&D), design, manufacturing, acquisition, delivery, integration, operations, and disposal/retirement of an organization’s ICT products (i.e., hardware and software) and services.” Finally, SCRM is framed in terms of four concepts: Security, Integrity, Resilience, and Quality:

> *“Security provides the confidentiality, integrity, and availability of information that*
>
> *(a) describes the ICT supply chain (e.g., information about the paths of ICT products and services, both logical and physical); or (b) traverses the ICT supply chain (e.g., intellectual property contained in ICT products and services), as well as information about the parties participating in the ICT supply chain (anyone who touches an ICT product or service throughout its life cycle);*

Integrity is focused on ensuring that the ICT products or services in the ICT supply chain are genuine, unaltered, and that the ICT products and services will perform according to acquirer specifications and without additional unwanted functionality.

Resilience is focused on ensuring that ICT supply chain will provide required ICT products and services under stress or failure; and

Quality is focused on reducing vulnerabilities that may limit the intended function of a component, lead to component failure, or provide opportunities for exploitation." (NIST, 2015)

Can we really determine if hardware or software will function as intended and only as intended? As it turns out, the answer is "yes" when it comes to "function as intended", but "no" with respect to "only as intended", (when it comes to any absolutes). However, we may be able to reach some assurance/confidence level through measurement and evaluation.

For example, any consumer of a product has a reasonable expectation that the purchased product will perform as advertised/indicated and function properly (safely & securely, under specified conditions), but many do not consider if there are any additional functions built into the product. For instance, there is some expectation that a laptop with a face-to-face (F2F) web-conferencing capability will have a webcam, and there is an expectation that the laptop webcam will function properly when enabled, but what if it is not enabled? Might it still function, even when turned off — violating your expectation of privacy? Or what if such a webcam capability was embedded in other electronic devices in your house and you had no expectations that those devices had webcams? We can test/determine if a known camera functions properly, but how do we determine if other devices have unknown camera capabilities? With respect to the camera capability example, there are some special tools that can find such devices, but maybe not for other functions/capabilities that may be currently activated or have the potential to be activated at a future time. We can develop tests and techniques to find known configurations and capabilities.

The principle of Zero Trust would apply equally to things you design but have vulnerabilities or natural defects. Taking the analogy to the microchip level, given specifications of a hardware/chip, we can use select tools and processes to determine that the chip's performance meets specifications, with an acceptable level of confidence. And, given any hardware, we can also use select tools and processes to test for known weaknesses, vulnerabilities and deviations from expected performance characteristics or behavior, but we can't determine/predict all states of possible anomalous behavior. We may be able to determine how well we've tested for known weaknesses/vulnerabilities and also document some volume of monitoring and diagnostics - all giving us some degree of coverage or confidence level that there are likely no unintended functions in the hardware.

There are a variety of entities that may test the hardware and provide data for such assurance consideration. Designer, developer/integrator, and provider communities might provide a description of design, fabrication, verification, and validation processes/tests and acquired data in their design and manufacture processes. When the provider collects such data, they can provide an Assurance Case to the acquirer/end-user. The acquirer, consumer, and user community may also conduct acceptance testing, both in static and dynamic situations, but also in a real or simulated operational environment (much like SW-testing). Additionally, the user may create several situations/conditions for the hardware (much like fuzzing for software). Additionally, both or either provider and/or acquirer can solicit third-party test/evaluation to gain additional independent data for assurance/confidence that there is no unintended functionality in the hardware/chip. Ideally, more than one source of data better informs this assurance/confidence level.

Table A2. SCRM Actions by Risk Tolerance Level (adapted from DODI 5000.90)

Risk Tolerance Level	Actions Required
High Risk Tolerance applies to simplified procurements, like computers at the Defense Commissary Agency.	PMs should: • Exercise caution regarding products originating from sources with identified foreign ownership, control, or influence concerns. • Utilize approved product lists. • Maintain assurance through industry standards. • Balance risk against mission type.
Moderate Risk Tolerance applies to structured procurements, like wireless networks at a forward deployed base.	PMs should implement all previous strategies and: • Use verifiable vendor processes for product integrity (e.g., SSAE18-SOC2). • Improve awareness of vendor/product limitations. • Manage critical SCRM risks through countermeasures.
Low Risk Tolerance applies to engineered procurements, like industrial control systems in a tank.	PMs should implement all previous strategies and: • Assess critical components. • Implement available countermeasures. • Utilize commercial assessment vendors, the Joint Federated Assurance Center, interagency and close and trusted international partners, national labs/FFRDCs, and intelligence and CI
Very Low Risk Tolerance applies to assured procurements, like nuclear command and control systems.	PMs should implement all previous strategies and: Follow all requirements in DoDI 5200.44 and NIST SP 800-161; including: • Conducting criticality analysis. • Documenting in Program Protection Plan. • Sending requests on critical components/suppliers to the DIA SCRM TAC or other CI sources. • Flagging reports that come back critical, high, or select medium.

ISO/IEC 15026-2 describes assurance cases that are generally developed to support claims in areas such as safety, reliability, maintainability, human factors, operability, and security, although these assurance cases are often called by specific names, e.g. safety case or reliability and maintainability

(R&M) case (ISO/IEC, 2011). ISO 26262 provides Automotive Safety Integrity Levels (ASILs), that are based on three variables: severity, probability of exposure, and controllability by the driver (ISO, 2018). ISO 26262 considers both HwA & SwA levels impacting safety. ISO 26262 mandates a functional safety development process (from specification all the way through production release) that automotive OEMs and suppliers must follow and document (for compliance) to have their devices qualified to run inside commercial (passenger) vehicles. It outlines a risk classification system (Automotive Safety Integrity Levels, or ASILs) and aims to reduce possible hazards caused by the malfunctioning behavior of electrical and electronic (E/E) systems. ISO 26262 is a representative case where an operational (end-user) ecosystem is developing methodologies to manage risk (in this case safety risk) in their system due to embedded HW & SW. In other ecosystems, the operational environments need to develop their own risk-based approaches with associated assurance (integrity) levels, learning from, but without duplicating the expensive Common Criteria Evaluation Criteria Levels (EALs) and testing regime.

Organizational processes can be documented and/or certified against commercial standards. ISO/IEC 20243 documents some of the best practices and standards for organizational processes (ISO/IEC, 2018). It establishes a set of guidelines, requirements, and recommendations that address specific threats to the integrity of hardware and software COTS ICT products throughout the product life cycle. This release of the Standard addresses threats related to maliciously tainted and counterfeit products.

The provider's product life cycle includes the work it does designing and developing products, as well as the supply chain aspects of that life cycle, collectively extending through the following phases: design, sourcing, build, fulfillment, distribution, sustainment, and disposal. While the ISO/IEC 20243 Standard cannot fully address threats that originate wholly outside any span of control of the provider, for example, a counterfeiter producing a fake printed circuit board assembly that has no original linkage to the Original Equipment Manufacturer (OEM), the practices detailed in the Standard will provide some level of mitigation. An example of such a practice would be the potential use of some sort of security labeling technique in legitimate products.

To gain further insight, consumers may want to perform more investigatory “due-diligence” on their potential suppliers, normally used when exploring mergers and acquisitions, considering history of financial performance, legal activities, and with what laws the organization must comply, etc. This could include privacy restrictions, lack of privacy protections, intellectual property protection laws, child labor laws, and other considerations. This is all very complex and requires extensive supply chain transparency which must be aligned with market incentives while affording the security needed. That leaves the question of how we manage this Cyber-Supply Chain Risk Management (C-SCRM) challenge on a broader scale? Ecosystems owners need to conduct criticality analysis of the functions/capabilities that enable them and prioritize the investigation of their supply chains. One could start to address some confidence/assurance levels based on the percentage of each tier identified or depth of tiers identified, but one must also address the degree of due-diligence needed at each level/tier and what mitigations have been used in the HW/SW implementation. The US Government Executive Order 14028 on Cybersecurity dated on 12 May 2021 requires near-term action on software bills of materials that could be extended into hardware in the future.

As before, organizations do not need to start from scratch when establishing Zero Trust life cycle practices - many standards and guidance documents exist, including ISO/IEC 27036-3 (ISO/IEC, 2013), which is currently under review/update to better align with ISO/IEC 15288 (2015), which states:

> *“ISO/IEC/IEEE 15288:2015 establishes a common framework of process descriptions for describing the life cycle of systems created by humans. It defines a set of processes and*

associated terminology from an engineering viewpoint. These processes can be applied at any level in the hierarchy of a system's structure. Selected sets of these processes can be applied throughout the life cycle for managing and performing the stages of a system's life cycle. This is accomplished through the involvement of all stakeholders, with the ultimate goal of achieving customer satisfaction.

ISO/IEC/IEEE 15288:2015 also provides processes that support the definition, control and improvement of the system life cycle processes used within an organization or a project. Organizations and projects can use these processes when acquiring and supplying systems.

ISO/IEC/IEEE 15288:2015 concerns those systems that are man-made and may be configured with one or more of the following system elements: hardware, software, data, humans, processes (e.g., processes for providing service to users), procedures (e.g., operator instructions), facilities, materials and naturally occurring entities." (ISO/IEC/IEEE, 2015)

And finally for consideration is the whole family of US NIST standards, with special consideration given to NIST Special Publication 800-53A/B Revision 5 (NIST 2020b) providing security control assessment procedures and NIST Special Publication 800-37 Revision 2 (NIST 2018) providing guidance on monitoring the security controls in the environment of operation. Additionally, there is NIST SP 800-171 (NIST 2020c) & 800-161 (NIST, 2015); which respectively cover "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations" and "Supply Chain Risk Management Practices for Federal Information Systems and Organizations". While not all commercial organizations may be subject to US federal standards or hold USG data, there may be best practices here to be leveraged in the commercial sector, much like what is going on globally right now with the NIST Risk Management Framework (RMF).

Appendix 5: Layers of Security – Examples of Current Practices and Gaps

Software vs. Hardware Security

The SolarWinds Orion IT Manager software breach showed weaknesses in an extraordinary number of security systems, including many United States agencies, including the U.S. Treasury Department, Cybersecurity and Infrastructure Agency (CISA), and Department of Homeland Security, as well as Microsoft's cloud security system. The hackers exploited a vulnerability in the SolarWinds supply chain and introduced malware into the application (Smith, 2020). The attack involved forging certificates to evade security measures. Microsoft's team was able to de-authenticate the trusted certificates and rapidly update Microsoft Defender to detect and handle illegitimate files (Microsoft Security Response Center, 2020). Prior to this attack, several others have been launched over the years. For example, in 2017, incorrect exception handling in the Jakarta Multipart parser for the Java-based open-source web development framework Apache Struts 2 allowed for a remote code execution attack to be employed against the software (CVE-2017-5638). This leads to a breach in the consumer credit reporting bureau Equifax, resulting in up to 143 million customers having their personal data exposed to hackers (Luszcz, 2018). Within days of realizing there was a critical error, Apache released a patch to alleviate the problem. Over the course of four months, Equifax was able to once again secure their customers' information (Wang & Johnson, 2018). This is not a new problem; Ken Thompson famously described such a thought experiment in his ACM lecture when he was recognized with the Turing Award in 1983 for his role in implementing UNIX. His lesson to the reader was:

> *"The moral is obvious. You can't trust code that you did not totally create yourself. (Especially code from companies that employ people like me.) No amount of source-level verification or scrutiny will protect you from using untrusted code. In demonstrating the possibility of this kind of attack, I picked on the C compiler. I could have picked on any program-handling program such as an assembler, a loader, or even hardware microcode. As the level of program gets lower, these bugs will be harder and harder to detect. A well-installed microcode bug will be almost impossible to detect."* (Thompson, 1983).

Although the attacks outlined above are detrimental, they benefit from rapid detection and rapid response from the software developers. This software strength is, unfortunately, unavailable when taking into consideration hardware. Once the hardware has been designed, no more modifications can be done during its lifetime. This downfall leads to a necessity for hardware design integrity and security to ensure legitimate chips are being created and sold. Yes, compromised chips can (potentially) be detected, but they will then need to be destroyed. In addition, the majority of consumers do not have the proper knowledge to authenticate parts before placing them in an electronic system. This makes hardware threat mitigation much more complicated than software threats. It is also more costly - detection post-manufacturing can significantly impact schedule and cost.

Runtime Monitoring: A system, be it hardware or software, should be secure at each step of execution. A software solution that has recently gathered traction focusing on Java and .NET platforms is the Runtime Application Self-Protection Technology (RASP) (Cisar & Cisar, 2016). This automated system monitors running applications and is able to detect and prevent real-time attacks (Gartner, 2021). While still not being a perfect solution for complete protection, when combined with other applications, it helps provide a higher level of software security (Cisar & Cisar, 2016). With hardware, there needs to be a method of monitoring to ensure that information is not being transmitted from the chip to a third party. Once a chip is

in possession of a user, it would be challenging to notice if any information is being leaked by the chip without added on-chip monitors. A subset of runtime monitoring is integrity verification. There needs to exist a method of ensuring the system, be it software or hardware, is authentic. In software implementations, a good example would be software license verification. It is easy to implement crypto primitives, allowing for constant updating of the software builds. With hardware, this becomes a bit more challenging. Hardware integrity involves needing to determine the legitimacy of the chip as well as ensuring that no tampering with the chip has occurred. Again, this incurs an overhead that customers do not typically want.

Authentication: Currently on the market are a variety of multi-factor authentication applications. These provide a second level of security for software users in the event a password or secret key of some kind is compromised. Google Authenticator is a popular software-based multi-factor authenticator for various video game companies, e-commerce websites, and government services (e.g., United States' official hiring website). The authenticator generates a time-based OTP generated by the device on which the application is installed (Gordin et al., 2019). Implementing dual-authentication-like infrastructure is much more difficult for hardware implementation. Another application for an authentication scheme is for end-point authentication. In software, end-point authentication can be implemented through various cryptographic primitives (e.g., MACs and digital signatures) as long as the basic functionalities are understood and properly used. With hardware, chip manufacturers will include additional components, such as physically unclonable functions (PUFs) to provide root of trust to trusted platform modules (TPM) to store secret keys. With physical access to the chip, such as during part of the supply chain, an adversary can launch physical attacks to obtain or modify on-chip assets.

Detection and avoidance of counterfeit ICs

Various counterfeit electronic parts, including recycled, remarked, overproduced, cloned, out-of-spec/defective, forged documentation, and tampered types, pose a severe threat to the security of our critical infrastructures (Tehranipoor et al., 2015; Guin et al., 2014a,b). Over the years, a class of solutions has been proposed to mitigate the widespread infiltration of these fake parts, and they can broadly be classified into two categories, such as counterfeit detection and avoidance approaches. Traditionally, physical inspection and electrical tests (SAE, 2016) are straightforward methods to detect counterfeit ICs; however, they suffer from excessive test time, lack of automation, and high test cost. Many researchers currently propose utilizing machine learning and image processing-based approaches to automate physical inspection (Asadizanjani et al, 2017). However, the lack of a golden data set makes these approaches challenging for obsolete chips. Moreover, manufacturing process variation makes traditional electrical tests inaccurate as there are no clear separations on the parameter variations from aging and process variation. Currently, Guin et al. (2019) showed that process invariant time zero reference parameters can be obtained from the startup values of SRAM cells. This approach can be applied to any chips that contain an SRAM-based memory. Counterfeit avoidance, such as design-for-anti-counterfeit (DfAC) approaches, prevents recycled ICs by modifying the original design (Kim et al., 2008). The most primary challenge for the counterfeit avoidance method is that it cannot be a solution for the chip that has already circulated in the market since it requires modification of design.

Detection of Hardware Trojans

Hardware Trojans (HT) can be inserted during any step of the IC design and manufacturing process due to the involvement of various untrusted entities. They can be mainly classified as combinational, sequential Trojan, or analog Trojans. Any Trojan can be activated by a rare trigger event that is not encountered during manufacturing tests, and the Trojan remains quiet during the normal operation. This detection problem manifolds for sequential and analog Trojans because they either require triggering multiple times or affect the circuit after a certain period once the Trojan is triggered. To cope with such

potential threats, researchers have proposed various methods to detect HT, broadly divided into three categories: logic testing, side-channel analysis, and reverse engineering analysis. Logic testing involves applying stimuli to primary inputs (PIs) and observing responses at primary outputs (POs) (Banga & Hsiao, 2011). A Trojan is detected when there is a mismatch between the observed and expected responses. However, these techniques are specific to finding the rare trigger pattern to activate a Trojan, which is practically infeasible, considering all possible Trojans (Zhou et al., 2018). Moreover, it is not feasible to detect sequential or analog Trojans considering their trigger action. The side-channel analysis uses physical characteristics such as power, temperature, delay, and radiation to detect the variation caused by the Trojan circuitry. The most significant advantage of side-channel analysis is that it can detect the HTs even if they are not activated. These methods are still in the research phase and will need continued development before they are effective assurance solutions. They rely on the availability of Trojan-free golden circuits, which can be very difficult to acquire. Besides, side-channel parameters are susceptible to process/environmental variations. Reverse engineering (Quadir et al., 2016) analysis uses destructive or non-destructive methods to obtain structure information from post-silicon devices. It compares them with the golden netlist using machine learning techniques to determine HTs. Reverse engineering analysis does not need to activate hardware Trojans; it can detect sequential Trojans added in the fabrication process (Stern et al., 2020). Full-blown reverse engineering could be costly. However, optical imaging techniques can be beneficial but require specific equipment and comply with the trade-offs between accuracy and imaging SEM parameters. In the future, the researchers can optimize the pattern generation process of logic testing and eliminate PV on side-channel analysis. Furthermore, hybrid HTs detection methods can be developed along with non-destructive reverse engineering.

Prevention of IP Piracy

The severity of IP piracy or theft has been the driving force for the research community to devise new countermeasures to secure the design. In recent years, several solutions have been proposed to limit the attacker's capability to gain information regarding an IC design. Primarily, these countermeasures can be categorized as (i) logic locking, (ii) IC camouflaging, (iii) split manufacturing and, (iv) IP watermarking. Among them, logic locking is the most prominent key-based hardware obfuscation technique which is based on the inclusion of key-bit controlled XOR gates in logic circuits. Unfortunately, logic locking can be broken by the SAT (Satisfiability) attack (Subramanyan at al., 2015), and the current solution in logic locking aims towards SAT resiliency and does not apply to non-logic classes of circuits such as RF, analog, and optoelectronics. Secure solutions from the design point of view include modifications in the original circuit and scan chain to prevent key leakage through scan-chain. Recently, logic locking was also exposed to other means of attacks such as implanting hardware Trojans attacks (Jain et al, 2021), probing based attacks (Rahman et al., 2020), oracle or oracle-less attacks (Zhang et al., 2020). On the other hand, 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, still demonstrating the intended logic functionality (Shakya et al., 2019; Li et al., 2017). The production of ICs is carried out in two different foundries, termed as the split manufacturing technique, to restrict the design access to the untrusted foundry. The upper metal layers are manufactured at a trusted foundry while the lower metal layers/transistors are completed by the untrusted foundry, in a way to restrict the untrusted foundry from gaining complete information regarding the design (Vaidyanathan et al., 2014; Yang et al., 2020). However, several attacks undermining the security achieved through split manufacturing have also been proposed in the past. The process of IP watermarking is based on embedding secret information of the IC designer inside the IP design itself to authenticate the IP owner uniquely. 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). Amongst the many solutions proposed so far, it is difficult to categorize any technique that can provide absolute defense against IP piracy. Mainly focused on logic locking due to its impact, future work

would focus on developing testing methods to detect/eliminate malicious modifications in the design. Additionally, physical or optical probing methods should be mitigated to protect the IC design once the key is programmed into the tamper-proof memory. The complete security for locking techniques can only be achieved when the above conditions are satisfied, followed by the selection of an SAT resilient locking technique.

Physical Attacks

Physical attacks mainly comprise fault injection attacks, side-channel analysis, and reverse engineering methods. Fault injection attacks intentionally disturb the computation of a chip to induce errors at the output response, followed by the exploitation of erroneous output to extract security-critical information such as a secret key or bypass security measures in the device (Kim & Quisquater, 2007). Fault injection attacks can be further classified based on the attack process or method, which includes – clock glitch, power variation, electromagnetic pulses or radiation, laser, and focused ion beam (FIB). The design-based defense techniques detect a fault by using recalculation or error detection code (Bu & Kinsy, 2018; Doulcier-Verdier et al., 2011) but are mostly applicable where design duplication is possible. Meanwhile, at the package level, sensor structures are studied to restrict the vulnerability against external fault injection (Matsude et al., 2018, 2016), which takes a respective action of powering down or flushing internal storage. However, these countermeasures can reveal the crucial information regarding the key-value through side-channel, etc. (Sugawara et al., 2019; Li et al., 2019). The correlation between side-channel leakages with the input data can also reveal security-critical information from the devices, which is called side-channel analysis. Differential power analysis (DPA) attacks are practical, non-invasive, and highly capable over a wide variety of cryptographic systems (Prouff et al., 2009). Many different countermeasures have been proposed to make the designs resistant to side-channel information leaks, such as masking (Schramm & Paar, 2006), dual-rail precharge (DRP) logic (Tiri & Verbauwhede, 2004), current-domain signature attenuation (CDSA) (Das et al., 2020). Reverse engineering techniques can also serve a malicious attacker's purpose to determine the design information either through destructive or non-destructive methods. The non-destructive techniques are gaining popularity due to their feasibility and the possibility of the device being operational even after the analysis (Rahman et al., 2020); however, they can be prevented by camouflaging (Shakya et al., 2019). The future trends against fault injection attacks should be intended to limit the fault site identification by the attacker, which will make it difficult for the attacker to perform the attack. Similarly, side-channel analysis is heavily dependent on leaks based on the key-dependent operation, which the designer should restrict or even-out to limit the information/traces available.

Appendix 6: On the Role of Trusted Suppliers

As we have mentioned, Zero Trust does not imply that we never have trust in any of our suppliers. Moreover, adopting a Zero Trust view still does not address gaps such as assured supply. Therefore, there is still an important role to be played by "trusted" suppliers within the microelectronics supply chain, such as the DoD Trusted Foundry Program. The program, managed by the Defense Microelectronics Activity (DMEA), accredits suppliers of integrated circuits across a broad range of areas such as design, manufacturing, packaging, and testing, to ensure that the suppliers are trusted sources which will: *"Provide an assured "Chain of Custody" for both classified and unclassified ICs; Ensure that there will not be any reasonable threats related to disruption in supply; Prevent intentional or unintentional modification or tampering of the ICs; Protect the ICs from unauthorized attempts at reverse engineering, exposure of functionality or evaluation of their possible vulnerabilities"* (DMEA, 2021).

Taking an enterprise-wide view, having a trusted supplier program and taking a Zero Trust posture are not mutually exclusive, but rather can serve as multiple layers in a comprehensive, risk-based security strategy while supporting contractual guarantees for access and availability and evolving this network of suppliers into an even more secure and robust onshore supply chain solution. The most effective way to avoid compromised microelectronics will always be to purchase them directly from an accredited, authorized, and trusted source (Livingston, 2007).

It may also be necessary to purchase components on the open "untrusted" market. This is when a lower level of initial trust and greater assurance through validation and verification is required. Depending on the organization's risk tolerance, and the criticality of the system, the decision to procure parts from an untrusted source will be a risk-based decision and involve multiple layers of countermeasures, third-party testing, and continuous fine-grained, multi-factor monitoring and authentication. A combination of securely documented information including intrinsic variability, multi factor authentication through statistical process controls, and analysis of the supply chain to ensure availability can provide an increased basis for assurance. These measures, added to an already highly complex process for semiconductor fabrication, would make a deliberate threat extremely difficult to execute. Therefore, a Zero Trust approach can exist alongside a trusted supplier infrastructure, and in fact the two can be complementary. Monitoring alone is insufficient, and microelectronics supply chains are not like IT systems or the internet where there are many redundancies and pathways for delivering services. For inline mitigations and remediation to be effective, organizations need to plan ahead with redundant alternative manufacturers and distributed supply chain paths.

Moreover, a company may have different business lines which have different supply chains and require different supply chain strategies (Simchi-Levi et al., 2013). Some supply chains support safety-critical or national defense related systems, whereas other supply chains within the same company might support consumer goods. Whereas for the safety-critical and defense systems, one may only want to procure from an accredited and trusted supply base, for consumer goods there is a lower risk and therefore a willingness to work with untrusted suppliers. Such supply chain differentiation is common (Beck et al., 2012), and the same theory applies to Zero Trust (Collier & Sarkis, 2021). Zero Trust may be appropriate for some situations, while inappropriate for others, and this determination requires thinking through the risks, costs, and benefits of applying a Zero Trust security strategy.

The Zero Trust approach utilizing Quantifiable Assurance as a means for implementation should complement and build upon existing programs, such as the DMEA Trusted Foundry Program. The Trusted Foundry Program could be used as a data source in the Zero Trust model that can quantify some

of the risk of the supply chain. Those suppliers in the Trusted Foundry Program would have a lower risk-based score as it relates to quantifying the supplier risk. The Trusted Foundry Program also includes options for contractual guarantees for access and availability to USG, enables access for low volume critical defense parts that would otherwise not pass industry business case hurdles for support, and in doing so enables the defense industrial base for their critical needs. Incentives for access and availability could be extended to other critical infrastructure areas important to the USG and national security in a synergistic manner.

—END—