INL/MIS-22-70124-Revision-0

Building Blocks for Secure and Prosperous Defense Critical Supply Chains: A Case Study from Microelectronics

December 2022

Changing the World's Energy Future

Howard D. Grimes, Gabriela F. Ciocarlie, Robert J. Butler, Wayne E Austad

Idaho National Laboratory

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/MIS-22-70124-Revision-0

Building Blocks for Secure and Prosperous Defense Critical Supply Chains: A Case Study from Microelectronics

Howard D. Grimes, Gabriela F. Ciocarlie, Robert J. Butler, Wayne E Austad

December 2022

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

Building Blocks for Secure and Prosperous Defense Critical Supply Chains: A Case Study from Microelectronics

Target Publications: *AFCEA Signal*

Authors: Grimes, Ciocarlie, Butler, Austad

United States (U.S.) critical supply chains are under siege. State-sponsored cyber actors are enlarging their threat vectors in both capabilities and active intentional use in supply chains. China's laws and policies support the active use of human intelligence to gather information regarding supply chains[1]. Recently, Chinese advanced persistent threat (APT) supply chain attacks were used to steal data from companies and their customers. These attacks were initiated by APT41 (also known as Barium, Winnti, Wicked Panda, and Wicked Spider)[2].

Russian state-sponsored and criminal cyber actors also have demonstrated capabilities to compromise IT networks, by using mechanisms to maintain long-term, persistent access to IT networks. This access allows exfiltration of sensitive data from IT networks (and also operational technology (OT) networks) by deploying destructive malware to disrupt critical industrial control systems (ICS)/OT functions.

Russia also actively targets critical energy infrastructure. BERSERK BEAR (also known as Crouching Yeti, Dragonfly, Energetic Bear, and Temp.Isotope) targeted entities in Western Europe and North America including the Energy Sector Industrial Base, Transportation Systems, and Defense Industrial Base (DIB) Sector organizations[3].

Additionally, the volume of cyber vulnerabilities in U.S. systems continues to increase dramatically. Adversaries now have greater freedom, political support within their home countries, and financial support from adversarial governments to deliberately introduce vulnerabilities into our critical infrastructure in the U.S. and other countries. The "Triton", "Dragonfly", and "Havex" operations sponsored by Russia demonstrate this approach. These cyberattacks resulted in malware being installed on more than 17,000 devices in the U.S. and abroad, including ICS/supervisory control and data acquisition controllers used by power and energy companies[4]. Importantly, Robert M. Lee, CEO of Dragos, described Triton as "the first piece of malware specifically designed to kill people."

[1] https://www.fbi.gov/investigate/counterintelligence/the-china-threat
[2] https://krebsonsecurity.com/2020/09/chinese-antivirus-firm-was-part-of-apt41-supply-chain-attack/
[3] https://www.cyber.gov.au/acsc/view-all-content/advisories/russian-state-sponsored-and-criminal-cyber-threats-critical-infrastructure
[4] https://www.securityweek.com/us-charges-russian-hackers-over-infamous-triton-havex-cyberattacks-energy-sector.

These vulnerabilities, whether native or inserted, are typically operationalized in legacy systems that were not designed to be secure, further increasing the vulnerability of our critical infrastructure supply chains.

It is extremely difficult to perform consequence management of defense and energy supply chains and enterprises. Current operations, manufacturing, and supply chains lack any semblance of a comprehensive risk register that would prioritize courses of action to protect enterprises. Today's service level agreements for IT systems typically do not take into account the (exponentially) growing risks to our defense and energy sectors.

Emerging cybersecurity technology innovations can, and must, support the design of more secure, resilient, and efficient defense critical supply chains. There is a national security imperative to make U.S. supply chains more resilient and cyber secure. In February 2022, the Department of Defense (DoD) issued a report entitled "Securing Defense-Critical Supply Chains"[5] in response to President Biden's Executive Order 14017, Executive Order on America's Supply Chains[6]. This report states "Our work to build resilient, competitive, and sustainable supply chains will be a long-term campaign."

Microelectronics supply chains are critical to national security and economic prosperity. They also represent one of the most challenging defense critical supply chains to secure because of their global reach; and, contributions from both friendly and unfriendly nations. Defense, commercial, and critical infrastructure sectors are all dependent on a diverse supply of microelectronics products manufactured in a global ecosystem.

To build resilient, competitive, and sustainable supply chains will require significant research, development, and deployment efforts encompassing the best expertise of government, industry, academia, and international organizations.

Production of these microelectronics is complex and typically follows a process of product design, fabrication (lithographic patterning and manufacturing of silicon die on a common substrate involving over 500 discrete processing steps that can take several months), packaging, assembly, testing, and quality control.

The microelectronics supply chain is globally dispersed and much of the manufacturing is centralized in the Asia-Pacific region. As summarized in the DoD report, the size and complexity of the global microelectronics supply chain can be inferred from the fact that there are over 10,000 large microelectronics distribution companies dispersed globally that serve as distribution

[5] https://media.defense.gov/2022/Feb/24/2002944158/-1/-1/1/DOD-EO-14017-REPORT-SECURING-DEFENSE-CRITICAL-SUPPLY-CHAINS.PDF
[6] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/

points for over 500,000 microelectronics components. These supply chains have little or no traceable integrity and often cannot be trusted which presents a profound challenge to our national security.

These microelectronic supply chains and technologies are a central component to achieve DoD advance capabilities. Thus, questions of extreme importance to our nation's defense and U.S. National Security are: 1) how can we secure the microelectronic industry? and 2) how can we introduce trusted traceable integrity into the microelectronic supply chain across the globe? In other words, when the U.S. receives chips, motherboards, or components from any manufacturer in the world, including potential global adversaries, how can we validate and verify the integrity of the electronics prior to using them in our critical infrastructure? Here we introduce two key approaches that support the U.S. microelectronics industry to *verifiable security properties and guarantees of physical functions.* These principles offer U.S. manufacturers guidance on how to identify, mitigate, and nullify potential weaknesses or faults in supplied parts—even those introduced intentionally. Thus, this approach results in quantifiable assurance for microelectronic supply chains.

What are the building blocks required for defense critical supply chains?

First, we must develop formal cybersecurity design specification and verification for the microelectronics industry (design for cybersecurity). By employing a new process for formal design specification and verification that spans implementation, integration, as well as operation, potential adversary attack vectors are significantly diminished before implementation and deployment, and providing security guarantees (e.g., integrity of the design file) that are propagated from design and implementation to operation. Moreover, eliminating or mitigating vulnerabilities earlier in the design stage is cost effective (Figure 1). This may not only involve the design of the parts, sub-assemblies, and products; but also, the critical supply chain processes involved in sourcing, manufacturing, and delivering the the final product to end-customers. Typically, 90% or more of the lifecycle cost of sourcing, manufacturing, and servicing a product is locked-in the design stage of the product and supply chain which limits opportunities for improvements later on in the lifecycle. Getting the design right from the beginning is critical. Given the significant new investments in the semiconductor industry over the coming years, this is the right opportunity to include formal design specification and verification in the next generation manufacturing systems.

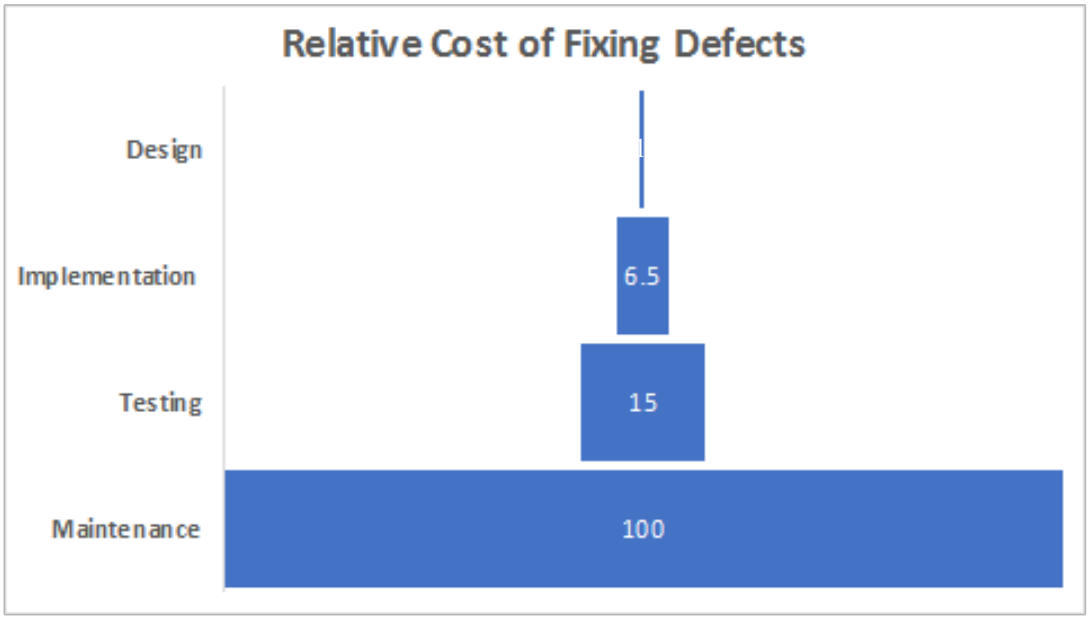

Figure 1. Relative Cost to Fix Software Defects (IBM System Science Institute Relative Cost of Fixing Defects[7]).

Specifically, a design specification based on formal models entails the following steps: a) define the components of a system along with its interfaces (e.g., communication port), b) identify the connected components within the system, c) define the desired security properties (e.g., authentication, encrypted connections) and productivity properties (e.g., component input and output constraints), d) verify that a design adheres to these defined properties. This formalism enables behavioral analysis of implementations, operations, and "digital twins" of real systems to verify the required security properties.

Microelectronics-specific models can be used to verify and validate properties throughout the planning and design phases of supply chain integration; to demonstrate the impacts of attacks, defenses, and control system faults; and, to identify the costs associated with design tradeoffs due to security risks and mitigations. Formal design specification and verification also provides the microelectronic industry an avenue for explainability of security decisions across the supply chain and mitigation of vulnerabilities at the design stage.

Second, we must incorporate traceable integrity into the microelectronic supply chain. Microelectronics manufacturers have requirements beyond their individual plants that extend to their entire supply chain network. This supply chain network is a high-value target for

[7] https://www.researchgate.net/publication/255965523_Integrating_Software_Assurance_into_the_Software_Development_Life_Cycle_SDLC

adversaries, as it serves as the conduit for proprietary intellectual property, sensitive commercial/operational data, and is the ideal injection point for untrusted components and materials. Hence, we need to develop and deploy innovations that provide end-to-end traceable integrity of the final product throughout the supply chain.

A cyber-physical passport (CPP) architecture should be developed and deployed to capture design details, equipment status, product history, and energy consumption and emissions profiles using a unifying data model, enabling interoperability and optimization across suppliers or original equipment manufactuers of various sizes and complexity. The cyber-physical passport is a foundational identity and activity validation element within a framework designed to support multiple parties.

As an example, the key element of provenance for the supply chain networks is a single manufactured "part". The provenance data relating to a part, such as: its components, origin, design, manufacturer, software associated with the manufacturing process, data associated with the manufacturing process, quality control data, ambient data, energy and emissions efficiency, etc., must all be securely captured and stored in the local manufacturing node. That information can be further used for analysis by using privacy-preserving techniques across multiple supply chain nodes to infer overarching properties such as productivity, product integrity, quality, and energy efficiency of the manufacturing process.

However, this information is rarely available for parts that originate from untrusted nodes in the global supply chain. In such cases, untracked (and also tracked) components are analyzed when reaching controlled supply chain nodes (e.g., compare the spectral analysis of a golden part and the untracked component) and the results of such analysis are recorded in a CPP to enable further integrity verification across the supply chain.

These cyber innovations can be applied to microelectronic manufacturing and semiconductor fabrication to prevent unauthorized changes to the microelectronic manufacturing and/or to verify the integrity of the design. The CPP automatically collects provenance information and analysis artifacts that enhance the quality of products, improves productivity of systems, reduces energy consumption, and significantly increases the cybersecurity of systems, operations, and supply chains.

Securing defense-critical supply chains, built on resilient and sustainable microelectronics fabrication and deployment, is a national imperative and one that requires an investment in basic and applied research, development, and deployment into industries in (and out of) the DIB. Critical next steps include the development of pilots for revolutionary concepts in a new formal verification model and the CPP concept for chain of custody. Critical infrastructure leadership should take action with a sense of urgency. Working in conjunction with the Under Secretary for Acquisition and Sustainment, the Assistant Secretary of Defense for Research and Engineering

should establish pilot programs with the Defense Advanced Research Projects Agency and the service labs to build and test both concepts in legacy and new system development.. Additionally, the Pentagon may be aware that an existing Manufacturing Innovation Institute is piloting, with the semiconductor industry, cyber innovations to provide *verifiable security properties and guarantees of physical functions to build a more cyber secure, resilient and efficient microelectronics supply chain.*

While all of these efforts are early in development (technology readiness level 2-3), they can be expedited as a national security imperative. Congress should review the results of these pilots and provide authority and funding to scale these architectural constructs on the nation's highest defense priorities. The Semiconductor Industry Association recognizes that the industry needs to invest an astounding $3 trillion in research and development and capital expenditure over the coming decade to meet increasing demands for semiconductors.[8] It is imperative to leverage these investments and emerging cybersecurity innovations in order to build risk-resilient high-technology supply chains from design to manufacture to operation. Designing supply chains for resilience is likely to be a much more cost-effective and profitable strategy than trying to retrofit existing ones.

[8] Semiconductor Industry Association, Strengthening the Global Semiconductor Supply Chain in an Uncertain Era, April 2021. See also Ronald Reagan Institute, A Manufacturing Renaissance: Bolstering U.S. Production for National Security and Economic Prosperity: Report of the Task Force on National Security and U.S. Manufacturing Competitiveness