Moving to a Zero Trust Supply Chain

Assurance Through Fabrication

06 August 2019

Mr. Neil W Schumacher Partner, GBS Public Sector Services, IBM Global Business Services

Dr. Jim Stathis Principal Investigator, DoD Advanced Technology Center, IBM Research

Dr. Effendi Leobandung Technical Director, DoD Advanced Technology Center, IBM Research

DoD Advanced Technology Center in Albany, NY



A trusted, assured, and protected ecosystem for advanced technology

IBM



IBM Aligned with Emerging DoD Requirements

- Developed the original security protocols for 1. **Trusted Foundry accreditation**
- 2. PMO: Defined the support and operational needs of the systems through the product lifecycle
- 3. Information Assurance: systems architecture and infrastructure, integration plans with commercial systems
- Manufacturing Assurance: Development of 4. CLASS manufacturing processes
- 5. Secure Facilities, Secure Network capabilities
- Targeted risk-based framework for 6. assessment of ongoing operations and gro of capabilities

owth	
(1) Monitoring and Governance • DCSA • NST controls and CLI • TAR • NST • NST • NST • NST • NST • A CLI • A CL	1) Assessment -People -Processes -Tools
- Controls - Orngliance - Verification - Verification - Verification - Verification - Verification - Verification - Verification	2) Implementation · Develop Security · Milgailons ge ge ge ge ge ge ge ge ge ge

Benefits:

Design methods and IP

Advanced recimologies				
Augment Trusted capabilities by creating new models to accredit commercial facilities to enable supplier diversification in Design, Mask and Fab (fully-enabled 14nm flow)				
Chip Design	Mask	> Foundry	> Test	
 Accredited Classified ASIC Design Centers (Burlington, WMA) Server Infrastructure, EDA tools, Design Kits to the 14nm node Seats 30 engineers, distributed Design Center model 	 Maintain accredited Trusted Mask capabilities Diversify Mask supply chain with additional US-based providers Enable new models for supplier qualification and security overlay 	Maintain Trusted access to current range of technologies in 200/300mm fabs Build security model for Trusted access to leading-edge 14nm commercial facilities Hybrid Process flow – new logistics and data	 Maintain Trusted and Classified Test and Packaging services (including Bromont) Enhance support production volume requirements Diversify tester platforms and service providers, support 	
Ready to host Secure		controls	widest range of	

Distributed Design Center Model

Accredited 14nm Foundry Test & Packaging

 Automation and embedded security

protocols augment

commercial controls

sensitive programs

2.5/3D Multi-chip

Assembly

module Packaging and

Advonced Technologies



Evolving Threat Landscape

Sample Event - Business Data Leaks

 Major DIB manufacturers had recent major data exposure which leaked trade secrets, IP libraries, factory layouts, blueprints, automation methods, robotic specs

Sample Event - Digital Connections & IoT

 Engineering service provider was breached, leaking all NDAs, describing details of sensitive work engagements with 100 companies, including SPI

Sample Event - National Attacks

 A Chinese state-owned company and a Taiwanese company were charged with conspiring to steal trade secrets from a U.S. chipmaker

Framing the Problem

- Zero Trust can open a broader range of technology offerings
- However, risk acceptance and mitigation strategies need to be properly measured against probability and consequence
- Defining risk for microelectronics fabrication will ultimately be determined by *national security imperatives*









- Metrics and data for fabrication assurance decision making can be developed
- Increased traceability and provenance will enable automated model with significantly reduced risk
- Data driven assurance will improve confidence
- Integrated policy and standards <u>are needed</u>