Next Steps

Serge Leef

CHIPS for AMERICA

Serge Leef

Microsoft Azure

Secure Microelectronics Design, Implementation, and Fabrication Enablement on the Cloud

Previously

- **DARPA**

  Secure Silicon, Next Generation Design Tools, and Domestic Microelectronics program

- **Siemens EDA (formerly Mentor Graphics)**

  Vice President of New Ventures: Strategies and Building Successful businesses around Design Automation Products

- **Silicon Graphics: High Speed Simulation Tools**
- **Microchip: Functional and Physical Design and Verification tools**

Challenges and Opportunities in Commercializing Security Research

Who Needs Help with **Hardware Security**

Huge merchant semiconductor companies *(Intel, Broadcom, Qualcomm…)*

- See the critical need and have large expert teams to create custom solutions

Mid-size semiconductor and system companies *(NXP, Cisco, Nokia…)*

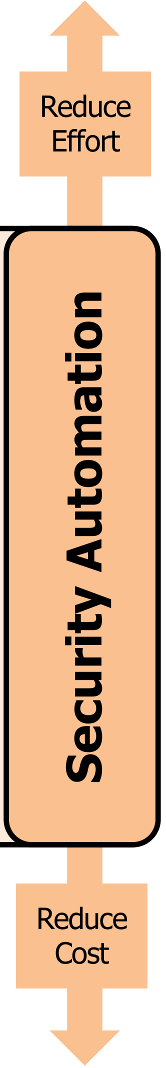
- Recognize problems but lack expertise and sufficient economic motivation

Defense contractors *(Honeywell, NG, Lockheed…)*

- Possess deep, but limited, expertise (craft) unevenly applied to specific chips

System integrators *(Ring, Fitbit, August…)*

- No interest due to time-to-market focus and lack of in-house competency

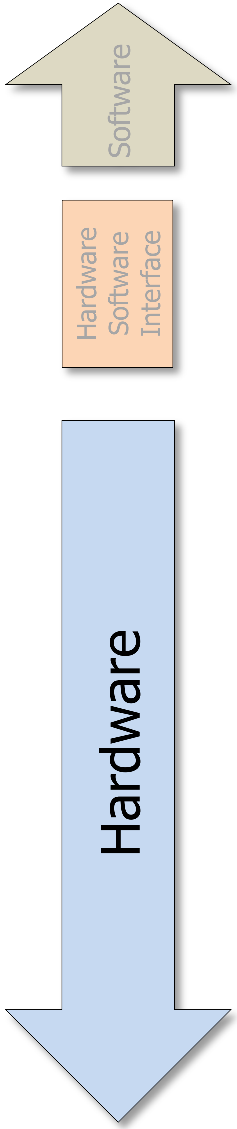


Reduce Effort

Security Automation

Reduce Cost

Attack Surface **Reference Model** SoC/ASICs)



- Substantial efforts are on-going in the software community

- Alteration of system behavior based on software-accessible points of illicit entry that exist due to hardware design weaknesses or architectural flaws

- **Side Channel** – extraction of secrets through physical communication channels other than intended
  (assumption: attackers are able to "listen" to emissions) → Economic Attackers

- **Reverse Engineering** – extraction of algorithms from an illegally obtained design representation
  (assumption: attackers have access to design files) → Economic Attackers *and* Nation States

- **Supply Chain** – Cloning, counterfeit, recycled or re-marked chips represented as genuine
  (assumption: attackers can manufacture perfect clones) → Economic Attackers

- **Malicious Hardware** – insertion of secretly triggered hidden disruptive functionality
  (assumption: attackers successfully inserted malicious function(s) into the design) → Nation States

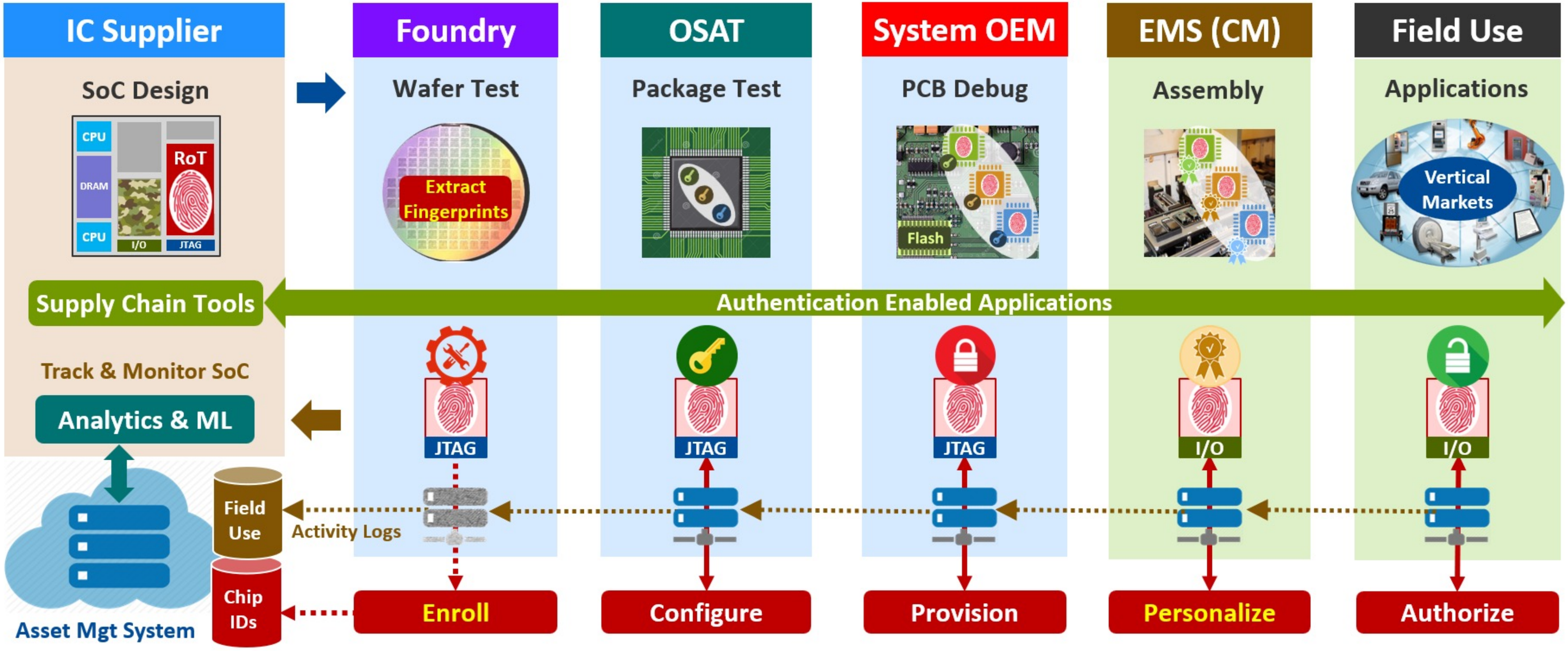
Hardware Security hasn't Developed as a Business

- **Security is a difficult value proposition**
  - Security is viewed as an abstract threat by the ASIC/SoC community
  - Half dozen hardware security companies generating << $20M each
  - Most of the revenue comes from penetration testing
  - Some business in professional services / consulting / IP licensing
  - **Product** business is minimal, mainly to advanced R&D customers
  - No standards, regulations or ecosystems – capabilities, not solutions

- **Urgency and essentiality are lacking**
  - Selling vitamins is much harder than selling heart medication
  - Decision hinges on **Fear** (liability) vs. **Greed** (area, speed, power)

Solution? **Infuse standards and regulations to tilt the equation**

Secure Silicon Flow Vision



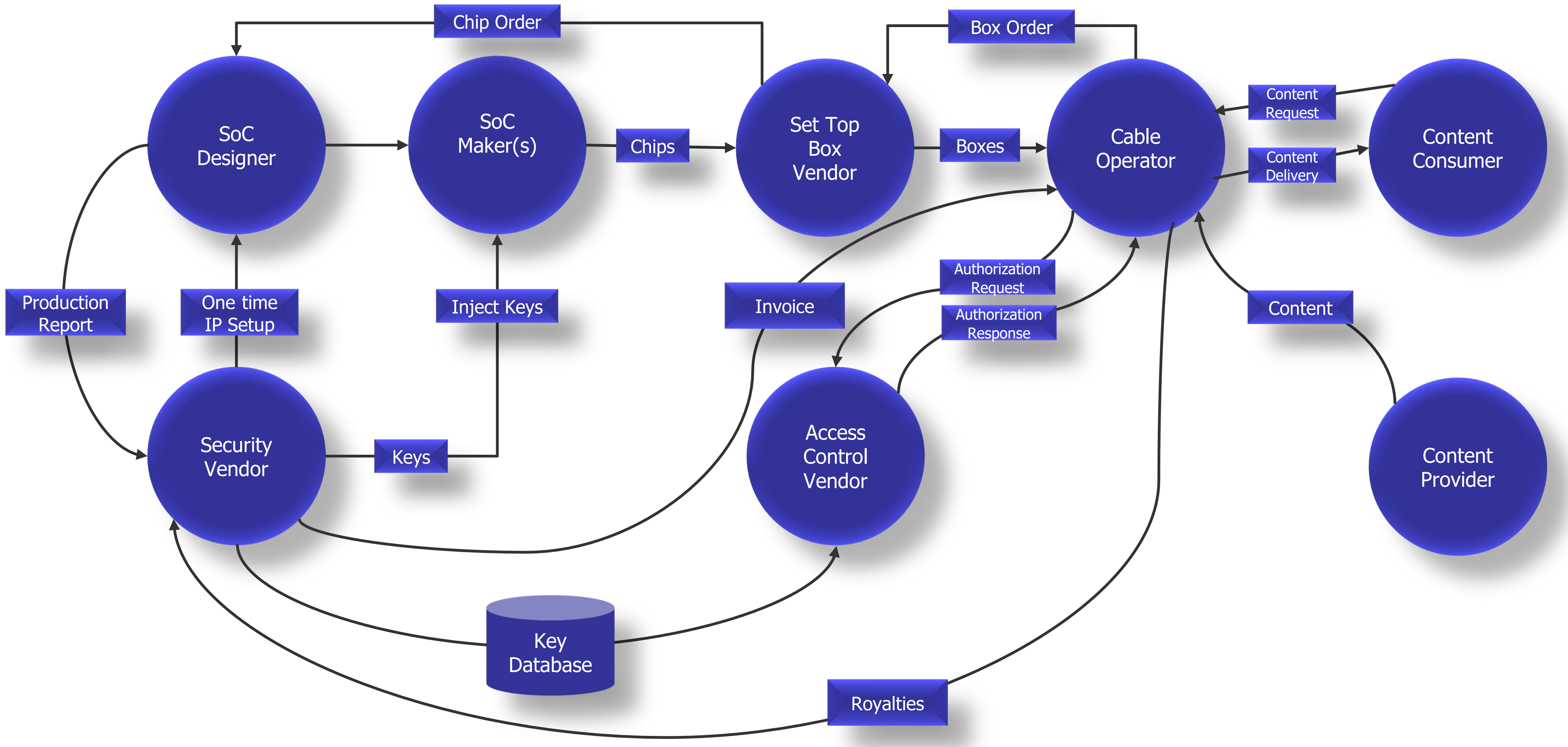
Source: Mentor Graphics, 2017

We Must Find Ways to **Drive an Ecosystem**

- **Standards**
  - PUF and error correction system interfaces
  - Edge to cloud enrollment, authentication and other protocols
  - Lifecycle data management and analytics interfaces
  - Logic encryption, obfuscation, camouflaging control interfaces
  - Digital circuit watermarking to IJTAG interfaces
  - …

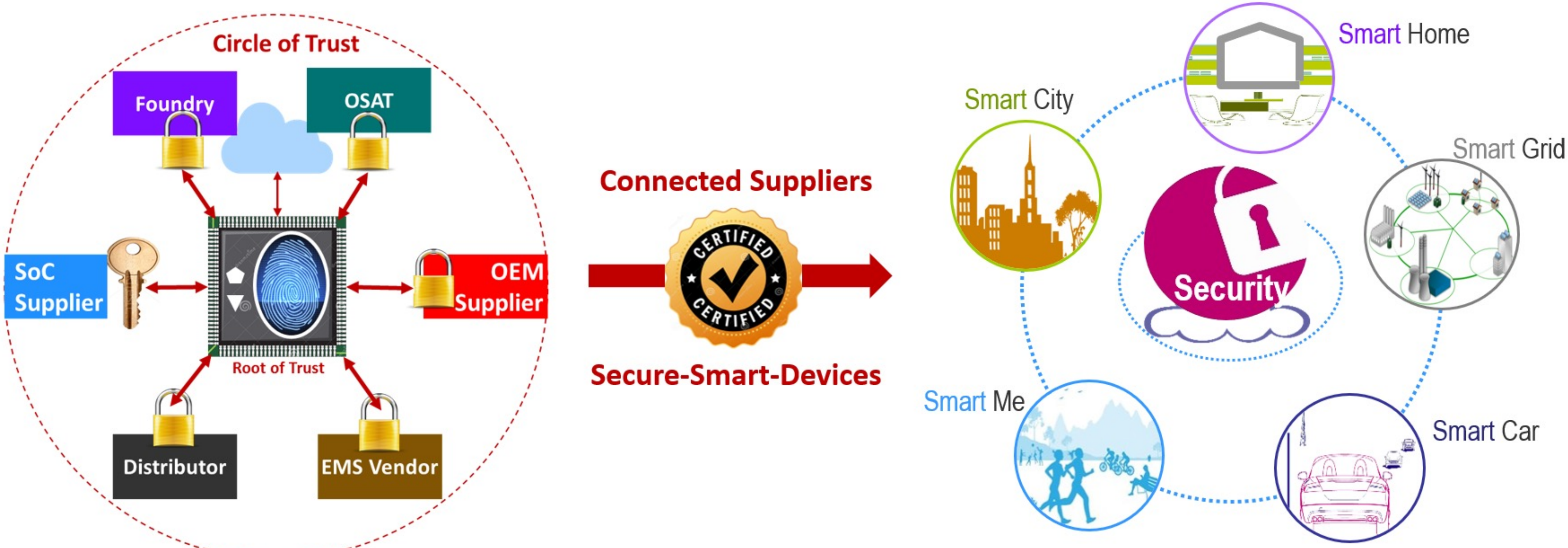
- **Regulation**
  - Government as a customer (ex: DoD) can demand compliance
  - Documentation of compliance must be defined in the acquisition process
  - Quantifiable trust scoring can drive government purchasing criteria
  - Demonstrable attack resistance collateral
  - …

Digital Broadcast Ecosystem example



Secure-Connected **Collaboration** Needed in

Vertical Markets Where Security has Clear Monetary and Legal Value



*Source: ST Microelectronics

Supply Chain Trusted Ecosystem Alliance is essential for Security

Q&A

Next Steps for HW Security Workshop

Sanjay Rekhi

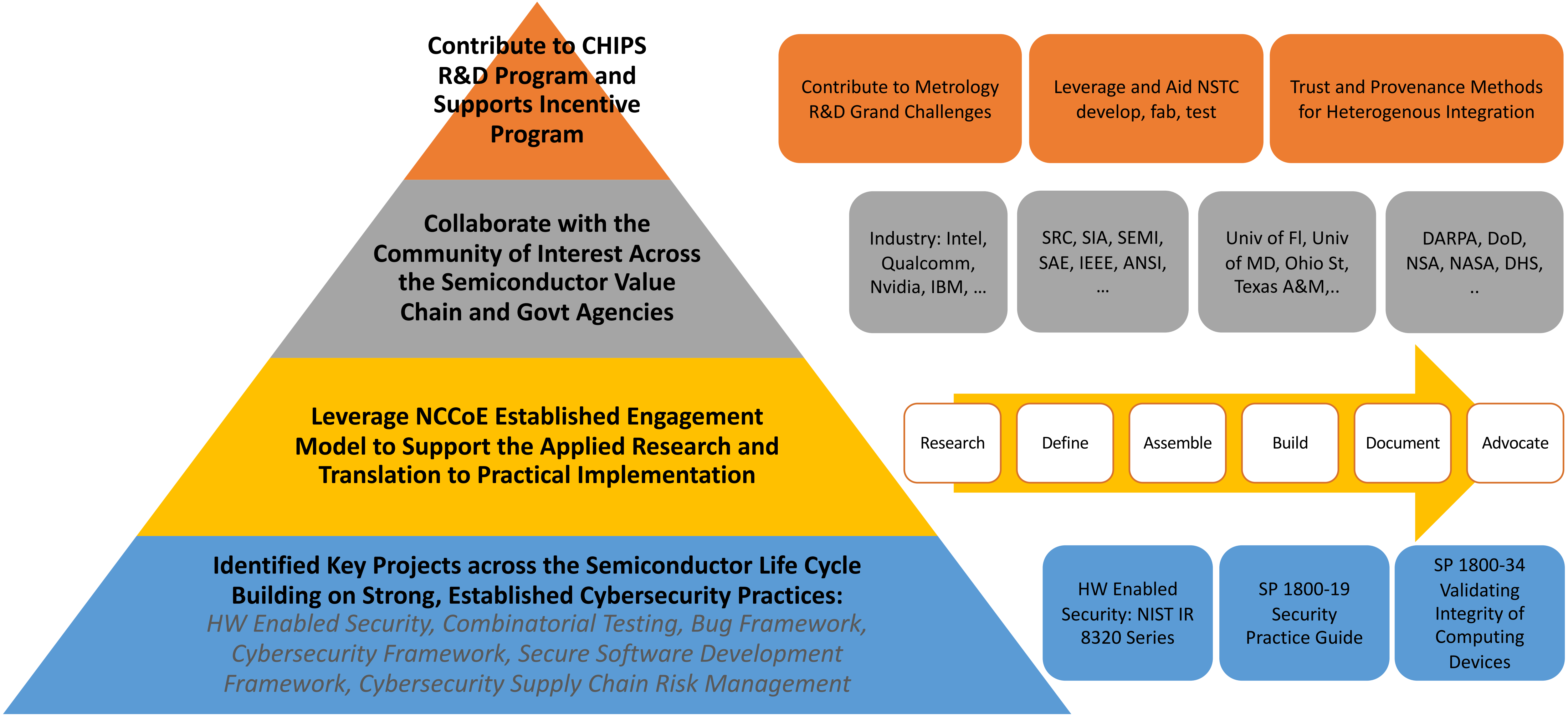
Group Leader, Security Components and Mechanism

National Institute of Standards and Technology

What’s Next?

- Synthesize NIST report
- Identify projects
  - directions on how to take them forward
  - request for stakeholder participation as we kick off initiatives
- Continue our engagement
- Feedback/Suggestions/Ideas: hwsec@nist.gov

Collaboration with the Community to Develop Guidance and Practical Implementations to Support Industry Needs



Contribute to CHIPS R&D Program and Supports Incentive Program

Contribute to Metrology R&D Grand Challenges

Leverage and Aid NSTC develop, fab, test

Trust and Provenance Methods for Heterogenous Integration

Collaborate with the Community of Interest Across the Semiconductor Value Chain and Govt Agencies

Industry: Intel, Qualcomm, Nvidia, IBM, …

SRC, SIA, SEMI, SAE, IEEE, ANSI, …

Univ of Fl, Univ of MD, Ohio St, Texas A&M,..

DARPA, DoD, NSA, NASA, DHS, ..

Leverage NCCoE Established Engagement Model to Support the Applied Research and Translation to Practical Implementation

Research → Define → Assemble → Build → Document → Advocate

Identified Key Projects across the Semiconductor Life Cycle Building on Strong, Established Cybersecurity Practices:
HW Enabled Security, Combinatorial Testing, Bug Framework, Cybersecurity Framework, Secure Software Development Framework, Cybersecurity Supply Chain Risk Management

HW Enabled Security: NIST IR 8320 Series

SP 1800-19 Security Practice Guide

SP 1800-34 Validating Integrity of Computing Devices https://csrc.nist.gov/Projects/hardware-security

hwsec@nist.gov

@NISTcyber