The Future of Advanced (Secure) Computing

This material is based upon work supported by the Assistant Secretary of Defense for Research and Engineering under Air Force Contract No. FA8721-05-C-0002 and/or FA8702-15-D-0001. Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Assistant Secretary of Defense for Research and Engineering.

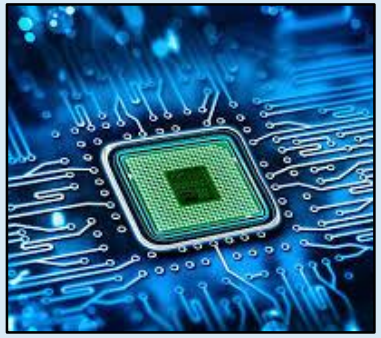
Dr. Paul Monticciolo

MIT Lincoln Laboratory

5 March 2018

Future Commercial Computing Technology Drivers

Hardware

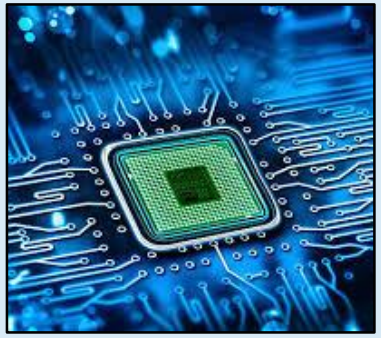


Software

Communications

Future Commercial Computing Technology Drivers

Hardware

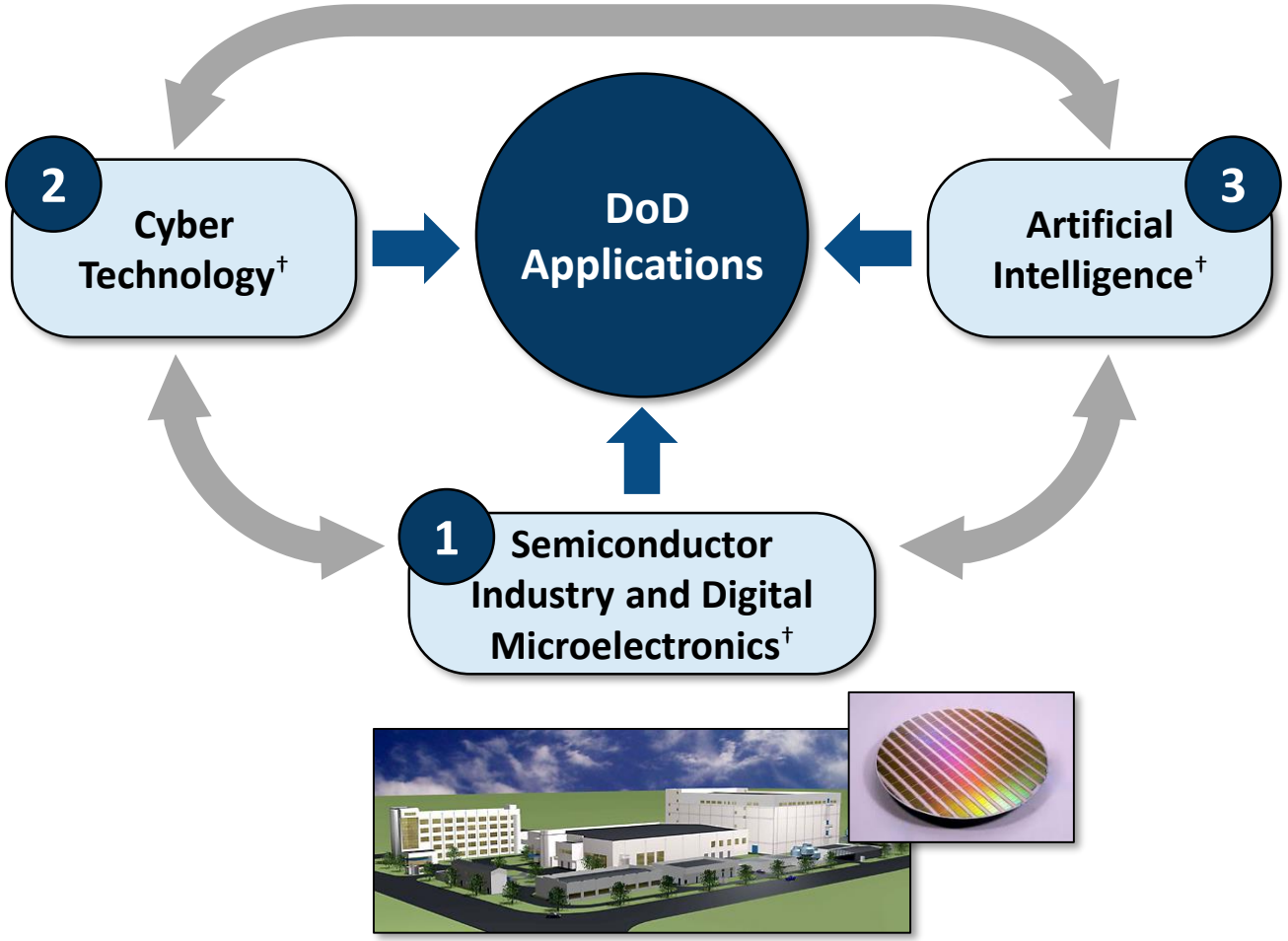


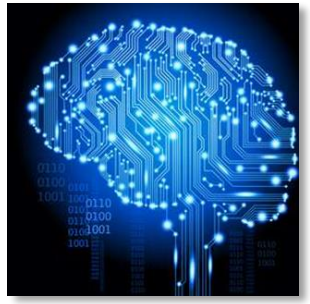
Software

Communications

Security

The *Digital Triad* for National Defense





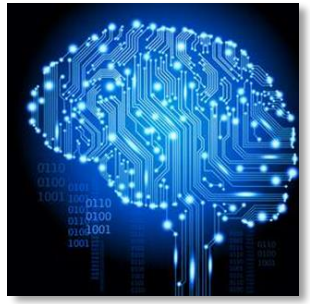
Challenge: independent development in each Triad component limits required secure computing solutions

† Addressed in other ARTS 18 sessions

Secure Computing Directions to Enable the *Digital Triad* for National Defense

Cyber Technology

1. ***Co-design*** **across Triad to meet performance and cost goals for DoD applications**
2. **Exploit advances in commercially developed technologies where possible**
3. **Leverage trusted DoD foundries to fabricate necessary components**



Artificial Intelligence

U.S. Semiconductor and Microelectronics Industry

Expanding the Digital Triad Ecosystem for Advanced Secure Computing

Secure Processing

Challenges in Building Secure Hardware Platforms

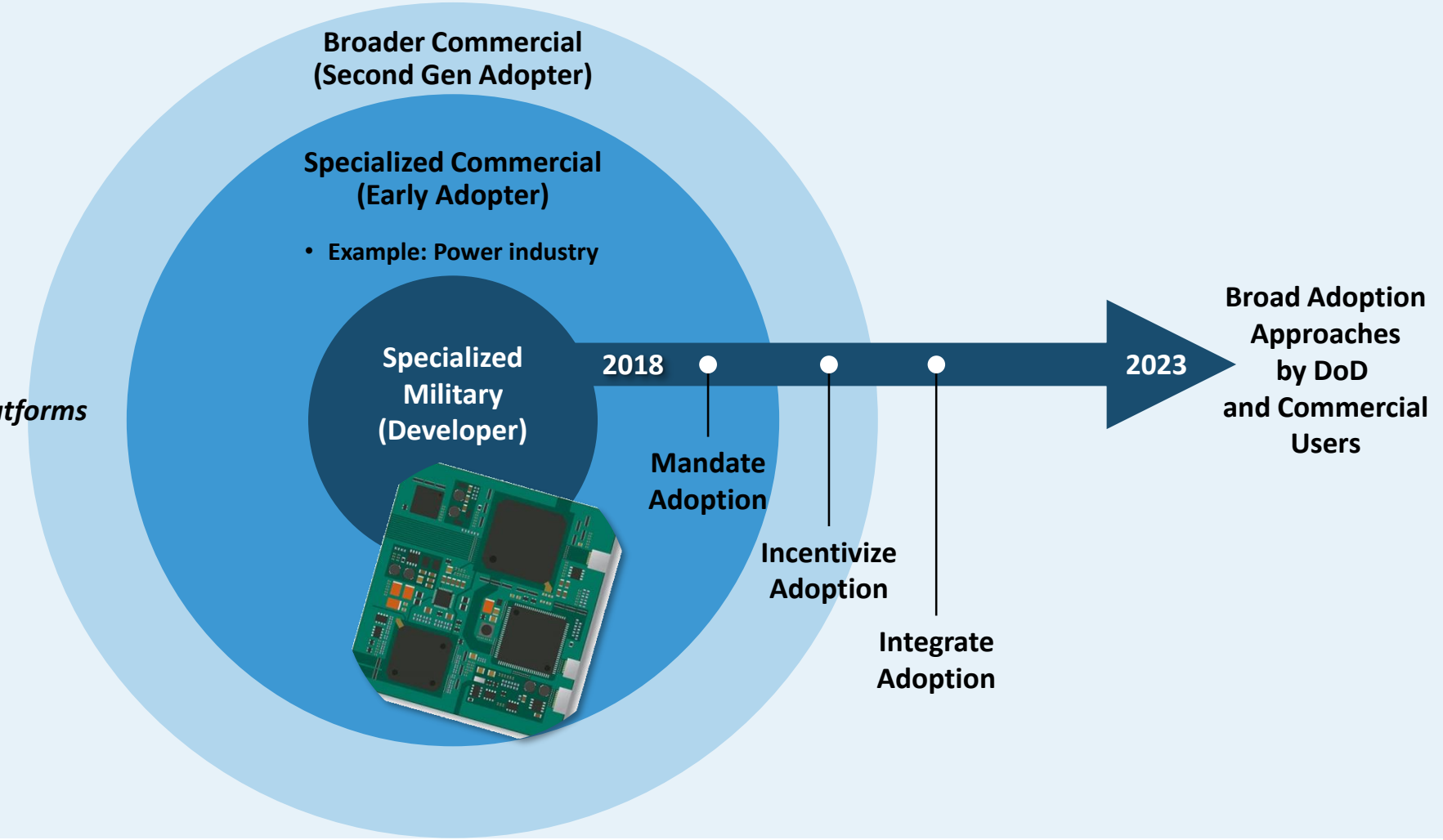
An Inherently Secure Computer

- New hardware architecture
- New software/operating system
- Trusted HW manufacturing

Advanced Data Protection

Data-Centric Secure Computing

- Crypto-bound, efficient data provenance
- Post-quantum cryptography
- Seamless crypto-key management
- "Data-centric" security



Expanding the Digital Triad Ecosystem for Advanced Secure Computing

Digital Triad synergy addresses critical defense applications and incentivizes future broader commercial adoption

The Artificial Intelligence Era

Quantum Computing with Trapped Ions and Superconducting Qubits
Data Science and Technology Research Environment

- National-security focused AI technologies
- Coupled to secure computing and vanguard U.S. microelectronics

Secure Processing

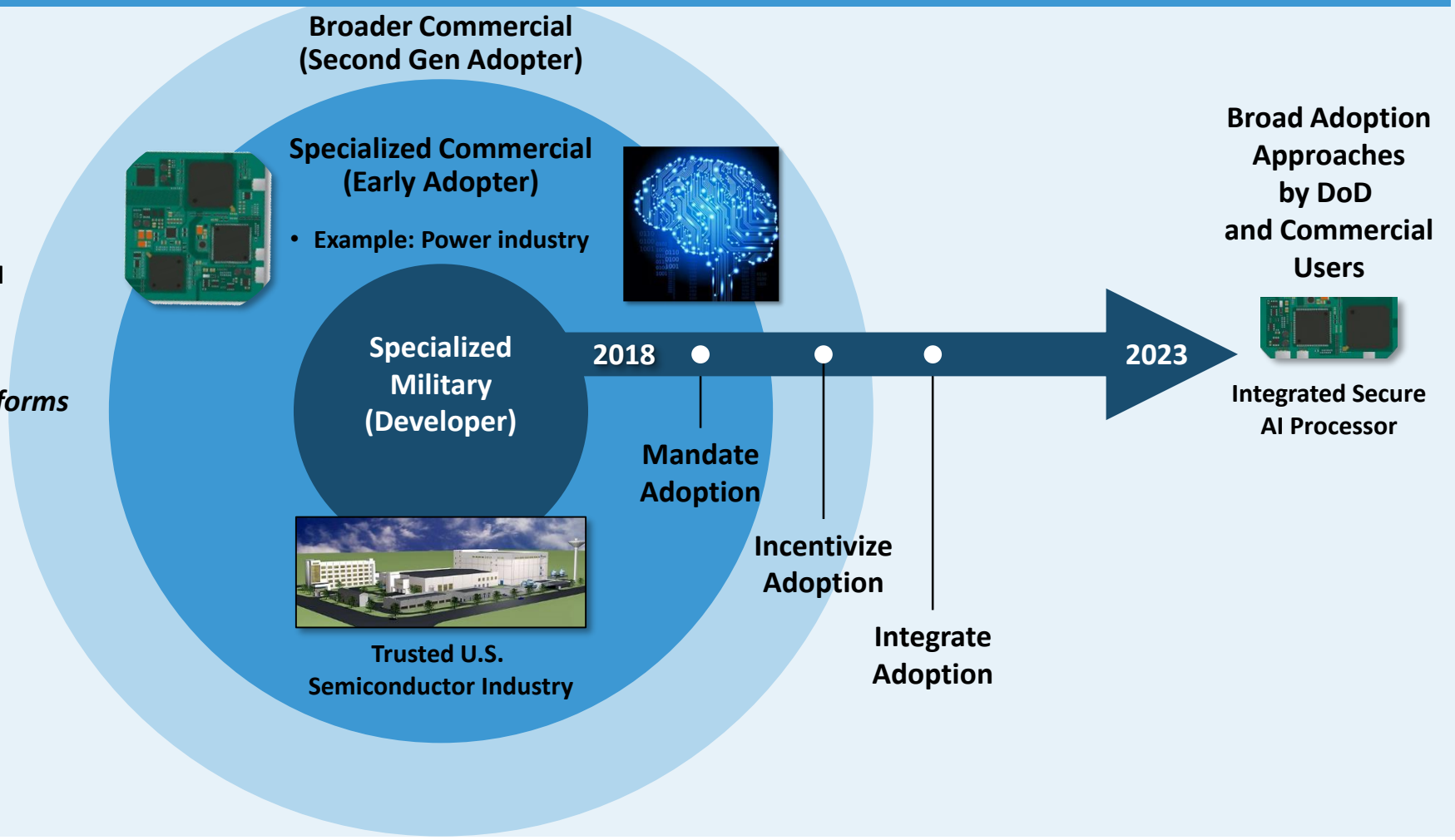
Challenges in Building Secure Hardware Platforms
An Inherently Secure Computer

- New hardware architecture
- New software/operating system
- Trusted HW manufacturing

Advanced Data Protection

Data-Centric Secure Computing

- Crypto-bound, efficient data provenance
- Post-quantum cryptography
- Seamless crypto-key management
- "Data-centric" security

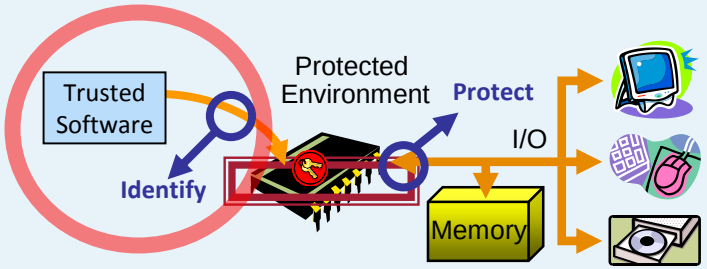


Session Overview

Keynote

Challenges in Building Secure Hardware Platforms

Prof. Srini Devidas

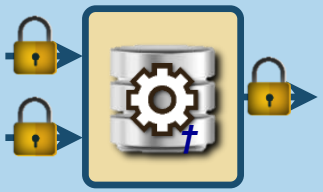


Presentations

Security

An Inherently Secure Computer

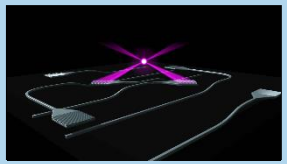
Hamed Okhravi



Data-Centric Secure Computing

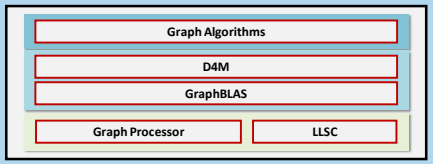
Emily Shen

Advanced AI Technologies



Quantum Computing

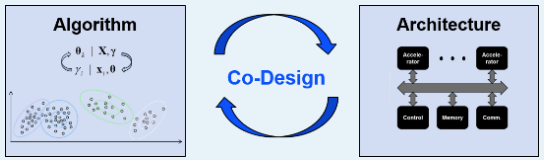
Eric Dauler



Data Science and Technology Research Environment

Vitaliy Gleyzer

Posters

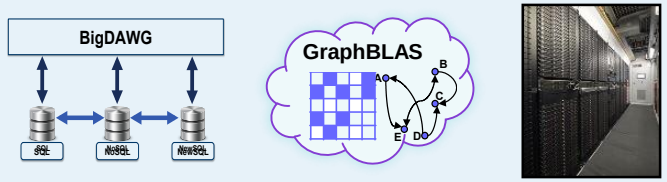


Custom Processor Architectures for Probabilistic Programming

William Song/Michael Hurley

Efficient Computing for the Internet of Things (IoT)

Karen Gettings/Huy Nguyen



Big Data Processing for DoD IoT and AI

Siddharth Samsi