Building Mission Assurance with Trusted Suppliers

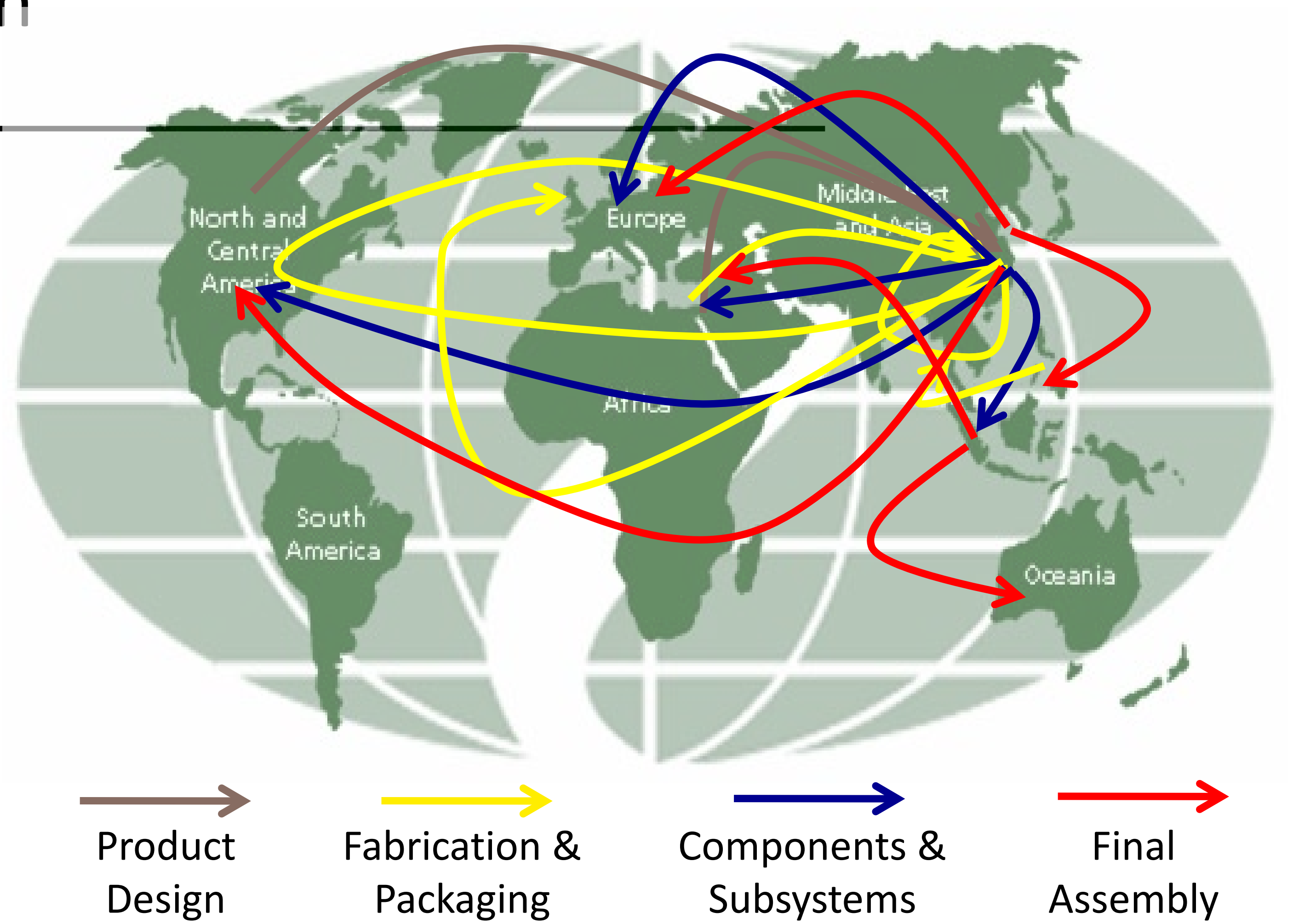
Systems and Mission Engineering Conference

October 30, 2024

Distribution Statement A: Approved for public release

A Global Supply Chain

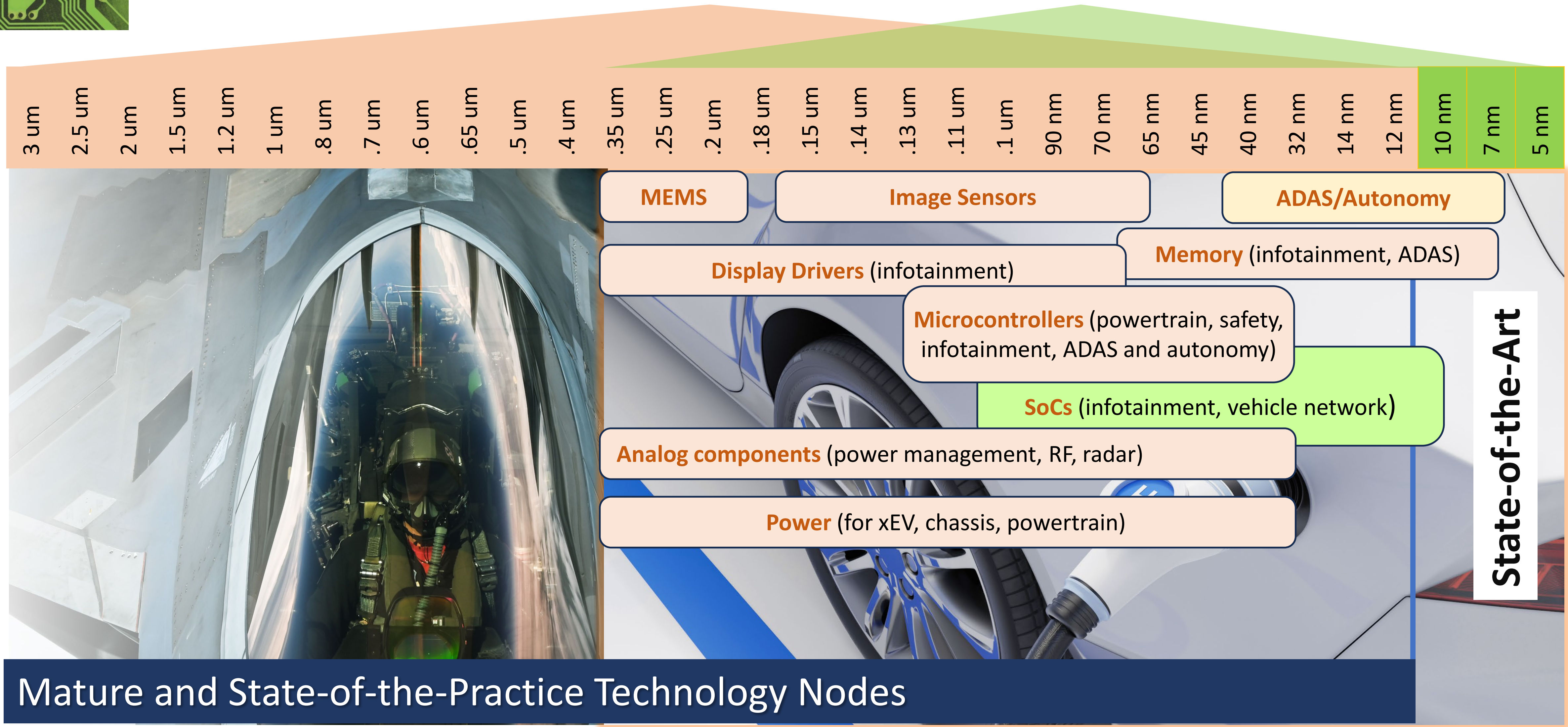
- Disruptions in the global supply chain, intentional or not, can greatly impact business and national security
- Defective and counterfeit parts are growing concerns and testing measures are inadequate
- Domestic systems developers can experience decreased ability to design and innovate information and communication technology



The sheer number of suppliers for a single electronic component makes security challenging, if not impossible, for commercial products and presents great opportunity for mischief

Distribution Statement A: Approved for public release

Trusted Supplier - Auto Technology Nodes



3 um, 2.5 um, 2 um, 1.5 um, 1.2 um, 1 um, .8 um, .7 um, .6 um, .65 um, .5 um, .4 um, .35 um, .25 um, .2 um, .18 um, .15 um, .14 um, .13 um, .11 um, .1 um, 90 nm, 70 nm, 65 nm, 45 nm, 40 nm, 32 nm, 14 nm, 12 nm, 10 nm, 7 nm, 5 nm

MEMS

Image Sensors

ADAS/Autonomy

Memory (infotainment, ADAS)

Display Drivers (infotainment)

Microcontrollers (powertrain, safety, infotainment, ADAS and autonomy)

SoCs (infotainment, vehicle network)

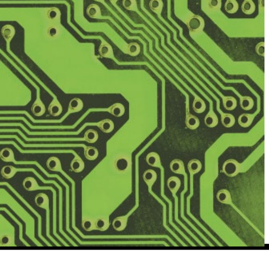
Analog components (power management, RF, radar)

Power (for xEV, chassis, powertrain)

State-of-the-Art

Mature and State-of-the-Practice Technology Nodes

Source: Semiconductor Trends in Automotive, Yole Intelligence

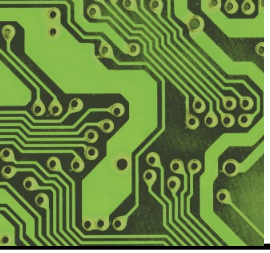


CISA ICT-SCRM Task Force – Threat Focus SCRM

- Executive Order on Securing the Information and Communications Technology and Services Supply Chain (E.O. 13873), May 2019
- ICT-SCRM cybersecurity overlay approach to defining a threat-focused selection of cybersecurity controls
- Deliberate adversary compromise of a component or service through the supply chain.
- Supply Chain Risk is…

> The risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of an item of supply or a system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of a system (The Ike Skelton National Defense Authorization Act for Fiscal Year 2011, Section 806).
>
> - CNSS directive (CNSSD) 505 [9]

Distribution Statement A: Approved for public release

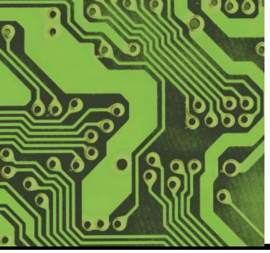


ICT-SCRM Task Force Hardware Threats

- FOCI Compromise of Pre-silicon Hardware (HW) Design
- Compromise of Pre-silicon HW Design
- Compromise of HW Back-end Design, Verification, Fabrication, Test, Packaging, or Distribution
- Compromise of HW During Personalization or Programming
- Compromise of HW During Board Integration
- Compromise of HW Key Architecture Compromised
- Use of High-Risk Markets for Scarce, Obsolete, or Legacy Products

Trusted Suppliers Mitigate These Threats

Source: AEROSPACE REPORT NO. TOR-2023-00502 – REV A, *ICT-SCRM Control Overlay: A Threat Based Approach*, August 2024



Trusted Foundry and Trusted Suppliers

Trusted - Is 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.

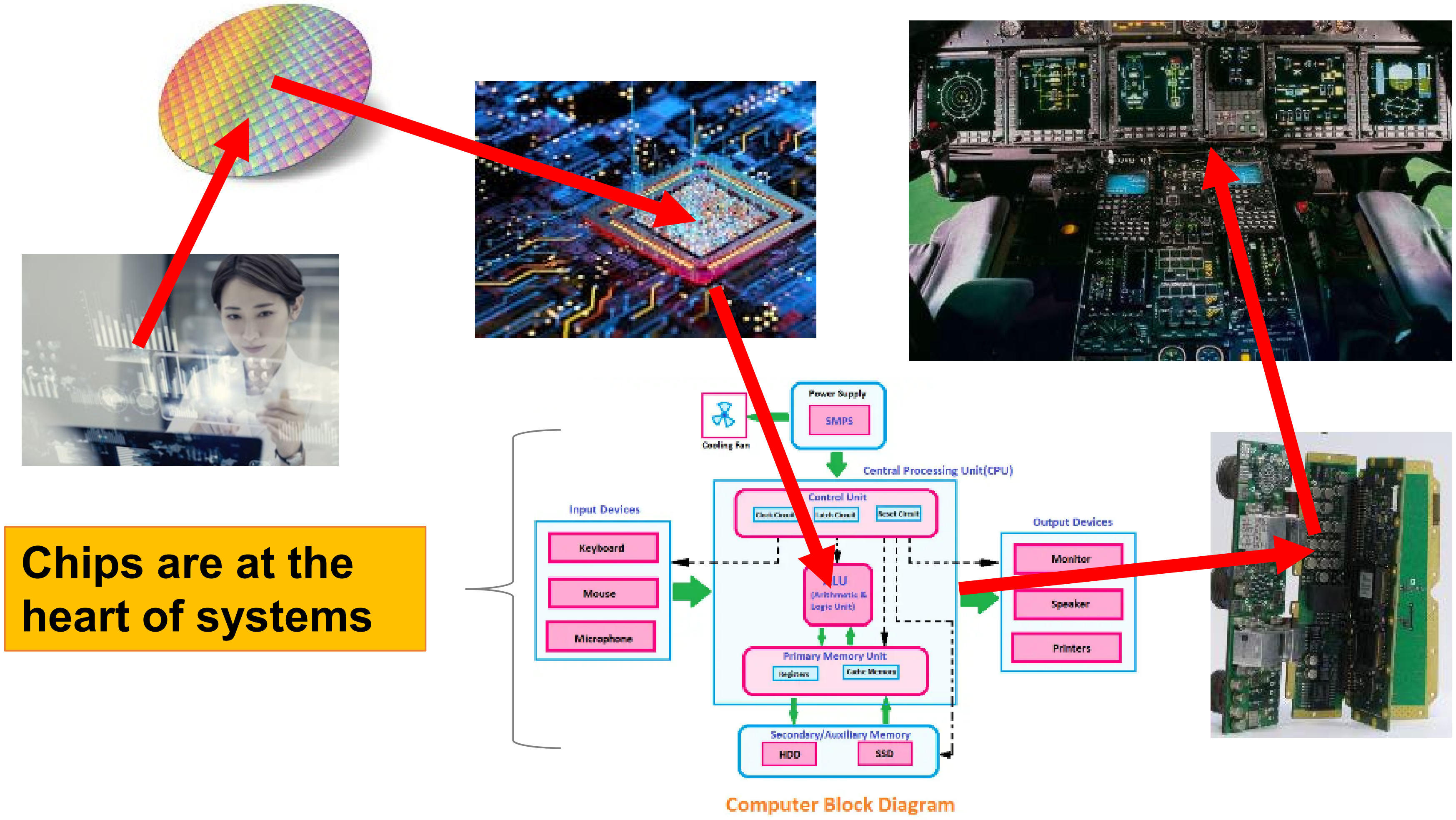
- DMEA Website /Trusted Program

- Within this context, "trusted sources" 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

Security is a Systems Engineering Task

Vulnerabilities and Attack Vectors exist at all layers of the stack

- Application
- Middleware
- OS UI
- OS Devices
- OS Drivers and runtimes
- Hypervisor
- Firmware (Bios)
- PC Boards
- Chips
- Wafers
- Design and IP

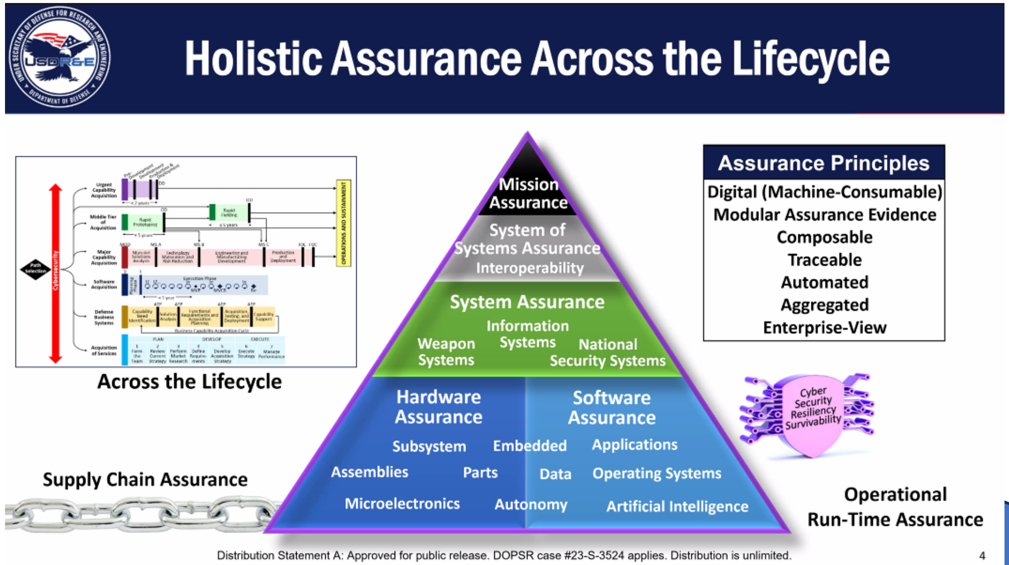


Chips are at the heart of systems

Computer Block Diagram

Source: Ezra Hall, GlobalFoundries, Trusted Supplier Networking Event, August 28, 2024

Foundation for Mission Assurance



Holistic Assurance Across the Lifecycle

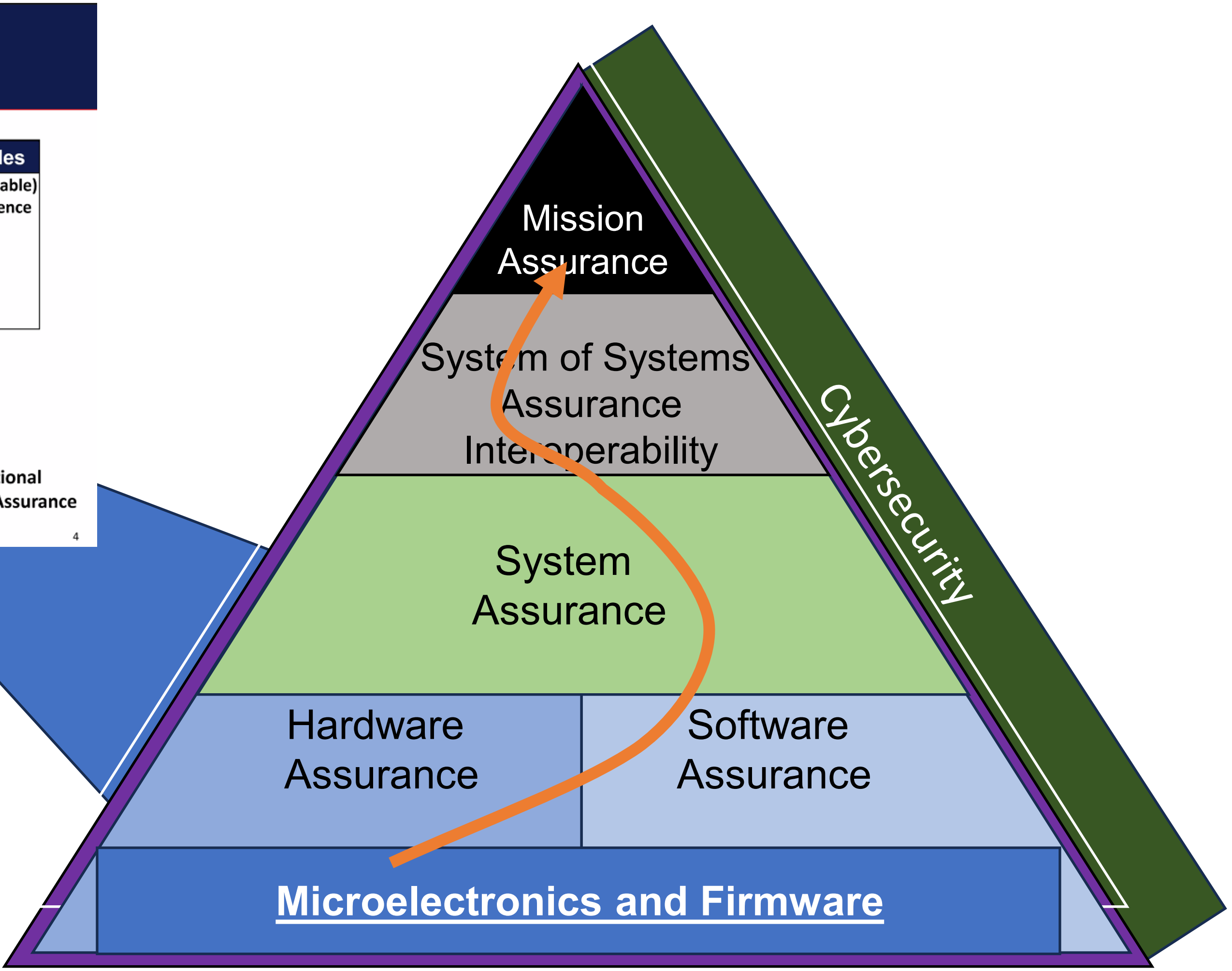
Assurance Principles

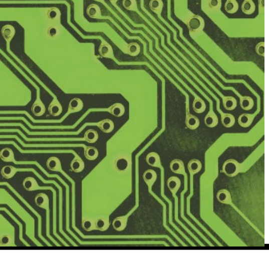
- Digital (Machine-Consumable)
- Modular Assurance Evidence
- Composable
- Traceable
- Automated
- Aggregated
- Enterprise-View

Distribution Statement A: Approved for public release. DOPSR case #23-S-3524 applies. Distribution is unlimited. 4

Joint Federated Assurance Center

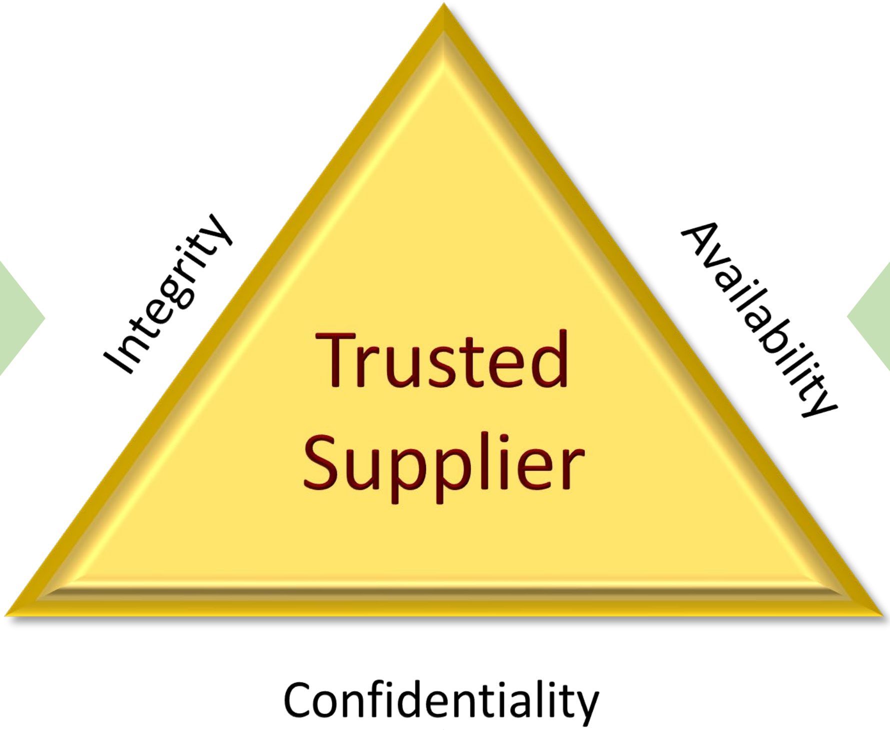
Trusted and Assured Microelectronics are the foundation of mission assurance





The Trusted Program Provides Assurance

- ✓ Prevents intentional or unintentional modification or tampering
- ✓ Provides an assured "Chain of Custody" for both classified and unclassified components



Integrity

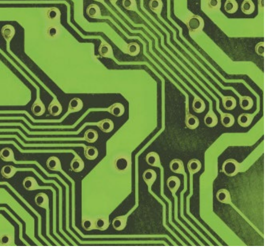
Trusted Supplier

Availability

Confidentiality

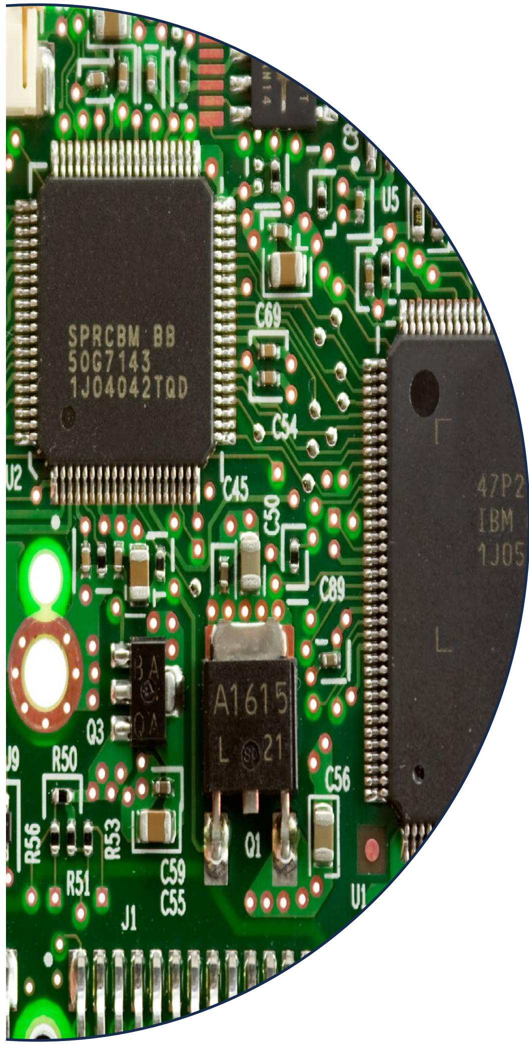
- ✓ Ensures that there will not be any reasonable threats related to disruption of supply beyond commercial lifecycles

- ✓ Protects components from unauthorized attempts at reverse engineering, exposure of functionality or evaluation of their possible vulnerabilities



Trusted Supplier DMEA Accreditation

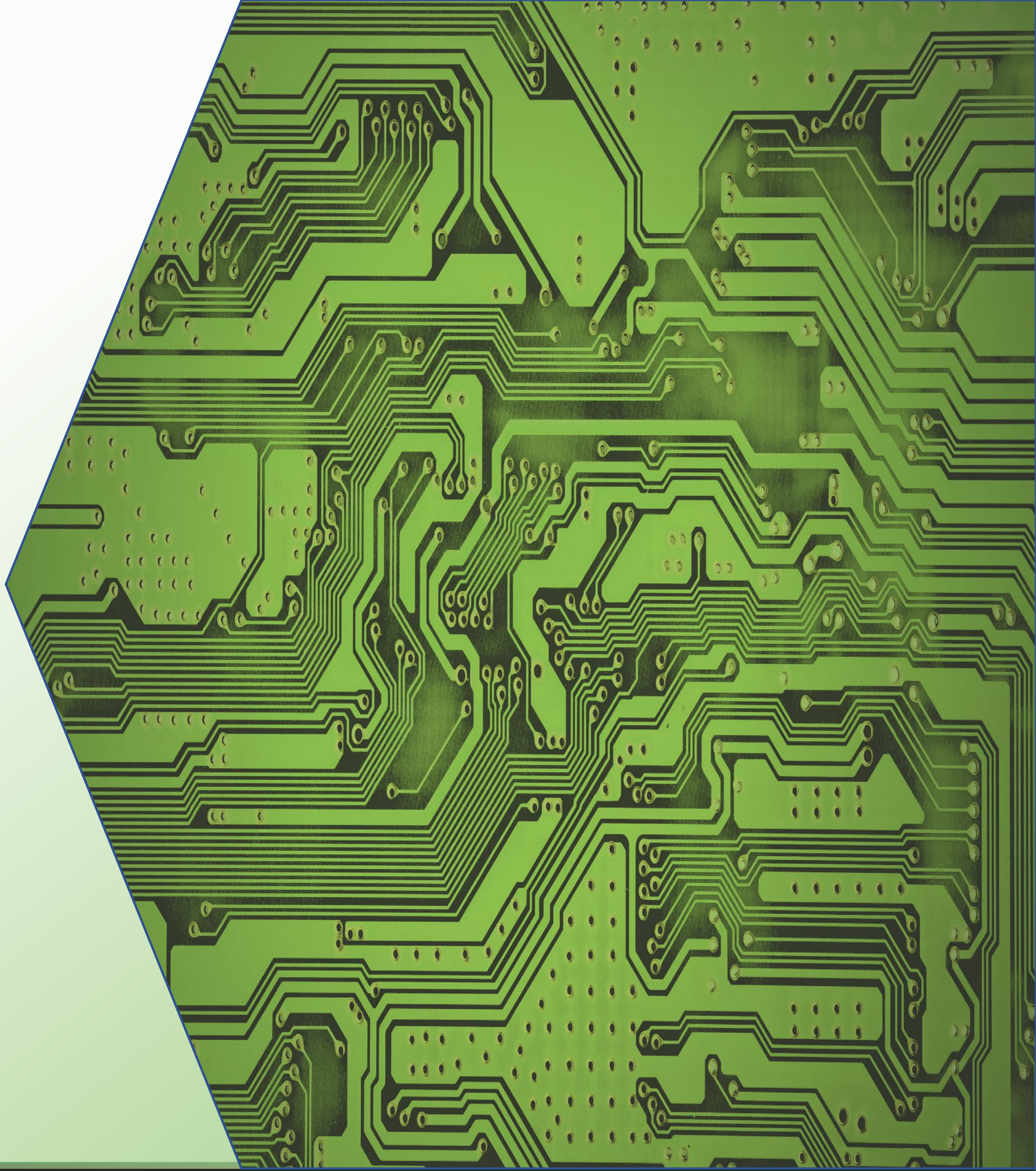
- Trustworthiness – Processes, Integrity, Quality, Data
  - Known accreditation criteria across entire microelectronics supply chain
  - Assures integrity, confidentiality, and availability for design and manufacturing
  - Design/Process/Product Integrity Provisions
    - ✓ Cleared facilities and personnel
    - ✓ Quality and Configuration Management Systems
    - ✓ Chain-of-custody plan, procedures and documentation
    - ✓ External and internal audits
    - ✓ Process controls



Trusted Supplier Panel

Trusted Supplier Steering Group

Building Mission Assurance with Trusted Suppliers



Trusted Supplier Steering Group

The TSSG is a self-formed alliance of companies that have been accredited by DMEA as trusted suppliers.

BAE SYSTEMS

NORTHROP GRUMMAN

Honeywell

IBM

skywater

cadence

PHOTRONICS

Vortex Aerospace Design & Labs, Inc.

jstf

TELEDYNE TECHNOLOGIES INCORPORATED

Building Mission Assurance with Trusted Suppliers Panel Discussion

Kaye Ortiz

CEO, Defined Business Solutions LLC

John Monk

Consulting Engineer, Advanced Technology Laboratory, Northrop Grumman Mission Systems

Dr. Brad Ferguson

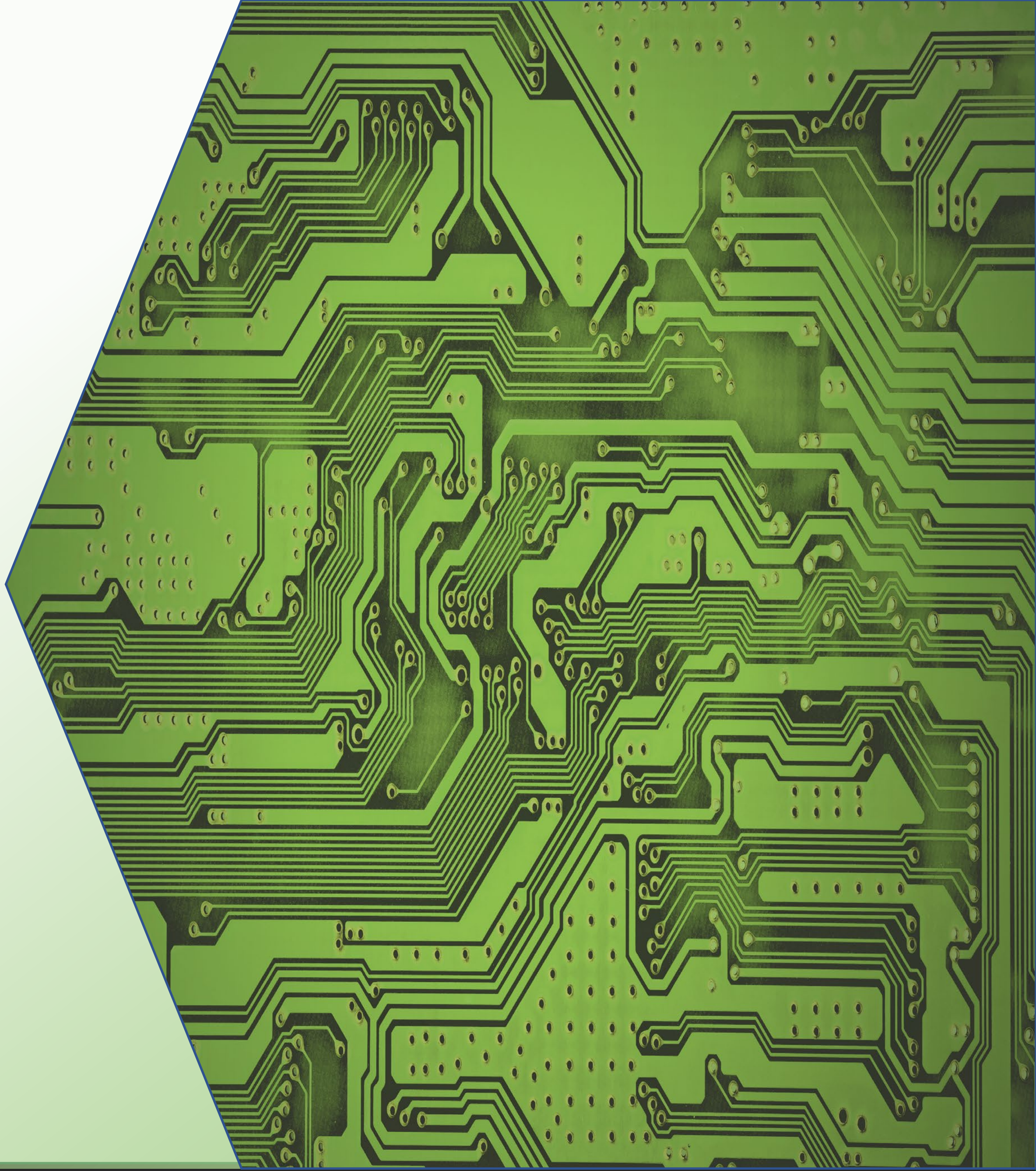
SVP Special Programs
President SkyWater Federal

Distribution Statement A: Approved for public release

Trusted Supplier Panel

Trusted Supplier Steering Group

Building Mission Assurance with Trusted Suppliers



Contacts

DMEA – DOD Program Management & Accreditation - tapo@dmea.osd.mil

DBS – Outreach (contractor) - dchesebrough@definedbusiness.com

Distribution Statement A: Approved for public release