NIST Interagency Report
NIST IR 8577

Semiconductors and Microelectronics Standards Working Group Annual Report for 2024

Annual Report to the Interagency Committee on Standards Policy by the Semiconductor and Microelectronics Standards Working Group

Jason Kahn, CHIPS Metrology Program
Chair of the Semiconductors and Microelectronics Standards Working Group

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8577

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Interagency Report
NIST IR 8577

Semiconductors and Microelectronics Standards Working Group Annual Report for 2024

Annual Report to the Interagency Committee on Standards Policy by the Semiconductor and Microelectronics Standards Working Group

Jason Kahn, CHIPS Metrology Program

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8577

May 2025

U.S. Department of Commerce
Howard Lutnick, Secretary

National Institute of Standards and Technology
Craig Burkhardt, NIST Director and Under Secretary of Commerce for Standards and Technology

NIST IR 8577
May 2025

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

NIST Technical Series Policies
Copyright, Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

Publication History
Approved by the NIST Editorial Review Board on 2025-05-20

How to Cite this NIST Technical Series Publication
Kahn, J., (2025) Semiconductors and Microelectronics Standards Working Group Annual Report for 2024. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency Report (IR) NIST IR 8577.
https://doi.org/10.6028/NIST.IR.8577

NIST Author ORCID iD
Jason Kahn: 0000-0003-3798-8668

Contact Information
jason.kahn@chips.gov

Abstract

This report of the Semiconductors and Microelectronics Working Group of the Interagency Committee on Standards Policy (ICSP) provides an overview of Federal government semiconductors and microelectronics standards activities and recommends standards focus areas and priorities for ICSP consideration. The Recommendations to the ICSP for Strategic Standards Priority Areas section of the report lists the current Standards Developing Organizations in which the Federal government participates that are related to semiconductors and microelectronics, identifies five focus areas and priorities, and identifies gaps and opportunities for possible impacts in the future. The Agencies/Offices Participating in the Semiconductors and Microelectronics Standards Working Group section of the report provides a listing of the participating agencies and entities. The Semiconductors and Microelectronics Working Group aligns with the United States Government National Standards Strategy for Critical and Emerging Technology.

Keywords

semiconductors; microelectronics; interagency; international technical standards; Federal agency standards activities; standards; standards developing organizations, SDOs, standards-setting organizations, SSOs, standards priority areas.

Table of Contents

Executive Summary....4
1. Introduction and Overview....6
1.1. Strategy and Policy for Government Engagement in Standards Development....6
1.2. Interagency Committee on Standards Policy....7
1.3. Semiconductors and Microelectronics Standards Working Group....8
1.4. Definition of Semiconductors and Microelectronics....8
2. Recommendations to the ICSP for Strategic Standards Priority Areas....9
2.1. Participation in Standards Setting Organizations (SSOs)....9
2.2. Current Focus Areas and Priorities....12
2.2.1. Supply Chain and Security....13
2.2.1.1. Secure Processors and Holistic Security....13
2.2.1.2. Authenticity and Counterfeit....18
2.2.1.3. Availability, Scarcity, and Obsolescence....21
2.2.2. Chiplets....22
2.2.2.1. Packaging and Advanced Packaging....22
2.2.2.2. Interoperability....26
2.2.2.3. Interconnects....29
2.2.3. Metrology and Measurement Science....29
2.2.3.1. Advanced Packaging....30
2.2.3.2. Future Microelectronics Manufacturing....32
2.2.3.3. Semiconductor Material Integrity and Security....33
2.2.4. Digital Twin....33
2.2.4.1. Manufacturing Process and Equipment Management....33
2.2.4.2. Supply Chain Management and Assurance....38
2.2.4.3. Quality Control....38
2.3. Gaps and Opportunities....38
2.3.1. Supply Chain and Security....38
2.3.2. Chiplets....40
2.3.3. Metrology and Measurement Science....41
2.3.4. Digital Twin....42
2.3.5. Others....43
2.3.5.1. AI accelerator chips....43
2.3.5.2. Photonics....43
2.3.5.3. Chiplets open standards and *de facto* standards organizations....44

2.3.5.4. Diminishing Manufacturing Sources and Material Shortages (DMSMS) 44
2.3.5.5. Government-Industry Data Exchange Program (GIDEP) 44
2.3.5.6. Stable EUV reflectivity structures 44
2.3.5.7. Potential adoption of larger EUV masks 45
2.3.5.8. CD-SEM structures with near-picometer (Sub-Å) tolerance 45
2.3.5.9. Overlay structures with Sub-nm tolerance 45
3. Agencies/Offices Participating in the Semiconductors and Microelectronics Standards Working Group 46
4. National Standards Strategy for Critical and Emerging Technology Strategy 47
5. References 48
5.1. References for Executive Summary and Section 1 Introduction and Overview 48
5.2. References for Section 2 Recommendations to the ICSP for Strategic Standards Priority Areas 48
5.3. References for Section 4 National Standards Strategy for Critical and Emerging Technology Strategy 53
Appendix A. Semiconductors and Microelectronics Standards Working Group 54
Appendix B. Abbreviations 56

Executive Summary

This report of the Semiconductors and Microelectronics Standards Working Group (SMSWG or Working Group) of the Interagency Committee on Standards Policy (ICSP) provides an overview of Federal government semiconductors and microelectronics voluntary consensus standards activities and outlines standards focus areas and priorities for ICSP consideration. Additionally, this report defines gaps and opportunities where the Federal government could potentially make an impact in the future.

The primary strategy for Federal agency engagement in standards development, as set out in Circular A-119 from the Office of Management and Budget (OMB) and the National Technology Transfer and Advancement Act (NTTAA) [1], focuses on reliance on private sector leadership supplemented by Federal government contributions to discrete standardization processes.

Participation by agencies in standards activities focuses on open, consensus-based, voluntary, private sector-led, and science- and engineering-informed standards that enable:

- Innovation in products and services;
- Interoperability across systems and devices;
- Open and competitive national and global markets; and
- Efficient and effective acquisition processes.

The SMSWG was chartered by the ICSP to enable interagency coordination on semiconductors and microelectronics standards efforts. Eight Federal agencies, departments, and offices participate in this interagency group.

This annual report of the Working Group to the ICSP provides current semiconductors and microelectronics standards (SMS) activities of participating Federal agencies and recommendations for strategic directions in relevant Federal standards efforts. This is done by outlining:

- The current Standards Setting Organizations (SSOs) in which the Federal government participates
- The current focus areas and priorities within SMS
- The identified gaps and opportunities for future influence in SMS.

The report's SMS focus areas and priorities section sets out four areas for consideration by the ICSP.

- **Supply Chain and Security** – The semiconductor supply chain encompasses the design, manufacturing, packaging, testing, and distribution of semiconductor devices, involving various entities across different countries. Security in this context means ensuring components' integrity, reliability, and availability throughout the supply chain. This includes protecting intellectual property, preventing tampering, and safeguarding against production disruptions. Effective security measures are vital for maintaining the trustworthiness of electronic systems used in consumer electronics,

automotive, and defense sectors. Securing the supply chain helps mitigate risks related to counterfeit components, vulnerabilities, and cyber threats.

- **Chiplets** – Chiplets are individual semiconductor dies that are integrated into a single package to function as a cohesive unit. Unlike traditional monolithic chips, which consist of a single large die, chiplets allow for the disaggregation of different functional components into separate dies. These dies are interconnected using advanced die-to-die interconnects, enabling high-speed communication between them. This approach allows for greater flexibility in design because different chiplets can be optimized for specific functions. Using chiplets can lead to improved performance, scalability, and cost efficiency in semiconductor products.
- **Metrology and Measurement Science** – Metrology is the science of measurement used to ensure accuracy and precision in quantifying physical properties. In the semiconductor and microelectronics sector, metrology is crucial for controlling and optimizing the manufacturing processes of integrated circuits (ICs). It involves measuring various parameters to ensure the quality and functionality of the chips. Since 50% of the steps in IC fabrication involve metrology, it plays a pivotal role in maintaining consistency and reliability across different manufacturing stages. Standardization in metrology practices is essential to facilitate data exchange and improve semiconductor devices' overall efficiency and performance.
- **Digital Twin –** A digital twin is a set of virtual information constructs that mimics the structure, context, and behavior of a natural, engineered, or social system (or system-of-systems), is dynamically updated with data from its physical twin, has a predictive capability, and informs decisions that realize value. The bidirectional interaction between the virtual and the physical is central to the digital twin. Data is collected from the real world, which is processed and analyzed by the digital twin whose outputs are then communicated back to the physical world for control or optimization. Digital twins can help accelerate the chip design and manufacturing process, improve performance, and enable solutions such as predictive maintenance and optimized scheduling and dispatch.

1. Introduction and Overview

1.1. Strategy and Policy for Government Engagement in Standards Development

As described below, it is the Federal government's policy to rely on private sector led voluntary consensus standards whenever possible. Voluntary consensus standards development processes are those that are open, balanced, and consensus-based, with provisions for due process and appeals. Voluntary consensus standards that are informed by sound science and engineering can be a powerful force for:

- Innovation in products and services development;
- Interoperability across systems and devices;
- Open and competitive national and global markets; and
- Efficient and effective acquisition processes.

The U.S. strategy for standards development promotes private sector leadership with supplemental contributions from the Federal government. This strategy is implemented in both legislation and policy. The National Technology Transfer and Advancement Act (P.L. 104-113 or NTTAA) [1] is the legislation that directs Federal agencies to use technical standards “that are developed or adopted by voluntary consensus standards bodies, using such technical standards as a means to carry out policy objectives or activities determined by the agencies and departments.” The Act further provides that “Federal agencies and departments shall consult with voluntary, private sector, consensus standards bodies and shall, when such participation is in the public interest and is compatible with agency and departmental missions, authorities, priorities, and budget resources, participate with such bodies in the development of technical standards.” The National Institute of Standards and Technology (NIST) coordinates the federal agency's implementation of NTTAA provisions.

The Trade Agreements Act of 1979 [4] (as amended) legislation prohibits U.S. agencies from engaging in standards-related activities that create unnecessary obstacles to trade and gives the U.S. Trade Representative (USTR) the responsibility to coordinate the consideration of international trade policy issues related to standards and conformity assessment procedures.

The Office of Management and Budget (OMB) Circular A-119 on Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity-Assessment Activities [1] is the primary policy guiding the implementation of the national strategy for documentary standards development. The Circular directs agencies to use voluntary consensus standards in lieu of government-unique standards except where inconsistent with law or otherwise impractical. It also provides guidance to agencies on participation in the development of voluntary consensus standards and articulates policies relating to the use of standards by Federal agencies.

The October 2011 memorandum from the Subcommittee on Standards of the National Science and Technology Council [5] provides a high-level overview of the legal and policy framework for government engagement in private-sector standards and sets out

the following fundamental objectives for Federal government engagement in standards activities.

- Ensure timely availability of effective standards and efficient conformity assessment schemes critical to addressing national priorities
- Achieve cost-efficient, timely, and effective solutions to regulatory, procurement, and policy objectives
- Promote standards and standardization systems that enable innovation and foster competition
- Enhance U.S. competitiveness while ensuring national treatment
- Facilitate international trade and avoid the creation of unnecessary obstacles to trade

1.2. Interagency Committee on Standards Policy

This technical report provides an analysis of the semiconductors and microelectronics standards landscape based on input from the participating Federal agencies. The Interagency Committee on Standards Policy (herein after referred to as the "ICSP" or "Committee") advises federal agencies on matters related to standards policy, as required under the National Technology Transfer and Advancement Act of 1995 (NTTAA). The ICSP provides a forum for coordination on policies related to Federal participation and use of standards and conformity assessment consistent with OMB Circular A-119. It reports to the Secretary of Commerce through the Director of the National Institute of Standards and Technology (NIST) and the Director of NIST's Standards Coordination Office (SCO).

The Committee's authority is set out in Section 13 b of OMB Circular A-119 Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities of the Office of Management and Budget (OMB). The Circular establishes policy to be followed by executive agencies in participating in activities of voluntary standards organizations and in adopting and using voluntary standards. The Circular was last revised on February 10, 1998 and was published in the Federal Register (63 FR 8545) on February 19,1998.

The purpose of the Committee is to promote effective participation by the Federal government in domestic and international standards and conformity assessment activities and the adherence to uniform policies by Federal agencies in the development and use of standards and in conformity assessment activities. Well-considered Federal policies reflecting the public interest can expedite the development and adoption of standards that stimulate competition, promote innovation, and protect the public safety and welfare. The objective of the Committee is to promote effective and consistent standards and conformity assessment policies in furtherance of U.S. goals and to foster cooperative participation by the Federal government, U.S. industry, and other private organizations in standards and conformity assessment

activities. More information is available at:
https://www.nist.gov/standardsgov/interagency-committee-standards-policy-icsp .

1.3. Semiconductors and Microelectronics Standards Working Group

The Semiconductors and Microelectronics Standards Working Group (herein after referred to as the “SMSWG” or “Working Group”) is established under the provisions of the charter of the Interagency Committee on Standards Policy (ICSP). The objective of the SMSWG is to facilitate coordination of Federal agency semiconductors and microelectronics standards (SMS) activities, respond to requests for information, and develop recommendations relating to SMS standards policy matters to the ICSP. The SMSWG is responsible for:

1. Assisting the ICSP in promoting effective and consistent federal policies in the area of semiconductor and microelectronics standards.
2. Providing an annual report to the ICSP on the current SMS activities of participating Federal agencies and recommendations for strategic directions in relevant Federal standards efforts.
3. Responding to requests for information and advising the ICSP on effective means of coordinating SMS activities with those of the private sector.
4. Sharing best practices in semiconductor and microelectronics standards among Federal agencies.
5. Coordinating Federal semiconductor and microelectronics standards interests across application areas such as transportation, energy, health, public safety, and others.

This technical report provides an analysis of the semiconductors and microelectronics standards landscape based on input from the participating Federal agencies. This report was developed under the provisions of item (2) above.

1.4. Definition of Semiconductors and Microelectronics

Semiconductors and microelectronics, in terms of the scope of this document, include the entire lifecycle of integrated circuits, chips, system-on-chips, and other related facets. It encompasses supply chain aspects, manufacturing, computing, memory, and storage technologies, all of which impact every facet of the global economy, society, and government, driving a range of innovations and capabilities. [2][3]

2. Recommendations to the ICSP for Strategic Standards Priority Areas

The SMSWG charter directs the Working Group to provide an annual report to the ICSP, including "recommendations for strategic directions in relevant Federal standards efforts." Through its regular meeting process, the Working Group identified participation in Standards Setting Organizations (SSOs), current focus areas and priorities, and gaps and opportunities.

2.1. Participation in Standards Setting Organizations (SSOs)

SSOs include traditional Standards Developing Organizations (SDOs), consortia, special interest groups, and other similar entities. The following is a list of the external SSOs in which the Federal government is currently participating that are related to SMS. Participation can include observing the outputs of an SSO, attending and participating in meetings and calls, making contributions to documentary standards of SSOs, or taking on leadership roles within an SSO. Although this list is accurate, it is not necessarily an exhaustive list:

- ANSI [1]
- ASME (The American Society of Mechanical Engineers) [2]
- ASTM International (formerly known as American Society for Testing and Materials) [3]
  Example:
    - Committee F42 on Additive Manufacturing Technologies
- EDA (Electrostatic Discharge Association) [4]
- ESDA (EOS/ESD Association) [5]
- IEC [6]
  Examples:
    - TC 29 Electroacoustics
        - WG 5 - Measurement Microphones
    - TC 47 Semiconductor devices
    - TC 65 Industrial-process measurement, control and automation
    - TC 73 Short-circuit currents
- IEEE SA (Institute of Electrical and Electronics Engineers Standards Association) [7]
  Examples:
    - APS/SC - Antennas and Propagation Standards Committee
    - C006 - Board Of Governors
    - C63 - Electromagnetic Compatibility
    - C63.27 - Evaluation Of Wireless Coexistence
    - IEEE P1900.8 - Machine Learning For Rf Spectrum Awareness In Dynamic Spectrum Access (DSA) And Sharing Systems (COM/DYSPAN-SC/MLSA)
    - MEMS – Microelectronmechanical Systems Standards Sponsor Committee

    - N42.38 - Performance Criteria For Spectroscopy Based Portal Monitors Used For Homeland Security
    - N42.49 - Performance Criteria For Personal Emergency Radiation Detectors (PERDs) For Exposure Control
    - Nuclear & Plasma Sciences Society
        - Nuclear and Space Radiation Effects Conference (NSREC)
    - TC-10 - Waveform Generation, Measurement And Analysis
    - TC9.P1451.5.10 - Standard for a Smart Transducer Interface for Sensors and Actuator -- Wireless Communication Protocols and Transducer Electronic Data Sheet (TEDS) NB-IoT Protocol Working Group (NB-IoT Protocol WG)
    - WG299 – Electromagnetic Shielding Enclosures
- IPC (Formerly Institute of Printed Circuits) [8]
  Examples:
    - 2-10 Electronic Product Data Description Committee
        - 2-15 Supply Chain Communication Subcommittee
        - 2-19 Supply Chain Traceability and Trust Subcommittee
            - 2-19b Trusted Supplier Task Group
    - 5-20 Assembly & Joining Committee
        - 5-22 Soldering Subcommittee
            - J-STD-001 Requirements for Soldered Electrical and Electronic Assemblies
    - 7-10 Testing Committee
        - 7-11 Test Methods Subcommittee
    - B-10 Packaged Electronic Components Committee
        - B-10a Plastic Chip Carrier Cracking Task Group
    - D-20 High Speed-High Frequency Committee
        - D-21 High Speed High Frequency Design Subcommittee
        - D-24 High Speed High Frequency Test Methods Subcommittee
    - D-30 Rigid Printed Board Committee
        - D-33 Performance Standards Subcommittee
            - D-33-ap Ultra HDI Subcommittee
    - D-50 Embedded Components Committee
        - D-54 Embedded Devices Test Methods Subcommittee
    - D-70 E-Textiles Committee
        - D-74 E-Textile Test Methods Development and Validation Subcommittee
            - D-74a Printed Electronics E-Textiles Electrical Test Task Group
    - Pb-Free Electronics Risk Management (PERM) Council
- ISO and ISO/IEC [9] [10]
  Examples:
    - TC 201 – Surface Chemical Analysis
        - SC 6 – Mass spectrometries
        - SC 10 - X-ray Reflectometry (XRR) and X-ray Fluorescence (XRF) Analysis

  - TC 213 – Dimensional and Geometrical Product Specifications and Verification
    - WG 6 – General Requirements for Geometrical Product Specification (GPS) Measuring Equipment
    - WG 16 – Areal and Profile Surface Texture
  - ISO/IEC JTC 1 Information technology
    - SC 37 – Biometrics
- ITRS (International Technology Roadmap for Semiconductors) [11]
  Examples:
  - Emerging Research Materials
  - Metrology Technical Working Group
- JEDEC (Joint Electronic Engineering Device Engineering Council) [12]
  Examples:
  - JC-13 Government Liaison
    Committee is "responsible for standardizing quality and reliability methodologies for solid state products used in military, space, and environments requiring special use condition capabilities beyond those of standard commercial practices."
    - JC-13.1 Discrete Devices
    - JC-13.2 Microelectronic Devices
    - JC-13.4 RadHard: Assurance-Characterization
    - JC-13.5 Hybrid, RF/Microwave, and MCM Technology
    - JC-13.7 New Electronic Device Technology
  - JC-16 Interface Technology
- RTCA (Radio Technical Commission for Aeronautics) [13]
- SAE (Society of Automotive Engineers) [14]
  Examples:
  - Aerospace Council
    - Systems Development, Safety, Component Process, Mgmt Systems
      - CE-11 - Component Parts
      - CE-12 - Solid State Devices
- SAE ITC [15]
  - ARINC [16]
- SEMI (Semiconductor Equipment and Materials International) [17]
  Examples:
  - Force3D Packaging & Integration Global Technical Committee
    - 3D Packaging & Integration Bonded Wafer Stacks TF
  - Silicon Wafer Global Technical Committee
    - Advanced Surface Inspection TF
  - Liquid Chemicals Global Technical Committee
  - Micropatterning (Microlithography) Global Technical Committee
  - Gases Global Technical Committee
  - Compound Semiconductor Materials Global Technical Committee
  - PV Materials Global Technical Committee
    - Inspection and Metrology Task Force

        - MEMS/NEMS Global Technical Committee
            - MEMS Reliability TF
        - Photovoltaic Global Technical Committee
        - Traceability Global Technical Committee
- SOSA (Sensor Open System Architecture) Consortium [18]

2.2. Current Focus Areas and Priorities

The SMSWG has identified four key focus areas within the semiconductor and microelectronics sector that are important to Federal government entities. Each focus area includes three associated sub-topics. The Working Group has prioritized these twelve sub-topics into two groups. A plan was developed and executed for a subject matter expert to present information on the first group of sub-topics to the SMSWG and engage in discussions with the Working Group in the calendar year 2024. In 2025, the other group of sub-topics will be covered by subject matter experts including subsequent discussions. Each sub-topic in the first group is presented in this report in divided sections:

- Introduction
- Current state of the sub-topic
- Standards Settings Organizations involved with the sub-topic
- Gaps and opportunities with the sub-topic

For sub-topics scheduled for discussion in the calendar year 2025, this report includes only a brief description. Below is a table that outlines the four main focus areas along with their corresponding sub-topics, including the calendar years scheduled for discussion.

Table 1: Focus Areas and Sub-topics with Calendar Year Discussed

Focus Areas and Sub-topics	Calendar Year Discussed
Supply Chain and Security	
Secure Processors and Holistic Security	2024
Authenticity and counterfeit	2024
Availability, scarcity, and obsolescence	2025
Chiplets	
Packaging and Advanced Packaging	2024
Interoperability	2024
Interconnects	2025
Metrology and Measurement Science	
Advanced Packaging	2024
Future Microelectronics Manufacturing	2025
Semiconductor Material Integrity and Security	2025
Digital Twin	
Manufacturing process and equipment management	2024
Supply chain management and assurance	2025
Quality control	2025

2.2.1. Supply Chain and Security

The semiconductor supply chain encompasses the design, manufacturing, packaging, testing, and distribution of semiconductor devices, involving various entities across different countries. Security in this context means ensuring the integrity, reliability, and availability of components throughout the supply chain. This includes protecting intellectual property, preventing tampering, and safeguarding against production disruptions. Effective security measures are vital for maintaining the trustworthiness of electronic systems used in consumer electronics, automotive, and defense sectors. Securing the supply chain helps mitigate risks related to counterfeit components, vulnerabilities, and cyber threats. [19][20][21][22][23]

2.2.1.1. Secure Processors and Holistic Security

INTRODUCTION

Secure processors are specialized processors and hardware components that enhance security by integrating features at the hardware level. They provide protected execution environments that safeguard sensitive information and cryptographic keys from unauthorized access or attacks. Examples include, but are not limited to, cryptographic processors (also known as cryptoprocessors), hardware security modules (HSM), and trusted platform modules (TPM). The goal of secure processors is to protect against physical tamper attacks, cyber threats, and supply chain vulnerabilities by embedding security within their architecture. Holistic security based on secure processors

encompasses a comprehensive approach that combines hardware and software security measures to safeguard data and operations across all layers of a system. [22][24][25]

CURRENT STATE OF SECURE PROCESSORS AND HOLISTIC SECURITY

The current state of secure processors is characterized by a significant focus on enhancing hardware security through the development of cryptographic processors, cyber-hardened processors, anti-tamper processors, and enhancing traditional processors. There are also Federal government designed and commissioned processors with highly advanced security features, such as the T-Core processor. Some key features that some secure processors may use include:

- cryptographic accelerators - hardware modules integrated into processors that are designed to speed up cryptographic operations for more efficient and secure data encryption and decryption.
- cyber-hardened cores - specialized components within processors that incorporate hardware-based defenses such as tagged architecture and secure cryptographic identity.
- hardware-based identity verification techniques - methods implemented at the hardware level that authenticate the identity of devices or users to ensure secure access and prevent unauthorized use.
- hardware-based key storage - secure storage mechanisms within hardware that protect cryptographic keys from external threats and unauthorized access.
- secure boot capabilities - features in a processor or system that ensure only verified and trusted software can execute at startup, protecting the system from malicious boot and authentication attacks.
- secure core architecture - a design approach that integrates security directly into the core components.
- secure cryptographic suite - a comprehensive set of cryptographic tools and protocols embedded in hardware and/or software to provide enhanced security for data transmission and storage.
- secure execution environments - isolated and protected areas within a processor where sensitive code can run securely, shielded from other less secure applications and potential threats.
- tagged memory systems - memory architectures that use tags or metadata with each memory block to enforce access controls and integrity checks.
- tamper detection mechanisms - security features designed to detect and respond to unauthorized attempts to physically alter or interfere with hardware.
- trusted platform modules - dedicated controllers that secure hardware through integrated cryptographic keys, providing secure generation, storage, and management of encryption keys.

Secure processors are increasingly incorporating features, such as trusted execution environments, secure cryptographic identity, and advanced verification and validation techniques, to provide a holistic security framework that addresses the full range of vulnerabilities.

Traditional Processors

Traditional processors are common and easily commercially available. They are designed primarily for performance and efficiency rather than to be secure. Many of the end products that use traditional processors do not need a lot of expensive and hard-to-implement security features. They need performance and low costs. However, there are some security aspects to some traditional processors. Traditionally, they relied on software-based protection methods. But with the increase in types and number of threats, there has been movement towards adding more hardware-based security features to some but not all traditional processors. This includes the use of cryptographic accelerators, trusted platform modules, and secure boot capabilities to enhance data protection, prevent unauthorized access, and mitigate tamper attacks. This aligns with the broader trend towards holistic security in microelectronics.

Cryptographic Processors

Cryptographic processors are specialized hardware designed specifically to handle cryptographic operations such as encryption, decryption, and key management. They are commonly implemented as co-processors, although not always. When acting as a co-processor, they enhance security by offloading cryptographic tasks from general-purpose or traditional processors. They incorporate features like hardware-based key storage, cryptographic accelerators, and secure execution environments to protect against threats and attacks. Cryptographic processors have these features designed directly into their hardware. Because of this, cryptographic processors provide a trusted platform for secure data that ensures the integrity and confidentiality of sensitive information.

Cyber-hardened Processors

Cyber-hardened processors are designed with enhanced security features designed directly into their hardware architecture, which offers protection against a variety of threats and physical tamper attacks. These processors utilize techniques such as cryptographic accelerators, secure core architecture, and

tagged memory systems to ensure data integrity and prevent unauthorized access. Cyber-hardened processors focus on holistic security, providing a trusted platform for critical applications. They utilize verification and validation processes to ensure reliability and assurance in high-risk environments. Cyber-hardened processors are designed to provide broad security against various threats and physical tampering across the entire system, whereas cryptographic processors specifically focus on cryptographic operations like encryption and key management.

Anti-tamper Processors

Anti-tamper processors are specialized hardware designed to protect sensitive cryptographic keys and data from physical tampering and side channel attacks. These processors incorporate security features such as tamper detection mechanisms, secure cryptographic suite, and hardware-based identity verification techniques to prevent unauthorized access and manipulation. Anti-tamper processors are specifically designed to protect against physical interference and tampering, while cyber-hardened processors focus on a broader range of security enhancements to guard against various cyber threats and vulnerabilities within the digital domain.

T-Core Processors

T-Core processors are Federal government-owned cyber-hardened processors designed with advanced security features to enhance the reliability and security of critical systems. These processors incorporate a cryptographic suite for secure communication, utilize tagged architecture, and employ hardware-based security measures to protect against cyber threats and physical tamper attacks. The T-Core's unique capabilities include generating a cryptographic identity for each individual processor which aids in secure boot processes and trusted software execution.

Protection Against Attacks

In general, secure processors are designed to protect against a variety of security threats. Three examples of threats are:

1. Side Channel Attacks: These involve extracting sensitive information from physical side effects of cryptographic operations, such as power consumption (commonly known as power analysis attacks), electromagnetic emissions, or timing information (commonly known as timing analysis attacks).

2. Physical Attacks: These include attempts to physically tamper with the hardware to bypass security measures. They may include techniques such as fault injection attacks and attacks that exploit physical vulnerabilities to extract data directly from the hardware components.
3. Boot and Authentication Attacks: These include unauthorized boot sequences and compromised firmware or software. Countermeasures are mechanisms like Secure Boot and Verified Boot, which ensure that only authenticated and integrity-checked code runs on the device from the initial boot phase.

Holistic Security

No single approach to protect against attacks and threats will be sufficient. If one area is made secure, attackers will search and find other areas of vulnerability. A holistic approach is needed. Holistic security is a comprehensive approach that uses multiple layers of protection by addressing many vulnerabilities (ideally all vulnerabilities) across hardware, software, and operational processes. Secure processors are important to holistic security since they provide a foundational layer of protection by having hardware-based security features designed in.

[22][24][25]

STANDARDS SETTING ORGANIZATIONS (SSOs) INVOLVED IN SECURE PROCESSESORS AND HOLISTIC SECURITY

Although there appears to be no clear SSO directly involved in secure processors, there are some SSOs that are involved in areas that could impact secure processors:

- International Organization for Standardization (ISO) - ISO develops and publishes international standards for a wide range of industries, including information technology and cybersecurity standards that can influence secure processor specifications.
- Institute of Electrical and Electronics Engineers (IEEE) - IEEE is known for setting standards in the electronics industry, which includes standards for computer architecture, cryptographic protocols, and cybersecurity measures.
- Internet Engineering Task Force (IETF) - While primarily focused on Internet protocols and standards, the IETF develops standards that ensure secure communication protocols that can be integral to secure processor operations.
- Trusted Computing Group (TCG) - TCG develops and promotes open, vendor-neutral, global industry standards for secure computing, including specifications for Trusted Platform Modules (TPM), which are often used in conjunction with secure processors.

GAPS AND OPPORTUNITIES FOR FEDERAL GOVERNMENT INVOLVEMENT

- Lack of Unified Standards and Best Practices:
    a. Gap: There is no single standards organization overseeing the development and implementation of secure processors, leading to fragmented approaches and potential vulnerabilities.
    b. Opportunity: Establish a unified standards body or framework that consolidates best practices, design principles, and security protocols for secure processors.
    c. Opportunity: Referencing the National Vulnerability Database and expanding it to include hardware vulnerabilities for semiconductors and microelectronics.
- Insufficient Integration of Cyber Assurance and Anti-Tamper Measures:
    a. Gap: Current efforts in cyber-hardened processors and anti-tamper technologies tend to operate in silos. There is no overall strategy that addresses holistic security.
    b. Opportunity: Develop integrated standards and guidelines that encompass both cyber assurance and anti-tamper measures, ensuring a multi-layered defense strategy that addresses holistic threats.
- Supply Chain Security and Transparency:
    a. Gap: The complexity of microelectronics supply chains has caused gaps in determining and proving provenance of microelectronics. It is very difficult to determine authenticity.
    b. Opportunity: Create standards and certification processes for supply chain security that include traceability, verification of components, and secure manufacturing practices.
    c. Opportunity: Referencing the National Vulnerability Database and expanding it to include hardware vulnerabilities for semiconductors and microelectronics.

[22][24][25][73]

2.2.1.2. Authenticity and Counterfeit

INTRODUCTION

The concept of "Supply Chain and Security - Authenticity and Counterfeit" focuses on ensuring that every component within the semiconductor supply chain is genuine and meets specified standards. Authenticity refers to the verification that a component is original and conforms to the required specifications, ensuring its reliability and performance. Counterfeit components, on the other hand, are unauthorized copies or substitutes that are often recycled, remarked, or cloned, posing significant risks to the integrity and functionality of electronic systems. To combat counterfeits, systematic test strategies, including sensitivity assessments and the use of standardized test articles,

are employed to detect and prevent these fraudulent parts from entering the supply chain. Managing supply chain risks requires evidence-based methods and automation to create a trusted and secure supply chain, especially in protecting against semiconductor authenticity and counterfeit issues. [23][26][27][28][29][30]

CURRENT STATE OF SUPPLY CHAIN AND SECURITY – AUTHENTICITY AND COUNTERFEIT

The current landscape of supply chain security in the context of authenticity and counterfeit detection is defined by a lack of precision in identifying counterfeit components. Existing detection systems often fall short in terms of sensitivity and reliability, with studies showing that their performance can be as unreliable as random chance. Even with established standards and guidelines, the effectiveness of these systems remains a point of concern, indicating a need for advancements in both methodologies and technologies.

Challenges in this area are driven by the need for more advanced detection systems that can reliably identify counterfeit components throughout the supply chain. Current systems lack standardized verification processes and calibration techniques, which are essential for ensuring consistent and trustworthy results. The development of innovative verification methods, such as second-order effects and more systematic testing strategies, is critical to improving detection accuracy and supply chain security. Additionally, challenges arise in the verification and validation of semiconductors and microelectronics for long-term use cases where their required lifespan significantly exceeds the typical lifecycle of microelectronics.

[23][26][27][28][29][30][74]

STANDARDS SETTING ORGANIZATIONS (SSOs) INVOLVED IN SUPPLY CHAIN AND SECURITY – AUTHENTICITY AND COUNTERFEIT

- SAE International
  Example:
  G-19 Counterfeit Electronic Parts Committee
    - AS6081 - Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition - Distributors

  G-19A Test Laboratory Standards Development Committee
    - AS6171 - Test Methods Standard; General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts AS6171
- ISO (International Organization for Standardization)
  Example:
  ISO/TC 292 Security and Resilience

  - ISO 28001 Security management systems for the supply chain – Best practices for implementing supply chain security, assessments and plans – Requirements and guidance
  - ISO 28002 Security management systems for the supply chain – Development of resilience in the supply chain – Requirements with guidance for use
  - ISO 28003 Security management systems for the supply chain – Requirements for bodies providing audit and certification of supply chain security management systems
  - ISO 28004 Security management systems for the supply chain – Guidelines for the implementation of ISO 28000 (Part 1-4)
- IEC (International Electrotechnical Commission)
  Example:
  TC 107 Process management for avionics
  - IEC 62668-1:2019 - Process management for avionics - Counterfeit prevention - Part 1: Avoiding the use of counterfeit, fraudulent and recycled electronic components
  - IEC 62668-2:2019 - Process management for avionics - Counterfeit prevention - Part 2: Managing electronic components from non-franchised sources
- IPC
  Example:
  2-10 Electronic Product Data Description Committee
  - 2-15 Supply Chain Communication Subcommittee
    - 2-15f Obsolete and Discontinued Product Task Group
  - 2-19 Supply Chain Traceability and Trust Subcommittee
    - 2-19a Critical Components Traceability Task Group
    - 2-19b Trusted Supplier Task Group
    - 2-19c Component-Level Authentication (CLA) Standard Task Group

GAPS AND OPPORTUNITIES FOR FEDERAL GOVERNMENT INVOLVEMENT

- Sensitivity Assessment of Detection Systems
  a. Gap: Current counterfeit detection systems often lack the sensitivity and precision needed to reliably identify subtle differences between genuine and counterfeit components.
  b. Opportunity: There is a significant opportunity to develop and optimize new detection methodologies, such as second-order effects and advanced data analysis techniques, to improve the sensitivity and accuracy of these systems.
- Standardized Test Articles and Verification

a. Gap: The lack of standardized test articles and systematic verification strategies makes it difficult to consistently evaluate the effectiveness of counterfeit detection systems across different platforms and environments.
b. Opportunity: Implementing standardized test articles and systematic verification strategies can provide a more reliable and repeatable framework for assessing the authenticity of electronic components.

- Long-term Drift and Calibration
  a. Gap: There is a mismatch between the lifecycle of microelectronics and the long-term needs of end-use products, especially in areas of defense.
  b. Opportunity: Conducting long-term drift studies and developing robust calibration methodologies can help ensure that detection systems remain accurate and reliable over time.

[23][26][27][28][29][30]

2.2.1.3. Availability, Scarcity, and Obsolescence

The recent global chip shortage, caused by increased demand and supply chain disruptions, has had a significant impact on industries around the world. In response, the semiconductor sector is prioritizing the expansion of manufacturing, diversifying supply chains, and investing in new technologies. To address vulnerabilities in the U.S. supply chain, it is essential to increase domestic production, establish strategic partnerships, and secure government support for innovation. This approach will help maintain a resilient and competitive industry. [31][32]

The U.S. semiconductor supply chain is facing major challenges, including a heavy reliance on foreign suppliers and manufacturing bottlenecks. Potential solutions involve increasing domestic production capacity, encouraging public-private partnerships, and making strategic investments in innovation. The global semiconductor shortages, driven by disruptions from the pandemic and rising demand, highlight the need for diversification and resilience. Countries are now focusing on creating more regionalized and secure supply chains. [31][32]

Obsolescence in the electronics industry is influenced by factors such as low market demand, rapid technological innovation, and supply chain disruptions. Many end-of-life notifications are issued unexpectedly, leaving companies unprepared for these changes. To manage this challenge, businesses need to adopt effective obsolescence management strategies. These should include better forecasting, identifying alternative components, and allocating budgets to address obsolescence risks. As semiconductor obsolescence occurs more frequently due to fast-paced technological advancements, strategies like lifecycle management, long-term supply agreements, and identifying substitute components are essential for maintaining production continuity. [33][34][75]

There are programs within the Federal government that rely on semiconductors and microelectronics that have far outlived their normal lifecycles. In many cases, the

systems are decades old. Programs are now seeking modern technologies and solutions to replicate the functionality of older microcircuits, ensuring the continued availability and support of critical systems. One such solution is GEM (Generalized Emulation of Microcircuits) and AME (Advanced Microcircuit Emulation).

- GEM (Generalized Emulation of Microcircuits) and AME (Advanced Microcircuit Emulation) – Technologies and programs that provide a continuing solution to the microelectronics diminishing manufacturing sources problem. The GEM program is responsible for production manufacturing and the AME program performs development and integration in support of future technology needs. The Programs deliver a permanent solution to microcircuit obsolescence that can be utilized during any phase of the weapon system life cycle. [35]

The Federal government is facing challenges in the semiconductor supply chain, particularly with regard to single-source suppliers and the increasing demand for advanced technologies like GaN and SiC. One example of how such challenges are being addressed is with MIL-PRF-19500. MIL-PRF-19500 is a military standard that sets rigorous performance and reliability standards for semiconductor devices used in military and aerospace applications. It ensures devices can withstand harsh environments and operate reliably in critical systems. Additionally, the government is working with manufacturers to develop new technologies and explore alternative suppliers. They are also focusing on critical microcircuit devices, such as those defined by MIL-PRF-38535 and MIL-PRF-38534, to ensure a reliable supply chain for military and space applications. Furthermore, the Federal government is working with industry partners to develop advanced packaging technologies like MCM, 2.5D, and 3D packaging to meet the increasing demands of modern electronics and space systems.

NOTE: The SMSWG is considering this topic in 2025, and more information will be available in next year's report.

2.2.2. Chiplets

Chiplets are individual semiconductor dies that are integrated into a single package to function as a cohesive unit. Unlike traditional monolithic chips, which consist of a single large die, chiplets allow for the disaggregation of different functional components into separate dies. These dies are interconnected using advanced die-to-die interconnects, enabling high-speed communication between them. This approach allows for greater flexibility in design, because different chiplets can be optimized for specific functions. The use of chiplets can lead to improved performance, scalability, and cost efficiency in semiconductor products. [36][37][80]

2.2.2.1. Packaging and Advanced Packaging

INTRODUCTION

Generally, packaging is the encapsulation of an integrated circuit in a specially designed housing. For chiplets, it involves integrating multiple semiconductor dies into a single, cohesive unit. This allows for efficient and high bandwidth communication between the dies. Leading semiconductor and microelectronics companies have started to utilize the concept of chiplets and advanced packaging to enhance the performance and scalability of their products. Government agencies and high-performance computing (HPCs) systems are increasingly using, or are planning to use, chiplets to improve design efficiency and reduce production costs. This method allows various computing elements to be integrated into a single package, providing greater flexibility and adaptability. The industry is actively working on creating open standards and manufacturing capabilities to support this technology, which is driving innovation and competitiveness in the semiconductor sector. [37][38][39][40]

CURRENT STATE OF CHIPLETS PACKAGING AND ADVANCED PACKAGING

The current state of chiplet packaging involves advanced integration techniques, allowing multiple dies to coexist within a single package, significantly enhancing computing power and efficiency. Industry leaders are leveraging chiplets to achieve higher bandwidth and modularity. Programs like the Defense Department's SHIP and the CHIPS National Advanced Packaging Manufacturing Program (NAPMP) are driving efforts to establish open standards and improve manufacturing processes, aiming to create a more robust and interoperable chiplet ecosystem. Advanced packaging is also being researched and utilized where possible.

> State-of-the-Art Heterogeneous Integrated Packaging Program (SHIP) – The Defense Department's SHIP (State-of-the-Art Heterogeneous Integrated Packaging) Program is an initiative focused on advancing semiconductor packaging technologies to enhance the performance, reliability, and security of defense-related electronic systems. The program aims to develop state-of-the-art packaging solutions, such as 2.5D and 3D integration, to enable more efficient and powerful systems while promoting IP reuse and modularity. By fostering collaboration between government, industry, and academia, the SHIP Program seeks to build a robust ecosystem for advanced packaging, ensuring that the U.S. military maintains technological superiority and national security.
>
> National Advanced Packaging Manufacturing Program (NAPMP) – The CHIPS National Advanced Packaging Manufacturing Program (NAPMP) is an initiative aimed at establishing advanced packaging technology in the United States to enhance the country's leadership in semiconductor manufacturing. NAPMP focuses on key areas such as substrates for advanced packaging, equipment and processes, power delivery and thermal management, and photonics and connectors, all of which are crucial for the effective integration of chiplets. By creating a national test bed for integration and prototyping, NAPMP supports the

development of a robust chiplet ecosystem, enabling innovations in co-design and electronic design automation (EDA).

Advanced Packaging – Advanced packaging involves innovative techniques for integrating multiple semiconductor dies into a single package to improve performance, power efficiency, and functionality. Unlike traditional packaging methods, advanced packaging includes technologies like 2.5D and 3D stacking, chiplets, and interposers, which enable higher interconnect density and better thermal management. These methods are essential for meeting the increasing demands of modern applications, such as high-performance computing (HPC), artificial intelligence (AI), and mobile devices, by allowing for more compact, powerful, and efficient electronic systems.

Packaging with chiplets poses significant challenges. This includes the need for efficient thermal management and power delivery to densely packed dies, which are critical for maintaining performance and reliability. There is also an urgent need for standardized interconnect protocols and packaging technologies to ensure interoperability between chiplets from different manufacturers. Additionally, reducing the complexity and cost of advanced packaging processes is essential to make chiplet integration more accessible to a broader range of companies. This will foster innovation and scalability in the semiconductor industry.

Until recently, the standards focus for chiplets has predominantly been on interconnects and die-to-die communication protocols. Organizations like UCIe [61], PCI-SIG [79], and JEDEC [12] have been working on developing standards that ensure efficient and reliable communication between chiplets. However, focusing solely on interconnects is not sufficient to address all the challenges and opportunities. Here are additional areas that need to be considered for the area of chiplets packaging:

1. Thermal Management and Power Delivery – Efficient thermal management and power delivery systems are crucial for ensuring the performance and reliability of densely packed chiplets. This is especially important as power densities and thermal loads increase. Establishing standards and best practices for thermal interfaces, heat dissipation techniques, and power distribution networks presents valuable opportunities to improve chiplet-based designs. Additionally, using chiplets and interposers with similar thermal expansion coefficients can reduce and minimize mechanical stress and reliability issues.

2. Mechanical and Physical Standards – It is important to maintain consistent mechanical and physical standards for chiplet sizes, bond pitches, and packaging materials. Doing so helps ensure compatibility and simplifies integration. By establishing guidelines for the physical dimensions and material properties of chiplets, there can be easier assembly, integration, and a reduction in manufacturing complexities and costs. In some 3DHI systems, intentionally

combining materials with different properties can enhance performance. This makes alternative reliability control methods necessary.

3. Testing and Validation – It's important to have comprehensive testing and validation standards to ensure the reliability and performance of chiplet-based systems. Developing standardized testing protocols for electrical, thermal, and mechanical performance will help to identify and address potential issues early in the design and manufacturing process.

4. Security and Reliability –Ensuring the security and reliability of chiplet-based systems is crucial, particularly for applications in defense, healthcare, and finance. Developing standards for secure communication, data integrity, and fault tolerance can improve the trustworthiness of chiplet-based systems, making them suitable for high-stakes applications. Additionally, ensuring the security and reliability of chiplet-based systems requires effective inspection techniques for buried layers in 3D heterogeneous integration (3DHI).

5. Software and Design Tools –Software tools and design methodologies are essential for supporting the co-design and integration of chiplets. Developing software standards and tools for multiphysics simulation, verification, and optimization, including electrical, thermal, and mechanical effects, can streamline the design process, enabling more efficient and effective chiplet integration.

6. Supply Chain and Manufacturing – Reliable and trustworthy supply chain and manufacturing ecosystems are crucial to support the widespread adoption of chiplets. By setting standards for supply chain management, quality control, and manufacturing processes, consistent production of high-quality chiplets can be ensured.

[37][38][39][40][76]

STANDARDS SETTING ORGANIZATIONS (SSOs) INVOLVED IN CHIPLETS PACKAGING AND ADVANCED PACKAGING

- JEDEC (Joint Electron Device Engineering Council) – Develops open standards for the microelectronics industry, focusing on memory interfaces, packaging technologies, and multi-chip packages. Example:
  - JC-63 (Multi-Chip Packages)
- SEMI (Semiconductor Equipment and Materials International) – Develops standards for semiconductor manufacturing and advanced packaging technologies crucial for chiplets. Example:
  - Standards Volume G: Packaging
- OCP (Open Compute Project) – Focused on "redesigning hardware technology to efficiently support the growing demands on compute infrastructure" from https://www.opencompute.org/projects/open-chiplet-economy. Examples:

    - Bunch of Wires (BoW)
    - OCP Server Project
        - Open Chiplet Economy
- IMAPS (International Microelectronics Assembly and Packaging Society) – Plays a significant role in the dissemination and development of knowledge related to microelectronics packaging, which includes workshops and publications on chiplets packaging technologies.
- Universal Chiplet Interconnect Express (UCIe) – Focuses on developing open standards for chiplets with an emphasis on die-to-die interconnects, enabling interoperability between chiplets from different manufacturers.

GAPS AND OPPORTUNITIES FOR FEDERAL GOVERNMENT INVOLVEMENT

- Standardization and Interoperability:
    a. Gap: Lack of universally accepted standards for packaging technologies, making it challenging to integrate chiplets from different manufacturers.
    b. Opportunity: Developing and adopting open standards like UCIe can facilitate interoperability and enable a more collaborative ecosystem, allowing for easier integration of third-party chiplets.
- Cost and Complexity:
    a. Gap: Advanced packaging technologies can be expensive and complex to implement, posing a barrier for smaller companies and increasing overall production costs.
    b. Opportunity: Innovations in packaging processes and materials can reduce costs and simplify the integration of chiplets, making advanced packaging more accessible to a broader range of companies.
- Thermal Management and Power Delivery:
    a. Gap: Efficiently managing heat and delivering power to densely packed chiplets remains a significant technical challenge, especially as power consumption increases.
    b. Opportunity: Research and development in thermal management solutions and power delivery systems can enhance the performance and reliability of chiplet-based packages, supporting higher power densities and more complex designs.

[37][38][39][40]

2.2.2.2. Interoperability

INTRODUCTION

Interoperability in chiplets refers to the ability of different chiplets, potentially from various vendors or manufacturers, to function together seamlessly within a single package. This requires standardization of both physical and logical interfaces to ensure

that chiplets can communicate regardless of their origin. Standards play a crucial role in defining these interfaces, which include aspects such as bandwidth, packaging technologies, and communication protocols. Achieving interoperability simplifies the integration process, reduces development costs, and accelerates time-to-market for new semiconductor products. However, it remains a complex challenge due to the need for detailed specifications and the diverse requirements of different applications. [37][41]

CURRENT STATE OF CHIPLETS INTEROPERABILITY

The current state of interoperability with chiplets is evolving but remains complex and fragmented. While there are several emerging standards aimed at facilitating interoperability (especially for communication protocols), achieving seamless integration across chiplets from different vendors is still challenging due to varying specifications and lack of universal standards. Efforts are ongoing to address these gaps, but widespread, plug-and-play interoperability has yet to be fully realized.

> Emerging Standards: The industry's focus on interconnect interoperability for chiplets has been communication protocols. Several standards are being developed from organizations like UCIe (Universal Chiplet Interconnect Express) and BoW (Bunch of Wires) to facilitate communication interoperability. No single universal standard has been widely adopted yet, although the protocols from UCIe are emerging as the most popular.
>
> Complex Integration: Integrating chiplets from different vendors remains complex due to varying specifications and the need for detailed physical and logical interconnects, which increases design complexity and development time. In terms of physical interconnects, three aspects that need to be addressed are bond pitch (the spacing between the interconnects such as bumps or wires that connect the chiplet), wiring density (the number of interconnects that can be packed into a given area), and thermal and power management (the power requirements and heat dissipation of the chiplets). In terms of logical interconnects, three aspects that need to be addressed are communication protocols (although this has been the focus of the industry, more consensus is needed), data encoding and decoding (includes defining the data packet structures, error correction methods, and synchronization mechanisms), and interface standards (the electrical and timing characteristics required for chiplet communication).
>
> Limited Examples of Multi-Vendor Integration: There are few successful examples of chiplets from different companies being integrated, indicating that achieving seamless interoperability across diverse chiplets is still a significant challenge.

The challenges of interoperability with chiplets include the lack of universal standards, which complicates the integration of chiplets from different vendors. Also, the complexity of managing physical and logical interconnects, such as bond pitch and communication

protocols, creates interoperability challenges. Technological needs to address these challenges include the development of comprehensive and widely accepted standards, advanced packaging technologies to facilitate high-density interconnects, and robust thermal and power management solutions to ensure reliable operation. Additionally, collaborative ecosystems and detailed specifications are essential to streamline the integration process and enhance interoperability.
[37][41]

STANDARDS SETTING ORGANIZATIONS (SSOs) INVOLVED IN CHIPLETS INTEROPERABILITY

- Universal Chiplet Interconnect Express (UCIe) – Focuses on developing open standards for chiplets with an emphasis on die-to-die interconnects, enabling interoperability between chiplets from different manufacturers.
- JEDEC (Joint Electron Device Engineering Council) – Develops open standards for the microelectronics industry, focusing on memory interfaces, packaging technologies, and multi-chip packages. Examples:
  - JC-42 (Solid State Memories)
  - JC-40 (Digital Logic)
- IEEE (Institute of Electrical and Electronics Engineers) – Develops a wide range of standards in electronics and electrical engineering, including semiconductor packaging. Examples::
  - IEEE P1838 (Standard for Test Access Architecture for Three-Dimensional Stacked Integrated Circuits)
  - IEEE P3405 (Standard for Die-to-Die (D2D) communication, focusing on the physical and logical layers necessary for chiplet interconnects.)
- OCP (Open Compute Project) – Works on open standards for data center hardware, including chiplet-based designs and packaging technologies. Example:
  - Bunch of Wires (BoW)
- OIF (Optical Internetworking Forum) - a consortium of companies that develops specifications for optical networking technologies.
  - Physical and Link Layer (PLL) Working Group: Develops standards for high-speed electrical and optical interfaces, which can be relevant for chiplet interconnects.
- Universal Chiplet Interconnect Express (UCIe) – Focuses on developing open standards for chiplets with an emphasis on die-to-die interconnects, enabling interoperability between chiplets from different manufacturers.

GAPS AND OPPORTUNITIES FOR FEDERAL GOVERNMENT INVOLVEMENT

- Standardization
  a. Gap: There is no single universal standard that ensures complete interoperability across all chiplets, leading to compatibility issues and increased complexity in integration.

  b. Opportunity: Developing and adopting more comprehensive and universally accepted standards can simplify the integration process, enhance interoperability, and foster a more collaborative ecosystem.

- Physical and Logical Interconnects
  a. Gap: The complexity of managing physical interconnects (e.g., bond pitch, wiring density) and logical interconnects (e.g., communication protocols, data encoding) from different vendors poses significant challenges.
  b. Opportunity: Innovations in advanced packaging technologies and the development of robust, standardized communication protocols can improve the efficiency and reliability of chiplet interconnects, making integration more seamless.
- Thermal and Power Management
  a. Gap: Ensuring consistent thermal and power management across chiplets from different sources is challenging, impacting the reliability and performance of the integrated system.
  b. Opportunity: Establishing uniform thermal and power management guidelines and leveraging advanced cooling and power delivery technologies can enhance the performance and longevity of chiplet-based systems, making them more viable for a wide range of applications.

[37][41]

2.2.2.3. Interconnects

In chiplet-based processors, multiple specialized chips are interconnected within a single package to enhance data flow and facilitate high-performance communication. These interconnects play a crucial role in optimizing processor functionality through high-bandwidth connections while managing varied requirements. Depending on the application, these interconnects can be configured in either serial or parallel arrangements to achieve the desired performance and efficiency.[42][43]
NOTE: The SMSWG is considering this topic in 2025, and more information will be available in next year's report.

2.2.3. Metrology and Measurement Science

Metrology is the science of measurement used to ensure accuracy and precision in quantifying physical properties. In the semiconductor and microelectronics sector, metrology is crucial for controlling and optimizing the manufacturing processes of integrated circuits (ICs). It involves measuring various parameters to ensure the quality and functionality of the chips. Given that 50% of the steps in IC fabrication involve metrology, it plays a pivotal role in maintaining consistency and reliability across different manufacturing stages. Standardization in metrology practices is essential to facilitate data exchange and improve the overall efficiency and performance of semiconductor devices. [44][45][46]

2.2.3.1. Advanced Packaging

INTRODUCTION

Metrology and Measurement Science for Advanced Packaging involve the precise quantification and analysis of various parameters critical to the packaging of semiconductor devices. This field addresses the challenges of integrating multiple chips and functionalities into a single package, requiring accurate measurements of thermal properties, alignment, and mechanical stresses. Advanced packaging metrology ensures that materials with different coefficients of thermal expansion (CTE) are compatible and that the overall system maintains its integrity under operational conditions. The development of robust measurement systems and standards is essential to achieve high interconnect density, reliable thermal management, and effective defect inspection. Ultimately, metrology in advanced packaging aims to enhance the performance, reliability, and cost-efficiency of semiconductor devices. [45][46][47][48]

Advanced packaging refers to the integration of multiple semiconductor chips and functionalities into a single package, enabling enhanced performance, energy efficiency, and miniaturization. It involves sophisticated techniques such as 3D stacking, chiplets, and hybrid bonding to achieve higher interconnect density and improved thermal management compared to traditional packaging. [45][46][47][48]

CURRENT STATE OF METROLOGY AND MEASUREMENT SCIENCE - ADVANCED PACKAGING

The current state of metrology and measurement science for advanced packaging is characterized by significant advancements but also notable gaps, particularly in areas like thermal management, defect inspection, and alignment. While there have been improvements in measurement techniques and tools, the lack of standardized methods and comprehensive understanding of complex packaging systems remains a challenge. The field is ripe with opportunities for innovation, especially in developing new test methods, AI-driven models, and industry-wide standards to enhance precision and reliability.

The challenges of metrology and measurement science for advanced packaging include managing thermal properties, ensuring precise defect inspection, and achieving accurate alignment in increasingly complex, multi-layered systems. Technological needs encompass the development of advanced thermal characterization techniques, high-resolution inspection tools, and robust measurement systems that can handle the intricacies of heterogeneous integration. Additionally, there is a pressing need for standardized measurement methods and data exchange protocols to ensure consistency and reliability across the semiconductor manufacturing ecosystem.

[45][46][47][48]

STANDARDS SETTING ORGANIZATIONS (SSOs) INVOLVED IN METROLOGY AND MEASUREMENT SCIENCE - ADVANCED PACKAGING

- IEEE Standards Association (IEEE-SA)
  Example:
  IEEE P1838: Standard for Test Access Architecture for Three-Dimensional Stacked Integrated Circuits.
- ASME (American Society of Mechanical Engineers)
  Example:
  ASME B89: Dimensional Metrology
- ISO (International Organization for Standardization)
  Examples:
  ISO/TC 201: Surface chemical analysis
  ISO/TC 202: Microbeam Analysis
  ISO/TC 213: Dimensional and Geometrical Product Specifications and Verification
- SEMI (Semiconductor Equipment and Materials International)
  Example:
  Advanced Packaging Heterogeneous Integration (APHI) Technology Community
- JEDEC (Joint Electron Device Engineering Council)
  Examples:
  JC-14: Quality and Reliability of Solid State Products
    - JC-14.1: Reliability Test Methods for Packaged Devices
    - JC-14.3: Silicon Devices Reliability Qualification and Monitoring

  JC-15: Thermal Characterization Techniques for Semiconductor Packages
- ASTM International (American Society for Testing and Materials)
  Example:
  E07: Nondestructive Testing
- IPC (Association Connecting Electronics Industries)
  Examples:
  IPC-6012: Qualification and Performance Specification for Rigid Printed Boards
  IPC-2221: Generic Standard on Printed Board Design

GAPS AND OPPORTUNITIES FOR FEDERAL GOVERNMENT INVOLVEMENT

- Thermal Management
  a. Gap: There is a lack of comprehensive understanding and measurement techniques for thermal interfaces, which are critical for managing heat in heterogeneous integration.
  b. Opportunity: Developing advanced thermal characterization techniques and uncertainty models can significantly enhance the reliability and performance of advanced packaging systems.
- Defect Inspection and Alignment

a. Gap: Current metrology tools are insufficient for detecting and measuring defects and alignment issues at the micro and nano scales, especially in complex, multi-layered packages.
b. Opportunity: Innovating high-resolution inspection and alignment technologies can enhance the precision and yield of advanced packaging processes, reducing costs and improving device performance.

- Standardization of Measurement Methods
  a. Gap: There is a lack of standardized measurement methods and data exchange protocols across the semiconductor manufacturing ecosystem, leading to inconsistencies and inefficiencies.
  b. Opportunity: Establishing industry-wide standards for measurement methods and data exchange can streamline manufacturing processes, improve interoperability, and ensure consistent quality across different production stages.
- Material Properties and Predictive Modeling
  a. Gap: The physical and mechanical properties of chips and packaging materials are not fully understood in predictive modeling for advanced packaging. Specifically, the effects of temperature, pressure, and mechanical stress during epoxy molding on long-term reliability and potential damage to circuits and components remain relatively unknown.
  b. Opportunity: Advancing research on material properties and developing predictive modeling frameworks can enhance reliability and improve processes.

[45][46][47][48]

2.2.3.2. Future Microelectronics Manufacturing

Future microelectronics manufacturing involves the development of new measurement methods, data, reference artifacts, models, and theories to enable higher device yields and reliability, lower costs, and improve fabrication and performance. Advances in measurement science, standards, materials, instrumentation, testing, and manufacturing capabilities will be needed to help design, develop and manufacture next-generation microelectronics. [44]

Advanced metrology is crucial for future microelectronics manufacturing, requiring the development of innovative tools and standards to keep pace with cutting-edge technologies. This includes modeling and simulating semiconductor manufacturing processes to optimize production, improve yields, and enhance competitiveness. Standardizing new materials, processes, and equipment is essential to accelerate innovation and ensure consistent quality across the industry. By addressing these areas, the semiconductor sector can achieve higher performance, reliability, and security in electronic devices, ultimately strengthening the U.S. position in the global market. [47][48]

NOTE: The SMSWG is considering the topic in 2025, and more information will be available in next year's report.

2.2.3.3. Semiconductor Material Integrity and Security

New metrology is needed to meet increasingly stringent requirements for semiconductor material purity, physical properties, and provenance. This involves the journey of a raw material from production to end use. [47]

Ensuring the purity and properties of semiconductor materials is essential for maintaining high manufacturing standards and preventing defects. Advanced modeling and simulation tools play a crucial role in designing and optimizing semiconductor materials, devices, and processes. Additionally, enhancing the security and provenance of microelectronic components throughout the supply chain is vital for protecting against vulnerabilities and ensuring the authenticity of electronic equipment. [48]

NOTE: The SMSWG is considering the topic in 2025, and more information will be available in next year's report.

2.2.4. Digital Twin

A digital twin is a set of virtual information constructs that mimics the structure, context, and behavior of a natural, engineered, or social system (or system-of-systems), is dynamically updated with data from its physical twin, has a predictive capability, and informs decisions that realize value. The bidirectional interaction between the virtual and the physical is central to the digital twin. [78]
Data is collected from the real world, which is processed and analyzed by the digital twin whose outputs are then communicated back to the physical world for control or optimization. Digital twins can help accelerate the chip design and manufacturing process, improve performance, and enable solutions such as predictive maintenance and optimized scheduling and dispatch.. [49][50][51][52][80]

2.2.4.1. Manufacturing Process and Equipment Management

INTRODUCTION

Digital twins in manufacturing involve creating virtual replicas of physical processes and equipment, enabling real-time monitoring, simulation, and optimization. These digital models are synchronized with their physical counterparts which can enable continuous data exchange and updates. This synchronization allows the collection of real-time data, which is then used to predict equipment failures, optimize production schedules, and improve overall operational efficiency. By utilizing digital twins, manufacturers can achieve more productive operations. This ultimately leads to better decision-making and

reduced downtime. The technology also requires bidirectional communication, where data from the physical world is processed in the digital model, and recommendations are sent back to adjust the physical system. This comprehensive approach ensures that manufacturing processes are not only efficient but also adaptive to changing conditions and requirements. [52][53]

CURRENT STATE OF MANUFACTURING PROCESS AND EQUIPMENT MANAGEMENT

The current state of digital twins in manufacturing involves the integration of various sensors and real-time data collection to create synchronized virtual models of physical processes and equipment. Standards like the International Organization for Standardization (ISO) 23247 series are being developed to ensure interoperability, validation, and effective bidirectional communication between the physical and digital systems. Despite advancements, challenges remain in achieving seamless integration and comprehensive VVUQ (Verification, Validation, and Uncertainty Quantification) to ensure the reliability and accuracy of digital twins in the industry.

International Organization for Standardization (ISO) 23247 series – The ISO 23247 series of standards is considered the first major digital twin framework standard. The ISO 23247 series of standards, titled "Digital Twin Framework for Manufacturing," provides a comprehensive framework for the development and implementation of digital twins in the manufacturing sector. The ISO 23247 series of standards for digital twins in manufacturing is built around four key concepts:

- Observable Manufacturing Element (OME): This concept covers all physical aspects of manufacturing processes, including personnel, equipment, materials, processes, facilities, assets, and systems.
- Digital Representation: This concept involves creating digital models or simulations of the physical manufacturing elements, which can be physics-based, data-driven, or a hybrid of both.
- Fit for Purpose: This concept emphasizes that digital twins should be designed for specific scopes so that only relevant data and models are used for the intended purpose.
- Synchronization: This concept ensures bidirectional communication between the physical world and the virtual world, allowing real-time data collection through sensors and enabling updates and adjustments to the physical system based on digital twin analysis.

These concepts are essential for the effective implementation, validation, and maintenance of digital twins in the manufacturing industry.

Synchronization and Data Collection – Synchronization and data collection are critical components of digital twin technology, ensuring that the virtual model accurately reflects the real-world counterpart. Synchronization involves continuous, bidirectional communication between physical systems and their digital twins, facilitated by IoT sensors that collect real-time data. This data is then processed and analyzed in the

digital model to make informed decisions, which can be sent back to adjust the physical system. Effective synchronization and data collection enables real-time monitoring, predictive maintenance, and optimization of manufacturing processes, enhancing overall operational efficiency.

Challenges and Technological Needs – The challenges of implementing digital twins in manufacturing include achieving seamless integration with existing systems, ensuring reliable bidirectional communication, and maintaining accurate real-time data collection through sensors. Technological needs encompass the development of comprehensive standards like ISO 23247 for synchronization, validation, and VVUQ (Verification, Validation, and Uncertainty Quantification) to ensure the reliability and accuracy of digital twins. Additionally, there is a need for advanced simulation and calibration techniques to optimize manufacturing processes and facilitate dynamic maintenance and operational adjustments.

VVUQ (Verification, Validation, and Uncertainty Quantification) – VVUQ (Verification, Validation, and Uncertainty Quantification) is a critical framework for ensuring the reliability and accuracy of digital twins.

- Verification – involves confirming that the computational model is mathematically correct and accurately implemented, ensuring no errors were introduced during the transition from the conceptual model to the final program.
- Validation – ensures that the digital twin accurately represents real-world observations and meets the intended purpose, confirming that the right model has been built.
- Uncertainty Quantification – involves generating and applying mathematical models to measure and manage uncertainties in data collection, processing, and interpretation, ensuring that the digital twin's predictions and recommendations are credible. Together, VVUQ processes are essential throughout the digital twin lifecycle, from design and deployment to maintenance and updates, to maintain trustworthiness and effectiveness.

[52][53]

STANDARDS SETTING ORGANIZATIONS (SSOs) INVOLVED IN MANUFACTURING PROCESS AND EQUIPMENT MANAGEMENT

- International Organization for Standardization (ISO)
    - ISO/TC 184/SC 4
        - WG 15: Responsible for the ISO 23247 series, which focuses on the Digital Twin Framework for Manufacturing.
            - 23247-1: General principles and requirements
            - 23247-2: Reference architecture
            - 23247-3: Digital representation
            - 23247-4: Information exchange
            - 23247-5: Digital Thread for Digital Twin
            - 23247-6: Digital Twin Composition

            - WG 12: Responsible for ISO 10303 series, also known as STEP (Standard for the Exchange of Product model data), which provides a comprehensive data model for the exchange and sharing of product information throughout the lifecycle of a product.
                - AP 238: Managed Model-Based 3D Engineering (MMBE)
                - AP 242: Model-based Integrated Manufacturing (MIM)
- International Electrotechnical Commission (IEC) – IEC collaborates with ISO on joint technical committees to develop standards for digital twins.
    - ISO/IEC JTC 1/SC 41/WG 6: Works on standards related to the digital twin concept, terminologies, and use cases.
        - ISO/IEC CD 30186: Digital twin — Maturity model and guidance for a maturity assessment
        - ISO/IEC AWI 30188: Digital Twin — Reference architecture
        - ISO/IEC TR 30172:2023: Internet of things (IoT) — Digital twin — Use cases
        - ISO/IEC 30173:2023: Digital twin — Concepts and terminology
- American Society of Mechanical Engineers (ASME):
    - ASME V&V 50 – Develops guidelines for verification, validation, and uncertainty quantification (VVUQ) in computational modeling for advanced manufacturing.
- Object Management Group (OMG) – Industry IoT Consortium (IIC) Digital Twin Interoperability Task Group (DTITG): Focuses on interoperability standards for digital twins.
- Digital Twin Consortium (DTC): Works on technical reports and guidelines for digital twin implementation and interoperability.
- MTConnect Institute - "The MTConnect Institute is a 501(c)(6) not-for-profit standards development organization for the MTConnect standard (ANSI/MTC1.4-2018). Its membership is made up of over 400 companies and research organizations in discrete manufacturing including automotive, aerospace, medical, and other industries as well as software developers, system integrators, and research organizations supporting those industries. Membership is free and open to anyone with a stake in MTConnect (join)." [from https://www.mtconnect.org/about]
    - MTConnect standard (ANSI/MTC1.4-201) – An open, royalty-free standard that enables real-time data collection and communication from manufacturing equipment using a common language and data model.
- Digital Metrology Standards Consortium (DMSC)
    - QIF (Quality Information Framework): An ANSI standard (ANSI QIF) that provides a unified XML framework for defining, exchanging, and managing quality information throughout the manufacturing process.
- OPC Foundation
    - OPC UA (Open Platform Communications Unified Architecture): A machine-to-machine communication protocol for industrial automation that ensures secure and reliable data exchange across diverse platforms and devices.
- Object Management Group (OMG)

  - UML/SYSML (Unified Modeling Language/System Modeling Language): UML is a standardized modeling language for specifying, visualizing, and documenting software systems, while SysML is a derivative of UML tailored for systems engineering applications.
- AutomationML e.V.
  - AutomationML (Automation Markup Language): A standardized data format based on XML for the exchange of plant engineering information, enabling interoperability between different engineering tools.
- Simulation Interoperability Standards Organization (SISO)
  - CMSD (Core Manufacturing Simulation Data): A standard that defines a data model for the efficient exchange of manufacturing simulation data between simulation software and other manufacturing applications.
- Data Mining Group (DMG)
  - PMML/PFA (Predictive Model Markup Language/Portable Format for Analytics): PMML is an XML-based standard for representing predictive models, while PFA is a JSON-based standard for specifying analytic models and their deployment in production environments.
- IEEE (Institute of Electrical and Electronics Engineers) – IEEE is involved in developing standards related to IoT, data exchange, and other technologies that support digital twin implementations.

GAPS AND OPPORTUNITIES FOR FEDERAL GOVERNMENT INVOLVEMENT

- Fragmented Standards Landscape
  a. Gap: There is a shortage of fully developed and widely adopted standards that cover all aspects of digital twin implementation for manufacturing, including interoperability, data exchange, and lifecycle management.
  b. Opportunity: Creating comprehensive and unified standards that encompass all aspects of digital twin technology, not just in manufacturing, can facilitate broader adoption and interoperability across the manufacturing industry.
- Enabling Seamless Integration
  a. Gap: Existing standards do not fully address the complexities of integrating digital twins with legacy systems, various software platforms, and different types of physical equipment.
  b. Opportunity: Developing standards that focus on seamless integration with existing systems and diverse platforms can help manufacturers more effectively use digital twins.
- Verification, Validation, and Uncertainty Quantification (VVUQ):
  a. Gap: More robust standards and methodologies are needed to ensure the reliability, accuracy, and trustworthiness of digital twins, particularly in real-time and dynamic environments.

b. Opportunity: Establishing detailed guidelines and standards for VVUQ can improve the credibility and reliability of digital twins, making them more useful for critical decision-making processes in manufacturing.

[52][53]

2.2.4.2. Supply Chain Management and Assurance

A supply chain digital twin is a virtual, data-driven model of a supply chain. It allows for simulations and real-time monitoring to identify and address potential issues like delays or shortages. By modeling the entire supply process, this tool helps pinpoint inefficiencies, improve resource allocation, and support more informed strategic decision-making. Also, through predictive analytics, it provides insights that enable businesses to enhance their operational resilience and proactively respond to disruptions. [54][55][77]

NOTE: The SMSWG is considering the topic in 2025, and more information will be available in next year's report.

2.2.4.3. Quality Control

Digital twins offer a revolutionary approach to quality control by using real-time data from sensors and other sources to create a dynamic replica of the physical product or service. This technology allows manufacturers to analyze individual components and predict potential issues before they impact product quality. By monitoring various factors, digital twins can pinpoint areas at risk of producing defective products. [56]

NOTE: The SMSWG is considering the topic in 2025, and more information will be available in next year's report.

2.3. Gaps and Opportunities

In addition to the current strategic priority areas, there were areas identified as gaps or opportunities. These include areas where there could be Federal government involvement but there is currently little or none; or Semiconductor and Microelectronics areas that are trending and there are currently gaps in Federal government involvement:

2.3.1. Supply Chain and Security

- Lack of Unified Standards and Best Practices for Secure Processors and Holistic Security:

a. Gap: There is no single standards organization overseeing the development and implementation of secure processors, leading to fragmented approaches and potential vulnerabilities.
b. Opportunity: Establish a unified standards body or framework that consolidates best practices, design principles, and security protocols for secure processors.
c. Opportunity: Referencing the National Vulnerability Database and expanding it to include hardware vulnerabilities for semiconductors and microelectronics.

- Insufficient Integration of Cyber Assurance and Anti-Tamper Measures:
    a. Gap: Current efforts in cyber-hardened processors and anti-tamper technologies tend to operate in silos. There is no overall strategy that addresses holistic security.
    b. Opportunity: Develop integrated standards and guidelines that encompass both cyber assurance and anti-tamper measures, ensuring a multi-layered defense strategy that addresses holistic threats.
- Supply Chain Security and Transparency:
    a. Gap: The complexity of microelectronics supply chains has caused gaps in determining and proving provenance of microelectronics. It is very difficult to determine authenticity.
    b. Opportunity: Create standards and certification processes for supply chain security that include traceability, verification of components, and secure manufacturing practices.
    c. Opportunity: Referencing the National Vulnerability Database and expanding it to include hardware vulnerabilities for semiconductors and microelectronics.
- Sensitivity Assessment of Detection Systems
    a. Gap: Current counterfeit detection systems often lack the sensitivity and precision needed to accurately reliably identify subtle differences between genuine and counterfeit components.
    b. Opportunity: There is a significant opportunity to develop and optimize new detection methodologies, such as second-order effects and advanced data analysis techniques, to improve the sensitivity and accuracy of these systems.
- Standardized Test Articles and Verification
    a. Gap: The lack of standardized test articles and systematic verification strategies makes it difficult to consistently evaluate the effectiveness of counterfeit detection systems across different platforms and environments.
    b. Opportunity: Implementing standardized test articles and systematic verification strategies can provide a more reliable and repeatable framework for assessing the authenticity of electronic components.
- Long-term Drift and Calibration

  a. Gap: There is a mismatch between the lifecycle of microelectronics and the long-term needs of end-use products, especially in areas of defense.
  b. Opportunity: Conducting long-term drift studies and developing robust calibration methodologies can help ensure that detection systems remain accurate and reliable over time.
- Gallium Nitride (GaN) and Silicon Carbide (SiC) Technology
  a. Gap: There is insufficient specification and supplier preparedness for GaN and SiC semiconductor devices, as well as laser diode technologies, which are crucial for achieving high-efficiency performance in extreme environments like high temperatures, low Earth orbit (LEO), geosynchronous Earth orbit (GEO), and deep-space missions.
  b. Opportunity: Creating detailed specifications for GaN and SiC transistors and discovering new suppliers for upcoming laser diode technologies can lead to faster and more efficient semiconductor devices that support advanced aerospace and defense applications.
- Advanced Technology Microcircuits (MIL-PRF-ATM)
  a. Gap: There are insufficient comprehensive specifications and standards for advanced microcircuits, such as multichip modules (MCM), 2.5D and 3D packages, Chip on Wafer on Silicon (CoWoS), and chiplets. These technologies are critical for next-generation AI and space applications.
  b. Opportunity: Partnering with microcircuit manufacturers and space communities to create strong specifications can facilitate the establishment of high-speed, reliable computing networks in spacecraft and other advanced technologies.
- Supply Chain Security with Device DNA (deoxyribonucleic acid) Marking
  a. Gap: Widespread adoption and implementation of DNA marking across critical components are necessary to ensure supply chain security and reduce the risk of counterfeit items in defense applications.
  b. Opportunity: Expanding the use of DNA marking for authentication in electronic microcircuits and other critical items can enhance strategies to mitigate counterfeiting, protect warfighters, and strengthen the reliability of essential defense missions.

2.3.2. Chiplets

- Standardization and Interoperability for Packaging:
  a. Gap: Lack of universally accepted standards for packaging technologies, making it challenging to integrate chiplets from different manufacturers.
  b. Opportunity: Developing and adopting open standards like UCIe can facilitate interoperability and enable a more collaborative ecosystem, allowing for easier integration of third-party chiplets.
- Cost and Complexity of Advanced Packaging:

   a. Gap: Advanced packaging technologies can be expensive and complex to implement, posing a barrier for smaller companies and increasing overall production costs.
   b. Opportunity: Innovations in packaging processes and materials can reduce costs and simplify the integration of chiplets, making advanced packaging more accessible to a broader range of companies.

- Thermal Management and Power Delivery:
   a. Gap: Efficiently managing heat and delivering power to densely packed chiplets remains a significant technical challenge, especially as power consumption increases.
   b. Opportunity: Research and development in thermal management solutions and power delivery systems can enhance the performance and reliability of chiplet-based packages, supporting higher power densities and more complex designs.
- Standardization for Chiplets Interoperability
   a. Gap: There is no single universal standard that ensures complete interoperability across all chiplets, leading to compatibility issues and increased complexity in integration.
   b. Opportunity: Developing and adopting more comprehensive and universally accepted standards can simplify the integration process, enhance interoperability, and foster a more collaborative ecosystem.
- Physical and Logical Interconnects
   a. Gap: The complexity of managing physical interconnects (e.g., bond pitch, wiring density) and logical interconnects (e.g., communication protocols, data encoding) from different vendors poses significant challenges.
   b. Opportunity: Innovations in advanced packaging technologies and the development of robust, standardized communication protocols can improve the efficiency and reliability of chiplet interconnects, making integration more seamless.

2.3.3. Metrology and Measurement Science

- Thermal Management with Advanced Packaging
   a. Gap: There is a lack of comprehensive understanding and measurement techniques for thermal interfaces, which are critical for managing heat in heterogeneous integration.
   b. Opportunity: Developing advanced thermal characterization techniques and uncertainty models can significantly enhance the reliability and performance of advanced packaging systems.
- Defect Inspection and Alignment with Advanced Packaging

a. Gap: Current metrology tools are insufficient for detecting and measuring defects and alignment issues at the micro and nano scales, especially in complex, multi-layered packages.
b. Opportunity: Innovating high-resolution inspection and alignment technologies can enhance the precision and yield of advanced packaging processes, reducing costs and improving device performance.

- Standardization of Measurement Methods
  a. Gap: There is a lack of standardized measurement methods and data exchange protocols across the semiconductor manufacturing ecosystem, leading to inconsistencies and inefficiencies.
  b. Opportunity: Establishing industry-wide standards for measurement methods and data exchange can streamline manufacturing processes, improve interoperability, and ensure consistent quality across different production stages.
- Material Properties and Predictive Modeling
  a. Gap: The physical and mechanical properties of chips and packaging materials are not fully understood in predictive modeling for advanced packaging. Specifically, the effects of temperature, pressure, and mechanical stress during epoxy molding on long-term reliability and potential damage to circuits and components remain relatively unknown.
  b. Opportunity: Advancing research on material properties and developing predictive modeling frameworks can enhance reliability and improve processes.

2.3.4. Digital Twin

- Fragmented Standards Landscape
  a. Gap: There is a shortage of fully developed and widely adopted standards that cover all aspects of digital twin implementation for manufacturing, including interoperability, data exchange, and lifecycle management.
  b. Opportunity: Creating comprehensive and unified standards that encompass all aspects of digital twin technology, not just in manufacturing, can facilitate broader adoption and interoperability across the manufacturing industry.
- Enabling Seamless Integration
  a. Gap: Existing standards do not fully address the complexities of integrating digital twins with legacy systems, various software platforms, and different types of physical equipment.
  b. Opportunity: Developing standards that focus on seamless integration with existing systems and diverse platforms can help manufacturers more effectively use digital twins.
- Verification, Validation, and Uncertainty Quantification (VVUQ):

a. Gap: More robust standards and methodologies are needed to ensure the reliability, accuracy, and trustworthiness of digital twins, particularly in real-time and dynamic environments.
b. Opportunity: Establishing detailed guidelines and standards for VVUQ can improve the credibility and reliability of digital twins, making them more useful for critical decision-making processes in manufacturing.

2.3.5. Others

There are many important topics in semiconductors and microelectronics that are too vast to be mentioned in this report.Many of those topics have standards gaps and opportunities for the Federal government. In addition to the established focus areas outlined earlier, several topic areas are detailed below that could gain more prominence in the industry as a whole and could be discussed in the SMSWG in the future.

2.3.5.1. AI accelerator chips

AI accelerator chips are specialized processors designed to handle the computational requirements of artificial intelligence tasks and calculations. By optimizing specific AI operations like matrix calculations and parallel processing, they offer faster performance and greater efficiency compared to general-purpose CPUs and GPUs. [57]
The economic landscape for AI accelerator chips is increasingly competitive, with established companies facing challenges from startups advancing specialized technology for various applications. Startups are capitalizing on growing demand and have raised significant funding to develop innovative chips that offer enhanced efficiency and performance. Standards in this space could be essential to facilitate interoperability and streamline development. [58]

2.3.5.2. Photonics

Photonics in semiconductors and microelectronics involves integrating optical components and pathways into electronic systems. This integration enables faster data transmission and improved processing efficiency. By using light for signaling, photonics addresses the limitations of traditional electronic interconnects by reducing power consumption and increasing bandwidth. It is paving the way for advanced applications, such as optical communication on chips and quantum computing technologies. [59]
Standards for photonics are crucial for ensuring consistent testing, manufacturing, and interoperability as the technology advances. Since photonics is used in various fields, such as medicine and quantum computing, there is a risk that developments may not align with the specific requirements of these areas. Increasing standardization in photonics can help address these compatibility issues. [60]

2.3.5.3. Chiplets open standards and *de facto* standards organizations

The leading organizations that are standardizing chiplets usage and interoperability are trending towards being private enterprises. Organizations and projects such as UCIe [61], Bunch of Wires (BoW) [62], and OpenHBI [63], among others, are composed of private companies and entities, and usually government involvement is not encouraged. The Federal government should actively seek membership and participation in organizations such as these to advance standardization.

2.3.5.4. Diminishing Manufacturing Sources and Material Shortages (DMSMS)

A DMSMS issue is the loss, or impending loss, of manufacturers, suppliers, or raw materials. Because many manufacturing facilities or material sources exist internationally and in sometimes hostile arenas, there is a potential for greater instability. The Department of Defense (DoD) has published two guidebooks, SD-22 [65] and SD-26 [66], to help manage DMSMS and parts management. Even though there are multiple standards that address DMSMS, to mitigate issues that result in obsolescence, loss of manufacturing sources, or material shortages, more or additional international standards that assess the potential of negative impacts and the resulting mitigation strategies may be needed. Alternatively, an agreement to adopt specific existing standards may be needed. [64]

2.3.5.5. Government-Industry Data Exchange Program (GIDEP)

GIDEP is a cooperative activity between government and industry participants seeking to reduce or eliminate expenditures of resources by sharing technical information essential during research, design, development, production, and operational phases of the life cycle of systems, facilities and equipment. Since GIDEP's inception, participants have reported over $2.1 billion in prevention of unplanned expenditures. That means without GIDEP, participants could have potentially realized additional expenses of over $2.1 billion. Proper utilization of GIDEP data can materially improve the total quality and reliability of systems and components during the acquisition and logistics phases of the life cycle and reduce costs in the development and manufacture of complex systems and equipment. Moving the GIDEP activities into an internationally recognized and standardized process could increase adoption of the concept. [67]

2.3.5.6. Stable EUV reflectivity structures

Stable EUV reflectivity structures are multilayer coatings designed to reflect extreme ultraviolet (EUV) light with high efficiency and minimal degradation over time. These structures are essential for EUV lithography. Research is needed for the manufacturing metrology and for new materials that have a higher resistance to degradation. [68]

2.3.5.7. Potential adoption of larger EUV masks

The potential adoption of larger Extreme Ultraviolet (EUV) masks is being considered to accommodate advanced semiconductor manufacturing. However, this shift includes the need for new infrastructure and equipment capable of handling larger masks which increases costs. Standards are needed for the use of the larger masks. [69] [70]

2.3.5.8. CD-SEM structures with near-picometer (Sub-Å) tolerance

Critical Dimension Scanning Electron Microscopy (CD-SEM) is a technique used to measure the dimensions of fine patterns on semiconductor wafers with high precision. Achieving sub-angstrom (sub-Å) tolerance in these measurements is crucial for the development of advanced semiconductor devices. Metrology standards are needed. [71]

2.3.5.9. Overlay structures with Sub-nm tolerance

Overlay structures with sub-nanometer tolerance ensure precise alignment of multiple layers during the lithography process. These structures help minimize edge placement errors and improve the overall accuracy and yield of semiconductor devices. There is a need for advanced overlay metrology techniques to further reduce edge placement errors. [72]

3. Agencies/Offices Participating in the Semiconductors and Microelectronics Standards Working Group

The following agencies, offices, and bureaus contributed and participated in the Semiconductors and Microelectronics Standards Working Group in 2024:

- Department of Defense (DoD)
- Defense Logistics Agency (DLA)
- Department of Homeland Security (DHS)
- National Institute of Standards and Technology (NIST)
- US Air Force
- US General Services Administration (GSA)
- US Navy
- US Space Force (USSF)

4. National Standards Strategy for Critical and Emerging Technology Strategy

The National Standards Strategy for Critical and Emerging Technology (NSSCET) [1][2] aims to ensure that the United States remains a leader in the global economy by promoting the development and use of standards for CET. The strategy focuses on four key objectives: investment, participation, workforce, and international engagement. The overall strategy calls for increased investment in pre-standardization research, translational research, and educational programs to promote innovation and workforce development in CET. It also calls for the promotion of participation by the private sector, academia, and other stakeholders in CET standards development activities. The strategy emphasizes priority areas such as Communication and Networking Technologies, Artificial Intelligence and Machine Learning, Quantum Information Technologies, Automated and Connected Infrastructure, Cybersecurity and Privacy, among others. There is alignment between the overall work of the SMSWG and NSSCET priority areas. Specifically, the NCCSET priority area:

- Semiconductors and Microelectronics, including Computing, Memory, and Storage Technologies, which affect every corner of the global economy, society, and government, and which power a panoply of innovations and capabilities. [2]

Additionally, the NSSCET defines specific applications that will impact our global economy and national security. Two of the applications align with the overall work of the SMSWG:

- Critical Minerals Supply Chains, where we will promote standards that support increased sustainable extraction of critical minerals necessary to manufacture renewable energy technologies, semiconductors, and EVs. [2]
- Cybersecurity and Privacy, which are cross-cutting issues that are critical to enabling the development and deployment. [2]

5. References

5.1. References for Executive Summary and Section 1 Introduction and Overview

[1] Key Federal Law and Policy Documents: NTTAA & OMB A-119
https://www.nist.gov/standardsgov/what-we-do/federal-policy-standards/key-federal-directives

[2] CRITICAL AND EMERGING TECHNOLOGIES LIST UPDATE
https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/02/Critical-and-Emerging-Technologies-List-2024-Update.pdf

[3] UNITED STATES GOVERNMENT NATIONAL STANDARDS STRATEGY FOR CRITICAL AND EMERGING TECHNOLOGY
https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/05/US-Gov-National-Standards-Strategy-2023.pdf

[4] The Trade Agreements Act of 1979
https://www.govinfo.gov/content/pkg/COMPS-2961/pdf/COMPS-2961.pdf

[5] The October 2011 memorandum from the Subcommittee on Standards of the National Science and Technology Council
https://www.nist.gov/system/files/documents/standardsgov/Federal_Engagement_in_Standards_Activities_October12_final.pdf

5.2. References for Section 2 Recommendations to the ICSP for Strategic Standards Priority Areas

[1] ANSI (American National Standards Institute): A private non-profit organization that oversees the development of voluntary consensus standards for products, services, processes, systems, and personnel in the United States.: https://www.ansi.org/

[2] ASME (The American Society of Mechanical Engineers).: https://www.asme.org/

[3] ASTM International: An international standards organization that develops and publishes technical standards for a wide range of materials, products, systems, and services.: https://www.astm.org/

[4] EDA (Electrostatic Discharge Association): https://www.esda.org/

[5] ESD Association: A professional voluntary association dedicated to advancing the theory and practice of electrostatic discharge (ESD) avoidance.: https://www.esda.org/

[6] IEC (International Electrotechnical Commission): An international standards organization that prepares and publishes international standards for all electrical, electronic, and related technologies.: https://www.iec.ch/homepage

[7] IEEE SA (Institute of Electrical and Electronics Engineers Standards Association): https://standards.ieee.org/

[8] IPC: Association Connecting Electronics Industries: A trade association that provides standards, training, and certification programs for the electronics manufacturing industry.: https://www.ipc.org/

[9] International Organization for Standardization (ISO): An independent, non-governmental international organization that develops and publishes standards for a wide range of industries.: https://www.iso.org/

[10] ISO/IEC Joint Technical Committee 1 (JTC 1): A joint technical committee of ISO and IEC that develops and publishes international standards for information technology.: https://www.iso.org/organization/70.html

[11] International Technology Roadmap for Semiconductors (ITRS): A collaborative effort by the global semiconductor industry to identify and address technology challenges facing the industry.: http://www.itrs2.net/

[12] JEDEC Solid State Technology Association: A global leader in developing open standards for the microelectronics industry.: https://www.jedec.org/

[13] RTCA (Radio Technical Commission for Aeronautics): https://www.rtca.org/

[14] SAE (Society of Automotive Engineers): A professional organization for mobility engineering professionals in the aerospace, automotive, and commercial vehicle industries.: https://www.sae.org/

[15] SAE ITC: https://www.sae-itc.com/

[16] ARINC: https://aviation-ia.sae-itc.com/

[17] SEMI: A global industry association that connects people, ideas, and solutions to advance electronic manufacturing.: https://semi.org/

[18] SOSA (Sensor Open System Architecture) Consortium.: https://www.opengroup.org/sosa

[19] RAND Corporation: A research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous.: https://www.rand.org/pubs/perspectives/PEA1394-1.html

[20] Arizona State University News: An article discussing how ASU researchers are working to secure the microelectronics supply chain from cyberattacks.: https://news.asu.edu/20220331-securing-microelectronics-supply-chain

[21] Center for Security and Emerging Technology (CSET): A research organization that studies the security implications of emerging technologies.: https://cset.georgetown.edu/publication/the-semiconductor-supply-chain

[22] Presentation to the SMSWG by Jonathan Heiner on March 3, 2024 on the subject of Supply Chain and Security - Secure Processors.

[23] Presentation to the SMSWG by Christian Eakins on August 5, 2024 on the subject of Supply Chain and Security - Authenticity and counterfeit.

[24] Survey of secure processors: https://ieeexplore.ieee.org/document/8344637

[25] Microsoft Is Making a Secure PC Chip—With Intel and AMD's Help: https://www.wired.com/story/microsoft-pluton-secure-processor/.

[26] Semiconductor Industry Association (SIA): An industry trade group that represents U.S.-based semiconductor companies on issues related to public policy, innovation, and competitiveness.: https://www.semiconductors.org/policies/anti-counterfeiting/

[27] Insight Analytical Labs: A company that provides authenticity analysis services for electronic components such as semiconductors.: https://www.ial-fa.com/authenticity-analysis/

[28] SIA Anti-Counterfeiting Whitepaper: A whitepaper discussing anti-counterfeiting measures in the semiconductor industry.: https://semiconductors.org/wp-content/uploads/2018/06/SIA-Anti-Counterfeiting-Whitepaper-1.pdf

[29] IEEE Xplore Digital Library: An article discussing metrology challenges in advanced semiconductor manufacturing processes.: https://dforte.ece.ufl.edu/wp-content/uploads/sites/65/2021/01/MTV_2013_submission_25.pdf

[30] Defense Systems Information Analysis Center (DSIAC): An article on combating counterfeit components in the DoD supply chain.: https://dsiac.org/articles/combating-counterfeit-components-in-the-dod-supply-chain/

[31] Harvard Business Review: An article discussing how to fix the U.S. semiconductor supply chain by increasing domestic production capacity and improving supply chain resilience.: https://hbr.org/2022/10/fixing-the-u-s-semiconductor-supply-chain

[32] World Economic Forum: An article on how the semiconductor industry is dealing with a worldwide shortage.: https://www.weforum.org/agenda/2022/02/semiconductor-chip-shortage-supply-chain/

[33] "Coping With Semiconductor Obsolescence": https://www.automation.com/en-us/articles/september-2022/coping-semiconductor-obsolescence.

[34] "Semiconductor Obsolescence Management Best Practices": https://www.z2data.com/insights/semiconductor-obsolescence-management-best-practices.

[35] GEM Energy Management Services: A company that provides energy management services to semiconductor manufacturers.: https://gemes.com/about-gem/

[36] IEEE Electronics Packaging Society Glossary: Definition of Interconnects.: https://eps.ieee.org/technology/definitions.html

[37] Presentation to the SMSWG by Bapi Vinnakota on May 13, 2024 on the subject of Chiplets - Packaging.

[38] A 101 Guide to the Integrated Circuit Packaging Process: https://www.thomasnet.com/insights/a-101-guide-to-the-integrated-circuit-packaging-process/

[39] IEEE Electronics Packaging Society Glossary: Definition of Interconnects: https://eps.ieee.org/technology/definitions.html

[40] IC Packages Types: https://www.engineersgarage.com/ic-packages-types/

[41] What are Computer Chiplets?: https://research.ibm.com/blog/what-are-computer-chiplets

[42] All About Circuits News: An article discussing innovative interconnects as a future solution for chiplet-based processors.: https://www.allaboutcircuits.com/news/innovative-interconnects-the-future-of-chiplet-based-processors/

[43] Chiplet Technology: A New Era in Microelectronics: https://nepp.nasa.gov/docs/etw/2021/15-JUN-21_Tues/1500_Ramamurthy-Chiplet-Technology-v3.pdf

[44] NIST Semiconductor Research: https://www.nist.gov/semiconductors

[45] Presentation to the SMSWG by Paul Hale on June 24, 2024 on the subject of Metrology and Measurement Science.

[46] Presentation to the SMSWG by Geroge Orji on June 24, 2024 on the subject of Metrology and Measurement Science - Advanced Packaging.

[47] NIST Report Outlines Strategic Opportunities for U.S. Semiconductor Manufacturing: https://www.nist.gov/news-events/news/2022/09/nist-report-outlines-strategic-opportunities-us-semiconductor-manufacturing

[48] “Strategic Opportunities for U.S. Semiconductor Manufacturing”: https://nvlpubs.nist.gov/nistpubs/CHIPS/NIST.CHIPS.1000.pdf

[49] What is Digital Twin?: https://www.twi-global.com/technical-knowledge/faqs/what-is-digital-twin

[50] Leveraging the Digital Twin in Smart Microelectronics Manufacturing: https://semiengineering.com/leveraging-the-digital-twin-in-smart-microelectronics-manufacturing/

[51] Digital Twin in Semiconductor Industry: https://blog.gramener.com/digital-twin-in-semiconductor-industry/

[52] Presentation to the SMSWG by Gordon Shao on April 15, 2024 on the subject of Digital Twin - Manufacturing Process and Equipment Management.

[53] The Digital Twin in Manufacturing: What You Need to Know: https://www.perforce.com/blog/vcs/digital-twin-manufacturing.

[54] Supply Chain Digital Twins – anyLogistix: https://www.anylogistix.com/features/supply-chain-digital-twins/.

[55] What is a Digital Supply Chain Twin? – AIMMS: https://www.aimms.com/story/what-is-a-digital-supply-chain-twin-and-how-can-it-support-your-strategic-decisions/.

[56] Digital Twins in Quality Control: https://medium.com/neurisium/digital-twins-in-quality-control-what-if-you-could-predict-changes-in-quality-102a2d26311a.

[57] "AI Accelerator Chips Overview and Comparison": https://hardwarebee.com/ai-accelerator-chips-overview-and-comparison/.

[58] "Startups challenging incumbents in AI accelerator chips, reveals GlobalData's Technology Foresights": https://www.globaldata.com/media/disruptor/startups-challenging-incumbents-ai-accelerator-chips-reveals-globaldatas-technology-foresights/.

[59] "Roadmapping the next generation of silicon photonics": https://www.nature.com/articles/s41467-024-44750-0.

[60] "Standards: The Next Step For Silicon Photonics": https://semiengineering.com/standards-the-next-step-for-silicon-photonics/.

[61] UCIe (Universal Chiplet Interconnect Express): https://www.uciexpress.org/

[62] Bunch of Wires (BoW) description: https://semiengineering.com/knowledge_centers/communications-io/on-chip-communications/bunch-of-wires-bow/

[63] OpenHBI description: https://www.opencompute.org/products-chiplets/477/openhbi-specification

[64] Diminishing Manufacturing Sources and Material Shortages (DMSMS): https://www.dsp.dla.mil/Programs/DMSMS/

[65] SD-22 DoD DMSMS Guidebook: https://www.dau.edu/cop/dsp/announcements/updated-sd-22-dod-dmsms-guidebook-now-available-assist-and-quicksearch.

[66] SD-26 DMSMS Contract Language Guidebook: http://everyspec.com/DoD/DoD-PUBLICATIONS/SD-26_01OCT2019_56848/.

[67] Government-Industry Data Exchange Program (GIDEP): http://www.gidep.org/

[68] Rigaku Innovative Technologies: https://www.rigakuoptics.com/euv.php

[69] "Big Changes Ahead For Photomask Technology": https://semiengineering.com/big-changes-ahead-for-photomask-technology/

[70] "ASML Dilemma: High-NA EUV is Worse vs Low-NA EUV Multi-Patterning Cost model for low- & high-NA EUV, Feature Fidelity, Technical Challenges": https://semianalysis.com/2023/12/11/asml-dilemma-high-na-euv-is-worse/

[71] "CD-SEM - What is a Critical Dimension SEM?": https://www.hitachi-hightech.com/global/en/knowledge/semiconductor/room/manufacturing/cd-sem.html

[72] "Intel and Nikon Litho Specialists Discuss Overlay Matching and Edge Placement Error for Production Beyond 20 nm": https://www.nikonprecision.com/ereview/spring_2013/news-02.html

[73] National Vulnerability Database: https://nvd.nist.gov/

[74] "5G Hardware Supply Chain Security Through Physical Measurements", NIST Special Publication 1278: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1278.pdf

[75] SEMI Supply Chain Management (SCM) initiative: https://www.semi.org/en/industry-groups/supply-chain-

management?utm_medium=email&utm_source=marketo&utm_campaign=HQ-WBN-20240517--SCM-Supply+Chain+Agility-AM

[76] "Quality and Reliability of 3D High-Performance Heterogeneous Integration through Die Stacking": https://meridian.allenpress.com/ism/article/2012/1/000249/34273/Quality-and-Reliability-of-3D-High-Performance

[77] "Digital twin with a perspective from manufacturing industry", H. Wang, et al., in Emerging topics in hardware security, Mark Tehranipoor, Ed., Springer, 2021: https://doi.org/10.1007/978-3-030-64448-2

[78] National Academies of Sciences, Engineering, and Medicine. 2024. Foundational Research Gaps and Future Directions for Digital Twins. Washington, DC: The National Academies Press: https://doi.org/10.17226/26894.

[79] PCI-SIG - Peripheral Component Interconnect Special Interest Group: https://pcisig.com/

[80] SUMMARY REPORT CHIPS R&D Chiplets Interfaces Technical Standards Workshop December 12–13, 2023; CHIPS R&D Digital Twin Technical Standards Workshop December 14–15, 2023: https://nvlpubs.nist.gov/nistpubs/CHIPS/NIST.CHIPS.1400-2.pdf

5.3. References for Section 4 National Standards Strategy for Critical and Emerging Technology Strategy

[1] FACT SHEET: Biden-Harris Administration Announces National Standards Strategy for Critical and Emerging Technology; https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2023/05/04/fact-sheet-biden-harris-administration-announces-national-standards-strategy-for-critical-and-emerging-technology/

[2] United States Government National Standards Strategy for Critical and Emerging Technology; https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/05/US-Gov-National-Standards-Strategy-2023.pdf

Appendix A. Semiconductors and Microelectronics Standards Working Group

Establishment

The Semiconductor and Microelectronics Standards Working Group (hereinafter referred to as the "SMSWG" or "Working Group") is established under the provisions of the charter of the Interagency Committee on Standards Policy (ICSP). The ICSP advises the Secretary of Commerce and the heads of other Federal agencies in matters relating to the implementation of OMB Circular A-119 and reports to the Secretary of Commerce through the Director of the National Institute of Standards and Technology (NIST).

Purpose

The objective of the SMSWG is to facilitate coordination of Federal agency semiconductor and microelectronics standards (SMS) activities, respond to requests for information, and develop recommendations relating to relevant standards policy matters to the ICSP. The SMSWG reports to the Chair of the ICSP and advises the members of the ICSP on relevant issues.

Functions

The SMSWG is responsible for:

- Assisting the ICSP in promoting effective and consistent federal policies in the area of semiconductor and microelectronics standards.
- Providing an annual report to the ICSP on the current SMS activities of participating Federal agencies and recommendations for strategic directions in relevant Federal standards efforts.
- Responding to requests for information and advising the ICSP on effective means of coordinating SMS activities with those of the private sector.
- Sharing best practices in semiconductor and microelectronics standards among Federal agencies.
- Coordinating Federal semiconductor and microelectronics standards interests across application areas such as transportation, energy, health, public safety, and others.

Organization

Participants include Federal agency representatives with expertise relevant to standards in semiconductor and microelectronics. Each participating Federal entity will identify one voting member to represent the entity. The SMSWG co-chairs comprise one NIST staff member designated by the ICSP Chair and serving as secretariat, along with other co-chairs as elected by majority vote of the SMSWG members present. The Working Group will follow a similar meeting schedule as the ICSP and

will meet at least three times each year. Other meetings may be called at the discretion of the co-chairs.

Approval and Renewal

Approved by the Interagency Committee on Standards Policy at its June 6, 2023, meeting. This charter expires three years after the date of approval unless renewed by the ICSP.

Appendix B. Abbreviations

AI - Artificial Intelligence

AMD - Advanced Micro Devices

AME - Advanced Microcircuit Emulation

ANSI - American National Standards Institute

ASME - American Society of Mechanical Engineers

ASTM - ASTM International (formerly known as American Society for Testing and Materials)

AutomationML - Automation Markup Language

BoW - Bunch of Wires

CD-SEM - Critical Dimension Scanning Electron Microscopy

CET - Critical and Emerging Technology

CMSD - Core Manufacturing Simulation Data

CoWoS - Chip on Wafer on Silicon

CPU - Central Processing Unit

CTE - Coefficients of Thermal Expansion

DHS - Department of Homeland Security

DLA - Defense Logistics Agency

DoD - Department of Defense

DMG - Data Mining Group

DMSC - Digital Metrology Standards Consortium

DMSMS - Diminishing Manufacturing Sources and Material Shortages

DNA - deoxyribonucleic acid

DoD - Department of Defense

DTC - Digital Twin Consortium

DTITG - Digital Twin Interoperability Task Group

EDA - Electronic Design Automation

EDA - Electrostatic Discharge Association

ESDA - EOS/ESD Association

EV - Electric Vehicles

EUV - extreme ultraviolet (EUV) light

GaN - Gallium Nitride

GEM - Generalized Emulation of Microcircuits

GEO - Geosynchronous Equatorial Orbit

GIDEP - Government-Industry Data Exchange Program

GPU - Graphics Processing Unit

GSA - General Services Administration

HPC - High-Performance Computing

HSM - Hardware Security Modules

IC - Integrated circuits

ICSP - Interagency Committee on Standards Policy

IEC - International Electrotechnical Commission

IEEE SA - Institute of Electrical and Electronics Engineers Standards Association

ISO - International Organization for Standardization

ITRS - International Technology Roadmap for Semiconductors

JEDEC - Joint Electronic Device Engineering Council

LEO - Low Earth Orbit

MCM - multichip modules

NAPMP - CHIPS National Advanced Packaging Manufacturing Program

NIST - National Institute of Standards and Technology

NSSCET - National Standards Strategy for Critical and Emerging Technology

OCP - Open Compute Project

OMB - Office of Management and Budget

OME - Observable Manufacturing Element

OMG - Object Management Group

OPC UA - Open Platform Communications Unified Architecture

OpenHBI - Open High Bandwidth Interface

PCI-SIG - Peripheral Component Interconnect Special Interest Group

QIF - Quality Information Framework

RTCA - Radio Technical Commission for Aeronautics

SAE - Society of Automotive Engineers

SDO - Standards Developing Organizations

SEMI - Semiconductor Equipment and Materials International

SHIP - The Defense Department's State-of-the-Art Heterogeneous Integrated Packaging Program

SiC - Silicon Carbide

SISO - Simulation Interoperability Standards Organization

SMS - Semiconductors and Microelectronics Standards

SMSWG - Semiconductors and Microelectronics Standards Working Group

SOSA - Sensor Open System Architecture Consortium

SSO - Standards Setting Organizations

TCG - Trusted Computing Group

TPM - Trusted Platform Modules

UCIe - Universal Chiplet Interconnect Express

US or U.S. - United States

USAF - United States Air Force

USN - United States Navy

USSF - United States Space Force

USTR - U.S. Trade Representative

VVUQ - Verification, Validation, and Uncertainty Quantification

VUQ - Validation and Uncertainty Quantification