

Semiconductor Manufacturing: Addressing Cybersecurity Risks and Traceability Gaps

Software and Supply Chain Assurance Forum

Melissa Grupen-Shemansky, PhD / CTO & VP Technology Coalitions / September 22, 2026

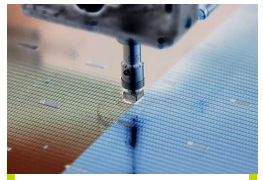
SEMI Connects the $3.0T+ Global Electronics Design and Manufacturing Supply Chain

SEMI OVERVIEW

From Chip Design to Electronics Systems



Design Automation
$15B



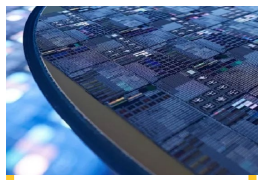
Materials
$72B
Subassemblies Components
$18B



Total Equipment
$107B



Assembly & Test Services
$40B



Semiconductors
$580B



Electronic Systems
$2.5T

SEMI

Smart Initiatives

SMART DATA-AI

SMART MANUFACTURING

SMART MEDTECH

SMART MOBILITY

Technology Communities

ESDA Electronic System Design Alliance

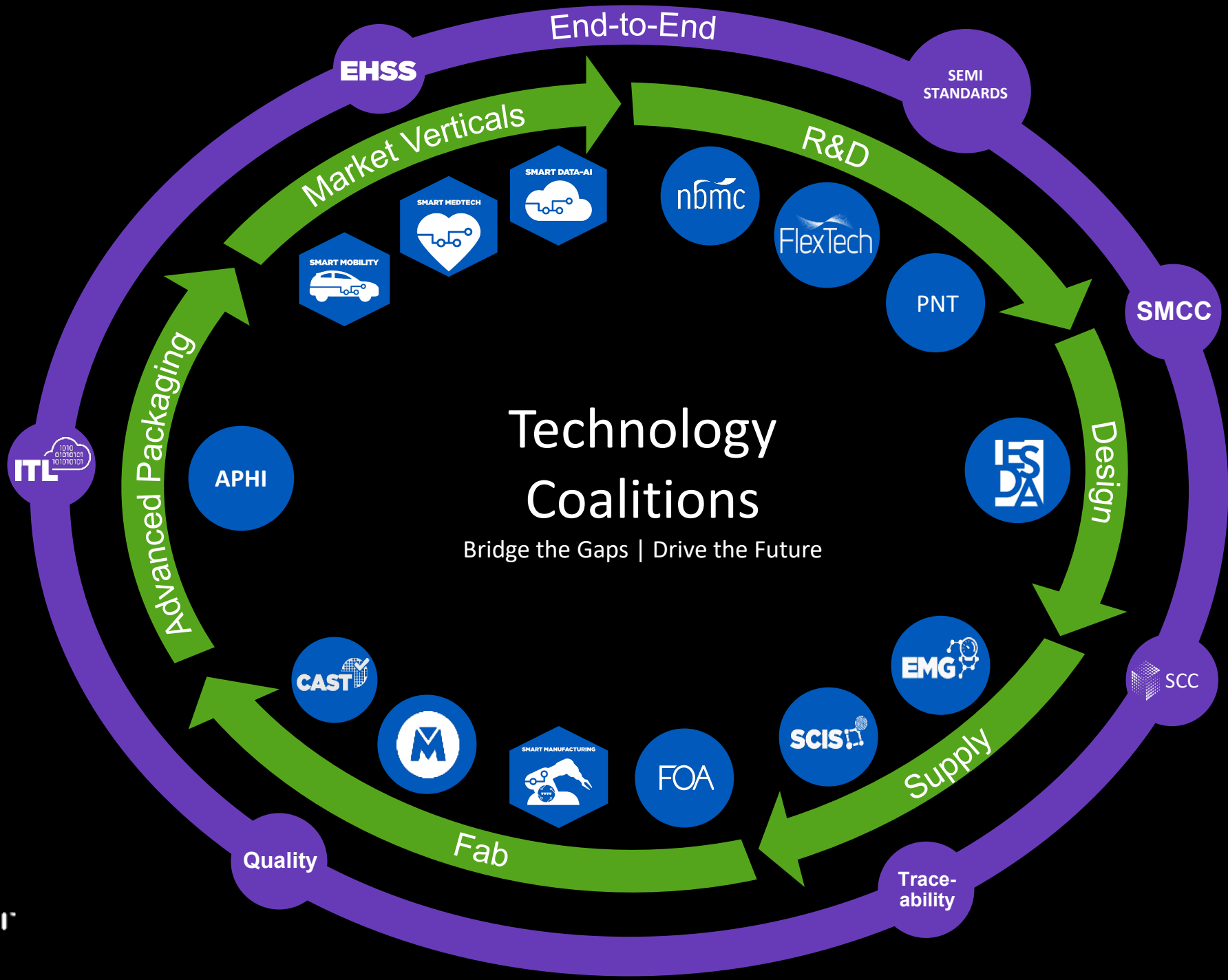
FOA fab owners alliance

FlexTech

MEMS & SENSORS INDUSTRY GROUP

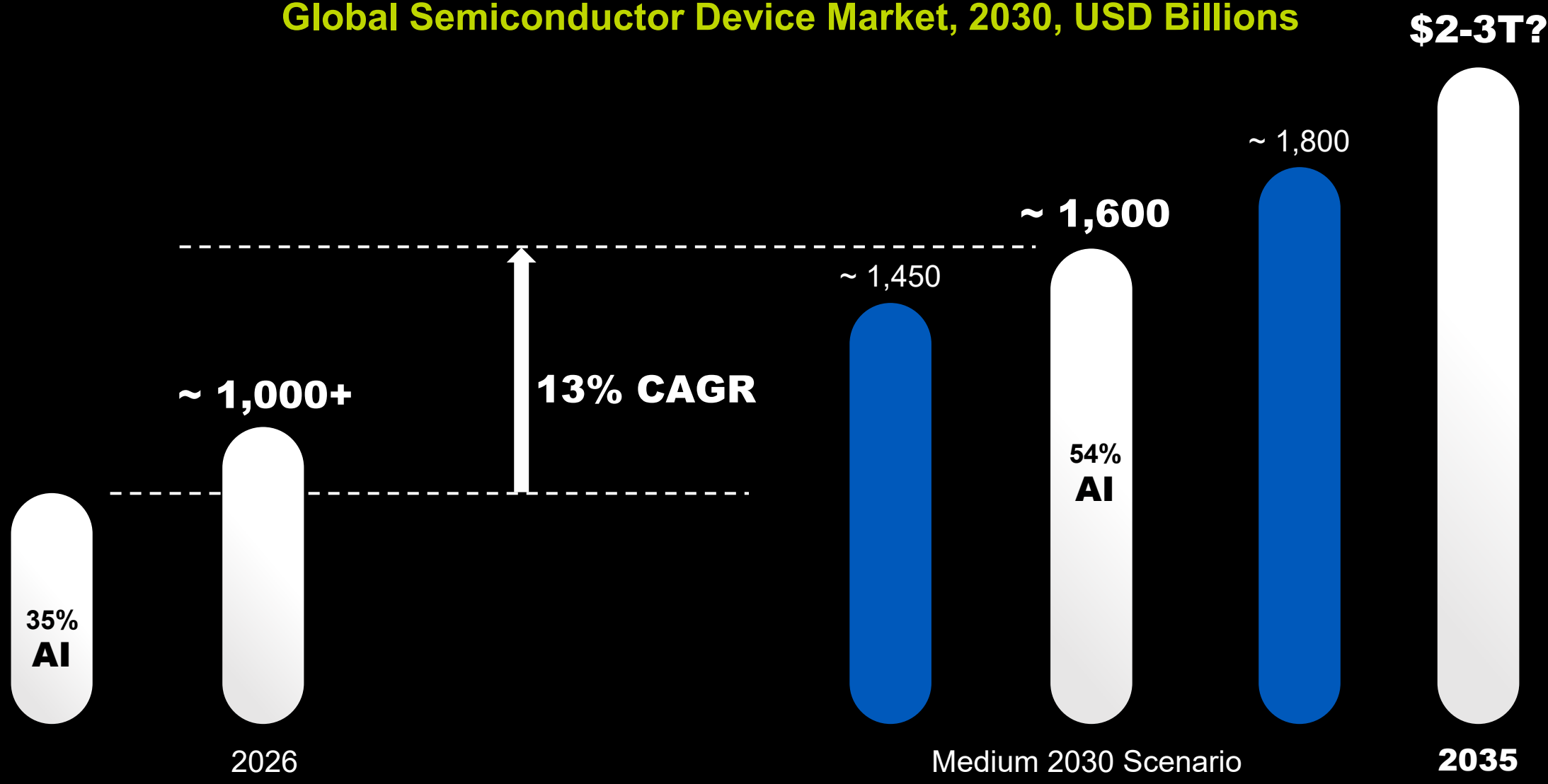
SOI industry consortium

2023 Market Data Estimates Sources: SEMI, IC Insights and TechInsights


End-to-End
EHSS
SEMI STANDARDS
SMCC
SCC
Trace-ability
Quality
ITL
APHI
Market Verticals
R&D
Design
Supply
Fab
Advanced Packaging
SMART DATA-AI
SMART MEDTECH
SMART MOBILITY
nbmc
FlexTech
PNT
ESDA
EMG
SCIS
FOA
SMART MANUFACTURING
CAST
Technology Coalitions
Bridge the Gaps | Drive the Future

Growth Beyond Prior Expectations – Fuelled by AI

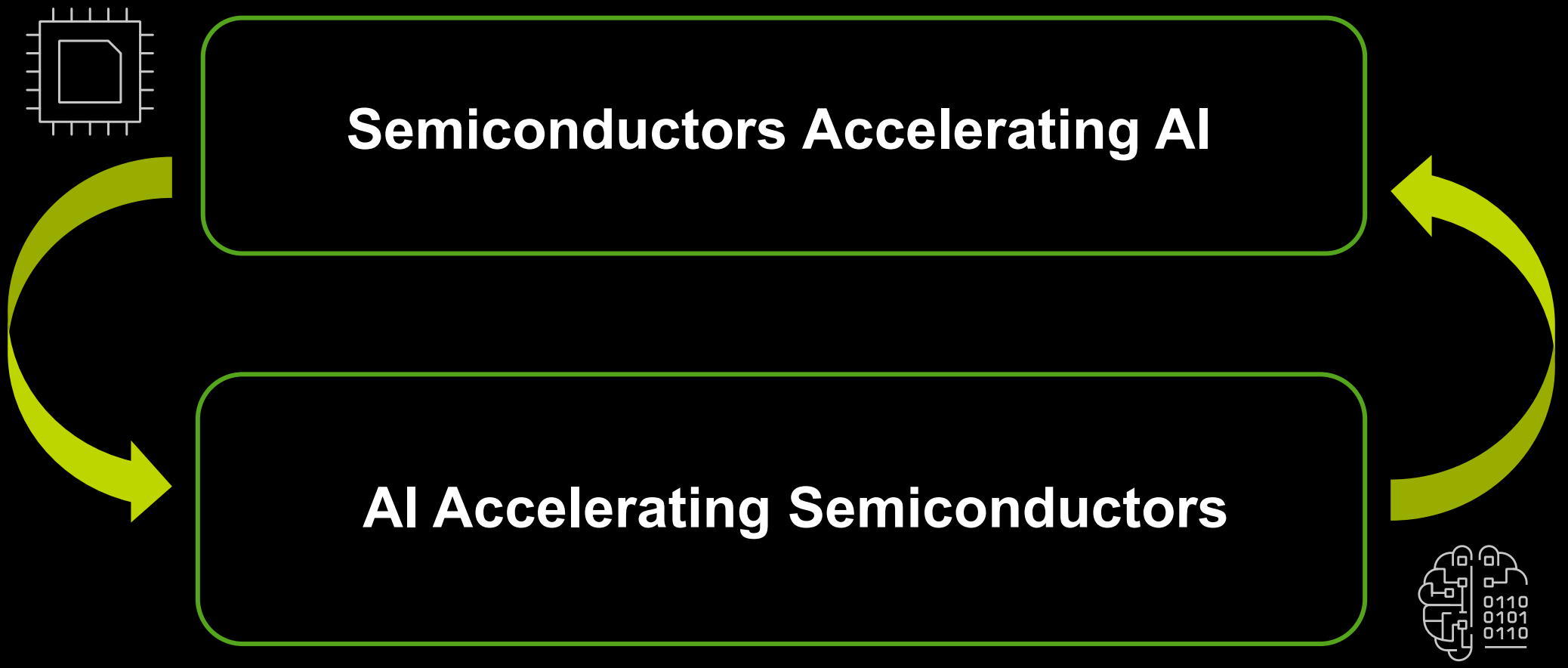
Global Semiconductor Device Market, 2030, USD Billions



Sources: SEMI and McKinsey & Co.

Virtuous Cycle of Semiconductors and AI

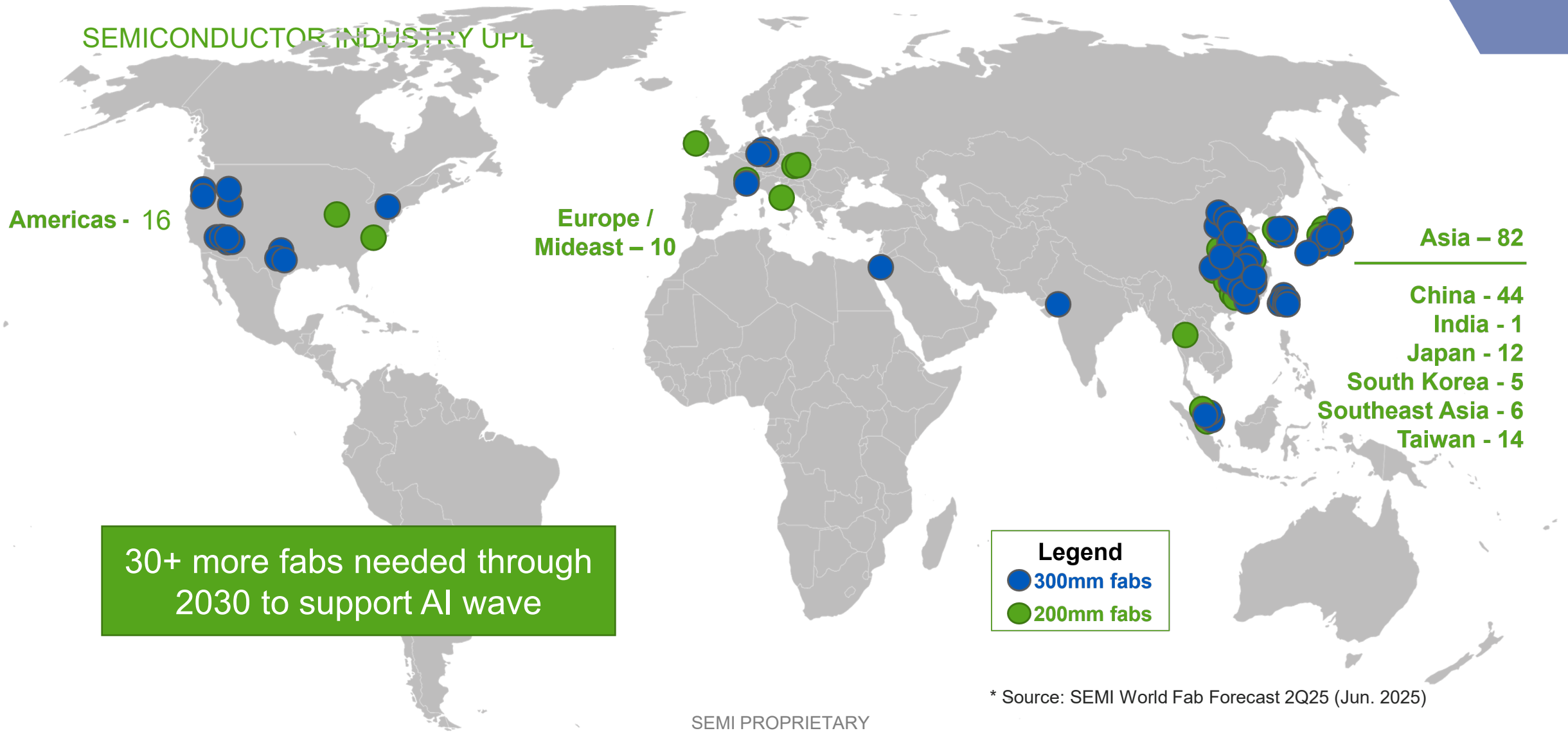
AI Helping to Advance Chips to Run More Powerful AI



semi™

Unprecedented Fab Expansions to Realize $1T

108 new fabs coming online between through 2028* - 90 in progress

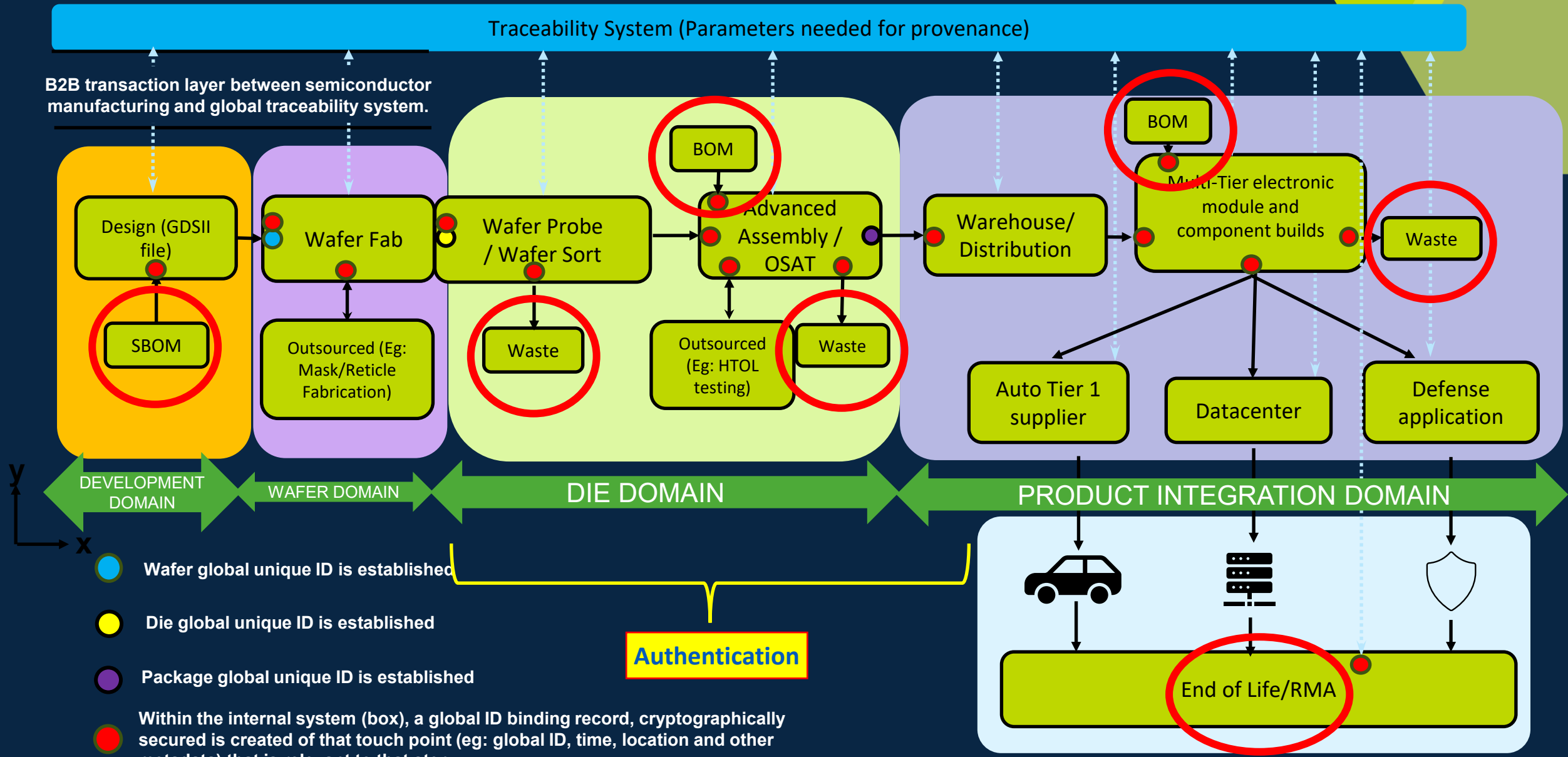


30+ more fabs needed through 2030 to support AI wave

* Source: SEMI World Fab Forecast 2Q25 (Jun. 2025)

SEMI PROPRIETARY

SEMI Phase 0 Chip Traceability: Journey from design to application



Motivation for Traceability

Question: What benefits can an industry wide scalable traceability system offer?

Supply Chain Visibility & Assurance

- Ensures accurate provenance of materials and genuine silicon
- Provides real-time, reliable information about any object in the supply chain.
- Enables consistent, interoperable data sharing across participants legitimizing data for high integrity AI, enhanced supply chain visibility, and supplier validation

Lifecycle Management and Sustainability

- Enables lifecycle tracking for reuse, recycling, and end-of-life management
- Improves monitoring of product reliability over time
- Can minimize error-prone human intervention improving efficiency, mitigate security vulnerabilities, and enhance forensics

Compliance and Governance

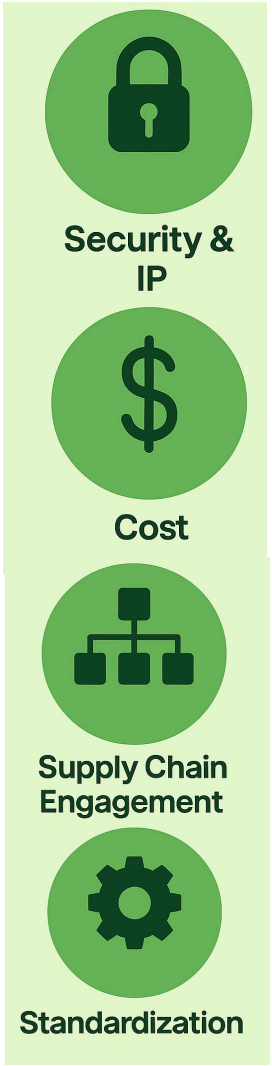
- Aligns industry with accepted standards and may support geo-regulatory and export control compliance

Competitive Advantage

- Stay ahead of non-participants of the traceability system
- Reinforces credibility through trusted parity among ecosystem members



Input from EDA, IDMs, Fabs, Fabless, & Solution Providers



Security and IP

- Risk of exposing sensitive or proprietary data during traceability processes and the inherent vulnerabilities from the traceability system.

Transparency vs. Confidentiality

- Balancing openness with the need to obfuscate proprietary data.

Data Integrity Issues

- Potential for wrong or misleading information about objects, impacting trust.

Full Supply Chain Engagement

- Difficulty in achieving compliance and participation across all tiers globally including industry and government stakeholders.
- Building a democratized, standardized framework across geographies is complex.

Cost Implications

- High infrastructure costs and unclear cost-benefit ratio for implementation.

Standardization Issues

- Lack of unified standards and governance, including no common traceability infrastructure, unclear ownership of a central record and difficulty integrating legacy devices and smaller suppliers.

AI-Driven Smart Factory Updated Roadmap

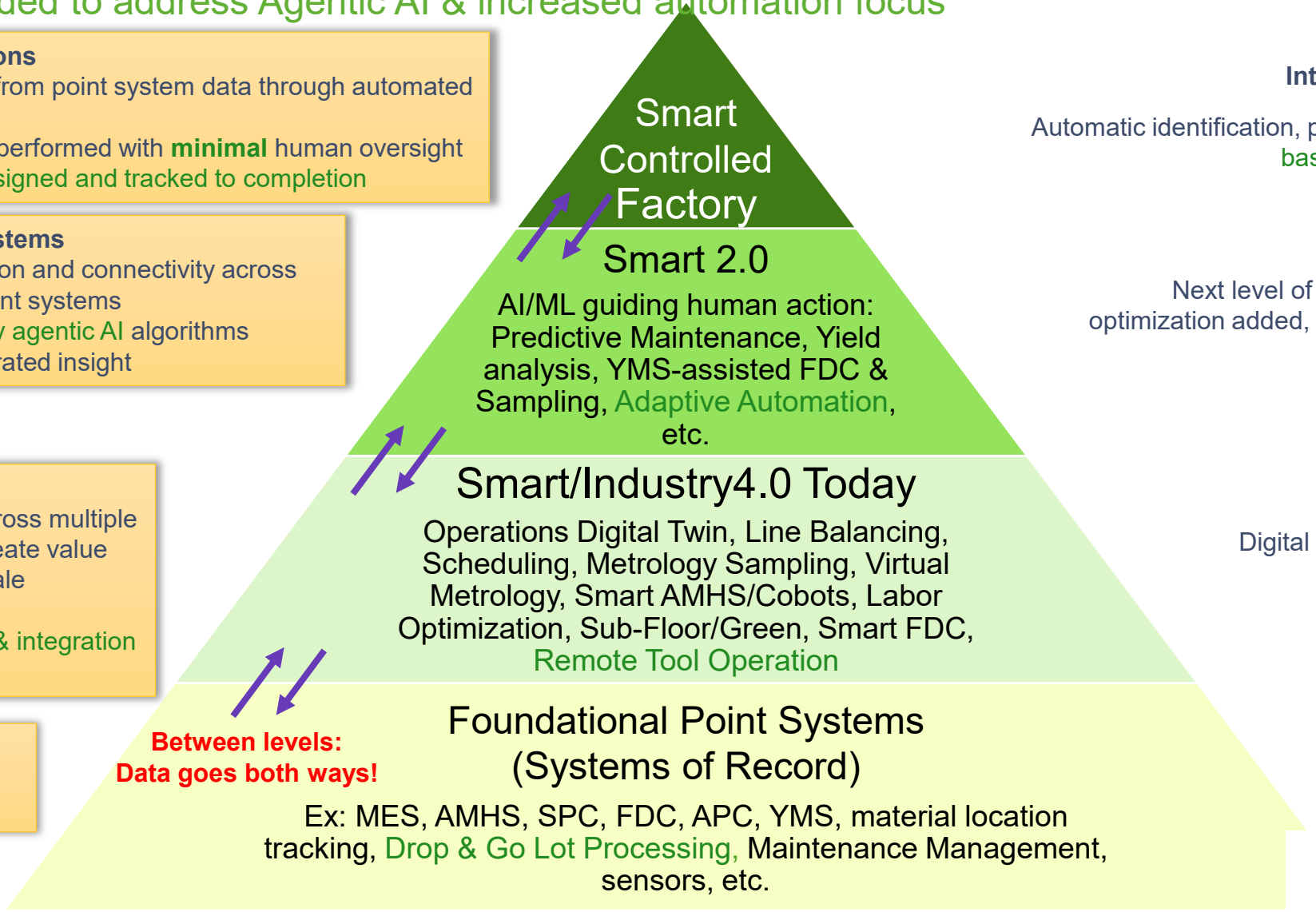
Green items added to address Agentic AI & increased automation focus

Autonomous solutions
- Closed loop action from point system data through automated learning/analysis
- Automated actions performed with **minimal** human oversight
- Optimized tasks assigned and tracked to completion

AI/ML-enhanced systems
- Novel data integration and connectivity across digital twins and point systems
- Deep learning, early agentic AI algorithms
- Automatically generated insight

Digital Twins
- Leveraging data across multiple point systems to create value
- Operations-time scale functionality
- Smart WIP routing & integration with automation

Point systems
- Application-specific data architecture



Integrated Autonomous Operation

Automatic identification, prioritization & assignment of tasks based upon real-time impact analysis

Smart Fab 2.0

Next level of Value with AI/ML, quality, & labor optimization added, integrated supply chain modeling

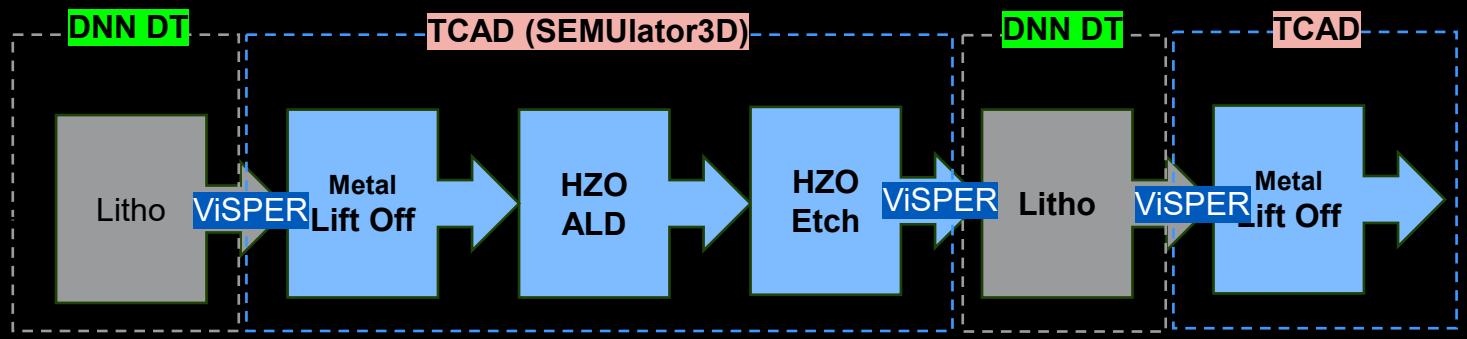
Today's Smart Fab

Digital Twin-Enabled Predictive Solutions

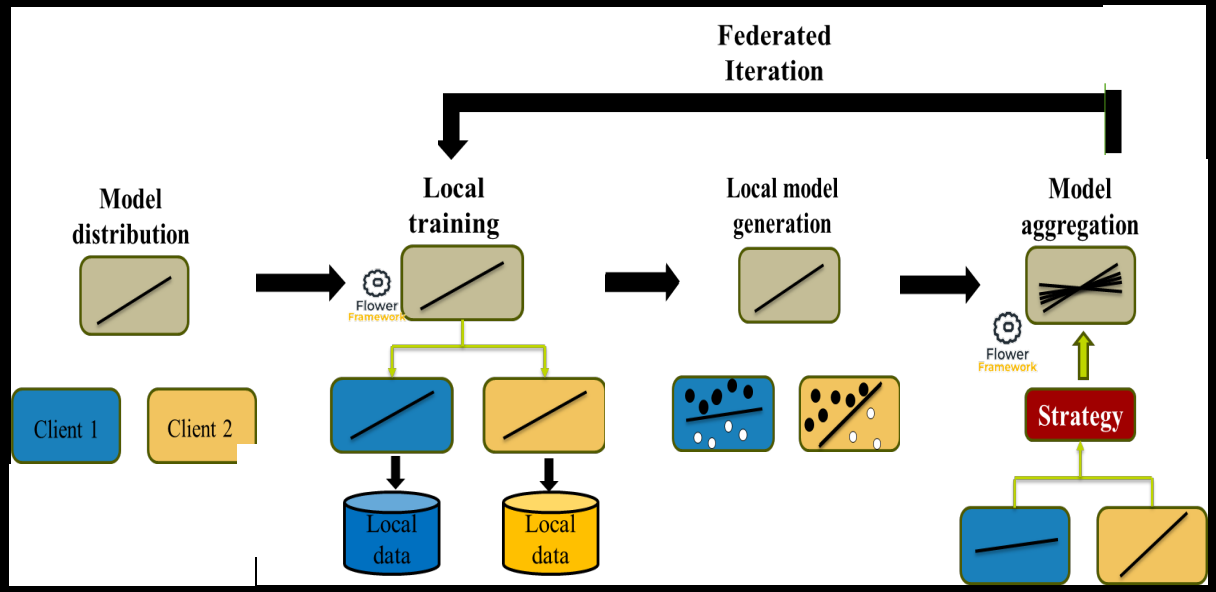
Legacy State of Practice Today

Point systems/ Systems of Record

Virtual Environment With Data/IP Security Using Federated Learning



Hybrid AI Environment with Digital Twins, Physical Data and Simulation



Federated Learning and Encryption to Enable Supply-Chain Collaboration

Sources: Flextech, Cornell University, Northeastern University

POSITION | The semiconductor industry needs a common way to connect cybersecurity requirements, implementation guidance, assessments, and operational practices across the semiconductor manufacturing lifecycle. SEMI SMCC is positioned to coordinate that effort across Equipment and Product Security, System Integration Security, and Fab Operational Cybersecurity, while supporting supply-chain assurance, standards and regulatory alignment, and workforce competence.

SMCC SEMICONDUCTOR MANUFACTURING CYBERSECURITY CONSORTIUM

Governing Council — Strategic oversight and bylaws & policies

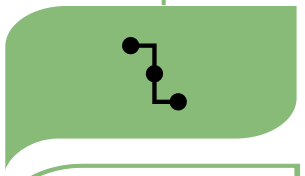
Steering Committee — Operational management, alignment



Operationalize and comply with SEMI E187 to ensure tools arriving in factories are cybersafe by default

Tue 5:00 PM PST

Standards Working Group (WG)



Establish methods for ecosystem (supply chain) security implementation and management

Mon 3:00 PM PST

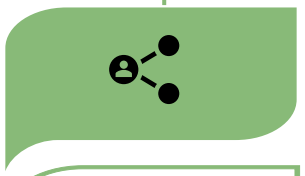
Supply Chain cybersecurity WG



Develop strategy for legislation & global standards such as NIST CSF 2.0, DFARS, IEC 62443

Thur 9:00 AM PST

U.S. Regulations WG



Architect comprehensive strategy for new & updated SEMI standards

Mon 4:00 PM PST

Pre-Standards engineering WG



Execute awareness campaigns for semiconductor cybersecurity

Fri 8:00 AM PST

Programs and Comms WG



Interpret CRA and educate the industry, develop a collective approach to implement EU CRA regulations

Wed 8:00 AM PST

EU Regulation and CRA WG



Understand local cybersecurity risks and coordinate with the larger SMCC.

Language: Korean

NEW: South Korea cybersecurity WG

SEMI's SMCC Next 5 Years

ROADMAP PRIORITY	2027 ESTABLISH	2028 EVALUATE	2029 FINALIZE	2030 INTRODUCE	2031 SUSTAIN
Equipment & Product Security	Align guidance with E187 certification; baseline OEM readiness against the 12 published requirements; expand notification beyond Taiwan; begin Security Level preparation later in the year	Use certification results within scope; track anonymized OEM progress; broaden validation support	Refine evidence use; address recurring validation findings through SEMI groups and scheme owners	Publish guidance; expand regional adoption; help device makers use certification results	Maintain guidance, supplier notification, validation and readiness tracking
System Integration Security	Define integration profile, assessment scope, certification criteria, asset visibility and Layer 3-to-0 segmentation expectations	Evaluate profile and assessment methods in representative new-build integrations, including critical-asset micro-segmentation	Evaluate brownfield and change cases; finalize scheme rules, body requirements and architecture evidence	Introduce the proposed SEMI system-integration certification scheme; publish guidance ◆	Review results; maintain profile, scheme, surveillance, reassessment and segmentation baselines
Fab Operational Cybersecurity	Define Operational Cybersecurity Guidance: secure connectivity, managed file transfer, AI risks, ACSSA applicability	Evaluate draft guidance in new-build and brownfield environments, including remote support and AI oversight	Finalize guidance for brownfield, recovery, compensating controls, engineering access, provenance, failure handling	Publish operational guidance and supporting resources for connectivity, file transfer and AI-enabled systems	Review implementation experience; update access, monitoring, recovery and AI-risk practices
Supply-Chain Assurance & SSCA	Define evidence, review status, validity, confidentiality, sharing and reassessment expectations	Apply the model in representative supplier-customer cases	Refine evidence sharing, reuse and reassessment guidance	Publish and support the SSCA implementation and evidence-use guide	Review adoption and maintain the guide
Standards & Regulatory Alignment	Establish the alignment matrix, including EU CRA, EU machinery requirements, CMMC, scope and applicability	Review mappings; identify overlap, gaps and duplicate evidence demands, including E187 and EU CRA	Publish coverage and gap findings; identify evidence that can and cannot be reused	Expand and maintain the published matrix for supplier and market use	Update the matrix when standards, regulations, guidance or market requirements change
Workforce Competence & Personnel Certification	Complete job and task analysis; define the competence framework; assess OT and fab skills gaps	Design the common core, three role pathways, assessments, governance and AI-focused education	Validate assessments; refine the certification scheme against observed OT practices	Introduce the proposed SEMI personnel certification program; expand education ◆	Evaluate results; maintain certification, recertification and employer-feedback mechanisms

◆ Proposed SEMI certification scheme introduced

SCCA = Standardized Semiconductor Cyber Assessment

Vision Papers

To begin publication release October 2026

- Advanced Materials
- Advanced Packaging and Heterogeneous Integration
- Cybersecurity
- Data/AI/Energy Efficient Compute/ Quantum
- Smart Medtech
- Compound Semiconductors
- Photonics
- Smart Manufacturing
- AI and Metrology

SEMI Workshops and Symposia

2023

- Digital Twins in Semiconductor Manufacturing| SEMI | Milpitas, CA | December 2023
- Future of Computing: Domain Specific Architectures, McKinsey & Co. and SEMI | Milpitas, CA | October 2023

2024

- From Concept to Reality: Advancing Digital Twins in Semiconductor Manufacturing | Milpitas, CA | December 2024
- Future of Computing Technology | SEMICON West July 2024

2025

- Agentic AI for Next-Generation Semiconductor Manufacturing | Milpitas, CA | June 2025
- Future of Computing: Sustainable AI Systems | Milpitas, CA | March 2025
- Future of Computing Technology Session | SEMICON West | October 2025

2026

- Smarter Sensors, Smarter Fabs: AI at the Edge in Semiconductor Manufacturing | Milpitas, CA | March 2026
- AI Techniques in Semiconductor Manufacturing | Milpitas, CA | August 2026
- Future of AI Computing: Bending the Power and Performance Curve | City of San Jose and SEMI | San Jose, CA | September 2026

THANK YOU

megshemansky@semi.org

