An Industry Plan for Semiconductor Cybersecurity

PRESENTER: Mayura Padmanabhan / Technical Project Manager / **SEMI**

ABSTRACT:

Semiconductor manufacturing facilities face mounting cybersecurity threats as high-value targets containing billions of dollars in intellectual property and equipment. Attacks range from financially motivated criminal groups to well-funded nation-state operations, both of which pose serious risks to production integrity and corporate secrets. The complexity of chip fabrication—reliant on a vast ecosystem of third-party tools, software, and services—introduces vulnerabilities throughout the supply chain. Recent data suggests that over 65% of security incidents in semiconductor factories originate from supply chain breaches. Addressing these challenges requires sweeping, coordinated changes to how equipment and systems are delivered, integrated, and maintained. However, imposing rigorous security standards without burdening innovation or cost presents a delicate balance.

To meet this challenge, SEMI has launched the SEMI Manufacturing Cybersecurity Consortium (SMCC), a global community uniting fabs, fabless firms, equipment makers, software providers, and other stakeholders. Together, members are developing collaborative frameworks and driving adoption of the SEMI E187 cybersecurity standard—designed to ensure secure, scalable compliance across all stages of manufacturing. This session will explore industry-wide implications of semiconductor cybersecurity, discuss SMCC's strategic vision, and introduce pathways for E187 compliance.