An Industry Plan for Cybersecurity

Brian Korn
bdkorn@gmail.com

Doug Suerich
PEER Group Inc.
doug.suerich@peergroup.com

Andrew Seward
Tokyo Electron America Inc.
andrew.seward@us.tel.com

Mayura Padmanabhan
SEMI
mpadmanabhan@semi.org

Abstract — Semiconductor factories are high value targets for cyberattacks. Protecting factories is challenging: the complex chip manufacturing process requires a web of third-party equipment, computer devices, and software – any one of which could expose a vulnerability that hackers can exploit. This paper explores the collaborative efforts of industry players to develop greater security through cooperation.

Keywords — cybersecurity, standards, semiconductor manufacturing, consortium

I. INTRODUCTION:

Cyber threats continue to increase at alarming rates, for instance According to Forbes, 2023 saw a 72% increase in data breaches since 2021, which held the previous all-time record **[8]**. The Federal Bureau of Investigation's (FBI) 2023 Internet Crime Report further revealed an 81% rise in financial losses due to cybersecurity complaints, escalating from $6.9 billion to $12.5 billion **[7]**.The semiconductor industry has become a prime target for cyberattacks due to the world's economic dependence on its technology. As a foundation of modern innovation, semiconductor manufacturing supports critical sectors ranging from consumer electronics to defense, making it a principal objective for nation-state actors, financially motivated attackers, and supply chain disruptions. Its highly interconnected global supply chain and reliance on cutting-edge science and engineering further compound its cybersecurity challenges. This paper details the SEMI Manufacturing Cybersecurity Consortium's (SMCC) efforts to develop and promote cybersecurity standards and best practices tailored to the semiconductor industry. Through collaborative working groups the SMCC has developed standards for equipment compliance (SEMI E191), as well as frameworks for supply chain security, and regulatory alignment. Additionally, the consortium facilitates cross industry information sharing initiatives, even among competitors, to rapidly identify and mitigate emerging threats. By leveraging standardized approaches, SMCC helps semiconductor manufacturers greatly enhance security while achieving cost efficiencies while reducing the burden of redundant security efforts across the supply chain.

Semiconductor factories are high value targets for cyberattacks, they are integral to a critical global industry and contain billions of dollars' worth of equipment, intellectual property, and trade secrets. Attacks can originate from opportunistic groups seeking financial rewards or nation-state actors using large teams with vast resources. Protecting factories is challenging: the complex chip manufacturing process requires a web of third-party equipment, computer devices, and software – any one of which could expose a vulnerability that hackers can exploit. Recent reports indicate that more than 65 per cent of cybersecurity incidents at semiconductor factories had a root cause starting within the supply chain. A unified, proactive cybersecurity strategy can prevent costly security breaches and reduce redundant compliance efforts, making security investments more efficient compared to the fragmented approaches of the past.

Defending the industry against cyberattacks requires active participation and consensus building from all members and levels of the semiconductor manufacturing supply chain. Furthermore, Digital Twins, Artificial Intelligence (AI) and other digital technologies are emerging as critical for industry growth, collaboration and the strengthening of regional supply chains across the world. For example, Cybersecurity will be a critical enabler for efforts like the MFG USA Institute being launched in the auspices of the U.S. Department of Commerce and NIST. Meeting these challenges will require fundamental changes to how equipment and software are delivered and supported within the factory environment. At the same time, these changes must balance security with cost and efficiency considerations, making this a challenging endeavor. "Success" in this endeavor will only be achieved through an unprecedented level of community-driven collaboration that has never been attempted in the semiconductor industry.

By forming the SEMI Manufacturing Cybersecurity Consortium (SMCC), SEMI is taking the lead in coordinating a response to this challenge. The SMCC is a global technical community comprised of factories, fabless, equipment manufacturers, software vendors, academia and other members of the supply chain **[2]**.

The SMCC is guided by the following vision and mission:

Vision: Strengthen cyber resiliency of the global semiconductor supply chain against the evolving threat environment.

Mission: Develop and promote a practical, standards-based, industry-wide approach to improving cybersecurity and resiliency throughout the semiconductor supply chain.

I. APPROACH

Under the direction of the SMCC Governing Council, seven working groups (WG) have been formed to realize the vision and mission statements:

WG1 – Factory Cybersecurity Implementation and Compliance

Starting with existing SEMI cybersecurity standards for equipment (SEMI E187 and SEMI E188), building a list of agreed upon interpretations and actions is required. The goal is to achieve a single consensus on how to operationalize these standards so that tools and equipment arriving at any factory are cybersafe by default, and security can be maintained over time. The goal also is to recommend remediation methodologies for nonconformance and establish guidelines for vendors to assert compliance either through self-certification or formal third-party certification

WG3 - Supply Chain Cybersecurity

This working group aims to minimize supply chain cybersecurity risks and accelerate best practice adoption by establishing a standardized approach for evaluating corporate cybersecurity readiness across all supply chain members. The goal is to create one standardized checklist for companies to evaluate each of the members of their supply chain, reducing the burden of redundant security audits. This approach minimizes compliance costs for both suppliers and customers while ensuring consistent cybersecurity readiness across the industry.

WG4 - Standards and Regulations

Integrate existing SEMI cybersecurity standards with the expanding array of global cybersecurity frameworks, guidelines, and legislation relevant to semiconductor manufacturing for greater ease of comprehension and adherence. While other industries have made significant advancements in this area, the semiconductor industry has an opportunity to adopt proven best practices. This initiative will include the creation of the NIST Cybersecurity Framework Semiconductor Community Profile and a comparative analysis of the SEMI standards against other common global publications such as the EU Cybersecurity Act, Defense Federal Acquisition Regulation Supplement, CHIPS Technology Protection Handbook, , ISA/IEC 62443 and others.

WG5 - Threat Sharing

Already, most cybersecurity impacts in our industry begin in the supply chain. Bad actors work quickly to find and exploit vulnerabilities and due to the significant supply chain overlap between competitors in the semiconductor industry, an attack on one vendor is likely to be rapidly expanded to attack others. Establishing an effective mechanism for sharing information about active threats between trusted industry participants will accelerate deployment of defense measures and mitigation of attacks.

WG6 - Cybersecurity Pre-Standards Engineering

Existing SEMI standards for cybersecurity are a good start, but more are required. Guiding the formal standards process with input from front line practitioners and real-world experience will streamline the process and result in higher quality standards. Standards need to be used in a consistent manner across different geographies and be well coordinated across multiple task forces operating in parallel. This working group works on macro-level guidance for the standards development groups.

WG7 – Outreach, Communications, and Events

The primary goal of this working group is to focus on providing educational resources and tools to reduce the cybersecurity impact that can be leveraged by small to large companies in our supply chain. This working group will also coordinate participation in key SEMI and other industry events. Ultimately, this group will identify collaboration opportunities ensuring all SMCC efforts are engaged.

WG8 – EU Regulation and Cyber Resilience Act (CRA)

On October 10, 2024, the European Union adopted the Cyber Resilience Act (CRA) **[6].** This broad new law introduces strict cybersecurity requirements for products with digital elements that are sold inside the EU. While primarily designed for consumer-facing products, the interpretation of the CRA is likely to include many elements of semiconductor manufacturing as well, including factory equipment. The potential financial penalties associated with the CRA are large. This group will seek to better interpret the precise impact of the CRA on SMCC members, and to educate and inform all industry players on how best to comply.

II. PROGRESS TO DATE

Since being inaugurated at SEMICON West in July 2023 **[1]**, the SMCC has made significant progress in laying the foundation to solve these industry challenges. A group of more than 180 representatives from 65+ industry leading companies are contributing time and expertise to the initiative. This includes two of the largest device makers, and seven of the top 10 OEMs measured by sales. The list of participants continues to grow.

Three early, tangible results have been: A) The joint creation of a community cybersecurity profile in conjunction with NIST Cybersecurity Framework 2.0, B) The development and publication of SEMI E191, a new cybersecurity standard, and C) A community led effort to ascertain the impact of the EU Cyber Resiliency Act

A. NIST CSF2.0 Semiconductor Manufacturing Profile

In May 2024, The National Cybersecurity Strategy Implementation Plan v.2 [4] specified initiative 5.5.5 “Develop guidance for secure development and manufacturing of semiconductors”. This directed NIST to collaborate with the semiconductor industry to develop guidance to secure this critical supply chain, with a target completion date in the third quarter of 2025.

Starting in February 2024, the SMCC WG4, partnered with NIST to write and advance this community profile specifically targeted to semiconductor manufacturing. This new profile is based on the NIST Cybersecurity Framework 2.0 and has been tailored to meet the specific needs of the semiconductor manufacturing environment and industry best practices. The document is intended to be used as part of a voluntary, risk-based approach to managing risks, and is not intended to replace existing standards and industry guidelines.

The document provides a “Target” profile that identifies desired cybersecurity outcomes and can be compared against the “Current” profile for a given entity. The document provides details on scope and three specific domains of interest.

1. Development of Secure Equipment and Tooling
2. Fab Environment
3. IT Infrastructure in Semiconductor Manufacturing

The profile has now been released and is open for public comment.

B. E191 – Specification for Computer Device Cybersecurity Status Reporting

In March 2022 **[5]**, SEMI Equipment Automation Software Technical Committee released two standards related to cybersecurity:

1. SEMI E187: Specification for Cybersecurity of Fab Equipment

2. SEMI E188: Specification for Malware Free Equipment Integration

These two standards provide a first generation of support for cybersecurity standards as the pertain to the design and maintenance of tools within the fab. SMCC members identified an opportunity to enhance these standards by creating a reporting mechanism specific to semiconductors to allow for the collection and monitoring of key variables related to cybersecurity. Based on input from WG6, the North American Fab & Equipment Computer and Device Security (CDS) Task Force developed E191 and E191.1, a set of standards that specify how tools can report operating system version information and other details to the factory over existing SECS/GEM communication channels. Once implemented, these standards will simplify the complex task of monitoring cybersecurity status of the hundreds or thousands of tools in a modern fab environment.

Future work may expand the scope of SEMI E191 to include additional variables, including malware and vulnerability scanning details, such as: engine used, last scan result, and more. These expansions will be based on broad-based community input facilitated by the SMCC and codified into standards by the CDS.

C. European Union Cyber Resiliency Act

On November 20th, 2024, the European Union officialy brought the Cyber Resilience Act (CRA) into force **[6].** This act creates broad rules for common cybersecurity standards for products with digital elements in the EU. These standards will certainly impact the products and devices that are the outputs from the semiconductor industry, but also impact the inputs, in particular the tools and equipment used during the manufacturing process. The act allows for a two year period for manufacturers to implement the new requirements, and a further one year to implement vulnerability and incident reporting. Given the complexity and long lead times normally associated with changes to advanceed semiconductor manufacturing tools and equipment, OEMs and Fabs will need to act quickly to become compliant.

Achieving compliance with the CRA is challenging due to a lack of common understanding of exactly what the law requires in the semiconductor manufacturing space. Emulating the success of WG4 in establishing a productive relationship with government entities to provide clarification and industry specific guidelines, Workgroup 8 has formed to achieve the folowing goals:

1. Understand the impact of the CRA on the ecosystem
2. Inform SEMI members and SMCC workgroups, and work towards aligned standards
3. Act as the representative of the semiconductor ecosystem in CRA standardization groups, and promote SEMI standards as a compatible solution for compliance

III. Next Steps

To date, SMCC has investigated the following roadmap items while achieving consensus on key foundational initiatives:

1) WG1,2- Factory Cybersecurity Implementation and Compliance

- Adopt an aligned definition of a supported operating system for compliance with E187.
- Create an industry adopted framework on patching and anti-virus strategy for production tools.
- Provided input on the development of a new set of SEMI Cybersecurity Standards (starting with E191) to collect information from factory network-facing computing devices to help equipment users assess what kind of cybersecurity risk they present.

2) WG3 – Supply Chain Cybersecurity

- Align on a universal supplier and sub-supplier cybersecurity questionnaire and assessment methodology.

3) WG4 – Standards and Regulations

- Create an executive dashboard of worldwide active and pending legislation and how these interact with semiconductor manufacturing standards, specifications, and requirements.
- Partnered with National Institute of Standards and Technology (NIST) for the development and adoption of a NIST Cybersecurity Framework 2.0 Profile for Semiconductor Manufacturing. This collaboration is important to identify and reduce cybersecurity challenges in semiconductor manufacturing.

4) WG5 – Threat Sharing

- Develop methods for cyber threat intelligence sharing that respect legal and SEC compliance constraints.

5) WG6 – Cybersecurity Standards Engineering

- Develop instructional material for the other workgroups to help them decide between creating new standards vs. advisory documents or other deliverables, and how to approach each option.

6) WG7- Outreach, Communications & Events

- SMCC marketing includes websites, newsletters, and social media. Coordinate participation in key SEMI and industry events. Provide educational resources and tools to reduce the cybersecurity impact that can be leveraged by small to large companies in our supply chain.

7) WG8- EU Regulation and CRA

- Perform a gap analysis between the CRA standards and the SEMI Cybersecurity Standards Suite, and the International Electrotechnical Commission (IEC) risk management process. Use the findings to create resources that help EU-based companies understand the CRA's impact and ensure compliance.

IV. Conclusion

The high value and visibility of the semiconductor manufacturing industry makes it inevitable that cyberattacks will continue to occur, and are likely to increase in both frequency and sophistication. To protect itself in an economical and effective fashion, the industry must collaborate to find the best possible solutions and countermeasures. Early work by the SMCC has proven the capability and commitment of industry players to look beyond short term commercial interests and competition to collaborate on finding these solutions. This initiative will continue to evolve.

REFERENCES

[1] D. Suerich and B. Korn, "New SEMI Cybersecuirty Consortium Sets Out to Strengthen Semiconductor Manufacturing Supply Chain Network Protections," 2 11 2023. [Online]. Available: https://semi.org/en/blogs/technology-and-trends/new-semi-cybersecurity-consortium-sets-out-to-strengthen-semiconductor-manufacturing-supply-chain-network-protections.

[2] S. Rambo, "Chip Industry Needs More Trust, Not Zero Trust," 13 7 2023. [Online]. Available: https://semiengineering.com/chip-industry-needs-more-trust-not-zero-trust/.

[3] J. Amano, "SEMI Publishes First Cybersecurity Standards," SEMI, 1 March 2022. [Online]. Available: https://www.semi.org/en/standards-watch-2022-March/SEMI-publishes-first-cybersecurity-standards. [Accessed 5 February 2025].

[4] European Union, "Regulation 2024/2487," 23 October 2024. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2024/2847/oj. [Accessed 06 02 2025].

[5] The White House, "National Cybersecurity Strategy Implementation Plan - version 2," The White House, Washington, DC, 2024.

[6] Identity Theft Resource Center, "ITRC Annual Data Breach Report," ITRC, El Cajon, CA, 2023.

[7] Federal Bureau of Investigation, "Internet Crime Report," Internet Crime Complaint Center, Washington, DC, 2023.

[8] "Cybersecurity Framework Profile for Semiconductor Manufacturing," NIST, 4 February 2025. [Online]. Available: https://www.nccoe.nist.gov/projects/cybersecurity-framework-profile-semiconductor-manufacturing. [Accessed 4 February 2025].

[9] M. S. John, "Cybersecurity Stats: Facts and Figures You Should Know," 28 August 2024. [Online]. Available: https://www.idtheftcenter.org/publication/2023-data-breach-report/.