Semiconductor Manufacturing Cybersecurity Consortium

Andrew Seward
- SEMI SMCC Supply Chain Cybersecurity Co-Chair
- Marketing and Analytics Manager – TEL

Jennifer Lynn
- SEMI SMCC Steering Committee Member
- SEMI SMCC Regulations and Standards Chair
- Cyber Defense Leader, IBM Semiconductors

NIST/National Cybersecurity Center of Excellence
Rockville, MD
27 Feb 2024
SEMI at Its Founding in 1970

<10 members, all U.S.-based

- Thought Leadership
- Standards
- Expositions/Conferences
- EHS
50+ Years Later: SEMI is More Than Ever and Growing!

<table>
<thead>
<tr>
<th>2024 Top Priorities</th>
<th>~3,100 members worldwide</th>
</tr>
</thead>
<tbody>
<tr>
<td>Talent Development, DEI &amp; e-learning</td>
<td>• Advocating for free and open global markets</td>
</tr>
<tr>
<td>Smart Initiatives</td>
<td>• Leading workforce development efforts</td>
</tr>
<tr>
<td>Think Tanks</td>
<td>• Connecting members</td>
</tr>
<tr>
<td>Supply Chain Management &amp; Cybersecurity</td>
<td>• Nurturing pre-competitive collaboration</td>
</tr>
<tr>
<td>Sustainability</td>
<td>• Accelerating innovation</td>
</tr>
</tbody>
</table>

- **Thought Leadership**: 1,000+ Standards
- **Worldwide Offices**: 2,300+ Program Hours
- **Market Intelligence Reports**: Tech partners: imec, Fraunhofer, CEA-Leti, IEEE, ITRI, AIST
- **Expositions/Conferences**: 170+ Tech Programs
- **EHS/ESG**: 20+ Tech Communities
- **Strategic Tech Communities**: ESDA, FOA, FlexTech, MSIG, SOIC

CONNECT - COLLABORATE - INNOVATE - GROW - PROSPER
Bringing the Supply Chain Together through Key SEMI Initiatives

Your gateway to the ~$2.8T electronics supply chain
(Expected to grow to $4.5T+ by 2030)

4th Industrial Revolution → Industry 5.0

- Robotics
- 3D Printing
- Smart Infrastructure
- Cybersecurity
- Realtime Configuration

SMART MANUFACTURING

SMART DATA-AI
- AI
- Quantum Computing
- Machine Learning
- 5G to 6G
- Near-zero fatalities

SMART MOBILITY
- Electric Vehicles
- Smart City
- Driver Assistance
- Fleet
- Smart City

SMART MEDTECH
- Human Performance Monitoring
- Fitness Tracking
- Wearables

SMART AUTOMATION
- Design Automation
- Assembly & Test Services

SEMI OVERVIEW

Bringing the Supply Chain Together through Key SEMI Initiatives

- Near-zero fatalities
- Zero Emissions

4th Industrial Revolution

- 4th Industrial Revolution
- Industry 5.0

2022 Market Data Estimates Sources: SEMI, IC Insights and TechInsights
Cyber Attacks Against Manufactures on the Rise

Details Impact of Computer Virus Incident

One of Apple's key chip manufacturers was hit with a virus that targets Windows computers — and it took nearly 3 days to recover

A bad day at the office

Computer virus cripples top Apple supplier

Used with permission
Suerich, D – PeerGroup (2023, July). Getting to “Safe” [PowerPoint Presentation], Semicon West 2023
Evolution of the SMCC
Problem Statement
The incidence of cyber threats is surging at an alarming rate year over year, leading to a continuous escalation of cybersecurity risks and their consequential impacts, all while implementation of solutions lag behind.

Objectives
- Establish a broad methodology for cybersecurity for manufacturing that incorporates lessons learned and embraces open collaboration
- Develop and promote a standards-based, semiconductor industry-specific framework to improve cybersecurity and accelerate implementation of actionable solutions for the entire supply chain
- Incorporate best practices from industries such as automotive and medical with the aim to modernize factory security protocols

SMCC Philosophy - Coordinated Global Effort
- Cybersecurity risks are solvable problems
- Time is now to fully protect our industry's ability to function
- Don't let "perfect" be the enemy of "good enough"
  - Constraints like efficiencies, cost effectiveness and utilizing the best solution can & will come later
  - Collaborative & creative forums are the fastest method to identify solutions

Approach
- Formation of a SEMI Technology Community to collaborate with our member companies, leveraging expertise and best practices from within any industry

Optimal Member Profile
- Mix of DMs & OEMs representing large and small companies
- Active participation in non-competitive environment with focus on problem-solving

Est: 1/26/2024 – Founded from industry consensus to accelerate addressing CyS risks through collaboration
SMCC Members – 30+ Corporations/Orgs

DMs: 5
OEMs: 14
Solution Providers: 16
Govt & NGOs: 6
Semiconductor Manufacturing Cybersecurity Consortium

SMCC Members – ~50 Corporations/Orgs

As of 1/31/24

<table>
<thead>
<tr>
<th>DMs</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intel</td>
<td>TSMC</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OEMs</th>
<th>16</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applied Materials</td>
<td>ASML</td>
</tr>
<tr>
<td>Oxford Instruments</td>
<td>SCREEN</td>
</tr>
<tr>
<td>Besi</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Solution Providers</th>
<th>19</th>
</tr>
</thead>
<tbody>
<tr>
<td>PeerGroup</td>
<td>IBM</td>
</tr>
<tr>
<td>netthunder</td>
<td>SAFE TECHNO LIMITED</td>
</tr>
<tr>
<td>Rockwell Automation</td>
<td>eInnoSys</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Govt &amp; NGOs</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEMI</td>
<td>imec</td>
</tr>
<tr>
<td>Prifysgol Abertawe Swansea University</td>
<td>NYCU</td>
</tr>
</tbody>
</table>
SMCC Members – ~50 Corporations/Orgs

DMs
7

OEMs
16

Solution Providers
19

Govt & NGOs
9

As of 2/20/24
2024 SMCC PROGRAM CALENDAR

**Communications & Events Major Deliverables**

(Q1) @ Intel Chandler, AZ - 3/6-7
Topics: Operationalize E187 & 3rd party vs self-certification
Sponsors: WG 1 & 2

(Q2) @ NIST HQ? – Mid-Apr
Topics: NIST industry profile & global legislation
Sponsors: WG 4 & 6

(Q2) @ SEMI HQ? – Mid-Apr
Topics: Self assessment questionnaire & TBD
Sponsors: WG 3

(Q3) @ SEMICON West
Topics: SMCC planning, roadblock elimination & 3rd party certification
Sponsors: All WGs

(Q4) @ SEMI HQ
Topics: Self assessment questionnaire & Sharing cyberthreat intelligence
Sponsors: WG 3 & 5

(WG6) Publish “Standards vs collateral” guide to WGs

(WG1) E187 implementation checklist & ref architecture

(WG2) Develop validation criteria for each requirement & establish certification scheme

(WG4) Dashboard of Worldwide Legislation

(WG6) New Standards Activity on E187 Revision

SMCC General Member Meeting @ SEMICON WEST

SMCC Program & Technical Session

SMCC Program & Technical Session

SMCC Program & Technical Session

SMCC Program & Technical Session

SMCC Program & General Session

SMCC Program

WG7 Events & Planning

General Member Meetings
### SMCC Working Groups

**Execution Focused**

**WG1: Factory Cybersecurity Implementation**
- Operationalize cybersecurity specs for factory tools & ID roadblocks
- Starting with SEMI E187

**WG2: Compliance Readiness**
- How to ensure tools are compliant with standards including 3rd party and self certification

**WG3: Supply Chain Cybersecurity**
- Establish methods for ecosystem (supply chain) security implementation & management

**WG4: Regulation & Other Specs**
- Develop strategy for pending legislation & global standards
  - ex. NIST CSF, EU Regulations, DFARS, ISA/IEC 62443

**WG5: Threat Sharing**
- Implement methods for cyber threat intelligence sharing

**WG6: CyS Pre-Standards Engineering**
- Architect comprehensive strategy for new & updated SEMI standards

**WG7: Outreach, Comms & Events**
- Execute cybersecurity education and awareness campaign for semiconductor manufacturing & supply chain

**Strategic Focused**

- Joining the SMCC will help us all secure our industry

Core-team members:
- 1 hour weekly or bi-weekly as aligned in WG
SEMI WG4 Ambition to Co-Author NIST CSF Semiconductor Industry Community and Target Profiles

- NIST Cybersecurity Framework
  - Current version Cybersecurity Framework V1.1 (April 2018)
  - Cybersecurity Framework v2.0 (anticipated 1H 2024)
    - Public Draft Released and Comments Period Closed November 2023

- (External) Community Profiles / Target Profiles
  - Manufacturing Profile https://www.nist.gov/cyberframework/examples-framework-profiles
  - No standard template for a profile from NIST – this is a positive
  - Target Profile can address a specific use-case or technology and can be used to address gaps
    - Target Profile could address our legacy systems and provide additional OT guidance

- Consult with NIST CSF Team for final publication online informative repository (OLIR)
Securing the digital threads of the semiconductor industry

Product Manufacturing: Design ➔ End of Life (Semiconductors / Process/ Metrology Tools)
Questions for our Hardware Security Audience Today

• How do you see integrating SEMI and the SMCC integrating into your HW security efforts?

• How can NIST and others outside of semiconductors help support this effort and avoid duplicating the wheel?

• How does EDA fit into this overall initiative?
SMCC Contacts

Have questions?

SEMI Team
• Primary contact via Cybersecurity@semi.org
• Paul Trio Ptrio@semi.org
  • Director, Standards
• Mayura Padmanabhan Mpadmanabhan@semi.org
  • SMCC Project Manager

SMCC Startup Team
• Brian Korn Brian.D.Korn@intel.com
  • Staff Technologist – Manufacturing Equipment Automation and Cybersecurity – Intel
• Doug Suerich Doug.Suerich@peergroup.com
  • Director of Marketing - PEER Group
• Kannan Perumal Kannan_Perumal@amat.com
  • VP & Chief Information Security Officer - Applied Materials

SMCC Governing Council
• Aernout Reijmer Aernout.Reijmer@asml.com
  • Chief Security Officer – ASML
• James Tu 屠震 ZTU@TSMC.COM
  • Head of Corporate Information Security - TSMC
• Kannan Perumal Kannan_Perumal@amat.com
  • VP & Chief Information Security Officer - Applied Materials
• Wes Sparks Thomas.W.Sparks@intel.com
  • Director - Manufacturing Equipment Automation and Cybersecurity - Intel
• Doug Suerich Doug.Suerich@peergroup.com
  • Director of Marketing - PEER Group

Want to shape how we protect our industry? Please email us:
BACK UP SLIDES
SEMI is a catalyst for **connection, collaboration, and innovation**, helping the semiconductor industry to deploy life-changing tech worldwide.

- Company Neutral
- Geolocation Neutral
- 3000 Member Companies and Organizations
- 50+ Years of uniting and advancing the microelectronics industry
- Through its programs, communities, initiatives, products, and advocacy, SEMI informs its members, cultivates industry collaboration, drives action, and synchronizes innovation.
- Passionate volunteers driving the SEMI Manufacturing Cybersecurity Consortium (SMCC)
SEMI Advances a Global Industry

SEMI Vision

Be the preeminent industry association for the ever-expanding global electronics design and manufacturing supply chain, serving as the empowering catalyst for the sustainable growth of SEMI members to enable diverse technology innovations that universally enhance societal and economic benefits.

SEMI Mission

To advance the growth and prosperity of our member companies’ ecosystems by constantly conceptualizing, developing and providing high-value products, services and solutions. SEMI advocates for a free and open global marketplace, leads workforce development efforts, connects members to new business opportunities in high-growth markets, nurtures pre-competitive collaboration, and helps accelerate innovation.
SEMI – A Global Scope for a Global Industry

Delivering a World of New Business Opportunities

<table>
<thead>
<tr>
<th>Regions</th>
<th>Locations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Americas</td>
<td>Milpitas, Washington DC</td>
</tr>
<tr>
<td>China</td>
<td>Shanghai</td>
</tr>
<tr>
<td>Europe</td>
<td>Berlin, Brussels</td>
</tr>
<tr>
<td>Japan</td>
<td>Tokyo</td>
</tr>
<tr>
<td>Korea</td>
<td>Seoul</td>
</tr>
<tr>
<td>India</td>
<td>Bangalore</td>
</tr>
<tr>
<td>Southeast Asia</td>
<td>Singapore</td>
</tr>
<tr>
<td>Taiwan</td>
<td>Hsinchu</td>
</tr>
</tbody>
</table>
Joining the SMCC will help us all secure our industry

Core-team members: 1 hour weekly or bi-weekly as aligned in WG

SMCC Working Groups

**Execution Focused**
- **WG1: Factory Cybersecurity Implementation**
  - Operationalize cybersecurity specs for factory tools & ID roadblocks
  - Starting with SEMI E187
  - Tues @ 4:30pm PST

**Strategic Focused**
- **WG2: Compliance Readiness**
  - How to ensure tools are compliant with standards including 3rd party and self certification
  - Wed @ 4:30pm PST

- **WG3: Supply Chain Cybersecurity**
  - Establish methods for ecosystem (supply chain) security implementation & management
  - Mon @ 3:30pm PST

- **WG4: Regulation & Other Specs**
  - Develop strategy for pending legislation & global standards eg. NIST CSF, EU Regulations, DFARS, ISA/IEC 62443
  - ?? @ 4:30pm PST

- **WG5: Threat Sharing**
  - Implement methods for cyber threat intelligence sharing
  - ?? @ 4:30pm PST

- **WG6: CyS Pre-Standards Engineering**
  - Architect comprehensive strategy for new & updated SEMI standards
  - Mon @ 3:00pm PST

- **WG7: Outreach, Comms & Events**
  - Execute cybersecurity education and awareness campaign for semiconductor manufacturing & supply chain
  - Tues @ 11am PST
Joining the SMCC will help us all secure our industry

**SMCC Working Groups**

**Execution Focused**

**WG1: Cybersecurity Implementation**
Operationalize cybersecurity specs for factory tools & ID roadblocks Starting with SEMI E187

**WG2: Compliance Readiness**
How to ensure tools are compliant with standards including 3rd party and self certification

**WG3: Supply Chain Cybersecurity**
Establish methods for ecosystem (supply chain) security implementation & management

**WG4: Regulation & Other Specs**
Develop strategy for pending legislation & global standards ex. NIST CSF, EU Regulations, DFARS, ISA/IEC 62443

**WG5: Threat Sharing**
Implement methods for cyber threat intelligence sharing

**Strategic Focused**

**WG6: CyS Pre-Standards Engineering**
Architect comprehensive strategy for new & updated SEMI standards

**WG7: Outreach, Comms & Events**
Execute cybersecurity education and awareness campaign for semiconductor manufacturing & supply chain
SMCC Members Companies – 30+ Corporations/Orgs

DMs 5

OEMs 14

Solution Providers 16

Govt & NGO 9

Semiconductor Manufacturing Cybersecurity Consortium

January 2023
SMCC Members Companies – 50 Corporations/Orgs

DMs
7

OEMs
16

Solution Providers
19

Govt & NGOs
9
Semiconductor Manufacturing Cybersecurity Consortium

Objectives
- Establish a broad methodology for cybersecurity for manufacturing that incorporates lessons learned and embraces open collaboration
- Develop and promote a standards-based, semiconductor industry-specific framework to improve cybersecurity and accelerate implementation of actionable solutions for the entire supply chain
- Incorporate best practices from industries such as automotive and medical with the aim to modernize factory security protocols

SMCC Philosophy - Coordinated Global Effort
- Cybersecurity risks are solvable problems
- Time is now to fully protect our industry’s ability to function
- Don’t let “perfect” be the enemy of “good enough”
  - Constraints like efficiencies, cost effectiveness and utilizing the best solution can & will come later
  - Collaborative & creative forums are the fastest method to identify solutions

Approach
- Formation of a SEMI Technology Community to collaborate with our member companies, leveraging expertise and best practices from within any industry

Optimal Member Profile
- Mix of DMs & OEMs representing large and small companies
- Active participation in non-competitive environment with focus on problem-solving

Problem Statement
The incidence of cyber threats is surging at an alarming rate year over year, leading to a continuous escalation of cybersecurity risks and their consequential impacts, all while implementation of solutions lag behind

Founded through industry consensus to urgently address CyS risks through a collaborative methodology
2024 SMCC PROGRAM CALENDAR

JAN  
Q1 @ SEMI HQ  
Topics: E187 Expectations & CyS KPI Measurements  
WG! & 2 Sponsor

FEB  
Q2 @ ASMC Albany  
Topics: WG4 & WG6  

MAR  

APR  

MAY  

JUN  

JUL  

AUG  

SEP  

OCT  

NOV  

DEC  

Cybersecurity No CyS No CyS  
2-day SMCC  
1-day SMCC & TW  

Q3 @ SEMICON West  
Topics: SMCC planning, roadblock elimination & 3rd party certification  

Q4 @ SEMI HQ  
Topics: Self assessment questionnaire & TBD  

SMCC Workshops

TBD

Edcuation & Awareness

Monthly Newsletter & Blog

monthly Newsletter & Blog

SMCC Conferences

Eiji Hagio / TEL / January 24, 2024 / SEMI FOA Meeting

FOA Collaborative Forum  
January 24-25  
Phoenix, AZ

SEMI Conferences  

@FOA  
January 25  
Phoenix, AZ

@SEMICON KOREA  
January 31  
Seoul, Korea

@SEMICON CHINA  
June 7-9  
Shanghai, China

No CyS Request  
@SEMICON  
China  
June 7  
Shanghai, China

No CyS Request  
@SEMICON  
SEA  
May 7  
Penang, Malaysia

2-day SMCC  
July 7  
San Francisco, CA

1-day SMCC & TW  
September 4-6  
Taipei, Taiwan

1-day SMCC  
November 7  
Munich, Germany

1-day SMCC  
December 7  
Tokyo, Japan

SEMICON® KOREA  
January 31  
Seoul, Korea

SEMICON® CHINA  
June 20-22  
Shanghai, China

SEMICON® SOUTHEAST ASIA  
May 28-30  
Penang, Malaysia

SEMICON® WEST  
July 9-11  
San Francisco, CA

SEMICON® TAIWAN  
September 4-6  
Taipei, Taiwan

SEMICON® EUROPA  
November 12-15  
Munich, Germany

SEMICON® JAPAN  
December 11-13  
Tokyo, Japan

SEMICON®® KOREA  
Jan 31- Feb 2  
Seoul, Korea

SEMICON® SOUTHEAST ASIA  
May 28-30  
Penang, Malaysia

30 Q1
30 Q2
30 Q3
30 Q4
Semiconductor Manufacturing Cybersecurity Consortium

SMCC - Governing Council
Councilmembers:
- DMs: Intel (Wes), TSMC (James)
- OEMs: AMAT (Kannan), ASML (Aernout)
- SP: PEER (Doug)
Removes roadblocks & sets priorities
Goals & Ambition Setting

SMCC - Steering Committee
WG Chairs:
- Intel (Brian), TSMC (Leon)
- AMAT (Lori), TEL (Hagio-san)
- IBM (Jennifer), ASML (Bill)
GC Sponsors: PEER (Doug) & AMAT (Kannan)
Validate Direction, Agenda, Objectives, Baselining, Roadmaps & Support of WGs

SMCC – Administration
Outreach, Communications & Events
Staff: Paul & Mayura (SEMI)

1. Cybersecurity Implementation
Scope:
- Operationalize specs
- Identify & eliminate roadblocks
Chair - Intel: Brian K.
Vice-chair - TSMC: Leon
Vice-chair - AMAT: Dave D.
Core team: (DMs)
- SK Hynix: Seung
- TI: Jared
- Intel: Omar
- AMAT: Manas
- LAM: Bharat/Chen/John W.
- TEL: Matsuda-san
- PEER: TBD
- SCREEN: Motoyasu
- TXOne: Dr. Liu

2. Compliance Readiness
Scope:
- Risk & Gap ID
- 3rd party certification
Chair - AMAT: Dave D.
Vice-chair - TSMC: Leon
Vice-chair - Intel: Brian K.
Core team:
- DM – Intel: Berto
- AMAT: Manas
- Teradyne: Dan
- Onto: Tim
- Siemens: Laurent
- TEL: Matsuda-san/Andy
- ITRI: Dr. Zuo

3. Supply Chain Cybersecurity
Scope:
- Ecosystem security implementation & measures
Chair - TEL: Hagio-san
Vice-Chair - AMAT: Lori
Vice-Chair - ASML: Bill
Core team:
- Skyworks: Madan
- Intel: Tiffany & Brian K.
- TEL: Kohriyama-san/Andy
- AMAT: Sanjay, Ramu & Anusha
- Onto: Tim
- SCREEN: Motoyasu
- CISCO: Steven
- LAM: Pradeep

4. Regulation & Other Specs
Scope:
- Education & awareness
- Pending legislation
- Non-SEMI standards
Chair - IBM: Jennifer
Vice-Chair – AMAT: Raj
Vice-Chair - ASML: Wilco
Core team:
- TI: Jared
- AMAT: Raj P.
- LAM: Chen/John W
- Siemens: TBD
- PEER: Albert
- Deloitte: Hideyuki
- TEL: Katsuki-san

5. Threat Sharing
Scope:
- Cyber threat intelligence
- Incident response
Chair - ASML: Bill
Vice-Chair - IBM: Jennifer
Vice-Chair – Polaris: Chet
Core team:
- DM – Intel: Mike T & William Long
- AMAT: Raj P.
- LAM: Chen/John W
- Oxford: Rhys
- Agileo: Fahad
- TEL: Fujikawa-san & Mochizuki-san

6. CyS Pre-Standards Engineering
Scope:
- SEMI branded spec
- Comprehensive global standards strategy
Chair - TSMC: Leon
Vice-Chair - Intel: Ryan
Vice-Chair - PEER: Albert
Core team:
- DM – Intel: Mike T &
- LAM: Chen/John W
- Oxford: Rhys
- Agileo: Fahad
- TEL: Fujikawa-san & Mochizuki-san