txOne networks *The Leader of OT Zero Trust*

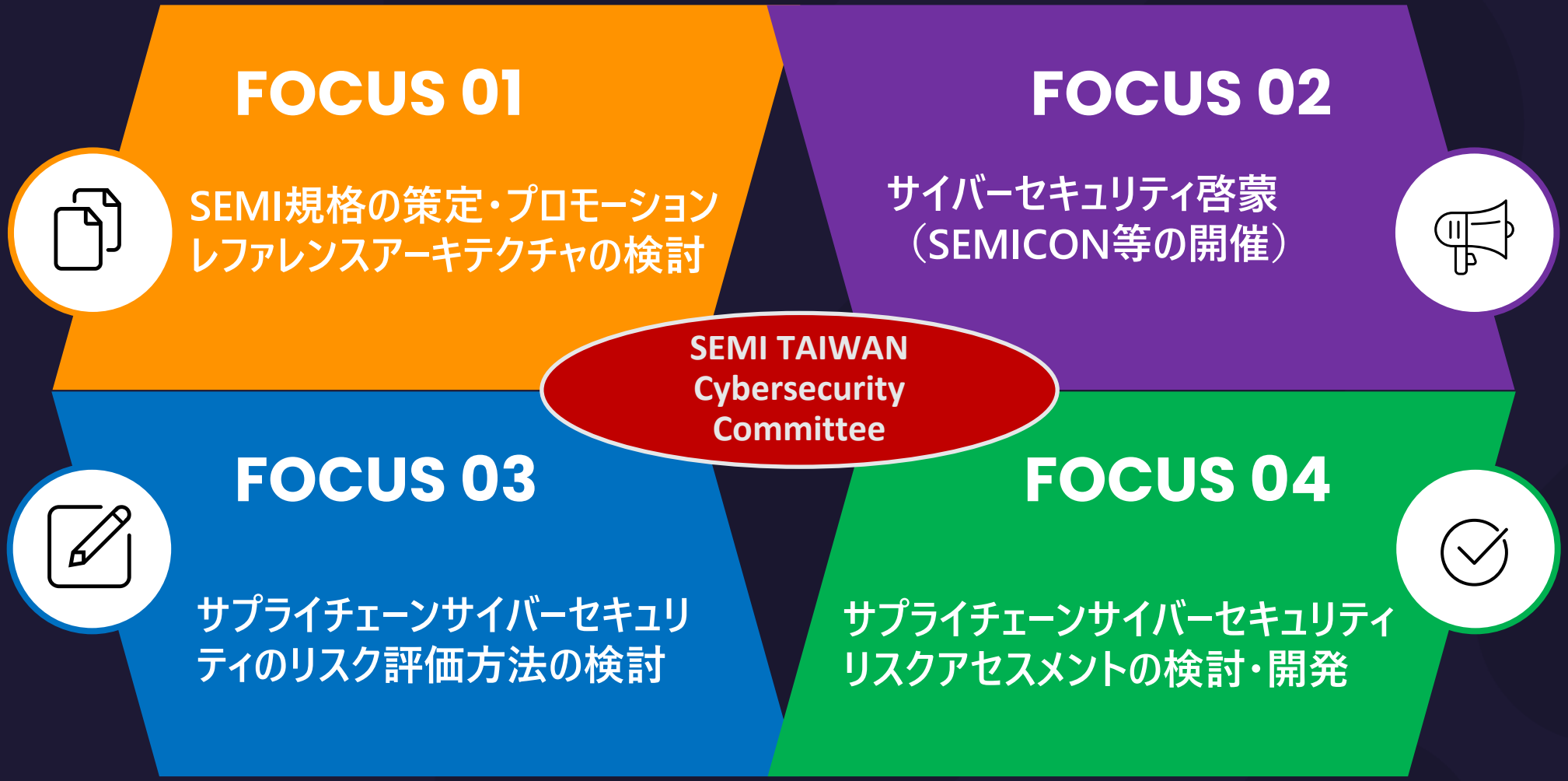
第6回 産業サイバーセキュリティ研究会 ワーキンググループ1 工場SWG

半導体セキュリティ規格 SEMI E187の動向

2023年10月6日

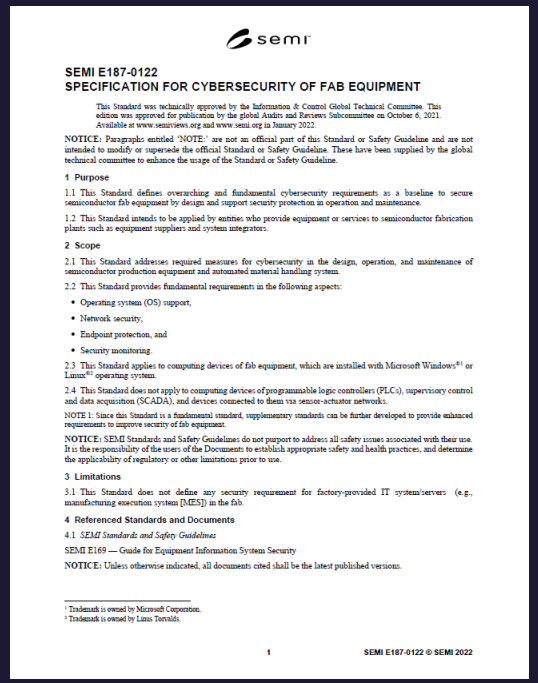
TXOne Networks Japan合同会社
業務執行役員　今野 尊之
takayuki_imano@txone.com

SEMI台湾 Cybersecurity Committee



SEMI台湾 Cybersecurity Committee

ファブ装置のセキュリティ規格
SEMI E-187発行



SEMI E187-0122
SPECIFICATION FOR CYBERSECURITY OF FAB EQUIPMENT

This Standard was technically approved by the Information & Control Global Technical Committee. This edition was approved for publication by the global Audits and Reviews Subcommittee on October 6, 2021. Available at www.semiviews.org and www.semi.org in January 2022.

NOTICE: Paragraphs entitled 'NOTE:' are not an official part of this Standard or Safety Guideline and are not intended to modify or supersede the official Standard or Safety Guideline. These have been supplied by the global technical committee to enhance the usage of the Standard or Safety Guideline.

1 Purpose

1.1 This Standard defines overarching and fundamental cybersecurity requirements as a baseline to secure semiconductor fab equipment by design and support security protection in operation and maintenance.

1.2 This Standard intends to be applied by entities who provide equipment or services to semiconductor fabrication plants such as equipment suppliers and system integrators.

2 Scope

2.1 This Standard addresses required measures for cybersecurity in the design, operation, and maintenance of semiconductor production equipment and automated material handling system.

2.2 This Standard provides fundamental requirements in the following aspects:

- Operating system (OS) support,
- Network security,
- Endpoint protection, and
- Security monitoring.

2.3 This Standard applies to computing devices of fab equipment, which are installed with Microsoft Windows®[1] or Linux®[2] operating system.

2.4 This Standard does not apply to computing devices of programmable logic controllers (PLCs), supervisory control and data acquisition (SCADA), and devices connected to them via sensor-actuator networks.

NOTE 1: Since this Standard is a fundamental standard, supplementary standards can be further developed to provide enhanced requirements to improve security of fab equipment.

NOTICE: SEMI Standards and Safety Guidelines do not purport to address all safety issues associated with their use. It is the responsibility of the users of the Documents to establish appropriate safety and health practices, and determine the applicability of regulatory or other limitations prior to use.

3 Limitations

3.1 This Standard does not define any security requirement for factory-provided IT system/servers (e.g., manufacturing execution system [MES]) in the fab.

4 Referenced Standards and Documents

4.1 *SEMI Standards and Safety Guidelines*

SEMI E169 — Guide for Equipment Information System Security

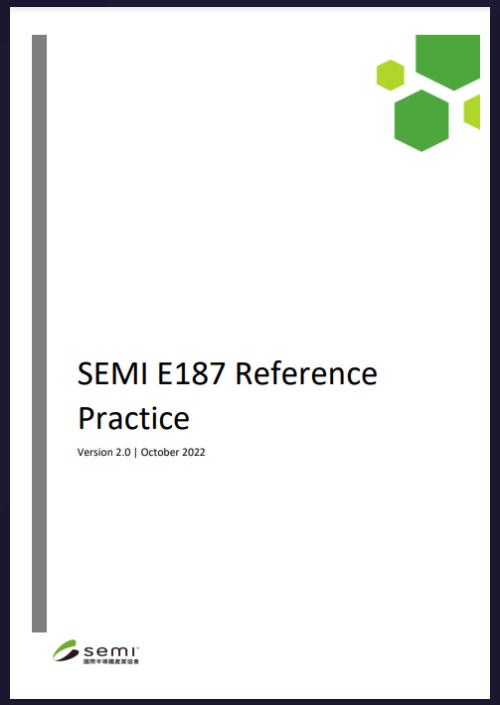
NOTICE: Unless otherwise indicated, all documents cited shall be the latest published versions.

[1] Trademark is owned by Microsoft Corporation.
[2] Trademark is owned by Linus Torvalds.

1 SEMI E187-0122 © SEMI 2022

2022年1月

SEMI E-187
Reference Practice発行

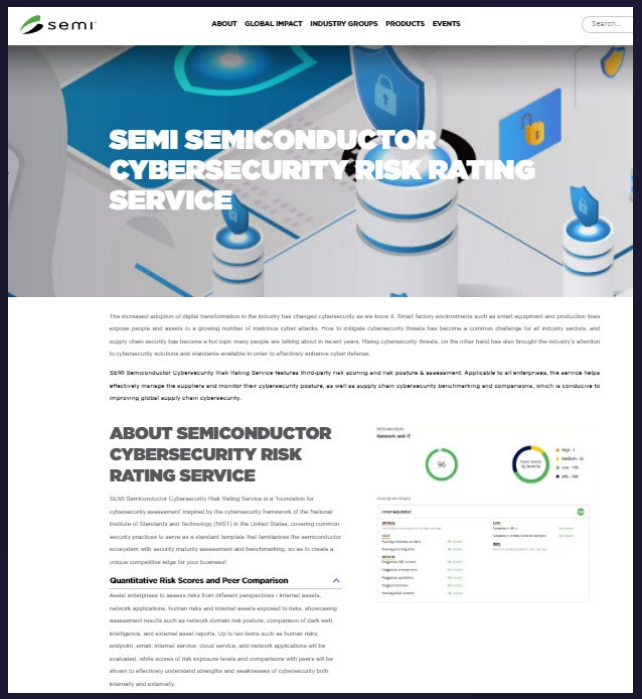


SEMI E187 Reference Practice

Version 2.0 | October 2022

2022年10月

SEMI Semiconductor
Cybersecurity Risk Rating Service



SEMI SEMICONDUCTOR CYBERSECURITY RISK RATING SERVICE

ABOUT SEMICONDUCTOR CYBERSECURITY RISK RATING SERVICE

Quantitative Risk Scores and Peer Comparison

2023年1月

TSMC Webサイトのアナウンスメント（2023年9月14日）

Dr. James Tu (fourth from the left), Head of Corporate Information Security, shares cybersecurity challenges and solutions at the 2023 SEMICON Taiwan Semiconductor Cybersecurity Global Summit. (Photo source: SEMI)

TSMC Strengthens "Specification for Cybersecurity of Semiconductor Equipment", Realizing Mutual Industry Benefits

TSMC has Upgraded the Security of its Factories by Requiring New Equipment to Comply with the Standards through Procurement Contracts, Strengthening the Cybersecurity Defense of its Supply Chain

2023/09/14

Leon Chang Jill Wang

TSMC is dedicated to fulfilling the commitments of its "Information Security Declaration". In response to the Company's development toward smart manufacturing, TSMC has initiated and promoted the global security standard "Specification for Cybersecurity of Fab Equipment" (SEMI E187) to enhance the cybersecurity of the semiconductor supply chain. In 2023, it was included as a tool procurement specification and verification mechanism, and established to ensure that suppliers comply with the standard before the introduction of any new equipment. Additionally, to accelerate the integration and networking efficiency of the entire factory system, TSMC has collaborated with the Semiconductor Equipment and Materials International Organization (SEMI) to define the "Cybersecurity Reference Architecture for Semiconductor Manufacturing Environment". This was first released at the SEMICON Taiwan international semiconductor exhibition in September and will be launched online in October. The architecture optimizes the cybersecurity management of semiconductor fabs and ensures production quality.

> In the face of global challenges to information security in the semiconductor industry, TSMC continues to collaborate with supply chain partners to strengthen defense and resilience, safeguarding the overall security of the industry chain.
>
> - Dr. James Tu, *Head of Corporate Information Security at TSMC and the Inaugural Chairman of SEMI Cybersecurity Committee*

TSMC Strengthens "Specification for Cybersecurity of Semiconductor Equipment", Realizing Mutual Industry Benefits

TSMCは「半導体装置のサイバーセキュリティ規格」を強化し、業界相互の産業利益を追求する。

URL: TSMC Strengthens "Specification for Cybersecurity of Semiconductor Equipment", Realizing Mutual Industry Benefits

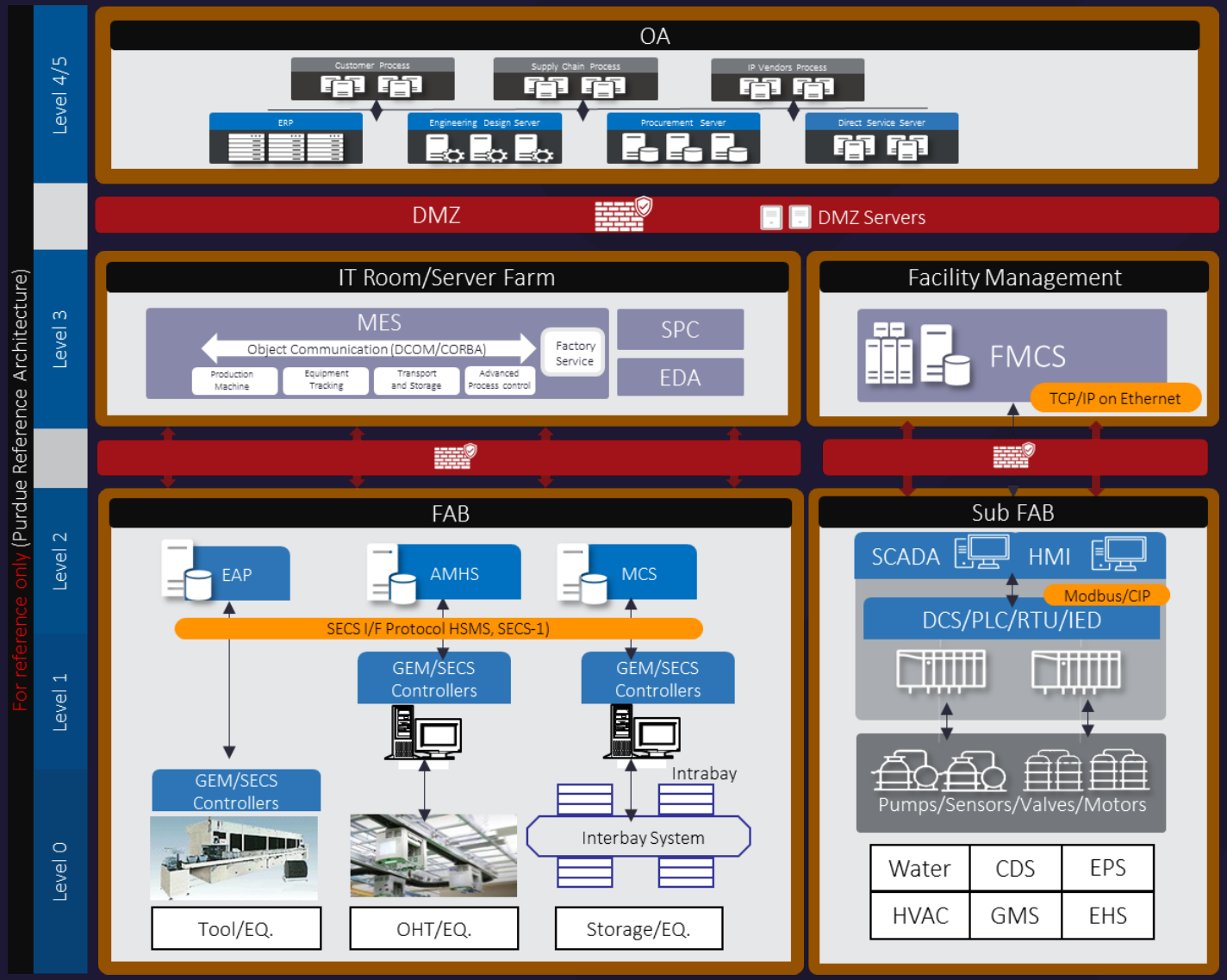
TSMCのアナウンスメント要約

1. 半導体工場のセキュリティをさらに強化するために、2023年より、半導体装置のセキュリティ規格（SEMI E-187）が、TSMCの**調達契約要件**のひとつとして、正式に盛り込まれた。
2. サプライヤーが新しい装置をTSMCに導入する際に、SEMI E187の準拠を検証する仕組みが確立された。
3. 2023年、SEMI台湾は台湾デジタル産業局(MODA)と協力し、半導体装置メーカーに対して、セキュリティ・チェックリストの適用を支援。その中で、**Gallant Precision Machining**（台湾）と**Contrel Technology**（台湾）は、SEMI E-187の要件を満たしていることを、認証機関によって証明された世界初のサプライヤーとなった。

TSMCのアナウンスメント要約

4. TSMCとSEMI台湾が協力し、**「半導体工場サイバーセキュリティ・リファレンス・アーキテクチャー」**を作成。**2023年10月**にSEMI台湾より、公開予定。
5. 2023年に**「SEMI半導体サイバーセキュリティ・リスク評価サービス」**をリリースし、企業がサイバーセキュリティの脆弱性を迅速に特定し、保護対策の有効性を監視できるよう支援する。年内に**1,000社以上**がこのサービスを採用する見込み。

Fabサイバーセキュリティ・リファレンス・アーキテクチャー



- 生産効率とサイバーセキュリティ防御を兼ね備えた、ハイテク工場を構築し、業界の競争優位性を維持するために、Fabのセキュリティ・リファレンス・アーキテクチャを作成
- 各設備やシステム毎に参照すべきセキュリティ標準やセキュリティ規格を整理

Keep the Operation Running