資料４

txOne networks *The Leader of OT Zero Trust*

半導体セキュリティ規格「SEMI E187」について

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

SEMI E187とは？

- Specification for Cybersecurity of Fab Equipment（ファブ装置のサイバーセキュリティ仕様）

- ファブ装置へのサイバー攻撃の急増を受け、SEMI台湾地区 Information & Control 技術委員会、Fab & Equipment Information Securityタスクフォースにおいて、3年にわたり開発され、3回の電子投票を経て2022年1月に出版。

- 装置のサプライチェーン全体におけるグローバルなサイバーセキュリティ・コンプライアンスの確立を目指す。

txOne networks

SEMI E187の目的と対象

- 半導体製造装置を設計上安全にし，運用・保守上のセキュリティ保護を支援するための基本的なサイバーセキュリティの要件を包括的に定義。

- 半導体製造工場に装置やサービスを提供する装置サプライヤー、システムインテグレータ等を対象として想定。

- 装置の設計段階で本規格の要求事項を考慮(Security by Design)すると同時に、設備所有者が装置のライフサイクルにおけるセキュリティポリシーや管理項目を設計する際のセキュリティベースラインとして活用することも期待。

txOne networks

SEMI E187の主要分野

①オペレーティングシステム

②ネットワークセキュリティ

③エンドポイント保護

④セキュリティモニタリング

txOne networks

SEMI E187の各要求事項

①オペレーティングシステム

1. 装置搭載OSに関する要求
2. パッチ適用手順の技術文書作成

②ネットワークセキュリティ

3. 安全な通信転送プロトコルのサポート
4. ネットワーク構成の技術文書作成

③エンドポイント保護

5. 脆弱性の軽減
6. マルウェアスキャン実行
7. アンチマルウェア対策
8. システムハードニング
9. 認証機構の適用
10. アクセス権の設定

④セキュリティモニタリング

11. セキュリティイベントログ
12. ログタイプ

txOne networks

SEMI TAIWAN Cybersecurity Committee

リファレンスアーキテクチャ
WGリーダー
Dr. Terence Liu
CEO, TXOne Networks

SEMI TAIWAN Cybersecurity Committee

FOCUS 01

SEMI規格のプロモーション
レファレンスアーキテクチャの検討

FOCUS 02

サイバーセキュリティ啓蒙
（四半期毎、随時開催のイベント開催）

FOCUS 03

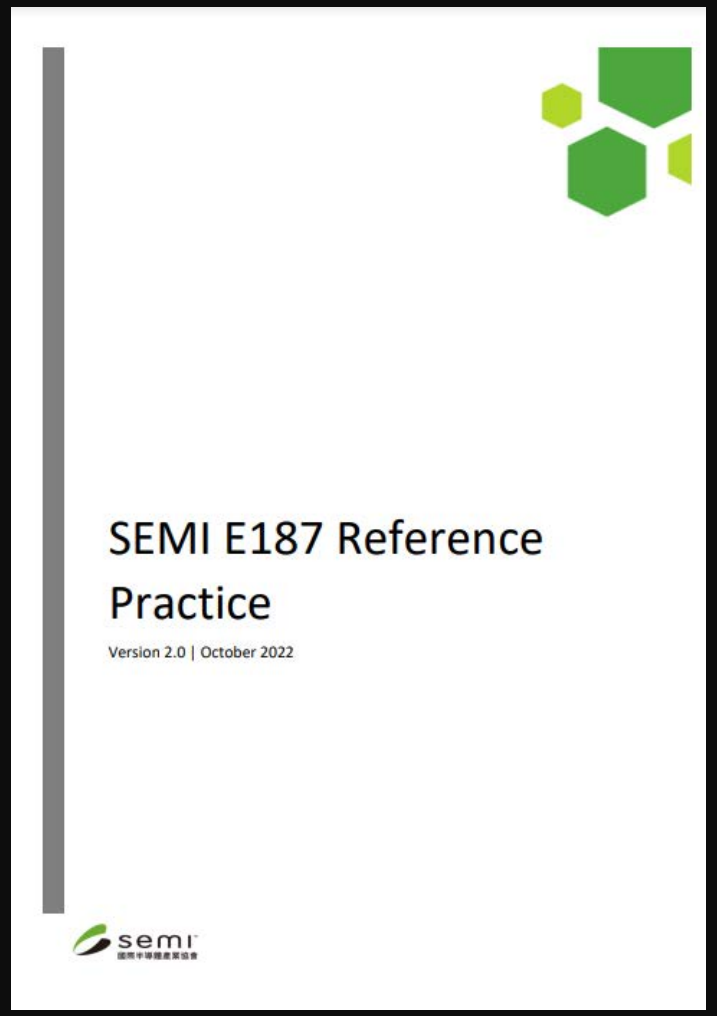
サプライチェーンサイバーセキュリティ
の評価方法の検討

FOCUS 04

NIST CSFをベースとしたサプライチェーン
サイバーセキュリティリスクアセスメントの検討

txOne networks

SEMI E187 Reference Practice (2022年10月発行)



- Taiwan Semiconductor Cybersecurity Committeeのリファレンス・アーキテクチャ・ワーキンググループがSEMI E187の実際の展開を支援するために作成。
- E187の各要求事項の解説とセキュリティ対策実装に関するQ＆Aおよび実践例を紹介

3.1.1 FAQ:

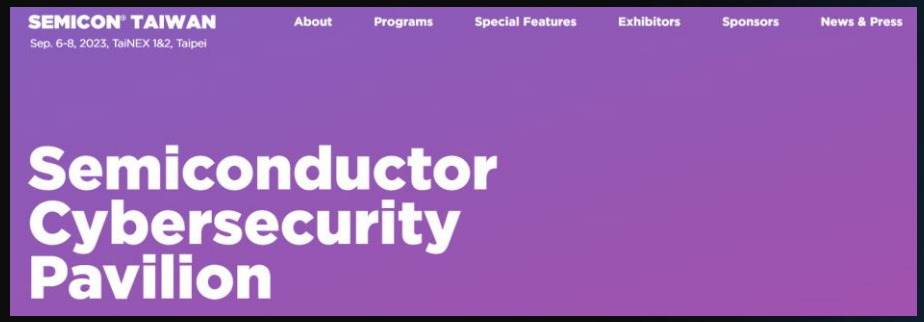
- ***Which operating systems are applicable in the scope of this standard?***
  This Standard applies to computing devices of fab equipment, which are installed with Microsoft Windows® or Linux® operating system.
- ***How does the equipment supplier know if the operating system is end of life?***
  It is recommended that the equipment provider periodically tracks the product roadmap information of the operating system vendors such as Microsoft ®, Red Hat ®, Ubuntu ®.

3.1.2 Practice and Example

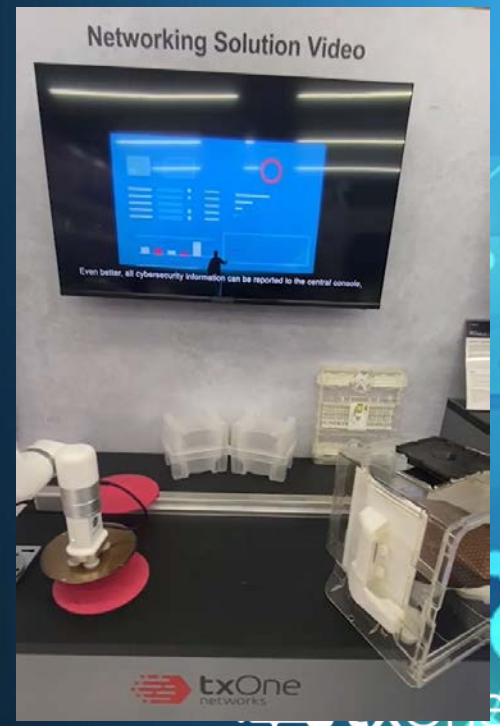
- Windows XP, Windows Vista and Windows 7 indicated in Table 1 are examples of end-of-support operating systems. When Microsoft stopped issuing updates and patches, these operating systems rapidly became orders of magnitude more vulnerable to security threats. Equipment vendors should not ship equipment with end-of-support operating systems. If an EOL operating system is needed to use on the fab equipment, both the user and supplier may agree on alternative methods to identify and fix vulnerabilities. However, negotiating such an agreement is out of the scope of SEMI E187.

txOne networks

TXOne Networksの普及啓蒙活動 ①



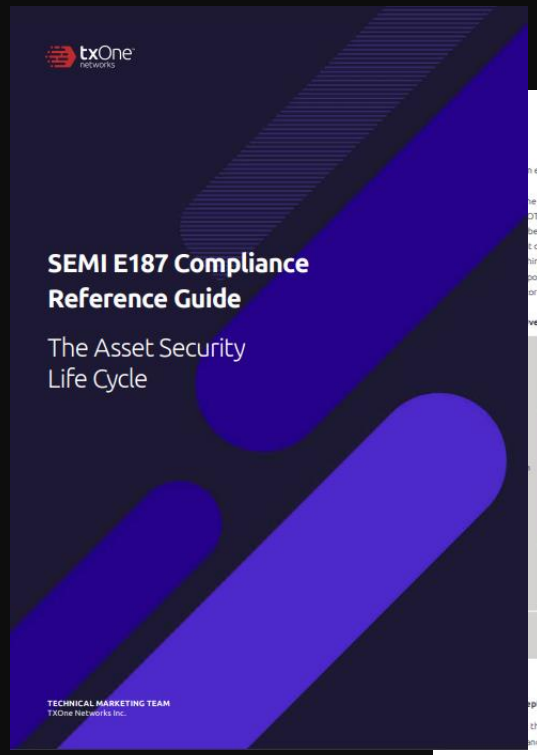
Wafer Handling System Demo

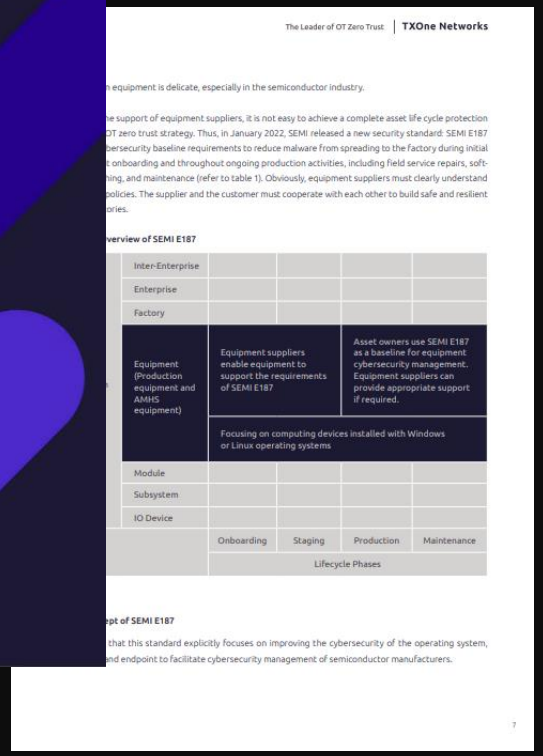


OHT（Overhead Hoist Transport) Demo

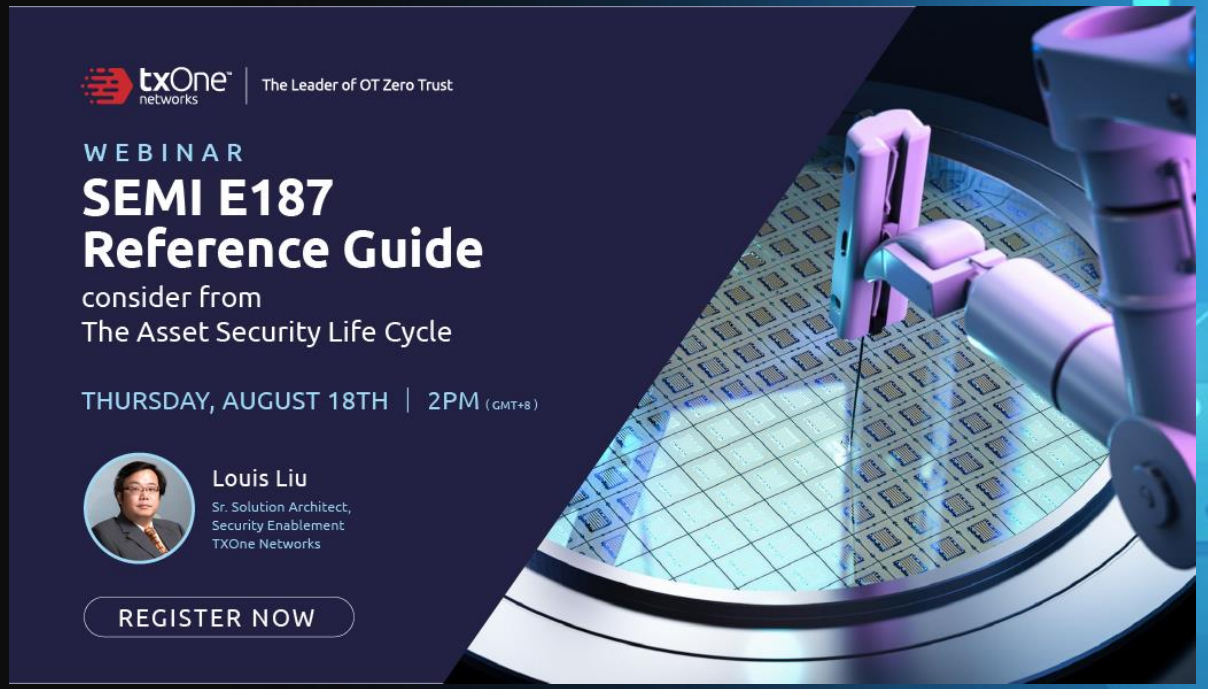
TXOne Networksの普及啓蒙活動 ②

SEMI E187 レファレンスガイド発行（2022/7/20）





SEMI E187 レファレンスガイド・ウェビナー開催



https://www.txone.com/case-studies/reference-guide-semi-e187-compliance-the-asset-security-life-cycle/

まとめ

- SEMI E187は「ファブ装置のサイバーセキュリティ仕様」として、4つの主要分野（オペレーティングシステム、ネットワークセキュリティ、エンドポイント保護、セキュリティモニタリング）の基本的なセキュリティ要件を定義

- SEMI E187は、半導体装置メーカーが自社の情報を保護する上で有効なだけでなく、サプライチェーン全体が協力して、業界全体として情報セキュリティの強化を図ることを目指す。

- リファレンス・プラクティスの開発を通じた、規格の普及啓蒙活動の他、セキュリティ評価手法、サプライチェーン全体の情報セキュリティ評価の長期計画や認証・認定制度の確立などが計画されている。

txOne networks

Keep the Operation Running