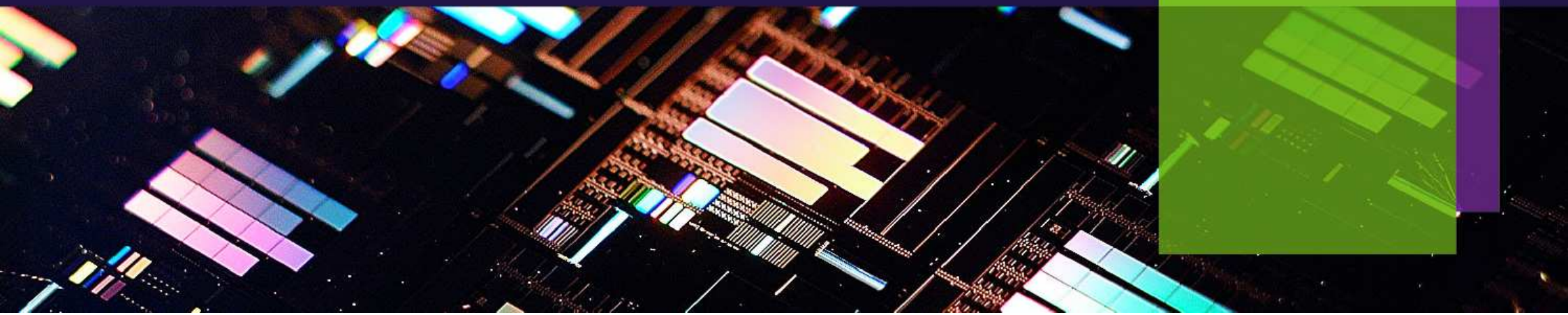
TOKYO ELECTRON

機能安全を実現する安全制御システムにおける セキュリティについての標準化の動き

平成29年10月18日　　日機連講演会

真白　すぴか
東京エレクトロン(株）システム開発センター



Disclaimer

- The views expressed are purely those of the writer, and may not, in any circumstances, be regarded as stating an official position of Tokyo Electron LTD, any group in the IEC, or The Japan Machinery Federation.

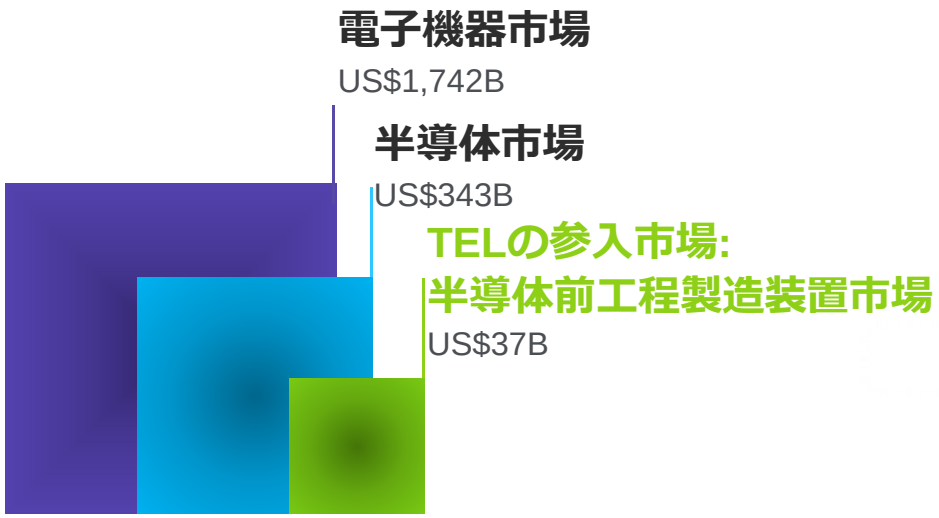
アウトライン

1. はじめに：会社紹介＆自己紹介
2. IEC63074開発の背景と動機
3. IEC63074CDの概要
4. IEC63074の課題
   - ISO12100との関係
   - TC65担当Security規格との関係
5. 開発のタイムライン
6. まとめ

アウトライン

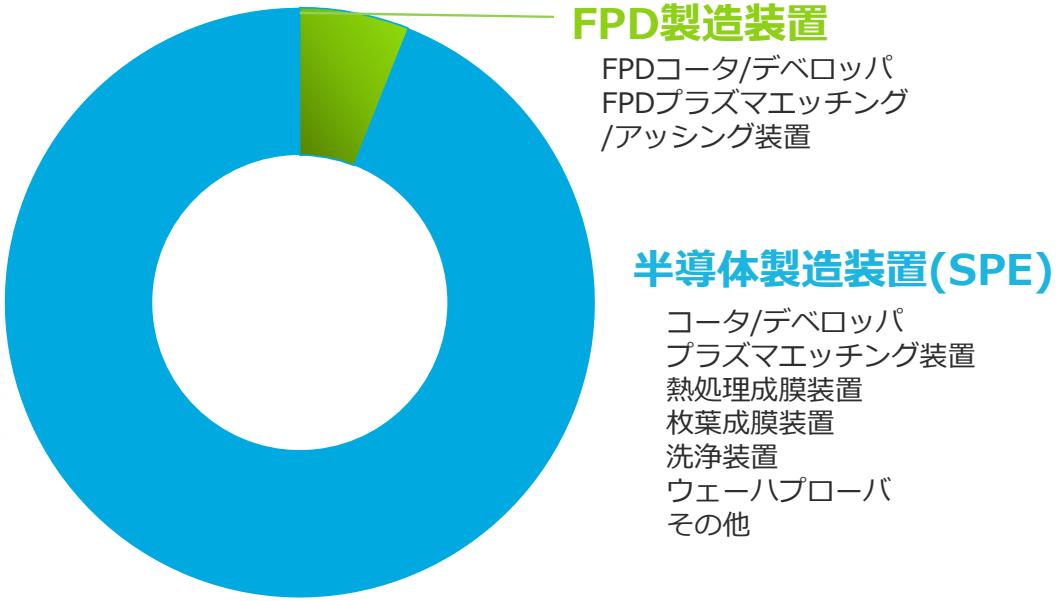
1. はじめに：会社紹介＆自己紹介
2. IEC63074開発の背景と動機
3. IEC63074CDの概要
4. IEC63074の課題
   - ISO12100との関係
   - TC65担当Security規格との関係
5. 開発のタイムライン
6. まとめ

東京エレクトロン（株）のご紹介



CY2016市場規模

出所：Gartner, “Forecast: Semiconductor Wafer Fab Manufacturing Equipment, Worldwide, 1Q17 Update” 13 April 2017
図はガートナーリサーチに基づき、東京エレクトロンが作成。

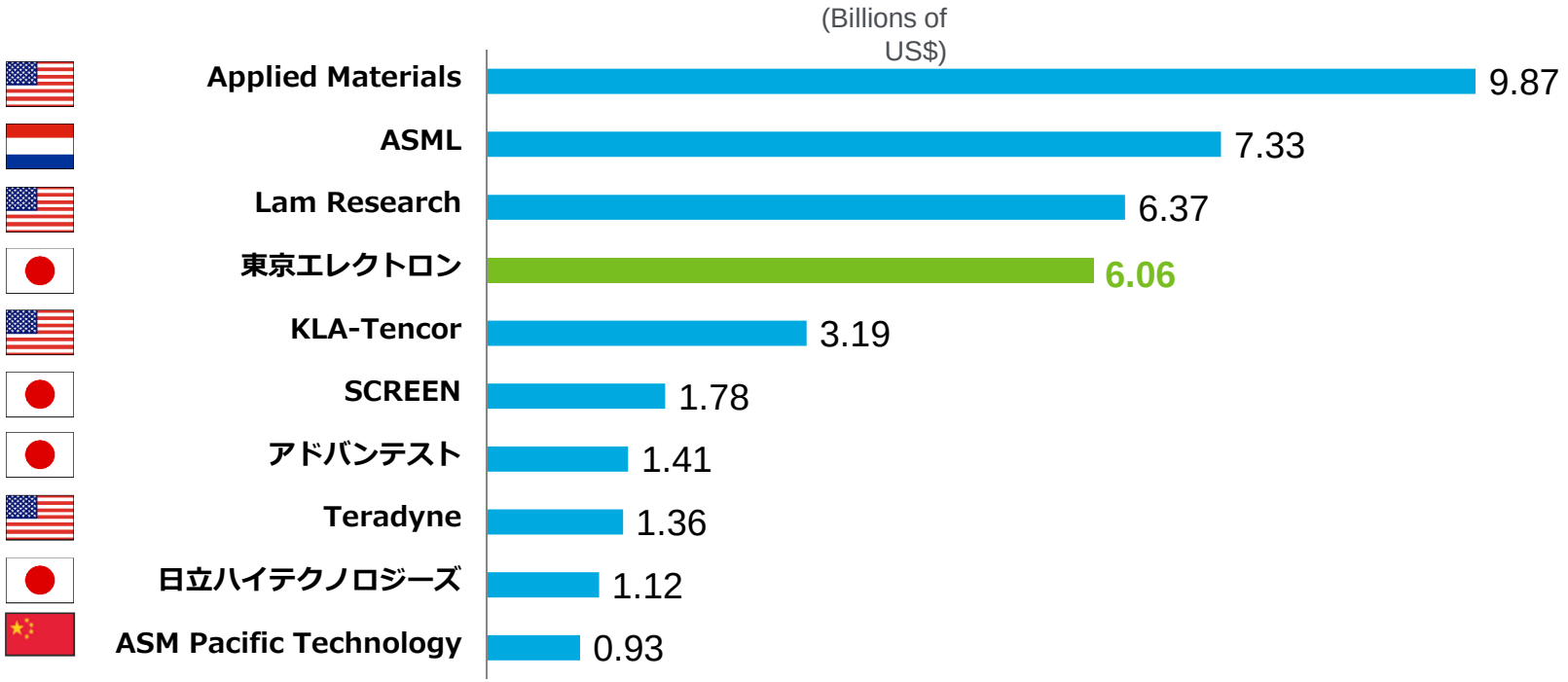


事業分野別　売上高構成比

2017年3月期連結売上高: 7,997億円

東京エレクトロン（株）のご紹介

CY2016 売上ランキング



出所：The Chip Insider Equipment & Emerging Markets (VLSI Research, May 2017)
為替レート： CY2015: 1US$=¥121.00 CY2016: 1US$=¥108.80

弊社製品における安全関連制御コンポーネントの使用

Coater/Developer
(aka. Clean Track)

コータ／デベロッパは、半導体製造プロセスのうち、フォトリソグラフィープロセスにおいて、フォトレジスト（感光剤）の塗布と現像を行う装置です。

- コータ／デベロッパでウェーハ上にフォトレジストを塗布した後、ウェーハは露光装置に送られ、微細回路パターンが転写されます。
- 次に、コータ／デベロッパに戻り、薬液により現像されます。
- これにより、光の当たった部分のフォトレジストは溶けて流れ、ウェーハ上に転写した回路パターンが凹凸に描かれます。
- このフォトリソグラフィープロセスは様々な工程ごとに繰り返し行われ、複雑な集積回路が作られます。

➔ 危険化学物質（毒性・可燃性）、加熱機構、高圧流体、可動部等多様な危険源と複雑な制御機構を持ちます。

➔ 様々な安全関連制御コンポーネントの使用が増加しています

Thermal
Treatment/Deposition

熱処理成膜装置は熱を利用してLPCVD（減圧・化学的気相成長）および酸化工程など、半導体製造プロセスにおいて、主にトランジスタ周辺の薄膜を形成するために用いられます。

- 減圧した処理室内でウェーハを高温に加熱し、プロセスガスを処理室に導入してウェーハ表面上で熱分解／反応させることにより所望の性質の薄膜を形成します。
- トランジスタ周辺の薄膜は特に不純物の混入を嫌うため処理室のウェーハやプロセスガスが接触する高純度の石英などで作られています。

➔ 特に可燃性･毒性が高いシラン、ホスフィンなどのガスの供給系、高温（数百～千℃）加熱機構、可動部等多様な危険源と複雑な制御機構を持ちます。

➔ とくに危険なガス供給系や排気ガス処理系を中心に安全関連制御コンポーネントの使用が増加しています

自己紹介：IEC63074にかかわるようになるまで

- 真空機器･真空応用成膜／加工処理装置メーカーのプロセスエンジニア出身
- 半導体製造用のプラズマエッチング装置、高密度プラズマCVD（化学気相成膜）装置、熱分解成膜装置等のプロセス･製品開発に携わるうちにシラン・ジシランなどの安全取り扱いガイド（Safety Guideline)の開発でSEMI Standardの世界にデビュー
- 一方、製品技術として、半導体製造工場と装置とのハード／情報系（制御・データ）両面のインテグレーション（Factory Integration)仕様作成を経験
- IEC60204シリーズに半導体製造装置に特化したパート(Part33)を作成した（TC44/WG11)際にTC44の活動に初めて参加、その後IEC60204-1MT、TC44/SC129B JWGでは機械メーカーの立場で国際エキスパートとして活動（この間に東京エレクトロンに転職し、装置のFactory Integration仕様に関係する内外スタンダード活動に従事）
- 最近汎用IT機器やOSの使用が半導体製造工場や装置で増加したこともあって、製造装置の保守のための外部システムやデバイスとの接続部の脆弱性、アンチウィルスソフトによる装置制御系への悪影響等のセキュリティリスク懸念が増してきていた。このタイミングで「セキュリティとセーフティ」のテーマをTC44で取り上げる動きが出てきたのを見て日本の参画を国内委員会に提議。WG15(Security)設立当初から国際エキスパートとして参加中。

アウトライン

1. はじめに：会社紹介＆自己紹介
2. IEC63074開発の背景と動機
3. IEC63074CDの概要
4. IEC63074の課題
   - ISO12100との関係
   - TC65担当Security規格との関係
5. 開発のタイムライン
6. まとめ

IEC63074開発の背景

- いわゆるConnected Fab, Smart Manufacturing/Industrie 4.0　などの動きでMachine（機械）のデータ･制御系の外部インターフェースが増えていく傾向でセキュリティリスクは増加傾向
- Control SystemのSecurity標準化に関するTC65の動き
  - TC65のWG10で策定が進められているIEC62443シリーズを汎用Control System以外に広く適用できるという考えの元、IEC62443に対する認証を推進しているグループがある。
  - IEC61508とのアナロジーでSectorスタンダードに対するCertification スキームとしてIEC62443を何にでも（機械も）使えるようにできるという立場
    - コンポーネントレベルのセキュリティに関してはCertificationも含めてIEC62443が妥当
  - IEC62443-3-2のDCではSecurity Riskのランキングが提案されているが客観的・定量的に評価できないものをあたかもできるように扱っている。
- ISO/TC199でもISO12100にしたがってリスクアセスメントをする際にセキュリティ（問題）が及ぼす影響の考慮に関して何らかのガイドが必要という認識

IEC63074開発の動機

- 機械のSafety Related Control Systems（SRCS)のSecurityは機械のSRCSの動作への影響（Safety Consequence)に配慮する必要があり、TC44が主体となってISを作るべきで、制御系を扱うTC65の担当ではない（というTC44側の思い）。
- 機械のSecurity確保は基本的にはUserの問題。ただし、Machine Builder/IntegratorがSecurityに関連する機械のVulnerability（Security攻撃の入り口になりうるI/Fやデバイスなど）とSafety Consequenceに関する情報を提供する必要はある。
- Security上のThreatに対する対策がSafety Related Control Systemの動作に悪影響を及ぼすことが無いようにすると言う観点も「機械の安全」すなわちTC44観点で必要
- IoT, Industrie4.0/ Smart Manufacturing等、機械をCPS（Cyber Physical Systems）に組み入れていく動きが活発化しているので早く手を打つ必要あり

アウトライン

1. はじめに：会社紹介＆自己紹介
2. IEC63074開発の背景と動機
3. IEC63074CDの概要
4. IEC63074の課題
   - ISO12100との関係
   - TC65担当Security規格との関係
5. 開発のタイムライン
6. まとめ

IEC63074CDの概要(0/8)

- FOREWORD
- INTRODUCTION
- 1 Scope
- 2 Normative references
- 3 Terms and definitions
- 4 Safety and security overview
- 5 Security requirements related to functional safety
- 6 Verification of security measures
- 7 Documentation to be provided to the user of machine

- Annex A (informative) Basic information related to threats and threat modelling approach
- Annex B (informative) Security risk assessment
- Annex C (informative) Example of information flow between device supplier, manufacturer of machine (integrator) and end user of machine
- Annex D (informative) Example of machinery applications

IEC63074CDの概要(1/8)

- SCOPE
  - 以下のようなSecurityの側面についての要求事項
    - Threats とVulnerability が機械のSafety-Related Control System (SCS)に影響することにより機械の機能安全に影響を与えるような場合
    - SafetyとSecurityの関係、とくに
      - SCSのVulnerabilityに乗じてSecurity Threatsが攻撃に成功した場合のSCSの安全機能や可用性への影響
      - 典型的なユースケースに対応したThreatのモデル

➔SCOPE記述ではTarget Audienceが機械メーカーであることが読み取れないため、FOREWORDで記述

IEC63074CDの概要(2/8)

- 4　　Safety and security overview
- 4.1一般事項
  - SafetyとSecurityの関係
    - 機械は適切なSafety Measureを有する
    - 個々のSafety Measureに対し許されていないような操作･乱用を防ぐためのSecurity Measureを持つことが可能
    - Security MeasureはSafety Measureの性能を低下させない適切なものにするべきである
- 4.2/4.3　Safety/Securityの目標
  - 機械の安全の見地でのSecurityの目標はSCSの機械の安全な運転を担保する能力を（Security Threatsから）守ること
  - 関係するシステム・サブシステムのSecurity ThreatsやVulnerabilityの情報の特定と文書化をしなくてはならない
- 4.4　Security Measureを決定するためのワークフロー
  - SCSのVulnerabilityアセスメント結果によりSecurity アセスメントおよびSecurity要求定義（Security Measures定義）を行う

IEC63074CDの概要(3/8)

- 5　機能安全に関わるSecurity 要求
- 5.1　Security リスクアセスメント
  - SCSに関係するSecurity リスクアセスメントは機械の使用環境における全体的Security リスクアセスメントの一部（機械ユーザーにより行われる）
  - Vulnerabilityアセスメント：SCSの意図される使用条件におけるVulnerabilityの特定と安全への潜在影響の評価
  - Vulnerabilityアセスメントは機械の使用環境におけるSCSのSecurity リスクアセスメントにINPUTされるものである。
  - 機械メーカーは（SCSに対する）Threatsを仮定しその仮定に基づいたSecurity Measuresを実装できるかもしれない→確認が必要
  - （SCS)のリスクアセスメントのその他の側面の例
    - 特定されたThreatsとそのSource
    - 追加Measureの必要性
    - Threatsを低減･除去するための手段もしくはその参考になる情報

IEC63074CDの概要(4/8)

- 5.2　Security リスクレスポンス
  - とりうるリスクレスポンスには
    - Risk Mitigation
      - 設計によりリスクをなくす（さける）
      - Securityリスクを限定的にする　等
      - Riskの移動・共有
    - 許容可能なリスクは受け入れる。
  - 機械の安全の分野におけるSecurity Risk Mitigationの戦略はSecurity Risk Assessmentの結果によって設定しなければならない。
  - とくにSCSのVulnerabilityは最終的なSecurity Risk Mitigationの戦略設定のINPUTとなる。

IEC63074CDの概要(5/8)

- 5.3　Security 要求仕様
  - SCSのVulnerabilityに基づいてSecurity 要求仕様を作成しなければならない。これには最低限以下に関する情報を含むこと：
    - 安全機能を果たしているSCS
    - SCSに影響するVulnerabilityと、該当する場合は仮定したThreats
    - 安全機能記述
    - 安全機能に対する帰結
    - 提案するSecurity Measureの記述

IEC63074CDの概要(6/8)

- 5.4　Security Measures
  - いかなるSecurity MeasuresもSCSの果たす安全機能に影響してはならない：安全機能反応の反応時間に対するSecurity Measuresの影響などのように更なる調査を行う必要がある。特に次のような点に留意することが推奨される。
    - ネットワークアーキテクチャー
    - ポータブルデバイス
    - 無線デバイスやセンサー
    - リモートアクセス
    - 他のシステムとのIFやHMI
  - Security要求の例
    - 5.4.1 SCSへの人間・SWプロセス・デバイスのアクセスをIdentification/Authenticationにより管理
    - 5.4.2 アクセス者の資格に応じたSCS使用許可範囲の管理
    - 5.4.5 データフローの制限の目的でネットワークをセグメント化するとSCS内のデータ通信速度に影響しひいてはSCSの反応時間が長くなることがありうる。

IEC63074CDの概要(7/8)

- 6.　Verification of Security Measures
  - Security Measuresの最終的verificationは機械ユーザーの責任
  - 機械メーカー（SCSの設計者）はSCSに組み込まれたSecurity Measures（サブシステム組み込みのものを除く）のverificationの責任を持つ
  - SCSのサブシステムメーカー（サブシステムの設計者）サブシステム組み込みのSecurity Measuresのverificationの責任を持つ

IEC63074CDの概要(8/8)

- 7.　機械ユーザーに供給されるべき文書
  - 機械メーカー（SCSの設計者）はSCSのユーザー（＝機械ユーザー）に特定されたVulnerabilityとそのSCSに対する波及効果とを文書化して供給しなくてはならない。これによりユーザーによる全体的Securityリスクアセスメントをサポートすることになる。
  - 機械の使用に関係する場合には実装済みのSecurity Measuresに関する文書化された情報
  - Security Measuresの適切性の検証に関する文書化された情報

アウトライン

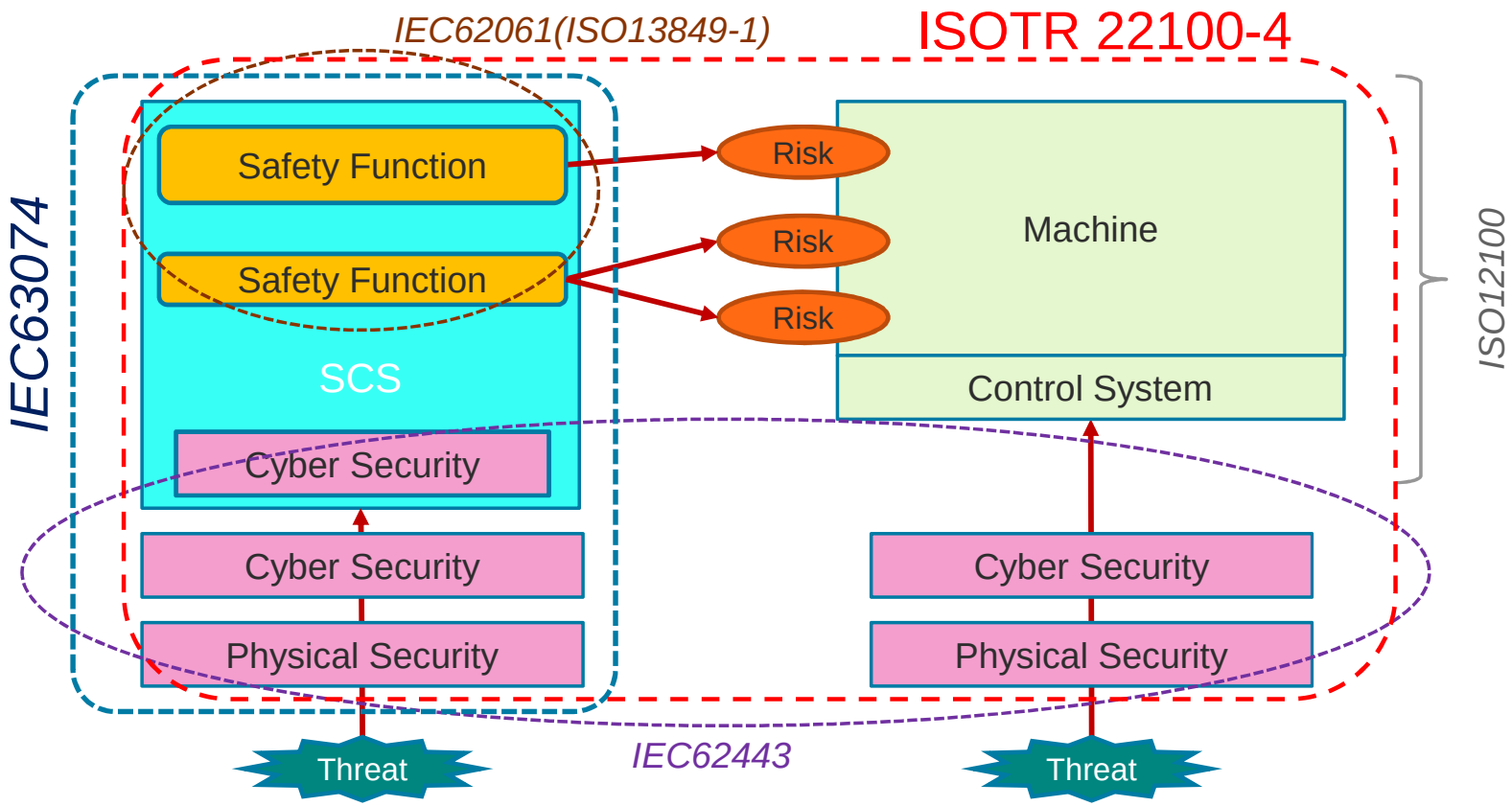
1. はじめに：会社紹介＆自己紹介
2. IEC63074開発の背景と動機
3. IEC63074CDの概要
4. IEC63074の課題
   - ISO12100との関係
   - TC65担当Security規格との関係
5. 開発のタイムライン
6. まとめ

IEC63074の課題 — ISO12100との関係

- ISO12100に基づく機械のリスクアセスメントにおいてSecurityアスペクトを考えることが必要とされてきている。
  - Safety Risk：機械の設計、使用条件が固定していれば静的
  - Security Risk：機械の設計、使用条件が固定でも、常に脅威は変化（Vulnerabilityも変化する可能性あり、動的

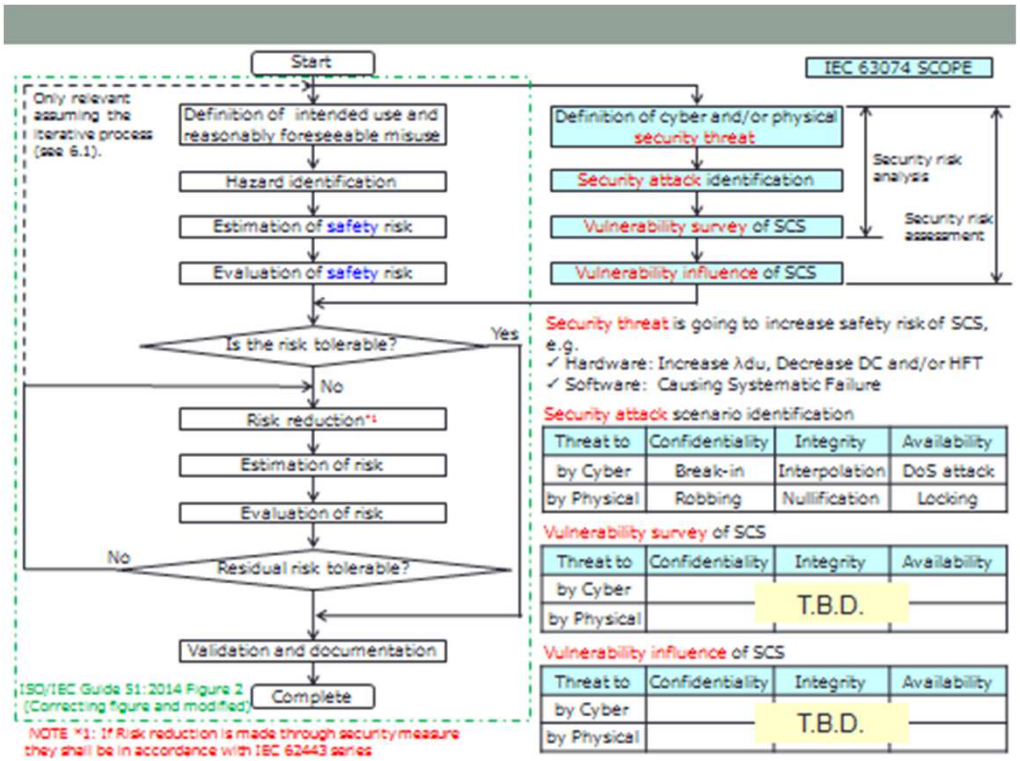
IEC63074の課題 — ISO12100との関係

IEC63074とISOTR 22100-4　(12100に関連するSecurityアスペクト）はScopeがオーバーラップ



IEC63074の課題 — ISO12100との関係

一つの方向性(日本案)→機械メーカの役に立つことに集中し、
ISOTR 22100-4の広すぎて難しいに対抗？



IEC63074の課題 — TC65担当Security規格との関係

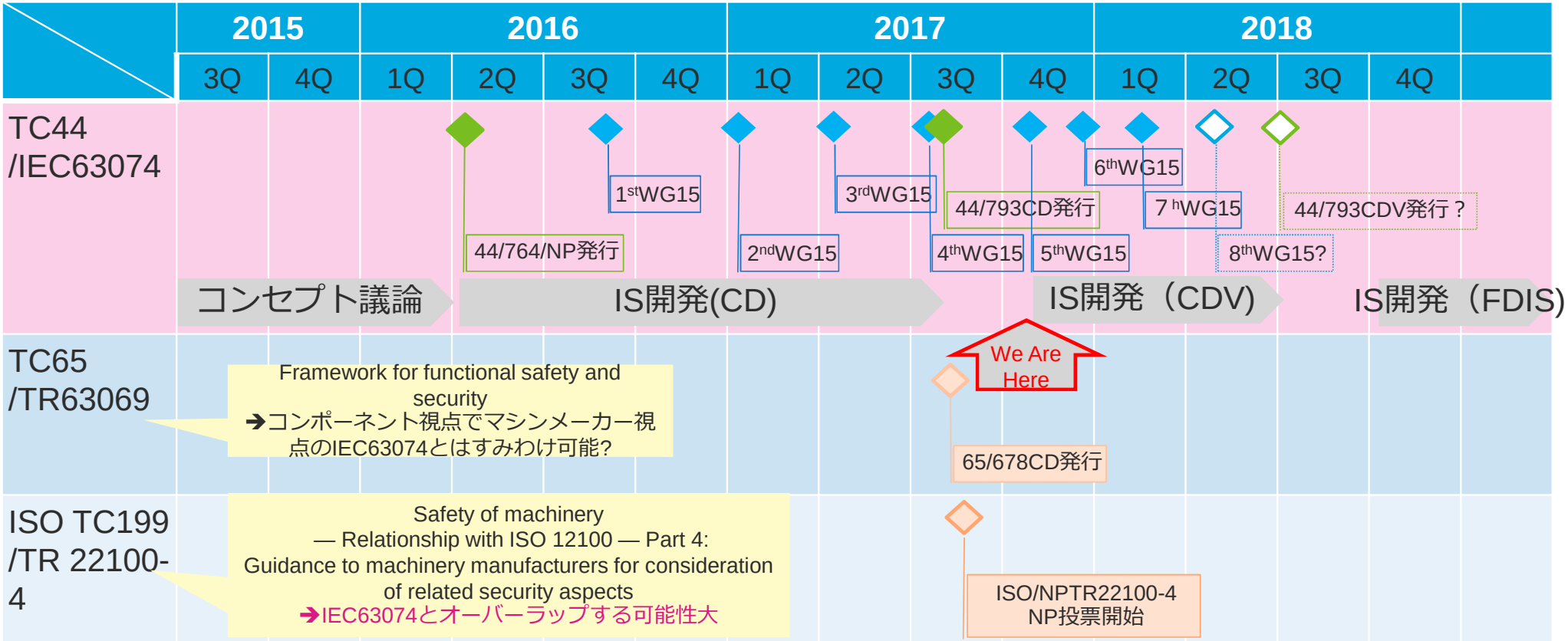
- SCSを構成するSafety ComponentのSecurityについてはIEC62443で担保されるべき
- 基本的にはSecurity Measuresの選択・実装はIEC62443による
  - 機械（Integration)レベルのSecurityにIEC62443を適用するのは実際的でない面がある（ワイヤレスコントロールに対する規定など）そのようなところにこのISは役立つのかどうかが課題
- TC65の下で “Framework for functional safety and security”(TR63069)の開発も進んでいるがこれはTarget Audienceの違いですみわけの方向

アウトライン

1. はじめに：会社紹介＆自己紹介
2. IEC63074開発の背景と動機
3. IEC63074CDの概要
4. IEC63074の課題
   - ISO12100との関係
   - TC65担当Security規格との関係
5. 開発のタイムライン
6. まとめ

IEC63074開発タイムライン

2018年中にFDIS発行をめざしているが・・・・

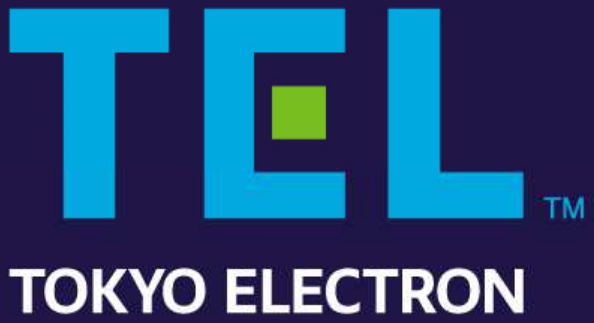


アウトライン

1. はじめに：会社紹介＆自己紹介
2. IEC63074開発の背景と動機
3. IEC63074CDの概要
4. IEC63074の課題
   - ISO12100との関係
   - TC65担当Security規格との関係
5. 開発のタイムライン
6. まとめ

まとめ

- IoT, Industrie4.0/ Smart Manufacturing等、機械をCPS（Cyber Physical Systems）に組み入れていく動きが活発化しているなかで、特にSecurity問題が機械の安全にも影響を与える可能性が高まっている。
- Securityが機械のSCSに影響を与えるモードは大きく分けると2通り
  - Vulnerabilityにつけこまれてシステムが直接攻撃をうけ、SCSの果たすべき安全性能が低下・喪失する。
  - Securityのための対策手段によりSCSの動作に関わる通信に影響が出て安全機能の反応速度が低下しSCSの果たすべき安全性能が低下・喪失する。
- 制御システムのSecurityに関してはTC65に実績があり、またISO TC199でもISO12100によるリスクアセスメントプロセスにおけるセキュリティ側面のガイド開発の動きがある中で、IEC63074が機械メーカーの役に立つISとして成立するためにはぶれないSCOPEと周りとの調整が不可欠


TEL
TM
TOKYO ELECTRON