安全関連制御システムの機能安全に関するセキュリテイ側面
－IEC(JIS) TR 63074－

- 令和 4年2月28日　日機連講演会

- 真白　すぴか
- 東京エレクトロン(株)

Disclaimer/お断り

- The views expressed are purely those of the author/presenter, and may not, in any circumstances, be regarded as stating an official position of Tokyo Electron LTD or any group in the IEC.
- 本講演において発表される内容は著者/発表者の見方を表現したもので、いかなる条件においても東京エレクトロン(株)もしくはIECのいかなるグループの公式な見解を延べるものではございません。

アウトライン

1. はじめに：自己紹介
2. IEC TR63074開発の背景と動機
3. IEC TR63074開発経過
4. JIS化原案作成経過
5. IEC TR63074:2019 及び(JIS) TR 63074の概要
6. IEC TR63074の課題
   - ISO12100との関係
   - TC65担当Security規格との関係
7. TS化の動き
8. まとめ

アウトライン

1. はじめに：自己紹介
2. IEC TR63074開発の背景と動機
3. IEC TR63074開発経過
4. JIS化原案作成経過
5. IEC TR63074:2019 及び(JIS) TR 63074の概要
6. IEC63074の課題
   - ISO12100との関係
   - TC65担当Security規格との関係
7. TS化の動き
8. まとめ

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です。
- 半導体製造装置のプロセス･製品開発に携わるうちに環境安全分野、装置と工場設備との各種インターフェース等について、業界標準であるSEMI Standardの開発活動に関与するようになりました。
- 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してきました。
- 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。ちょうどそのようなタイミングで「セキュリティとセーフティ」のテーマをTC44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案。WG15(Security)設立当初から国際エキスパートとして参加継続中です。
- IEC TR 63074発行後はTR B 63074原案作成委員会で委員長を務めさせていただきました

アウトライン

1. はじめに：自己紹介
2. IEC TR63074開発の背景と動機
3. IEC TR63074開発経過
4. JIS化原案作成経過
5. IEC TR63074:2019 及び(JIS) TR 63074の概要
6. IEC63074の課題
   - ISO12100との関係
   - TC65担当Security規格との関係
7. TS化の動き
8. まとめ

IEC63074開発の背景

- Connected Fab, IIoT(Industrial Internet of Things),Smart Manufacturing/Industrie 4.0　などの進展により、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に従い、機械に対するセキュリティリスクは増加傾向であり、安全制御系の安全機能を妨げる可能性が高まっている
- 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かのように扱っている
- ISO/TC199においては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→実際はIEC63074に若干先行してISO/TR 22100-4の開発を開始

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観点で必要との認識
- 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という認識

アウトライン

1. はじめに：自己紹介
2. IEC TR63074開発の背景と動機
3. IEC TR63074開発経過
4. JIS化原案作成経過
5. IEC TR63074:2019 及び(JIS) TR 63074の概要
6. IEC63074の課題
   - ISO12100との関係
   - TC65担当Security規格との関係
7. TS化の動き
8. まとめ

IEC TR 63074出版までのヒストリー

年	月	主要な動き
15	9	TC44総会のアドホックとしてSafety & Security会議開催。IS開発のNWPを起こす方向に合意
16	5	44/764/NP（SECURITY ASPECTS RELATED TO FUNCTIONAL SAFETY OF SAFETY-RELATED CONTROL SYSTEMS）投票→承認
17	7-9	44/793/CD投票
17	10	StandardではなくTRとする方針変更にWG内合意

年	月	主要な動き
18	3-6	44/813/CD発行　（TRとして出版を目指してのCD）
18	9	44/838/CC発行
18	10-11	44/842/DTR投票
18	12	44/842/DTR承認
19	5	IEC TR 63074:2019　出版

アウトライン

1. はじめに：自己紹介
2. IEC TR63074開発の背景と動機
3. IEC TR63074開発経過
4. JIS化原案作成経過
5. IEC TR63074:2019 及び(JIS) TR 63074の概要
6. IEC63074の課題
   - ISO12100との関係
   - TC65担当Security規格との関係
7. TS化の動き
8. まとめ

国際規格提案からTRへの変更、JIS化に至る経緯

- IEC TR63074の開発開始当初は、産業用システム全般のセキュリティを扱うIEC 62443（規格群）やISO 27001において必ずしも十分な考慮がなされていないセキュリティ上の脅威やそれに対する対応と機械の安全システムの安全機能の確保との間のギャップをなくすために必要な要求事項を国際規格(IS)として発行することを意図して提案された。
- 開発の途上で，機械の安全関連制御システムの安全機能動作に影響を及ぼす可能性のあるセキュリティ側面に焦点を当てて，IEC 62443（規格群）の機械への適用の指針を与える国際標準報告書(TR)としての発行が適切であるとして，最終的に国際標準報告書として発行された。
- 当初のISからTRへの方針変更について「前述のギャップを埋める国際文書をできるだけ早期に発行して機械の安全に貢献する」という観点から日本は支持した。そこで，国内においてIEC TR発行を受けJIS化をすることになった。

JIS TR B63074 進捗状況

年	月	主要な動き
19	5	IEC TR 63074:2019　出版
19	7	第1回 JIS B TR63074原案作成委員会
20	1	第7回 JIS B TR63074原案作成委員会（原案完成）
20	3	JIS TR B 63074原案様式調整依頼提出
21	7	JIS化申出

アウトライン

1. はじめに：自己紹介
2. IEC TR63074開発の背景と動機
3. IEC TR63074開発経過
4. JIS化の進捗
5. IEC TR63074:2019 及び(JIS) TR 63074の概要
6. IEC63074の課題
   - ISO12100との関係
   - TC65担当Security規格との関係
7. TS化の動き
8. まとめ

IEC TR63074:2019 及び(JIS) TR 63074の概要(0/12)：全体構成

- FOREWORD
- INTRODUCTION

1. Scope
2. Normative references
3. Terms and definitions
4. Safety and security overview
5. Security aspects related to functional safety
6. Verification and maintenance of security countermeasures
7. Information for the user of the machine(s)

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

IEC TR63074:2019 及び(JIS) TR 63074の概要(0/12)：全体構成

a) 適用範囲（箇条1）
b) 引用規格（箇条2）
c) 用語及び定義（箇条3）
d) 安全側面及びセキュリティ側面の概要（箇条4）
e) 機能安全に関するセキュリティ側面（箇条5）
f) セキュリティ対策の検証・維持（箇条6）
g) 機械の使用者のための情報（箇条7）
h) 附属書A（参考）脅威及び脅威モデリングアプローチに関する基礎情報
i) 附属書B（参考）セキュリティリスクアセスメントのきっかけ
j) 附属書C（参考）装置供給者，機械の製造業者（インテグレータ）及び機械の使用者間の情報フローの例

IEC TR63074:2019 及び(JIS) TR 63074の概要(1/12)

- 適用範囲（SCOPE）
  - 安全関連制御システム（SCS）が実施し実現する機能安全に影響を与え，機械を安全に運転することを維持する能力の喪失につながる，セキュリティ脅威及び脆弱性において，IEC 62443（規格群）の使用に関する指針を示す

➔IEC TRの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に記載してあり、JISにおいては序文に反映した

  - SCSに関連する可能性がある機械のセキュリティ側面
    - セキュリティ攻撃・侵害を引き起こしうるようなセキュリティ脅威が利用する可能性のある，機械の他の部分を介した直接的又は間接的なSCSの脆弱性
    - SCSの安全特性及びその機能を適切に実行する能力への影響
    - 典型的な事例の定義及び対応する脅威モデルの適用

IEC TR63074:2019 及び(JIS) TR 63074の概要(2/12)

- 4　　安全側面及びセキュリティ側面の概要（Safety and security overview）
- 4.1　一般事項
  - 安全面とセキュリティ面との関係は次のように特徴付けられる
    - 機械は適切な保護方策(protective measure)を有する
    - 機械に適用するセキュリティ対策(security countermeasures) は，安全機能を実行する保護方策のパフォーマンス低下を避けるために適切なものであるべきである。
- 4.2　安全性の目的(Safety objectives)
  - 機械のSCSが実行する安全機能は，JIS B 9961に適合するSIL又はJIS B 9705-1に適合するPLと同等の安全度レベルを達成しなければならない。

IEC TR63074:2019 及び(JIS) TR 63074の概要(3/12)

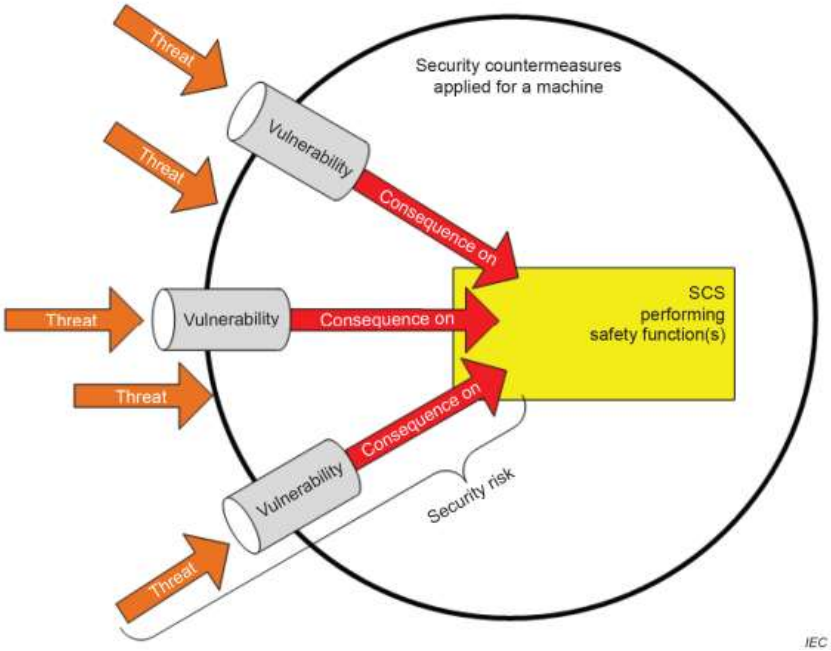
- 4　　安全側面及びセキュリティ側面の概要（Safety and security overview）
- 4.3　セキュリティの目的 (Security objectives)
  - セキュリティの3目的（機密性，完全性，及び可用性を達成すること）の例。
    - 操作に対する完全性
    - セキュリティ及び産業オートメーションの両分野が，一般的に受け入れている方法による機密性
    - 機械（安全機能を含む）の可用性（通常，非常に一般的）
  - セキュリティリスクアセスメント
    - セキュリティリスクアセスメントは製品又はシステムごとに脅威及び既知の脆弱性のある使用環境を含めて実施する。これは機械が総合的なセキュリティの目的を達成するために必要なセキュリティ対策を導き出すことを目的として行われる。
  - 機械類の安全性に関連して，セキュリティ対策は，機械類の安全な運転を維持する能力を保護することを意図している。また、セキュリティ対策の実装はいかなる安全機能に対しても悪影響を及ぼさないようにすることが望ましい。

➔セキュリティアセスメントは定期的、及びイベントトリガーで繰り返し実施が必要

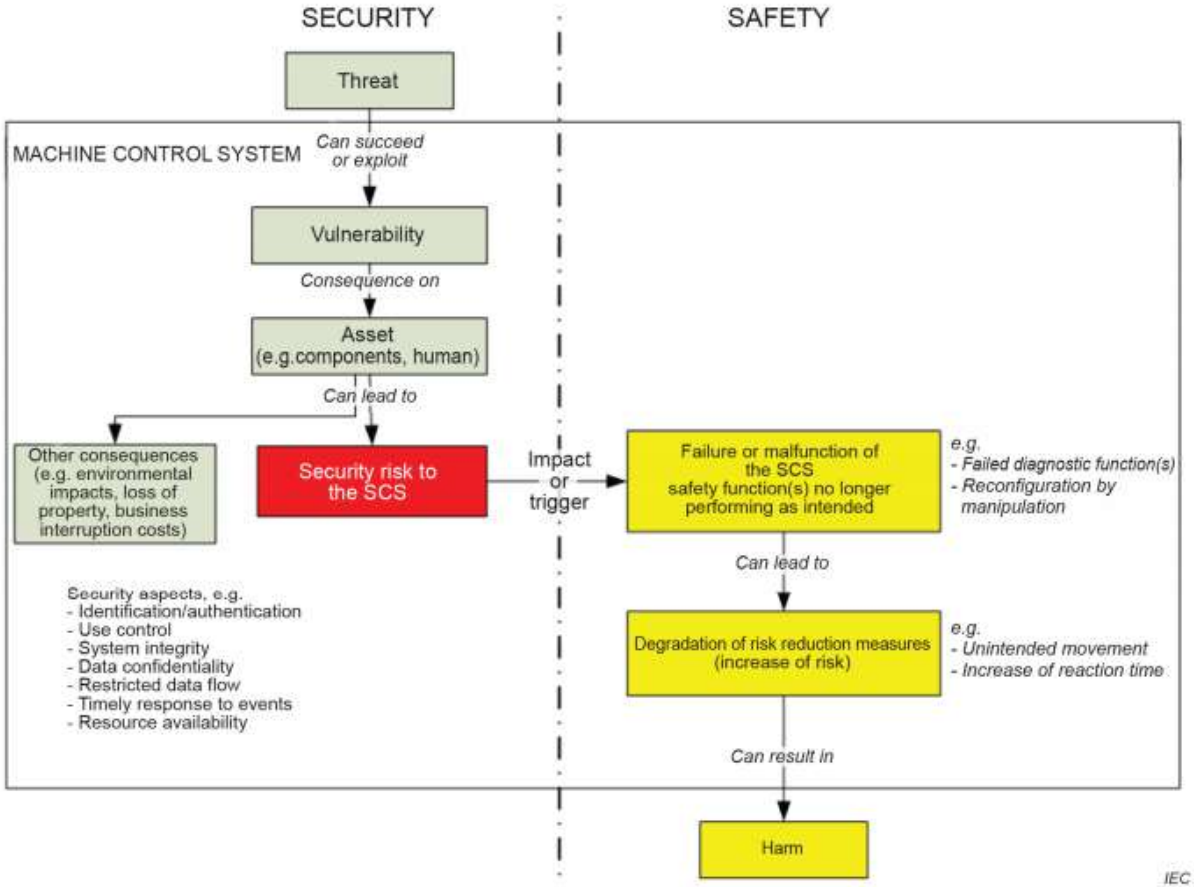
➔セキュリティリスクアセスメントの結果で対策をとった場合、安全機能のパフォーマンスを再度チェックする必要が出る可能性もある

IEC TR63074:2019 及び(JIS) TR 63074の概要(4/12)

- 4　安全側面及びセキュリティ側面の概要



安全機能を実行するSCSに対するセキュリティリスクと脅威，ぜい弱性及び結果との関係



SCSに対するセキュリティリスクの影響の可能性

IEC TR63074:2019 及び(JIS) TR 63074の概要(5/12)

5. 機能安全に関するセキュリティ側面

- 5.1　一般
  - 5.1.1セキュリティリスクアセスメント
    - SCSに関するセキュリティリスクアセスメントは，その環境における機械の全体的なセキュリティリスクアセスメントの一部であり，設計，実装，立上げ，運転，保守などの様々な段階の考慮を含む。
      - NOTE：一般に機械の使用環境における全体的なセキュリティリスクアセスメントは通常，機械ユーザーと機械製造業者とが協働して実施する。
    - 脆弱性アセスメントは，セキュリティリスクアセスメントの一部であり、機械の脆弱性（脅威によって利用され得る。）及び安全性に関連する潜在的な影響を特定するために，脆弱性の評価を実施することが望ましい。
    - 脆弱性の評価で利用すべき情報
      - a)　脆弱性の評価の対象となる装置（例えば，SCSに接続された他の装置）の説明
      - b)　脅威によって悪用され，セキュリティ上のリスクをもたらす可能性が特定された脆弱性の説明
      - c)　セキュリティ対策によって保護されることが望ましいSCSの部分（HW・SWなど）の説明

IEC TR63074:2019 及び(JIS) TR 63074の概要(6/12)
（5.1.1セキュリティリスクアセスメント続き）

- 機械の製造業者は，脅威について何らかの仮定を立て（NOTE：機械ユーザーとのコミュニケーションが取れない等でも），脆弱性アセスメントに基づいてセキュリティ対策を実施することが可能である。
- 全体的なセキュリティリスクアセスメントに照らしてセキュリティ対策が適切であることを確かめるために検証を行うことが望ましい。
  - NOTE:　セキュリティ対策が適切であることの検証は，通常，機械ユーザーの環境において実行され，想定される脅威の情報を必要とする可能性がある。

– セキュリティリスクアセスメントの側面の例

- 特定した脅威及びその原因（ハードウェア，アプリケーションプログラム，及び関連ソフトウェアに対する意図的な攻撃を含む。）
- 特定した脅威と脆弱性との組合せに起因する潜在的な結果（セキュリティリスク）の説明
- 追加の方策のための要求事項の決定
- 脅威を軽減又は除去するために取られた対策に関する情報の説明又は参照。
  - NOTE：初期は脆弱性が限られていた安全関連制御システム SCSは，環境の変化，技術の変化，システムの故障，機器交換不能，要員の変更，及び脅威インテリジェンスなどの状況によって，より脆弱になる可能性がある。

IEC TR63074:2019 及び(JIS) TR 63074の概要(7/12)

– 5.1.2　　セキュリティリスク対応戦略

- セキュリティリスク対応戦略は，セキュリティリスクアセスメントの間中に決定され，セキュリティリスクアセスメント全体において考慮することが望ましい。
- 機械類の安全性分野におけるセキュリティ上のリスクへの対応には，次のものが含まれる。
  - 次のいずれかによる許容できないセキュリティリスクの軽減
    a. セキュリティリスクを排除する（回避する）設計
    b. セキュリティリスクの制限（例えば，機械の製造業者が直接適用した，機械の使用者が適用した，又は機械製造業者と使用者との間で連携した対策）
  - NOTE: セキュリティリスク対応戦略は，IEC 62443-4-1:2018の図3による多層防御戦略をとっても良い。
  - 許容できるならばセキュリティリスクを受け入れる。（それ以上の対応不要）

IEC TR63074:2019 及び(JIS) TR 63074の概要(8/12)

- 5.2　セキュリティ対策
  - 5.2.1　　一般
    - 機械に適用されるセキュリティ対策は，SCSによって実行される安全機能に悪影響を及ぼさないことが望ましく，更にそのことを検証する必要がある。例えば，セキュリティ対策による安全に対する影響のより深い調査（例えば，安全機能の応答時間）である。
    - NOTE：通常の運転機能（機械機能）に適用されるセキュリティ対策は，SCS が実行する安全機能に影響を及ぼす可能性がある。
    - 特に，ネットワークアーキテクチャ（ネットワークゾーニングなどの設計、ファイアウォール構成、ユーザー承認と認証、異なるプロセスネットワークとの接続、ワイヤレス通信、外部ネットワークへのアクセス）、携帯機器、ワイヤレスデバイス、リモートアクセス、他のシステムとのインタフェース又はヒューマン マシン インタフェースを考慮するべき。
    - NOTE：セキュリティ対策は，機械の外部で行うことが可能である（例えば，ポリシーの手順及び認識，物理的セキュリティ，ネットワークセキュリティ，コンピュータセキュリティ，及びアプリケーションセキュリティ）。
    - セキュリティ対策は，IEC 62443規格群の基本要求事項とSCSへの影響とを考慮し、また攻撃の動機及び結果に見合うように設計することが望ましい。

IEC TR63074:2019 及び(JIS) TR 63074の概要(9/12)

- 5.2.2　識別及び認証
  - SCSへのアクセスを識別し，認証する能力が必要となることがある。
  - 無許可のアクセス及び変更を防止するための例には，人間である使用者の識別及び認証、ネットワークの接続認証、ソフトウェアのアカウント管理、パスワードによる認証、個々の使用者に対するパスワード生成及び有効期間の制限、機械間の識別及び認証手順、などがある。
- 5.2.3　使用管理
  - 使用者を識別し認証する場合，SCSは，許容する行為を認証された使用者の割り当てられた権限のみに制限する必要がある可能性がある。
- 5.2.4　システムの完全性 (integrity)
  - 機械ユーザー（例えば，資産所有者）は，通常，無許可の操作を防止するために，SCSを含む制御システムの完全性を維持することに関与する。
  - 例としては、信頼できないネットワークにおける暗号化による完全性保護の使用や、懸念のあるインタフェース（例えば，USB，PLC又はSCSに対するプログラミングインタフェース）を考慮した，悪意のあるコードからの保護などの措置がある

IEC TR63074:2019 及び(JIS) TR 63074の概要(10/12)

- 5.2.5　データ機密性
  - 一般に，制御システムが生成する情報には，その情報が一時保持中又は伝送中のいずれであっても機密性が高く，慎重に扱うべき性質のものがある。これは相当する通信チャネルや蓄積データを傍受及び無許可でのアクセスから保護する必要があることを意味する。
- 5.2.6　制限データフロー
  - 情報フロー制限の要求事項は，総合的なセキュリティリスクアセスメントによって決定する。
  - NOTE: 詳細は，IEC 62443-3-3:2013の箇条9参照。
  - 情報フローの制限による伝送遅延又は応答時間の増加は，SCSの安全度に影響を及ぼす可能性がある。
- 5.2.7　イベントに対する適時対応
  - 機械ユーザー（例えば，資産所有者）は，セキュリティ侵害に対するタイムリーな応答のために必要な，セキュリティ方針及び手順，並びに通信及び制御の適切な回線を確立していることが望ましい。
  - この側面は，全体的なセキュリティリスクアセスメントにおいて考慮され，SCSのsafety integrityに関連する可能性がある。
- 5.2.8 リソース可用性
  - 目的は制御システムが様々なタイプのサービス妨害（DoS）イベントに耐えることを保証すること。

IEC TR63074:2019 及び(JIS) TR 63074の概要(11/12)

6. セキュリティ対策の検証・維持

- セキュリティ対策の実装は，機械ユーザー，機械の製造業者，及びサブシステム製造業者が，適宜，検証し，維持することが望ましい（5.1.セキュリティリスクアセスメント，5.1.1も参照）
  - Security Measuresの最終的verificationは機械ユーザーの責任
  - 機械製造業者（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のサブシステム製造業者（サブシステムの設計者）はサブシステム組み込みのSecurity measuresの検証責任を持つ

IEC TR63074:2019 及び(JIS) TR 63074の概要(12/12)

7. 機械ユーザーのための情報

- 機械の製造業者は，総合的なセキュリティリスクアセスメントをサポートするために，機械ユーザーに情報を提供することが望ましい。
- 代表的なものとしては、安全機能（アーキテクチャ，ネットワークトポロジーなど）の概要、脆弱性アセスメント（5.1.1参照）に基づく情報，又は必要に応じて，特定又は報告された脆弱性に関する情報、必要に応じて，機械内で実装済みのセキュリティ対策に関する情報（5.2参照）、等が含まれる

アウトライン

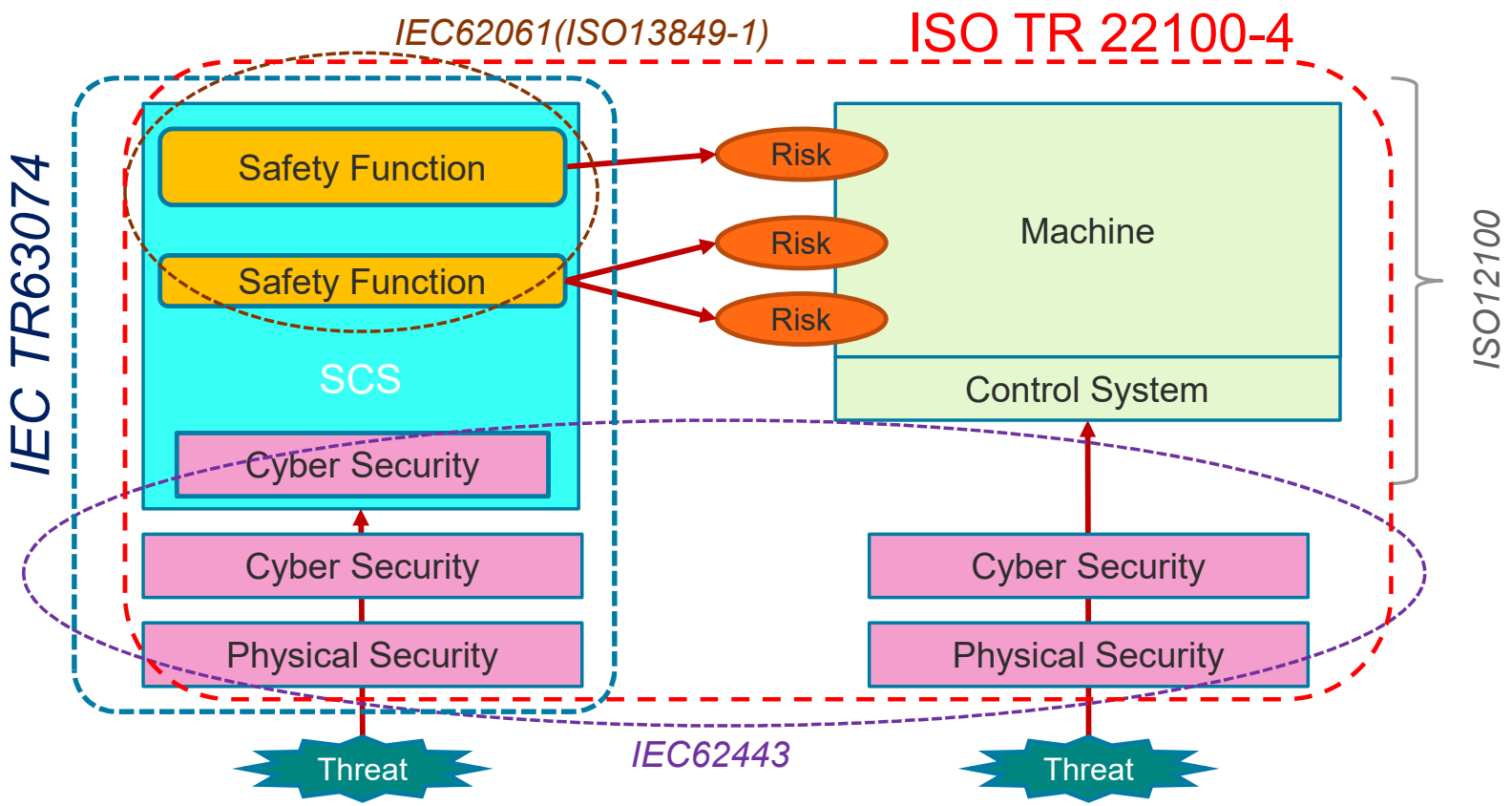
1. はじめに：自己紹介
2. IEC TR63074開発の背景と動機
3. IEC TR63074開発経過
4. JIS化の進捗
5. IEC TR63074:2019 及び(JIS) TR 63074の概要
6. IEC63074の課題
   - ISO12100との関係
   - TC65担当Security規格との関係
7. TS化の動き
8. まとめ

IEC TR63074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

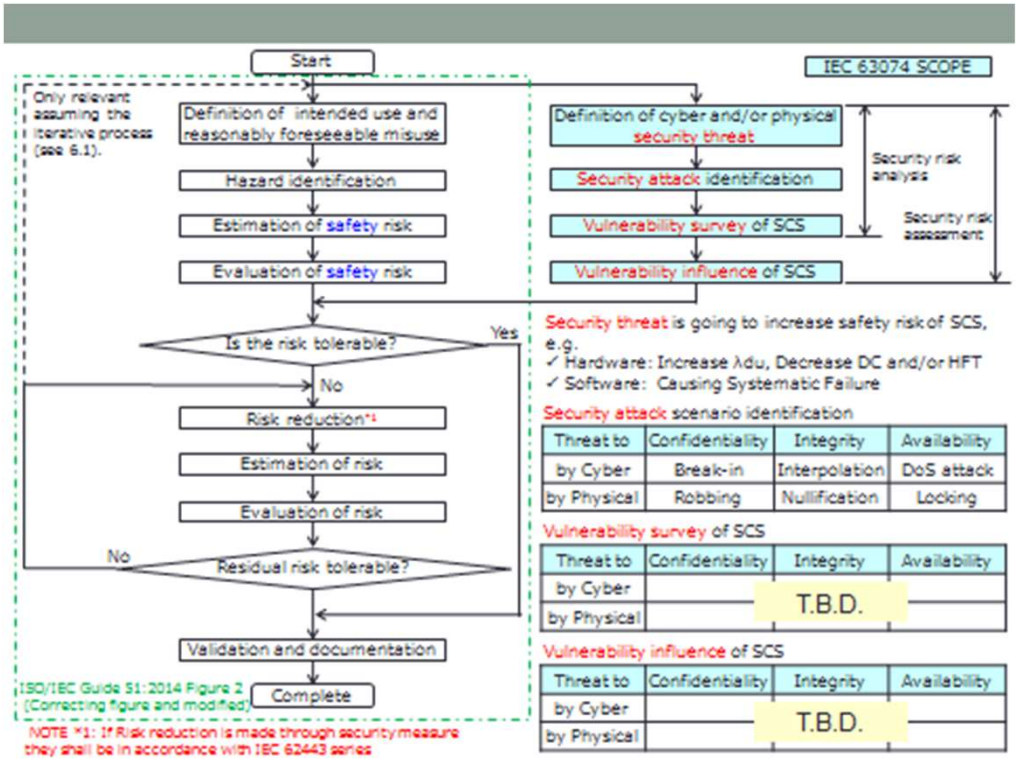
IEC TR63074の課題 — ISO12100との関係

IEC TR63074とISO TR 22100-4　(12100に関連するSecurityアスペクト）はScopeがオーバーラップ



IEC TR63074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に集中し、ISO TR 22100-4の広すぎて難しいに対抗？



IEC TR63074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TRは役立つのかどうかが課題
- TC65の元で “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：自己紹介
2. IEC TR63074開発の背景と動機
3. IEC TR63074開発経過
4. JIS化の進捗
5. IEC TR63074:2019 及び(JIS) TR 63074の概要
6. IEC63074の課題
   - ISO12100との関係
   - TC65担当Security規格との関係
7. TS化の動き
8. まとめ

IEC63074 TS化の動き

- 動機
  - 法規制動向への対応（特に欧州MPR）
  - 機械に固有の条件への対応
    - 安全制御に関連する機械内の機器が安全にかかわらないシステムにも接続されるような状況におけるセキュリティリスクへの対応
    - 安全制御の要求パフォーマンスを達成するうえで重要な接続(ハードウェア）を意図的もしくは事故による改変から保護する必要性
    - 安全要件への適合の為に重要なソフトウェアやデータの特定と、それらを意図的もしくは事故による改変から保護する必要性

IEC63074 TS化の経過と予定

年	月	主要な動き
21	6	44/917/NP（Safety of machinery – Security aspects related to functional safety of safety-related control systems）でIEC TR63074をTS化する提案
21	9	NP可決（日本も賛成しExpertを出すことに）
21	10	Kick Off会議　（NPへのコメント審議とTS案の作成作業開始）

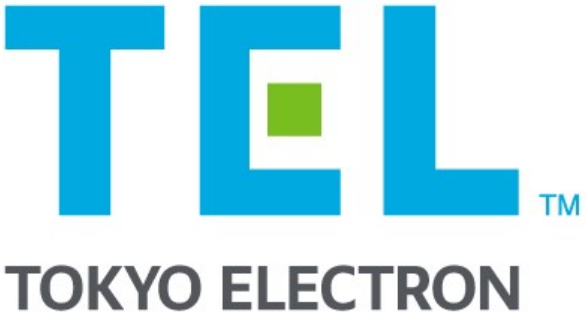
年	月	主要な動き
22	1	（NPへのコメント審議とTS案CD作成完了）
22	1	**44/943/CD**（TS 63074 ED1のCD）投票開始
22	3	18日に投票締め切り
22	4	CDへのコメント審議開始
22	?	承認

アウトライン

1. はじめに：自己紹介
2. IEC TR63074開発の背景と動機
3. IEC TR63074開発経過
4. JIS化の進捗
5. IEC TR63074:2019 及び(JIS) TR 63074の概要
6. IEC63074の課題
   - ISO12100との関係
   - TC65担当Security規格との関係
7. TS化の動き
8. 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
  - 脆弱性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
  - セキュリティ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ISO 12100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ISO TR 22100-4も発行されている状況下IEC TR63074を機械メーカーの役に立つTS、ひいてはISに発展させるためにはぶれないSCOPEと周りとの調整が不可欠であると考えられる


TEL
TM
TOKYO ELECTRON