基礎コース

安全の基本　in Society5.0

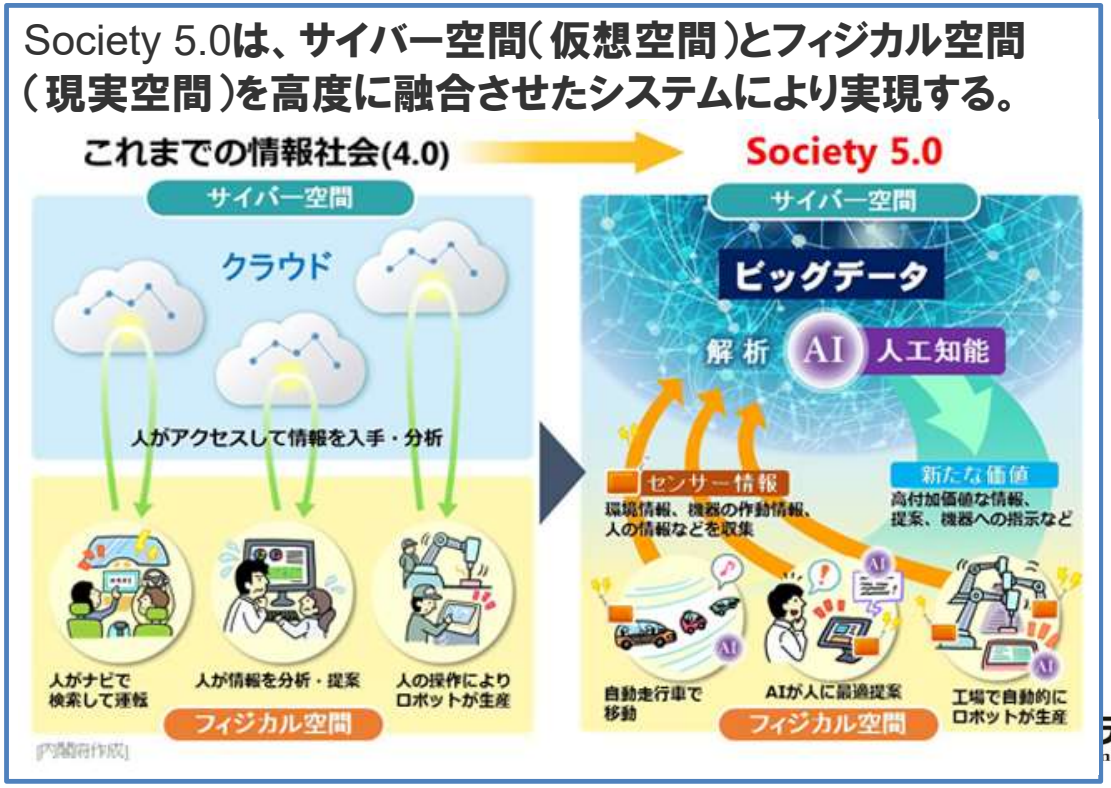
2022年9月28日

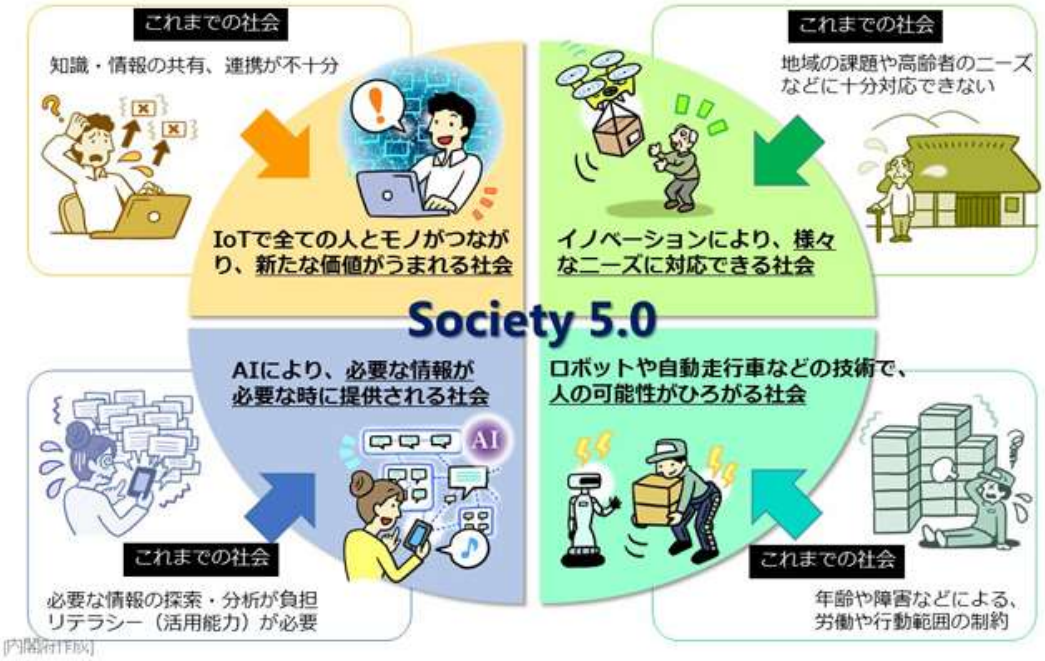
安全性向上委員会
小水　元（㈱村田製作所）

一般社団法人 組込みシステム技術協会
Japan Embedded Systems Technology Association

まえがき

Society5.0と呼ばれる時代を迎えた今、セーフティとセキュリティを両立させないといけないような多様なソリューションが増えるなど、従来の安全性対策では網羅しきれない安全要求が増えている。



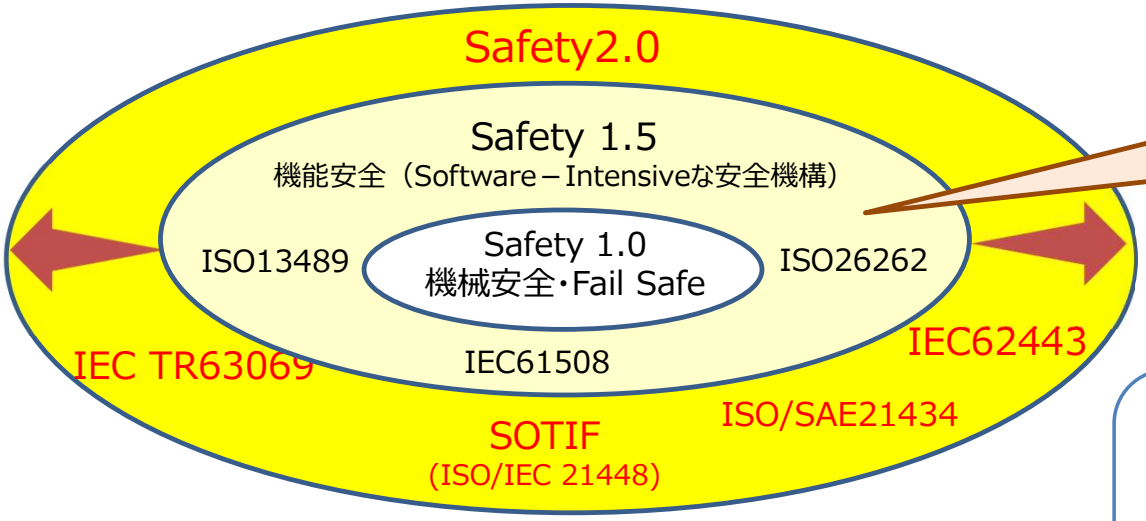


まえがき

AI・IoT時代の大規模で複雑なシステムに対して
安全な製品を開発し、世の中に送り出すには
安全分析の背景、リスクアセスメント、
安全論証や安全規格を理解し使っていく上で必要となる
安全の考え方を学ぶ必要がある

では、安全を脅かすアクシデントとは？

なぜ安全性の向上が必要なのか？



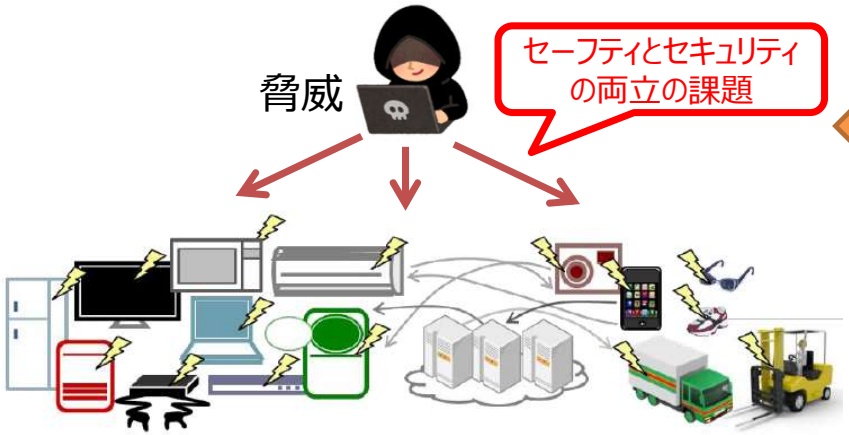
◆これまでの安全要求
「壊れにくい高品質」
「壊れることを前提とするが危険にはつながらない」

これからは・・・

既存規格では対処しきれない領域の問題

- システムの複雑化
- AI技術の普及した環境
- 「つながる」ことによる新たな懸念
- 「コトづくり」による加点主義（100点でなくて良い）

事例



安全論証（説明責任を果たす）を行うベースは変わらないが、**安全要求の定義が難しくなる**

【参考】「コトづくり」の安全性

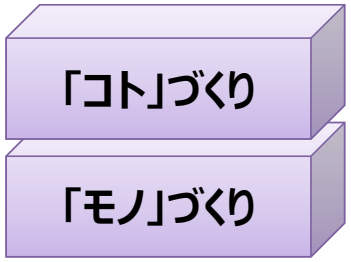
システムは複雑になりセーフティとセキュリティの両立が課題になるこれから、**ビジネスは「モノづくり」から「コトづくり」へ**

=>「コトづくり」時代の“安全性”を品質保証の観点から考える

■モノの品質保証：「品質を決めるのは、お客様(ユーザ)である」を優先した品質保証
【これまで】「所有する」車の品質　＝　安全性、耐久性など　（※プロダクトアウトでも良かった）
【これから】「利用する」車の品質　＝　耐久性よりも故障する前にメンテナンスを行える“予測機能”、快適性、より目的に見合った機能の車など　（※マーケットインでなければ取り残される）

■コトの品質保証：「人と人を取り巻く環境・社会に役立つことを中心に据えた品質保証」
【これまで】「モノ」の品質　＝　機能的価値、ハードの価値（機能的品質）、モノを中心に据えた品質保証
【これから】「コト、サービス」の品質　＝　体験や経験価値、時間や空間などソフトの価値（※感情的品質、スピードも重視）
・人を取り巻く環境・社会を中心に据えた品質保証（どれくらい役に立っているか？、快適か安全で安心か？）

（参考文献）「2030年の品質保証」



注）「コト」づくりが上位にくる2階建て
「モノづくり」が無くなるわけではない

100点満点が当たり前の減点主義から新しいことは60点でも認められる加点主義へ

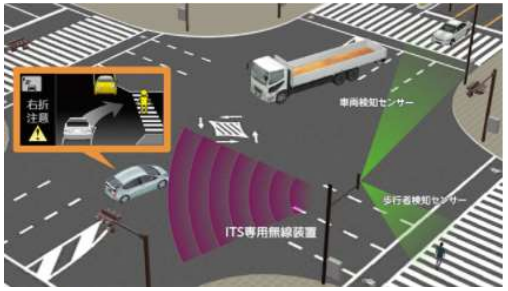
安全性が軽視されるのか？

一般社団法人 組込みシステム技術協会 Japan Embedded Systems Technology Association

【参考】「コトづくり」の安全性

壊れ難い車

ぶつからない車



診断する車

【搭乗者を診断】
- ドライバーの体調が悪い場合はエンジンがかからない

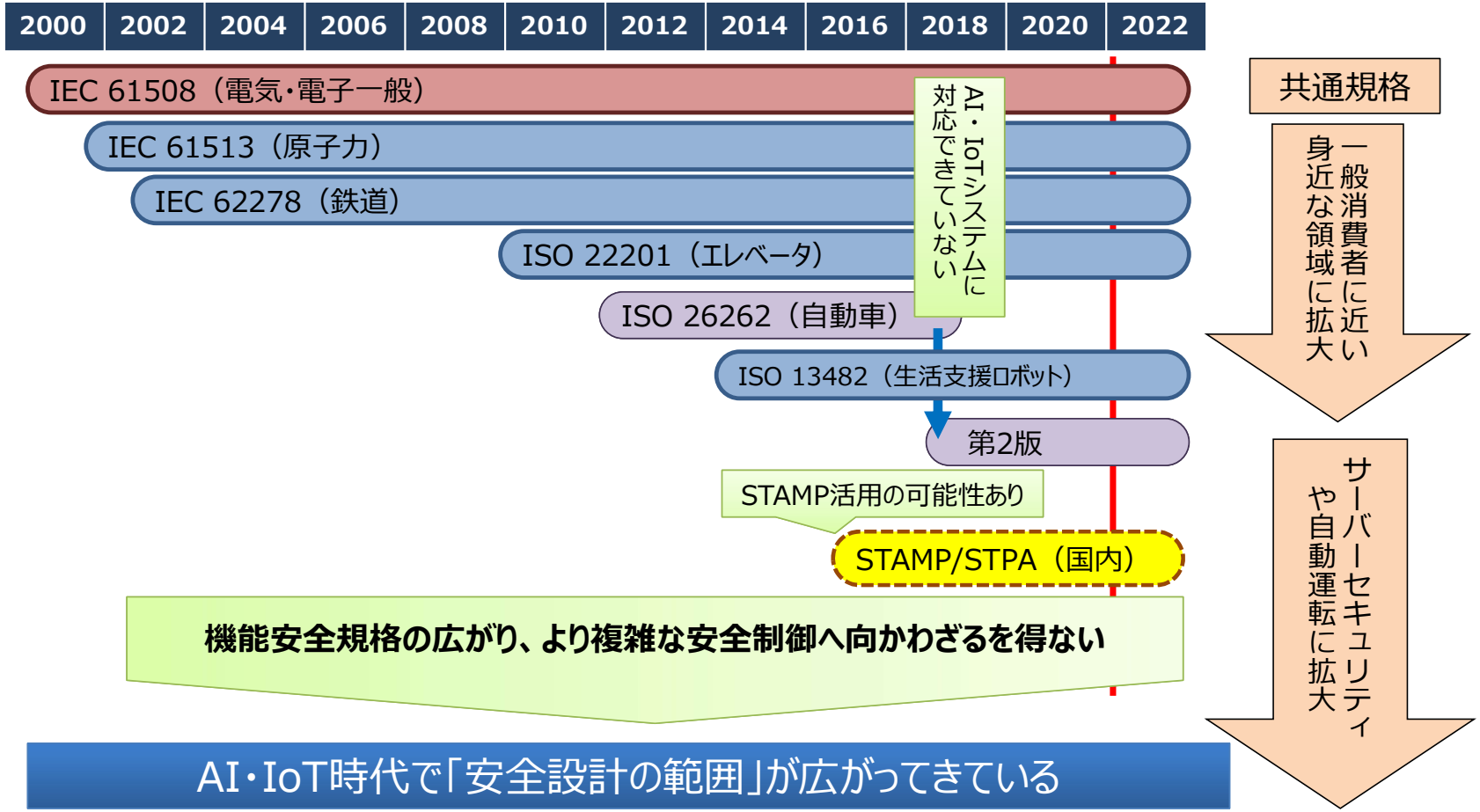
【自己診断】
- 故障予測によるメンテナンス情報を定期的にメーカーにUpload

安全要求は変化していく

過去の安全要求が無くなるわけではなく累積

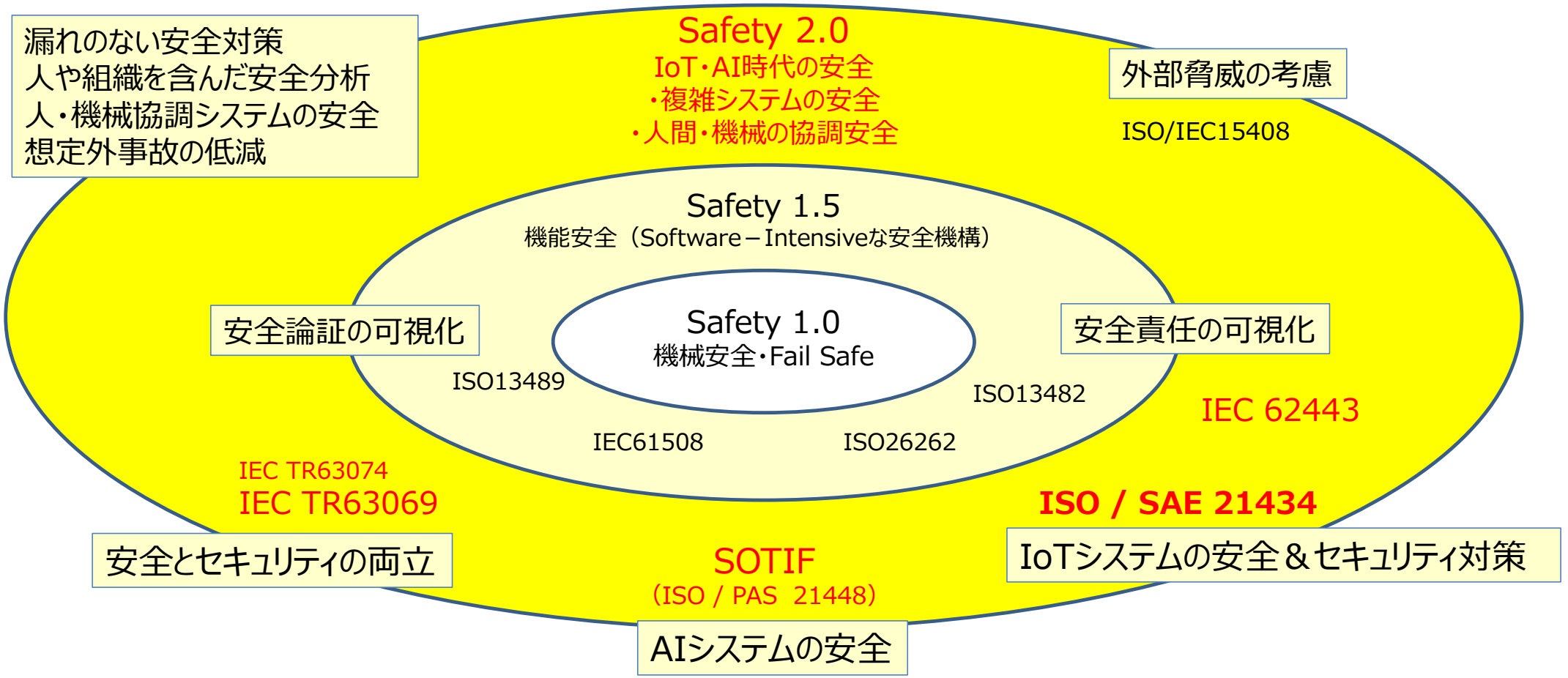
昨今のセーフティを取り巻く規格動向

AI・IoT時代の課題と今後のセーフティ



一般社団法人 組込みシステム技術協会 Japan Embedded Systems Technology Association

Safety2.0時代の「安全設計」範囲の広がり



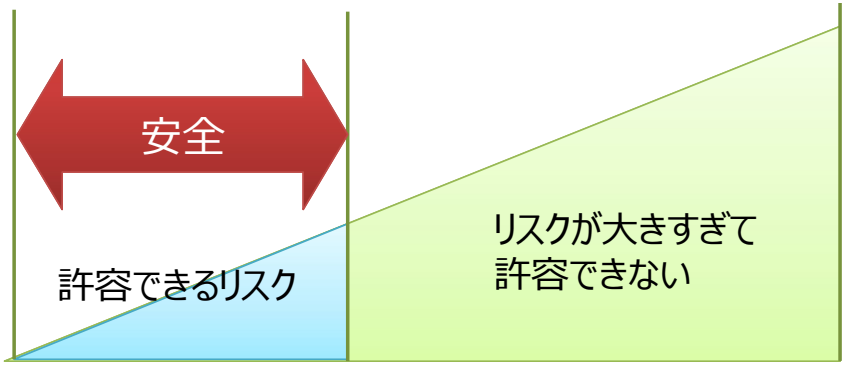
安全（セーフティ）とは？

つまり、アクシデントにならないようなシステムの状態

安全とは「許容できないリスクがないこと」

（ISO/IEC GUIDE51:2014）

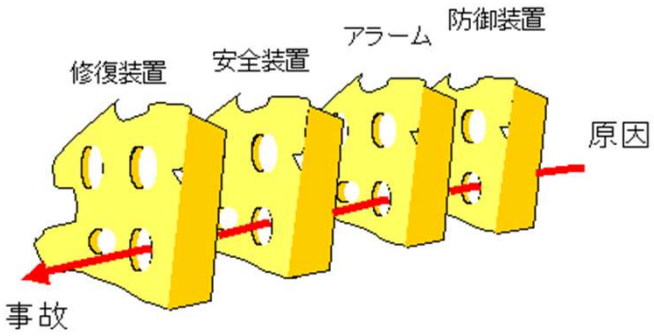
※許容できないリスクとは、その時代の社会の価値観に基づき、
　特定のコンテキストにおいて受け入れられる水準のリスク



安全の基本概念

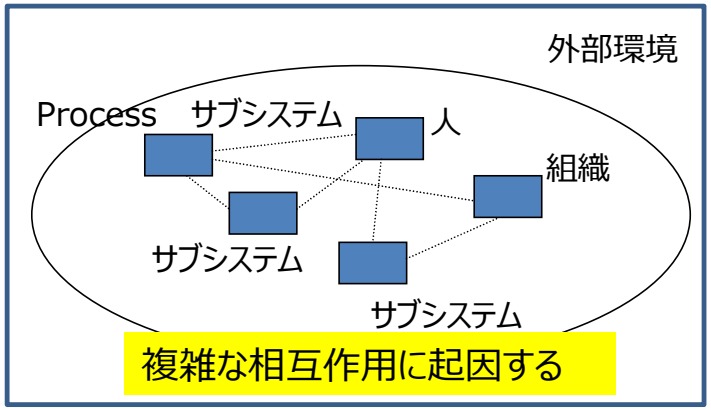
◆従来の事故モデル

スイスチーズ事故モデル

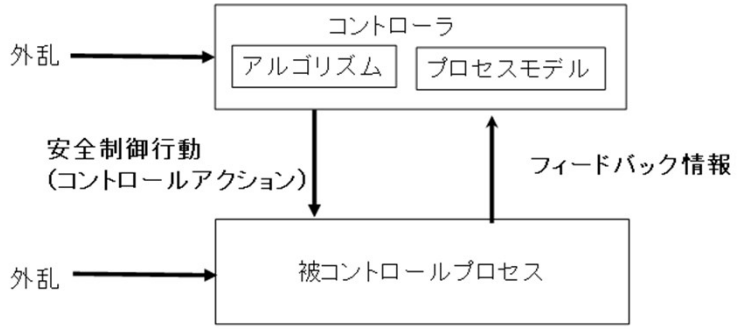


事故の一方向の連鎖進行モデル

◆複雑システムの事故



共通のシステムの事故モデルを介して議論することが有効
⇒**STAMPモデル**

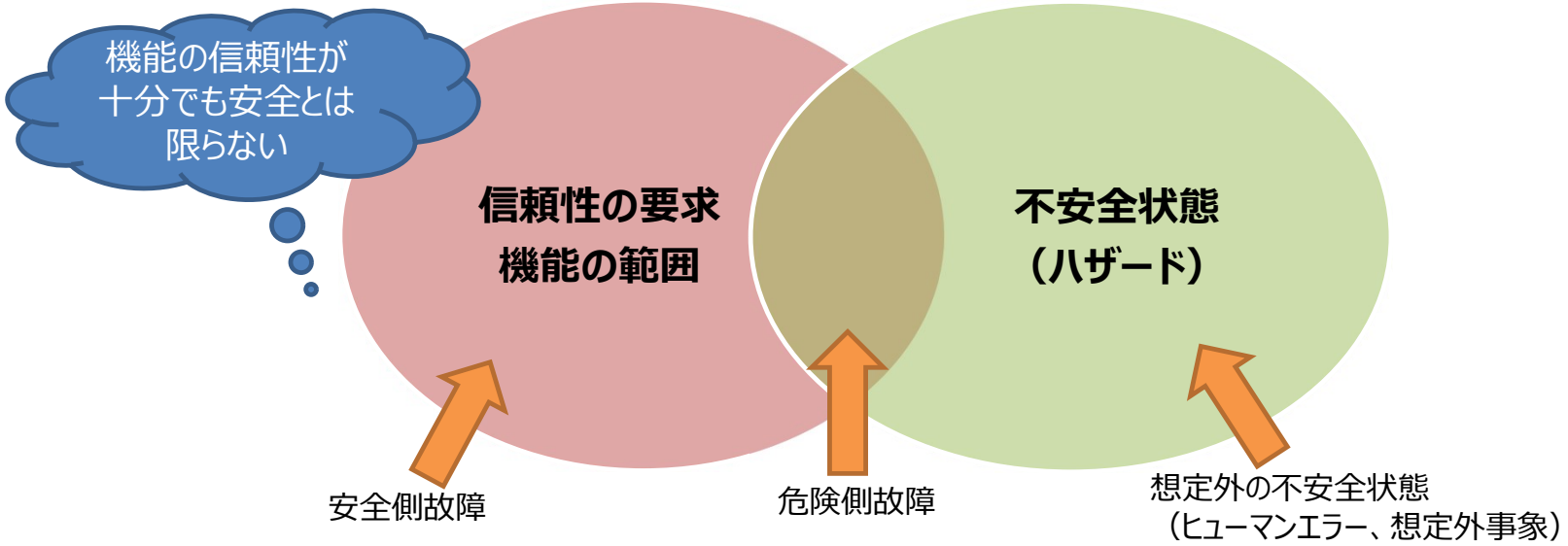


安全の基本概念

＜信頼性と安全性＞

- 信頼性：製品の機能を実現する能力があること
- 安全性：製品の機能とは無関係にリスクが低いこと

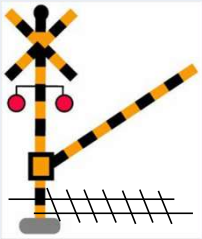
} ともに満たすことが必要



安全側故障　⇒ 機械が壊れても安全が保たれる
危険側故障　⇒ 機械が壊れると安全が保証されない
想定外の不安全状態 ⇒ 機械が正常でも安全が保証されない

安全の基本概念

＜本質安全と機能安全＞

リスクに対する方策	本質安全	機能安全
それぞれの説明	（潜在）危険源そのものを除去する	（潜在）危険源は存在するが、そのリスクを許容できるレベルまで軽減する
【事例】 鉄道と道路の交差部	立体交差化 	踏切システムの設置 
【事例】 自動車	メカ部の強度向上 ソフトウェアのデバッグ メカストッパーの追加 ・・・	冗長化 フェールセーフ 故障診断 ・・・

安全の基本概念

＜機能安全の概念＞

機能による安全

- 危険となる事象から守るための機能を追加し、機能による安全を確保（踏み切りの警報機の例）

機能の安全

- 製品の機能が壊れないこと。
- 万が一故障しても安全が維持できる対策

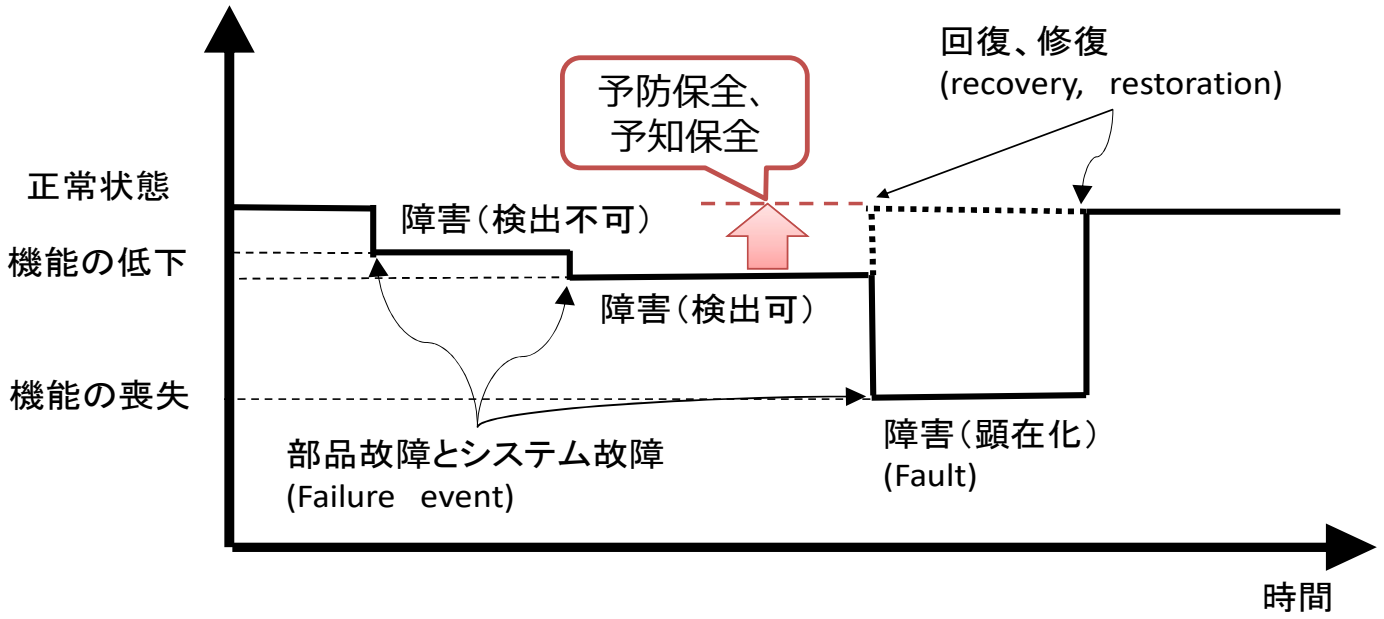
「機能による安全」と「機能の安全」の両方が求められる

安全の基本概念

＜故障と障害＞

故障（Failure）：要求された機能を実行するシステムの能力が停止する（事象）

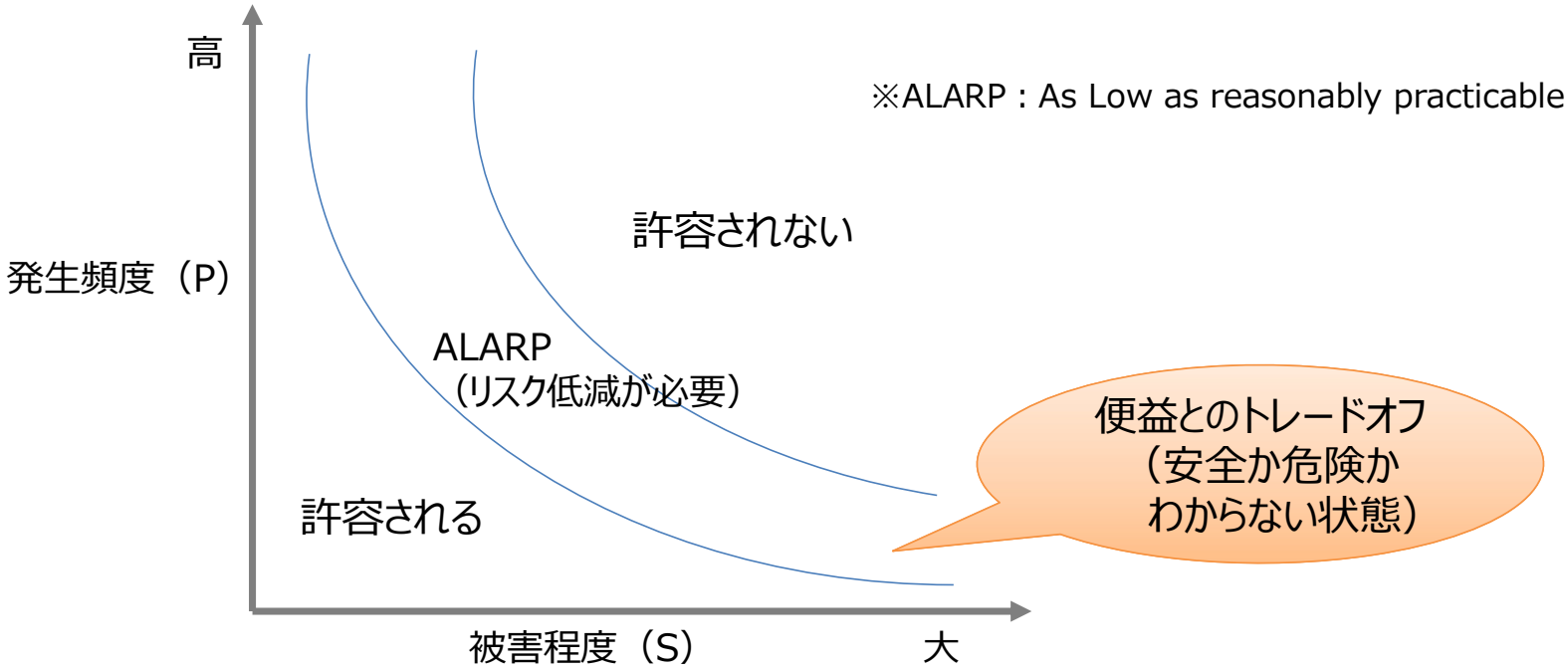
障害（Fault）：システムの故障を引き起こす可能性のある異常な状態



リスクとは

リスクとは危害（ハザード）の**発生頻度**およびその危害の**被害度**の組み合わせ
（ISO/IECガイド51より）

<リスクの程度>



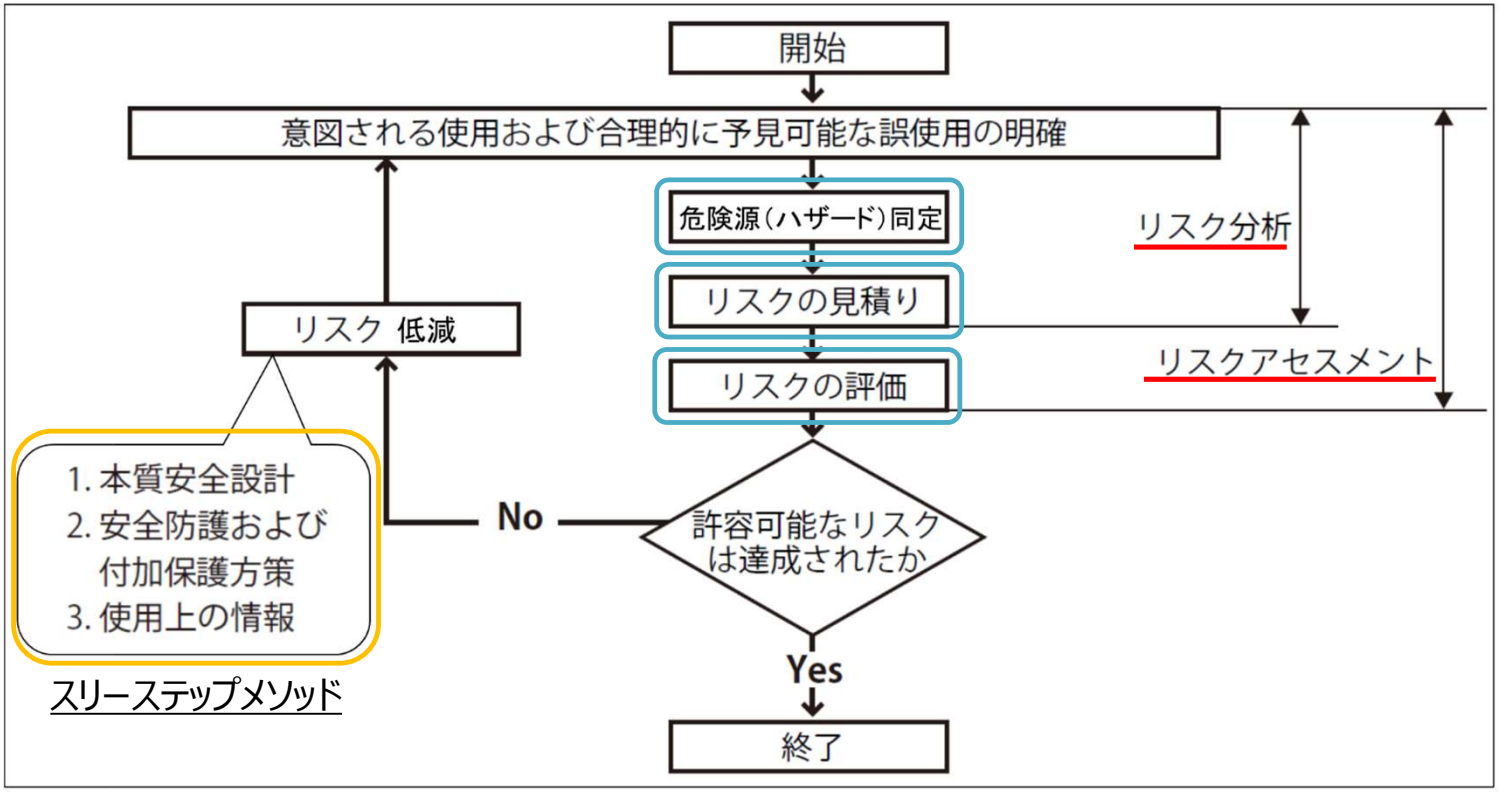
※ALARP：As Low as reasonably practicable

リスク（R）＝ 発生頻度（P）× 被害程度（S）

一般社団法人 組込みシステム技術協会 Japan Embedded Systems Technology Association

リスクアセスメント

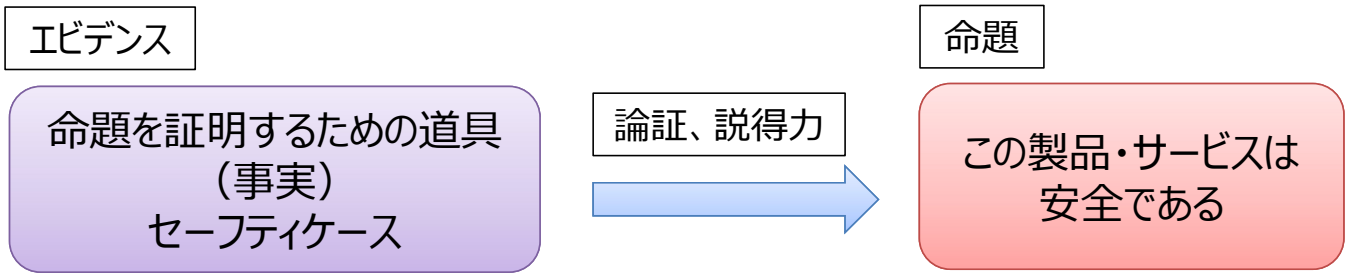
安全な設計を行うためには、危険を分析・評価し、不合理なリスクが存在せずに、リスクを低減するための方策を行う必要があり、最大限実行可能なリスク低減を達成することがリスクアセスメントの目的である。



安全論証（Safety Argument）の考え方

安全論証とは ・・・ システムが許容可能な程度に安全であること、不合理なリスクが無いことを論理的かつ合理的に説明できること（説明責任が果たせること）

※完全な証明(Prove)や絶対安全を保証するものではない

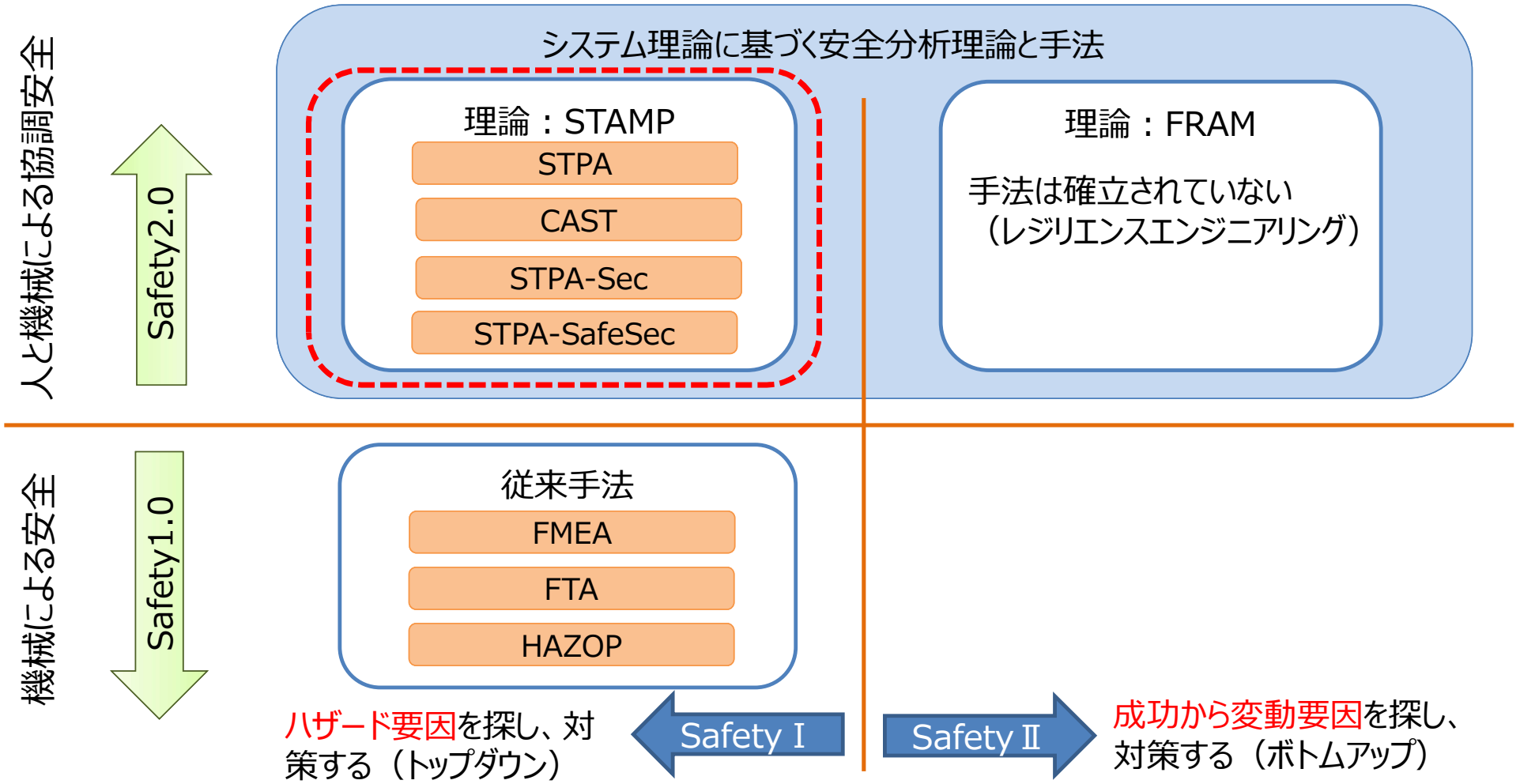


※国際安全規格の要求事項を満たしていることを論証、説明していくことではない

- ソフトウェアがシステムの役割の中心となりつつある昨今、システム毎に安全性の考え方や安全性の達成方法は一律ではない
- 安全論証の必要性は今後も高まる

  ⇒ セキュリティの分野にも取り入れられていく（例：ISO 21434）

安全分析理論と手法



一般社団法人 組込みシステム技術協会 Japan Embedded Systems Technology Association

STAMP/STPAとは

システム全体をみたシステム思考的アプローチ（システムズ理論）に基づく安全分析手法

- STAMP（**S**ystem-**T**heoretic **A**ccident **M**odel and **P**rocess）
  ・・・システムズ理論に基づくアクシデントモデル
- STPA（**S**ystem-**T**heoretic **P**rocess **A**nalysis）
  ・・・STAMPに基づく安全分析手法

※マサチューセッツ工科大学のNancy G.Leveson教授が2012年に提唱
システムを構成する一つ一つのサブシステムやコンポーネントに不具合がなくとも、サブシステムやコンポーネントの組み合わせによって全体のシステムにおいて不具合が発生するシステム全体の制御のやり取りに着目したモデル。

STAMPへの期待

- 従来の安全分析法に代わるということではなく、新しい製品開発に際して、故障に起因しない事故（想定外事故、要求仕様・設計仕様の限界による事故）を防ぐことに役立つかもしれない
- セキュリティに起因する事故を考えるきっかけになるかもしれない
- 要求仕様の論理的妥当性を示す安全論証にも役立つかもしれない

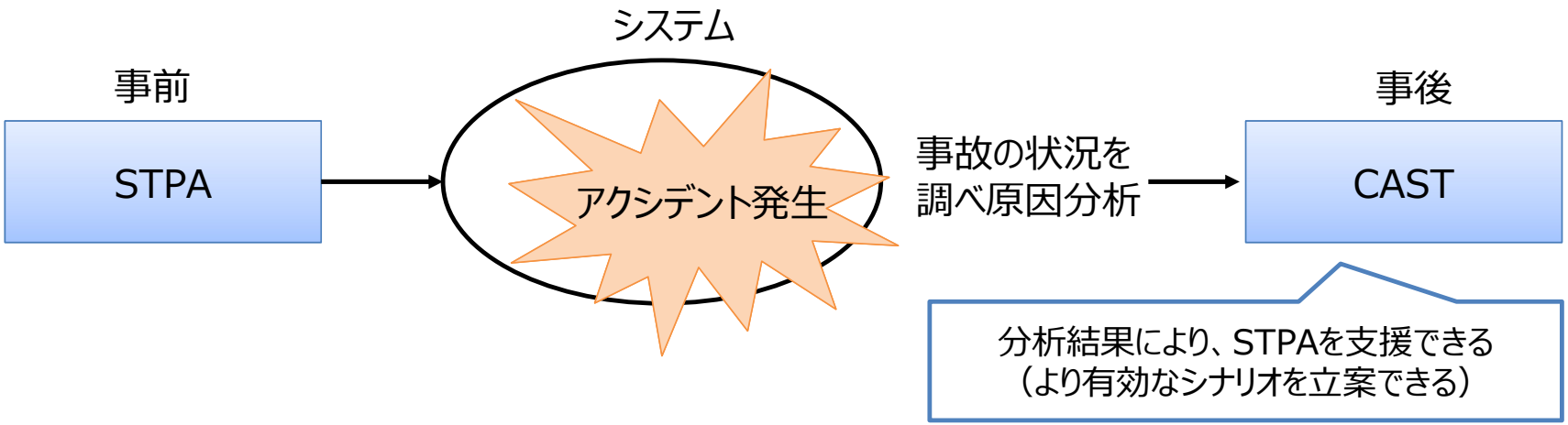
STAMP/CASTとは

【目的】：相互作業によって発生したハザードを分析するため

【特長】：さらなる損失を防ぐ為に排除または管理する必要があるもっともらしいシナリオ（弱点）を識別できる

- 発生した特定のシナリオのみを識別できる
- 安全制御構造の破綻にフォーカスし、先入観や偏見による影響や偏りを小さくする（後知恵の偏り防止）

STPAとCASTの違いは適用のタイミングが異なる



まとめ

リスクアセスメント＝

製品の安全性を高めるノウハウ ＋ **安全であることの説明責任を果たす**

により、成り立っている

- リスクアセスメント手法（安全分析手法）に良し悪しはなく、分析で期待する内容によって適材適所を選択することが大事。
- 安全性向上委員会では世間の最新動向を反映した、現場で必要とされる技術の検討・普及を目指している。

安全設計ガイドの出版

「システム技術に基づく安全設計ガイド」の出版

◆現市場でのソリューションでは・・・

- ✓ 体系化した書籍、文献が極めて少ない
- ✓ 最新規格に対応していない、規格そのままの内容
- ✓ ロボット安全（規格解説）など特定分野の書籍はそもそも存在しない
- ✓ 安価な教育の機会が少ない

「システム技術に基づく安全設計ガイド」を出版

- ✓ 予備知識なく読める初心者にもおススメの内容
- ✓ 現行の国際安全規格を幅広く網羅
- ✓ 豊富な具体事例
- ✓ 規格の裏にある本質的な考え方まで解説
- ✓ AI・IoT時代を見据えた新しい安全分析の概念を解説
- ✓ ソフトウェア技術の重要性を指摘
- ✓ 十分なボリュームと手に取りやすい価格

大幅改訂

10年間の環境変化
（IEC61508からAI/IoT時代の安全性へ）

（¥2,700+税）

一般社団法人 組込みシステム技術協会
Japan Embedded Systems Technology Association

システム技術に基づく安全設計ガイドの構成

本書の構成

安全の基本

第1章「安全の基本」
安全の基本、安全設計の原理、安全論証の考え方、安全設計の基本戦略

第2章「安全規格体系と概要」
安全規格と標準化、基本規格である

第3章「リスクアセスメント」
ISO / IEC Guide 51, ISO 12100

現状の規格

第4章「機械系安全規格から見た安全設計の基本」
ISO 13849 機械類の制御システムの安全関連部

第5章「機能安全設計の基本」
IEC 61508 E/E/PE安全関連系の機能安全

第6章「自動車の機能安全」
ISO 26262

第7章「生活支援ロボットの安全規格」
ISO 13482

今後の安全

第8章「システム思考で考えるこれからの安全/STAMP」
システム理論に基づく安全分析手法（STAMP/STPA）について、背景にあるシステム思考の考え方、分析手順をいくつかの具体例を通して解説

第9章「ソフトウェアエンジニアのための安全設計」
システム理論に基づく安全分析手法(1)ウォーターフォールとアジャイル開発プロセス、(2)モデルベース開発、(3)モデル検査、(4)コーディングガイド、(5)ソフトウェアFMEA

【安全性向上委員会】
2022年9月28日 発行

発行者　一般社団法人 組込みシステム技術協会
東京都中央区日本橋大伝馬町6-7
TEL: 03(5643)0211、 FAX: 03(5643)0212
URL: http://www.jasa.or.jp/