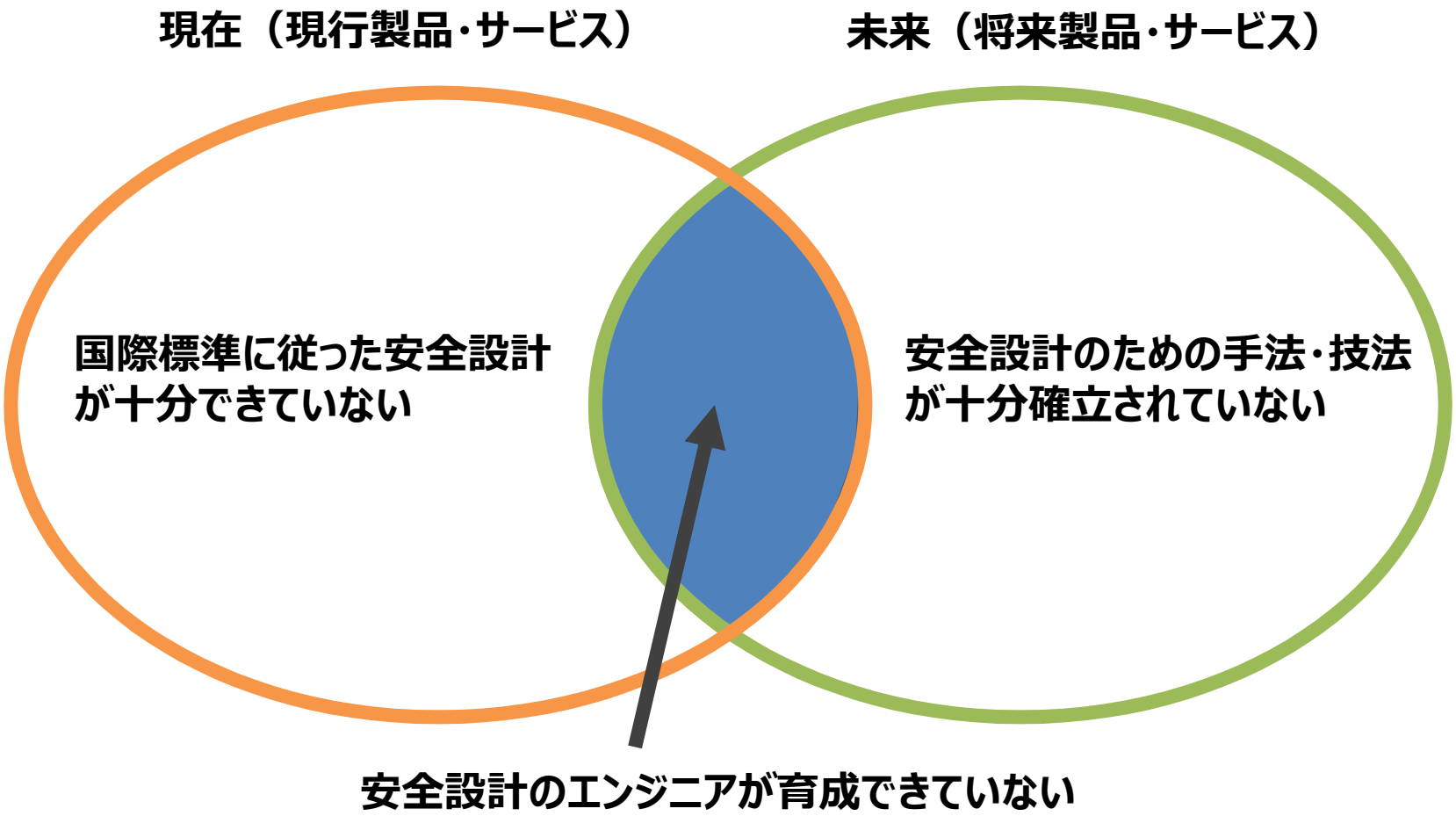
（JASA安全仕様化WG）
AI･IoT時代を見据えた
セーフティ設計技術の知見を体系化する取組み

2019年6月13日~14日

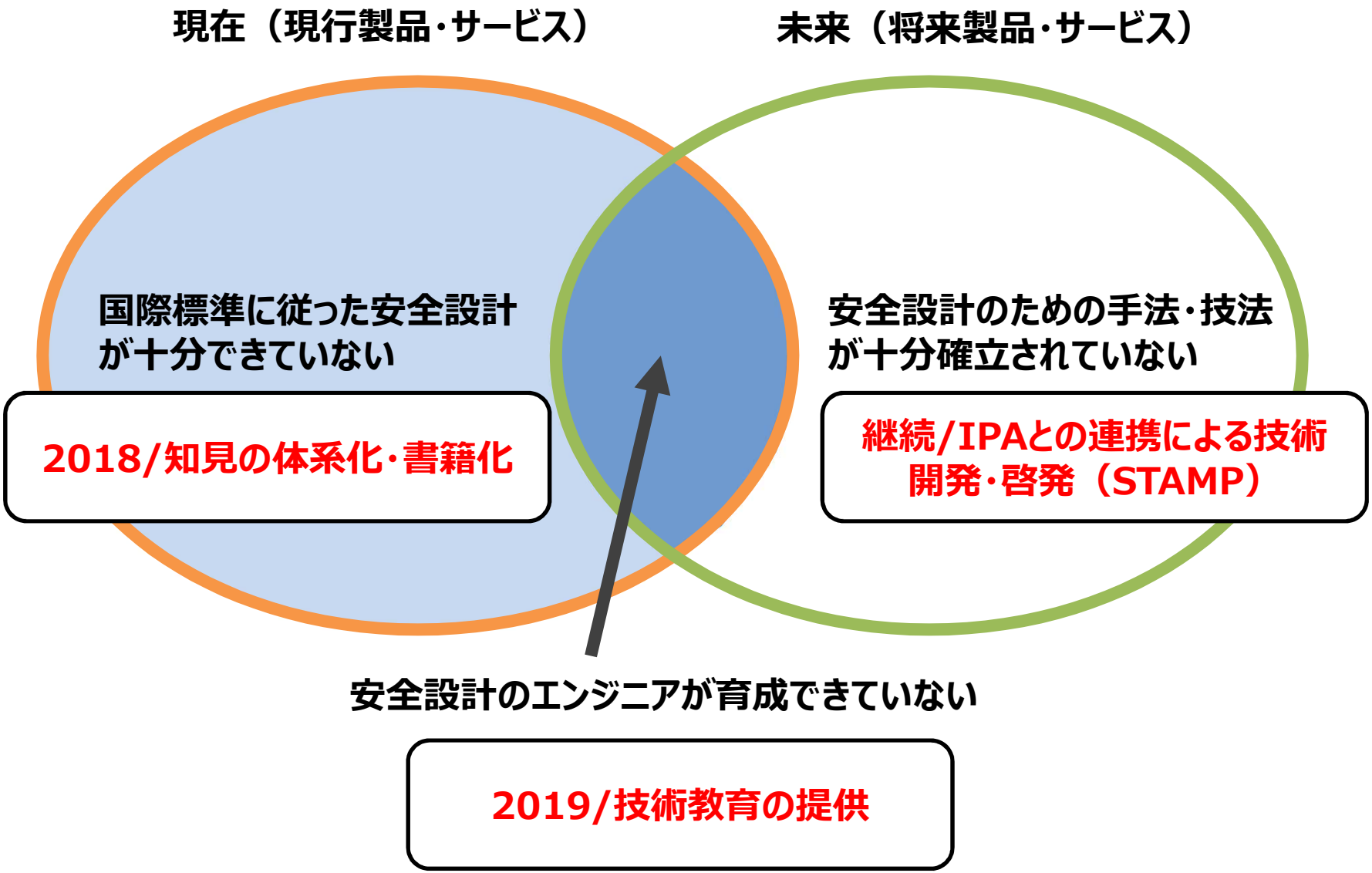
株式会社東芝　余宮尚志
hisashi.yomiya@toshiba.co.jp

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

AI・IoT時代における安全設計の主な課題



JASA安全仕様化WGのアプローチ



知見とは

- 「実際に見て知ること。また、見聞きして得た知識」
- 「知識によって得た見解」

  （国語辞書 - 大辞泉）

- JASA安全仕様化WGの思い･･･単なる知識ではなく、知識のある専門家による経験や議論に基づく解釈を体系化すること

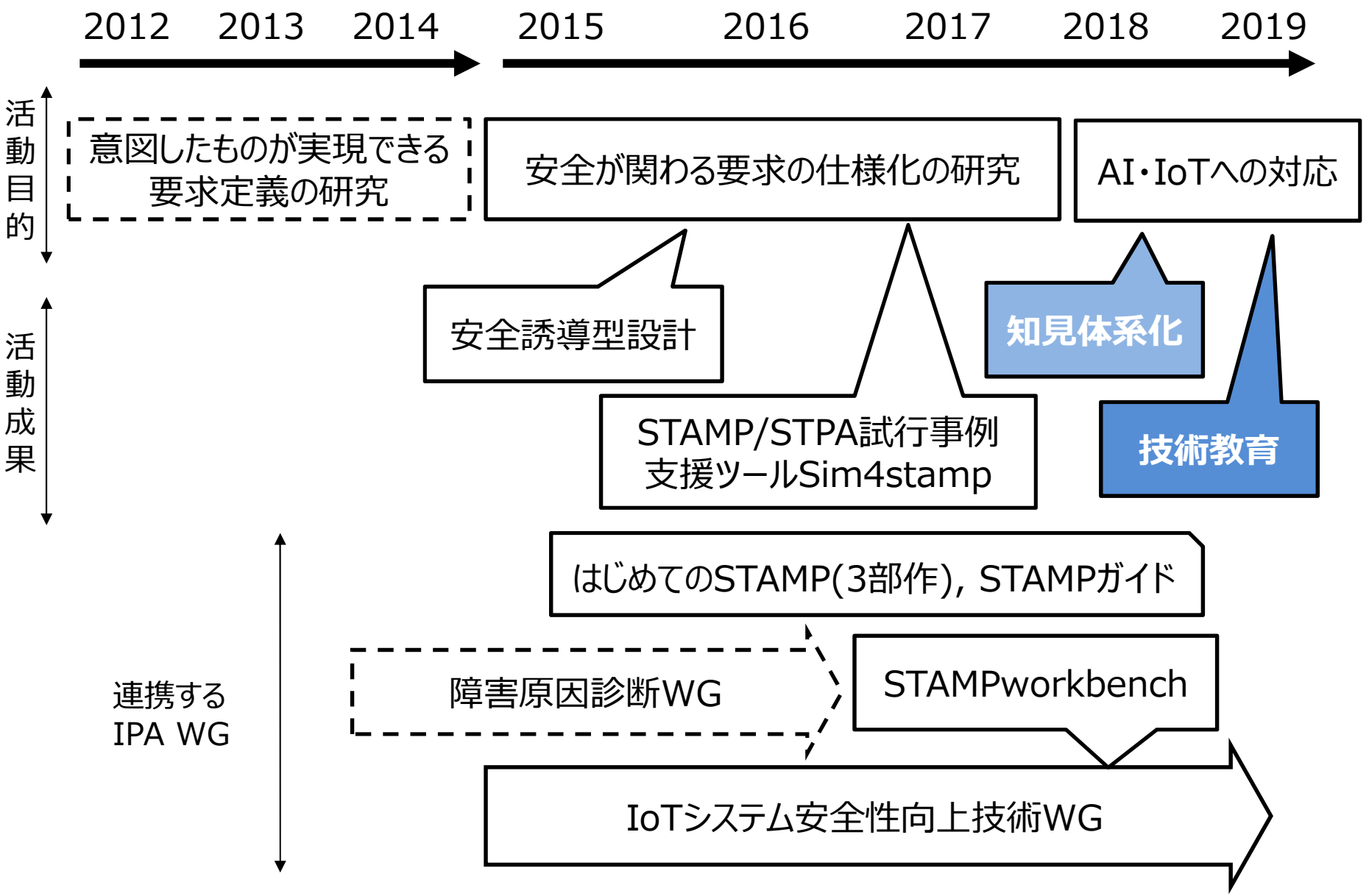
発表内容

1. JASA安全仕様化WGの活動紹介
2. 知見の体系化・書籍化の取組み
3. 書籍の一部紹介
    - リスク低減とリスク見積りの考え方
    - ソフトウェアのリスク分析(FMEA)の考え方
    - STAMP/STPAの考え方
4. まとめ

JASA安全仕様化WGの活動紹介

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

活動推移


2012
2013
2014
2015
2016
2017
2018
2019
活動目的
活動成果
意図したものが実現できる要求定義の研究
安全が関わる要求の仕様化の研究
AI・IoTへの対応
安全誘導型設計
STAMP/STPA試行事例
支援ツールSim4stamp
知見体系化
技術教育
はじめてのSTAMP(3部作), STAMPガイド
連携する
IPA WG
障害原因診断WG
STAMPworkbench
IoTシステム安全性向上技術WG

2018年度活動紹介

① 知見の体系化・書籍化

本日の主な発表

② IPA連携によるSTAMP/STPAの事例開発、啓発

③ ET(WEST, 横浜, 名古屋)での講演

④ ET(横浜)でのパネル展示

⑤ Sim4stamp(STAMPシミュレータ)の改良

②IPA連携によるSTAMP/STPA事例開発・啓発

		2015	2016	2017	2018
成果物	目標	知る •STAMP紹介、基本的手法解説 •既存設計手法との連携解説	分かる •STAMP事例解説、適用ノウハウ紹介 •システム俯瞰の必要性を警告	できる •STAMP事例解説、場面に応じた解説 •新技術:FRAM, Safety2.0解説	定着 •有効な活用方法と、効果的な事例紹介 •新技術:Securityとレジリエンス
	結果	はじめてのSTAMP入門編 10,229ダウンロード	はじめてのSTAMP実践編 2,171ダウンロード	はじめてのSTAMP活用編 2,750ダウンロード	STAMPガイドブック ツールダウンロード2,100件
			ツール仕様検討	ツール開発	ツール公開
普及活動	目標	STAMP認知度向上	STAMP認知度向上	STAMP認知度向上	STAMP認知度向上 理解度向上
	結果	ETにて紹介 ETWestにて紹介	ETにて紹介 ETWestにて紹介	ETにて紹介 ETWestにて紹介 ET名古屋にて紹介	ETWestにて紹介 ET出展せず ET名古屋出展せず
			第1回STMP-WS 参加者：**117名**	第2回STAMP-WS 参加者：**180名**	第3回STAMP-WS 参加者：**280名**

STAMPはAI・IoTを見据えた次世代の新しい安全分析手法
6名の安全仕様化WGメンバがIPA委員として連携活動
技術の確実な開発・定着・啓発が進んだ

③ET横浜での講演

JG-1

11月14日（水）13:30-14:30
会議センター［211＋212］

システムズ理論によるソフトウェアの安全設計・現状と今後

自動車、列車、ロボットからプラントまで現在の工学システムはソフトウェアで安全が保たれており、そのソフトウェアはますます複雑化している。現状の安全設計法や安全規格の限界も見えており、システムズ理論による新しい安全解析法STAMP/STPAにも注目が集まっている。本講演では、ソフトウェア集約型のシステムの安全設計に焦点を当てて、その現状と今後の動向を紹介する。

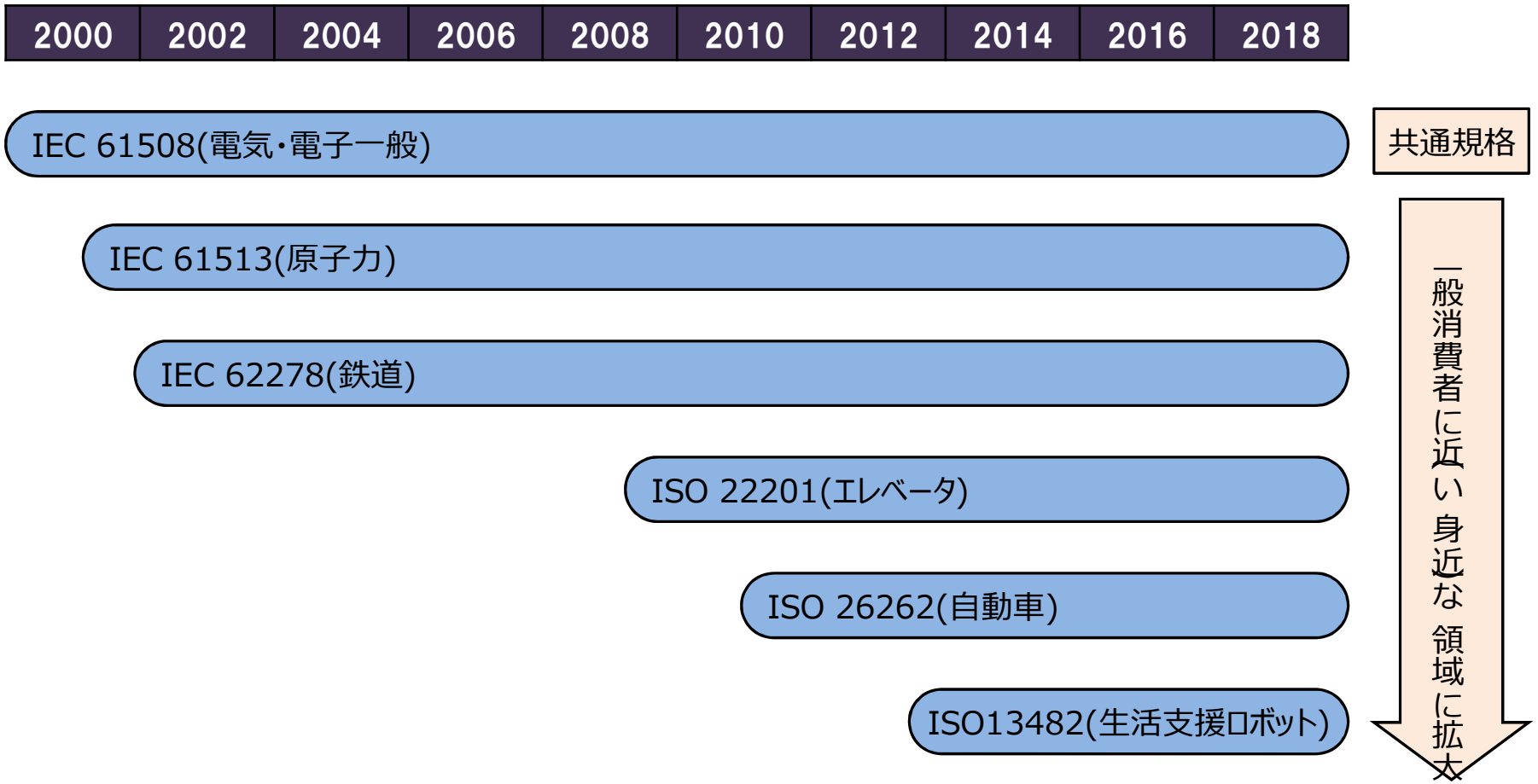
知見の体系化・書籍化で進めている内容と、STAMP解説を講演
130名の講演申込み、実聴講者80名以上と盛況

知見の体系化・書籍化の取組み

(課題と動機～取組み詳細・成果)

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

セーフティの重要性：機能安全規格の広がり



国際標準に従った安全設計が急務となっている

自動車業界におけるセーフティ：技術範囲の広がり

2010	2012	2014	2016	2018	2020	2022

ISO 26262:2011

ISO 26262:2018（第二版）

SOTIF※

ISO 21434

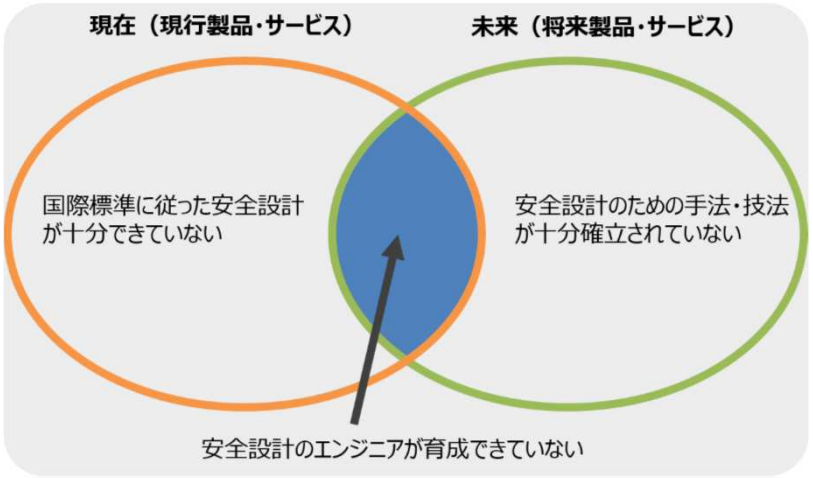
サイバーセキュリティや自動運転に拡大

※SOTIF（Safety Of The Intended Functionality）

AI・IoT時代で「安全設計の範囲」が広がってきている

セーフティ設計技術を取り巻く環境と課題

- 現在
  - システムの大規模化・複雑化
  - **国際標準に従った安全設計**
- 未来
  - AI・IoT時代の到来
  - より大規模化・複雑化するシステム・ソフトウェア
  - 国際安全規格の限界、及びその対応
  - 体験したことのない未知の製品・サービスでの危険・脅威増
- 現在～未来　共通
  - **エンジニア不足、スキル不足**
  - **安価な技術習得機会がない**（たとえば、中小企業での対応が難しい）



課題に対する現市場でのソリューション

- 情報源
  - 体系化した書籍、文献が極めて少ない
  - 数少ない書籍は、専門家向けではない
  - 最新規格に対応していない、規格そのままの内容(単なる知識)
  - 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

- 教育の機会
  - 教育自体が少なく、少し不親切で、かなり高額である

JASA安全仕様化WGの2018年度の成果

- (既存の)知見を体系化
- 電波新聞社さまに趣旨・内容に共感頂き書籍化を実現
- 「**システム技術に基づく安全設計ガイド**」
  （2019年9月上旬に発売予定）

Why in JASA ?

「会員企業の積極的な参加により一企業では難しいさまざまな課題に取り組んでいます。」…JASAのHPより

JASAの取組む「人材育成」にも非常に関連性が強い

⇒ **会員企業様にも喜んで頂けると考えました**

「書籍:安全設計ガイド」の特色

- **予備知識なく**読める内容
- 現行の**国際安全規格を幅広く**網羅
- 各分野の専門家による解説
- 豊富な具体事例

企業の実務家、大学教員
など日本を代表する専門家
8名が執筆に参加

- 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も解説
- **ソフトウェア技術**の重要性を指摘(豊富なソフトウェア安全設計の技術解説)

- 十分なボリュームと手に取りやすい価格

260ページ前後、2,600円(予価)

「書籍:安全設計ガイド」の紹介　1/4

- 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を解説

- 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ISO/IEC Guide 51やISO 12100の解説。規格の適用範囲や規格の限界にも言及

- 第3章「**リスクアセスメント**」

  リスクアセスメントの原理原則、プロセスを解説。FMEA, FTA, HAZOPなど既存の安全分析手法の紹介と豊富な事例

国際安全規格の体系「ISO/IEC Guide 51」

- ISOとIECが共同で策定した「ISO/IEC Guide 51」（第2章）では、安全規格の階層構造や、基本的な用語が定義されている

規格の種類	ISO/IEC規格
基本安全規格 （タイプA規格）	• ISO 12100 • ISO 14121
グループ安全規格 （タイプB規格）	• IEC 61508 • ISO 13849 • IEC 60204 など
製品安全規格 （タイプC規格）	• ISO 26262 • ISO 13482 • IEC 60745 など

（第3章）リスクアセスメントの原則

（第5章）コンピュータ

（第6章）自動車の電子制御系

（第7章）生活支援ロボット

ISO/IEC Guide 51が定める安全規格の階層構造

「書籍:安全設計ガイド」の紹介　2/4

- 第4章「**機械系安全規格から見た安全設計の基本**」
  機械系安全規格ISO 13849に基づいたリスク低減方策として、3ステップメソッドを中心に解説（旧版のみに対応）

- 第5章「**機能安全設計の基本/IEC 61508**」
  電気・電子・プログラマブル電子の機能安全規格IEC 61508の要求事項に基づいて、安全関連系の設計・開発方法について解説
  IEC 61508:2010に対応

- 第6章「**自動車の機能安全/ISO 26262**」
  自動車の機能安全規格ISO 26262について、規格の概略や全体構成、安全ライフサイクル、規格の主要なパートにおける考え方を中心に解説
  ISO 26262:2018に対応

「書籍:安全設計ガイド」の紹介　3/4

- 第7章「**生活支援ロボットの安全規格/ISO 13482**」

  生活支援ロボットの安全規格であるISO 13482について、規格の構成や安全設計の流れについて、簡単な事例を用いながら、概略を説明

  ISO 13482:2014に対応

- 第8章「**システム思考で考えるこれからの安全**」

  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

「書籍:安全設計ガイド」の紹介　4/4

- 第9章「**ソフトウェアエンジニアのための安全設計**」

  安全設計で近年重要度を増すソフトウェアについて、(1)ウォータ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という5つの要素技術を解説

- 豊富なコラム
  - ディペンダビリティと安全性
  - リスク管理
  - ハードウェア故障とソフトウェア故障
  - サイバーセキュリティと安全
  - 性能限界や誤操作、誤使用をカバーする規格―SOTIF
  - ソフトウェア障害発生に関する課題 etc

10以上の豊富なコラムで、周辺技術、最新トピックスを網羅

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

書籍の一部紹介

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

トピックス(1)

リスク低減とリスク見積りの考え方

資料をご希望の方には、ご連絡くだされればメールで送付させて頂きます。

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

トピックス(2)

ソフトウェアのリスク分析(FMEA)の考え方

資料をご希望の方には、ご連絡くだされればメールで送付させて頂きます。

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

トピックス(3)

STAMP/STPAの考え方

資料をご希望の方には、ご連絡くだされればメールで送付させて頂きます。

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

まとめ

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

まとめと、今後のWG活動計画

- まとめ
  - AI・IoT時代のセーフティ設計技術に前提となる知見の体系化・書籍化を進めてきた(2019年9月に書籍発売決定)
  - 外部への情報発信、及びAI・IoT時代におけるコア技術の開発・啓発をIPAと連携して取り組んできた
  - 書籍の中から技術トピックスをいくつか紹介した

- JASA安全仕様化WGの2019年度からの活動計画
  - 技術教育を提供
  - コア技術の調査・開発・普及を促進(継続)
  - AIのセーフティ設計技術、情報セキュリティと協調するセーフティ設計技術の研究