

ISO26262「**確証方策**」の より**効率的な実施の取り組み**

～組織・プロジェクトの特性に応じた
フレキシブルな実施を目指して～

菅沼由美子

パナソニック株式会社

オートモーティブ&インダストリアルシステムズ社

技術本部 プラットフォーム開発センター

システム技術開発部 機能安全推進課

目次

1. 背景
2. 課題&改善方針
3. 改善の取組
4. まとめ

車載分野の機能安全

車載分野では機能安全（ISO26262）への対応が必要

用語	説明
機能安全	安全に対するリスクを、安全方策により許容可能な範囲内に抑えるという考え方で、本質安全とは異なる概念
ISO26262	車載E&Eにおける機能安全の規格
ASIL	ISO26262で用いる安全度水準で、ASIL A,B,C,Dの順に高くなる（なお、ASILA未満のQMは一般的な品質管理を意味する）
確証方策	ISO26262 Part2で要求される3つの活動で、実施者に対し、ASILに応じた第三者性の要求がある

3つの確証方策

これらの第三者による確認活動が必要になった

	確証レビュー	機能安全監査	機能安全 アセスメント
評価対象	作業成果物 (表1に規定あり)	機能安全に要求 されているプロセ スの実施	対象のアイテム
責任	作業成果物の ISO 26262要 求への 準拠性 の 評価	要求される プロセ スの実装 の評価	達成された機能 安全 の評価
実施 タイミング	活動完了後 生産リリースまで	プロセスの実施中	順次or一括 生産リリースまで

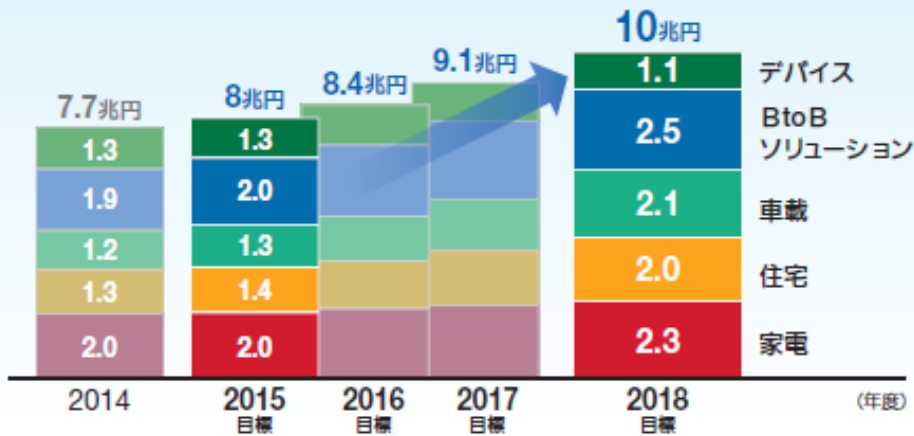
※ISO26262 Part2 表2 より

パナソニックの車載事業

http://www.panasonic.com/jp/corporate/ir/pdf/panasonic_ar2015_j.pdf

Annual Report より

2018年度売上高10兆円に向けて



先進の自動車用デバイスで 交通事故の防止に貢献

交通事故防止に大きな効果を発揮する「先進運転支援システム (ADAS)」の普及が急速に進んでいます。日本や欧米などの先進諸国では、すでに新車の多くに自動ブレーキなどの安全技術が搭載されはじめています。

こうしたニーズの高まりを受け、パナソニックはグローバルトップシェアを誇る「カメラモジュール」や、車両周辺の障害物を検知する「バック&コーナーセンサ」、車体の傾きなどを検知する「角速度センサ」などのデバイスと、画像処理技術や通信技術を駆使した電子制御ユニット (ECU) の連携によってドライバーの「認知・判断」をサポートするシステムの提案を拡大しています。

さらなる技術進化を目指し2014年4月には「ADAS開発センター」を新設。各種デバイスや画像関連技術など全社の知見を結集した研究開発を加速しており、すでに「後方接近物検知システム」「緊急ブレーキシステム」などを開発・受注。今後も自動車メーカーと新技術の共同開発を進め、社会課題の解決に貢献するとともにADAS分野での事業拡大を目指していきます。

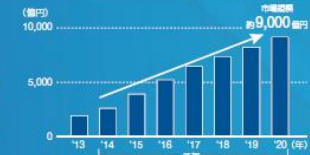


安全を支えるセンサ群・ECU

先端技術を駆使したカメラモジュールや各種センサと電子制御ユニット (ECU) が連携することで危険運転や障害物を自動的に検知、事故や衝突を未然に回避するシステムを実現しています。

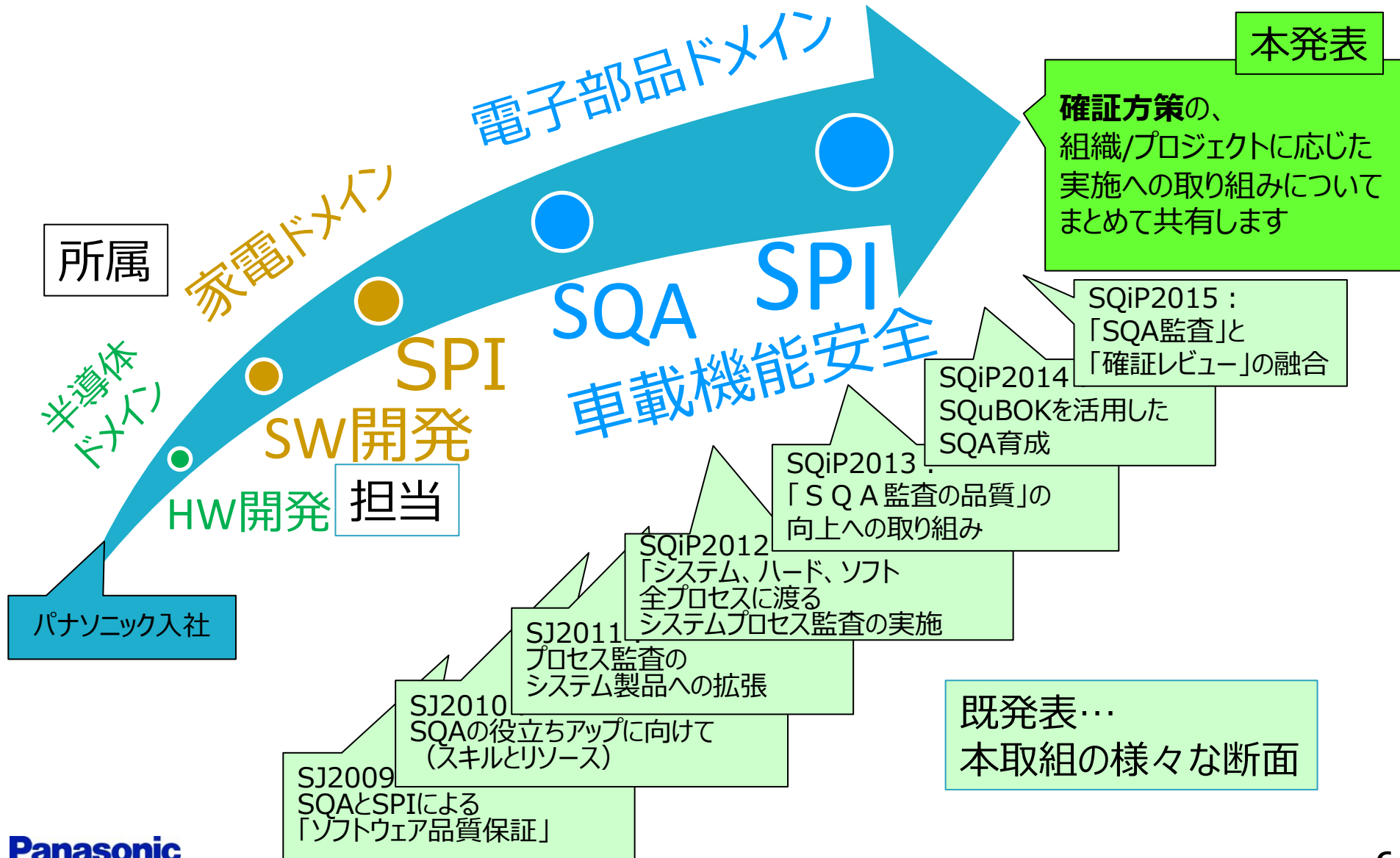
ADAS用キーデバイス/コンポーネント市場

世界のADAS用キーデバイス/コンポーネント市場は、2014年には前年比40%以上と大きく拡大。欧州ではすでに新車の安全評価項目にADASが加えられ、日本・米国でも追加が検討されていることから、今後も年平均25%の成長が続き、2020年には9,000億円規模にまで拡大すると予想されています。



出典：矢野経済研究所「先進運転支援システム (ADAS) 用キーデバイス/コンポーネント世界市場に関する調査結果2014」

私のこと…業務と関心



目次

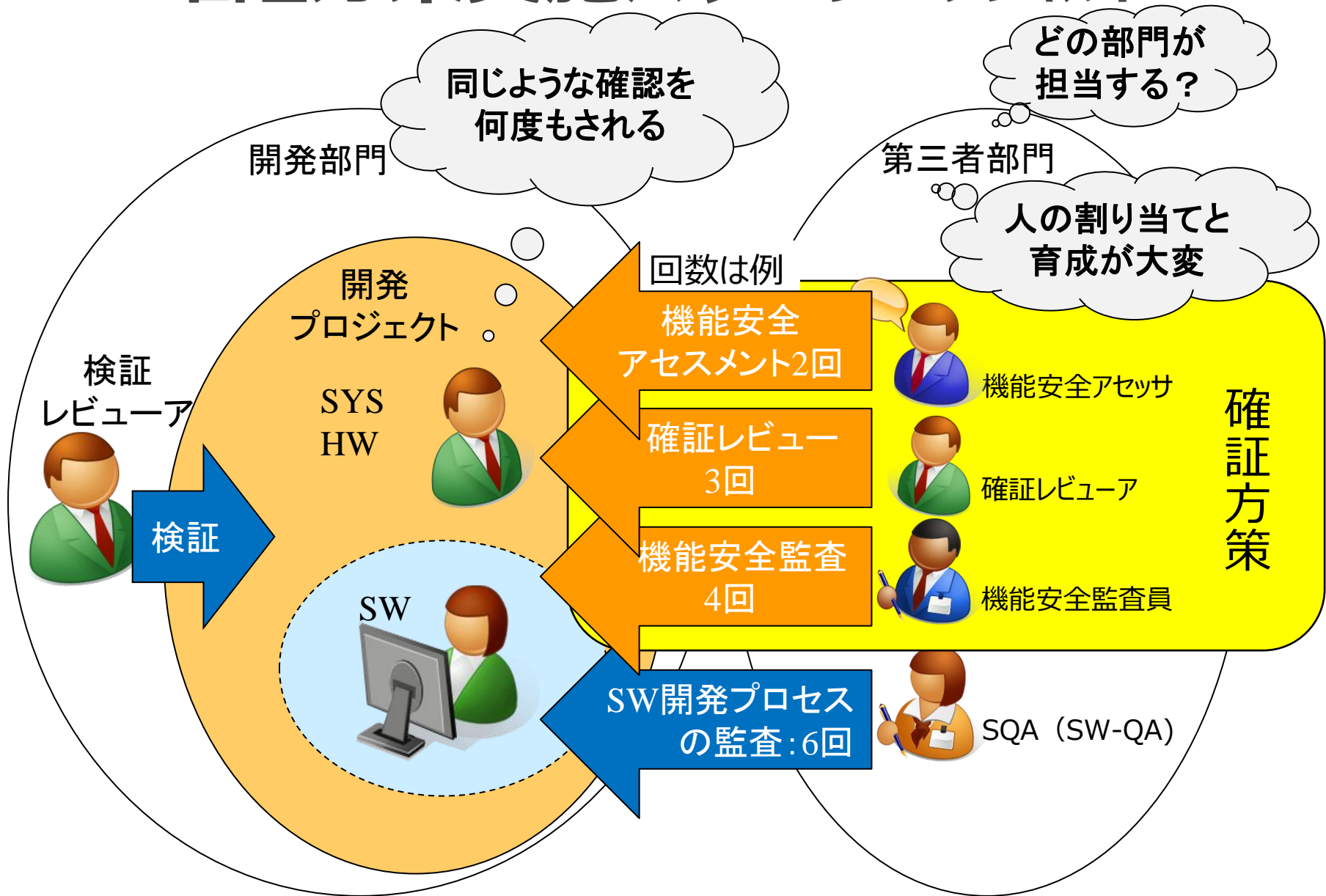
1. 背景

2. 課題&改善方針

3. 改善の取組

4. まとめ

確証方策実施パターン：デフォルト



課題

■ プロジェクトにとって

- イベント増加による対応工数
 - 特に小規模短期プロジェクトには負担が大きい

■ 組織にとって

- 確証方策担当者のリソース、スキル
 - 第三者性（ISO26262要求）の要求あり

■ ⇒ サプライアとして

- ISO26262要求である確証方策を確実に実施したい
- しかし、プロジェクトや組織の負担は最低限に抑えたい
 - プロジェクトや組織によって負担感の重さは異なる

効率化が必要

改善の方針

目的

確証方策実施の
効率化

目標

組織/プロジェクトに応じた、確証方策の
効率的実施方法の選択肢の構築

- 目的：確証方策の効率的な実施
- 目標：組織/プロジェクトに応じた実施方法の選択肢を構築する
 - 対象…パナAIS社各組織での車載開発プロジェクト
 - 小規模開発～大規模開発
 - ASIL低～ASIL高
- 取組の切り口（できることから順次やっていく）
 - イベントの統合
 - 視点の整理

切り口と狙い

■ イベントの統合

■ 狙い：プロジェクトの負担を減らす

実施パターン	SQA監査回数	機能安全監査 想定回数	確証レビュー 想定回数	機能安全アセスメント 想定回数	イベント回数計
デフォルト	6回	4回	3回	2回	15回
取組①	6回		3回	2回	11回
取組②	6回			2回	8回

- ・回数が削減できるのは明らか
- ・改善のポイントは「無理なく統合できるか」→ 前提：プロセス構築

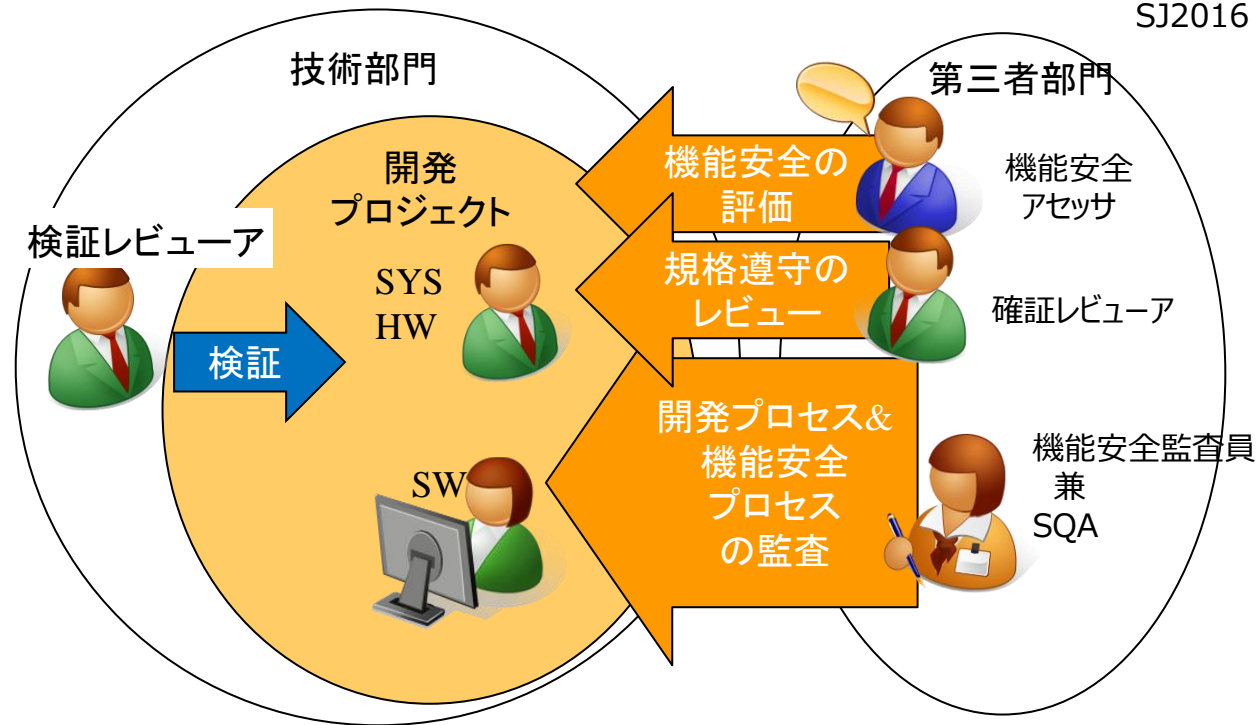
■ 視点の整理

■ 狙い：実施する第三者の負担を減らす

- ・必要な視点はなに？
- ・改善のポイントは「同時に見るメリット/分けて見るメリット」の考察

目次

1. 背景
2. 課題&改善方針
- 3. 改善の取組**
4. まとめ



取組① SQA監査と機能安全監査の統合

取組① SQA監査と機能安全監査の統合

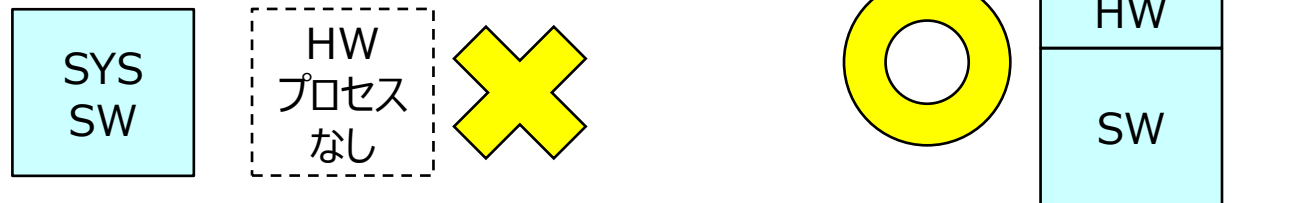
■ 準備…プロセス拡張

■ 目的：

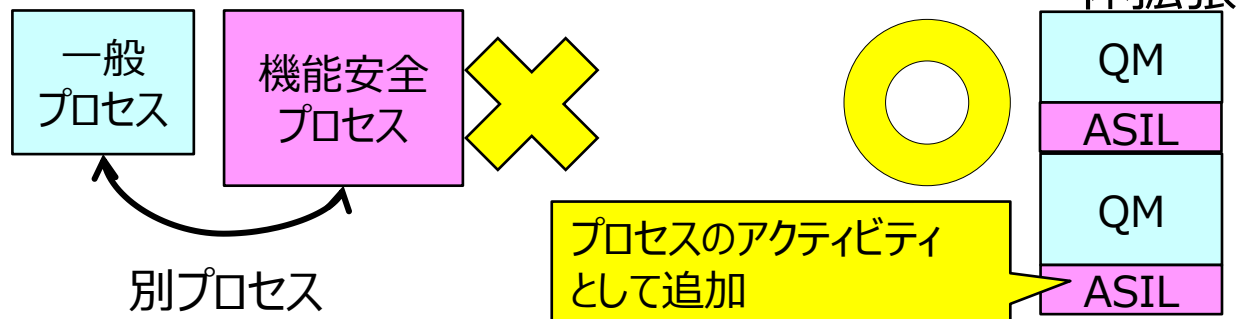
- イベントを無理なく統合できるようにプロセスを拡張する

■ 実施内容：

- HWへのプロセス拡張と監査の仕組み



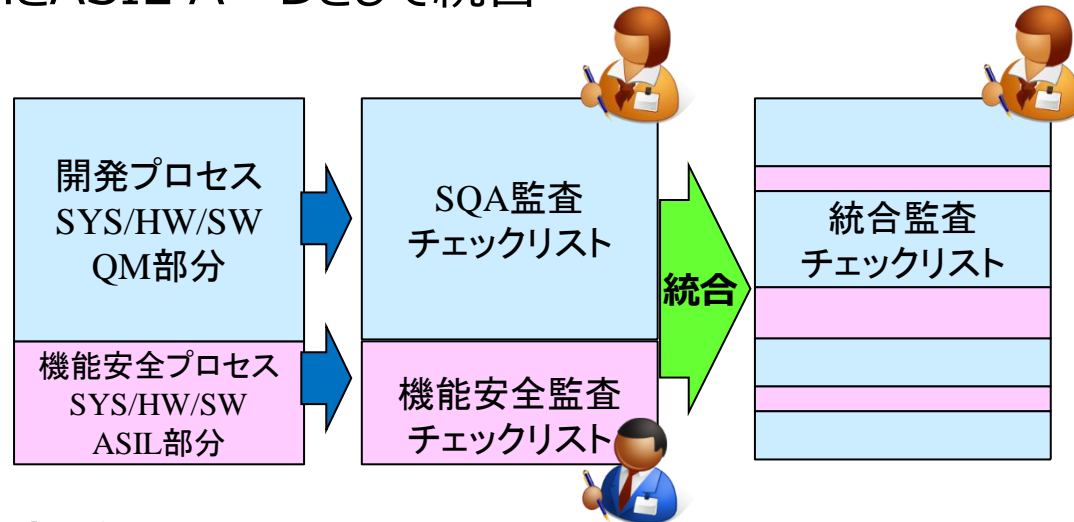
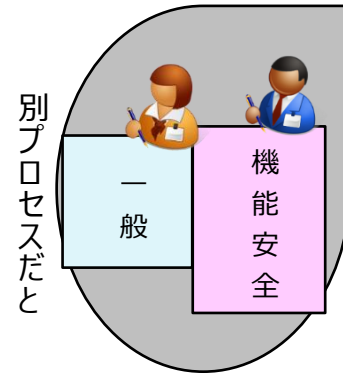
- QMからASILプロセスへの一体拡張



取組① SQA監査と機能安全監査の統合

■ 実施事項

- SQA監査と機能安全監査のチェックリストを統合
 - 通常のSQA監査は、機能安全的にはQMに相当
 - ⇒QMとASIL A～Dとして統合



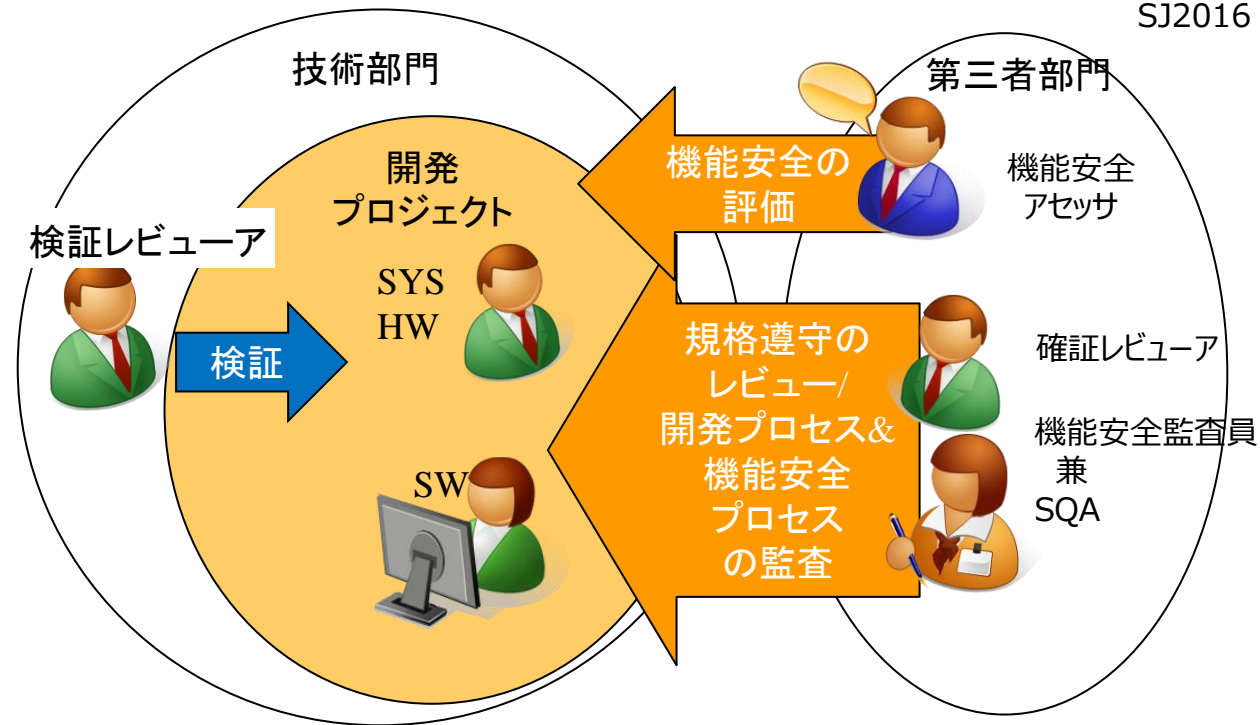
■ リスクと軽減策

- 監査員のスキル
 - SQA教育 + 機能安全教育
 - …監査担当は技術部門による機能安全教育を受講

取組① SQA監査と機能安全監査の統合

■ 評価

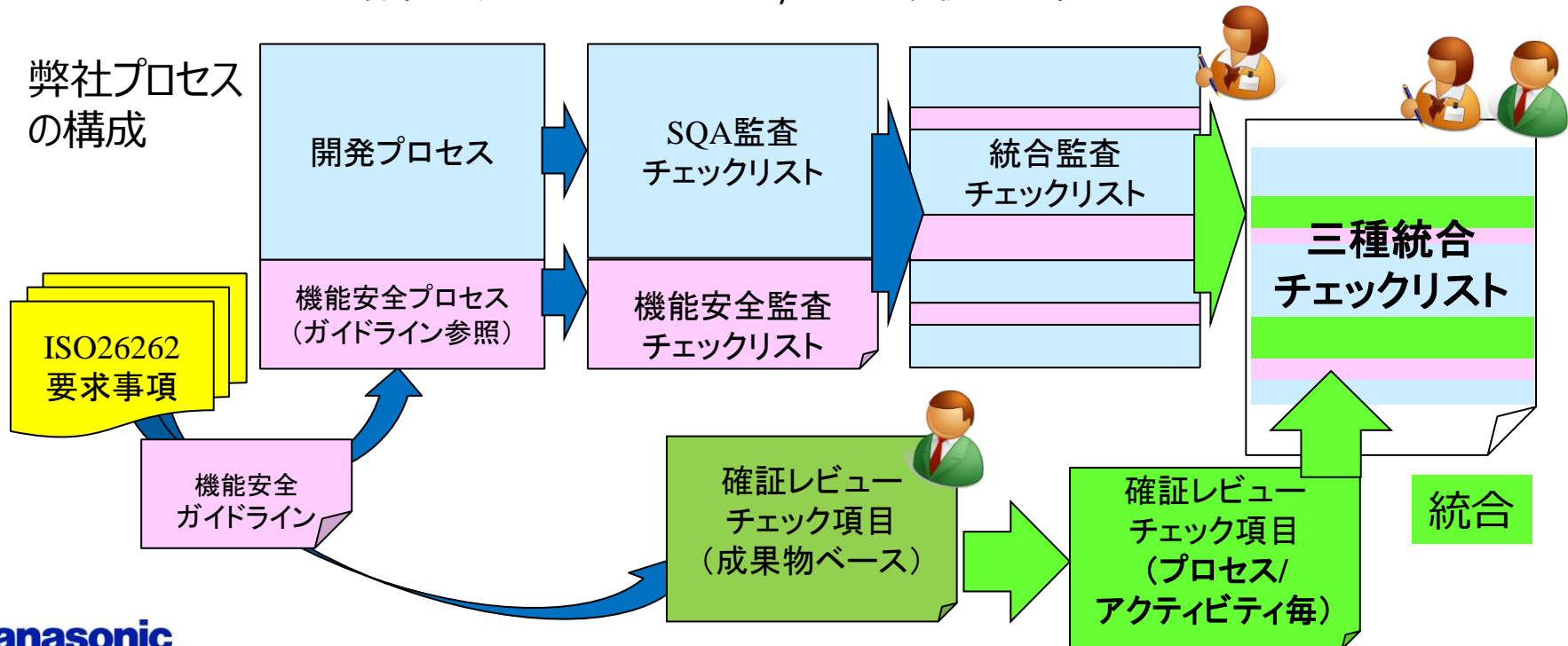
- 想定した効果あり（プロジェクトのイベント回数減）
- + プロジェクト開始後のASIL変更への監査対応も容易
 - ASIL（顧客要求）の確定が遅れるプロジェクトがある
 - 本方式なら、確認項目の増減のみで、監査対応可能
- + 統合により、効率的な監査が可能
 - トータル監査時間減…両監査のまとめで、確認のダブリも減った



取組② 確認レビューと機能安全監査の統合

取組② 確証レビューと機能安全監査の統合

- 背景…取組①を実施後に、更なる統合に取り組んだ
- 実施事項
 - **プロセス確認**
 - 機能安全監査チェックリストと確証レビューチェックリストを統合
 - **成果物確認**
- リスクと軽減策
 - 確認視点が漏れる→確証レビューと機能安全監査員が同時参加
 - イベント数削減が目的なので、監査/レビュー実施者は削減しなくてもよとする

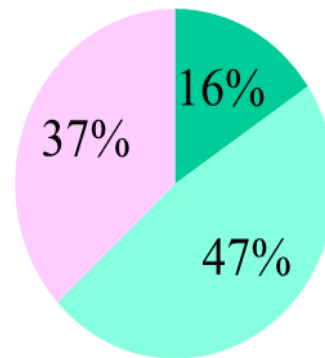


取組② 確証レビューと機能安全監査の統合

■ 評価

- 想定した効果あり（プロジェクトのイベント回数減）
- + 監査と確証レビューのチェック項目のダブリが削減
（機能安全監査チェック項目の63%）

機能安全監査
チェック項目の内訳



- 確証レビュー項目と同じ
- 確証レビュー項目を参照可能
- 監査項目が単体で存在

- + 確認項目の関連付けの効果
 - ⇒ 確証レビューと機能安全監査を別に行う場合にも、項目がダブらないよう分担可能

成果物ごとに、
確証レビューと機能安全監査の
視点を、再度明確にして
視点のダブりをなくす

取組③視点ごとに確認イベントを整理

取組③視点ごとに確認イベントを整理

■ 準備 …再度、規格の解釈を行う

項目	機能安全 監査	確証レビュー	機能安全 アセスメント
対象	機能安全に要求されているプロセスの実施	作業成果物（表1） ・安全計画 ・アイテム統合とテスト計画 ・妥当性確認計画 ・安全分析 ・ソフトウェアツールの基準の評価報告と認定報告 ・セーフティーケースの完全性	アイテム定義されたアイテム（確証レビュー、機能安全監査の結果を考慮） 次工程に対する確証を重視する 準拠確認は全成果物に必要
目的に関する記載	プロセス実施の評価 ・機能安全に要求されるプロセスの実施の評価	対象成果物の確証 ・作業成果物のISO26262の要求への準拠性の評価 ・ISO26262の要求に関して、形式、内容、適切さ、完全性についての正しさのチェックを含む	達成した機能安全の評価 ・安全計画に要求される 全作業成果物の規格準拠 の評価 ・機能安全プロセスの実施の評価 ・実施された安全方策の適正と効果のレビュー

取組③視点ごとに確認イベントを整理

■ 実施事項

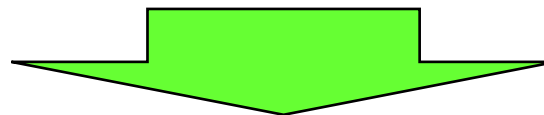
■ 確認視点の見直し

視点	機能安全 監査	確証 レビュー	機能安全 アセスメント
プロセス遵守	○		○
成果物の規格準拠 …形式、内容など		○ 表 1 成果物	○ 全成果物
次工程に対する十分性 …成果物の適切性、完全性		○ 表 1 成果物	
安全方策の適正と効果、 機能安全の達成			○

一緒に見ると効率的

分けてみると効率的

■ イベントを視点で整理



取組③視点ごとに確認イベントを整理

- イベントを3つの視点に整理

対象成果物	視点	プロセス遵守 &規格準拠	対次工程 の確証	機能安全 の達成
表1の成果物 (+α)		○	○	全成果物 と論証
その他：技術系成果物		○	—	
その他：管理系成果物		○	—	

- 各チェックリストを構築

プロセス&規格
を遵守しているか

次工程に対し
十分か

機能安全達成
に対し十分か

取組③視点ごとに確認イベントを整理

■ リスクと軽減策

■ 実施者のスキル

- 従来トレーニング体系、必要に応じ個別指導（勉強会、OJT）
- 次工程への確認のレビューには、技術部門メンバーを入れる
 - 規格準拠確認は機能安全監査と同等のスキルでOK

■ 効果：

- 現在試行中（複数事業部、複数プロジェクトで実施）だが、下記効果が期待できそう
 - 視点が明確で確認が行いやすい
 - 視点により担当者を適切に分けることが出来る
 - 機能安全達成を強化
 - 次工程への確認（表1）により機能安全達成のリスクを低減
 - どのイベントで何を保証しているのかが、より明確
 - 機能安全アセスメントでの参照が容易

取組④ 成果物ごとに視点を統合

取組④成果物ごとに視点を統合

■ 準備

- 取組③の実施

■ 実施事項

- 組織・プロジェクトに応じ、取組③のイベントを統合、同時実施
 - チェックリストは統合しない（視点を重視）
 - 機能安全アセスメントを含めた統合も可能

対象成果物	視点	プロセス遵守 & 規格準拠	対次工程 の確証	機能安全 の達成
表1の成果物 (+α)		○	○	
その他：技術系成果物		○	—	全成果物 と論証
その他：管理系成果物		○	—	

- 評価 (今後実施予定)

統合パターンは選択

目次

1. 背景
2. 課題&改善方針
3. 改善の取組
4. まとめ

目標の達成

目標	組織/プロジェクトに応じた、確証方策の効率的実施方法の選択肢の構築
----	-----------------------------------

結果	確証方策実施方法の4つの選択肢を構築 ⇒ 全組織/プロジェクトでの効率化が可能
----	--

選択肢		推奨する使用		
			小規模	大規模
イベントの統合	取組① SQA監査と機能安全監査を統合			
	取組② 確証レビューと機能安全監査を統合	ASIL低	① + ②	①
視点の整理	取組③ 視点ごとに確認イベントを整理			
	取組④ 成果物ごとに視点を統合	ASIL高	① + ③ or ④	① + ③

各選択肢の特徴

選択肢		メリット	注意点
イベントの統合	① SQA 監査と機能安全監査を統合	<ul style="list-style-type: none"> ・イベント回数削減（15→11） ・監査を統合（SQAが機能安全監査を担当）できる 	<ul style="list-style-type: none"> ・プロセス定義が重要 ・実施者のスキル（SQAと機能安全）
	② 確証レビューと機能安全監査を統合	<ul style="list-style-type: none"> ・イベント回数削減(15→8) ・機能安全監査チェック項目の63%で、確証レビューとの重複を削減 ・機能安全監査員が確証レビューを担当できる 	<ul style="list-style-type: none"> ・実施者のスキル（すべての視点の確認スキル） ・スキル不足の場合は、複数担当者で補いあうこと
視点の整理	③ 視点ごとに確認イベントを整理	<ul style="list-style-type: none"> ・視点が明確で確認が行いやすい（視点により担当者を適切に分けることが出来る） ・機能安全達成を強化（次工程への確証により機能安全達成のリスクを低減） ・どのイベントで何を保証しているのかが、より明確（機能安全アセスメントでの参照が容易） 	<ul style="list-style-type: none"> ・実施者のスキル（特に、次工程への確証の確認スキル） ・スキル不足の場合は、複数担当者で補いあうこと ・次工程への確証は、次工程開始前に行うこと
	④ 成果物ごとに視点を統合	<ul style="list-style-type: none"> ・小規模開発では、③が更に効率化できる 	<ul style="list-style-type: none"> ・大規模で行う場合は、アセスメント + 他イベントという統合のみ可能

この取組で思ったこと

- やっぱり、土台はプロセス！
 - 何をしたいかに合ったプロセスを作る
- SPI活動とSQA活動は一緒にしなくちゃ！
 - 部門を越えた連携が出来ると効果的
- 改善の切り口は一つじゃない！
 - 状況に応じた色々な答えがある

ご清聴ありがとうございます
ございました

(参考文献)

- ① SPI-Japan 2011「プロセス監査のシステム製品への拡張 ～機能安全を追い風に～」 パナソニック(株) 菅沼由美子
- ② SPI-Japan 2012「車載用機能安全規格ISO26262に対応した高信頼開発プロセス ～機能安全開発を実現するソフト・ハードの協調～」 パナソニック(株) 安倍秀二
- ③ SPI-Japan 2012「車載ソフトウェア搭載製品の機能安全監査と審査」 パナソニック(株) 菅沼由美子
- ④ SQiP2012「システム、ハード、ソフト全プロセスに渡る システムプロセス監査の実施 ～車載機能安全規格要求への対応～」 パナソニック(株) 菅沼由美子
- ⑤ SQiP2015「「SQA監査」と「確証レビュー(ISO26262対応)」の融合 ～SQAの更なる役立ちに向けて～」 パナソニック(株) 菅沼由美子
- ⑥ SPI-Japan 2015「「SQuBOK」と「ワークショップ」を活用したSQA育成 ～こんなSQAを育てよう！～」 パナソニック(株) 菅沼由美子
- ⑦ SPI-Japan 2015「機能安全開発を支える安全文化の確立と実践 ～機能安全開発スキル強化とスキル認定制度～」 パナソニック(株) 安倍秀二