76

「SQA 監査」と「確証レビュー ISO 26262 対応」の融合[1]

～プロジェクト負荷を低減する品質保証担当の取り組み～

1. 概要

近年、車載のソフト開発においては、機能安全（ISO 26262）対応が必要になっている。ISO 26262 では、機能安全の確証のための「確証方策」として「確証レビュー」「機能安全監査」「機能安全アセスメント」の実施が要求されている。確証方策のより効率的な実施方法を検討し、2012 年に SQA[2]監査と機能安全監査を一体化させる取り組みを行った。さらに、2015 年に、確証レビューをプロセス監査（SQA 監査と機能安全監査を一体化したもの）に融合させることに取り組んだ。確証レビューはプロセスではなく、作業成果物に対する確認である。ただし、プロセス監査の中に、成果物視点を明示的に取り込むことで、プロセス監査（SQA 監査と機能安全監査）と確証レビューを一体化して、同時に実施することが可能と考えた。そこで、従来技術部門が用いていた確証レビューのチェックリスト（ISO 26262 の要求事項の確認）を監査チェックリストに融合させ、監査と確証レビューが同時に行えるようにした。これにより、確証方策の実施方式としてプロジェクトが対応するイベント数を減らすとともに、本来、生産リリースまでに実施であった確証レビューを早期（プロセス監査時）に実施できるパターンを実現できた。

2. 取り組みの目的

2.1 背景

2.1.1. パナソニックの事業分野、組織構造、SQA 活動について

パナソニックは、「家電」「住宅」「車載」「BtoB ソリューション」「デバイス」という主要５分野での事業を行っている。本事例を含む車載分野においても、事業を通じて社会に貢献すべく、様々な活動を行っている。

パナソニックは、自社全体のスコープで活動するパナソニックコーポレート機能と、個別の事業分野での活動を行う４つの「カンパニー」から成っている。各カンパニーは、カンパニー全体のスコープで活動を行うカンパニーコーポレート機能と、実際のモノづくりを行う複数の「事業部」もしくは「ビジネスユニット」などから成っている。本編の事例は、パナソニックの車載分野の中心となるカンパニーのパナソニック オートモーティブ&インダストリアルシステムズ社

[1] 事例提供: 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 インダストリアル品質保証センター 菅沼 由美子 氏

[2] SQA(Software Quality Assurance) ソフトウエア品質保証担当者、品質保証活動を示す

の取り組みである。以降、「パナソニック」という場合、この「パナソニック オートモーティブ&インダストリアルシステムズ社」を示すこととする。

また、パナソニックにおいて、「SQA」という単語は、ソフトウェア品質保証活動およびその担当者を意味する。パナソニックコーポレート部門が定めている SQA の業務指針には、下記の「パナソニック SQA の 10 業務」が記載されている。（図 76-1 参照）

(1) プロジェクト早期段階でのプロジェクト計画完成度向上の促進
(2) プロジェクト活動の監視及び是正促進
(3) 外部委託管理状況の監視及び是正
(4) ソフトウェア完成度の確認
(5) メトリクス分析
(6) 製品セキュリティ対策の監視及び是正
(7) 問題解決支援（コンサルテーション）
(8) 再発防止活動
(9) 開発標準の改善促進
(10) SQA 活動のプロセス改善

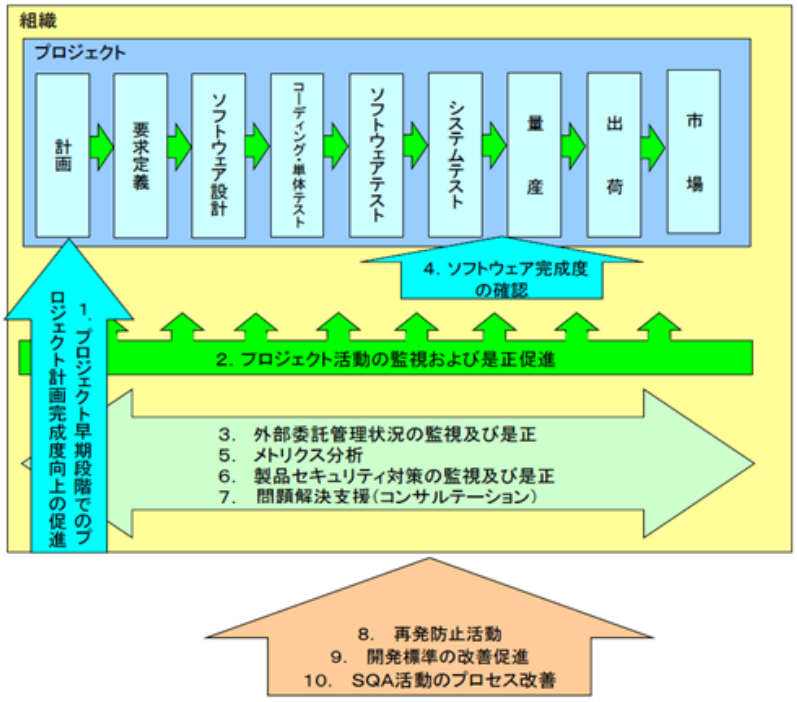


図 76-1　パナソニック SQA の 10 業務

前述の組織の階層構造に伴い、SQA も図 76-2 に示すような階層構造を持ち、役割分担を行っている。また、技術部門に属する開発プロジェクトと、品質部門に属する SQA は第三者の関係にある。

本取り組み事例は、パナソニック オートモーティブ&インダストリアルシステムズ社コーポレートの SQA としての仕組み整備の活動である。

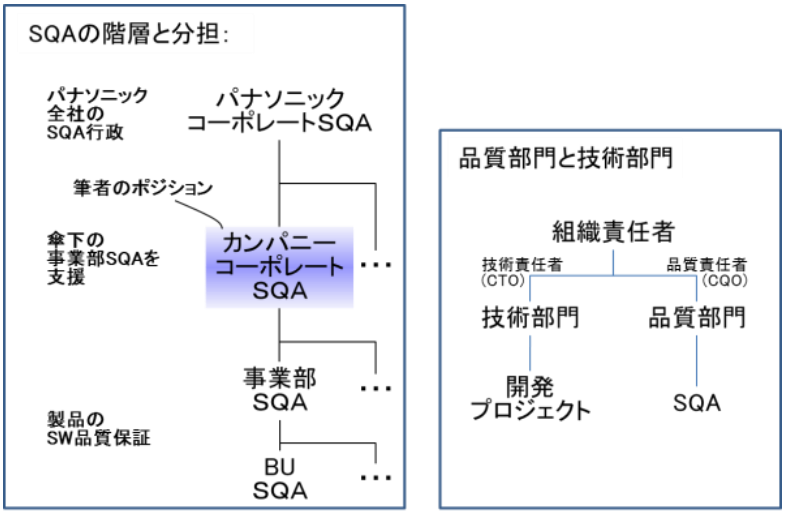


図 76-2　パナソニック SQA の階層構造

2.1.2. パナソニックの一般的なソフト開発における部門と役割

パナソニックにおける一般的なソフト開発は、ハードとソフトを含む製品開発プロジェクトの一部である。また、品質部門に所属する SQA が、技術部門に属する開発プロジェクトのソフト開発に対するプロセス監査を行うことが一般的である。パナソニックにおける開発プロセス定義において SQA 監査は、開発プロジェクトの開始から完了までに、通常、少なくとも 6 回実施される。

一方、ソフトウェアに対する検証レビューは、プロジェクト内もしくはプロジェクト外の技術部門メンバーにより、作業成果物の欠陥を取り除く目的で、漸次実施される（図 76-3 参照）。

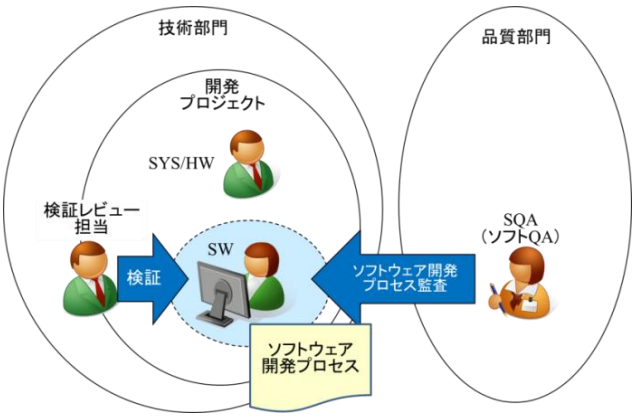


図 76-3　部門と役割：パナソニックの一般的な例

開発プロセス定義では、必要な場合にソフト開発プロセスの定義をシステム開発に拡張することができる。ソフトウェア開発プロセスのみではなく、システム開発プロセスとハードウェア開発プロセスも定義されており、SQA によるシステム開発プロセスとハードウェア開発プロセスの遵守確認が実施可能である。「システム拡張」と呼ばれる、このプロセス定義とプロセス監査の場合、”SQA”の S はソフトウェア（ソフトウェア品質保証）ではなく、システム（システム品質保証）を意味する（図 76-4 参照）。

システム拡張の場合も、SQA 監査は、開発プロジェクトの開始から完了までに、通常少なくとも 6 回実施される。

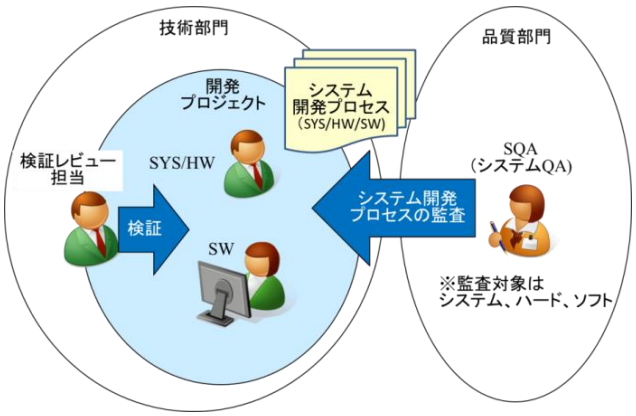


図 76-4　部門と役割：システム拡張の例

2.1.3. 機能安全

近年、「IEC 61508」を始めとして「機能安全」という考え方が広まっている。機能安全とは、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（リスクを排除する）とは異なる概念である。車載製品においては、車載分野のセクター規格である「ISO 26262」が発行され、機能安全に関する要求が明確化された。ISO 26262 では、Part2 で機能安全の管理、Part3 でコンセプトフェーズ、 Part4 でシステムレベルにおける製品開発、Part5 でハードウェアレベルにおける製品開発、 Part6 でソフトウェアレベルにおける製品開発、などの要求事項が記載されている。このなかで、Part2 の要求事項である「確証方策」について、表 76-1 に概要を示す。

表 76-1 確証方策の概要

項目	内容
確証方策	ISO 26262 Part2 で要求される、機能安全の確証に関する 3 つの活動 実施者に対し、ASIL[3]に応じた独立性（第三者性）の要求がある （ただし、実施部門は特定されていない）
確証レビュー	・作業成果物が ISO 26262 の要求事項を満たすことの確認 ※検証レビューとは異なる ・生産へのリリースまでに行う ・確証レビュー対象成果物は、システム、ハードウェア、ソフトウェアの開発成果物、開発計画書、などを含む ・実施者に対し、ASIL に応じた独立性（第三者性）の要求がある
機能安全監査	・機能安全に要求されているプロセスの遵守の確認 ・プロセスの実施中に行う ・監査対象プロセスは、システム、ハードウェア、ソフトウェアの開発プロセス、計画プロセス、などを含む ・実施者に対し、ASIL に応じた独立性（第三者性）の要求がある ・ASIL B 以上で実施が要求される
機能安全アセスメント	・達成した機能安全の評価 ・確証レビュー、機能安全監査の結果を考慮する ・生産へのリリースまでに行う ・実施者に対し、ASIL に応じた独立性（第三者性）の要求がある ・ASIL B 以上で実施が要求される

2.2 課題

従来の確証方策の実施パターンと課題

(1) パターン①

機能安全対象プロジェクトにおいて、機能安全の確証方策（機能安全監査、確証レビュー、機能安全アセスメント）を実装する方法として、一般的には、それぞれ、機能安全監査員、確証レビューア、機能安全アセッサが実施する方法が考えられる。システム拡張を行うまでは、SQA によるソフト開発プロセスの監査を実施していたが、機能安全監査はシステム開発プロセス、ハードウェア開発プロセス、ソフトウェア開発プロセスを含むプロセスの遵守確認を要求している。そのため、機能安全対応プロジェクトにおいては、SQA によるソフト開発プロセス監査に確証方策を加え、図 76-5、図 76-6 に示すような、4 種類の第三者確認が存在することとなった。この実装方法を「パターン①」と呼ぶ。確証方策の実施者は、第三者性の要求はあるが、実施部門は特定されていない。従って、開発プロジェクトとの第三者性が要求レベルを満たしていれば、確証方策の実施部門は、品質部門のほかに、たとえば、開発プロジェクトを抱える技術部門とは独立した技術部門など、組織として開発プロジェクトとは独立した部門があてられる。

[3]ASIL(Automotive Safety Integrity level) 安全性要求レベル。安全水準を 4 段階(A,B,C,D)に設定している。

実施パターン	概要	SQA監査	機能安全監査	確証レビュー	機能安全アセスメント
パターン①	4イベントを別々に実施	SQA	機能安全監査員	確証レビューア	アセッサ

図 76-5　確証方策の実装例：パターン①

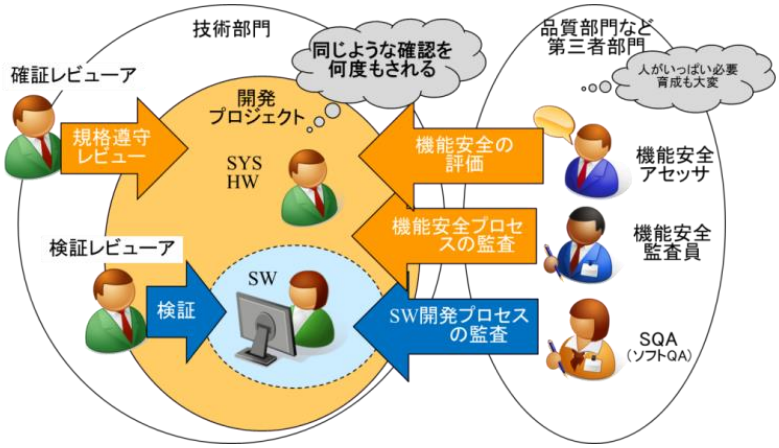


図 76-6　部門と役割：パターン①

パナソニックの開発プロセス定義において、SQA 監査は、開発プロジェクトの開始から完了までに、通常、少なくとも 6 回実施される。

機能安全の拡張方策については、規格では実施回数は規定されていない。一例として、機能安全監査は SQA 監査と同様に、開発フェーズ移行時に 6 回、確証レビューは成果物作成時期に応じて 4 回、機能安全アセスメントはプロジェクトの終盤に 1 回、それぞれ行うとした場合、SQA 監査 6 回、機能安全監査 6 回、確証レビュー 4 回、機能安全アセスメント 1 回の、計 17 回の確認イベントが発生する。大規模かつ長期の開発プロジェクトにおける場合で、確証方策実施者のリソースが豊富で、フェーズ移行の間隔が広く、開発プロジェクト側のリソースも豊富で確証方策対応工数が負担にならないプロジェクトでは、パターン①の実装は問題ないかもしれない。しかし、小規模かつ短期のプロジェクトで、確証方策実施者のリソースも不足しており、確証方策実施の間隔が狭いプロジェクトなどの場合では、たとえば 17 回のイベント実施は、対象となるプロジェクトメンバーも、同じような確認を異なる人員から何度もされる、という印象をもち、負担感が大きい。また、確証方策実施者 3 名の、必要スキルを備えたリソースが必要となり、確証方策実施者のリソースが不足するという課題がある。

パターン①の課題をまとめると、下記となる。

- 確認イベント（SQA 監査、機能安全監査、確証レビュー、機能安全アセスメント）の数が多く、開発プロジェクトの対応工数が増加する。
- 確証方策実施者として、1 開発プロジェクトあたり 3 名の、必要スキルを備えた人員の確保が必要となる。（リソースの確保が困難）

- 確証方策実施者として、1 開発プロジェクトあたり 3 名の、必要な独立性（第三者性）を備えた人員の確保が必要となる。（リソース確保が困難）
- そこで、開発プロジェクトや確証方策実施組織の負担の少ない、確証方策の実装方法を検討した。

(2) パターン②

まず、プロセス監査をまとめることを考えた。すなわち、もともと実施していた SQA によるプロセス監査と、新規に追加する機能安全監査員による機能安全監査を、一つのイベントとして実施する。（図 76-7、図 76-8 参照）

機能安全監査はシステム開発プロセス、ハードウェア開発プロセス、ソフトウェア開発プロセスを含む。そのため、SQA がシステムに対して監査する「システム拡張（図 76-4 参照）」を採用することで、機能安全監査として要求されるシステム、ハード、ソフトの全領域に対して、SQA の監査と機能安全監査を統合することが可能となる。本実施例は、2012 年の SQiP シンポジウムで発表している。発表タイトルは『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～』　である。[4]

図 76-7　確証方策の実装例：パターン②

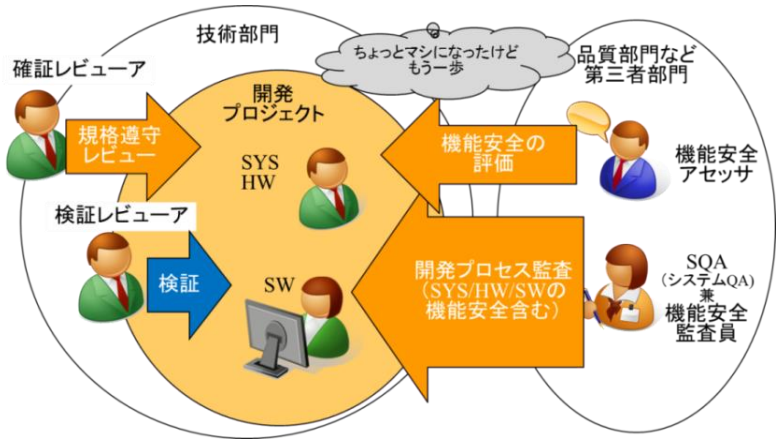


図 76-8　部門と役割：パターン②

[4] http://www.juse.jp/sqip/symposium/archive/2012/day2/files/A4-3.pdf

パターン②によって、少なくとも、プロセス確認（定められた手順に従って実施したかという視点の確認）は、一種類にまとめることができた。たとえば、17 回のイベントを 11 回に削減して、かつ確認内容を減らすことなく実施することができた。

次に、さらに、確証方策の効率化を検討した。

3. 解決のための施策

3.1 施策案

確証方策のさらなる効率化として、パターン②のイベントに、確証レビューを融合することを考えた。すなわち、機能安全監査員による機能安全監査（兼 SQA によるプロセス監査）と、確証レビューアーによる確証レビューを一つのイベントとして実施するパターン③である（図 76-9、図 76-10 参照）。

図 76-9　確証方策の実装例：パターン③

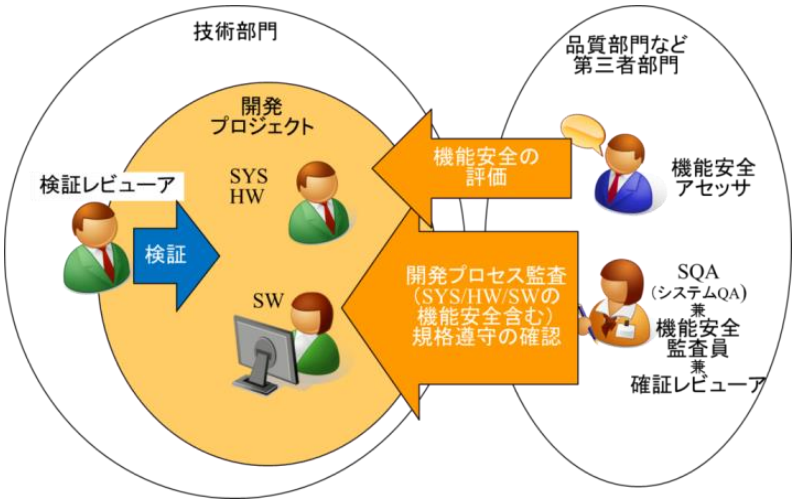


図 76-10　部門と役割：確証方策パターン③

3.2 施策案の評価

たとえば、パターン①では 17 回、パターン②では 11 回のイベントが、パターン③によって、７回で実施できる。すなわち、融合イベント６回と機能安全アセスメント１回である。このように、確証方策実施のリソースを減らすことができる上に、プロジェクト側のイベント対応の負担を減らすことができる。加えて、機能安全監査と確証レビューの判断基準のすり合わせや、プロジェクトの状況の認識の共有、などが自動的に行えるというメリットが考えられた。しかしながら、パターン③のイベントを一人で行うことになり、実施者（監査員兼レビューアー）のスキル不足が発生するリスクや、統合、融合することで、実施者のスキルによっては確認視点が狭くなる可能性があるなどのリスクが想定された。施策案に対する、想定されるメリットとリスクを表 76-2　施策案のメリットとリスクに示す。

表 76-2　施策案のメリットとリスク

項目	メリット	リスク
リソース	・プロジェクトに対する確認イベント数の削減 ・プロジェクトのイベント対応工数削減 ・確証方策担当者のイベント実施工数削減	・イベント実施者のスキル不足が発生する可能性あり
実施面	・機能安全監査と確証レビューの判断基準のすり合わせや、プロジェクトの状況の認識の共有、などが自動的に行える ・成果物（安全ケース）の段階的レビュー	・実施者のスキルによっては、確認視点が不足する可能性あり
成果物	・エビデンスの一元化	・結果の記載方法によっては、確証レビューと機能安全監査の結果の区別が、不明確になる可能性あり

3.3 施策案の改善策

想定したメリットのうち最大と考えたのは、「プロジェクトに対する確認イベント数の削減」と、「プロジェクトのイベント対応工数削減」である。また、リスクとして最も心配されたのが、「実施者のスキルによっては、確認視点が不足する可能性あり」である。そこで、メリットを活かしつつリスクを軽減する対策を検討し、「チームで実施」することを考えた。まずは、イベントを減らすが実施者は減らさない。すなわち、機能安全監査員による機能安全監査（兼 SQA によるプロセス監査）と、確証レビューアーによる確証レビューを、監査員と確証レビューアーで一つのイベントとして共同で実施する。これにより、メリットを活かしつつリスクを軽減することができる。この、機能安全監査員と確証レビューアが共同で融合イベントを実施するパターン③改を、図 76-11、図 76-12 に示す。

図 76-11　確証方策の実装例：パターン③改

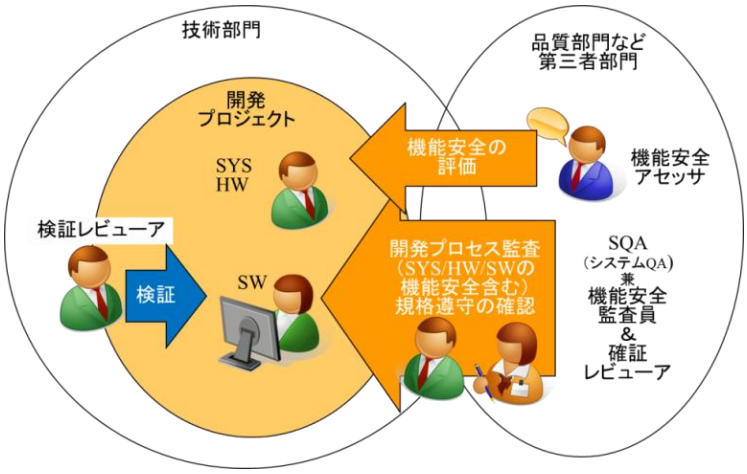


図 76-12　部門と役割：確証方策パターン③改

4. 取り組みの実施

4.1　チェックリストの融合

パターン③改を実施するに当たり、イベント融合の効果を高めるために、チェックリストの融合の検討を行った。もともと、SQA 監査、機能安全監査、確証レビューは、それぞれ個別のチェックリストを組織として準備していたが、このうち、SQA 監査と機能安全監査のチェックリストについては、両方のチェック内容を含む監査チェックリストを既に作成していた。従って、この監査チェックリストに確証レビューのチェックリストが融合できれば、3 種類のチェックリストをひとつにまとめることができる。

ここで、パナソニックにおける、標準的な機能安全関連のプロセスとチェックリストの成り立ちを図 76-13 に示す。

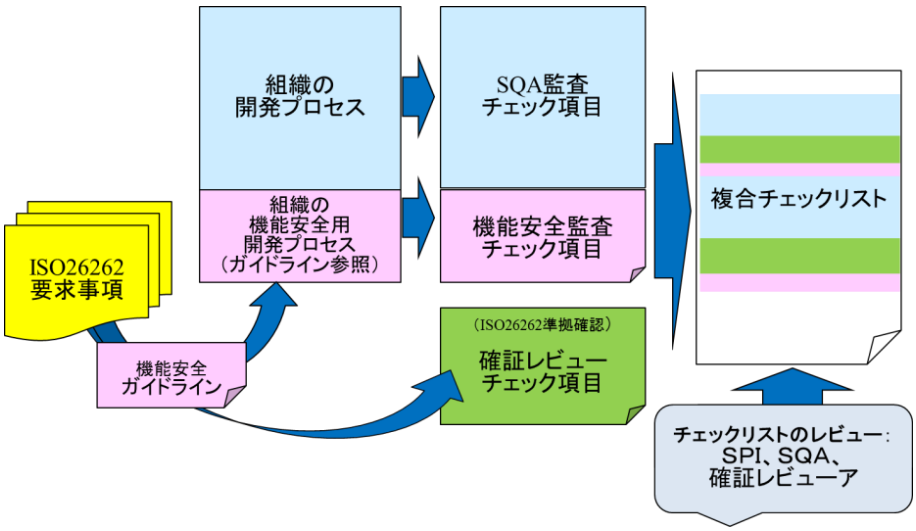


図 76-13　機能安全関連のプロセスとチェックリスト

ISO 26262 における､機能安全監査と確証レビューへの要求内容は Part2 で要求されている。機能安全監査は、機能安全関連プロセスの遵守を確認する監査である。確証レビューは、機能安全の要求事項が満たされていることの成果物ベースの確認である。

パナソニックでは、図 76-13 に示すように、ISO 26262 に規定されている要求事項を、「機能安全ガイドライン」として組織のガイドラインに取り込んだ。そのうえで、プロセスとしてガイドラインの遵守を定義し、確証レビューチェックリストはガイドライン記載事項のチェック項目として作成している。従って、もともと ISO 26262 に規定された要求の、プロセス面での確認と成果物面での確認という位置づけになっている。

監査においては、活動が実施された結果の成果物をエビデンスとして確認しながら、プロセスが遵守されたことを確認する。つまり、プロセス鑑査においても成果物を確認する。また、確証レビューは、成果物が機能安全要求事項を満たしていることの確認である。従って、機能安全監査と確証レビューは、同じ成果物を見ながら、二つの観点で評価することになり、チェックリストを融合することは意味のある取り組みであると考えた。

融合の取り組みは、下記の手順で行った。

（1）　確証レビューチェックリスト（成果物ベースのチェックリスト）を、実施プロセスに分割する。

（2）　（1）を、プロセスベースの監査チェックリストの、該当するプロセスのアクティビティの下に挿入する。

（3）　（2）で挿入した行に、対応する ISO 26262 の項番号を併記する。

4.2　チェック項目の分析とチェックリストの改善

チェックリスト融合の、確証方策の実施側のメリットとして、確認内容の整理がある。機能安全監査と確証レビューのチェック項目についての分析を行った結果を図 76-14 に示す。図からわかるように、監査チェック項目の 16%は確証レビュー項目と同じであり、監査チェック項目の 47%は確証レビュー項目を参照可能であった。

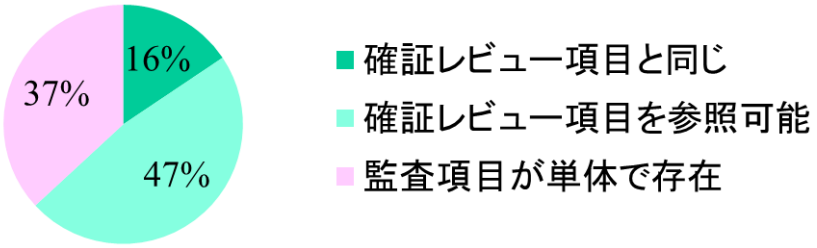
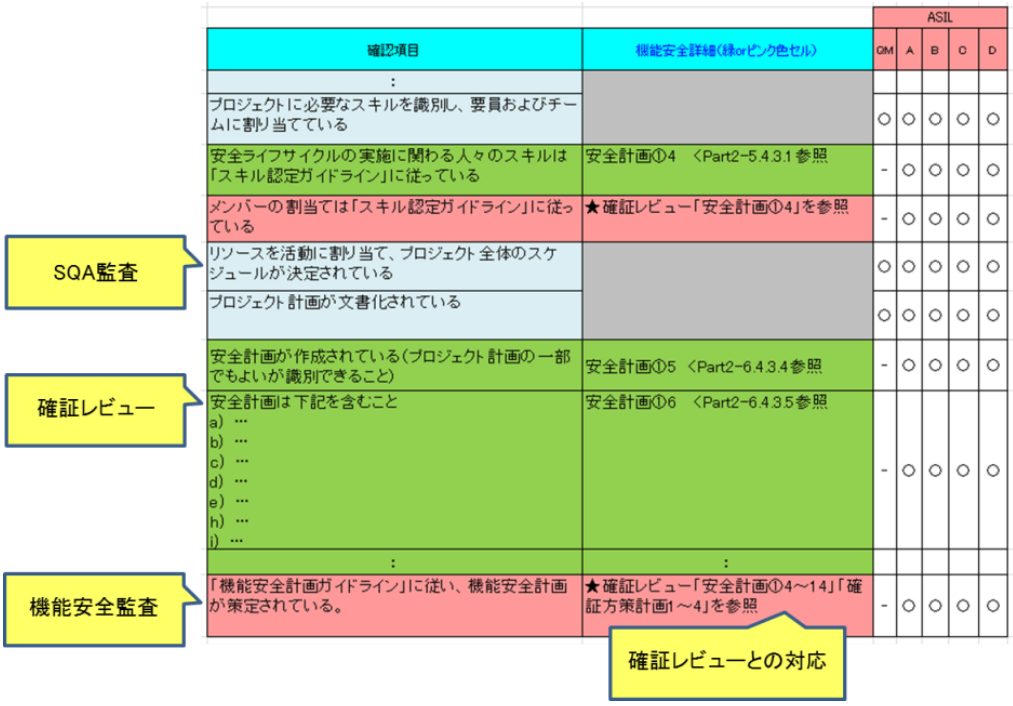


図 76-14　機能安全監査チェック項目の内訳

そこで､機能安全監査のチェック項目に､参照可能な確証レビュー項目を記載することとした。これにより、機能安全監査と確証レビューの関連が明確になる。

チェックリストのイメージを図 76-15 に示す。(図 76-15 の確認項目の記載内容ははパナソニックの実際のチェック項目ではなく、一般的なプロセスモデルからの引用である)



確認項目	機能安全詳細(緑orピンク色セル)	ASIL QM	A	B	C	D
:						
プロジェクトに必要なスキルを識別し、要員およびチームに割り当てている		○	○	○	○	○
安全ライフサイクルの実施に関わる人々のスキルは「スキル認定ガイドライン」に従っている	安全計画①4　〈Part2-5.4.3.1 参照	-	○	○	○	○
メンバーの割当ては「スキル認定ガイドライン」に従っている	★確証レビュー「安全計画①4」を参照	-	○	○	○	○
リソースを活動に割り当て、プロジェクト全体のスケジュールが決定されている		○	○	○	○	○
プロジェクト計画が文書化されている		○	○	○	○	○
安全計画が作成されている(プロジェクト計画の一部でもよいが識別できること)	安全計画①5　〈Part2-6.4.3.4 参照	-	○	○	○	○
安全計画は下記を含むこと a) … b) … c) … d) … e) … h) … i) …	安全計画①6　〈Part2-6.4.3.5 参照	-	○	○	○	○
:	:					
「機能安全計画ガイドライン」に従い、機能安全計画が策定されている。	★確証レビュー「安全計画①4～14」「確証方策計画1～4」を参照	-	○	○	○	○

図 76-15　チェックリストのイメージ

パターン③改で、確証レビューアーと監査員が同時に融合イベントを行う場合には、それぞれの確認内容が明確であるため、事前確認などの役割分担を行うことができる。

パターン③で、一人の担当者が確証レビューと機能安全監査を行う場合は、確証レビューを行いながら、関連する監査項目を同時に確認することができる。

パターン①②などで、確証レビューと機能安全監査を別々に実施する場合、確証レビューが先に実施されていれば、機能安全監査員は、確証レビュー結果を効率的に参照することができる。確証レビューより先に機能安全監査を実施する場合には、監査の際に確証レビューの確認項目を参照することで、確認の観点を知ることができる。

4.3 融合イベントの実施

作成したチェックリストを用い、融合イベントを実施した。イベント融合の最大のメリットは、事前に想定したとおり、イベント数の削減と、プロジェクトのイベント対応工数の削減であった。パターン①では 17 回、パターン②では 11 回のイベントが、パターン③改で、監査と確証レビューを融合させたことにより、7 回で実施できた（融合イベント 6 回と機能安全アセスメント 1 回）。

また、融合イベント一回の会議時間が延びることが懸念されたが、実施した結果では、監査のみに比べほとんど延びなかった。ただし、成果物の確認をあらかじめ監査員もしくは確証レビューアーが実施する事前確認については例外だ。融合イベントの場合は、従来の確証レビューの粒度で実施することになる。そのため、確証レビューアーやが参加せずに監査員のみで実施するパターン③では、監査員の事前確認時間が増加すると思われる。今回のパターン③改では、確証レビューアー、監査員は、融合イベントの中で、それぞれの確認業務を実施する。そのため、準備工数は増加しない。このように、確証方策の要求は満たしながらプロジェクトの負担を減らすことができた。

また、ISO 26262 においては、確証方策の実施時期は、「確証レビューは量産リリースまでに実施、機能安全監査はプロセスの実施中での確認、」という要求が記載されている。共に、具体的な実施時期の要求は無いが、本取り組みを実施した組織において、監査は、フェーズ移行のタイミングで実施している。融合イベントでは確証レビューも監査と同時のタイミングで実施されるため、確証レビューもフェーズ移行時に確実に実施されることになる。機能安全監査と確証レビューの実施時期として確証方策を行いながら開発を進めるのは、成果物（安全ケース）の段階的レビューができる良い方法である。

4.4 SQA 監査＆機能安全監査＆確証レビューの実施者の育成

表 76-2 で上げた「イベント実施者のスキル不足が発生する可能性有り」「実施者のスキルによっては、確認視点が不足する可能性有り」というリスクについては、今回は確証レビュー担当と

監査員が同席して実施したため発生しない。しかしながら、今回実施した印象では、監査員が確証レビューを行うことは充分可能と思われた。検証レビューは欠陥を抽出するレビューであるため、高い技術レベルが必要である。しかし、確証レビューは、ISO 26262 の要求事項が実施されたかを判断するレビューのため、問われるのは ISO 26262 の要求事項の理解である。機能安全監査員も同様に ISO 26262 の要求事項の理解を必要とするため、確証レビューと機能安全監査は、同種類の知識を必要とする。従って、一人の担当者が、機能安全監査と確証レビューの両方を実施するための教育は、比較的容易である。

現在、パナソニックでは、機能安全関連のトレーニング体系と、車載 SQA のトレーニング体系が構築済みで、必要なスキル、リソースの育成を進めている。

5. まとめ

以上述べたように、機能安全 ISO 26262-Part2 の要求事項である確証方策のなかの機能安全監査と確証レビューを、効率的に実施できる新パターンを構築することができた。

この取り組みの結果、組織や開発プロジェクトの特性に応じて、図 76-16　確証方策の実装パターンに示すパターン①、パターン②、パターン③、パターン③改の 4 通りの実施パターンから、確証方策の実施方法を選択することができるようになった。

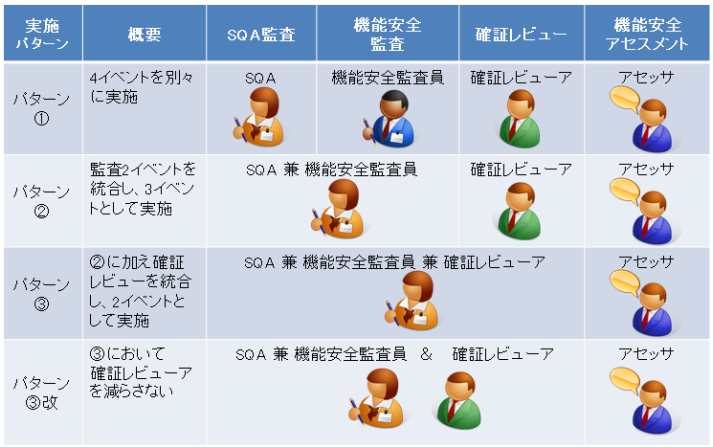


図 76-16　確証方策の実装パターン

上記パターンのどれで実施するかの選択時に、たとえば下記のような内容を考慮する。

- 当該プロジェクトに要求される確証方策実施者の独立性（第三者性）度合い（ISO 26262 に規定）
- 開発プロジェクトの規模（作業成果物の種類と量）
- 開発プロジェクトの規模（人員）
- 開発プロジェクトの開発期間
- 確証方策を実施できる第三者のスキルとリソース

また、パターン③及びパターン③改での使用を想定して作成したチェックリストは、機能安全監査のチェック項目と確証レビューのチェック項目の関連を明示したものである。想定したパターン以外においても、確証方策の実施に使用することで、観点の明確化などのメリットを活かすことができる。

6. 今後の課題

確証方策の二つである「確証レビュー」「機能安全監査」についての実施方法の検討を行ってきた。もう一つの確証方策である「機能安全アセスメント」も別途実施している。今後さらに、「機能安全アセスメント」の効果的な実施方法、「機能安全アセスメント」の効率化のための「確証レビュー」「機能安全監査」との連携方法などについても検討し、仕組み構築を行う予定である。

独立行政法人情報処理推進機構 技術本部 ソフトウェア高信頼化センター（IPA/SEC）