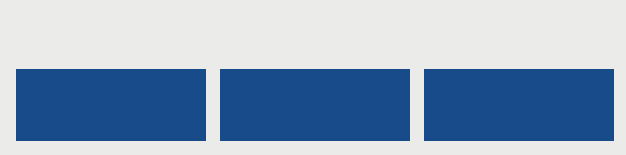
本稿では、ISO 26262で定義された確証手法をさまざまな面からご説明し、ASIL（Automotive Safety Integrity Level）準拠の目標を達成する上で確証手法が果たす役割とその重要性を考察します。

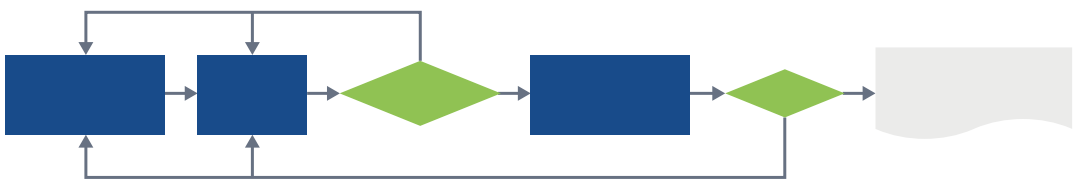


半導体の確証手法に関するISO 26262の条項をどのように適用するかは、半導体エレメントが評価されるコンテキストに応じて個別調整されます。例えば、半導体デバイスがSEooC（Safety Element out of Context）として開発されている場合、これらの条項はそのレベルで適用できます。半導体またはIPサプライヤーの場合、一般的にアイテム・レベルの安全に関する確証手法は責任の範囲外であるため、除外されます。

安全計画には機能安全を達成するための活動と手順が定義されており、これには確証レビュー、機能安全監査、および機能安全アセスメントのスケジューリングが含まれます。確証手法の実施担当者の独立性は、ASILに基づいて安全計画で規定されます。確証手法のスケジューリングは、セーフティ・マネージャーが責任を負い、確証手法の詳細はその方策に責任を負うリソースによって計画されます。

確証レビューは確証手法を構成する重要な要素の1つです。作業成果物の確証レビューでは、その作業成果物が機能安全を実証する上で十分なエビデンスとなっていることを確認します。確証レビューの目標は、一連のISO 26262規格への適合を確実にすることにあります。この目標の達成に万全を期すため、レビュー担当者は一連のISO 26262規格の要求事項に照らし合わせて作業成果物の正しさ、完全性、一貫性、適切性、および内容を確認します。

ISO 26262ではいくつかの作業成果物が規定されていますが、確証レビューは安全計画、技術安全コンセプト（TSC）、従属故障解析（DFA）や故障モード影響診断解析（FMEDA）などの各種安全解析、およびセーフティ・ケースなどの作業成果物に対して実施されます。どの作業成果物を確証レビューの対象とするかは、安全計画で個別調整します。機能安全活動に変更がある場合、その根拠を安全計画に記載し、安全計画の確証レビュー時に確認します。確証レビューはさまざまなアプローチで実施できます。例えば、安全計画に基づく組織固有のチェックリス



機能安全監査は、機能安全に必要なプロセスの実装を評価するもので、実装されたプロセスがプロセスの目標を達成しているかどうかを確認します。機能安全に必要なリファレンス・プロセスは、ISO 26262 規格に定義されています。アイテムまたはエレメントに関するプロセスは、安全計画で参照または指定された活動を通じて定義されます。セーフティ・ケースの確証レビューは、セーフティ・ケースに記載された論証を評価し、その論証に十分な説得力があるかどうかを判定します。

機能安全アセスメント（FSA）は、アイテムが機能安全を達成しているかどうか、またはエレメントがアイテムの機能安全レベルに貢献しているかどうかを判定するために必要となります。機能安全の達成はアイテム・レベルでのみ可能であり、アイテムの要素であるエレメントを開発しているサプライヤーの FSA は範囲が限定され、次の統合レベルで行われる FSA への入力としての役割を果たします。アイテムが機能安全を達成しているかどうかは、アイテム開発の最終的な顧客である自動車メーカーが任命した人員による全体的な FSA によって判定します。この判定には、受け入れ、条件付き受け入れ、またはアイテムの機能安全却下に関する提言が含まれます。公正で客観的な視点を確保し、利害の衝突を避けるため、FSA は適切な独立性をもって実施さなﾆま能定曜

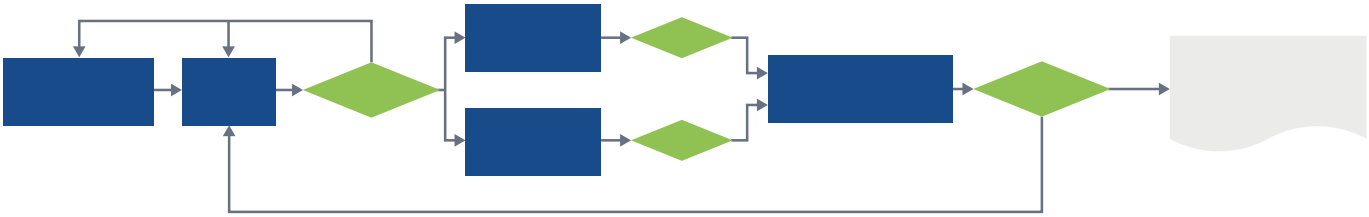


図4：確証方策の活動

図5：機能安全監査の入出力