SYNOPSYS®

WHITE PAPER

車載システム開発における機能安全規格ISO26262準拠性確認手法の果たす役割

米国シノプシス

品質/機能安全担当プリンシパル・エンジニア
Shivakumar Chonnad

品質/機能安全担当ディレクター
Vladimir Litovtchenko

品質/機能安全担当シニア・スタッフ・エンジニア
Vrezh Sargsyan

はじめに

現在の車載システムは、機能安全と長期信頼性、そして品質を基盤に構築されています。車載用のシステム・オン・チップ（SoC）にはハードウェアおよびソフトウェア・システムで構成されるいくつかのIPエレメントが含まれ、これらがメカトロニクス（機械＋電子）からのデータを特定用途向けに処理および制御します。セーフティ・クリティカル・システムにおいてハードウェア/ソフトウェアと機械の連携が進む中、機能安全開発プロセスでは安全関連製品のライフサイクル全体で発生するランダム・ハードウェア障害およびそれに起因する故障に、体系的な方法で対処することが求められています。

そのための枠組みとして、ISO 26262規格では安全分析に関する客観指向の確証手法と必要な作業成果物が規定されています。機能安全プロジェクトでは、ランダム・ハードウェア障害に関してSPFM（Single Point Fault Metric）とLFM（Latent Fault Metric）の指標を達成することのみを最小限の目標とする場合もあれば、ISO 26262規格の全体をカバーし、プロジェクトが体系的な形で規格に従っていることを実証することを目標とする場合もあります。ISO 26262に適合するための広範な体系的活動の1つに、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から成る確証手法があります。

確証は、主要な作業成果物が機能安全の達成への貢献に関して説得力のある十分なエビデンスを提供しているかどうかを判定するために実施されます。このため、確証が完了すれば、安全ライフサイクルの結果（確証の結果を含む）を考慮してアイテムまたはエレメントを量産リリースすることを正式に決定できます。図1に、体系的な機能安全開発プロセスにおける確証手法の位置付けを示します。

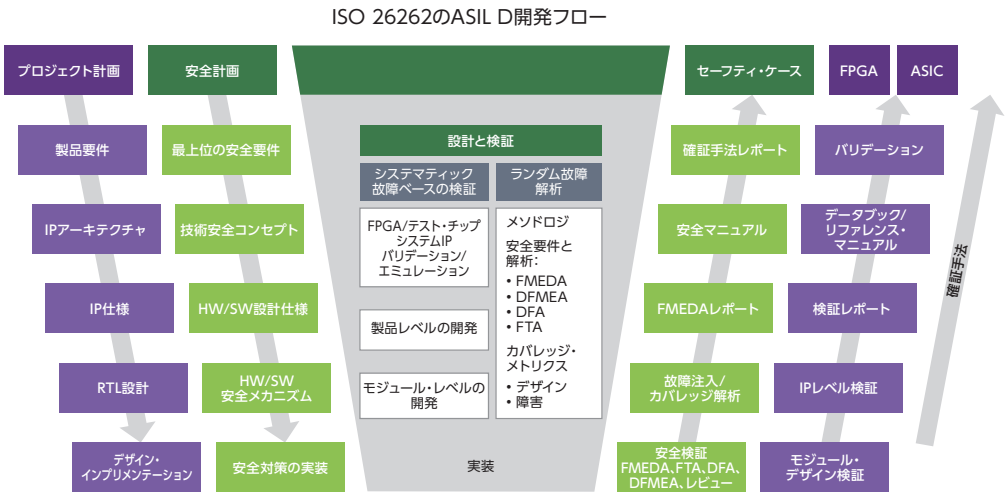

図1：確証方策を使用した機能安全開発フロー

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。

確証手法の概要

ISO 26262規格では、安全ライフサイクルにおいてさまざまな安全活動が定義されていますが、中でも安全ライフサイクル管理全体で確証手法を体系的な活動として実施することが1つの重要な責務となっています。確証手法には、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が含まれます。確証手法の実施にあたっては、適用されるASILに応じてリソース、管理、およびリリース権限に関して十分な独立性が求められます。図2に、確証手法の範囲を示します。

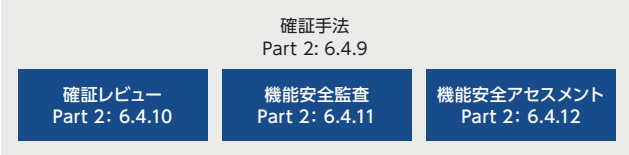

図2：確証手法とその構成要素

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トで構成し、半導体デバイスを評価するコンテキストに応じて必要とされる活動および作業成果物を列挙することもできます。確証レビューの結果に基づき、レビュー対象の作業成果物がISO 26262に適合しているかどうかを判定し、達成していない場合はレビュー結果を共有して作業成果物を更新します。安全計画に記載された確証レビューの実施責任者には、プロジェクトに適用されるASILに応じた独立性が求められます。最後に、作業成果物の貢献によって機能安全が達成されたかどうかを判定した確証レビュー・レポートが提供されます。これを図3に示します。

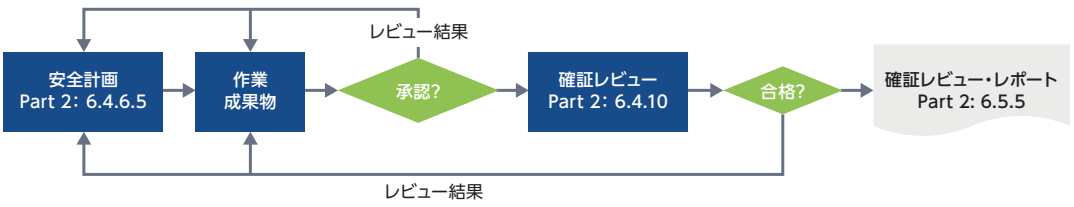

図3：一般的な確証レビュー活動のフロー

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れます。本稿で使用する「独立性」という用語は、組織内での独立性のことを指します。例えば、適用されるASILに応じて、対象となる作業成果物の作成責任者とは異なる人員、直属の上司が異なる人員、または別の部署の人員が確証方策を実施するようにします。

図4に、安全計画から機能安全アセスメント・レポート（FSAR）までのすべての確証活動のフローを示します。

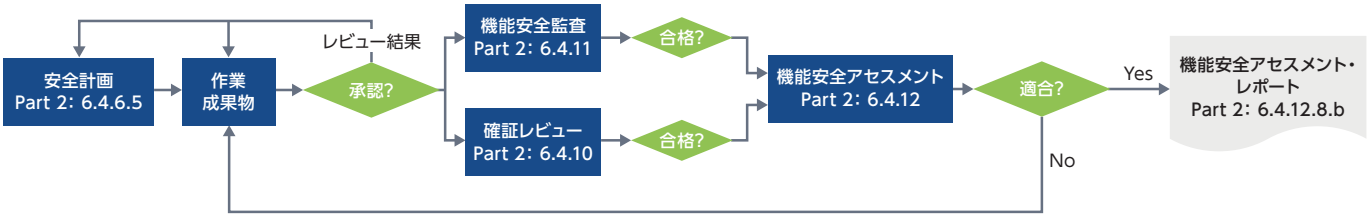

図4: 確証方策の活動

機能安全監査

機能安全監査は、確証手法の範囲に含まれます。ISO 26262において、機能安全監査とは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する作業と定義されています。機能安全監査の目的は、組織の手続きがISO 26262の要求事項に適合しているかどうか、および製品開発のさまざまなフェーズで組織が独自のポリシーおよび機能安全プロセスに従っているかどうかを確認することにあります。ISO 26262では、ASIL（B、C、またはD）が必要な場合に機能安全監査の実施が必須とされています。機能安全監査は、量産リリースの前に完了しておきます。監査の実施責任者（監査人）は十分なレベルの技能、能力、資格を有し、責務の遂行に必要な権限を与えられている必要があります。機能安全監査への一般的な入力としては、プロセス、監査の範囲、および被監査者が作成した文書があります。出力としては、監査レポートおよび機能安全監査に関する組織固有の更新されたチェックリストがあります。これを図5に示します。

図5: 機能安全監査の入出力

機能安全監査の目的は、製品開発プロセス、機能安全タスク、および活動に潜む体系的な故障を特定することにあります。必要な機能安全レベルが達成されているかを判定する機能安全アセスメントとは異なり、機能安全監査はプロセスが要件に従って実装されているかどうかを確認することをのみを目的としています。機能安全監査は、製品開発の少なくとも2つのフェーズで実施します。1つは、プロジェクトの早期段階で製品要件とアーキテクチャの定義が完了した時に実施します（一般に、これを準備監査と呼びます）。プロジェクトの早期段階で機能安全監査を実施することには、プロセスの弱点を特定できるというメリットがあります。

もう1つの機能安全監査は、実装フェーズで設計と検証が完了した後に実施されます（これを実装監査と呼びます）。図6に、これら2つの監査が一般的にプロジェクト・フローのどの段階で実施されるかを示します。この図は概略図であり、ここに示した以外に中間フェーズが存在することもあります。

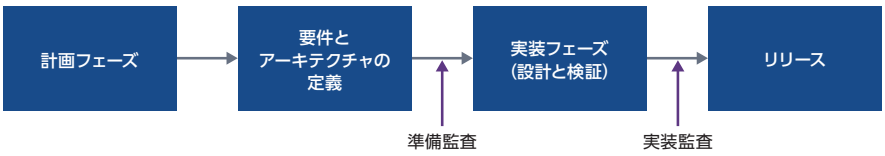

図6：プロジェクトで機能安全監査が実施される2つのフェーズ

これら2つの機能安全監査は目的と範囲がそれぞれ異なっており、監査前に規定され、周知されます。準備監査の目的は、プロジェクトの実行準備が完了しているかをチェックすることにあります。このステージでは、プロジェクト計画、安全計画、および各種のサポート・プロセス（構成計画、変更計画、文書管理計画など）を監査の対象範囲とします。準備監査では、チームが過去の教訓（もしあれば）を再確認し、過去の監査結果に対処しているかどうかも確認します。

デザインの実装と検証が完了したら、実装監査を実施して機能安全プロジェクトの実行が適合しているかどうかをチェックします。実装監査では、さまざまなフェーズでレビューが実施されたかどうか、そして安全計画で必要とされている作業成果物が必要な開発フェーズで作成され、レビューと承認を受けたかどうかを確認します。実装監査では、過去の監査結果に対処したかどうか、および教訓が反映されているかどうかも確認します。実装監査では、安全活動が計画通りに実施されたことを証明するエビデンスとして、作業成果物、レビュー・レポート、記録などを求めます。この監査では、以下の点を考慮します。

- 実装されたプロセスの評価
- 安全計画に記載され、組織固有の規則とプロセスに従って作成された作業成果物の入手性
- 実施または実装した安全対策の適切性と有効性
- 一連のISO 26262規格のプロセスに関連した目標が達成された理由についての論証（もしあれば）

機能安全監査の結果は、組織の取り決めに基づき、ISO 26262または組織のプロセスに対するNCON（不適合）またはOFI（改善の機会）に分類されます。NCONは、意図した結果を達成する能力に影響します。機能安全監査は、検出されたすべてのNCONが解決するまで完了とは見なされません。OFIとは、意図した結果を達成する能力に影響しないプロセス（またはその実装）の潜在的な欠陥を言います。いずれのフェーズの監査でも、すべての監査結果をまとめた監査レポートを作成します。機能安全監査が完了したら、次に機能安全アセスメントを開始します。

機能安全アセスメント

機能安全アセスメント（FSA）は、達成されたアイテムの機能安全、または開発されたエレメントによる機能安全達成への貢献を判定するために実施します。これは、ASIL CおよびDの場合に該当します。FSAは、製品の機能安全目標に関する技術目標が達成されたかどうかの判断に基づくことができます。この判断では、これら規格の対応する要求事項、現在の技術水準に照らし合わせたソリューションの妥当性、および開発時点で適用可能な工学分野の知識を考慮します。FSAを開始する際には、確証レビューおよび機能安全監査の計画を考慮する必要があります。FSAでは、過去のFSAおよびその結果として実施された是正措置のフォローアップ（該当する場合）、または開発インターフェイス契約（DIA）に従ってサプライヤーが開発したエレメントや作業成果物に関するFSAの結果も考慮します。

FSAは、遅くともシステム・レベルでの製品開発の開始時には計画されます。FSAは製品開発の進行に合わせて実施し、量産リリース前には完了しておく必要があります。FSAは、任命を受けた1名以上の人員（機能安全判定者）によって実施されます。FSAの範囲には、安全計画および作業成果物とその確証レビューが含まれ、機能安全監査の結果に基づいてプロセスの実装を評価することができます。機能安全判定者は、機能安全の目標が達成されたかどうかを判定し、その結果を機能安全アセスメント・レポート（FSAR）にまとめます。機能安全判定者には、安全活動とその結果に対する分析の幅や深さなどを自らの裁量で決定してFSAを実施する権限があります。分散開発を伴うような大規模なプロジェクトでは、同じサプライチェーンに属するメーカーとサプライヤーがそれぞれの責任領域に対処しながらFSAを実行できます。

FSARは確証手法の結果であり、分析した作業成果物またはプロセス文書の名前とリビジョン番号を含みます。このレポートには、条件付き受け入れ（特定された条件を解決した場合のみ受け入れ可能）に関する提言が含まれることがあります。条件付き受け入れに関する提言の場合、FSARには必要な是正措置が含まれます。FSARの提言が機能安全達成の却下である場合、適切な是正措置を実施した後、FSAを再度実行します。確証方策の完了後にアイテムに変更があった場合は、妥当な確証方策を繰り返すか、追加で実施します。

まとめ

確証手法の実施結果には、IP開発プロセスおよびシステマティック/ランダム・ハードウェア障害の回避に関するエビデンスと論証が含まれます。これらのレポートは、プロジェクト内で体系的に追跡できるようにしておく必要があります。半導体IPの場合、一般的な確証方策の出力としては、確証レビュー・レポート、機能安全監査レポート、機能安全アセスメント・レポートがあります。これらのレポートは、製品が機能安全を達成しているかどうかを判断するのに役立ちます。サプライヤーがコンプライアンスのために作成した作業成果物は、半導体メーカーの安全論証の一部となります。自動車メーカーは、統合されたアイテムの機能安全をアイテム・レベルで評価します。この評価の一部に、1社以上のサプライヤーから提供された作業成果物や情報（FSARなど）を含めることができます。

シノプシスのオートモーティブIP

体系的な自動車コンプライアンス・プロジェクトにおける機能開発プロセスの一環として、シノプシスの体系的なオートモーティブIP製品はISO 26262の確証手法に従っています。このような体系的な自動車コンプライアンス・プロジェクトの成果物の一部として機能安全アセスメント・レポートをSEooC開発元から取得することは、次のTierでインテグレーターの安全論証を加速するのに役立ちます。

Pub: Jan. 2023