自動車の機能安全

SGS-TÜV Saar社　Functional Safety for Semiconductors責任者　Wolfgang Ruf氏

自動車の機能安全の現状について、SGS-TÜV Saar社、Functional Safety for Semiconductors責任者のWolfgang Ruf氏にご説明いただきます。さらに、この分野への新規参入企業に向け、実践的アドバイスをいくつかご紹介いただきます。

SGS-TÜV Saarは、複数の業界にまたがる機能安全コンプライアンスを専門とする世界屈指の認証機関であり、世界の主要半導体ベンダや自動車業界のOEM企業、Tier 1サプライヤ、Tier 2サプライヤにサービスを提供しています。このようなさまざまな階層の企業との密接なつながりを活かし、当機関は業界全体に機能安全対策を行き渡らせる方法について独自のノウハウを蓄積しています。当機関の顧客である多くの半導体企業は、昨今の自動車のエレクトロニクス化の進展に強い関心を示しています。けれども、機能安全に関する実績が何もないままこの業界に乗り出そうとする企業が多いのも事実です。

これは問題と言わねばなりません。なぜなら、半導体メーカーは社内に限定された専門技術しか持たないため、ISO 26262規格（機能安全規格）に従って機能安全プロセスを構築し、それを製品につなげる方法を、明確にイメージすることができないからです。ISO 26262に適合するための最低限の要求事項さえ知らないということも少なくありません。たとえば、機能安全の要求を満たすためにTier 1、Tier 2サプライヤがどの文書を必要とするかさえ知らないケースもあるのです。

当機関は、こうした例を実際に何度も目の当たりにしています。というのも、スタートアップ企業を含む多くのIPプロバイダが、画像機器関連のようなコンシューマ用アプリケーションから車載アプリケーションへの転換を図ろうとしており、そのような企業からのトレーニング依頼が増加しているからです。

ISO 26262について知っているということと、半導体チップ設計のために作成された複雑な機能安全規格を理解し内容を汲み取ることができることは別であり、誤った解釈を避けるためには多くのスキルや経験が必要です。

安全文化の構築

ISO 26262の重要な要件の1つは、組織全体に安全文化を構築することです。企業はISO 26262-2の付属書Bに含まれる以下のような推奨事項に従うことで、安全文化を構築することができます。主要な項目は以下のとおりです。

- 経営陣がISO 26262への準拠に同意している
- 機能安全のトレーサビリティや説明責任が開発ライフサイクルの中で優先されている
- 安全性の確保に最も高い優先度が与えられている
- 報酬システムによって機能安全の実効性確保に対する動機づけを行う。また、安易な方法をとることによって安全や品質を軽んじる者を処罰する
- 検証プロセスに適切な安全性確認工程が組み込まれている

設計チームが取り組むべき課題

自動車に搭載される電子部品の数は急激な勢いで増えています。そのため設計チームは通常の問題に加えてさらに多くの課題に取り組まなければなりません。

機能安全を実現するということは、設計のさらなる複雑化に対処するということであり、安全に関わる検証と妥当性確認を（関連する安全メカニズムも含めて）取り入れるということです。

「ブラック・ボックス」化されているサードパーティ製または自社製のIPを組み込むにあたって、チップ内外のインターフェイスを正しく設計するには、センサー、アクチュエータ、マイクロコントローラなどのコンポーネントに対応した故障シミュレーションを行うための特別なスキルが必要です。たとえば、設計チームは、センサー、システム、アクチュエータ間のインターフェイスのどこかで故障が起きた場合でも、それをシステムが検出し回復できることを実証できなければなりません。これらのインターフェイスには、デジタル・ブロックを使用しなければ故障シミュレーションが行えない容量負荷や抵抗負荷が含まれるため、確認作業は一層複雑になります。

また、設計チームは診断範囲（DC：Diagnostic Coverage）の見積りも行う必要があります。DCとは、安全メカニズムが故障を検出できる確率（%）です。DCの見積りは容易ではありません。そのため当機関は、シノプシス社との連携により、見積り計算を自動化するためのツールと方法論を導入しています。

機能安全が開発期間に及ぼす影響

通常、半導体企業は機能安全対策をゼロから始める必要はありません。普通は何らかの機能安全対策がすでに設計フローに組み込まれているからです。まずは、どの程度の安全性レベル（ASIL）を達成できるかを検討するところから始めます。

最初の段階として、チップの設計と検証のプロセスに機能安全対策を導入します。当機関の経験では、この作業には6ヶ月から2年を要します。その企業がISO 26262に対する知識をどれだけ持っているかや、機能安全のための文書やテンプレートを用意するためのリソースがどれだけあるかによって、かかる時間は変わります。

時間を節約するため、プロセスの導入と並行して最初の機能安全製品の開発が行われるのが普通です。ASILの要件にもよりますが、最初の製品の開発で設計と検証にかかる期間はコンシューマ向け製品の場合より数ヶ月ほど長くなります。それ以降の設計サイクルでは、設計チームが誤り訂正やパリティ・チェックなどのデザイン・イン経験を重ねていくため、プロジェクトのリードタイムは短縮されていきます。最終的には、ISO 26262は普通の日常的なプロセスの一部となるはずです。多くの組織で品質マネジメント・システムISO 9000が日常業務に溶け込んでいるのと同様です。

今後のISO 26262

当機関はISO 26262の標準化委員会に属しており、現在はISO 26262のPart 11の標準化作業を行っています。Part 11では、ISO 26262の概念の半導体への適用、特に以下の項目への対応が検討されています。

- 半導体IP
- 基本の故障率の見積り
- 半導体依存故障の分析
- 半導体部品への故障注入
- 半導体の生産と運用
- 半導体の分散開発のインターフェイス
- 半導体の確証方策および機能安全監査
- 半導体のハードウェア統合とテストに関する説明

また、以下のような半導体特有の技術や適用領域についても対応が検討されています。

- デジタル・コンポーネントおよびメモリー
- アナログ / ミックスド・シグナル・コンポーネント
- プログラマブル・ロジック・デバイス
- マルチコア・コンポーネント
- センサーおよびトランスデューサー

新規参入企業への実践的アドバイス

自動車業界への参入にあたってISO 26262への準拠を必要としている企業に向けて、開発期間の短縮とリスク削減のための実践的なアドバイスをご紹介します。

1: ISO 26262の開発プロセス認証を取得する

ISO 26262認証の取得を目指して車載電子部品の開発プロセスを改善するためには、製品の開発ライフサイクル全体を刷新しなければなりません。できるだけ短期間で効率よく認証を取得するには、トレーニングによるスキルの向上を図るのも有効ですし、プロフェッショナル・サービスを利用するという方法もあります。その場合、クオリフィケーションや認証だけでなく、コンサルティング、アセスメント、監査にも対応できるプロフェッショナル・サービスを提供できる企業を選択するとよいでしょう。

2: 製品(ファミリー)のASIL適合認証を取得する

新規参入企業は、公認の機能安全パートナー（ISO / IEC 17025準拠）の協力を仰ぐとよいでしょう。概念の評価、テクニカル・レポートの発行、製品安全アセスメントの実施、ASILリスク分析などに関する支援を受けることができます。

3: システム、IC、IPのレベルと、DC、検証、妥当性確認の関係を理解する

ICへのIPの組込みとシステムへのICの統合に対して検証と妥当性確認を効率よく実施するには、設計チームのスキルの向上を図り、適切な自動化ツールを使用する必要があります。たとえば、デザインの中から機能安全上の弱点を見つけ出す技能を高めたり、ICレベルとシステムレベルに効果的なDFT機能を導入して弱点を軽減する方法を習得したりする必要があるのです。このときに大切なのが、故障の妥当性確認の概念です。

故障の妥当性確認

故障の妥当性確認は、自動車業界に新しく参入する多くのサプライヤにとって馴染みの薄い概念です。ISO 26262のプロセス構造を導入すると、故障を発見しやすくなるという効果があります。設計チームは機能について検討し説明しなければならないので、回路の中の潜在的な問題点を認識しやすくなるのです。この方法は、IPやICに不具合が生じたときにどのようにして問題点を検出するかを考える際にも役立ちます。

問題は、どの程度の故障検出率であれば必要な機能安全を十分に確保できるかということです。その答えは、IPやICのレベルなのか、それともシステムのレベルなのかによって異なるでしょう。IPやICのレベルの場合、故障注入などのツールを使用したり、静的解析ツールと動的解析ツールを組み合わせれば、予期していなかった故障を発見することができます。ハードウェアにおける単一箇所の故障と潜在的な故障の範囲を考えることによって、問題が起きたときに検出と修正が可能かどうかを判断できます。

ISO 26262のASIL CおよびDの要件に基づいて故障率を低減するために多くの設計チームが採用している方法は、CPU、センサー、アクチュエータの二重化（CPUについてはロックステップ方式を採用）です。また、バウンダリ・スキャンやBISTのようなDFT手法を用いることにより、製造段階で発生しうる故障を設計段階で未然に防ぐこともできます。

ASIL Dの達成を目指す場合、以上のような問題に対応するためには故障モード影響診断解析（FMEDA）、FTA（Fault Tree Analysis）、DFA（Design For Assembly）のような解析メソッドが欠かせません。検証と妥当性確認のための故障注入を実行するツールはいくつも市場に出回っていますが、適正なツールを使用すれば、最小限の労力でISO 26262に準拠した設計を行うことができます。機能安全のためIPやICの検証と妥当性確認を行うには、結局のところ高度なツールが必要になるのです。

安全とセキュリティ

自動車は、外の世界との接続が多くなるほどハッカーの標的になりやすく、サイバー犯罪に対して脆弱になります。ISO 26262が扱っているのは自動車の安全だけであることを忘れてはなりません。サイバーセキュリティという新たな問題に対しては、SAE J3061（ISOの標準化活動がまもなく開始予定）や、IEC 62443のようにすでに公開済みの規格があり、さまざまな側面から取り組みが行われています。当機関では、サイバーセキュリティに対する世間の関心の高まりを予見して、機能安全とITセキュリティのためのグローバル・コンピテンス・センター（Global Competence Center for Functional Safety and IT-security）を設立し、ITセキュリティに関する認定を取得しています。

機能安全の今後の課題

自動車業界の次なる目玉は自動運転です。自動運転を実現するには、たとえば自動車と自転車を区別するなど、路上の他の車両や歩行者を安全に検出する必要がありますし、他にも多くの複雑な要件を満たさなければなりません。現在さまざまな研究開発チームが最先端技術を開発し、それを自動運転車に搭載することによってそうした要件を満たせることを証明しようと、さまざまな試みが行われています。自動車には確かな安全性とセキュリティの両方が必要です。このことは今後、コネクテッド・カーや自動運転車の開発に途方もない影響を与えることになるでしょう。従来の車とは次元が異なる新しい輸送手段の安全性ニーズを満たすため、当機関は業界の関係各社と協力しつつ、常に最新の動向を取り込みながらISO 26262の改定に取り組んでいく所存です。

SGSグループについて

SGSグループは、全世界で8万人の社員をようする、検査、検証、試験、および認証の分野における世界的な認証機関です。ドイツにあるグローバル・コンピテンス・センター SGS-TÜV Saarと世界各国の専門家チームの連携により、ローカル、グローバルを問わず、さまざまな業界の製造企業に機能安全のあらゆる問題に関するサービスを提供しています。機能安全ならびにITセキュリティの認定機関であり、対応する標準化委員会のメンバーでもある当機関は、トレーニング、個人の資格取得、コンサルティング、安全性分析、審査、監査および認証の分野で活発な活動を展開しています。

著者紹介

Wolfgang Ruf : SGS-TÜV Saar社Functional Safety for Semiconductors責任者。同社にて機能安全分野で6年以上の実績を持つ。それ以前は、半導体業界で20年以上勤務。ISO 26262 Committeeのメンバー。