機能安全単独から包括的なシステム安全の達成に向けての課題（小西）

先日、自動運転レベル３の機能を搭載した自動車が、2020 年度中に市場に投入されることが発表されました。国内の法律が整備されてきたことで、量産化に向けた自動運転技術の進化が加速しているように感じます。各国の法律が整備されることで、更に技術進化は加速していくでしょう。

本メルマガでは、日経クロステック 日経 Automotive 主催セミナー「ISO 26262 2nd 実践と将来動向 ~CASE 時代の包括的なシステム安全の基盤に~」にて、弊社土屋が講演する機能安全単独ではカバーできない安全領域を含む包括的なシステム安全の達成を目指す際の課題について紹介します。

自動運転レベル３機能搭載車の国内における型式認証では、サイバーセキュリティ確保の方策が性能の一部として要求されています。要素の故障やシステマティック故障をシステムの安全上のリスク要因として対策するだけでなく、サイバー攻撃に晒される脆弱性が安全目標の達成に影響する場合は、このリスク要因を対策することが必要になります。前者は ISO 26262 がカバーする範囲ですが、後者のサイバーセキュリティにおけるリスク分析と対策はサイバーセキュリティ規格（ISO/SAE 21434）がカバーする範囲になります。また今後は、システムの誤使用や AI 技術などの不確実さを含めた性能限界による安全上のリスク低減を考えることが必要になります。これは、SOTIF（ISO/PAS 21448）でカバーされます。これらの規格は、ISO 26262:2018 とは独立して発行されますが、リスクベースのアプローチという面では共通なので、包括的にリスクアセスメント、リスク低減活動を実施することが重要になります。

開発対象システムのリスクを特定し、リスクを低減するリスクベースのアプローチを実施するために、最初にシステムの範囲を明確にします。従来の車載システムは、車におけるその役割を果たす単独システムとして開発されてきました。例えば、電動ブレーキシステムは、ドライバーのブレーキペダル操作量に応じて、ブレーキ圧力（流量）を出力する単独システムです。この場合、システム構成要素、システムの入力と出力要素を基に、ブレーキペダルからブレーキアクチュエータまでをシステムの範囲として容易に決定できます。ADAS や自動運転では、それらの機能が複数のサブシステム（エンジン、ステアリング、ブレーキ、カメラ、LIDAR、HMI など）の集合で実現される階層的なシステム構造になります。システム全体の目的、システムが使われる環境、ユーザーとシステムの相互作用、対象システムの外にある他システムへの影響または、他システムから受ける影響などを俯瞰的に捉えることが必要です。

ADAS や自動運転システム開発では、従来の OEM を頂点とした垂直統合型の産業構造から、それぞれの得意領域を活かして迅速に開発を進める水平分業型への変化が起こっています。ISO 26262:2018 では、この変化に合わせて、SEooC（背景によらない安全関連エレメント）におけるプロバイダー（提供者）とインテグレータ（使用者）の責務が明確に定義されました。

SEooC では、プロバイダーは異なる OEM へシステムを提供するので、特定の OEM 要求に基づいてシステムが開発されず、想定の元で開発されます。そのため、上位システムの安全要求が実現できない、要求される ASIL への対応能力に乖離するといった不整合が発生する可能性があります。不整合を発生させないために、SEooC 統合を前提とした製品コンセプト、標準化されたアーキテクチャやモジュラー設計の採用などの方針に沿って、システム開発を進めることが必要です。

本メルマガで触れた課題に対するアプローチについては、冒頭で紹介しましたセミナーにて弊社土屋が解説いたします。ご興味がある方は是非セミナーへお申し込みください。

https://www.nikkeibp.co.jp/seminar/atcl/nxt/nat201215/

2020/11/20 小西 晃輔