上流品質技術強化 コンシューマデバイス機能安全規格化の取組み

SEC 統合系プロジェクト 研究員　内田　功志
SEC 統合系プロジェクト 研究員　室　修治

1 はじめに

機能安全の規格は、専門家が使用することを前提としたシステムを対象とする規格が先行して制定されてきた。

一般消費者が使用する製品については、自動車の機能安全規格 ISO 26262 がようやく発行されたところである。

そこで，一般消費者向けのシステムを対象とした製品群を“コンシューマデバイス（消費者機械）”と呼び、分野横断的なコンシューマデバイスにおいて、多様な利用者・利用環境に対応するために必要とされる安全性に可用性や信頼性、保全性を確保するための規格を、自動車の機能安全規格 ISO 26262 をベースとして提案することとした。

2 機能安全規格の概要

コンシューマデバイスは表 1 に示すように、産業機械とは異なり、技術者の手を離れて多様な環境で多くの一般消費者に利用される。そこで、産業機械とは考慮すべき条件が異なる場合も多く、また達成すべき信頼性や安全性にも特別の考慮が必要と考えられる。しかしながら安全性に関する標準化の取組みは前述のように産業機械や工業プラントに対するものが先行しており、コンシューマデバイスの安全性に対する標準化の取組みは遅れている状況である。

表 1　産業機械の違いとコンシューマデバイス

	産業機械	コンシューマデバイス
生産数	少～多	多～
利用者	専門家	一般消費者
要求コスト	（高）	低
メンテナンス	設置現場	ユーザ、サービスステーション
環境	工場など（限定的）	ユーザ環境（多様）

異種のシステムが組み合わされたシステムにおいて個々のシステムについて世代を越えて管理しなければならないことは、今日の社会システムや製品開発に共通の課題である。コンシューマデバイスはそのような複雑なシステムを構成する要素でもあり、些細な不具合が波及して、重大な社会問題を引き起こす可能性を排除できない。すなわち、コンシューマデバイスの安全性、信頼性、セキュリティを含めたディペンダビリティ※1 を保証する枠組みを構築することが、今日の重要な課題となっている。

コンシューマデバイスの標準化を検討するに当たり、まずベースとなる ISO 26262 を分析した。ISO 26262 の分析では UML におけるクラス図を利用してメタモデルという形で表現し、検討に当たるメンバ間で共通の理解を得られるようにした。また ISO 26262 における安全についての概念を整理するため、Part1 から Part3 までを分析の対象とした。

ISO 26262 の Part3 は主にハザード分析 に関する考え方やセーフティケースの記述に関する考え方、セーフティメカニズム の必要性、変更に関するインパクト分析、さらには Proven in Use（使用実績による証明）に関する取扱いなど、内容が盛り沢山である。特にセーフティケースを使用して、安全であることを明確にすることは、ISO 26262 では必須要件項目になっている。

コンシューマデバイスに関する現在までの検討結果では、対象モデルの記述においてはセーフティケースからディペンダビリティケース※2 へと拡張することを考えている。これはコンシューマデバイスやそれらが複合したシステムの特性を考慮し、単に安全であるだけでなく可用性や信頼性、保全性などのコンシューマデバイスに求められる要素についても配慮すべきとの考えからである。

ディペンダビリティを確保するためには、想定と試行の素早い繰り返しによる改善が有効であり、そのような開発プロセスも規格に盛込むこととした。

3 おわりに

上記の検討内容も踏まえて、OMG※3 に提出した提案要請（RFP）は、2013 年 3 月に正式発行された。今後は、この RFP に対する具体的な規格化への提案を進めていく予定である。

【脚注】
※1　ディペンダビリティ：信頼性性能、保全性性能及び保全支援能力を記述するために用いられる包括的な用語とされている
※2　ディペンダビリティケース：ディペンダビリティを保証するために階層的、系統的に構成する論拠の示し方
※3　OMG：Object Management Group