コンシューマ・デバイスを対象としたディペンダビリティ保証への取り組み

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

自動車産業における機能安全規格であるISO 26262が2011年に正式発行され、自動車関連業界の対応が本格化している。IPA/SECではシステムの信頼性や安全性を確保するための取り組みを行ってきたが、一連の機能安全規格の中から消費者向け用途のシステムを対象として、自動車にとどまらない日本のシステム産業全体にとって有益なディペンダビリティ保証とはどうあるべきかを、自動車の機能安全規格ISO 26262を参考として検討を開始した。

1　はじめに

機能安全の規格には、製品分野を特定しないIEC 61508、原子力（IEC 61513）や鉄道（IEC 62278、62279）といった一般消費者向けではないシステムを対象とする規格から制定されてきている。今回の検討を開始するに当たってはISO 26262を除き既存の規格が対象としていない分野、また日本の産業にとって重要である一般消費者向けのシステムを対象とし、その製品群を“コンシューマ・デバイス”と呼ぶこととした（以前IPAで使用していた呼称“消費者機械”は、“コンシューマ・デバイス”に変更した）。なおISO 26262が対象とする自動車や、今後出てくるであろう家庭用のサービスロボットなどもコンシューマ・デバイスに含まれるものとしている。

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ユーザに利用される。そこで、専門家が対象で数的にも限りのある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り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り組みは遅れている状況である。

典型的なコンシューマ・デバイスである自動車は高い安全性と信頼性が求められると同時に、動力方式の変更や環境面への対応が必要となる。また新しい社会システムとの連携などへの対応も求められるようになり、自動車の制御システムは急速に複雑化している。自動車のエンジン制御だけでも、筒内空気量推定、燃料噴射制御、点火時期制御、エンジントルク制御、排気ガスエミッション低減、異常診断などのシステムが複雑に絡み合っている。それぞれのシステムが多様な要求で独自に成長していくので、世代を越えて製品の信頼性を保証し続けることは容易ではない。更に、自動車は単体としての機能や効率向上を図ることは当然として、交通、配送、エネルギー供給、情報システムなどと連携して付加価値を創造する時代になっており、自動車の制御システムは一層複雑化が進展することが予想される。このようなシステムの複雑化、大規模化の傾向は、多くのコンシューマ・デバイスにも当てはまる状況となっている。

表1　コンシューマ・デバイスと産業機械の違い

	産業機械	コンシューマ・デバイス
生産数	少	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	限定的	多様

また社会全体も交通、配送、エネルギー供給、情報システム等々が絡み合って複雑なネットワークを構成する、いわゆる社会システムとも呼べるようなものになってきている。このような、異種な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を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することは出来ない。すなわち、コンシューマ・デバイスの安全性、信頼性、セキュリティー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。

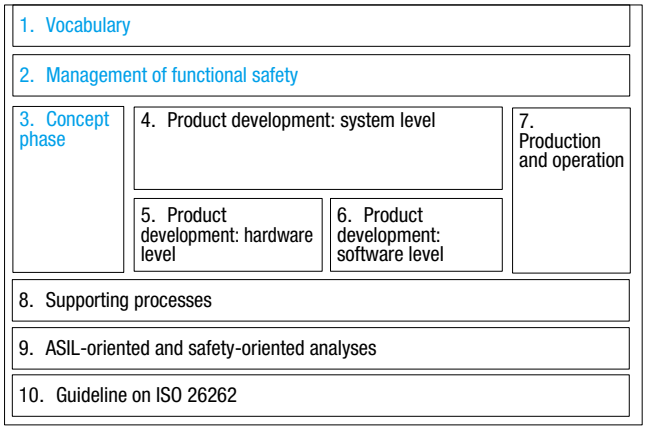

図1　ISO 26262の構成とメタモデル作成範囲

2 ISO 26262を分析しディペンダブルなコンシューマ・デバイスの実現に向けたポイントを抽出

コンシューマ・デバイスの標準化を検討するに当たり、まず先行する機能安全規格であるISO 26262を分析した。ISO 26262に限らず、このような規格は人によって解釈が異なることも多く、また概念の定義にとどまり、規格を実現するための具体的な実施方法まで規定されていないことが一般的である。そのため、ISO 26262の分析ではUML※2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では主にハザード分析※3に関する考え方やセーフティケース※4の記述に関する考え方、セーフティメカニズム※5の必要性、変更に関するイン

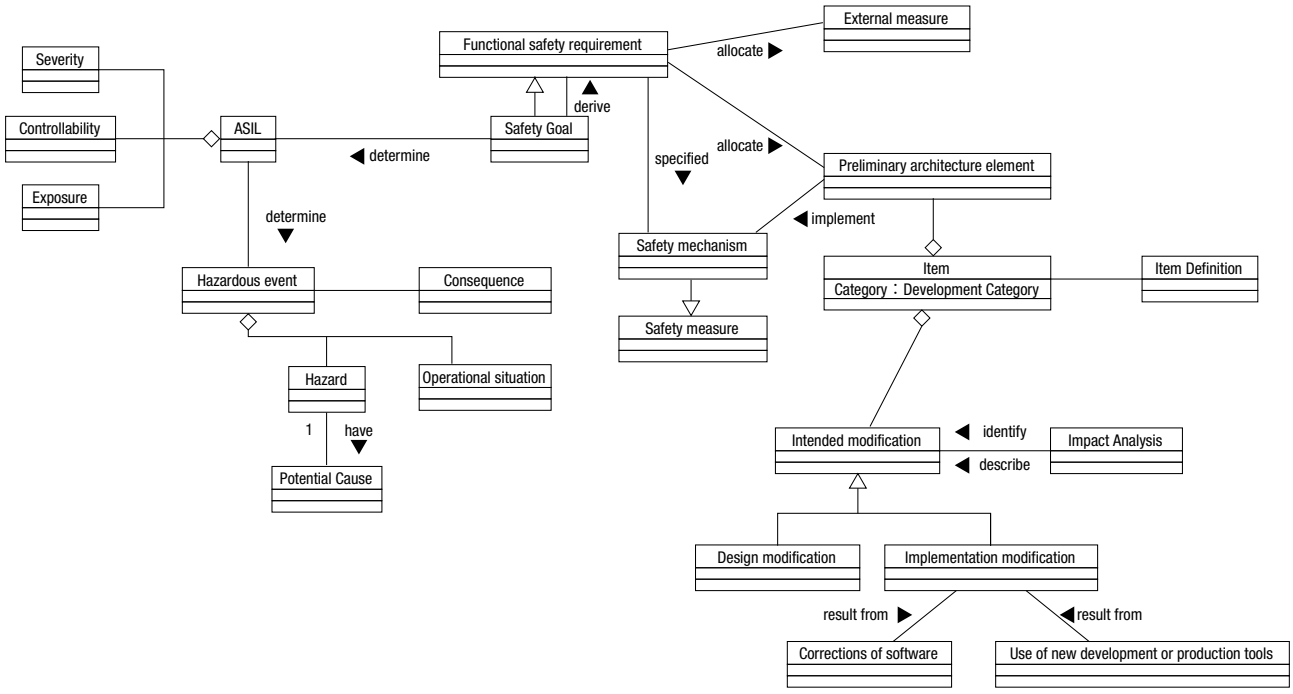

図2　ISO 26262　Part3のメタモデル

表2　コンシューマ·デバイスとISO 26262の比較

コンシューマ・デバイス	ISO 26262
ディペンダビリティ分析	安全分析
ディペンダビリティゴール※7	安全ゴール

パクト分析※6、さらにはProven in Use（使用実績による証明）に関する取り扱いなど､内容が盛り沢山である。とく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※8へと変更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、保全性などといったまさにコンシューマ・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。

日本の製造業の視点から見ても、およそ考え得るほとんどの種類のコンシューマ・デバイスが開発されてきている。規格とはなっていなくても、国内の企業は多くの知見、技術を有しており、コンシューマ・デバイスの標準化が行われた場合でも、諸外国と比べて優位性の確保が期待出来る。

またハザード分析やリスク分析については、その具体的な実施方法としてディペンダビリティケースに基づく記述も必要となる。

ディペンダビリティケースに関しては、日本発のディペンダビリティケースであるD-Case（JST※9のDEOS※10のプロジェクトで開発）を使用して記述することを検討している。

この技術は今後システムを開発する際に必須になると考えられているものであり、検討の結果D-Caseを推奨することとした。

Part4以降の具体的な開発段階に対する規格の検討ポイントとして、前述のディペンダビリティケースの具体的な利用方法をはじめ、ディペンダビリティゴールへのインパクト分析の方法、離散系と連続系が混在するモデルの記述方法、V&V※11手法など、日本の開発現場で実施されている技術を盛り込むことが挙がっている。また、長く日本型の製品開発において高品質を支えてきたイタレーティブ※12開発手法のエッセンスを適切に反映することも挙げられている。

3　IPA/SECでの標準化提案の状況及び今後の方針

IPA/SECではコンシューマ・デバイスを対象とした機能安全規格の検討を実施するに当たり、機能安全にかかわる有識者からなる委員会を設置し、前述のように検討を進めてきた。同時に成果の規格化についても視野に入れて活動を開始している。

規格の標準化と発行までには、相当な期間を要するため、前項Part3までの検討範囲については、前述したハザード分析やリスク分析の具体的な実施方法を盛り込んだ提案をまとめ、まずはOMG※13に対し提案を行っていく（2013年3月提案要請（RFP）として提出予定）。

OMG標準の規格は、「世間で一定の認知を得られている」、「他の組織の規格と比べ標準化に要する期間を短く出来る可能性が高い」、「OMGで標準化したあと、ISO化を行うときにファストトラックが利用出来る」という優位な面があることなどからこの方法をとる。またOMG側からも本取り組み内容に対して標準化の提案をするように要請があったことも背景にある。

今後は、実現のためのポイントとして挙がっている事項を再整理するとともに標準化に向けた戦略も具体化しながら活動を推進していく。

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　UML：Unified Modeling Language，OMG標準のオブジェクト指向ソフトウェアを記述するための言語
※3　ハザード分析：危害要因分析
※4　セーフティケース：ある環境のあるアプリケーションにおいて，システムの安全の的確性の議論と裏付けとなる証拠の書類。
※5　セーフティメカニズム：安全状態を達成または維持する目的で障害を検出または故障を制御するために必要となる技術的解決手段。
※6　インパクト分析：影響分析
※7　ディペンダビリティゴール：最上位のディペンダビリティ目標
※8　ディペンダビリティケース：ディペンダビリティに対する保証ケース
※9　JST：Japan Science and Technology Agency，独立行政法人科学技術振興機構
※10　DEOS：Dependability Engineering for Open Systems
※11　V&V：Verification & Validation
※12　イタレーティブ：iterative，反復
※13　OMG：Object Management Group

GSN で記述。
GSN（Goal Structuring Notation）は英国ヨーク大学の T. Kelly らが考案した、アシュアランスケース・安全ケースの分析、記述のための図式表現である。

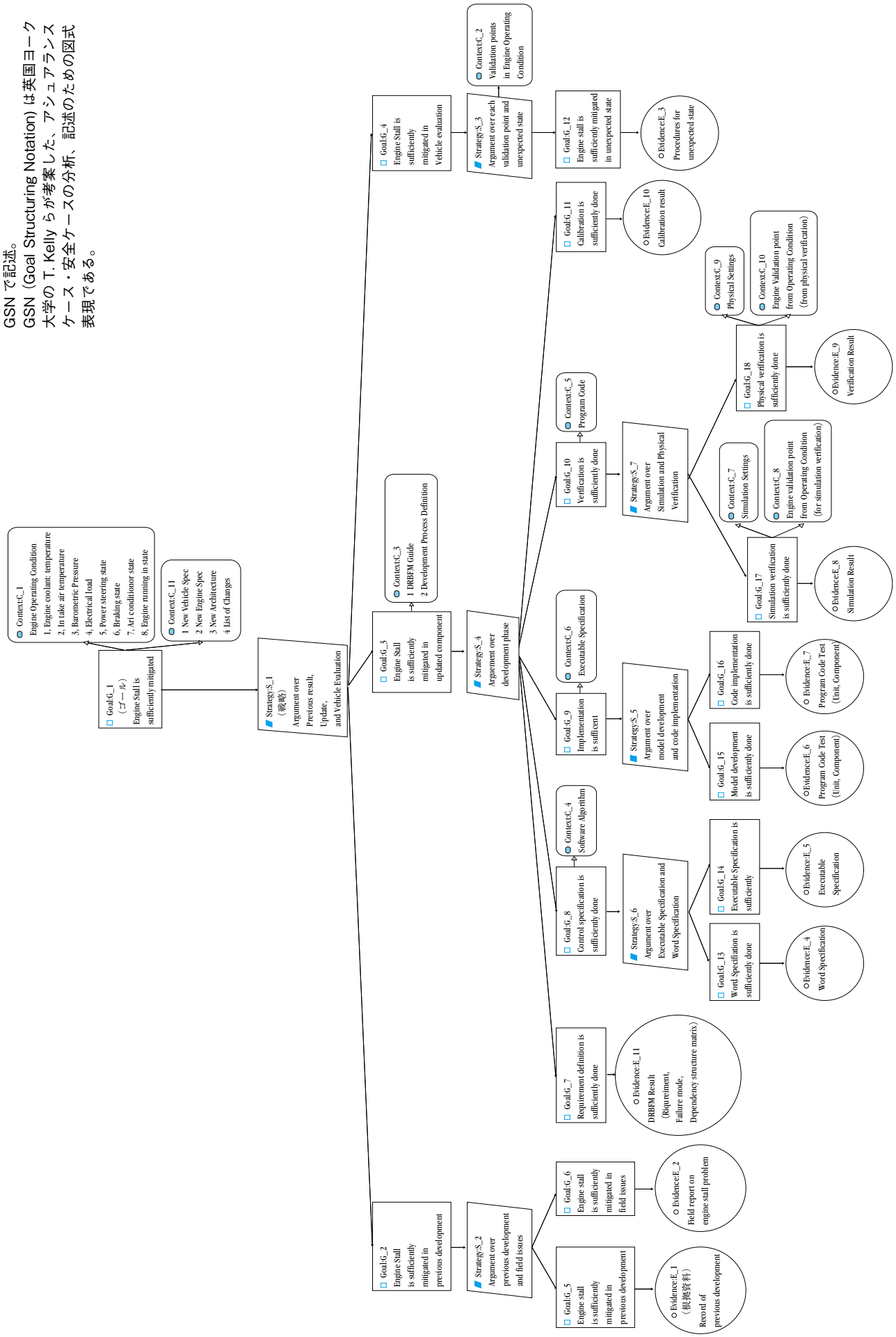

図3　エンストに関するD-Case（RFPドラフト版より）
D-Case参考:http://www.dcase.jp/introduction.html#a2