技術紹介

EPS開発におけるISO 26262対応への取組み

石　末　郁　人

1　はじめに

ISO 26262とは，2011年11月に国際規格として発行された自動車向けの機能安全規格である．規格の対象は，車両総重量が3,500kgまでの量産される乗用車に適用される電気・電子（以下E/E）システムである．

KYBで開発を行っている電動パワーステアリング（以下EPS）システムは，自動車の３つの基本機能[注1)]の１つである「曲がる」を担っており，要求される安全性のレベルも非常に高い．そのためシステムの安全性確保は，開発における最重要課題として位置付けられている．

本報ではEPS開発におけるISO 26262対応への取り組みについて報告する．

注１）「走る，曲がる，止まる」の３つの機能．

2　ISO 26262規格の概要

2.1　規格制定の背景

高機能化，複雑化するE/Eシステムが自動車に与える影響は増大しており，小さな１つの電子部品の故障が大事故の原因となることも考えられる．また分散開発が主流となり，グローバル化する調達体制の中で，各社個別の対応だけで自動車全体の安全性を確保するには限界がある．

グローバルで共通化された安全指標であるISO 26262は，それらの対策として策定された．

2.2　機能安全の考え方

「機能安全」という言葉は，英語の「Functional Safety」の日本語訳であり，規格において「E/Eシステムの機能不全のふるまいにより引き起こされるハザード[注2)]が原因となる，不合理なリスクの不在」と定義されている．すなわち，車載E/Eシステムの故障によるリスクを社会的に受け入れられるレベルまで低減することが求められる．

また「機能，部品が故障したとしても，安全機構によりシステムの安全性を確保する」という考え方をとっており，正しく動作することを求める品質とは異なる概念である．

注２）危険な事象．

2.3　規格の構成

ISO 26262は用語集，ガイドライン含め全10Partから構成されており，開発に直接関わるプロセスは，Part3のコンセプトフェーズからスタートする（図１）．Part3で導出されるコンセプト（車両）レベルの安全要求は，製品開発フェーズへと伝達される．製品開発フェーズでは，伝達された安全要求をPart4のシステムレベル，Part5のハードウェアレベル，Part6のソフトウェアレベルまで順に詳細化し，それらの安全要求を達成するための設計活動が実施される．

Part3は車両レベルの活動となるため，自動車メーカが実施するのが一般的である．システム設計を担当するKYBにおいては，Part4が主に対応する範囲となり，それ以降のPart5，Part6は協力会社へ開発依頼することが多い．

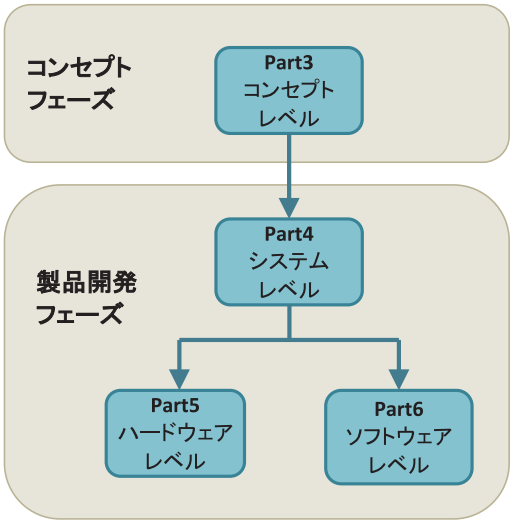

図１　開発に直接関わるプロセス

2.4　要求される安全性レベルとASIL

E/Eシステムに要求される安全性レベルはASIL[注3)]により定義され，開発から生産，影響があれば廃棄まで含め，自動車のライフサイクル全体を通して管理される．システムの機能不全により引き起こされる各ハザードは表1に示す3つの指標により評価され，「A」から「D」の4つのASILレベルに分類される（図2）．

E/Eシステムの開発において，ASILレベルに応じたプロセスの適用，安全の機能性能，品質目標といった基準を達成することが求められる．

表1　ASILの決定指標

指標	説明
シビアリティ	機能不全が引き起こす障害の大きさ（重傷，軽傷など）
曝露の確率	動作状況の頻度（高速走行をする状況など）
コントローラビリティ	危険を回避できる可能性（ほとんどのドライバが危険を回避可能など）

EPSシステムの代表的なハザードの1つにセルフステア[注4)]がある．車の走行中にセルフステアが発生すると，車の進む方向をドライバがコントロールすることが困難となり，車線の逸脱，大きな事故に至る危険性が高くなる．そのためEPSシステムでは，最も厳しいASIL Dでの開発が顧客より求められている．

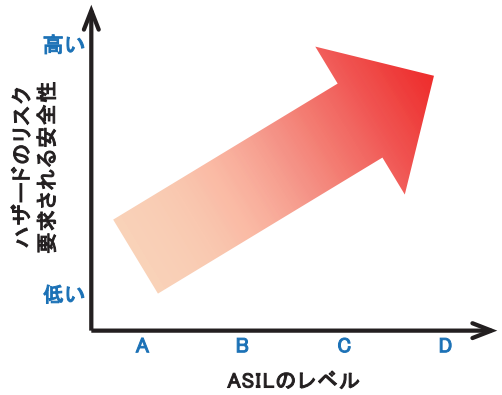

図2　ASILのレベルとリスク，求められる安全性

注3）Automotive Safety Integrity Levelの略．
自動車の安全度水準のこと．

注4）ドライバの意志に関係なく，車のハンドルが勝手に切れてしまう事象．

3　ISO 26262対応プロセスの構築

3.1　規格で要求されるプロセス

機能安全を達成するためには，正しく開発を行うための基準，開発プロセスの構築が組織として必要となる．規格に準拠した機能安全プロセスに加え，そのベースとしてISO 9001やISO/TS 16949といった品質管理プロセス（以下QMS）が要求される．

3.2　活動方針の決定

当部の所属する岐阜北工場の開発では，従来からISO/TS 16949に準拠したQMSを運用している．規格対応の課題を明確にするため，まず始めにこの既存のQMSとISO 26262とのギャップ分析を行った．

岐阜北工場で開発される製品は，油圧技術をベースとした機械製品が大半を占めており，E/Eシステムの開発はそれほど多くない．そのため既存のQMSは機械製品の開発に重点が置かれており，E/Eシステム，特にソフトウェア開発の観点において十分でないことが明らかになった．

そこで規格対応の活動方針として，ISO 26262に対応する新たな「機能安全マニュアル」と，既存のQMSをE/Eの観点で補完し，システム開発の全体を定義する「E/E開発要領」の構築を同時に進めることを決定した．図3に規格で要求されるプロセスと構築する社内プロセスの関連を示す．

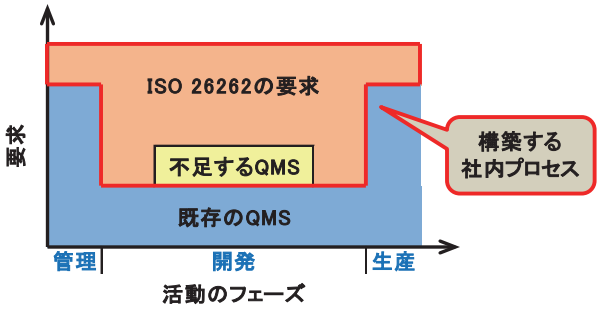

図3　規格で要求されるプロセスと構築する社内プロセス

3.3　機能安全プロセスの構築

3.3.1　機能安全プロセスの構造

新たに定義した機能安全マニュアルは，機能安全の活動を規定する最上位に位置する文書であり，そこから具体的な活動を定義した「規則・要領」，作成する成果物の「帳票・記述方法」，実際の活動成果となる「作業成果物」が順に参照される．これらは図4に示すピラミッド構造となっている．

3.3.2　E/E開発要領の作成

E/E開発要領では「既存のQMSで不足していたソフトウェア開発の観点」の補完に加え，機能安全

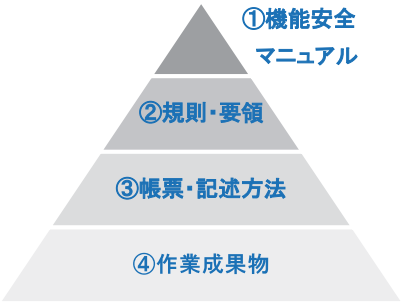

図4　機能安全プロセスの構造

マニュアルの要求を盛り込み，機能安全対応のE/Eシステムを開発するために必要なタスクをすべて定義している．各タスクでは「開始と終了の条件」，「入力と出力の文書」，「実施する活動内容」，「役割と責任」を明確にしている．図5に定義したE/E開発要領の一部を示す．

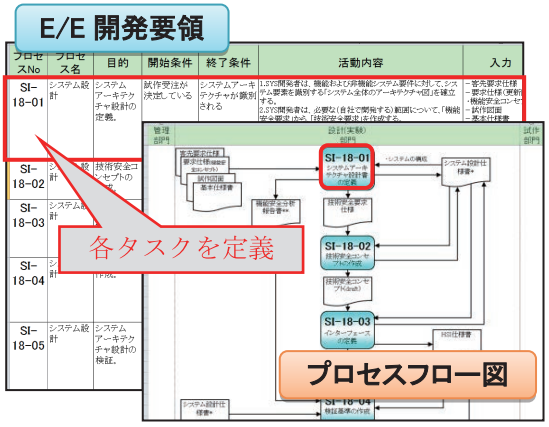

図5　定義したE/E開発要領

3.3.3　技術検討とガイドラインの整備

規格の要求を実行するためには，規格特有の概念，手続きの理解に加え，様々な技術的な解釈も必要となる．そこで部内に技術的な検討を行うワーキンググループ（以下WG）を立ち上げ，既存のEPSシステムを題材として，実際に規格で要求される成果物の検討，作成を行った．前述した通りKYBでの活動は規格Part4のシステム設計が中心となるが，上流の車両レベルでどのような検討がなされるのかを把握することは，それ以降の活動を正しく実施するために重要と考えられる．そこでWGの活動は，Part3及びPart4をメインの対象範囲として実施した．

一方で実際の開発担当者がプロセスを正しく，かつ効率的に実施するためには，プロセスの適用をサポートするガイドライン類の存在が欠かせない．WGでの活動成果をガイドライン，チェックリストとして登録することで，効率的な開発ができる環境を整備している（図6）．

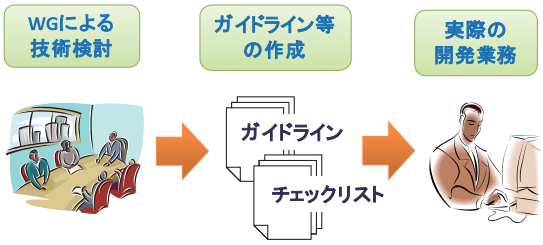

図6　WGの活動

3.4　アセスメントとプロセス改善

開発製品を機能安全に対応させる目的は安全なシステムを開発することである．そのため定義したプロセスを実際の開発に適用し，またそのプロセスが有効に機能していることを検証することが重要となる．

そのため実際の開発プロジェクトにおいて，プロセスの適用状況，成果物を評価し，その結果をプロセスの改善にフィードバックする仕組みを構築している（図7）．評価は規格で要求されているアセスメントに準拠する観点で行い，客観性を持たせるため外部コンサルタント会社の協力を得ながら定期的に実施している．

また客観性を持ったアセスメントを社内で実施するため，他部署によるアセスメント体制の構築，社内アセッサーの教育にも力を入れている．

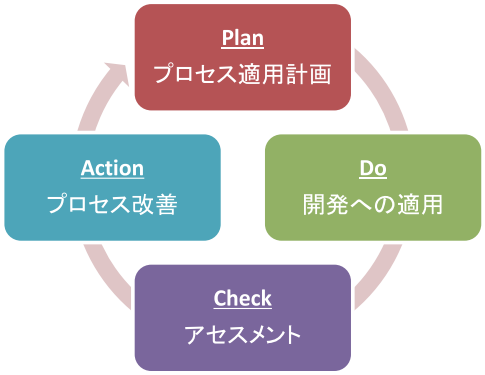

図7　改善サイクル

3.5　機能安全の教育

機能安全にかかわる業務の担当者は，規格の要求を正しく理解し，実践することが求められる．そのための教育の仕組みも重要となる．KYBでは社内で機能安全教育のプログラムを作成，担当する業務内容により受講が必要な教育を定義している．実際の機能安全対応のプロジェクトにおいてプロジェクトリーダが担当者を任命する際には，機能安全教育の受講記録を含め「必要な機能安全関連業務を遂行

する能力を有していること」の確認を実施している．

4 要求管理ツールの導入

規格Part3で導出された安全要求は，以降の各フェーズで詳細化される．これらの安全要求は不変ではなく，実際の開発において様々な要因から変更されることが頻繁に起こる．要求が変更された際には，変更が影響を及ぼす範囲，見直しが必要な活動，成果物を正確に特定する必要が生じる．そのため規格において，安全要求，各成果物に対して双方向のトレーサビリティ情報の管理が要求されている．これらの情報は「表計算ソフト」を利用するなどの方法で管理することができるが，管理する情報量が膨大となり，情報が複雑な関連性を持っている場合には限界がある．これらの情報を管理するためには，要求管理ツールと呼ばれる専用のツールが必要となる．専用ツールを利用した要求管理イメージを図８に示す．

KYBにおいても要求管理ツールの導入が現在進められており，現場導入のための運用ルールづくり，マニュアルの整備を行っている．

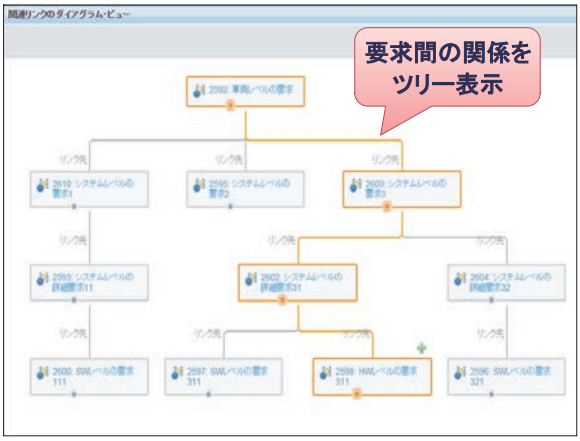

図８　専用ツールによる要求管理イメージ

5 おわりに

規格の発行を受け，各社プロセスへの対応は勿論のこと，新たな安全機能，技術の開発を加速させている．また規格の求める安全は絶対的なものではなく，社会情勢，技術の進歩にともない変化していく．最近では運転を自動化する「自動運転車」の開発も盛んに行われており，ステアリングシステムに求められる安全機能も大きく変化していくことが予想される．

これらの環境変化に対応していくため，構築したプロセスを活用しながら継続した技術開発を行っていく必要がある．

著　者

石末　郁人

1997年入社．オートモーティブコンポーネンツ事業本部 ステアリング技術部．電動パワーステアリングの設計，開発に従事．