機能安全（ISO26262）対応電動パワーステアリング用 ECU ハードウェアの開発

Development of ECU hardware for EPS conforming to Functional Safety (ISO26262)

伊藤健宏　T. ITO

The automotive safety standard ISO26262 (Functional Safety) was established in 2011, making compliance imperative for EPS, a main product of JTEKT. I will therefore introduce actual case examples of the application of functional safety within recent development of ECU hardware for EPS, with a focus on the newly added quantitative analysis of the fault of electronic components, and the development process that has been created.

Key Words: functional safety, ISO26262, hardware, process

1．はじめに

自動車分野の安全規格である ISO26262（機能安全規格）は，2011 年に正式に発行された．このため，当社の主要製品である電動パワーステアリング（EPS）でも対応が必須となったことから，今回 EPS 用 ECU ハードウェアの開発に機能安全を適用した事例について述べる．EPS は自動車の基本機能の『走る，曲がる，止まる』の内，『曲がる』を担う重要な部品で，特に誤動作は危険な状態に結びつくことから，機能安全規格の中で最も厳しい基準である ASIL-D（詳細は後述）を適用した開発が必要とされている．一方，自動車部品の機能安全開発を大きく分けるとシステム開発，ハードウェア開発およびソフトウェア開発に分けられる．システム開発とソフトウェア開発は，以前より Automotive SPICE の活動から開発プロセスの定義と改善が実施されているため，本報では機能安全対応として適用範囲を拡大した ECU ハードウェア開発について述べる．中でも，新規に追加された部品故障時の定量値分析を中心に紹介する．

2．EPS の ASIL レベル

ASIL レベルは**表 1** に示す三つの指標と，それぞれに定義される段階の組合せで決まる．

表 1　ASIL 決定の指標
Indices of ASIL determination

指標	内容	段階
Severity	影響度（人体への影響度）	4 段階 S0（小）～ S3（大）
Exposure	頻度（車両の使われ方の頻度）	5 段階 E0（小）～ E4（大）
Controllability	操作性（車両のコントロールの可能性）	4 段階 C0（易）～ C3（難）

図 1 に示すように，それぞれの指標の段階が 1 番大きい場合に ASIL が最も厳しい ASIL-D となり，1 段階下がるごとに ASIL のレベルも一つずつ下がる．

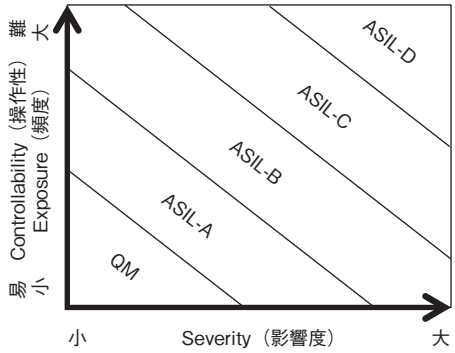

図 1　各指標と ASIL の関係
Relationship of each index with ASIL

EPS の例では，次項のように各指標が最も大きくなり，ASIL は機能安全規格の中で最も厳しい ASIL-D となる．

・Severity……EPS の誤動作で運転者の意図しない車両挙動に繋がる可能性あり S3
・Exposure……EPS の誤動作は頻度の高い車両の直進状態を考慮する必要があるので E4
・Controllability……EPS の誤出力で車両を操作が難しくなる状況があるので C3

2. ECU ハードウェア開発における機能安全対応の要求

EPS 用 ECU ハードウェアは**図2**に示す構成である.

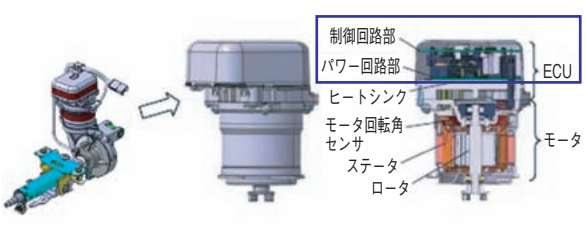

図2　ECU／モータ構造図
Structural drawing of ECU/motor

今回，ハードウェア開発における機能安全対応では，主に以下の 2 項目が定義された.
①安全目標（Safety Goal）を定義した安全設計
②ハードウェアの電子部品故障時の定量値分析

2.1　安全目標（Safety Goal）を定義した安全設計

自動車メーカが定義する車両レベルの安全目標の達成を証明する手段として，機能安全 V 字プロセスの遵守が必要となっている．V 字プロセスとは**図3**に示すように，安全目標からハードウェア開発とソフトウェア開発までのトレーサビリティを確保した開発である.

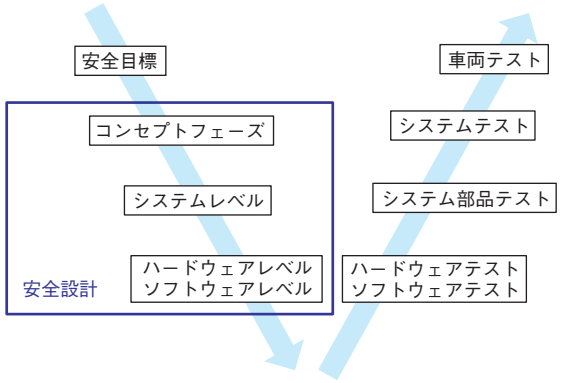

図3　機能安全対応の V 字プロセス
V-model of compliance with functional safety

具体的には，安全目標からコンセプトフェーズの機能安全要求／コンセプト（FSR/FSC），システムレベルの技術安全要求／コンセプト（TSR/TSC）と詳細化していき，技術安全要求／コンセプト（TSR/TSC）をインプットとしてハードウェアレベルとソフトウェアレベルの安全設計を実施している．本報の対象となるハードウェアレベルの詳細プロセスは，**3章**の「ハードウェア設計プロセス」で説明する.

2.2　ハードウェアの電子部品故障時の定量値分析

従来の開発では，電子部品故障時の FMEA は定性的なレベルで実施してきた．これに対し，機能安全規格ではハードウェアの電子部品故障時の定量値分析として FMEDA を実施し，以下の 2 項目の評価を要求されている.
①ハードウェアアーキテクチャメトリックの評価
　・安全目標ごとに算出される故障の検出確率
②ランダムハードウェア故障による安全目標侵害の評価
　・安全目標ごとに算出される時間当りの安全目標侵害の確率

この 2 項目を算出するため，**図4**に示すように従来の定性的 FMEA に部品故障率と安全機能による故障の検出確率を追加することで対応した．定量的 FMEA では部品故障率は部品の種類やサイズ，および環境温度などにより決まる数値で，安全機能による故障の検出確率は安全機能の検出手法により決まる確率である.

これらの項目を，**3章**の「ハードウェアの設計プロセスの⑧，⑨」に組込み標準化した.

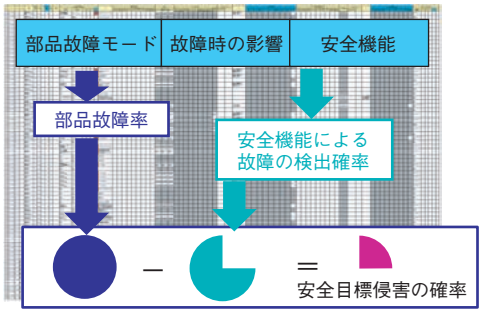

図4　定量的 FMEA のイメージ図
Conceptual drawing of constant FMEA

3. ハードウェア設計プロセスの構築

今回構築した，機能安全対応のハードウェア設計プロセスを**図5**に示す．

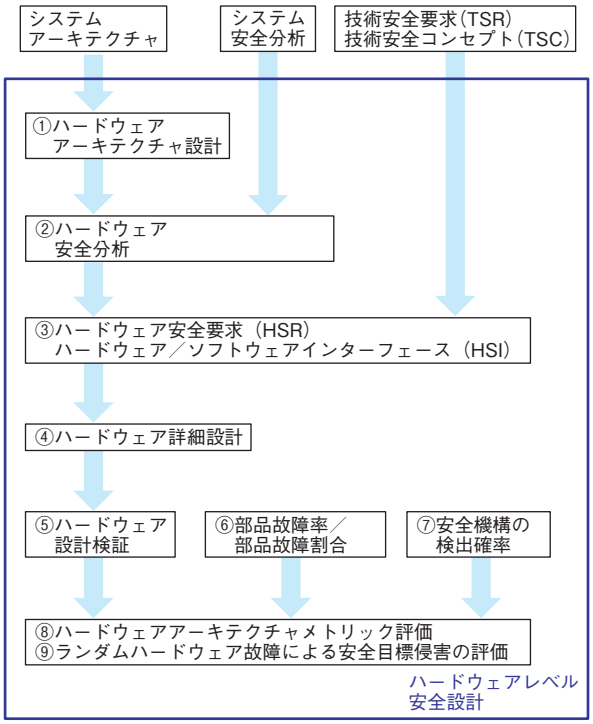

図5　ハードウェア設計プロセス
Hardware design process

以下，各工程ごとに定義した実施内容を説明する．

①ハードウェアアーキテクチャ設計
- システムアーキテクチャをインプットとし，ハードウェアアーキテクチャを設計する．

②ハードウェア安全分析
- システム安全分析をインプットとし，ハードウェアアーキテクチャの安全分析を実施する．

③ハードウェア安全要求（HSR），ハードウェア／ソフトウェアインターフェース（HSI）
- 技術安全要求（TSR）／技術安全コンセプト（TSC）をインプットとし，ハードウェア安全分析からハードウェア安全要求（HSR）とハードウェア／ソフトウェアインターフェース（HSI）を定義する．この中には，安全機構や FTTI（fault tolerant time interval）などが含まれる．

④ハードウェア詳細設計
- ハードウェア安全要求（HSR），ハードウェア／ソフトウェアインターフェース（HSI）をインプットとして，回路設計を実施する．

⑤ハードウェア設計検証（定性的）
- ハードウェア詳細設計で設計した回路に対して電子部品レベルの FMEA を実施し，安全要求に対して網羅的に安全設計ができていることを確認する．

⑥部品故障率／部品故障割合（定量値）
- ハードウェアの使用部品と故障率算出規格をインプットとし，各部品の故障率と故障割合を算出する．

⑦安全機構の検出確率（定量値）
- 各部品の故障を検出／処置をする安全機構の検出確率を算出する．

⑧ハードウェアアーキテクチャメトリック評価（定量値）
- 電子部品レベルの FMEA に部品故障率／部品故障割合と安全機構の検出確率を追加し，FMEDA を作成する．FMEDA から安全目標ごとのシングルポイントフォールトメトリック（SPFM）とレイテントフォールトメトリック（LFM）を算出し，評価を実施する．

⑨ランダムハードウェア故障による安全目標侵害の評価（定量値）
- FMEDA から安全目標ごとのランダムハードウェア故障の確率的メトリック（PMHF）を算出し，評価を実施する．

4. おわりに

今回，機能安全に対応した EPS 用ハードウェア開発プロセスを構築するとともに，製品開発を推進することができた．今後は改善活動を継続するとともに，EPS 用ハードウェア以外の電子部品についても，今回構築したハードウェア設計プロセスを展開し標準化していきたい．

筆　者

伊藤健宏*
T. ITO

*　自動車部品事業本部　第 1 電子技術部