ECU内のASILデコンポジション

ISO 26262 1st edition : 2011 が発行されてから既に 10 年程の時が経っていますが、2023 年となった今でも規格の解釈、プロセス構築などの困りごとを抱えていらっしゃる会社様が依然として多くいらっしゃいます。今回は ECU 単体で ASIL デコンポジションは成立するのかについて考察します。

ASIL デコンポジションとは？

ASIL デコンポジションは、元々一つのエレメントが担っていた安全要求を冗長かつ独立に分解し、それを複数のエレメントに割り当てることであり、より低い ASIL で開発が行えることがメリットです。要件は「冗長な安全要求」と「エレメント間の独立性担保」であり、独立性とはカスケード要因とコモンコーズ要因が存在しないことを指します。また表記のルールとしては元々与えられていた ASIL を分解後の ASIL にカッコ書きで記載する形になります。（図 1 参照）

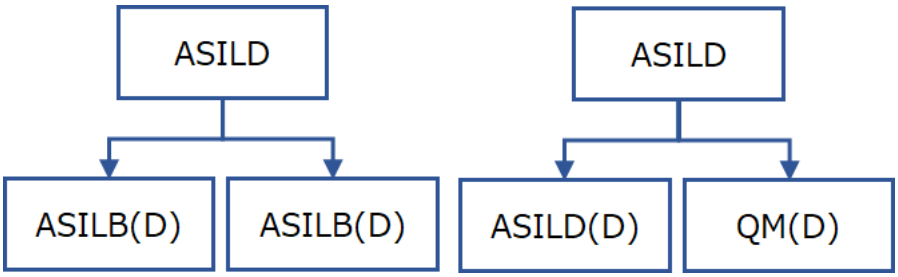

図 1 ASIL デコンポジションの例

ECU 内の ASIL デコンポジション考察

今回は ECU 等の部品内において ASIL デコンポジションは成立するのか、について考察していきたいと思います。シンプルな構成として「IF（=Intended Function）」と「SM（=Safety Mechanism）」の 2 つとし、IF 側のエレメントは高機能なマイコン、SM 側のエレメントはサブマイコンあるいはハードウェアであると仮定します。このとき、もし IF 側を QM(D)、SM 側を ASILD（D）という形でデコンポジションできるのであれば開発工数に対して多くの恩恵をもたらすはずです。

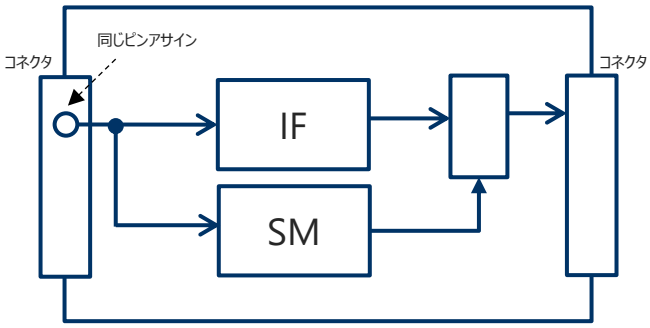

図 2　ECU 構成例

Copyright 2023 Business Cube & Partners, Inc. All rights reserved.

まず結論からですが、この例における ASIL デコンポジションは成立しません。図 2 の ECU 構成例では IF と SM が同じピンアサインとなっているため、コモンコーズ要因を解消できず、IF と SM 間でエレメント間の独立性を担保できないからです。このようにコネクタのピンアサインが指定されている、あるいは対向エレメント（センサなど）が 1 つしか存在しないなど、OEM 側で定められたシステム上の制約があるため、ECU 単独でのデコンポジションはできないということになります。

とはいえ ECU 開発において複雑なソフトウェアが実装された高機能なマイコンを持つエレメントの ASIL は下げて開発したいものです。ところが個々の部品、例えばマイコンの機能だけに頼る、また、単に監視機能を追加するアプローチを用いてしまい、かえってシステムが複雑になり疲弊してしまっている開発現場もあるのではないでしょうか。

話は変わりますが、機能安全規格の上位規格である ISO 12100 : 2010 ではリスク低減のための手法として「本質的安全設計」、「付加的保護方策」、「使用上の情報」を定義しています。機能安全対応は「付加的保護方策」だけであると捉えている方が非常に多くいらっしゃいますが、これは違います。高機能化、高性能化が進む中、今後も現場は限られたリソースで効率良く開発を進めてくことが求められます。今こそ「本質的安全設計」に立ち返り、取り組んでいくことが非常に重要であると感じています。

弊社では安全工学の各種技法を用いることでシステムを複雑化させることなく安全設計を行うコンサルティングサービスを提供可能です。ISO 26262 2nd edition : 2018 の実装支援トレーニングも実施していますので是非ご利用下さい。

本記事が読者様の一助となれば幸いです。

トレーニング（ISO 26262 機能安全実装支援コース）のご案内

弊社では ISO 26262 2nd edition の実装支援トレーニングを実施しています。車載 ECU システム開発（システム／ハードウェア／ソフトウェア）を担当するエンジニアが、これから ISO 26262 に対応した安全設計を実施して行くために必要な基礎知識の習得に有効なトレーニングコースです。貴社にてプライベート開催も実施可能です。是非、ご受講をご検討ください。

2023/6/28 山田 毅

※現在、一般開催のトレーニングは実施しておりませんが、プライベート開催は可能です。
プライベート開催のご希望はこちらからご連絡をお願いいたします。
トレーニングの詳細は以下の申し込みページからご確認いただけます。

トレーニングの申し込みページ
https://biz3.co.jp/publictraining_category/iso26262engineer

Copyright 2023 Business Cube & Partners, Inc. All rights reserved.