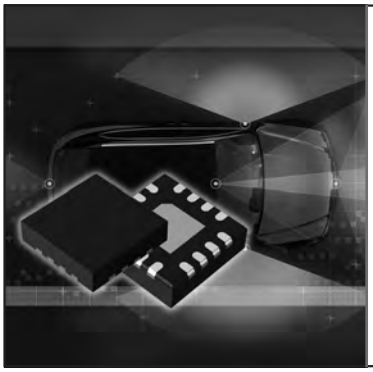
短期連載



安全の基本から規格書の構成と読み方，
設計フロー，最新動向まで

世界に負けない製品づくりに取り組む

車載向け電気/電子システムの機能安全規格「ISO 26262」入門

第4回 規格書の中身②：安全分析およびガイドライン

中嶋 崇順 Takayuki Nakashima

本連載では，自動車の電気/電子システム向けに策定された最新の機能安全規格ISO 26262を例に，製品づくりで安全性を担保する方法を解説していきます．

前回に続いて，実際の規格書の中身を具体的に見ています．今回は，安全分析およびガイドラインの内容について，Part9からPart10の内容を見ていきます．なお，Part9では1節から4節が，Part10では1節から3節が適用範囲や用語などの説明になっているので，それ以降から解説します．

1 安全分析

機能安全の達成を客観的に示すため，定性的，定量的な安全分析を実施します．

● 予備知識…安全目標のレベルを定義する「ASIL」

ISO 26262規格では，開発する製品のことを「アイテム」と呼びます．また，最上位の安全要求である「安全目標」を決定するなかで，ASIL(Automotive Safety Integrity Level；自動車用安全度水準)が定義されます．Dが最も厳しいレベルとなります．このASILは，傷害度(シビアリティ：S0～S3)，暴露の確率(エクスポージャ：E1～E4)，回避の可能性(コントローラビリティ：C0～C3)により，**表1**に従い決まります(S0またはC0の場合はQM)．

表1 ASILのレベル決定表
ISO 26262:2018，和英対訳版，Part3，より抜粋

S, E, Cのクラス		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	ASIL A
	E4	QM	ASIL A	ASIL B
S2	E1	QM	QM	QM
	E2	QM	QM	ASIL A
	E3	QM	ASIL A	ASIL B
	E4	ASIL A	ASIL B	ASIL C
S3	E1	QM	QM	ASIL A
	E2	QM	ASIL A	ASIL B
	E3	ASIL A	ASIL B	ASIL C
	E4	ASIL B	ASIL C	ASIL D

● Part9：自動車用安全度水準(ASIL)指向及び安全指向の分析

▶9-5「ASILテーラリングのための要求のデコンポジション」

1つのアイテムを複数のエレメントで構成し，それらのエレメントが十分に独立している場合は，「ASILデコンポジション」と呼ばれる特別な分割をしてよいこととなっています．

通常，開発中アイテムのASILは，アイテム全体にわたって適用されますが，この「ASILデコンポジション」を用いることによって，開発するエレメントのASILレベルを下げることができます．ただし，Part5の第8節，第9節で要求される，ハードウェアアーキテクチャメトリックの評価とランダムハードウェア故障による安全目標侵害の評価は，ASILデコンポジションを実施しても変更してはいけません．

● デコンポジション可能な分割例

ASIL D ⇒ ASIL C(D) + ASIL A(D)
ASIL D ⇒ ASIL B(D) + ASIL B(D)
ASIL D ⇒ ASIL D(D) + QM(D)
ASIL C ⇒ ASIL B(C) + ASIL A(C)
ASIL C ⇒ ASIL C(C) + QM(C)
ASIL B ⇒ ASIL A(B) + ASIL A(B)
ASIL B ⇒ ASIL B(B) + QM(B)
ASIL A ⇒ ASIL A(A) + QM(A)

例えば，ASIL Dの要求がASIL CとASIL Aにデコンポジションされた場合，ASIL C(D)，ASIL A(D)のようにカッコ内にデコンポジション前のASILを記します．

▶9-6「エレメントの共存に関する基準」

通常，エレメントが複数のサブエレメントから構成されているとき，それぞれのサブエレメントは上位のエレメントと同じASILレベルとなります．