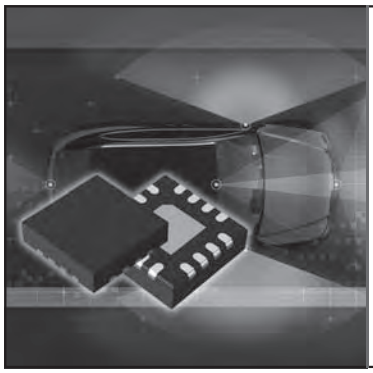
短期連載



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6回 設計時の安全分析

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．

今回は，機能安全規格を適用した設計をするときに必要な作業について解説します．

1 Tier1とのやりとり

● DIA（Development Interface Agreement：開発インターフェース協定）

ISO 26262規格では全部で109個の作業成果物が要求されます．例えば半導体メーカ（以下，サプライヤ）がISO 26262規格に準拠してICを開発する場合，Tier1とサプライヤのどちらがどの作業成果物を作成するかを事前に決めておく必要があります．このような情報をまとめたものをDIAと呼び，開発開始の段階からTier1とサプライヤの間でやりとりをします．

DIAの具体例は，誌面で紹介するには大きすぎるため，次のURLから参照できるようにしました．

https://toragi.cqpub.co.jp/Portals/0/support/2020/iso_dia.pdf

（提供：ローム）

表の左のほうに作業成果物が並び，それぞれの作業成果物に対してどちらが作成，実行，協働，情報の責任を負うか記載していきます．Tier1側の仕様に合わせて開発するカスタムICに近い場合は，Tier1側から要求という形でサプライヤ側に渡す場合が多く，汎用品に近い場合は，サプライヤ側からTier1に渡す場合が多いようです．

それぞれの責任分担については，以下のような分類にすることが多いようです．

- R：Responsible
  作成責任：作業成果物の作成に責任をもつ
- E：Execution
  実行責任：作業成果物に記述された作業を遂行する責任をもつ
- C：Cooperation
  協働責任：作業成果物に記述された作業を分担して遂行する責任をもつ
- I：Information
  情報共有：作業成果物に関する情報を多組織へ連絡する責任をもつ

2 Tier1に提出する安全分析のデータ

ISO 26262規格では，アイテム全体の機能安全を達成していることの証明のために，定量的な安全分析が求められます．ICの内部回路は複雑なので，Tier1ではICの安全分析を行うことが困難であるため，サプライヤからICのFIT値やFMEDAなどを提出する必要があります．

● FIT値（Failure In Time）

故障率を示す単位のひとつで以下の式で表されます．

$$\text{平均故障率} = \frac{\text{稼働時間中の総故障数}}{\text{稼働時間} \times \text{稼働数}} = \frac{1}{10^9} = 1\ \text{FIT} \quad \cdots\cdots(1)$$

1 FIT = 10^{-9}/h，つまり1時間あたり10^{-9}個の故障が発生することになります．言い換えると，100,000個のものが10,000時間稼働した場合に1個不良が出ることになります．半導体製品のように，大量生産され故障率が極めて低い製品によく用いられます．

このFIT値を算出する方法として以下の3種類が規格書に示してあります．

> Part5-8.4.3 ハードウェア部品の故障率の見積もり
> 分析に使用するハードウェア部品の故障率の見積もりは下記a），b），c）のいずれかの手段で算出する．
> a）認知された産業界情報源からのハードウェア部品の故障率データを使用する
> b）市場返却品又はテストに基づく統計を用いる．この場合は少なくとも70％の信頼度を有することが望ましい
> c）論証に基づくエキスパートの判断を使用する