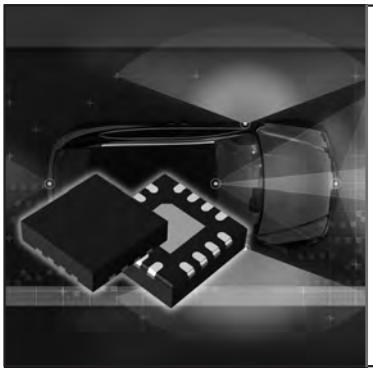
短期連載



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5回 規格書の中身③：安全分析およびガイドライン（つづき）

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きます．**図1**に示すのは，ISO 26262の全体構成です．

今回は，半導体のガイドラインの内容についてPart11の内容を見ていきます．なおPart11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 ガイドライン（つづき）

● Part11：半導体へのISO 26262適用のガイドライン

Part11は2nd Editionになって新しく追加され，我々ユームのような半導体メーカが，ISO 26262規格に準拠して設計をする際に参考となることが細かく記載されています．他のどのPartよりも分厚く（なんと178ページ！），すべてを理解するのは大変な作業となりますので，まずは必要な項目から見ていくとよいでしょう．

▶11-4「半導体コンポーネント及びその分割」

●11-4-1「半導体コンポーネントの考え方」

半導体コンポーネントをISO 26262規格に準拠して開発する場合，顧客が開発するアイテムの一部として安全目標から導出されたハードウェア安全要求に基づいて開発します．半導体コンポーネントに割り当てられた目標値に基づいて安全分析を実施する必要があります．

システムを想定した安全機構をもつ半導体コンポーネントであるSEooC（Safety Element out of Context）として開発することもできますが，この場合はアイテムの安全目標から導出された安全要求を想定する必要があります．

●11-4-2「半導体コンポーネントの部品への分割」

半導体コンポーネントは，CPU（Central Processing Unit；中央処理装置）やADC（Analog-to-Digital Converter；A-Dコンバータ）などの内部ブロックを部品として捉えることができます．

●11-4-3「フォールト，エラー，故障モードへの分配」

半導体コンポーネントにおいても**図2**のようにフォールトはエラーを引き起こし，そのエラーは故障に至

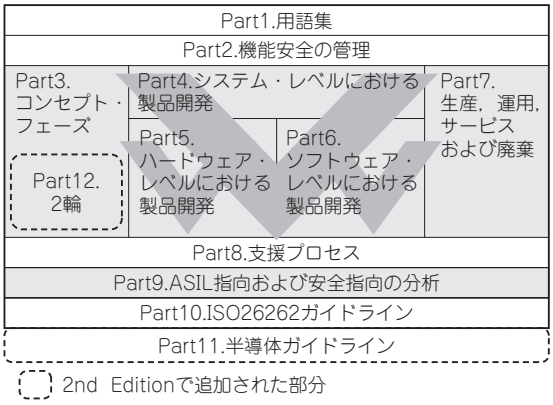


図1 自動車の電気/電子システム向け機能安全規格「ISO 26262」の全体構成

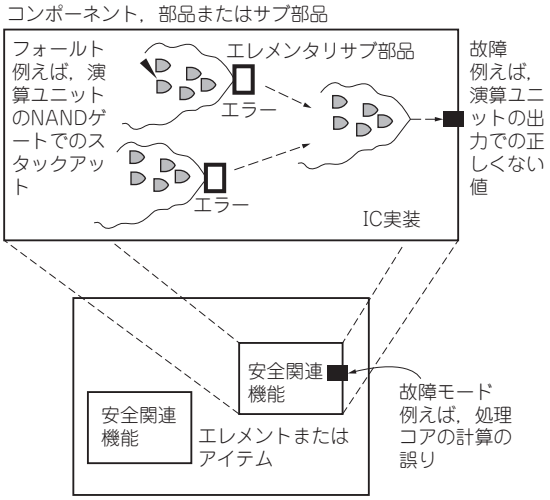


図2 半導体におけるフォールト（障害）やエラーと故障の関係

ISO 26262:2018，和英対訳版，Part11 図3-ハードウェアのフォールト及び故障モードの関係，より抜粋