ISO 26262（自動車の機能安全に関する規格）

ISO 26262、この夏国際規格へ

2011年夏ごろ国際規格として発行される予定のISO 26262は、自動車の安全制御に使われる電子回路の信頼性を評価する規格で、自動車産業が対象となるため、わが国でも大きな関心を呼んでいます。この規格の発行に至る経緯と規格の概要をご紹介します。

認証制度開発普及室
室長　浅田純男

参与　櫛山哲郎

副主査　神賀 誠

自動車の安全を制御する電子システムの信頼性を評価する規格

ISO 26262は、自動車に搭載された電子制御部品の機能安全を評価する国際規格です。現在、FDIS(最終ドラフト)の段階で、この夏頃に国際規格として発行される予定です。

現代の自動車は、数多くの電子回路でさまざまな機能を制御しています。エンジンの回転数を適切な状態にしたり、ブレーキをかけた時にタイヤがスリップするのを防いだり、間欠ワイパーの動作をコントロールしたりといった機能は、すべて電子回路によって制御されています。今や自動車の安全性を議論するうえで電子回路の信頼性の確保は必要不可欠なものになっているのです。しかし電子回路は、機械部品のようにハードウェアのみで作られているのではなく、ハードウェアとソフトウェアが組み合わせられたシステムであり、信頼性を高めるためにはそのシステムが正しく作られているかどうかのマネジメントも評価の対象にする必要があります。ソフトウェアには、いわゆる「バグ」と呼ばれる「ある条件が整えば必ず起きる不具合」があります。それを防ぐには、開発段階からの管理(マネジメント)に頼るしかないからです。そのため欧米の自動車会社を中心として、国際的な安全規格を求める声が高まりました。

一方で、1990年代の末にヨーロッパを中心として「機能安全」という考え方が発展してきました。この機能安全のベースとなる国際規格としてIEC 61508が知られていますが、この規格はもともと多発する大規模プラント事故に対応するために作られたものです。このIEC 61508を元にして、自動車や自動車産業にマッチした機能安全規格を作ろうという動きが起き、構想されたのがISO 26262です。

欧米メーカーが綱引きして策定

「機能安全」というのは耳慣れない言葉ですが、英語の「Functional Safety」を直訳したもので、「本質安全」との対比で説明するとよくわかります。

たとえば自動車にはワイパーがあり、雨や雪の時はこれを作動させて視界を確保します。この時、ワイパーという機能を使って安全を確保しているわけで、必要な時にワイパーという安全機能を維持することが「機能安全」です。

しかし、水を弾く特殊な窓ガラスをフロントウインドーとした自動車を考えてみると、雨が降っても視界は雨滴に妨げられません。この場合、ワイパーという機能に頼らなくても視界という安全が確保できています。こういうものを「本質安全」といいます。

ほかによく引用される例としては、交通を分離して本質的に安全を確保する立体交差と、信号という機能によって安全を確保する踏切があります。

ISO 26262は自動車の安全に関わる電気・電子システムを対象にした規格ですが、その策定は最初にヨーロッパの自動車メーカーが主導で進め、のちにアメリカが主導権を握って進められたといわれています。

IEC 61508との関係ですが、評価の対象がハードとソフトとマネジメントであるという点や、細分化と具現化の間で検証を行っていく「Vモデル」など、基本的な考え方はIEC 61508を踏襲しています。しかし、規格の詳細な内容は、自動車用電子部品の安全性確保に必要な要件を一から構築したもので、従来の機能安全の規格とは多くの部分で異なっています。

例えば、IEC 61508には「SIL(safety integrity level=安全度水準)」という概念が安全性の指標として導入されていますが、ISO 26262ではこれを根本的に改めた「ASIL(automotive SIL)」を採用しています。両者は名前こそ似ていますが考え方は大きく異なっており、SILに多く見られる確率論的な要素がASILでは排除され、より使用実績や品質管理を重視した考え方に置き換えられています。具体的には、ハザード（潜在的な危険）ごとに、「被害の深刻度」「発生頻度」「運転者など安全装置以外による回避容易性」の3つの要素からASILを4段階に規定し、それぞれに応じた安全方策の評価方法や管理方法が書かれています。これらは、プラントという大規模で数が少なく、高度な訓練を受けた専門の運転員が操作するものを対象にした規格と、自動車という大量生産品で一般大衆がユーザーであるものの違いが反映された結果といえるでしょう。

ISO 26262の適用範囲ですが、自動車といってもバスやトラックのような大型車は除外されていて、総重量3.5tまでの乗用車で、運転手も含んだ乗員8名までのものだけが対象になっています。また、自動車用電子部品であっても、自動車の安全性に関係しない部品は規格の対象になりません。

将来的には、IEC 61508をベースに家電品など他の量産品の機能安全規格も制定が予定されています。

ISO 26262が自動車メーカーの取引要件に

欧米主導で策定が進められたISO 26262ですが、過去の例から見ても、国際規格として発行されればISO/TS 16949と同様に自動車メーカーとの取引要件となる可能性が高いでしょう。少なくとも、欧米の自動車メーカーに部品を納入する際には、必須要件になっていくと考えられ、実際に自動車メーカーから対応の準備を指示された部品メーカーも出てきているようです。

ISO 26262によって自動車産業界は、部品メーカーと自動車メーカー間の意思疎通、つまり情報のやりとりに国際的なルールがもたらされます。それによって安全情報の共有化がなされれば、最終製品においてより高い安全性が確保されるようになるでしょう。

ちなみにISO 26262は10部で構成されており、全体では非常に内容の厚いものになっています。今から読んで参考にしたい場合は、第10部の「ガイドライン」を先に読むことをおすすめします。ガイドラインに目を通してから、関心のある部分へと読み進めればよいでしょう。

JQAは、IEC 61508をベースとした「機能安全評価サービス」の一環として、ISO 26262に関するサービスも提供いたします。

JQAの「機能安全評価サービス」は、製品のライフサイクルに沿って機能安全マネジメント（KAM）評価・認証、設計コンセプト評価・認証、製品評価・認証という3段階で構成され、KAM認証単独で、あるいはKAM認証取得後に設計コンセプト認証だけを取得することも可能です。もちろん、3つすべてを取得されることが理想です。

JQAではISO 26262のみならず機能安全全般について、お客さまへの技術情報提供もサービスの一環として用意しておりますので、どうぞお気軽に認証制度開発普及室までお尋ねください。

■ ISO 26262に関するお問合せ先

認証制度開発普及室
TEL: 03-6212-9225 (代)
（浅田／櫛山／神賀）