機能安全への取り組み

機能的に工夫して安全を確保

「機能安全」とは、安全な製品開発のために有効と考えられる管理や手法適用を定めたものです。

機能安全の分かりやすい説明として、日本電気制御機器工業会（NECA）の技術委員会の報告書で記されている踏切の例がよく使われます。列車と車両などとの事故の危険性がある踏切で安全を確保するためには、立体交差にすれば踏切上で両者が接触・衝突する可能性は排除できるという「本質安全」の考え方があります。これに対し、踏切に警報機や遮断機を設置する、といった安全機能の導入により許容できるレベルの安全を確保することを機能安全と呼んでいます。

1990年代末にヨーロッパなどで策定され、10年余り前から日本でも注目されるようになった機能安全規格ですが、国際規格であるIEC 61508をベースとしており、製品カテゴリごとの安全規格があります（**図-1**）。自動車分野向けには2011年11月にISO 26262がリリースされました。ISO 26262はPart1～10に分かれ、マネジメントからハードウェアを含めたエンジニアリング、構成管理などのサポートプロセスなど、広範囲の安全に関わる要求が規定されています。

車載メーカーでは初期段階の規格対応はすでに一巡し、発展期に入っています。IPA(独立行政法人 情報処理推進機構)や車載に関わる団体の一つである一般社団法人JASPAR (Japan Automotive Software Platform and Architecture) では安全分析(STAMP/STPA)、安全設計のデザインパターンなどの新たな取り組みや、セキュリティを含めた開発プロセスの検討を行っています。当社もこれらの団体に参加し発展に寄与するとともに、得られた成果を社内標準プロセスなどにフィードバックし活用しています。

ISO 26262は、2018年には2nd Editionに更新される予定です。半導体の要求の充実、大型車や二輪車といった乗用車以外への適用拡大、自動運転などの時代を見据えた安全要求の見直しなどが盛り込まれる見込みです。

図-1　IEC 61508から派生した個別の安全規格

車載機器ビジネスの実績に安全をプラス

当社では車載関連の開発を長年行ってきましたが、ここ数年、機能安全に関わる開発が急増してきました。機能安全ではハザードやリスクに関して安全分析を行いますが、既に保有する製品知識や経験だけでは十分とは言えず、機能安全に対する正しい知識が必要となります。そのため数年前から機能安全教育を行い、現在までに200名を超える技術者を育成してきました。

受託開発ではお客様の開発プロセスの適応を求められることが多くありますが、各社・部署毎に考え方や粒度が異なります。本教育により、開発メンバー全体が同じ知識ベースでお客様のさまざまな要求に応えられ、安全・品質向上を実現できることが当社の強みとなります。また、事業部幹部・営業を含めた教育も実施し、機能安全開発の難しさや組織の役割を理解し開発に取り組んでいます（**図-2**）。

(エンベデッドシステム事業部　市川 一夫)

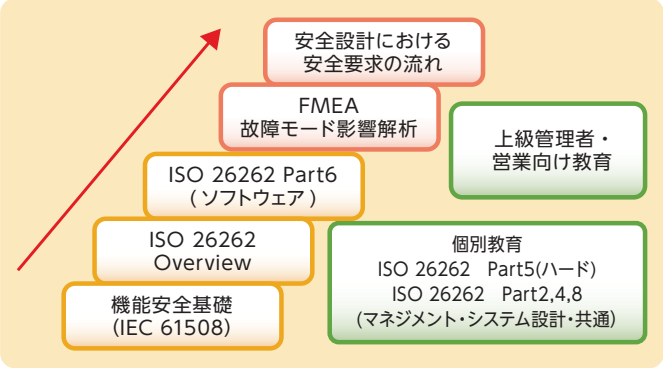

図-2　機能安全教育コース