TOPICS

適用範囲を拡大する機能安全

1. はじめに

交通システムや社会インフラ設備の安全関連部は，故障や誤不動作を起こさないよう機械的なフェイルセーフ機構で構成されていた．その後，1999年のIEC61508「電気／電子／プログラマブル電子装置の機能安全」規格の制定により，マイコンやソフトウェアを用いて安全回路を構築できるようになった．今では，自動車の自動ブレーキ装置や洗濯乾燥機の扉ロックなどに，機能安全技術が広く適用されている．本稿では，機能安全技術の分野展開の状況について解説する．

2. 機能安全とは

多数の乗客を預かる鉄道システムでは，高速化や効率化のために高信頼かつ高性能な信号システムや保安装置が必要となるため，安全制御系の電子化が進んでいた．また，石油化学プラントでも大規模爆発事故を防ぐための安全計装システムが開発された．IEC61508:1999は，それらの分野で蓄積された電子安全技術の集大成であり，いまでは機械，自動車，家電にまで幅広い適用が進んでいる（**図1**）．

機能安全規格の要求を列挙する．

(1) SIL（Safety Integrity Level）－システムに潜む危険源について，その被害規模と事故確率からリスクを見積もり，対策に必要な安全レベル（SIL）を決定する．SILごとに，以降の要求内容が詳細に定義されている．

(2) 体系的故障のない開発プロセス－体系的故障とは，設計ミスあるいはバグであり，それが極力発生しないように安全関連の品質管理を行う．

(3) ハードウェア信頼性－故障には，フェイルセーフとなる安全側故障と安全機能不全である危険側故障があり，危険側故障についてSILごとに定量的要求が決められている．

(4) ソフトウェアによる診断－上記(3)の定量的要求を満足するために，SILごとに安全回路の診断手法が決められている．

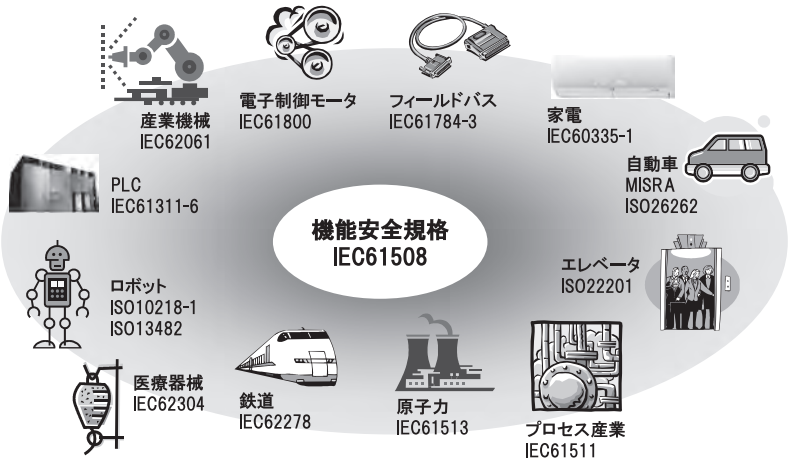

図1　機能安全の分野展開

機能安全の導入が難しいとよく言われるのは，(1)から(4)の要求事項が，安全基準，開発プロセスの見直しおよび新技術の導入を同時に伴うからである．

3. 機能安全の導入効果

当初，多くのメーカは安全規格への適合はコスト要因と考えて，機能安全技術の導入は消極的であった．ところが，機能安全すなわち安全制御のプログラム化は，安全装置のコンパクト化と省コスト化，安全装置の高性能化による製品高性能化，安全制御詳細化による運転効率向上などの効果を生んだ．

たとえば，機械設備の場合，従来は非常停止で制御盤全体の電源遮断により安全確保することが一般的であった．ところが，人に危害を与える箇所だけ電源遮断すれば安全確保できるので，安全PLC（Programmable Logic Controller）を用いた安全制御が導入されるようになった．安全PLCを用いることで，無駄な設備の停止を抑制し，非常停止からの復旧を迅速にできる．さらに，機能安全対応の安全センサや安全駆動装置との組合せによって，きめ細かい安全制御を省コストで実現できる．すなわち，機能安全により安全性と生産性を両立できるので，機械設備への機能安全の導入は注目されている．

4. 機能安全の教育制度

2章に示したように，機能安全は広く体系的な専門知識を必要とし，さらに開発要員にそれぞれの能力要件の管理を求めている．これまで，これらを満足できる教育カリキュラムは国内に未整備であった．そこで，（一財）日本規格協会は，機能安全の実践的カリキュラムを構築し，2013年から「JSA機能安全セミナー」の運用を開始した．本講習の修了者は，安全関連ハードウェア，ソフトウェア開発要員として十分な能力を持つとみなすことができる．主な認証機関も，本セミナーが要員の能力認定として有効であると認めつつある．2015年冬と夏に実施を計画しているので，興味のある方は聴講いただきたい．

5. おわりに

大事故や人命に関わる安全制御をプログラマブル機器により実現する機能安全規格は，安全化だけでなく，安全を担保したうえで機械の性能向上や効率化を可能とする重要技術である．日本規格協会など，機能安全導入に直接効果のあるカリキュラムの運用も始まった．日本のお家芸である安全・安心にさらなる磨きをかけるためにも，機能安全技術の導入はますます加速するであろう．

（原稿受付　2014年9月19日）

〔神余浩夫　三菱電機（株）〕