計装豆知識

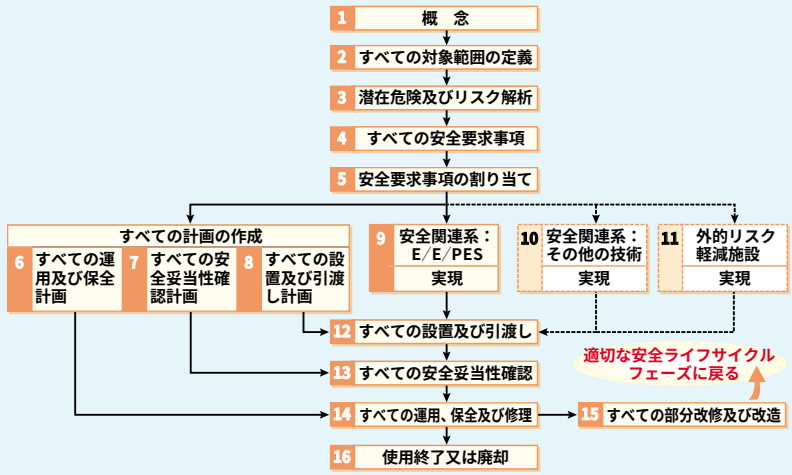
機能安全とIEC規格61508について(1)

最近、「機能安全」や「SIL」という言葉を耳にされる方が多いと思います。今月から4回にわたって、電子機器を用いた機能安全に関するIEC規格61508[注1)]について簡単に説明します。

今日、PLCなど多数の電子機器がシステムの制御の目的に使用されていますが、それに加えて、システムの安全確保に関連する分野でも電子機器が使用される例が増えてきました。説明のための簡単な例として、ボイラの圧力を制御するため、圧力センサの値と目標値を比較し、燃料弁などを調整する制御システムを想定します[注2)]。また、万一の異常事態に備えて、安全弁や防護壁を設け、さらに圧力センサで異常を検知した場合に燃料系統の緊急遮断弁を閉じるシステムを想定します。このような異常事態に備えるシステムを安全関連系と呼び、それに対する要求事項を規定しているのが、IEC 61508「Functional safety of electrical/electronic/programmable electronic safety-related systems[注3)]」です。この規格の中では、機能安全を「EUC[注2)]とEUC制御系の全体に関する安全のうち、E/E/PE[注4)]安全関連系、他技術安全関連系及び外的リスク軽減施設の正常な機能に依存する部分」と定義しています。

上記のボイラ制御を例にすると、圧力異常を検知し燃料弁を緊急遮断するシステムが、E/E/PEで構成されている場合に、この規格の適用対象になり、安全弁や防護壁は規格の対象外です。また、安全関連系で使用される機器自体に起因する危険(たとえば、機器に触れての感電)や故意の働きかけ(たとえば、テロリストによる破壊活動など)も適用対象外です。

IEC 61508では、安全関連系の構想段階から設計・開発を含め保守・廃棄に至るまでを16のフェーズに分け、それぞれのフェーズ毎に要求事項が決められています。なお、この体系を「全安全ライフサイクル」と呼んでいます(**図1**参照)。フェーズ1～4[注5)]の段階では、EUCおよびEUC制御系に異常があった場合のリスクを分析し、リスクを軽減するために必要な安全要求仕様を決定します。フェーズ5にて、安全関連系の機器や施設に安全要求機能を割り当て、各安全機能に対して安全度水準(SIL＝Safety Integrity Level)を割り当てます。フェーズ6～8では、設置から保守に至る工程で安全を維持するための計画を策定し、フェーズ9～11では要求されたSILを実現します。エム・システム技研の信号変換器に代表される計装コンポーネントに対しては、フェーズ5で必要なSILが割り当てられ、フェーズ9で実現されます。フェーズ10はボイラの例では安全弁に、フェーズ11は防護壁にそれぞれ該当しますが、この規格の対象外です。しかし、全安全ライフサイクル中で、安全要求機能を割り当てる対象のフェーズとして記述されています。フェーズ12～16では、設置から廃棄に至る工程での安全を維持します。 ■



備考．ボックス10とボックス11は、この規格群の対象外である。

図1　全安全ライフサイクル

注1) IEC 61508シリーズは61508-1～61508-7の7部構成となっています。なお、この規格は基本規格であり、この規格を基にして特定分野を対象とする規格も制定されています。たとえば、プロセス制御には安全計装に関する規格61511があります。

注2) この場合、ボイラをEUC(Equipment under control)、制御システムをEUC制御系と呼びます。

注3) 「電気・電子・プログラマブル電子系の機能安全」と訳し、下線表示部を「E/E/PES」と略します。

注4) Electrical/Electronic/Programmable Electronic(電気/電子/プログラマブル電子)の略。

注5) フェーズの名称は、**図1**の各ボックス内に示されていますが、紙幅の関係上、本稿では番号で呼びます。

【(株)エム・システム技研　開発部】