再発見！新発見！

計装豆知識

役立つ知識が粒揃い!!

機能安全とIEC規格61508について(4)

先月に引き続き、機能安全を規定しているIEC規格61508について説明します。

今月は、フェーズ9[注1)]、「E/E/PE[注2)]安全関連システム：実現」について説明します。フェーズ9の要求事項の目的は、E/E/PES安全要求事項仕様書に適合するE/E/PE安全関連システムを構築することです。ハードウェアに関する要求は、IEC 61508-2に、ソフトウェアに関する要求は、IEC 61508-3に詳細が書かれています。ここでは、ハードウェアに関する要求について説明します。フェーズ9のハードウェアに関する安全ライフサイクルは、本稿の**図1**に示すようにさらに細かく分けられています。

フェーズ9.1：各々のE/E/PE安全関連系に対して、要求する機能安全を達成するために、フェーズ5で割り当てられた安全機能と安全度水準(SIL)によって、要求事項を定めます。

フェーズ9.2：E/E/PE安全関連系による安全性の妥当性確認を計画します。このフェーズは、通常E/E/PESの設計および開発に平行して実施されます。

フェーズ9.3：E/E/PE安全関連系に対して定められた安全機能および安全度に係る要求事項に適合するように、当該安全関連系のハードウェアを設計し開発を行います。このフェーズでは多くの要求があり、ここではそのすべてを説明できないため、以下に一部を紹介します。

- 設計の文書化
- 自己診断率、プルーフテスト間隔の決定
- 安全度水準(SIL)に応じた検出できない危険側故障の割合
- FMEDA（Failure Modes, Effects and Diagnostic Analysis）による故障解析

IEC 61508の特徴として機器の故障は、ランダムハードウェア故障（random hardware failure）と決定論的原因故障（systematic failure）に分けられます。ランダムハードウェア故障とは部品の劣化などによる偶発的な故障であり、決定論的原因故障とはシステムの仕様や運用方法に起因する故障です。これら2つの故障に対しては異なるアプローチをとります。ランダムハードウェア故障に対しては故障確率によって定量的に、決定論的原因故障に対しては安全ライフサイクルに基づいた手順と文書化により定性的に対処します。

フェーズ9.4：E/E/PE安全関連系の統合およびテストを行います。E/E/PE安全関連系は、フェーズ9.3で定められたE/E/PES設計に従って統合し、また定められたE/E/PES統合テストに従ってテストします。PESへの安全関連系ソフトウェアの統合は、IEC 61508-3の7.5項に従って行われます。ここでは、E/E/PE安全関連系の統合テストの文書化が要求されます。その中では、当該テスト結果および設計と開発とのフェーズで定めた目的と基準に適合しているかどうかを明示しなければなりません。

フェーズ9.5：E/E/PE安全関連系に要求する機能安全が、運用と保全の期間中に保持されることを確実にするための手順を確立します。

フェーズ9.6：E/E/PE安全関連系が、すべての観点から、要求する安全機能および安全度に関して、安全に係る要求事項に適合している妥当性を確認します。この安全妥当性確認は、フェーズ9.2であらかじめ準備した計画に従って実施しなければなりません。

＊　＊　＊

以上、4回にわたり機能安全について簡単に説明してきました。規格の発祥地である欧州やその影響が強い東南アジアでは、購買の条件として認証までは要求しないものの、規格適合を条件とするケースが増えているため、IEC 61508は無視できない規格になりつつあります。■

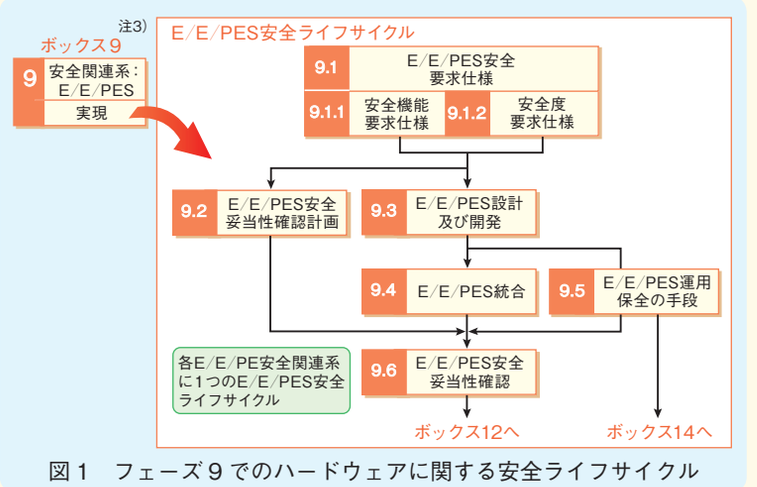

図1　フェーズ9でのハードウェアに関する安全ライフサイクル

注1)フェーズの名称は、本稿の**図1**および『エムエスツデー』誌2007年12月号に掲載した「計装豆知識」の**図1**で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。

注2) E/E/PE（Electrical/Electronic/Programmable Electronic）とは「電気/電子/プログラマブル電子」という意味です。

注3) E/E/PES（Electrical/Electronic/Programmable Electronic Systems）とは「電気/電子/プログラマブル電子系」のことです。