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(2)

先月に引き続き、機能安全に関するIEC規格61508について説明します。今月と来月は、全安全ライフサイクル（先月号（2007年12月号）の「計装豆知識」 図1参照）の中で、重要と思われるフェーズ[注]について説明します。今回は、フェーズ1～5です。

フェーズ1：EUC（Equipment under control）とそれが設置される環境（法的環境等を含む）を理解することが求められています。

フェーズ2：EUCとEUC制御系との境界の明確化と潜在危険およびリスク解析範囲を特定します。

フェーズ3：合理的に予見可能なEUCおよびEUC制御系の潜在危険と危険事象の明確化、危険事象につながる事象連鎖の明確化およびEUCリスクの明確化が求められます。

「リスクの明確化」すなわちリスクの解析は、異常発生による被害の程度と異常が発生する頻度を考慮して、リスクの大小を決定します。一つの方法として、異常発生によって起こる被害の大きさと頻度を想定列挙し、**表1**に示すようなマトリックスに当てはめて、リスクの等級を決定します。

表１　リスクの等級

頻　度	結　果			
	破局的な（Catastrophic）	重大な（Critical）	軽微な（Marginal）	無視できる（Negligible）
頻繁に起こる（Frequent）	I	I	I	II
かなり起こる（Probable）	I	I	II	III
たまに起こる（Occasional）	I	II	III	III
あまり起こらない（Remote）	II	III	III	IV
起こりそうもない（Improbable）	III	III	IV	IV
信じられない（Incredible）	IV	IV	IV	IV

表２　リスク等級の説明

リスク等級	説　明
等級 I	許容できないリスク
等級 II	好ましくないリスク リスク軽減が、非現実的すなわち、リスク軽減にかかる費用対効果比が著しく不均衡であるときだけ許容しなければならない好ましくないリスク
等級 III	リスク軽減にかかる費用が得られる改善効果を超えるときに許容できるリスク
等級 IV	無視できるリスク

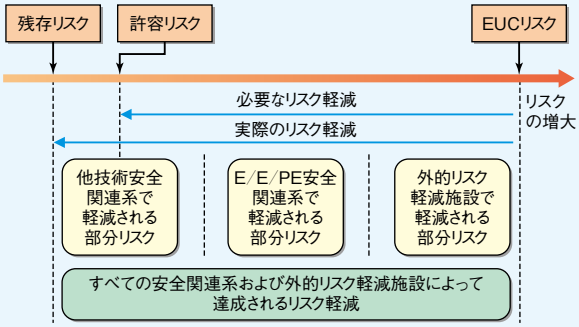

図１　リスク軽減：一般概念

フェーズ4：フェーズ9～11で実現される各機器や施設に対する安全機能と安全度要求に関するすべての安全要求仕様を決定します。後のフェーズでこれらが実現されることによってリスクが軽減されます（**図1**参照）。

ただし、リスクは許容可能な範囲まで軽減しますが、ゼロではありません。**表2**にも示すように、リスク軽減の費用と効果も考慮されます。さらに、フェーズ1で「法的環境等」について言及されているように、許容可能なリスクは社会情勢や法的規制の有無によって異なります。たとえば、同じようなボイラ制御システムに同じようにIEC規格61508を適用しても、設置する国によって国民一人あたりのGDPや人口密度、あるいは社会の成熟度などが異なり、それによって安全要求仕様が異なることが考えられます。

また、異常発生の頻度も適用される分野によって異なってきます。たとえば同じ輸送機関でも、自動車事故と航空機事故の発生頻度は大きく異なっています。余談ですが、この規格では、EUCおよびEUC制御系の異常は当然として、地震などの天災に起因する異常も考慮の対象にしています。日本では、1995年の阪神淡路大震災以来、大きな地震が頻繁に起こるようになり、震度7の地震にいつ襲われても不思議ではないというのが実感です。これも、EUCの設置環境を理解する必要がある理由の一つでしょう。

フェーズ5：フェーズ9～11で実現される各機器や施設に対してすべての安全要求仕様に含まれる安全機能を割り当て、各安全機能に対して安全度水準（SIL）を割り当てます。 ■

注）フェーズの名称は、先月号（2007年12月号）の「計装豆知識」**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】