



あの事故は なぜ起きたのか!!

機能安全の 認証



北村邦明

安全マネジメント規格「IEC 61508」に関する解説の最終回である。今回は製品がIEC 61508に適合していることを証明する方法・過程について述べる。
(編集部)

これまで5回にわたって機能安全国際規格IEC 61508に基づく安全ライフサイクル、リスク分析、ハードウェア設計、ソフトウェア設計などについて解説をしてきました。これらは安全な製品を作るための取り組み方を紹介するものでした。

それでは、本当に安全な製品ができたことを証明するにはどうしたらよいでしょうか。今回は連載の締めくくりとして、機能安全の認証について解説します。

現在、IEC 61508に基づいて機能安全の認証をしてくれるのは、海外の認証機関に限られているようです。中には日本法人を置いているところもありますが、認証を取得する場合には、関連する文書や記録を英語で整備し、アセスメント(Assessment)にも英語で対応するなどの手間がかかることも考えておかねばなりません。認証の具体的方法は、認証機関がそれぞれ定めていますので、そこに直接確認していただく必要があります。ここでは認証の一般的な方法および考え方について解説します。

● 認証は必要なのか?

IEC 61508の適用は法律で要求されているものではありません。従ってIEC 61508を適用するのは、顧客から要求された場合、あるいは競合他社との差別化を図るなど営業戦略上の必要性がある場合ということになります。また

IEC 61508には、「機能安全が達成されているかどうかのアセスメントを行え」という要求はありますが、「認証を取得せよ」という要求はありません。このことから、製品がIEC 61508に適合していることを証明するためには、二つの方法が考えられます。

- 自己宣言…自社でアセスメントして証明する。
- 認証取得…認証機関のアセスメントを受けて認証書の交付を受ける。

自己宣言をした場合には、顧客がそれをどのように受け止めてくれるかが問題になります。専門性のある第三者機関のアセスメントを受けている場合の方が、より信用されるかもしれません。

● 部品のSIL認証

IEC 61508は安全度水準としてSIL(Safety Integrity Level)を1から4まで規定しています(本誌2008年10月号、pp.137-141の連載第4回を参照)。ここで注意していただきたいのは、SILはシステム[センサからアクチュエータ(踏切の遮断機などのように安全状態を作るための機器)までを含む]について定義されるということです。

例えば単一チャンネルのシステムでは、センサがSIL 3であっても、アクチュエータがSIL 2ならば、そのシステムはSIL 2になってしまいます。このように部品レベルのSILをシステムのSILと区別して考える必要があります。

最近部品レベルの認証には、SIL capableという言葉が使われるようになりました。SIL capableは、IEC 61508が推奨する決定論的な危険側故障を回避し、制御する要求

Keyword

IEC 61508, 認証, アセスメント, 機能安全マネジメント, 安全コンセプト, ハードウェア設計, ソフトウェア設計