機能安全、リスク管理、EMC/EMI

Keith Armstrong

1. 機能安全とは何か?

製品、システム、設備の安全性は、2 つの部分に分けることができる。

i)「基本的」な安全性：感電、高温、強い放射線、火災、爆発、爆縮、打撲、挟まれる、粉砕、切断、有毒ガスの放出など。
ii)「機能的」な安全性：制御されているものが正しく機能せず、これにより健康へのリスクが増加する可能性がある場合。

機能安全は、常に機械、空気圧、油圧制御システムに存在し、電気機械、電気空気圧、電気油圧の制御システムにも存在している。

しかし、それが IEC や ISO の規格に値するトピックになったのは、マイクロプロセッサが物の制御に使われるようになってからである。

なぜかというと、マイクロプロセッサ（もしくはマイクロコントローラや FPGA など）および／または、そのソフトウェアが機能しなくなる可能性のある全ての方法で、試験ができないためである。例えば、自動運転など最新の「コンピューター化された」制御システムなどは、予想可能なデジタル状態についての試験を1つずつ実施するのに、1 試験あたり 1 マイクロ秒としても約 150 億年という宇宙の年齢より長い時間が必要であり、要は不可能である。

これは、デジタルシステムは本質的に非線形（ノンリニア）なので生じる問題である。つまり、たとえあり得る状態の 99% が試験でき