宇宙船の設計で考える?!

研究！モノづくりの最新コモンセンス「機能安全」

第10回　機能安全は構想設計が大切

森本 賢一

図1　いきなり詳細設計図から始めるのがよいのだろうか

今回のテーマ

● 普通まず考えられる機能安全対策…部品表から故障確率を解析する

これまで，設備に発生する危険を防護するようなコンピュータ・システムが実現すべき信頼性（＝完全性）とはどのようなものか，解説してきました．

完全性を示すレベルSIL（Safety Integrity Level）は，イザというときに失敗するかもしれない確率（*PFD*/*PFH*）で評価します．それに加えて，内部にある危険側かつ検出できない故障確率λ_{DU}の割合で，多重化による完全性向上の仕組みを評価します（*SFF*；Safe Failure Fraction）．より良いアーキテクチャには，λ_{DU}を削減したり，共通要因故障を削減したりする構造が必要です．

機能安全規格IEC 61508が求めるのは，前述のようなハードウェアのランダム故障に基づく故障確率だけではありません．仕事の仕方や人員の教育，レビュー体制，またソフトウェア作成のプロセスなど，システマティックな問題を排除するための要件も，完全性達成のための条件になっています．

いくら*PFD*や*SFF*がSIL3の許容値に入っても，開発プロセスの要件を満たさなければ，対応するSILレベルとはいえません（この観点は次回以降に解説）．

とはいえ，まずは手元にある部品表から当たりを付けたいと感じるのは悪いことではありません．故障モード影響診断解析FMEDA（Failure Modes Effects and Diagnostic Analysis，前回最後に説明）が，その最終的な故障確率を算出するための作業です．

● ホントにそれがいいか？

このように解説すると，多くの方が，回路図と部品表（およびその故障率）が機能安全の要なのだと感じるかもしれません．

全くの新規設計の場合は別として，皆さんが機能安全を達成しようとする場合，多くは既存の類似製品がすでにあるでしょう．構想設計に関する図書は全くなくても，手元に回路図や部品表があるはずです．こうなると，機能安全への準拠作業は，まずはFMEDAからスタートしよう，となるのもやむを得ません．

でもこれは効率の良いアプローチではないのです（**図1**）．

今回は，これまでの説明を踏まえ，構想設計の重要性と，評価段階の故障挿入試験について解説していきます．

障害物検知システム危険判定部の故障確率算出

● ターゲット回路

タキオンによる障害物検知システムの危険判定部分には，**図2**のようなマイコンを搭載した基板が使われているとします．この基板には3.3Vの直流電源を生成する電源回路（**図2**の⬚部）が搭載されています．大切な電源ですので，2重化しています．それぞれDC-1，DC-2と呼ぶこととします．

この電源ブロックは，さらに**図3**のような回路で構成されています．LM01は電源レギュレータICです．

第1回　業界用語「機能安全」と「本質安全」（2015年8月号）
第2回　「リスク」「安全」…用語の定義（2015年9月号）
第3回　評価を繰り返して「安全」を目指す…リスク・マネジメント（2015年10月号）