生業プログラマ必読！リスクを減らす考え方＆しくみ　宇宙船の設計で考える?!

モノづくりの最新コモンセンス「機能安全」

第6回　購入部品のリスク評価＆対策

森本 賢一

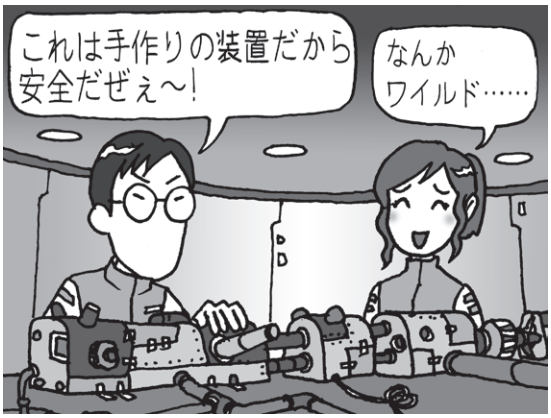

図1　自分たちで作った装置なら機能安全的に保証できそう

図2　買ってきた部品は機能安全的に信用ならない!?

信頼性の評価でいつもひっかかる…購入部品のリスク

● 信頼性を保つために欠かせないこと…リスク分析の過程の資料化

信頼性の高いシステムを実現する基盤は，リスク・マネジメントと構想設計です．それをもとに，その構想をどう実現し，結果を試験でどう確認するか，という段階に進みます．

この信頼性に関する一連の取り組み，そしてその中でなされた議論や試験の結果をまとめて，Safety Case（セーフティ・ケース）と呼ぶことがあります．この資料は，装置や設備が完成したあと，直接の使用者だけではなく，その設備に影響を受ける人々に，その信頼性（安全性）を説明するためのもので，第三者が理解できるように作成します．リスク・マネジメントや構想設計で，なぜそう判断したのかという意図（Intention）も記録することが望まれます．リスク分析のハザードごとに，できればそのときの議論の要点，最終的な結論に至る紆余曲折も記録できていることが望ましいです．

● 購入部品のリスクを知るのは難しい

この記録を作成していると，大きな問題に直面します．それは，自分たちで作らない（内部構造がわからない）部分がシステムの中にある場合，それをどう扱えばよいのだろうということです．自分たちで作った装置であれば，稼働実績や出荷後のトラブル事例の統計をベースに，リスク分析や障害解析をできそうです（**図1**）．しかし，全く初めての装置や部品を買ってくると，その信頼性の評価は難しくなります（**図2**）．

インターフェースが規格化されていないものや，機材への組み込みにC言語などの制限がゆるい言語を用いているもの，さらに新しく登場したデバイスを使用する場合などは，認証済みマークがあるからと目をつぶって組み込むわけにはいきません．自分たちが開発するシステムにどのような影響があるのか，十分に吟味しておく必要があります．

機能安全認証済みとカタログにある機材や部品を自社製品に組み込むときは，この点に注意する必要があります．誰かのSIL3のシステムに使われた部品でも，あなたのSIL3システムで有効とは限りません．もちろん，機能安全のプロセスに基づいて開発されたものであり，かつ必要な情報がすべて図書に記載されていて，ハードウェアの故障確率などの数値も明確であれ

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）