ご購入はこちら

生業プログラマ必読！安心を作る考え方＆しくみ

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11回 機能安全のソフトウェア開発で求められること

森本 賢一

今回と次回のテーマ

● 信頼性を上げるにはハード故障対策が重要

これまでハードウェア（電子回路）の不動作確率について解説してきました．電子部品の故障をFMEDA（Failure Modes Effects and Diagnostic Analysis）によって洗い出し，『いざというときにちゃんと動作しないかもしれない確率（*PFD*/*PFH*）』を見積もります．FMEDAでは，ランダム・ハードウェア故障にする対策メカニズムに応じたDC（Diagnostic Coverage）の割合だけ，λ_{DU}（最も減らしたい検出できない危険側故障確率）をλ_{DD}（検出できる危険側故障確率）に振り替えることができます．これによってシステムの*PFD*/*PFH*や，*SFF*（Safe Failure Fraction）を小さくしていきます．

この途方もない作業を効率良く進めるためには，ハードウェアとソフトウェアをまたいだ構想設計（アーキテクチャ作りとシステムFMEA/FTA）がとても大切です．アーキテクチャ作りとそれに対するシステムの故障解析が機能安全の要（かなめ）と言っても過言ではありません．

● ハード故障対策もソフトウェアの重要な仕事

このような対策メカニズムを自己診断（Diagnostics またはSelf-Test）と呼ぶこともあります．自己診断は，自動的に定期的に実行されることが要件です．人の手によって数カ月に1回検査するという診断は，自己診断とはいいません．そうなると，当然このようなメカニズムはマイコンやFPGAによって実現することになります．そのシステムには実現すべき元来の機能があります．ソフトウェアはもちろんその機能を実現しなければなりませんが，構想設計で明らかになった基板の電子回路のランダム・ハードウェア故障への対策メカニズムも，ソフトウェアで実現すべき大切な機能です．

このように，機能安全は組み込みソフトウェアにとても大きな負担がかかります．ハード屋さんのFMEDAも途方もない作業ですが，組み込みソフトウェアに元来の機能以外の処理をたくさん詰め込むことは，ソフト屋さんの負担も大きくなります（**図1**）．小型化し可能な限り発熱を減らす必要のある組み込みシステムでは，CPUの処理能力や空きメモリに限りがあるからです．今回と次回（最終回）は，機能安全においてソフトウェアに求められる要件を整理していきます．

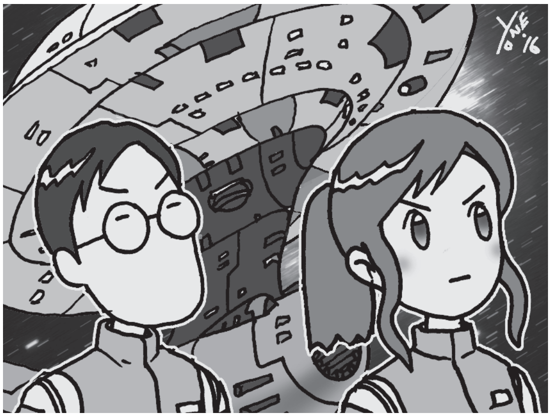

図1 機能安全では組み込みソフト屋さんの負担もすごく大きい

超重要！ ソフトウェア・アーキテクチャの設計

前回にも登場した，タキオンによる障害物検知システム危険判定部のCPU基板を見てみましょう（**図2**）．今回はこの基板に搭載されているCPUのソフトウェアについて考えていきます．

●「ソフトウェア」って言葉の範囲を整理しておく

CPUはプログラム・カウンタで指定されたアドレスの命令を実行します．010101010101という2進数の並びがソフトウェアの全てです．にもかかわらず，ソフトウェアとしてイメージする範囲が人によって異なっています．

例えば「障害物検知システム危険判定部」のCPU基板におけるソフトウェアとはどのような部分を指すで

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）