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」

最終回 第12回

最初に全部決めるのが最重要… 機能安全マネジメントFSM

森本 賢一

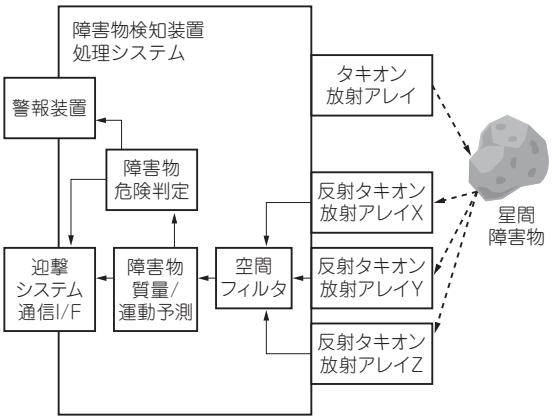

図1　今回のターゲット装置…障害物検知装置（以前設計）

図2　ほんのちょっとの式の違いでもアルゴリズムのミスは危な過ぎる…システマティック故障

● 今回のテーマ…ソフトウェアによるシステマティック故障を低減するための基本

いざというときに確実に動作する，信頼性（安全完全性レベル：SIL）の高いシステムを開発するためには，ハードウェアとソフトウェアを俯瞰したシステムの構想設計がとても重要です．

システムにはランダム・ハードウェア故障と，システマティック故障の2種類があります（これまでの連載でも紹介）．これまで解説してきたのは，主にランダム・ハードウェア故障についての対策でした．

今回最終回は，機能安全規格において，システマティック故障をどのように低減し，安全完全性を高めようとしているのかを解説していきます．

ほんのささいなことで痛恨の一撃… なんて恐ろしいシステマティック故障

● 今回のターゲット装置…障害物検知装置

図1は今回のターゲットである障害物検知装置の機能ブロック図です．タキオンの反射スペクトルの分析によって，障害物の質量や運動量，および相対的な速度を算出し，警告・回避・迎撃のいずれかの判断を下します．以前の連載では，タキオン検知アレイや放射アレイに故障が発生したケースへの対処を解説しました．今回はシステマティック故障としてどのような故障があり得るか考えてみましょう．

● あり得るシステマティック故障の例…原理・アルゴリズムの間違い

障害物の質量や運動方向を予測する物理モデルは，さまざまな法則に基づき設計されています．計算は極めて高度な数学を使用しますから，ほんのささいな計算アルゴリズムの間違いが，大きな誤差となって間違った予測を導く可能性があります（**図2**）．速度が速くなるほど誤差が大きくなるような間違いならば，初期の試験航行では問題が発見できないかもしれません．

クリティカルなシチュエーションは試験として実施できない場合もあります．例えば無重力かつ光速移動の場合に初めて露呈する間違いは，地上の試験で事前に確認することは困難です．

機能安全マネジメントFSM… システマティック故障を低減する

● 機能安全の最も重要な設計思想…最初に活動から人材まで全部決める

原理・アルゴリズムでの間違いを防止するために

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）
第4回　ハードもソフトも把握した「構想設計」が信頼性UPの近道（2015年11月号）
第5回　リスク分析手法「FMEA」で障害を洗い出す（2015年12月号）