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9回　システムの安全性を高める多重化＆多様化

森本 賢一

図1　多重化で安全性を高める

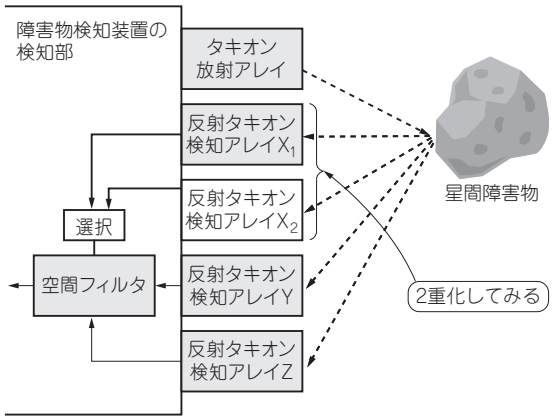

図2　宇宙船の障害物検知装置の検知アレイを2重化する
空間フィルタから先の処理は第7回の図2と同じ

● 今回解説すること

システムの危険側不動作確率*PFD*とは，電子部品の故障などにより，「万一の際に，きちんと動作しないかもしれない確率」を意味し，システムの完全性を評価する大切な数値です．設備のリスク・レベルに応じて必要な完全性のレベルが決まります．それをSILといいます．そのSILに応じてシステムが最低限達成しておくべき*PFD*が決まります[注1]．

必要な完全性を達成するためには，*PFD*の計算式にある，λ_{DU}を小さくすることが必要です（第8回で詳しく解説）．λとは部品故障率のことで，λ_S（安全側），λ_D（危険側），の分類に加え，λ_{DU}（危険側かつ検知できない），λ_{DD}（危険側かつ検知できる）に分類されます．このうちλ_{DU}が*PFD*の計算で重要な役割を果たします．λ_{DU}を小さくするために，安全メカニズム（自己診断などのメカニズム）をシステムの要件に追加してゆく必要があります．

危険側不動作確率*PFD*を低くする方法は大きく二つあります．

(1) 適切に検出して対策する安全メカニズムがあれば，その対象となる故障は，λ_{DU}ではなくλ_{DD}にカウントできることとなり，*PFD*の低減を図れる
(2) 多重化することで*PFD*の低減を図る

前回は(1)を紹介しましたので，今回は(2)を紹介します．

● *PFD*を小さくするための方策：多重化？

今回は，安全メカニズムの追加以外で，システムの危険側不動作確率*PFD*を小さくする手法として，多重化について説明します（**図1**）．細かい解説をしなくても，2重化，3重化すれば，システムの信頼性が上がることは感覚的に理解できると思います．多重化により片方が故障している間に故障側を修理するなど，障害への対処ができることも大きなポイントです．

しかし単に多重化するだけでは，極端には信頼性（完全性）が向上しません．

今回のターゲット…障害物検知装置の2重化

● 基本思想…2台使えば失敗する確率を2乗で小さくできる？

前回（第8回，2016年5月号）取り上げた障害物検知装置について考えます．前回は，反射タキオン検知ア

注1：例えばSIL3では，*PFD*は10^{-4}のレベルです．これは，「万一の事態」が10,000回発生した場合，その対処を1回程度失敗する可能性があることを示します．

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)