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5回　リスク分析手法「FMEA」で障害を洗い出す

森本 賢一

図1　イライラして出力120%…こんな暴走も防げる過負荷防止装置を考える

● チーム設計の基本…全員で同じ景色を見る

信頼性の高いシステム，堅牢なシステムを設計するには，ハードウェア担当，ソフトウェア担当として作業を分担する前の構想設計が大切です．技術分野を越えて全体を俯瞰する，つまり関係者全員が同じ景色を見るのです．

▶同じ景色を見るだけでは信頼性は上がらない

さて，同じ景色を見れば問題はすべて解決するのでしょうか．「同じ景色を見る」とはやや文学的な表現ですが，こんな精神論でシステムの信頼性が高まるとは思えません．はい，私も思いません（笑）．

● 解決法…起こりうる障害をリストアップ

今回はこの問題の解決方法について考えます．システムFMEAといいます．システムHAZOPとかシステムFMECAという場合もあります．どれも構想設計段階のアーキテクチャに対して，障害解析を行うことを指します．

実は同じ景色を見るというのは，その活動の前提条件でしかありません．これを充実させるためにアーキテクチャ図を作るのです．これを充実させるためにメンバーの意思疎通を密にしておくのです．構想設計とは，アーキテクチャ図づくりとそれに対する障害解析がセットになった活動ともいえるのです．

今回の考察対象…ワープ機関暴走防止装置

● 許容できないリスク…ワープ機関の暴走を防止する装置

今回は，前回に引き続きワープ機関を例に考えてみます．宇宙船にとってワープ機関の暴走や破壊は致命的な危害を招く，まさに許容できないリスクです．信頼性の高い仕組みでリスクを低減することを考えなくてはなりません．そこで，今回はワープ機関の異常な出力を制限する装置を考え，障害解析を行います．

▶操作ミスなど万一のリスクを下げる

この過負荷防止装置があるからといって，ワープ機関が暴走しなくなるわけではありません．運転手が出力120%と叫んでレバーを引くリスクは厳然としてあります（**図1**）．危険そのものはなくなりませんが，この防止装置があれば，そんな無茶な操作をしてまっても，エンジンに無理がかかることを回避できます．つまり万一のリスクを下げることができるわけです．機能安全的ですね．

● アーキテクチャ

ワープ機関の波動エンジンには，タキオンと呼ばれる粒子が原動力として使われています．このタキオンは，SFの世界でよく知られている物質です．

エンジンの出力状態は，発生しているタキオンを計測すれば推定できます．タキオンが発生し過ぎていれば，エンジンに無理な負担がかかっています．そのような場合にエンジン出力を下げるには，動力部へのタキオンの供給を停止します．緊急事態ですから，この際，配管の扉を開けてタキオンを宇宙空間に逃がすこととしましょう．この扉をタキオン緊急放出弁と名付けます．これを**図2**のようにアーキテクチャで描いてみます．

図2はハードウェアに偏った内容です．同じ図の中にCPUのソフトウェアの処理も書き込めれば良いのですが，あまり大きな図になっても扱いが面倒です．このような場合は別な図に展開します．その場合に

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）