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7回　システムの安全性を診断する方法

森本 賢一

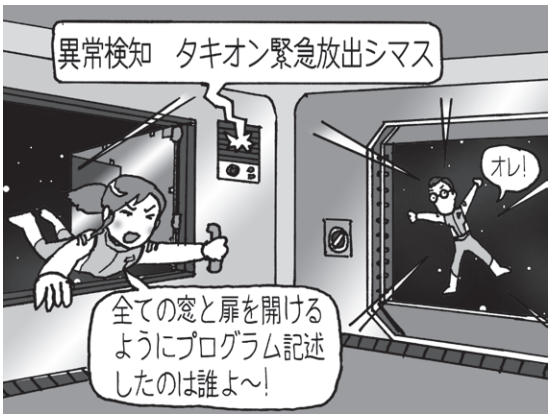

図1　障害対策は具体的な動作に落とし込まなきゃ…おならを検知したら運転指令室の窓を開放！

前回まで構想設計とアーキテクチャを障害解析するお話をしました．この障害解析にはアーキテクチャを改善するという役割だけではなく，詳細設計のあと最終的なシステムの信頼性を定量的に評価するという大切な役割があります．

詳細設計後に部品が確定すれば，最終的には確率で定量的に良否を判定する必要があります．

組み込みシステムの確率による評価作業は部品が決定したあと行います．しかしその評価の際に危険な事象の発生確率の「数値を低くするための仕組み」は，アーキテクチャの検討段階における障害解析の結果から決まってくるのです．このため，構想設計段階の障害解析の結果を整理しておくことが大切です．

今回はこの障害解析の中で取り決めた「対策」の整理から話を始めます

障害対策は具体的動作に落とし込む

● これまでの障害対策は表現が不明確

一通り構想設計の「アーキテクチャの作成」と「障害解析（システムFMEA）」を繰り返して形がまとまってきたら，次は障害解析の結果，危険のある障害に対して，自分たちが考えだした「対策」を整理します．

連載の第5回（2015年12月号）のワープ機関暴走防止装置では，「タキオン検出器のA-Dコンバータの異常（値が下限にはりつく）を検知したら，タキオン緊急放出弁を開放する」という対策を決めました．

第6回（2016年1月号）では，「波動砲発射トリガ装置には，通信経路の異常を検知する仕組みを経路の両端に設置する」を対策としましたが，それによって通信データの異常が検知されたときに，どのようなアクションをとるのかは明確にしませんでした．

● 「検知方法→システム動作」の形式に落とし込む

そこで，人それぞれさまざまな書き方で障害解析の対策が書かれているものを，一貫した表現になるように見直します．基本は，対策を「検知方法」→「システムの振る舞い」の形式に表現を直します．また同じ内容には同じ表現を使い，それぞれの対策にID番号を付けます．もし同じ内容の対策ならば，同じID番号を付けます．

前者では「タキオン緊急放出弁を開放する」とありますが，システムとしてどのような動きをすればよいのか書いていません．たとえばその代わりに「（あるアドレスの）接点信号をONにする（またはOFFにする）」などのシステム側の振る舞いに記載を変更しましょう．また，A-Dコンバータの異常をどのように検知するのかの手段が不明確です．このような場合は「2台のA-Dコンバータで結果を比較する」などのように手段を明確にします（**図1**）．

後者の通信部分では手段は明確ですね．「CRCを付ける」などの対策です．しかし検出した際にどうするのか決まっていません．たとえばこのような場合も「タキオン緊急放出弁を開放する」としましょうか．ならば，前述と記述を合わせて「（あるアドレスの）接点信号をONにする」という表現に直します．

安全性の診断手段の抽出

整理した対策の一覧表を，システムのSRS（Safety

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）