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」

新連載 第1回　業界用語「機能安全」と「本質安全」

森本 賢一

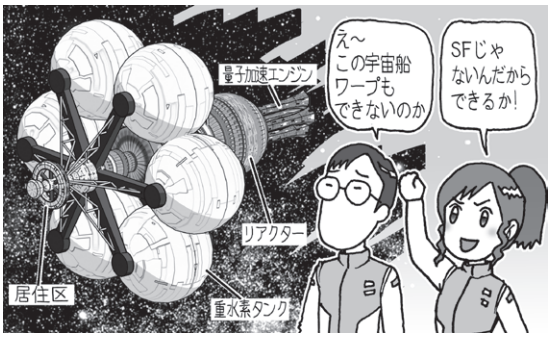

図1　星間飛行の宇宙船設計のミッションを乗り越えながら「機能安全」を考えてみる

マイコンやICなどで，「機能安全規格に準拠」とうたう製品が増えています．機能安全という言葉はわかりにくい表現ですが，モノにあらかじめ搭載したしくみによって，生じる危険を抑えようという考え方です．完全には取り除けないリスクと向き合うための技術です．

この考え方は主に欧州で規格化され，仕様を決める前のリスク分析～仕様決定～試作～評価～量産～廃棄処分に至るまでが機能安全と言われています．しかも欧州では，これに対応していないと製品を売れないという状況になりつつあり，市販の製品に搭載されるハードウェアとソフトウェア，つまりシステム全体にも適用されるようになってきました．この流れは日本はもちろん，世界中に広まりつつあります．つまり，マイコン・プログラマに縁遠い話ではありません．

そこで，本連載ではこの「機能安全」を解説します．題材として，**図1**のような星間飛行の宇宙船の計画・設計を取り上げながら，しくみの全体や用語の意味などを紹介していきます．（編集部）

機能安全とは

● 万が一に備えて用意しておくしかけ＝機能安全

皆さんの周りで機能安全という言葉が最近よく話題に上りませんか？「安全」という言葉を考えると，皆さんはどのような対策を思い浮かべるでしょう．ヘルメットを被ることも安全対策ですし，感電しないように電気機器を絶縁体で覆うのも安全対策です．

機能安全とは，平たく言えば，

「危険の根源を除去や回避できない場合，万一その危険な状態に直面した時に，それが災害につながらないようにするしかけ」

です．学術的には本質安全（後述）と対をなす安全を達成するためのアプローチです．

このようなしくみにはコンピュータが不可欠です．このため機能安全とプログラマは知らずのうちに深い関係にあるのです．

● モノづくりに必須になってきた

日本では自動車向けの機能安全規格ISO 26262が有名ですが，機能安全は自動車だけの規格ではありません．化学プラントや発電プラント，交通システムなどの安全性を求める設備分野では，20年以上前から必要とされています．また大掛かりなインフラ設備のみならず，皆さんの身の回りにも規格への準拠が必要な分野が増えています．

欧州で機器を販売するための規格であるCEマーキングで，家庭用機器向けの規格にIEC 60730というものがあります．家庭用といえども，電気・ガス・太陽熱などの燃料や熱，エネルギを扱う機器には，危険度のレベル付けをして，機能安全への対応を求めています．近年ではCEマーキング取得に必要な参照規格にも挙げられており，日本からの輸出の際に対応が必要となる製品分野が増えています．

▶機能安全を知るとモノの信頼性を高められるかも

機能安全の知識は，今どきのエンジニアには不可欠です．その考え方を身につけると，組み込みシステムの信頼性向上や品質向上に役立ちます．

機能安全では，リスク分析から始めます．モノづくりの途中でも設計のアウトプットに対するリスク分析を徹底して安全性を高めます．これは，品質管理規格として知られるISO 9001に新たに加わる（今年2015