第1章

複雑化するシステムの信頼性確保には冗長設計が欠かせない

冗長設計の位置付けから具体的な手法まで

檜原弘樹

ここでは，機器の信頼性を高める手段の一つ，冗長設計について，その位置付けから設計の取り組み方までを解説する．冗長設計においては，設計者自身が担当する回路だけでなく，システム全体を理解し，どの部分を冗長構成とすることが最善なのかを見極めるバランス感覚も大切である．（編集部）

高信頼性システムを実現するためには，特集1で述べられているように，さまざまな設計解析手法や設計技術が使われます．本稿では，対策の一つとして用いられる冗長設計の枠組みについて説明します．

1 冗長設計の位置付け

冗長設計を行うことにより，どのような効果が見込まれるのでしょうか．高信頼性を要求されるシステムには，故障や誤動作を起こさないように，設計余裕を持たせる必要があります（図1）．

ハードウェアを構成する部品や材料のばらつきを考慮した設計余裕を持たせるとともに，システムが使われる環境や，装置が耐えられる環境（温度範囲，湿度範囲，気圧範囲，振動・衝撃レベル，放射線レベルなど）も考慮する必要があります．

● ばらつきへの配慮はソフトウェア設計においても必要

製造時のばらつきについても考慮する必要があります．これはハードウェアの設計ばかりでなく，ソフトウェアの設計にも当てはまります．例えば，デバイスや製造時の調整のばらつきがソフトウェアに対する割り込みのタイミングに影響を与えたりすることもあります．

万が一，故障が検出されたり誤動作が発生したりした場合でも，破局的な故障には至らず，最悪でもいったん機器の動作を中断し，マニュアル操作によって運転や復帰ができるようなフェイルセーフ（fail-safe）機能が必要とされます．

● 耐故障への要求は高まるばかり

近年，組み込みシステムの提供する機能やサービスの高度化（インテリジェント化）が進んでいます．マイクロプロセッサを内蔵するばかりでなく，さまざまなセンサや通信機能が組み込まれ，個々のセンサ出力やネットワーク経由で送信された情報を有機的に統合して運用する自動化・自律化機能なども求められるようになってきました．

組み込みシステムに用いられるマイコンの高度化により，このようなシステムはますます増えるものと考えられます．これらの機器は，オペレータの操作を必要とするものばかりでなく，一度システムが起動されると以降は長時間無人で稼働する機器も増えており，無人で運用する組み込みシステムへの信頼性要求も高度化しています．さらに，航空機やロボットの自動操縦システムのように，組み込みシステムがオペレータと協調的に動作するような高度な自動化技術も求められるようになってきています．

● 単一故障点を除去するのが冗長設計

このような組み込みシステムでは，フェイルセーフからさらに進み，異常や故障が生じても適切な動作を継続する

KeyWord フェイルセーフ，fail-safe，フェイル・オペラティブ，fail operative，耐故障性，故障ケース，クロス・ストラップ，コールド・スタンバイ方式，待機冗長方式，ホット・スタンバイ方式，常用冗長方式

フェイル・オペラティブ(fail operative)機能が求められるようになってきています．特に，安全性が求められるシステムに実装するフェイル・オペラティブ機能は，信頼性の高いものでなければなりません．一つ故障が発生しても継続して稼働できるものを1フェイル・オペラティブと言います．人命にかかわるようなシステムや，社会インフラにかかわるようなシステムでは，二つ故障が発生しても破局的な故障には至らず，最低でも正常動作に復帰できる2フェイルセーフであることが求められることが少なくありません[注1]．

組み込みシステムへの耐故障性の要求はますます高度化してきており，フェイルセーフ，さらにフェイル・オペラティブ機能を実現するためのさまざまなアーキテクチャが開発されています．これらのアーキテクチャの一つとして用いられるのが，冗長構成です．ある特定の部分の故障によりシステムの機能が失われてしまうとき，その部分を単一故障点(single point of failure)と呼びます．システムから単一故障点を除去するための手段として冗長設計が用いられます(図2)．

2 さまざまな立場から見た冗長設計がある

冗長設計は，組み込みシステムが持つ演算機能や，故障検出機能，故障分離機能，再構成機能，再同期機能をそれぞれ分散化することにより行われます．

● 各機能を分けて考えることから始まる

演算機能を冗長化する方式としては，多数決方式や，時間軸上の冗長設計として同じ演算を2回以上実行して結果を確認する方式などがあります．

故障検出機能を冗長化する方式としては，誤り検出・訂正符号や，複数のプロセッサがプロセッサそのものの出力とほかのプロセッサの出力とを比較する方式などがあります．

故障分離機能を実現するためには，故障が生じた部分を物理的，あるいは論理的に隔離できる必要があります．システムがうまく階層的に構成されている場合には，故障をマスクしてほかに波及させずに済ますこともできます．故障した部分が自発的にシステムから離脱できるようにすれば，故障分離機能も分散化した冗長設計を行えます．このようなシステムをセルフ・パージング・システムと呼びます．

図1 冗長構成の例1
予定時刻に起きるための準備を念入りに行った．

故障分離機能が実現できていれば，冗長系に切り替えたり，故障した部分を切り離したりするなどして，失われた機能をほかの機能で肩代わりさせるようなシステムに発展させることも可能です．これらは再構成機能と呼ばれますが，完全に元の機能・性能を維持せずに，一部の機能を縮退させたり，性能を落としたりすることによりシステムの運用を継続することを優先させる場合もあります．

システムに故障が発生する以前の状態が保持されていれば，システムを再構成した後に，その時点までいったん後戻りして処理を継続させることも可能です．このような再同期機能が組み込まれていれば，速やかに通常の処理サイクルに復帰させることが可能になります．

● 故障の解析を徹底し，冗長設計の方針を決める

これらの冗長設計を行う際は，十分に故障ケースの解析を行い，一過性の故障に対応するのか，永久故障に対応するのかなども考慮して最適な方式を選択する必要があります．

例えば，人工衛星に搭載されるコンピュータについて見てみましょう(1)．宇宙機器搭載用のオンボード・コンピュータ(onboard computer：OBC)は，通常の組み込みシステム用計算機と比較すると，その使われる環境において多くの点を考慮しなければなりません．外部環境としては，宇宙空間特有の温度差や放射線環境を考慮する必要があります．温度差については，衛星システムの熱制御技術の進歩により，運用中の衛星内部の温度変化を非常に緩やかにすることが可能となっています．しかし，輸送，打ち上げ

注1：技術的に簡単な方から並べると，1フェイルセーフ(一つ故障が発生しても正常動作に復帰できる)，1フェイル・オペラティブ，2フェイルセーフ，2フェイル・オペラティブ(二つ故障が発生しても継続して稼働できる)となる．