TTC標準
Standard

JT-K131

通信装置のソフトエラー対策設計法

Design methodologies for telecommunication systems applying soft error measures

第 1 版

2019 年 2 月 21 日制定

一般社団法人
情報通信技術委員会

THE TELECOMMUNICATION TECHNOLOGY COMMITTEE

TTC Telecommunication Technology Committee

目　　次

＜参考＞

１．国際勧告との関連

本標準は、2018 年 1 月に ITU-T にて承認された ITU-T 勧告 K.131 に準拠したものである。

２．上記国際勧告等との相違点

なし

３．改版の履歴

版　数	発　行　日	改　版　内　容
第 1 版	2019 年 2 月 21 日	制　定　(ITU-T K.131 (1/2018) 準拠)

４．工業所有権

本標準に関わる「工業所有権等の実施の権利に係る確認書」の提出状況は、TTC ホームページでご覧になれます。

５．その他

なし

６．標準作成部門

伝送網・電磁環境専門委員会

要約

本標準は、[ITU-T K.131]に従いキャリア通信ネットワークを構成する通信装置に対するソフトエラー対策設計原則および手法について述べる。はじめに、ソフトエラー対策の観点から対象となる通信装置の基本構成、ソフトエラーに対する信頼度基準の定義と策定方法および信頼度基準適合に向けたソフトエラー対策の装置開発手順について述べる。次に、対象の通信装置を設計する際に、上記信頼度基準に適合させるためにソフトエラー対策が必要な個所（回路ブロックやパッケージ等）を抽出する方法を述べる。次に、具体的な各種ソフトエラー対策設計法とその効果を示すとともに、ソフトエラー対策設計時の主な注意点について述べる。最後に、適用したソフトエラー対策設計の妥当性および信頼度基準の適合性を確認するための机上および実機によるソフトエラー信頼度評価法について述べる。

キーワード

クライアント信号、中性子照射試験、サイレント故障、ソフトエラー、SRAM、通信装置

まえがき

大容量、高性能、高品質が要求されるキャリア通信ネットワークを構成する通信装置の開発において、高集積化・微細化された半導体デバイスの利用は必須である。しかし、ソフトエラーの発生自体を完全に防ぐことはコスト等の問題から現実的ではない。そのため、半導体デバイスでのソフトエラーの発生が通信装置の故障の原因とならないように対策する必要がある。この対策には、通信装置を構成する各半導体デバイスのソフトエラーに対する特性を把握し、デバイスレベル、装置レベルにおいてソフトエラー対策を実装する必要がある。

一方、ソフトエラーは通信装置 1 台あたりで見れば非常に稀であるので、導入台数が少ないにも関わらず過度にソフトエラー対策を講じる必要はない。しかし、数千台の通信装置でネットワークを構成した場合は、ネットワーク全体で 1 日に数回ソフトエラーが発生してしまう可能性もある。そのため、通信装置の仕様検討段階で通信ネットワークでの運用条件を考慮に入れソフトエラーに対する信頼度基準を定め、それを達成するように設計段階でソフトエラー対策を講じる必要がある。

この様に、ソフトエラー対策は信頼度基準の設定からデバイス、装置の構成や動作に渡り幅広い知識とノウハウが必要となる。本勧告はソフトエラー起因故障を減少させるための通信装置における設計手法についてまとめたものである。

１．適用

キャリア通信ネットワークを構成する通信装置で、キャリアサイトに設置されるコア系（リンク／ノード）装置、アクセス系装置に対し、信頼度基準を満足させるためのソフトエラー起因故障に対する適切な対策設計原則と設計手法を提供するものである。本標準では信頼度基準の制定原則を記載するが基準値については対象外とする。

本標準で記載する PNF(Physical Network Functions)-based ネットワークを構成する専用ハードウェアと今後導入が期待される VNF(Virtual Network Functions)-based ネットワークを構成する汎用ハードウェアに対しては、同一の装置設計手法が適用可能と考える。しかしながら、VNF ネットワークの装置に対する詳細な対策原則については検討中である。

２．引用規格

[JT-K124] TTC標準 JT-K124 (11/2018), 通信装置の粒子放射線影響の概要

[JT-K130] TTC標準 JT-K130 (2/2019), 通信装置の中性子照射試験法

[TR-KSup.11] TTC技術レポート TR-KSup.11 (2/2019), JT-K131補足資料-FPGAにおけるソフトエラー対策

３．定義

本標準では、以下の用語を定義する。

3.1 他で定義されている用語

なし

3.2 本標準で定義する用語

3.2.1 FIT：failure in time

稼働 10^9 時間中に派生する故障数の期待値を示す単位

3.2.2 ハードウェア故障：hardware failure

装置の誤動作を引き起こすハードウェアの異常

3.2.3 ソフトエラー：Soft error

半導体デバイス内のデータの 1 または複数ビットが反転する現象。半導体デバイス自体の損傷ではない。

3.2.4 物理欠陥：physical fault

物理的にデバイスが劣化して誤動作する現象

3.2.5 **ソフトエラー故障**：Soft error failure

ソフトエラー起因のハードウェア故障

3.2.6 **物理欠陥故障**：physical fault failure

物理欠陥起因のハードウェア故障

3.2.7 **ソフトエラー発生率**：Soft error rate

単位時間当たりのソフトエラー発生数

3.2.8 **ソフトエラー故障発生率**：Soft error failure rate

デバイス内のソフトエラーに起因した装置故障の単位時間当たり発生数

3.2.9 **パッケージ**：circuit pack

ユニットに挿入され、保守者が容易に交換可能な回路基板

3.2.10 **信号影響有ブロック**：signal-effect block

ソフトエラー発生中および初期設定等のソフトエラー対策実行時にクライアント信号影響がある回路ブロック

3.2.11 **信号影響無ブロック**：non-signal-effect block

ソフトエラー発生中および初期設定等のソフトエラー対策実行時にクライアント信号影響がない回路ブロック

3.2.12 **警報機能信頼度**：alert function reliability

設備運用の観点からの信頼度

3.2.13 **サービス信頼度**：service reliability

サービス提供の観点からの信頼度

3.2.14 **保守信頼度**：maintenance reliability

設備保守の観点からの信頼度

3.2.15 ECC **訂正**：ECC correction

ECC 符号によるエラー訂正

3.2.16 **サイレント故障**：silent failure

クライアント信号影響があるにもかかわらずネットワーク保守装置や保守要員への警報が発せられない故障

４．略語と頭字語

本標準では次の略語を使用する。

AR	Alert function Reliability	警報機能信頼度
ASIC	Application Specific Integrated Circuit	
ASSP	Application Specific Standard Product	
BRAM	Block Random Access Memory	
CPLD	Complex Programmable Logic Device	
CPU	Central Processing Unit	
CRAM	Configuration Random Access Memory	
CRC	Cyclic Redundancy Check	巡回冗長検査
DICE	Dual Interlocked Storage Cell	
DRAM	Dynamic Random Access Memory	
ECC	Error Correction Code	
FIT	Failure in Time	
FPGA	Field-Programmable Gate Array	
LSI	Large Scale Integration	大規模集積回路
MCU	Multiple-Cell Upset	
MLC	Multi Level Cell	
MRAM	Magnetoresistive Random Access Memory	磁気抵抗メモリ
MR	Maintenance Reliability	保守信頼度
OAM	Operations, Administration and Maintenance	
PNF	Physical Network Functions	
RAM	Random Access Memory	
RCC	Reinforcing Charge Collection	
ROM	Read Only Memory	
SCU	Single-Cell Upset	
SDH	Synchronous Digital Hierarchy	
SER	Soft Error Rate	ソフトエラー発生率
SEFR	Soft Error Failure Rate	ソフトエラー故障発生率
SLC	Single Level Cell	
SRAM	Static Random Access Memory	
SR	Service Reliability	サービス信頼度
TLC	Triple Level Cell	
TMR	Triple Modular Redundancy	三重化冗長回路
ULA	Ultra-low Alpha	
VNF	Virtual Network Functions	
WDT	Watchdog Timer	

５．慣例

なし

６．通信装置の基本構成

本章では、ソフトエラー対策設計の観点からキャリア通信ネットワークを構成する通信装置の基本構成について述べる。

6.1　基本機能構成（クライアント信号影響からみた機能ブロックの分類）

図 6.1 に、ソフトエラー影響の観点からみた通信装置の基本機能構成を示す。

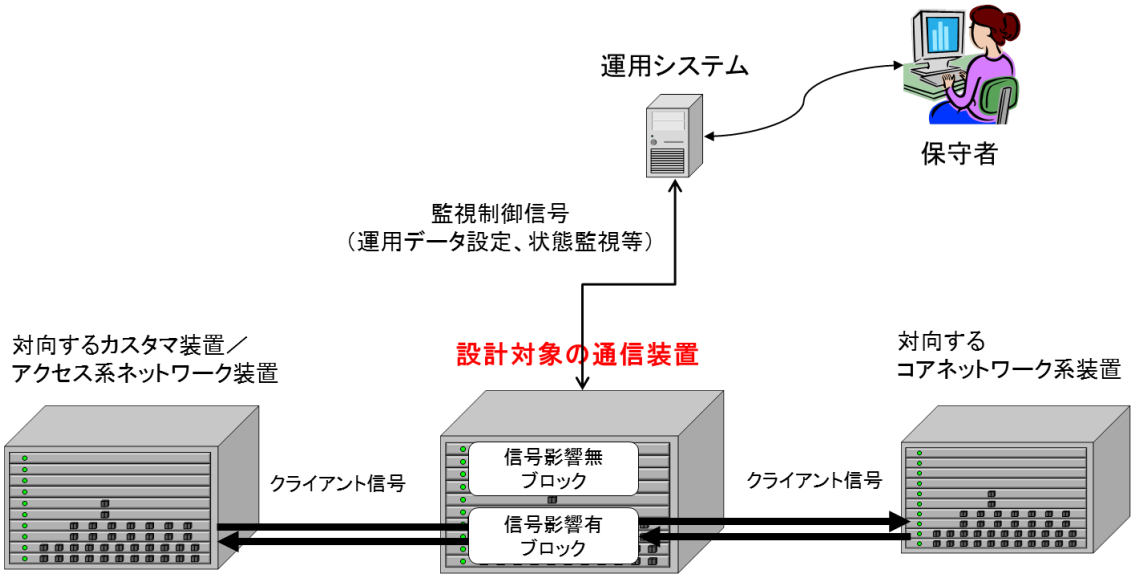

図 6.1　ソフトエラー影響の観点からみた通信装置の基本機能構成

通信装置の主要な役割は、通信サービスを提供するために正常にクライアント信号を導通させることにある。したがって、ソフトエラー対策実行時にクライアント信号が断状態になる等のサービス影響を極力発生させないことがソフトエラー対策設計上は重要である。そこでソフトエラー対策においては通信装置の基本機能ブロックを、ソフトエラー発生時およびソフトエラーを復旧させるため初期化等の対策実行時にクライアント信号影響のある信号影響有ブロックと影響のない信号影響無ブロックに大別する。具体的には、信号影響有ブロックは、ユーザ装置および対向通信装置と接続しクライアント信号を送受する機能部や、クライアント信号を通過させるために、たとえばパケットデータのルーティング処理や時分割データのスイッチング処理等の動作を行う機能ブロックが該当する。一方、信号影響無ブロックは、保守者インタフェースを有する運用システムと接続し、保守者からのパス設定、パッケージ登録、状態変更等の通信装置の運用設定制御オーダを実行する部分や、故障状態、運用状態等の装置状態監視情報の保守者への通知を行う部分が該当する。

6.2　装置構成（部品、パッケージ、ユニット）

図 6.2 に通信装置の基本ハードウェア構成を示す。

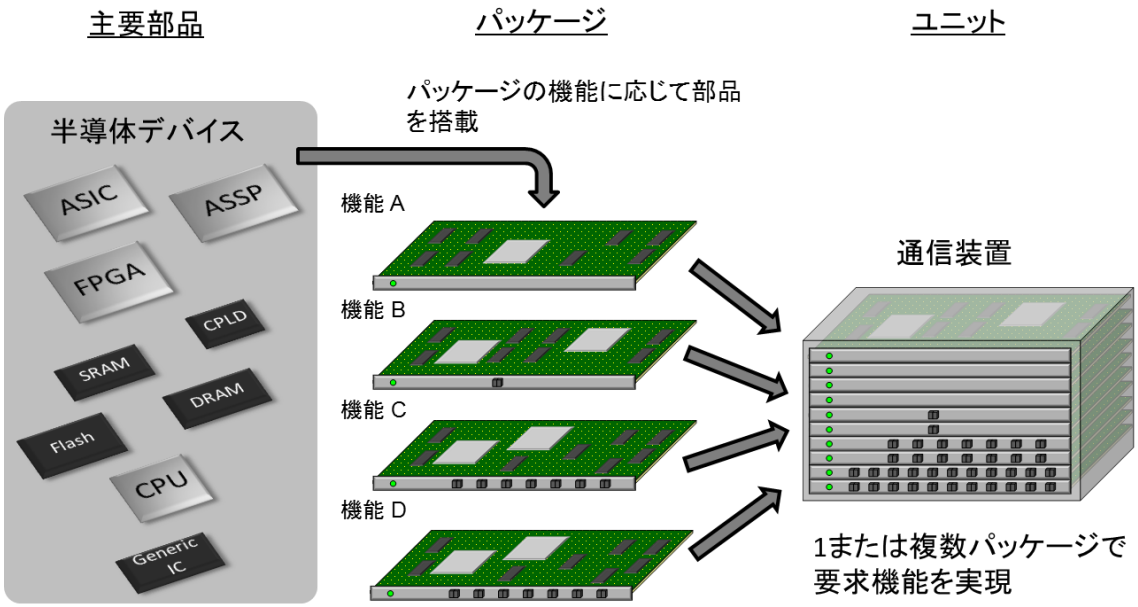

図 6.2　通信装置の基本ハードウェア構成

主要部品としては、ソフトエラーが発生する可能性のある半導体デバイスを使用している。これらの部品を機能に応じて組み合わせ、パッケージに搭載する。通信装置は、１枚または複数枚のパッケージからなるユニットで構成される。通信装置のハードウェア故障発生時は一般的に、パッケージ交換による復旧が行われている。

6.3　対策時に考慮すべき機能構成

この章では、装置のハードウェア構成と関連した機能構成について、ソフトエラー対策の観点から明らかにする。以下に述べる点を考慮しソフトエラー対策を設計することが重要である。

6.3.1　ハードウェアへの基本機能ブロック配備

図 6.3 に基本機能ブロックのハードウェアへの配備法を示す。機能の実現規模に応じて、信号影響有無ブロックを(1) 一つのデバイスで実現、(2) 別デバイスであるが１パッケージで実現、(3) 別パッケージで実現する構成がある。たとえば、(3)のようにパッケージ分離されており個別にリセット等を行えるのであれば、信号影響無ブロックのソフトエラー対策はサービスに影響なく実施できることになる。このように、ソフトエラー対策を設計するにあたり、信号影響有無ブロックが物理的にどのように分離／統合されているかを把握することが重要である。

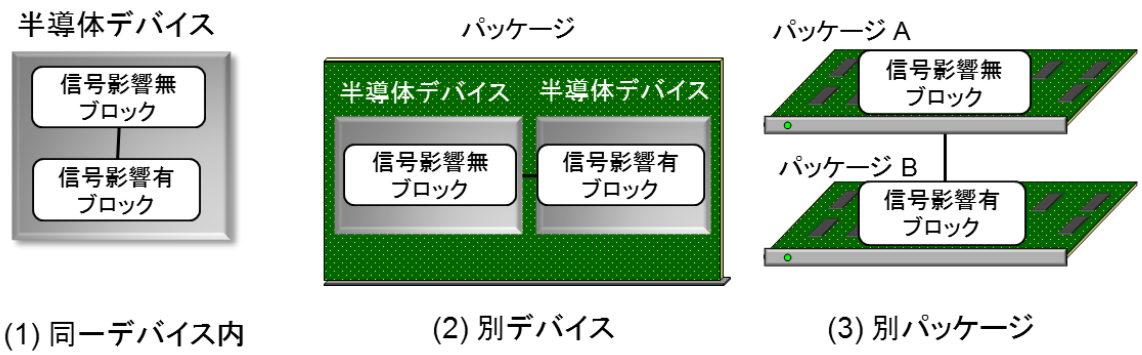

図 6.3　基本機能ブロック配備法

6.3.2　冗長構成

図 6.4 に通信装置の冗長構成を示す。ハードウェア故障等を考慮した信頼性確保のために必要に応じて、ネットワーク内や通信装置内で冗長構成をとるのが一般的である。これによりソフトエラー発生に対しても、運用系切替えでサービスを継続することができるとともに、サービスに影響なく非運用系でソフトエラー対策を実施できる。このため、ソフトエラー対策を設計するにあたり、冗長構成をとる機能ブロックや装置、冗長構成の切替単位（パス／回線／回路／パッケージ／ユニット等）および切替時間を理解して対策設計を行う必要がある。

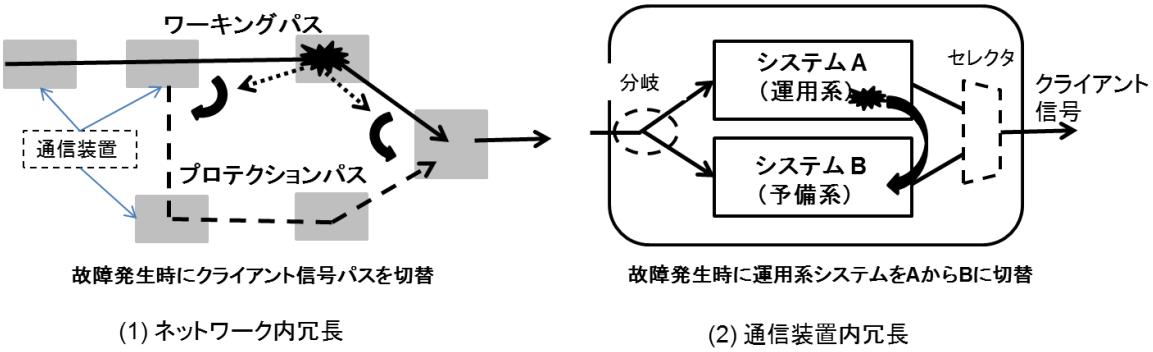

図 6.4　冗長構成

6.3.3　初期立上げ構成

図 6.5 に装置の初期立上げ構成を示す。通信装置の立上げ時等に必要なデータやプログラムは一般的に通信装置内の不揮発性メモリに格納される。通信システムにおいては装置復旧のための再立ち上げやバージョンアップ作業は稀であり、これらのメモリにあるデータは長期間アクセスされない。したがって、このメモリにソフトエラーが発生し適切に修復されなかった場合、多数の装置で長期間誤ったデータが保存される。その結果、このメモリへのアクセスが発生する運用中の通信システムの制御プログラムを一斉にバージョンアップした時やシステムダウン状態からの再立ち上げした時にはじめて、誤ったデータが多数の装置で供給されて、故障が多発する可能性があり、故障取替パッケージが不足する等の懸念がある。そのため、装置初期設定に関する情報のエラー発生時の影響度について把握しソフトエラー対策を設計することが重要である。

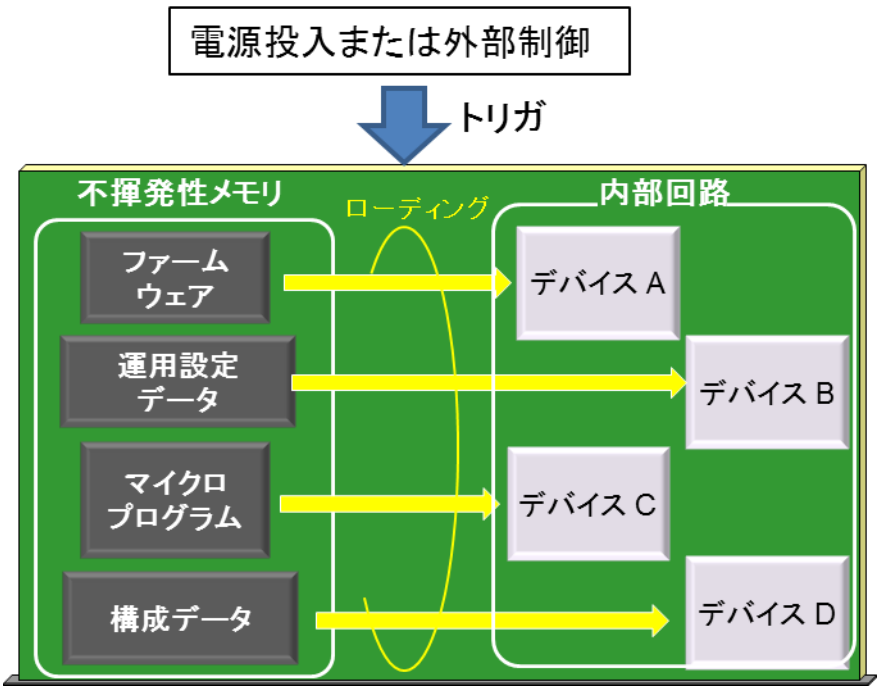

図 6.5　初期立上げ構成電源

7．ソフトエラーに関する信頼度基準と対策装置の開発手順

本章では、通信装置のソフトエラー故障率に対する信頼度基準を定義し、その信頼度基準適合に向けた対策を導入する装置の開発手順について述べる。

7.1　信頼度基準

図 7.1 に、故障発生から正常復旧までの必要な回復手順を、物理欠陥故障の場合とソフトエラー故障に対し 9 章で述べる対策を実施した場合を示す。通信装置の信頼度基準は正常に機能を回復しない確率や、故障の影響の度合いで基準するものであり、故障発生から正常復旧までの段階で必要な 3 つのステップで分類する。物理欠陥故障、ソフトエラー故障ともに基本的な手順は同じであるが、物理欠陥故障では必ず保守者による復旧作業が必要であるのに対して、ソフトエラー対策が完璧であれば殆ど保守者の介在が不要であることが異なる。

ソフトエラー故障においては、3 つの判断基準で信頼性を分類する。

1）　故障が発生したときに故障を検出して警報を発出することが正常にできるか

2）　クライアント信号が正常に疎通してサービスが復旧可能か

3）　装置全体が保守者介在なして自動的に復旧するか

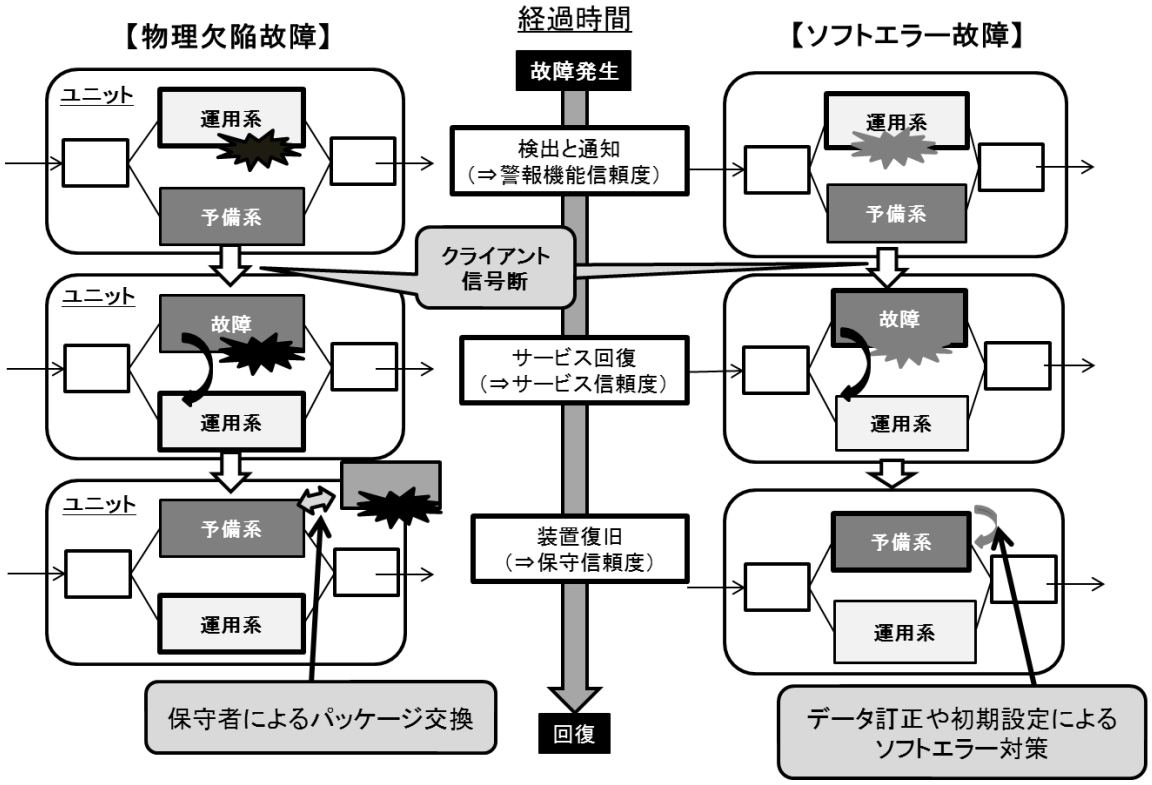

図 7.1　物理欠陥故障とソフトエラー故障からの復旧手順

表 7.1 に本勧告で基準する通信装置のソフトエラー故障に対する信頼度基準種別と定義を示す。下記の 3 種類の信頼度基準を設ける。

１）　設備運用の観点から警報機能信頼度（AR : Alert function Reliability）基準

２）　サービス提供の観点からサービス信頼度（SR：Service Reliability）基準

３）　設備保守の観点から保守信頼度（MR：Maintenance Reliability）基準

また、信頼度基準毎に基準クラスを設け、適用ネットワークの条件により対象装置の要求信頼度を選択可能な基準とする。信頼度クラスおよび基準値は、表 7.1 のそれぞれのタイプについて基準する。

表 7.1　信頼度基準種別

種別	略語	内容
警報機能信頼度基準	AR	設備運用の観点からの信頼度。 クライアント信号に影響するソフトエラー起因故障発生時の故障検出および警報発出性能により基準をクラス分け。
サービス信頼度基準	SR	サービス提供の観点からの信頼度。 ソフトエラーによるクライアント信号断の継続時間および発生頻度により基準をクラス分け。
保守信頼度基準	MR	設備保守の観点からの信頼度。 保守者がソフトエラー故障を復旧させるために遠隔操作や現地パッケージ交換を実施する頻度により基準をクラス分け。

7.2　緩和対策を実現するための装置開発手順

図 7.2 に装置開発の各段階におけるソフトエラー故障の緩和対策導入時の検討内容を示す。

はじめに、仕様検討段階において提供サービスおよび導入数量等を考慮し要求信頼度を定める。これは、前項で述べるソフトエラー信頼度基準における適用クラスを選択することになる。

次に、設計段階において、ソフトエラー故障率を机上で見積もり、選択した信頼度クラスに適合するための対策を講じ、SFER の評価が仕様を満足するまで上記の手順を繰り返す。

最終的に、試験段階において、実機を用いて半導体部品へのエラー挿入試験や加速器中性子源による中性子照射試験を行い、ソフトエラー対策の妥当性およびソフトエラー信頼度基準を満足することを確認する。

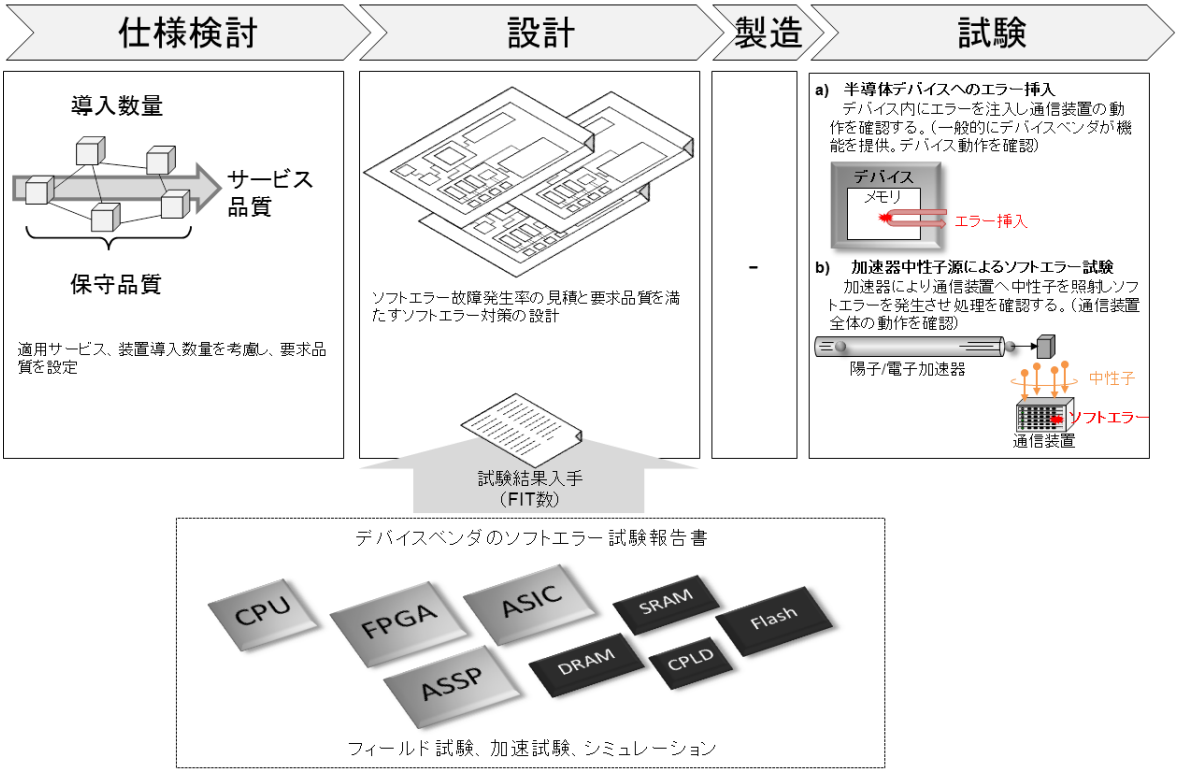

図 7.2　装置開発段階におけるソフトエラー対策導入手順

８．ソフトエラー影響予測

本章では、設計段階における通信装置のソフトエラー影響およびソフトエラー故障率の予測手法について述べる。

8.1　ソフトエラー影響のあるデバイス

8.1.1　半導体デバイス回路のソフトエラー発生傾向

通信装置の主要部品でソフトエラーの影響を受けやすい半導体デバイスは、主にメモリ回路や論理回路から構成される。メモリ回路は、SRAM、DRAM、フラッシュメモリに、論理回路は順序回路と組合わせ回路に分類できる。表 8.1 に、回路種別ごとのソフトエラー発生率の傾向を示す。

表 8.1　ソフトエラー発生率に関する半導体デバイス回路の特徴

回路種別		特徴	SER
メモリ回路	SRAM	高速 記憶素子としてフリップフロップ回路を用い、高速性が要求される用途で使われることが多い 低容量 DRAMほど高密度に実装できず、大容量メモリには向かない （注）FPGA内のコンフィグレーションデータ格納用CRAMにも使用されている	高 SERはLSIの製造プロセスの微細化により増加
	DRAM	大容量、揮発性 コンデンサとトランジスタにより電荷を蓄える回路を記憶素子に用い、大容量メモリとしてコンピュータの主記憶装置に広く利用されている	低 単位容量当たりのSER は構造上小さい 単位容量当たりのSER は SRAMの 1/1000～1/10000 であるが、DRAMは高密度のためSERが無視できない場合もある
	フラッシュメモリ	大容量、不揮発性 書き換え可能であり、電源を切ってもデータが消えない不揮発性の半導体メモリ	中～低 単位容量当たりのSER は SRAMの1/100程度 但し、NOR型およびNAND型セルがともに微細化し容量が増加、さらに構造がSLCからMLC、MLC からTLCに変化するに伴い増加傾向にある.
論理回路	順序回路	内部状態が保持されており、外部入力と内部状態により出力を決める回路 例：フリップフロップ、ラッチ等	中～低 一般的に論理回路はソフトエラー耐性が高く、通信のフィールドでも現状論理回路のソフトエラーは問題となっていない しかし、微細化・低電圧化に伴い増加傾向にある。
	組合せ回路	外部入力だけで出力が決まる回路 例：インバータ、NAND/NOR 等	

製造プロセスの微細化や低電圧化、高速動作化により全般的にチップ面積当たりのソフトエラー発生率は増加傾向にあり、特に SRAM におけるソフトエラー発生率が高く通信装置において顕在化し問題になっている。また、現状は問題となっていないが、フラッシュメモリや論理回路においてもソフトエラー発生率の増加傾向が顕著になってきており今後の動向を注意する必要がある（付録 I 参照）。

図 8.1 に SRAM の製造プロセス世代（図中横軸の Design rule と等価）とチップ面積当たりのソフトエラー発生率の関係を示す。これは、地表の中性子エネルギースペクトル分布と SRAM の製造プロセス世代ごとのソフトエラー発生クロスセクション分布のシミュレーション結果とから算出したものである[b-IEEE-1]。微細

化とともにビット当たりのソフトエラー発生率は減少するが高集積化が図られ、図 8.1 に示すようにチップ面積当たりではソフトエラー発生率は増加傾向にある。さらに、２ビット以上反転する MCU の確率も無視できなくなってくる。

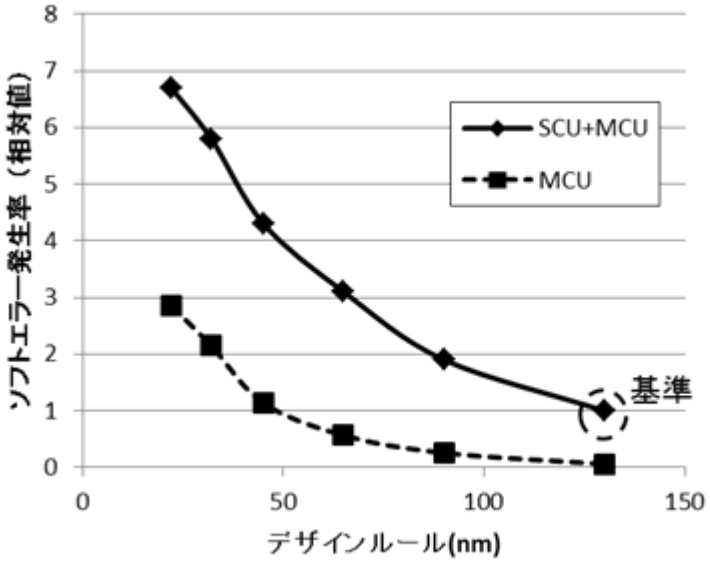

図 8.1　半導体製造プロセスとソフトエラー発生率の関係

8.1.2　半導体デバイス毎の使用回路種別

表 8.2 に主要部品の半導体デバイスごとに使用する回路種別を示す。SRAM と論理回路はほとんどのデバイスで使用されている。特に、最近の通信機器に利用される LSI の主流である FPGA では回路構成を決定するコンフィグレーションデータを SRAM に格納し任意の機能の実現が可能な構成としている。このように SRAM を多用していることから FPGA ベンダでは物理構造面からの対策を行うのみでなく、様々なソフトエラー対策ツールをユーザに提供している（TR-Ksup.11 参照）。

表 8.2　半導体デバイス毎の使用回路種別

半導体デバイス	メモリ回路			論理回路	
	SRAM	**DRAM**	フラッシュメモリ	順序回路	組合せ回路
ASIC	✓	✓		✓	✓
ASSP	✓			✓	✓
FPGA	✓		✓ （小規模のみ）	✓	✓
CPLD	✓		✓	✓	✓
RAM/ROM	✓	✓	✓		
CPU	✓			✓	✓
Generic IC				✓	✓

8.1.3　SRAM 使用形態とソフトエラー影響度

SRAM については、装置における使用形態によりソフトエラー影響の差異がある。設定データ格納メモリ、動作制御メモリ、データバッファメモリの３種類の使用形態に分類できる。表 8.3 に使用形態ごとに動作概

要、ソフトエラー影響および使用例を示す。

表 8.3　SRAM 使用形態とソフトエラー影響度

使用形態	動作概要	未対策時のソフトエラー影響度	使用例
設定データ格納メモリ	一旦データ書込み後はデータ保持動作および読出し動作のみを継続	大 書込み後はエラーデータの修復機会がないので、装置動作に継続的に影響あり	動作パラメータ スイッチング情報 コンフィグレーションデータ ファームウェア マイクロプログラム
動作制御メモリ	読出し、書込み動作を繰り返すので、エラーデータは一時的に使われるが長期間メモリ内に残らない	大 エラーデータを使用するとその後の動作に影響が生じることがある	クライアント信号動作制御 CPU キャッシュ
データバッファメモリ		小 間欠的なデータエラーで、影響度は装置構成や提供サービスに依存する	クライアント信号バッファ 制御信号送受信バッファ

設定データ格納メモリおよび動作制御メモリの場合に、ソフトエラーの機能影響が大きく、ソフトエラー対策が必要となる可能性が高い。データバッファメモリの場合には、常時新たなデータが上書きされ上書き後のデータからは正常となることから、影響はソフトエラーが発生したデータのみに限られる。したがって、ソフトエラー対策を行わなくても単発のビットまたはパケットまたはフレーム断後に正常復旧するので影響は小さい。ただし、エラーデータが他の領域に流出し機能影響を及ぼす場合には、対策を施す必要がある。また、サービス条件からこのような単発のクライアント信号断が許容されない場合には、反転データを正常データに書き換えて取り出す対策が必要になる。

8.2　ソフトエラー故障率の予測手法

ハードウェア設計における使用部品設計完了段階において、8.1 節に示すソフトエラー発生傾向を踏まえソフトエラー故障発生率を予測する。

図 8.2 に装置の部品構成例を示す。これをもとに、ソフトエラーの発生観点から部品とその回路種別の項目一覧を作成する。表 8.4 に例を示す。

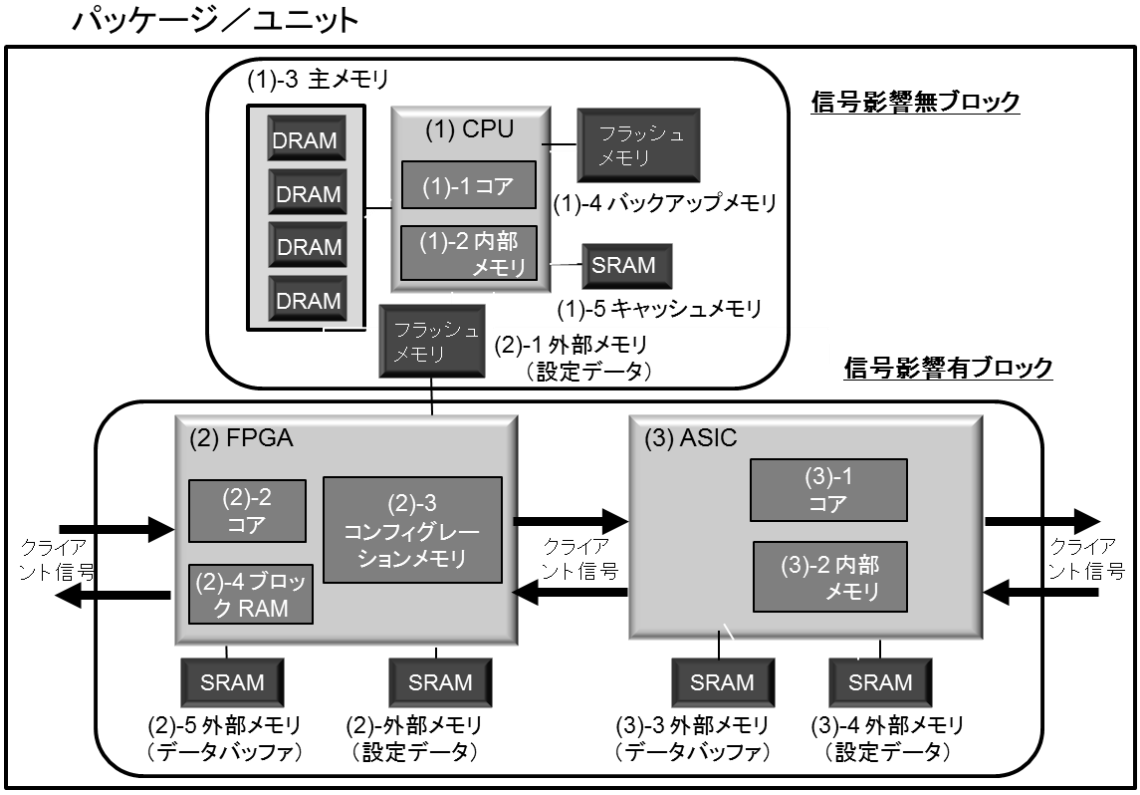

図 8.2　ソフトエラー影響のあるデバイスの特定例（装置の部品構成例）

表 8.4　ソフトエラー故障発生率の予測項目例

機能ブロック故障時のクライアント信号影響 (図 6.1)	種別		機能／使用形態	回路種別	SEFR計算値（FIT）	
					サービス信頼度	保守信頼度
影響無	(1) CPU 周辺回路	1	コア	論理回路	対象外	算出対象
		2	内部メモリ（動作制御、設定データ、データバッファ）	SRAM		
		3	主メモリ（動作制御、設定データ、データバッファ）	DRAM		
		4	バックアップメモリ （設定データ）	フラッシュメモリ		
		5	キャッシュメモリ（動作制御）	SRAM		
	(2) FPGA 周辺回路	1	外部メモリ（設定データ）	フラッシュメモリ		
影響有		2	コア	論理回路	算出対象	
		3	コンフィグレーションメモリ（設	SRAM		

			定データ）			
		4	ブロックRAM（動作制御、設定データ、データバッファ）	SRAM		
		5	外部メモリ（データバッファ）	SRAM		対象外
		6	外部メモリ（設定データ）	SRAM		算出対象
	(3) ASIC 周辺回路	1	コア	論理回路		
		2	内部メモリ（動作制御､設定データ､データバッファ）	SRAM		
		3	外部メモリ（データバッファ）	SRAM		対象外
		4	外部メモリ（設定データ）	SRAM		算出対象

各項目のソフトエラー故障発生率は、ベンダが通常参照する標準的な手法で測定したベンダ提示値の使用を基本とする。データが公表されていない場合には、装置設計ベンダが部品ベンダから個別に情報を入手するか類似部品から類推する必要がある。参考例として、Xilinx 社製 FPGA の公表値を[b-Xilinx]に示す。これには、部品単体レベルの値が示されている。したがって本表から、メモリの使用形態や装置構成を考慮し、装置対策前のソフトエラー発生率を予測する。装置としての発生率は、複数種・複数枚パッケージで構成されている場合は、それらすべてパッケージの合計値になる。算出した発生率と要求信頼度との関係から対策が必要な個所を抽出する。

ソフトエラー故障発生率は、サービス信頼度と保守信頼度に分けて調査する。サービス信頼度に対してはクライアント信号影響のある部分のみが対象である。一方、保守信頼度については、影響を受ける機能に関係なくソフトエラー状態が継続する部品すべてが対象となる。なお、データバッファメモリについてはエラー状態が継続しないため、保守信頼度基準に対しては本表のソフトエラー発生率には含まない。

９．ソフトエラー対策実現法

本節では、仕様検討段階に選定したソフトエラー信頼度基準に適合させるためのソフトエラー対策手法について述べる。

9.1　対策原理

ソフトエラー対策は、低減、隔離、訂正の３つの原理に分類できる。表 9.1 に各原理別に対策方法と具体例を示す。

表 9.1　ソフトエラー対策原理

原理	対策方法		例
低減	1	材料変更	磁気抵抗メモリ（MRAM） 極低α線放出（ULA）パッケージ材料
	2	物理構造の工夫	３次元トランジスタ構造（FinFET等） 論理回路のRCC （reinforcing charge collection）技術
	3	ソフトエラー発生領域の削減	FPGAのASIC化によるCRAMの除去
隔離	1	回路構成の工夫	三重化冗長回路 （TMR） ビットインタリーブ構成メモリ
	2	機能影響有無個所の識別	未使用RAMの非監視化 FPGAの未使用CRAMの非監視化
訂正	1	ハードウェアによる自律訂正	ECC 訂正、訂正データ上書き DICE (dual interlocked storage cell) 構成論理回路
	2	装置制御プログラムによる自律訂正	設定データ上書き 初期設定
	3	保守者操作による訂正	遠隔制御リセット

9.1.1 低減

低減の原理は、物理的対策によりソフトエラー発生そのものを抑制するものである。ソフトエラー発生のない磁性体材料を用いた MRAM 等の部品を使用することでソフトエラーの発生を無くすことができる。また、α線放出量の小さい ULA（ultra-low alpha）パッケージ材料を使用することでα線起因のソフトエラーの発生を抑制できる。また、FinFET のような３次元トランジスタ構造を利用することで入射する中性子の影響を受ける面積を縮小できる。RCC 技術を適用することで高速イオンがシリコンに衝突して発生する電荷をダミーのインバータ回路で吸収させることができる。中性子照射に対する耐力の小さい SRAM の使用量を少なくすることでソフトエラーを低減できる。ソフトエラー低減対策は、装置設計の時に部品を選定することによって物理的に対策できる。したがって、ソフトエラー故障率の予測手法で述べた表 8.4 の調査段階ではすでに盛り込まれた対策となる。

9.1.2 隔離

隔離の原理は、ソフトエラーが発生しても信頼度影響がないように発生部分を隔離するものである。三重化回路構成としソフトエラー発生個所は切り離し動作を継続する、メモリをインタリーブ構成とし MCU の影響を軽減するなどの回路構成を工夫する方法がある。また、機能影響の有無を識別して注意または警報の発出を抑制することで保守稼動を低減することができる。ソフトエラー隔離対策は、回路設計および制御プログラム設計段階の対策となる。

9.1.3 訂正

訂正の原理は、正しいデータで上書きするか、またはデータ全体を再初期化することによって、ソフトエラーが発生したメモリデータを自律修正することを意味する。ソフトエラーは半導体デバイス自体が壊れるので

なく保持しているデータの一部のビットが反転してしまうという事象であることから、この方法が効果的である。

訂正を行う契機の違いからハードウェア自律訂正、装置の制御プログラムと連携した装置自律訂正、保守者からの指示による 3 種類の訂正方法がある。

訂正を行う契機の違いからハードウェア自律訂正、装置の制御プログラムと連携した装置自律訂正、保守者操作による訂正の方法がある。ハードウェア自律訂正方法としては、主にメモリ回路に対する ECC 訂正または訂正データ上書き機能が使用される。DICE 構造は DICE 内のラッチで発生したソフトエラーを補償するためソフトエラー耐性が高い。自律的に訂正することが可能なエラーを検出した場合には制御プログラムが訂正動作を開始することを指示する。これに対して訂正手順においてサービスに大きな影響を及ぼす可能性がある場合には、保守者が、エラー検出時にエラー影響および訂正影響を見て訂正手順を決定する必要がある。したがって、本方法のみが保守信頼度に影響する。

いずれの対策もソフトエラーの検出と訂正の２段階で行うことになる。そこで、9.2 節でソフトエラー検出法、9.3 節でソフトエラー訂正法について述べる。9.4～9.6 節では、ソフトエラーの影響が大きい SRAM についてソフトエラー訂正対策手法例を示す。さらに各手法のサービス信頼度基準および保守信頼度基準への影響について述べる。また、9.7 項にソフトエラー検出ができないために訂正対策が取れず、大きな影響が発生するサイレント故障について述べる。サイレント故障は警報機能信頼度に影響する。

これらのソフトエラー検出および訂正対策は、回路設計および制御プログラム設計段階の対策となる。

9.2　ソフトエラー検出法

通信装置においてソフトエラー発生後にハードウェアや装置のコントロールプログラムや保守者が 9.1.3 項の訂正する対策を開始するには、まず装置内のソフトエラー発生を検出する必要がある。表 9.2 にソフトエラー検出法一覧を示す。

表 9.2　ソフトエラー検出法

分類	検出法	特徴（利点／欠点）
冗長ビット付加	パリティチェック	奇数ビットエラーにのみ有効
	CRC チェック	複数ビットエラーを検出可能
	ECCチェック	1および２ビットエラーを検出可能 1ビットエラー時はエラー個所を特定可能
冗長回路	冗長回路出力データ照合（二重化冗長回路）	エラー検出に対してのみ有効 いずれの回路がエラー状態にあるかの判定不可
ヘルスチェック	WDT監視	ビットエラーによるプログラム暴走を検出可能.
	OAMデータ送受信	クライアント信号や制御信号等の有効データの送受信がない場合でも検出可能
	周期メモリ読出し	必要時に時々アクセスするメモリのエラー検出に有効 メモリアクセス前に早期エラー検出が可能

検出方式としては、冗長ビット付加方式、冗長回路方式、ヘルスチェック方式に分類できる。これらは物理欠陥故障検出法と同一であり、ソフトエラー要因の故障か否かは 9.3 節の訂正処理の実行により復旧するか

否かで判断することになる。

冗長ビット付加方式は、クライアント信号や制御信号等のデータに一定の規則に従った冗長ビットを付加し、その後、そのデータがルールに適合しているかチェックしてエラーを検出するものである。奇数ビットエラー(ソフトエラーでは奇数ビットエラーは 1 ビットエラーにほぼ限定される)検出が可能なパリティチェック、複数ビットエラー検出が可能な CRC チェック、2 ビットエラーまでの検出が可能でかつ 1 ビットエラーの場合はエラー個所の特定が可能な ECC チェックがある。なお、エラー検出が可能なエラービット数、エラー位置の特定が可能なエラービット数については ECC チェック方式の拡張により開発世代ごとに向上する傾向にある。これらの方式は、メモリ回路のエラー検出に有効である。

冗長回路方式は、同一のデータを２つの同一回路に入力し出力を常時比較することで正常性を監視する方式である。エラー検出はできるがいずれの回路がエラー状態にあるかは判定できない。本方式は、論理回路のエラー検出に有効である。

ヘルスチェック方式は、機能ブロックが正常に動作しているか否かを機能ブロックの外部回路により監視する方式である。ヘルスチェック手法として、WDT 監視、OAM データ送受信、周期メモリ読出しがある。WDT（Watchdog Timer）監視は、ハードタイマをリセットするプログラムを定期的に動作させ、本プログラムが動作しないためタイマがオーバーフローすることで異常検出するもので、プログラムの暴走検出に有効である。OAM データ送受信は、クライアント信号や制御信号等のデータ送受信を行っている機能ブロックに試験用のデータを周期的に送受し正常性を確認するものである。これにより、ユーザ情報や制御情報等の有効データの送受信がない状態においても監視可能であり、信号送受信パスの異常検出に有効である。周期メモリ読出しは、メモリ読出し機能ブロックや上記冗長ビットが付加されたデータ格納時にはメモリセルの異常を検出するもので、常時非アクセスのメモリのエラー検出やアクセス前の早期エラー検出に有効である。

9.3 ソフトエラー訂正法

表 9.3 にソフトエラー訂正法一覧を示す。9.1.3 項で述べたようにソフトエラー故障は物理欠陥故障と異なり、エラー発生個所への正常データの上書きまたは初期設定により復旧でき、正常動作の継続が可能となる。

表 9.3　ソフトエラー訂正法

分類	訂正法	手段	内容
データ訂正	ECC 訂正	ハードウェア	出力データのエラービットを特定し ECC を使用した論理処理により出力データを訂正
	訂正データ上書き	ハードウェア	エラービットを特定し当該ビットを保持しているメモリ領域に論理処理により訂正したデータを上書き
	設定データ上書き	制御プログラム	ソフトエラー発生確率の低いフラッシュメモリ等に格納されている元データを上書き.
初期設定	パッケージリセット	制御プログラム／保守者	パッケージ全体の初期設定
	デバイスリセット		対象デバイスのみの初期設定。パッケージリセットに比べ訂正時間は短縮されるが、周辺回路との連携が必要
	FPGA リコン		フラッシュメモリからのデータ

	フィギュレーション		再読込み、周辺回路との状態整合処理が必要な場合あり
	CPU リブート		プログラム初期設定

データ訂正方式は、ECC 訂正、訂正データ上書き、設定データ上書きに分類される。ECC 訂正はメモリ内容の訂正は行わず出力データのみを訂正する。ECC 訂正と訂正データ上書き方式は、ハードウェアが自律でエラービットを特定し論理処理によるエラー訂正データを上書きする方法である。設定データ上書き方式は、制御プログラムにより別途格納されている正常データを上書きする方法である。いずれもメモリ回路に有効である。ECC 訂正および訂正データ上書きの方法では訂正が可能なビット数が限定されるのに対し、設定データ上書きの方法では全データの訂正が可能である。なお、ECC 訂正および訂正データ上書きの訂正可能ビット数はチェックおよび訂正方式の拡張により開発世代ごとに向上する傾向にある。

初期設定方式は、初期設定範囲からパッケージリセット、デバイスリセット、FPGA リコンフィグレーション、CPU リブートの各種方法に分類される。パッケージリセットの場合は、保守単位と一致するため特殊な制御を伴わずに実現できる。一方、デバイスリセットや FPGA リコンフィグレーションの場合には、訂正時間の短縮が可能となるが、正常動作を継続させるために周辺回路との状態整合処理に注意する必要がある。これら訂正処理の実行制御手段としては、制御プログラム自律で行う場合と保守者の指示による場合がある。初期設定実行時、サービス影響が大きくなる可能性がある場合は、保守者が影響度合いを評価して実行の可否を判断すべきである。

9.4　設定データ格納メモリに対するソフトエラー訂正の対策例

設定データ格納メモリに対するソフトエラー訂正の対策例を表 9.4 に示す。

表 9.4　設定データ格納メモリに対するソフトエラー訂正の対策例

項番	ソフトエラー訂正の対策例		MCU対策への有効性	サービス信頼度への影響	保守信頼度への影響
	検出法	訂正法			
1	パリティチェック	設定データ上書き	無	有	無
2		CPU リブート	無	無（＊）	無
3	CRC チェック	設定データ上書き	有	有	無
4	ECC チェック	ECC訂正／訂正データ上書き	無	無	無
5		ECC 訂正／訂正データ上書き（対SCU）+ 設定データ上書き（対MCU）	有	有	無
6	ECCチェック（ビットインタリーブ構成のメモリの場合）	ECC訂正／訂正データ上書き	有	無	無

＊信号影響無ブロックへ適用する場合が一般的のため“無”としたが、装置構成上信号影響有ブロックに適用する場合には“有”となる。

パリティ符号や CRC の様に訂正機能がない検出方法を適用したメモリを使用する場合は、別途不揮発メモリ等に格納されている設定データの上書き処理を行うのがよい。
また、ECC 訂正や訂正データ上書きでエラー訂正機能がある方法を採用する場合で、MCU による故障率が要求信頼度クラスを満たさない場合は、設定データ上書き処理をすることにより MCU からの復旧を実施すべきである。さらに、ビットインタリーブ構成としたメモリであれば MCU に対しても ECC 訂正が可能である。
また、CPU の場合はパリティエラーを検出した場合はリブートを行うことでソフトエラーから回復可能である。

9.5　動作制御メモリ／論理回路に対するソフトエラー訂正の対策例

動作制御メモリ／論理回路に対するソフトエラー訂正の対策例を表 9.5 に示す。

表 9.5　動作制御メモリ／論理回路に対するソフトエラー訂正の対策例

項番	ソフトエラー訂正の対策例		MCU 対策への有効性	サービス信頼度への影響	保守信頼度への影響
	検出法	訂正法			
1	パリティチェック	デバイス／パッケージリセット	無	有	無
2		遠隔リセット制御	無	有	有
3		CPU リブート	無	無（＊）	無
4	CRCチェック	デバイス／パッケージリセット	有	有	無
5		遠隔リセット制御	有	有	有
6	ECCチェック	ECC 訂正／訂正データ上書き	無	無	無
7		ECC 訂正／訂正データ上書き（対 SCU） (to SCU) ＋デバイス／パッケージリセット（対MCU）	有	有	無
8	冗長回路出力データ照合	デバイス／パッケージリセット	有	有	有
9	WDT監視	CPU リブート	有	無（＊）	無
10	OAMデータ送受信	デバイス／パッケージリセット	有	有	無

＊信号影響無ブロックへ適用する場合が一般的のため“無”としたが、装置構成上信号影響有ブロックに適用する場合には“有”となる。

パリティチェックや CRC チェックの様に訂正機能までない機能のみを搭載したメモリの場合は、エラー検出時にデバイス／パッケージのリセットを行ってソフトエラーから回復することが可能である。ただし、デ

バイス/パッケージのリセット時に無視できないクライアント信号断が伴う場合には、ソフトエラー故障発生率からサービス信頼度基準を満たすかを確認する必要がある。もし、満たさないようであれば、ECC 訂正や訂正データ上書き機能の実装、冗長構成化等の改善を行う必要がある。

ECC 訂正や訂正データ上書きの様なエラー訂正機能のみを搭載している場合で、MCU のソフトエラー故障率が要求信頼度クラスを満たさない場合は、デバイスまたはパッケージリセット処理をすることにより、MCU まで復旧させるべきである。

ソフトエラー故障発生率から保守信頼度基準を満たすようであれば、サービス影響を考慮しエラー検出をトリガに保守者判断で遠隔リセット制御を行うことでよい。

また、パリティ符号のようなエラー検出符号を適用できない論理回路には回路の二重化による照合または OAM データ送受信によるエラー検出を行うことで異常を検出し、デバイス／パッケージリセットを行うことによりソフトエラーから回復が可能である。なお、回路の二重化による照合で検出する場合には、いずれの回路でエラーが発生しているか不明のため保守者の裁量が要求される。

また、CPU の場合はパリティもしくは WDT によりエラーを検出した場合はリブートを行うことでソフトエラーから回復可能である。

9.6　バッファメモリに対するソフトエラー訂正の対策例

バッファメモリについては 8.1 節で述べたように、常時新たな正常データが上書きされることから、ソフトエラー影響は一時的なものであり、ソフトエラー対策を行わなくても信頼度への影響は小さい。ソフトエラー影響をなくしエラーデータの後位装置への流出防止や短時間のクライアント信号断回避のための対策例を表 9.6 に示す。基本的に ECC 対策を推奨するものであり、さらにメモリのビットインタリーブと ECC を組み合わせることで MCU まで対処可能となる。

表 9.6　バッファメモリに対するソフトエラー訂正の対策例

項番	ソフトエラー訂正の対策例		MCU対策への有効性	サービス信頼度への影響	保守信頼度への影響
	検出法	訂正法			
1	ECC チェック	ECC 訂正	無	無	無
2	ECCチェック（ビットインタリーブ構成のメモリの場合）	ECC 訂正	有	無	無

9.7　サイレント故障の定義と考察

この勧告で定義されているソフトエラーによって引き起こされるサイレント故障は、勧告 K. 124（第 7.2 節）に記述されているように、故障によってクライアント信号に無視できない影響があっても、キャリアネットワークのオペレーションシステムまたはメンテナンス担当者に故障が報告されないことである。その故障に保守者が気づく前に、ユーザからの申告があることもある。

9.7.1　キャリアネットワークにおけるクライアント信号監視機能構成

図 9.1 はキャリアネットワークに収容されているユーザ間のクライアント信号の接続形態を示す。

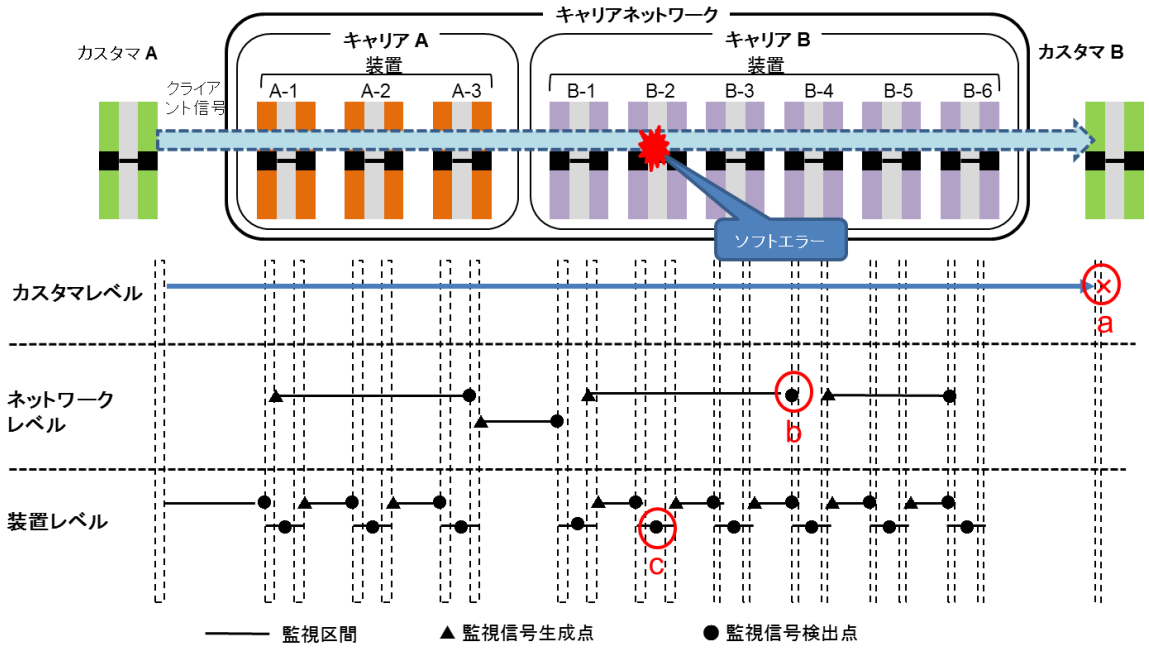

図 9.1　キャリアネットワークにおけるクライアント信号の正常性監視機能配備

カスタマ A からカスタマ B へのクライアント信号伝送経路と、各キャリアネットワーク内にある複数の装置を示している。あわせて、同図にキャリアネットワーク内の伝送区間ごとのネットワークレベル監視と個々の装置の装置レベル監視を併用した、クライアント信号伝送のエラー監視機能の一般的な配備構成を示す。

ネットワークレベルの監視は、クライアント信号にオーバーヘッドを付加した SDH フォーマット伝送やクライアント信号ルートへの OAM パケットの重畳により監視するものである。これら監視信号の生成個所から検出箇所間の装置すべてが監視区間となるため、複数装置が含まれた場合には異常個所を装置単位で特定はできない。一方、装置レベルの監視は、装置内および対向装置からの信号の異常を装置内に配備した機能により検出するもので、異常個所を装置単位で特定が可能である。

9.7.2　サイレント故障と警報機能信頼度の関係

図 9. 1 の構成のネットワークにおけるサイレント故障の例について述べる。

装置 B-2 でソフトエラーが発生し、カスタマ B で異常を検出したとする。この場合、ネットワークレベルの b 点と装置レベルの c 点で異常を検出すべきであり、これにより異常個所が装置 B-2 と特定できる。この状態であればサイレント故障対策が図られており本故障モードは警報機能信頼度基準の対象外となる。これに対し、b 点、c 点ともに異常が検出されない場合は、キャリアネットワークでサイレント故障が発生したことになり装置 B-2 の警報機能信頼度基準の対象となる。

一方、b 点では検出するが c 点は未検出の場合、ネットワークレベルでは異常を検出しており、定義を厳格に適用するとサイレント故障ではないが、異常装置の特定ができず、特定に時間を要することになる。このため、このような場合はサービスや保守への影響は大きくサイレント故障と似た影響が発生する。したがって、これをサイレント故障として警報機能信頼度基準の対象とするか否かはキャリアと装置ベンダ間の合意によって決めるべきである。

9.7.3　サイレント故障対策設計時の注意点

装置設計においてサイレント故障回避対策を実現するうえで主に以下の点を注意すべきである。

(a) 従来から一般的に使用されてきたパリティチェックでは、発生頻度が高くなったメモリのマルチビットエラーを検出できず、サイレント故障回避効果が小さくなってきている。

(b) ソフトエラーの故障モードは部品の劣化故障と異なりメモリ１ビット、または論理ゲート１個、配線１本程度の局所故障となる。それゆえ、機能異常検出回路を実装設計するに当たり、故障パターンを網羅することが困難な場合がある。特にメモリ（CRAM）に回路構成を設定する FPGA においてこの特徴が顕著である。CRAM の使用率は一般的に 10～20％程度であり、CRAM におけるソフトエラー起因のビット反転の大半が未使用部分で発生する機能に影響のないエラーである。このため、装置として CRAM エラー検出による警報通知は行わず、別の機能による異常検出回路を実装して対策をとることがある。

１０．ソフトエラー対策適用時の注意点

本節では、ソフトエラー対策適用時に装置設計上注意すべき点について述べる。

10.1　冗長構成機能ブロックのソフトエラー対策

冗長構成を活用する装置のソフトエラー対策では、ECC 訂正のようなサービス影響のない方法で訂正が不可能なソフトエラーを検出した時には、6.3.2 項で述べたようにクライアント信号を冗長パスに即時に切替えを行うことが基本である。その後、故障状態にある装置に対して初期設定等のエラー訂正処理を行う。

しかし、図 10.1 に示すように複数のクライアント信号を一つのパッケージで処理する構成の場合には以下の考慮が必要である。

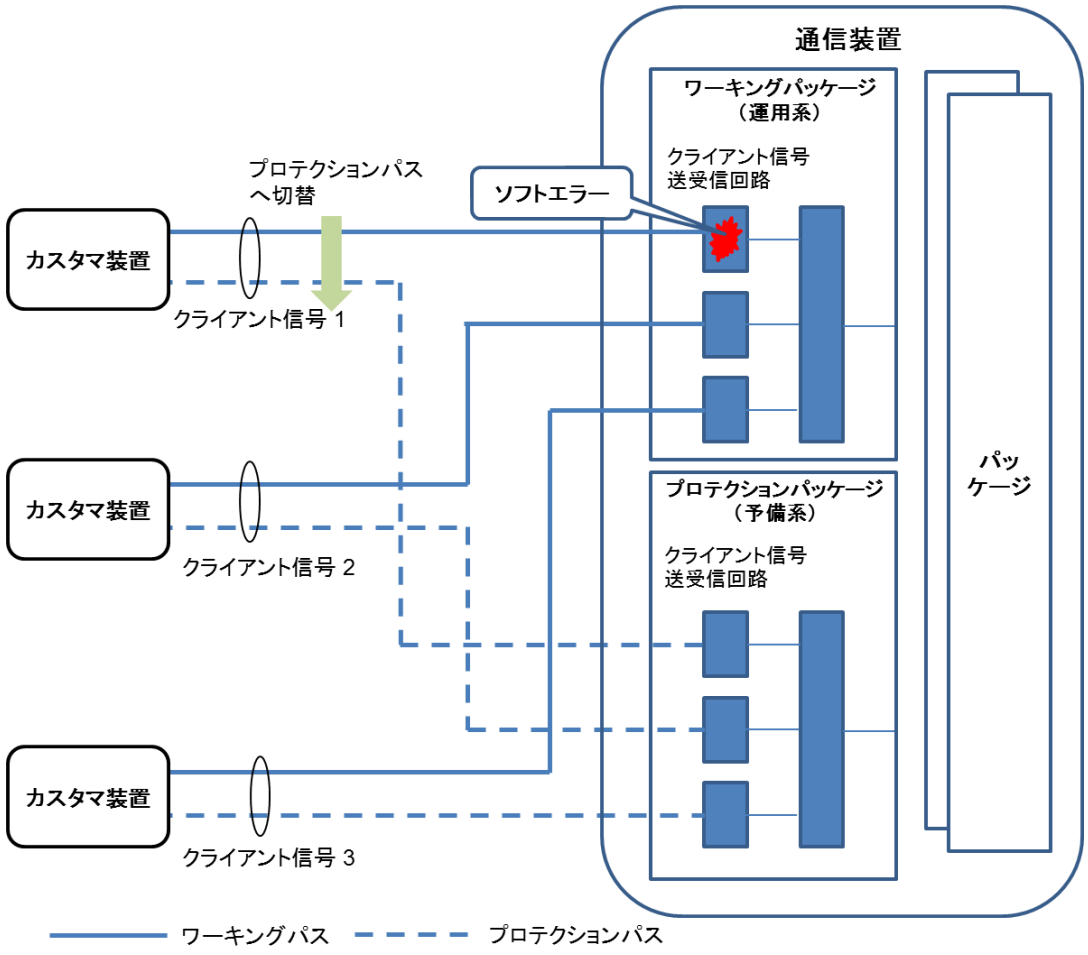

図 10.1　パッケージの冗長構成例

図 10.1 の例では、冗長構成による対策の実行が以下のように限定されるとする。

(a) ソフトエラーを検出したクライアント信号送受回路ブロックは他のブロックと無関係に、運用系の切り替えが可能である。

(b) 回路ブロック単位でのリセットや設定データ上書きはできず、ソフトエラーを復旧させるためにはパッケージの初期設定が必要である。

図 10.1 は、ワーキングパッケージとプロテクションパッケージで冗長構成を組んでおり、クライアント信号 1～3 のワーキングパスはすべて現用系のワーキングパッケージで動作している図である。ここで、すべてのクライアント信号 1～3 がワーキングパッケージの送受信回路で伝送されているときに、クライアント信号 1 の回路でソフトエラーが発生した場合を想定する。クライアント信号 1 についてはプロテクションパスを使用するために前提(a)で示すクライアント信号回路切替機能により装置自律でプロテクションパッケージのクライアント信号送受信回路を運用系に切替えることで、クライアント信号の瞬断のみでサービスを継続できる。

しかし、ソフトエラー訂正し設備復旧するためには、ワーキングパッケージに対して前提(b)で示すパッケージのリセットを実施する必要があるので、クライアント信号 2,3 もプロテクションパスを使用するために、プロテクションパッケージのクライアント信号送受信回路に切替える必要がある。この場合は、ソフトエラー影響のなかったクライアント信号 2,3 も、切替時に瞬断を発生させることとなる。

このとき発生するクライアント信号 2，3 の瞬断の影響が大きい場合には、例えばサービス影響の少ない時間を選んで実施する必要がある。保守者とユーザの協力の下で切替のタイミングを決定し手動で切り替えることになる。この場合には保守稼働が増加するので保守信頼度基準の対象となる。

クライアント信号の瞬断が許されるかどうかはキャリアの要求条件によって異なる、従って、ソフトエラー対策の適用方法すなわち装置自律で実行するか、保守者の判断で実行するかは、事業者によって選択できる設計とすることが望ましい。

10.2 ソフトエラー対策を考慮した通知メッセージ設計法

ソフトエラー対策実施時の、保守者への通知メッセージ推奨設計法について述べる。

物理欠陥故障の復旧にはパッケージ交換等の現地保守作業が基本である。これに対し、ソフトエラーの復旧には下記の装置対策動作および保守アクションとなり、パッケージ交換作業は不要である。

- 大抵の場合は、装置自律の復旧処理が可能で保守者対応が不要である
- 保守者介在の復旧処理でも遠隔操作による対応が基本であり現地対応は非常に稀である。

保守者対応が必要となるソフトエラーの通知メッセージの発出法は自律回復対策が適用されている場合と異なる。Annex A に通知メッセージの詳細について述べる。

次の全ての条件が満たされる場合には、通知メッセージの発出は不要である：

(1)ソフトエラー対策をハードウェア自律処理等により実現し、

(2)サービスへの影響なく瞬時に訂正し、

(3)対策実行時に冗長切替や初期設定等の装置状態変化を伴わない。

ただし、その場合でも保守者が取得できるパフォーマンスモニタにソフトエラー発生履歴を保存しておくことが望ましい。

10.3 ソフトエラー発生履歴の保存

ソフトエラー対策時は、10.2 節で述べた保守者通知を行うことを推奨する。さらに、装置側の故障解析のた

めに、ソフトエラー履歴を残すことは重要である。そこで、ソフトエラーとして認知した事象については、エラー検出時間およびパリティエラー、CRAM エラー、デバイスエラー等のエラー内容をログとして保存すべきである。これによって、故障返却時に該当パッケージ内のログで故障要因を容易に特定できるようにすることが望ましい。また、そのログについては将来の故障原因調査のために装置寿命の間は保存できることが望ましい。

10.4　初期立上げデータ格納メモリのソフトエラー対策

6.3.3 項で述べたように初期立上げ時等に必要なデータやプログラムは一般的に装置内の不揮発性メモリに格納されている。これらにソフトエラーが発生したまま放置した場合、故障が多発し、故障取替パッケージが不足する等の懸念がある。これが装置信頼上許容できない場合には、ECC 訂正対策により自律復旧させる、あるいは定期読出しによりエラーを早期に検出して訂正する対策を行うことを推奨する。

10.5　物理欠陥故障の区別による訂正処理のリピート防止

物理欠陥故障の場合はソフトエラー対策で実行した訂正処理後もエラーは継続するので、ソフトエラー訂正処理がリピートしないようにする必要がある。その際に、ソフトエラー訂正処理が有効に働いたか否かを判定するための適切な復旧保護時間を設け、ソフトエラーと物理欠陥故障の切り分けができるようにする必要がある。

10.6　CPU 内部メモリ使用上の注意

汎用ＣＰＵデバイスでは、内部メモリにパリティチェックや ECC チェック機能もないものがある。プログラムが動作しており、内部メモリがワークエリアとして使用されている場合はＷＤＴ検出できるが、設定データ格納メモリで使用する場合は上書き動作もなくソフトエラー状態が継続したままとなり誤動作要因となる。したがって、パリティチェックも ECC チェック機能がない場合には、設定データ格納メモリ用途では使用しないことを推奨する。

１１．ソフトエラー信頼度評価法

本節では、装置設計後のソフトエラー信頼度評価法について述べる。

表 11.1 に評価法を示す。これらの評価は、ハードウェア、制御プログラム等を含めた装置の総合動作についてのソフトエラーに対する信頼度を推定するものであり、これらを基に対策妥当性および基準への適合性を分析する。その結果、要求基準を満足しない場合には装置の設計を見直す必要がある。

表 11.1　ソフトエラー信頼度評価法

種別		方法	主要用途	参照先
机上	ソフトエラー対策設計の信頼度算出	表8.4を更新し、ソフトエラー対策設計後の発生率を算出	装置製造ベンダによる対策設計の妥当性確認	表11.2
実機	エラー挿入試験	装置動作中にデバイス内の任意のビットを反転させ擬似的にソフトエラーを発生		TR-Ksup.11
	中性子照射試験	粒子加速器からの高速中性子ビームを装置全	信頼度クラス適合性の確認	JT-K130

		体に照射	試験	

設計初期段階に 8.2 節で示した予測手法に従って、設計初期に計算したソフトエラー故障発生率に対し、回路設計および装置設計段階で盛り込んだソフトエラー対策を反映した後のソフトエラー故障発生率を算出する。評価は、表 11.2 の項目に対して行う。

表 11.2　ソフトエラー対策設計評価例

機能ブロック故障時のクライアント信号影響 (図 6.1)	種別		機能／使用形態	回路種別	SEFR計算値（FIT）	
					サービス信頼度	保守信頼度
影響無	(1) CPU 周辺回路	1	コア	論理回路	ソフトエラー対策後のFIT数を算出	
		2	内部メモリ（動作制御、設定データ、データバッファ）	SRAM		
		3	主メモリ（動作制御、設定データ、データバッファ）	DRAM		
		4	バックアップメモリ （設定データ）	フラッシュメモリ		
		5	キャッシュメモリ（動作制御）	SRAM		
	(2) FPGA 周辺回路	1	外部メモリ（設定データ）	フラッシュメモリ		
影響有		2	コア	論理回路		
		3	コンフィグレーションメモリ（設定データ）	SRAM		
		4	ブロックRAM（動作制御、設定データ、データバッファ）	SRAM		
		5	外部メモリ（データバッファ）	SRAM		
		6	外部メモリ（設定データ）	SRAM		
	(3) ASIC 周辺回路	1	コア	論理回路		
		2	内部メモリ（動作制御、設定データ、データバッファ）	SRAM		
		3	外部メモリ（データバッファ）	SRAM		

		4	外部メモリ（設定データ）	SRAM	

実機評価手法としてはエラー挿入試験と中性子照射試験がある。エラー挿入試験は、装置動作中に装置内メモリの任意のビットを反転させ擬似的にソフトエラーを発生させて行う試験である。これによりソフトエラー対策の装置としての動作の妥当性を評価できる。特に、ソフトエラーの影響を受けやすい FPGA の CRAM に対しては、FPGA ベンダが提供するエラー挿入試験ツールを利用できる。中性子試験は、加速器中性子源を用いて動作中の装置に中性子を照射させ、実環境に対したとえば数百万倍という加速を与える試験である。中性子照射試験では実際と同じ装置構成と動作状態でソフトエラーの影響を評価できる。

ソフトエラー対策設計評価計算およびエラー挿入試験は、主に装置開発ベンダの設計妥当性評価用途である。これに対し中性子照射試験は、ソフトエラー信頼度基準への適合性評価用として利用可能であり、評価結果はキャリアと装置開発ベンダが互いに装置のソフトエラー信頼度として共有できる指標である。

付属資料 A：ソフトエラー対策用通知メッセージの設計法

10.2 節で述べたソフトエラー対策用通知メッセージ設計の考え方の詳細を以下に示す。

A.1　装置自律のソフトエラー対策実行時の通知メッセージ

図 A.1 に、ソフトエラー対策を装置自律で実行する場合の通知メッセージ発出法の設計例を示す。

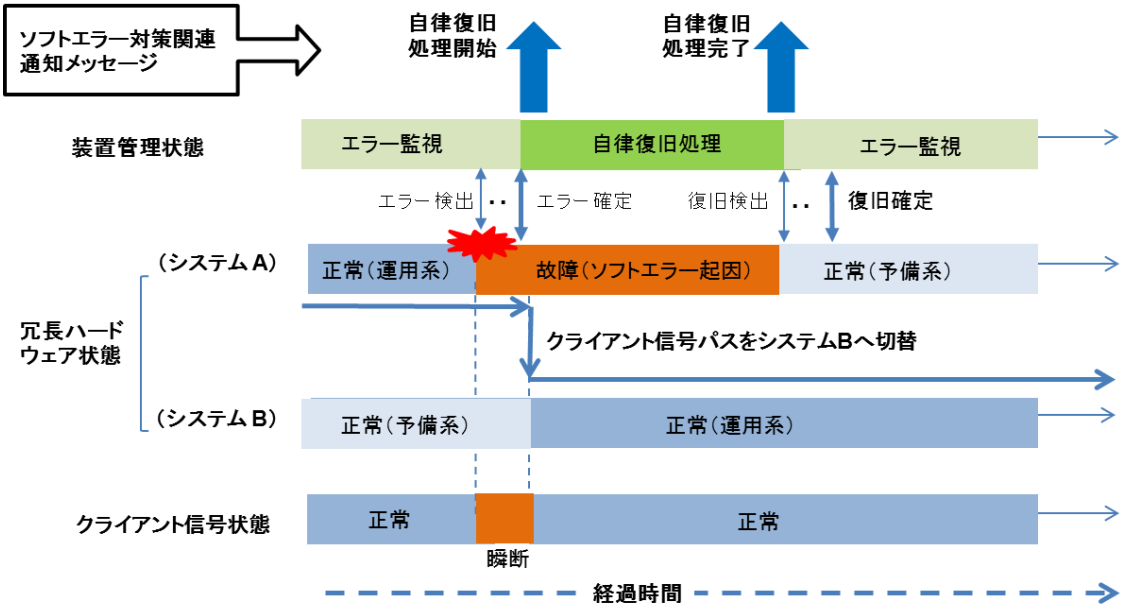

図 A.1　装置自律のソフトエラー対策実行時の通知メッセージ発出法

図 A.1 は、クライアント信号状態、そのクライアント信号を転送する冗長構成を持つ回路のシステム A およびシステム B のハードウェアの状態、それらのハードウェア状態を管理する制御機能ブロック（プログラム）による装置管理状態、および発出されるソフトエラー対策関連の通知メッセージを左から右への時間経過として示している。

この時、ソフトエラーに対する故障対策を行なっていない場合はシステム A ハードウェアの修理対応を保守者に促すために装置故障アラームの通知メッセージを発出するのが一般的である。しかしソフトエラー対策を盛り込んだ場合には、不要な保守者稼働を回避するために装置故障アラームは発出しない。

その代わりに運用系の切替を行い非運用系となったシステム A に対し、9.3 節で述べたソフトエラー訂正対策を装置自律で実行する。この装置自律復旧処理の開始と完了を通知するために、これらの事象の通知メッセージを両方の時点で発出する。その後装置としては、一定の保護時間をとり復旧したことを確認する。これらの対となる通知メッセージは、ソフトエラー発生履歴を通知するためのものであり、保守者対応は不要であることから、注意レベルの通知とするのが望ましい。なお、図 A.1 ではクライアント信号に影響ある場合の例を示したが、クライアント信号に影響ない場合でもソフトエラー対策のために冗長切替が発生する場合は、通知メッセージ発出法は同一とすることを推奨する。

一方、ハードウェア故障発生時点ではソフトエラー故障と物理欠陥故障を区別できない。物理欠陥故障が原因の故障でソフトエラー対策の手順が実行された場合の通知メッセージの発出例を図 A.2 に示す。

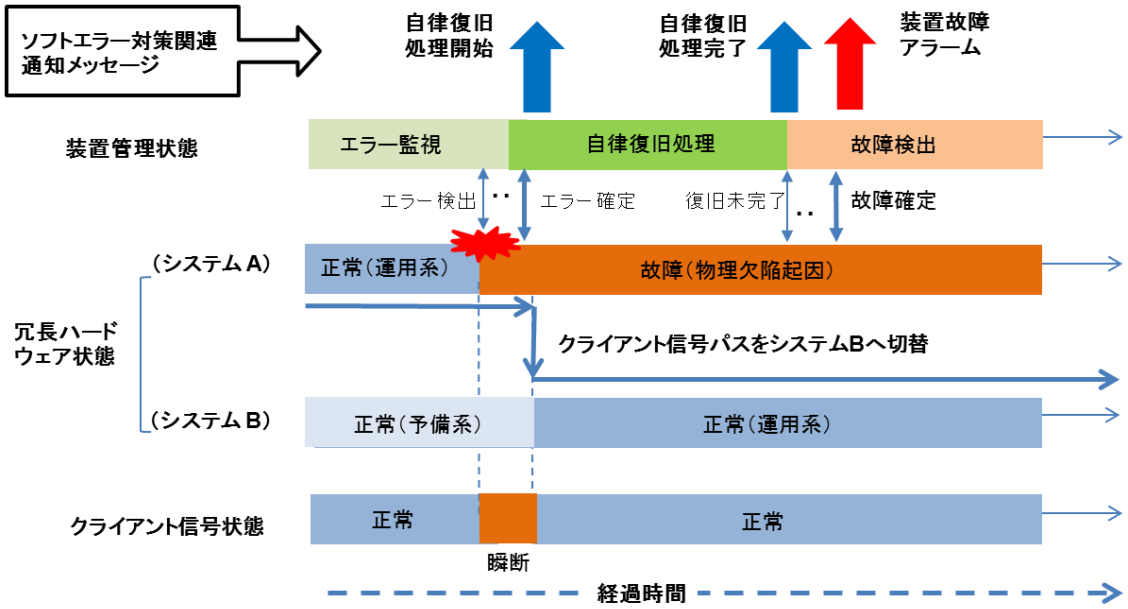

図 A.2　物理欠陥故障修復のため装置自律のソフトエラー対策実行時の通知メッセージ発出法

ソフトエラーの復旧手順を実行している期間、すなわち、ソフトエラー自律復旧処理開始／完了の通知メッセージは送出するまでは、図 A.1 と同一である。しかし、物理欠陥故障時は、故障は復旧せず、復旧処理完了後も故障状態が継続することになる。この場合には、保守者によるパッケージ交換等の対応を促すことが必要になることから、故障が持続していることが判明した時点で装置故障アラームメッセージを発出する。このように、装置信頼度の向上及び保守者稼働の削減の観点からソフトエラー被疑の故障に対しては物理欠陥修復よりソフトエラー対策を優先して実行するが、故障復旧ができなかった場合には装置故障アラームを発出する必要がある。

A.2　保守者介在のソフトエラー対策実行時の通知メッセージ

図 A.3 に、ソフトエラー対策を保守者介在が必要な場合の通知メッセージ発出法の設計例を示す。この例では、図 10.1 で示す構成の装置で、ソフトエラーがクライアント信号 1 のクライアント信号送受信回路で発生した場合を示している。ワーキングパッケージとプロテクションパッケージで冗長構成を組んでおり、クライアント信号 1～3 のワーキングパスはすべて現用系のワーキングパッケージで動作する。また、10.1 節の仮定(a)、(b) を適用する。

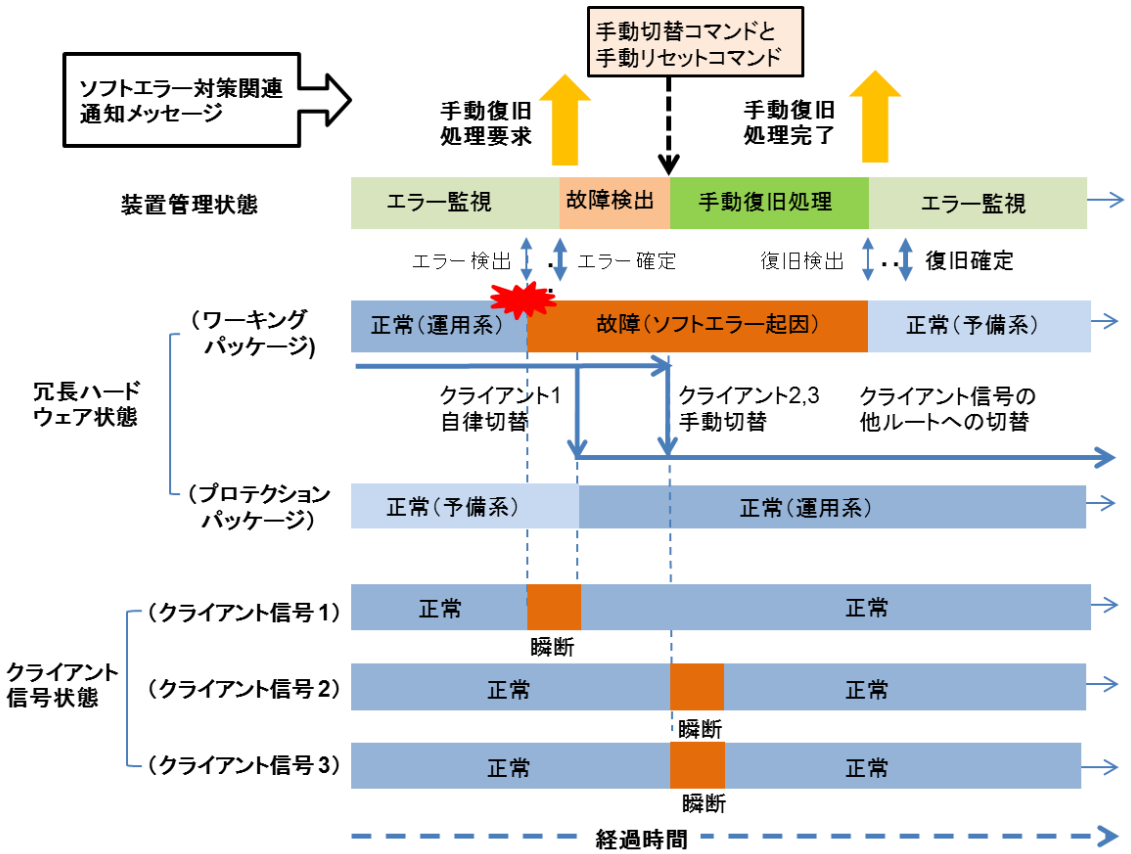

図 A.3　保守者介在のソフトエラー対策実行時の通知メッセージ発出法

クライアント信号 1 の送受信回路で、ソフトエラーが発生し故障を確定すると、クライアント信号 1 は信号経路をプロテクションパスに切替える。これによりクライアント信号 1 は瞬断のみでサービスは継続できる。

ここで、信号パス切替や初期設定のようなソフトエラー対策をワーキングパッケージに対して実施する場合には、ワーキングパスを使用しているクライアント信号 2, 3 に信号断等の影響が発生する。このため 10.1 節で説明したように保守者による手動制御が必要となる。従って、ソフトエラー対策対応を保守者に要求することを表す通知メッセージを発出する。保守者はこれを受け、サービス影響が許容されるときにクライアント信号 2, 3 の信号パスをプロテクションパッケージに切替えワーキングパッケージを予備系にする。その後に保守者は遠隔からリセットを行い、パッケージを修復する。

次に、ソフトエラー対策の復旧処理が完了した時点で、通知メッセージを発出しその後、一定の時間後に復旧したことを確認する。

このように、通知メッセージから保守者がソフトエラー起因の故障であり正常に復旧したと認識できた場合は、そのまま装置を継続使用でき、パッケージ交換等の対応を行わなくて済む。また、これらの対となる手動復旧処理要求／完了の通知メッセージは保守者介在を促す意味から装置故障アラームと同等のアラームレベルの通知とするのが望ましい。

図 A. 3 の回復手順を実行しその結果故障が物理欠陥起因の故障であった場合の例を図 A. 4 に示す。

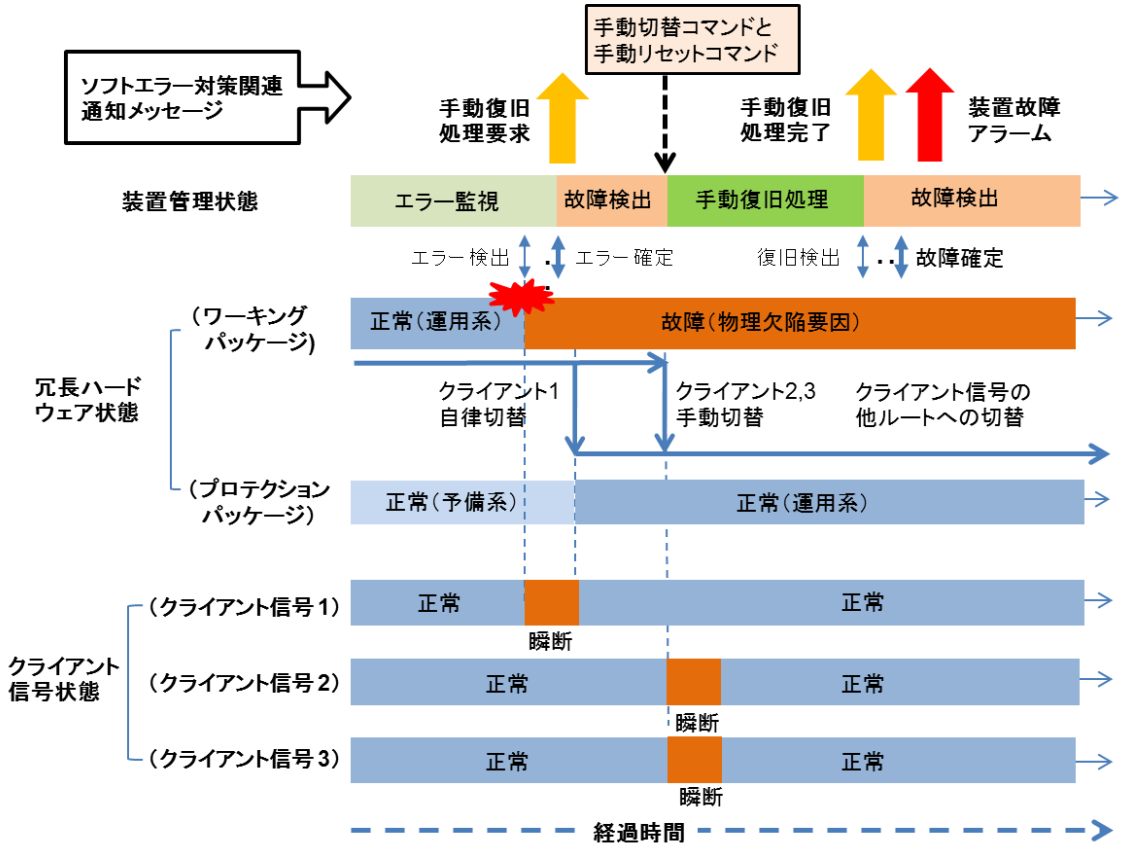

図 A.4　物理欠陥故障修復のための保守者介在ソフトエラー対策実行時の通知メッセージ発出法

保守者介在のソフトエラー対策が完了し通知メッセージを発出するまでは図 A.3 と同一である。しかし、物理欠陥故障時は、故障は復旧せず、復旧処理完了後も故障状態が継続することになる。この場合には、保守者によるパッケージ交換等の対応を促すことが必要になることから、故障が持続していることが判明した時点で装置故障アラームメッセージを発出する。このように、装置信頼度の向上及び保守者稼働の削減の観点からソフトエラー被疑の故障に対しては物理欠陥修復よりソフトエラー対策を優先して実行するが、故障復旧ができなかった場合には装置故障アラームを発出する。

付録Ⅰ：半導体のソフトエラー耐性の傾向

SRAM

論理回路や DRAM、SRAM、フラッシュメモリなどの回路の中では SRAM がソフトエラーに最も弱いということは半導体業界では良く知られている。LSI プロセスの微細化により発生頻度が増加傾向にあり、影響が顕著になる傾向であり、フィールドにおける最近の発生もほとんどが SRAM である。

SRAM のソフトエラーでは、一回の中性子入射により単一メモリセルのみ反転する場合と隣接する複数メモリセルが同時に反転する場合を想定する必要がある。反転値は保持されるため、正常化には再書き込みが必要であるという特徴がある。対策として、ECC 付加やインタリーブ、定期的保存データチェック等の対策が取られている。

DRAM

ソフトエラーは 1980 年頃、DRAM セルキャパシタで問題視されていた。IC パッケージ材料に微量不純物として含まれる放射性物質のウラン(U)から発生するアルファ線が DRAM のソフトエラーの主な原因であったため、^{238}U や ^{232}Th をはじめ、放射線を放出する不純物を IC パッケージ材料から低減するなど、様々な対策を施した。また 1Mbit DRAM 以降（現状は Gbit メモリが主流)、DRAM セルキャパシタの構造がプレーナ型から積み上げ型(スタック型) またはサブストレートプレート型のトレンチ構造に変更され、トランスファートランジスタの最少化が図られたことでソフトエラー耐性が高まったため、DRAM におけるソフトエラー発生率は大きく改善し、単位容量当たり SRAM の 1/1000～1/10000 と非常に小さい。但し、装置設計時は使用容量に対応した実際のソフトエラーレートを算出して対策の要否を考慮すべきである。

フラッシュメモリ

フラッシュメモリでは過去、ソフトエラーは起こらないとされてきた。フラッシュメモリのメモリセルは、絶縁膜で周囲を囲まれた電極に電荷(電子)を蓄えてデータを記憶する(フラッシュメモリの主流であるフローティングゲート方式の場合)。フラッシュメモリセルに荷電粒子が突入しても、蓄積されたデータの破壊が発生することはないと考えられている。しかし最近になってフラッシュメモリでも微細化によって蓄える電子の数が減少し、ソフトエラーが発生することが分かってきた。単位容量当たりソフトエラーの発生確率そのものは、SRAM に比べると 100 分の 1 程度にとどまっているとの実験例はあるが、NOR 型、NAND 型共に、微細化及び高容量化に加え、セル構造が SLC⇒MLC⇒TLC となり、ソフトエラー発生率が増加傾向にある。25nm MLC フラッシュメモリでは、bit 当たりの中性子断面積が SRAM と同程度の 1×10^{-14} オーダであるとの実験結果も報告されている[b-RADEC]。したがって、装置設計時は使用容量に対応した実際のソフトエラーレートを算出して対策の要否を考慮すべきである。

論理回路

ソフトエラーはこれまで、半導体メモリで問題となってきた。マイクロプロセッサのキャッシュに使われる SRAM では、パリティチェックや ECC チェックなどのソフトエラー対策が半ば常識となっている。2009 年頃になって注目を集めだしたのが、大規模ロジック、すなわち論理回路のソフトエラーである。半導体製造技術の微細化とともに、クローズアップされるようになってきた。論理回路はメモリ回路と違い、ソフトエラー対策に ECC チェックが使えない。このため、論理回路に適したソフトエラー対策の研究が活発になって

きた。

論理回路は大別すると、順序回路と組み合わせ回路に分かれる。順序回路は、内部の状態が保持されており、外部からの入力と内部の状態によって出力が決まる。代表的な回路素子にはフリップフロップやラッチ、カウンターなどがある。これに対して組み合わせ回路は、外部からの入力だけによって出力が決まる。代表的な回路素子にはインバータや NOR ゲート、NAND ゲートなどがある。順序回路と組み合わせ回路では、ソフトエラーの起こりやすさに圧倒的な違いがある。順序回路の回路素子は内部状態を保持しているので、ここを中性子衝突によって生成された荷電粒子が通過すると保持された論理値は簡単に反転してしまう。例えば 32nm の CMOS プロセスで製造した組み合わせ回路のソフトエラー発生率は順序回路のソフトエラー発生率の 10%未満に過ぎなかったという研究報告がある [b-IEEE-2]。そこで論理回路のソフトエラー対策とは、順序回路のソフトエラー対策が主眼になっている。

しかし、ごく最近では組み合わせ回路のソフトエラーを問題視する研究も出てきている。ソフトエラーは高周波化により発生確率が上昇する可能性があるとされ、高速動作するプロセッサ等で問題になる可能性がある。これはラッチするクロック周波数が高速になればその分ラッチ回数が増えるため、ソフトエラーが発生した際その誤情報のラッチ率も上昇するためである[b-IEEE-3]。現時点で、このエラーを低減させる安価な対策が十分把握されていないので、組み合わせ回路のソフトエラー率改善に向けた高速で高精度の解析技術が求められている。中でもソフトエラー脆弱性見積もり技術はいくつか提案されつつある。

以上のように半導体加工技術の微細化と半導体デバイスの高密度化に伴い、今後は論理回路でもソフトエラーを考慮しなければならない局面が増えると想定される。たとえば、冗長回路は確実なソフトエラー対策である半面、シリコン面積の増加が大きいという弱点を抱えており、より実用的な各種対策が研究されている段階にある。現時点で、論理回路のソフトエラーがフィールドの装置や加速器中性子源による実験において問題になっているケースは見られないが、今後の動向を注視する必要がある。

参考文献

[b-IEEE-1] Eishi Ibe, *et al*., *Scaling Effects on Neutron-Induced Soft Errors in SRAMs from a 250 nm to a 22 nm Design Rule*, IEEE TRANSACTIONS ON ELECTRON DEVICE, VOL. 57, No. 7, July 2010.

[b-IEEE-2] Matthew J. Gadlage, *et al*., *Comparison of Heavy Ion and Proton Induced Combinatorial and Sequential Logic Error Rates in a Deep Submicron Process*, IEEE TRANSACTIONS ON NUCLEAR SCIENCE, Vol. 52, No. 6, December 2005.

[b-IEEE-3] B. Gill, et al., *Comparison of Alpha-particle and Neutron-induced Combinational and Sequential Logic Error Rates at the 32nm Technology Node*, 2009 IEEE International Reliability Physics Symposium.

[b-RADEC] M. Bagatin, et al., *Neutron and Alpha SER in Advanced NAND Flash Memories*, Radiation and Its Effects on Components and Systems (RADECS), 2013, H-3.

[b-Xilinx] Xilinx, *Device Reliability Report UG116*