プログラマブル電子安全システムの要求水準

【仕様】以下の PESSRAL 基準（ISO22201）等の要件を有すること。

・電気安全装置の安全度水準(SIL)は、表 A.1、表 A.2 による。

・すべての安全度水準に共通な安全機能の最小限の要件は、表 B1、表 B2、表 B3 による。また、SIL 1、2、3 について要求される手段は表 C1、表 C2、表 C3 による。

・安全でない改造を避けるために、PESSRAL のプログラムコードと安全に関連するデータに対する許可のないアクセスを防止する措置を、たとえば、EPROM、アクセスコードを用いて実施すること。

・PESSRAL と安全に関連しないシステムが同じハードウェアを共有する場合には、PESSRAL についての要件を満たすこと。

・PESSRAL と安全に関連しないシステムが同じプリント基板を共有する場合には、二つのシステムの分離に関する EN81-1:13.2.2.3 の要件を適用する。

(注) 表 B,表 C に記載する EN 61508-7:2001 の条項は、EN 61508-2:2001 と EN 61508-3:2001 中の関連する要件を引用している。

(*) 電気、電子、プログラマブル電子安全関連系の機能安全
EN 61508、IEC 61508、JIS C 0508(IDT IEC61508)

表 A.1　電気安全装置のリスト

EN81の条項	チェックの対象装置	SIL
5.2.2.2.2	点検用ドア、非常用ドア、点検用トラップドアの閉鎖状態をチェック	2
5.7.3.4a)	ピットの中の停止装置	2
6.4.3.1b)	機械装置の不動作位置のチェック	3
6.4.3.3e)	かごの中の点検用トラップドアと点検用ドアの閉鎖状態をチェック	2
6.4.4.1e)	ピットに立ち入るための戸が鍵を使用して開くことをチェック	2
6.4.4.1f)	機械装置の不動作位置のチェック	3
6.4.4.1g)	機械装置の動作位置のチェック	3
6.4.5.4a)	折りたたみ式のプラットフォームの完全に折りたたんだ位置のチェック	3
6.4.5.5b)	可動ストップの完全に折りたたんだ位置のチェック	3
6.4.5.5c)	可動ストップの完全に伸ばした位置のチェック	3
6.4.7.1e)	出入り口ドアの閉鎖位置のチェック	2
6.4.7.2e)	出入り口ドアの閉鎖位置のチェック	2
6.7.1.5	綱車室の中の停止装置	1
7.7.3.1	乗り場の戸の施錠のチェック －7.7.4.2に従って自動的に動作する乗り場の戸 －手動による乗り場の戸	 2 3
7.7.4.1	乗り場の戸の閉鎖位置のチェック	3
7.7.6.2	錠のないパネルの閉鎖位置のチェック	3
8.9.2	かごの戸の閉鎖位置のチェック	3
8.12.4.2	かごの非常用トラップドアと非常ドアの施錠のチェック	2
8.15b)	かご上の停止装置	3
9.5.3	2ロープタイプと2チェーンタイプの懸垂式の場合のロープまたはチェーンの異常な相対的伸張のチェック	1
9.6.1e)	コンペンロープの張力のチェック	3
9.6.2	はねかえり防止装置のチェック	3
9.8.8	非常止め装置の動作のチェック	1

9.9.11.1	かごの上昇過速防止装置を作動せずに過速を検出	1
9.9.11.1	かごの上昇過速防止装置を作動させて過速を検出	2
9.9.11.2	調速機の開放のチェック	3
9.9.11.3	調速機ロープの張力チェック	3
9.10.5	かごの上昇過速防止装置のチェック	1
10.4.3.4	緩衝器の正常な伸張位置への復帰のチェック	3
10.5.2.3b)	かごの位置の伝達用装置（ファイナル・リミット・スイッチ）中の張力のチェック	1
10.5.3.1b)2)	トラクション駆動式エレベーター用のファイナル・リミット・スイッチ	1
11.2.1c)	かごの戸の施錠のチェック	2
12.5.1.1	取り外し可能なホイールの位置のチェック	1
12.8.4c)	かごの位置の伝達用装置（スローダウンチェック装置）中の張力のチェック	2
12.8.5	ストロークが低下した緩衝器の場合の遅延のチェック	2
12.9	ボジティブ・ドライブ・エレベーターのロープのたるみとチェーンのたるみをチェック	2
13.4.2	遮断器の接触器による主スイッチの制御	2
14.2.1.2a)2)	床合わせ動作と再床合わせ動作のチェック	2
14.2.1.2a)3)	かごの位置の伝達用装置（床合わせ動作と再床合わせ動作）中の張力のチェック	2
14.2.1.3c)	点検運転を有する停止装置	3
14.2.1.5b)	ドッキング運転を有するかごの移動限界	2
14.2.1.5i)	ドッキング運転を有する停止装置	2
14.2.2.1f)	エレベーター機械にある停止装置	2
14.2.2.1g)	非常パネルとテストパネルにある停止装置	2

表 A.2　PESSRAL と関連して使用する場合の安全機能の分類を必要とする電気安全装置

EN81の条項	チェックの対象となる装置	SIL
14.2.1.3	点検運転スイッチ	3
14.2.1.4	非常用電気運転スイッチ	3

表 A.1, 表 A.2 別添

安全度水準	低頻度作動要求モード運用※1 （単位時間当たりの危険側故障確率　Ｉ/時間）
４	１０の－５乗以上　１０の－４乗未満
３	１０の－４乗以上　１０の－３乗未満
２	１０の－３乗以上　１０の－２乗未満
１	１０の－２乗以上　１０の－１乗未満

備考：エレベーターでは、水準４を適用するものはなし

安全度水準	高頻度作動要求又は連続モード運用※2 （単位時間当たりの危険側故障確率　Ｉ/時間）
４	１０の－９乗以上　１０の－８乗未満
３	１０の－８乗以上　１０の－７乗未満

２	１０の－７乗以上　１０の－６乗未満
１	１０の－６乗以上　１０の－５乗未満

備考：エレベーターでは、水準４を適用するものはなし

※１低頻度作動要求モード　:安全関連系への作動要求の頻度が１（回/年）より大きくなく、かつ、プルーフテストの頻度の２倍よりも大きくない場合

※２高頻度作動要求モード　:安全関連系への作動要求の頻度が１(回/年)より大きい、又はプルーフテストの頻度の２倍よりも大きい場合

表 B1　故障の回避と検知のための共通の手段－ハードウェアの設計

番号	目　的	措　置	EN 61508-7:2001 の参照項目
１	処理ユニット	ウオッチドッグの使用	A.9
２	構成要素の選択	構成要素をその仕様の範囲内でのみ使用	
３	I/Oユニットとインタフェース、コミュニケーションリンクを含む	停電またはリセットの場合の定義された安全状態	
４	電源	電圧超過または電圧過小の場合の定義された安全なシャットオフステート	A.8.2
５	可変記憶レンジ	ソリッドステートメモリーのみの使用	
６	可変記憶レンジ	起動手続き中の可変データメモリの読み取り／書き込みテスト	
７	可変記憶レンジ	情報データ(たとえば統計)のみに対するリモートアクセス	
８	固定記憶レンジ	システムによる自動的な、あるいは遠隔介入による、プログラムコードの変更の可能性なし	
９	固定記憶レンジ	少なくともサムチェックテストに均等な方法による、起動手続き中のプログラムコードメモリと固定データメモリのテスト	A.4.2

表 B2　故障の回避と検知のための共通の手段－ソフトウェアの設計

番号	目　的	措　置	EN 61508-7:2001 の参照項目
１	構成	最新の技術水準によるプログラム構成(すなわち、モジュラリティ、データの取り扱い、インタフースの定義)(EN 61508-3を参照)	B.3.4/C.2.1 C.2.9/C2.7
２	起動手順	起動手順中にエレベーターを安全状態に維持すること	
３	割り込み	割り込みの限定的使用:すべての可能な割り込みのシーケンスが予測できる場合にのみ、入れ子になった割り込みを使用	C.2.6.5
４	割り込み	他のプログラム・シーケンス条件と組み合わせる場合を除き、割り込み手続きによるウオッチドッグの始動なし	A.9.4
５	停電	電源が落ちた場合にデータをセーブ(保存)する等の、安全関連機能についての手続きなし	
６	メモリ管理	適切な反応手続きを伴うハードウェアと／またはソフト	C.6.2.4/C.5.4

		ウェアのスタックマネジャー	
7	プログラム	たとえばループ数の制限、あるいは実行時間のチェックによる、システム反応時間よりも短い反復ループ	
8	プログラム	使用したプログラミング言語に含まれていない場合には、アレー・ポインターのオフセット・チェック	C.2.6.6
9	プログラム	（ゼロによる除算、オーバーフロー、可変範囲のチェック等の）例外の定義された取扱方法により、システムを定義された安全状態へと強制する	
10	プログラム	推奨されているオペレーティングシステム内で、あるいは高レベル言語コンパイラ内で、十分に試された標準ライブラリを例外として、反復的プログラミングなし。これらの例外については、別個のタースクのための別個のスタックを、メモリ管理ユニットにより提供して制御	C.2.6.7
11	プログラム	少なくともユーザープログラムそれ自体と同程度に完全な、プログラミングライブラリーのインタフェースとオペレーティングシステムの文書化	
12	プログラム	安全機能に関連するデータ、たとえば入力パターン、入力範囲、内部データ等について蓋然性をチェック	C.2.5/C.3.1
13	プログラム	テストあるいは検証のためにいずれかの運転モードを選べる場合には、そのモードを終了するまではエレベータの平常運転ができないこと	EN 61508-1: 2001:7.7.2.1
14	（外部および内部の）コミュニケーションシステム	コミュニケーションの喪失、あるいはバス・パーティシパント中の誤りの場合に、安全機能を有するバス・コミュニケーション・システム中のシステム反応時間を十分考慮にいれて安全状態に到達	A.7/A.9
15	バスシステム	起動手続き中を除き、CPU-バスシステムのリコンフィギュレーションなし。　注 CPU-バスシステムの定期的なリフレッシュはリコンフィギュレーションとはみなさない	C.3.13
16	I/Oハンドリング	起動手続き中を除き、I/Oラインのリコンフィギュレーションなし。 （注） I/Oコンフィギュレーション・レジスタの定期的なリフレッシュはリコンフィギュレーションとはみなさない	C.3.13

表 B3　プロセスの設計と実施のための共通の手段

番号	措　置	EN 61508-7:2001 の参照条項
1	アプリケーションの機能的、環境的ならびにインタフェースの側面の評価	A.14/B.1
2	安全性要件を含む仕様の要件	B.2.1
3	すべてのアプリケーションの検証	B.2.6
4	F.6.1においてまた追加で必要とする設計文書: －システムアーキテクチャとハードウェア／ソフトウェアの相互作用を含む機能説明 －機能とプログラムのフローの説明を含むソフトウェアの文書	C.5.9
5	設計検証リポート	B.3.7/B.3.8 C.5.16
6	故障モードと影響分析（FMEA)等の方法を用いた信頼性のチェック	B.6.6

7	製造者のテスト仕様、製造者のテストリポートおよびフィールドテストリポート	B.6.1
8	使用目的の制限を含む取扱説明書	B.4.1
9	製品が改造された場合には、上記の手段を繰り返して更新する	C.5.23
10	ハードウェアとソフトウェアならびにその互換性のバージョン管理の実施	C.5.24

表 C1　SIL 1 による特定の手段

構成要素 及び 機 能	要　件	手　段	表D中の 番号	EN 61508-7: 2001 の参照項目
構成	単一のランダムな障害を検知して、システムを安全状態にするように構成すること	自己テストを持つ1チャンネルの構成、又は比較を持つ複数チャンネル	M1.1 M1.3	A.3.1 A.2.5
処理ユニット	不正確な結果に導くおそれのある、処理ユニット中の障害を検知すること。このような障害が危険な状況に導くおそれがあれば、システムは安全状態にならなければならない	障害を訂正するハードウェア、又はソフトウェアによる自己テスト、又は2チャンネル構成ついてのコンパレータ、又は2チャンネル構成についての、ソフトウェアによる相互比較	M 2.1 M 2.2 M 2.4 M 2.5	A.3.4 A.3.1 A.1.3 A.3.5
非可変記憶レンジ	不正確な情報の修正、すなわち、すべての半端なビットまたは2ビットの障害、および一部の3ビットおよび複数ビットの障害を、遅くともエレベーターの次の走行の前に検知すること	以下の措置は1チャンネル構成にのみ該当する。 1ビット冗長度（パリテイビット）、又は1ワード冗長度を持つブロックの安全性	M 3.5 M 3.1	A.5.5 A.4.3
可変記憶レンジ	アドレス指定、書き込み、記録および読み取りの間の包括的な障害ならびにすべての半端なビット及び2ビットの障害、および一部の3ビットの障害および複数ビットの障害を、遅くともエレベーターの次の走行の前に検知すること	以下の措置は1チャンネル構成にのみ該当する。 複数ビット冗長度を持つワード保存、若しくは静的又は動的障害にたいするテストパターンによるチェック	M 3.2 M 4.1	A.5.6 A.5.2
コミュニケーション・リンクを含むI/Oユニット及びインタフェース	I/Oライン上の静的障害とクロストーク、並びにデータフロー中のランダムな、また系統的な障害を、遅くともエレベーターの次の走行の前に検知すること	コードの安全性、又はテストパターン	M 5.4 M 5.5	A.6.2 A.6.1
クロック	処理ユニットのためのクロックの生成における周波数変調または停止等の障害を、遅くともエレベーターの次の走行の前に検知すること	別のタイムベースを持つウオッチドッグ、又は相互モニタリング	M 6.1 M 6.2	A.9.4

プログラムシーケンス	安全に関連する機能の誤ったプログラムシーケンスと不適切な実行時間を、遅くともエレベーターの次の走行の前に検知すること	プログラムシーケンスのタイミングのモニタリングと論理モニタリングの組み合わせ	M 7.1	A.9.4
注　故障を検知した場合には、エレベーターの安全状態を維持しなければならない				

表 C2　SIL2 による特定の手段

構成要素 及び 機 能	要件	手段	表D中の 番号	EN 61508-7: 2001 の参照項目
構成	単一のランダムな障害を、システムの反応時間を十分考慮して検知して、システムを安全状態にするように構成すること	自己テストとモニタリングを持つ1チャンネルの構成、又は比較を持つ複数チャンネル	M 1.2 M 1.3	A.3.3 A.2.5
処理ユニット	不正確な結果に導くおそれのある処理ユニット中の障害を、システム反応時間を十分考慮に入れて検知すること。このような障害が危険な状況に導くおそれがあれば、システムを安全状態にしなければならない	障害を訂正するハードウェア、及び1チャンネル構成についてはハードウェアによりサポートされる ソフトウェア自己テスト、又は2チャンネル構成についてコンパレータ、又は2チャンネル構成についてソフトウェアによる相互比較	M 2.1 M 2.3 M 2.4 M 2.5	A.3.4 A.3.3 A.1.3 A.3.5
非可変記憶レンジ	不正確な情報の修正、すなわち、すべての半端なビットまたは2ビットの障害、及び一部の3ビットおよび複数ビットの障害を、システムの反応時間を十分考慮して検知すること	以下の措置は1チャンネル構成にのみ該当する。　1ワード冗長度を持つブロックの安全性、又は複数ビット冗長度を持つワードの保存	M 3.1 M 3.2	A.4.3 A.5.6
可変記憶レンジ	アドレス指定、書き込み、記録および読み取りの間の包括的な障害並びにすべての半端なビット及び2ビットの障害、及び一部の3ビットの障害及び複数ビットの障害を、システムの反応時間を十分考慮して検知すること	以下の措置は1チャンネル構成にのみ該当する。　複数ビット冗長度を持つワードの保存、又は静的又は動的欠陥にたいするテストパターンによるチェック	M 3.2 M 4.1	A.5.6 A.5.2
コミュニケーション・リンクを含むI/Oユニットおよびインタフェース	I/Oライン上の静的障害とクロストーク、並びにデータフロー中のランダムな、また系統的な障害をシステムの反応時間を十分考慮して検知すること	コードの安全性、又はテストパターン	M 5.4 M 5.5	A.6.2 A.6.1
クロック	処理ユニットのためのクロックの生成における周波数変調又は停止等の障害を、システムの反応時間を十分考慮して検知すること	別のタイムベースを持つウオッチドッグ、又は相互モニタリング	M 6.1 M 6.2	A.9.4
プログラムシーケンス	安全機能の誤ったプログラムシーケンスと不適切な実行時	プログラムシーケンスのタイミングのモニタリングと論理モニ	M 7.1	A.9.4

	間を、システムの反応時間を十分考慮して検知すること	タリングの組み合わせ		
注　故障を検知した場合には、エレベーターの安全状態を維持すること				

表 C3　SIL3 による特定の手段

構成要素及び機 能	要　件	手　段	表D中の番号	EN 61508-7: 2001 の参照項目
構成	単一のランダムな障害を、システムの反応時間を十分に考慮して検知して、システムを安全状態にするように構成すること	比較を持つ複数チャンネル	M 1.3	A.2.5
処理ユニット	不正確な結果に導くおそれのある処理ユニット中の障害を、システム反応時間を十分考慮に入れて検知すること。このような障害が危険な状況に導くおそれがあれば、システムを安全状態にしなければならない	2チャンネル構成についてコンパレータ、又は 2チャンネル構成についてソフトウェアによる相互比較	M 2.4 M 2.5	A.1.3 A.3.5
非可変記憶レンジ	不正確な情報の修正、すなわち、すべての1ビット又は複数ビットの障害を、システムの反応時間を十分考慮して検知すること	ブロック複写を持つブロック安全手続き、又は複数ワード冗長度を持つブロックの安全性	M 3.3 M 3.4	A.4.5　A.4.4
可変記憶レンジ	アドレス指定、書き込み、記録及び読み取りの間の包括的な障害並びに静的ビットの障害及び動的カップリングを、システムの反応時間を十分考慮して検知すること	ブロック複写を持つブロック安全手続き、又は「ガルパット」等の点検チェック	M 4.2 M 4.3	A.5.7 A.53
コミュニケーション・リンクを含むI/Oユニットおよびインタフェース	I/Oライン上の静的障害とクロストーク、並びにデータフロー中のランダムな、また系統的な障害を、システムの反応時間を十分考慮して検知すること	複数チャンネルパラレル入力、及び複数チャンネルパラレル出力、又は出力読み戻し、又はコードの安全性、又はテストパターン	M 5.1 M 5.3 M 5.2 M 5.4 M 5.5	A.6.5 A.6.3 A.6.4 A.6.2 A.6.1
クロック	処理ユニットのためのクロックの生成における周波数変調または停止等の障害を、システムの反応時間を十分考慮して検知すること	別のタイムベースを持つウオッチドッグ、又は相互モニタリング	M 6.1 M 6.2	A.9.4
プログラムシーケンス	安全関数の誤ったプログラムシーケンスと不適切な実行時	プログラムシーケンスのタイミングのモニタリングと論理モニ	M 7.1	A.9.4

	間を、システムの反応時間を十分考慮して検知すること	タリングの組み合わせ		
注　故障を検知した場合には、エレベーターの安全状態を維持すること				

表 D　故障制御のための可能な手段

構成要素及び機能	措置番号	手　段
構 成	M.1.1	**自己テストを持つ1チャンネルの構成** 説明:　この構成は単1チャンネルから構成されているが、安全なシャットダウンを確保するために冗長出力パスを備えること。自己テスト（周期的）を、アプリケーションに依存する時間間隔で、PESSRALのサブユニットに適用すること。 これらのテスト（たとえばCPUテストあるいはメモリテスト）は、データフローから独立している潜在的な障害の検知を意図している。障害を検知した場合には、システムを安全状態にしなければならない。
	M.1.2	**自己テストとモニタリングを持つ1チャンネルの構成** 説明:　自己テストとモニタリングを持つ1チャンネルの構成は、別個のハード・ウェアモニタリング・ユニットから構成され、そのユニットは、アプリケーションから独立して、自己テスト手続きから生じる可能性があるテストデータを、システムから定期的に受領する。データが誤っている場合には、システムを安全状態にしなければならない。 処理ユニットそれ自体により、あるいはモニタリング・ユニットにより、シャットダウンを行うことができるように、少なくとも2つの独立したシャットダウン路が、必要である。
	M.1.3	**比較を持つ複数チャンネル** 説明:　安全に関連する2チャンネルの構成は、2つの独立した、またフィードバックのない機能的ユニットから構成される。これにより、指定された諸機能を各チャンネルにおいて、独立して処理することが可能となる。1つの安全装置の機能について専用であることを意図する、2チャンネルPESSRALについては、チャンネルの構成は、ハードウェアとソフトウェアの点では同一であってもよい。（例えば、いくつかの安全機能を組み合わせる）複雑な回路で使用する2チャンネルPESSRALの場合には、また方法または条件が明確に確認できない場合には、様々なハードウェアとソフトウェアを考慮するべきである。 この構成は障害の検知を助けるために、内部信号を比較する（たとえばバス比較）かつ／または安全機能に関連する出力信号を比較する機能を含んでいる。チャンネルそれ自体により、あるいはコンパレータにより、シャットダウンを行うことができるように、少なくとも2つの独立したシャットダウン路が、必要である。比較それ自体もまた、障害の認識の対象としなければならない。
処理ユニット	M.2.1	**障害を訂正するハードウェア** 説明: このようなユニットは、特殊な障害認識回路技術、あるいは障害訂正回路技術を用いて実現可能である。これらの技術は単純な構成については知られている。
	M.2.2	**ソフトウェアによる自己テスト** 説明: 安全に関連するアプリケーションにおいて使用される、処理ユニットのすべての機能を周期的にテストしなければならない。
	M.2.3	**ハードウェアによりサポートされる ソフトウェア自己テスト** 説明:　自己テスト機能をサポートする特殊なハードウェア装置を、障害の検知の

		ために使用する。たとえば、特定のビットパターンの定期的な出力をチェックするモニタリング・ユニットである。

処理ユニット（続き）	M.2.3	**ハードウェアによりサポートされる ソフトウェア自己テスト** 説明: 自己テスト機能をサポートする特殊なハードウェア装置を、障害の検知のために使用する。たとえば、特定のビットパターンの定期的な出力をチェックするモニタリング・ユニットである。
	M.2.4	**2チャンネル構成についてのコンパレータ** 説明: 1 ー コンパレータ ー 2 ハードウェアによるコンパレータを有する2チャンネル: a) 両者の処理ユニットの信号を、ハードウェアユニットを用いて周期的にあるいは継続的に比較する。コンパレータは外からテストされるユニット、または自己モニタリング装置として設計されても良い。又は、 b) 両者の処理ユニットの信号を、処理ユニットを用いて比較する。コンパレータは外からテストされるユニット、または自己モニタリング装置として設計されても良い。
	M.2.5	**2チャンネル構成の相互比較** 説明: **1 コンパレータ ー コンパレータ 2** 安全に関連するデータを相互に交換する2つの冗長な処理ユニットを使用する。データの比較はそれぞれのユニットにより行われる。
非可変記憶レンジ（ROM, EPROM...）	M.3.1	**1ワード冗長度を持つブロック安全手続き（たとえばシングル・ワード幅を持つ、ROMを経由するシグネチャ形成）** 説明: このテストでは、ROMのコンテンツを特定のアルゴリズムによって、少なくとも1つのメモリワードに圧縮する。そのアルゴリズム、例えば周期的冗長度チェック(CRC)は、ハードウェアを用いてまたはソフトウェアを用いて実現することができる。
	M.3.2	**複数ビット冗長度を持つワードの保存（例えば、修正されたハミング・コード）** 説明: メモリーのすべてのワードが、いくつかの冗長ビットにより拡張されて、少なくとも4のハミング距離を持つ修正されたハミング・コードを生成する。あるワードを読み取るごとに、その冗長ビットをチェックして、コラプションが生じたか判断できる。相違が見つかった場合には、システムを安全状態にしなければならない。
	M.3.3	**ブロック複写を持つブロック安全手続き** 説明: アドレス・スペースは2つのメモリーを備えている。第1のメモリーは通常の方法で動作する。第2のメモリーは同じ情報を含んでいて、第1のものにパラレルにアクセスされる。その出力を比較して、相違を検出した場合には、障害があるものと想定する。特定の種類のビットエラーを検出するために、そのデータを反転して2つのメモリーの1つに格納して、読み取る際にもう1度反転する。ソフトウェア手続き中で、両方のメモリ領域のコンテンツを、プログラムを用いて周期的に比較する。
	M.3.4	**複数ワード冗長度を持つブロック安全手続き** 説明: この手続きでは、CRCアルゴリズムを用いてシグネチャを計算するが、その結果生ずる値のサイズは少なくとも2ワードである。拡張されたシグネチャを格納して、再計算し、1ワードの場合と同様に比較する。相違が生じた場合には、障害メッセージが生成される。

	M.3.5	**1ビット冗長度を持つワード保存** 説明: メモリーのすべてのワードを、1ビット(「パリティ」ビット)で拡張するが、それにより各ワードが論理1の偶数個または奇数個に完成される。データワードを読み取るたびごとに、そのパリティをチェックする。1の個数が誤っていることが見いだされた場合には、障害メッセージが生成される。障害の場合に(0しかない)ゼロワードと(1しかない)ワンワードのどちらかが、より不利な場合に、そのワードが有効なコードではないように、偶数パリティと奇数パリティを選択しなければならない。また、データワードとそのアドレスの連結のためにパリティを計算する際に、アドレス動作の障害を検出するためにパリティを使用するこもできる。
可変記憶レンジ	M.4.1	**静的または動的欠陥にたいするテストパターンによるチェック、たとえば、RAMテスト「ウォークパス(walkpath)」** 説明: テストするメモリー範囲を、均1なビットストリームで初期化する。それから、第1のセルを反転して、残りのメモリ領域を点検して、バックグラウンドが正しいことを確認する。その後、第1のセルを再び反転してその元の値に戻し、次回のためにプロセス全体を反復する。「ワンダリング・ビット・モデル(wandering bit model)」の2回目の実行を、反転したバックグラウンドのプリアセスメントで遂行する。相違が生じた場合には、システムを安全状態にする。
	M.4.2	**ブロック複写を持つブロック安全手続き、例えばハードウェアまたはソフトウェアの比較を伴うダブルRAM** 説明: アドレス・スペースは2つのメモリーを備えている。第1のメモリーは通常の方法で動作する。第2のメモリーは同じ情報を含んでいて、第1のものにパラレルにアクセスされる。その出力を比較して、相違を検出した場合には、障害があるものと想定する。特定の種類のビットエラーを検出するために、そのデータを反転して2つのメモリーの1つに格納して、読み取る際にもう1度反転する。ソフトウェア手続き中で、両方のメモリ領域のコンテンツを、プログラムを用いて周期的に比較する。
	M.4.3	**静的または動的欠陥についてチェックするための点検方法、例えば「GALPAT」** 説明: a) RAMテスト「galpat」: 反転要素(inverse element)を標準的なあらかじめ割り当てられたメモリに書き込んで、それから全ての残りのセルを点検して、それらのコンテンツが正しいことを確認する。残りのセルの1つにたいする読み取りアクセスがすべて終わったあとで、反転して記載したセルも点検して、これに加えて読み取る。このプロセスをすべてのセルについて繰り返す。反転プリアサインメント(事前割当)で、2回目の実行を遂行する。相違があった場合には障害を想定する。あるいは、 b) 透明な「galpat」テスト: テストの開始にあったって、テストされるメモリー範囲のコンテンツに関して、ソフトウェアあるいはまたハードウェアを用いて、「シグネチャ」を形成し、これをレジスターに格納する。これはgalpatテスト中のメモリーのプリアサインメントに対応する。それでコンテンツを反転した形でテストセル中に書き込んで、残りのセルのコンテンツを点検する。テストセルのコンテンツもまた、これらのセルの1つにたいする読み取りアクセスがすべて終わったあとで読み取る。残りのセルのコンテンツは実際知られていないので、それらのコンテンツは個々に点検されないが、再びシグネチャを形成することにより点検される。この第1のセルに対する最初の実行のあとで、このセルに対する第2回目の実行が、何度か反転されたコンテンツ、－それ故、再び真(real)となったコンテンツで行われる。このようにして、メモリーの元のコンテンツを、再び確立する。他のすべてのメモリセルも、同様な方法でテストする。相違がある場合には障害があると想定する。

I/Oユニットおよびインタフェース	M.5.1	**マルチチャンネル・パラレル入力** 説明: これは規定された許容領域（時間値）を順守する、独立入力の、データフローに依存する比較である。
	M.5.2	**出力のリードバック(read back)（モニターされた入力）** 説明: これは規定された許容領域（時間、値）を順守する独立入力と出力とのデータフローに依存する比較である。障害は必ずしも欠陥ある出力に関連しているわけではない。
	M.5.3	**マルチチャンネル・パラレル出力** 説明: これはデータフローに依存する出力の冗長度である。障害の認識は技術プロセス経由で直接に、あるいは外部コンパレータ経由で行われる。
	M.5.4	**コードの安全性** 説明: この手続きは偶発的障害（coincident failure）と系統的障害（systematic failure）に関して入力情報と出力情報を保護する。それは情報リダンダンシイ、か つ／又は時間リダンダンシイを有する入力ユニットと出力ユニットの、データフローに依存する障害の認識を提供する。
	M.5.5	**テストパターン（モデル）** 説明: これはデータフローに依存しない、入力ユニットと出力ユニットの周期的テストで、指定されたテスト用パターンの助けを借りて遂行し、実測値を対応する予想値と比較する。テスト用パターンの情報、テスト用パターンの受け取り、およびテスト用パターンの評価は、たがいに独立していなければならない。すべての可能な入力パターンがテストされると想定しなければならない。
クロック	M.6.1	**別のタイムベースを持つウオッチドッグ** 説明: プログラムの正しい動作によりトリガーされる、別のタイムベースを持つハードウェアのタイマー。
	M.6.2	**相互モニタリング** 説明: 他のプロセッサのプログラムの正しい動作によりトリガーされる、別のタイムベースを持つハードウェアのタイマー。
プログラムシーケンス	M.7.1	**プログラムシーケンスのタイミングと論理モニタリングの組み合わせ** 説明: プログラムシーケンスをモニタする、時間に基づく機能(facility)は、プログラム・セクション（プログラムの部分）のシーケンスが正しく実行された場合にのみ、再トリガされる。