STM32L4の安全機能の対応に関するプレゼンテーションへようこそ。

本プレゼンテーションでは、安全規格のコンプライアンスとSTマイクロエレクトロニクス がお客様がターゲットとしているプロジェクトの安全規格をどのようにサポートするかについて説明します。

概要

- 幅広い電子アプリケーションは、以下の様な深刻な障害を防ぐための基本安全要求に対応する必要があります。
  - 人体や動物の死や怪我
  - 環境被害
  - プロセスの破壊や価値の低下
  - 2次的要因
    - 電子デバイスの信頼性や不具合
    - 顧客の不満
- 安全規格
  - 開発 - 国内外の機関による立法と執行
  - 機器 - 世界的に認められたテストラボ

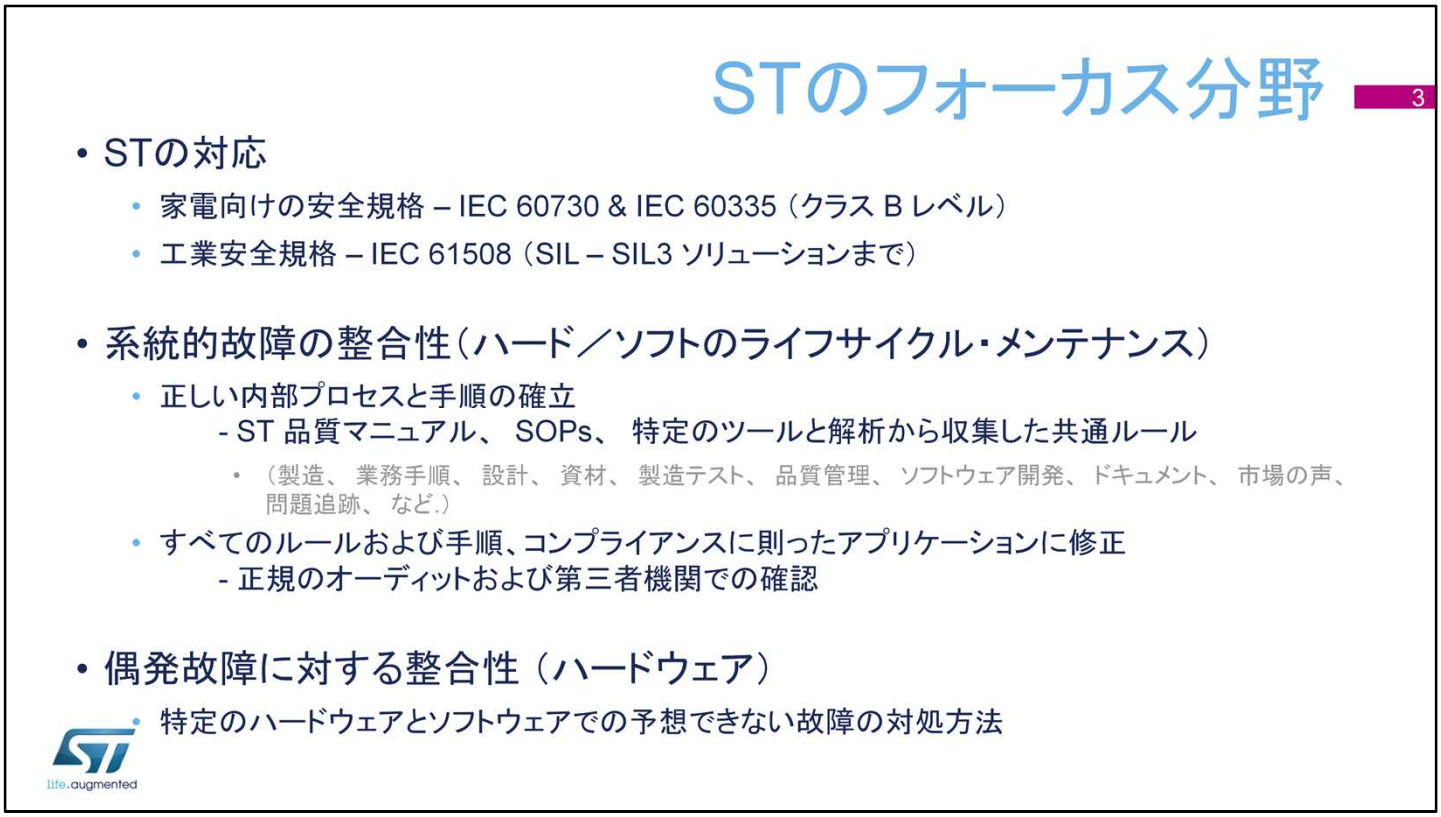
アプリケーションの利点

- ユーザのソフトウェア開発と認証プロセスの加速
- 安全規格のコンプライアンスの確実性

life.augmented

電子デバイスの安全要求は、我々の幅広い活動範囲への電子制御システムの使用の拡大に合わせて永久に増加していきます。 これらのデバイスの大規模な拡大は特定の安全規格への対応が要求されます。 主な目的は人の死や怪我、ならびに、環境被害を防ぐことにありますが、これらは重要なデータや接続、電源または制御、その他の損失を含む産業プロセスの価値の低下など、より下位レベルの重要な要素が他にも沢山存在します。 国内外レベルで協調された規格の開発プロセスはやや複雑です;時に完全に逆の取り組みが発生します(例: 国内市場保護対国際化)。
いかなる場合でも、影響を与える主な要素は、現場の経験、市場要求、保険の問題、および、貿易またはビジネスの国際化です。 規格は特定の立法および執行機関から生まれる一方で、世界中で認められた認証機関がすべての要求機器に対してコンプライアンスの為の検証と調査を実施します。
安全をターゲットにしているアプリケーションではソフトウェア開発の加速という利点を享受できます。 特定のハードウェ

ア機能と適切なハードウェアおよびソフトウェア手法を用いた効率的および早期診断により、コンポーネントの不具合による危険なイベント発生の可能性を下げることができます。 適切なハードウェア設計と製造方法により、更にコンポーネントの信頼性を上げることができます。

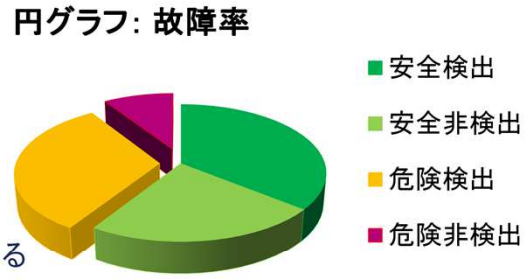


STマイクロエレクトロニクスは2つの基本的な一般安全規格に対応します- 1つは”クラスB”や”クラスC”として知られる家電向け安全規格、そしてさらに一般的な工業規格”SIL”と呼ばれる安全度水準規格をターゲットにしています。 SILは異なるアプリケーション分野のために多くの派生規格を作る一般的な規格です。
STはこれらの規格に従って、系統的故障と偶発故障の両方に対応します。 系統的故障は予想可能で、回避方法や監視方法は産業の実践的な経験によって入手されるものが基準になっています。 系統的故障は主に製品のライフサイクルを通して正しい内部プロセスの適用によって回避することができます。 これらの要求は、特定の内部品質ドキュメントに定義されています。 正規の検査と監査により、これらの内部ルールが適応されて、認められた安全規格に従うことを確実なものにします。 偶発故障に対して確実に整合性をとるためには、次のスライド以降にある特定のソフトウェア手法とハードウェア設計技術を適用する必要があります。

偶発故障について（1）

4

- 偶発故障の識別
  - 安全（安全側故障割合：SFF）& 危険（診断率：DC）
  - 検出可& 検出不可
- 偶発故障のタイプ
  - ハードウェア – コンポーネントが永久にダメージを受ける
  - ソフトウェア – リカバリ可能
    - ラッチアップ – SWまたはHWのテスト、または診断で識別可能
    - 一時的な故障- 高速HWテスト、または、診断のどちらか一方で識別可能
  - 製品間の故障の基準
    - 単一故障点 (SPF) – 即時
    - 潜在故障 (LF) – 潜伏、 他の故障と統合される可能性あり
    - 共通原因故障(CCF) –即時、 いくつかのコンポーネントが影響を受ける
      -複雑な安全構造の破壊の可能性有り（電源、クロック、温度、タイミング）



life.augmented

すべての偶発故障が危険事象であるとは限らず、中には安全性の視点から安全であるとされる故障もあるかもしれません。 基本的に安全規格は直接もしくは間接的に安全に関連し、危険な状況を引き起こす可能性がある危険側故障を検出するために監視を要求します。 安全および危険なエラーは共にシステムによって検出されるか、未検出（隠れている）のままになります。

一定時間内に頻繁に危険なエラーが発見され防止されればされるほど、危険なイベントに伝わる故障の可能性が低下します。 危険なエラー検出と危険なイベント防止に必要な時間は、システム（例：センサ、または、アクチュエータ）の可能性のあるすべての遅延と応答時間を含む、利用できる全体的なプロセス·セーフティ·タイム (PST)に含まれなければなりません。

定量化の目的で、安全規格は安全側故障割合と診断率を識別します。安全側故障割合(SFF)は、安全側故障のレート (検出された危険側故障のレートを含む)と、安全側故障レートと検出と非

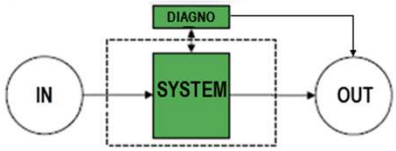
検出を含む危険側故障の全体の故障レートとの比率です。 診断率(DC)は、検出された危険側故障の確率と、全危険側故障の確率との比率です。 偶発故障は、修復不可能なエラーまたは修復可能なエラーを引き起こします。 ハードウェア故障はコンポーネントに永久的な物理的ダメージを与え、システムは正常動作できなくなります。 故障への補償がない場合には、システムは修理されるまでセーフステートへ移行する必要があります。

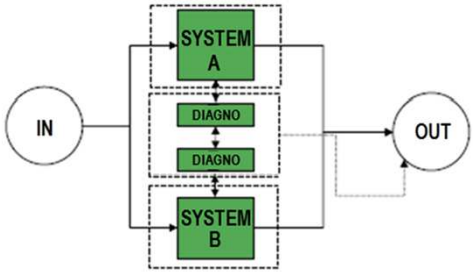
偶発的なソフトウェア·ラッチアップ、および、一時的な故障は復旧可能で、通常いくつかの復帰プロセスが適用できます。この検出に加えて、これらの故障もまた特定のケースで補償されます。 一時的な故障が高速ハードウェアでの処理のみを必要とするのに対し、ラッチアップ故障は、ソフトウェアとハードウェアの両方で管理されます。 ソフトウェア·テストは、実行時間が非常に遅く制限されているため、効率的にこれらの一時的かつ一瞬のエラーを補償することはありません。

製品間の視点から、単一故障点、潜在故障、または、共通原因故障の故障原因を認識することができます。 共通原因故障は、とても複雑な安全構造でも潜在的に破壊することができるので特別な配慮を必要とします。

偶発故障について（2）

- 偶発故障の制御技術
  - 検出
    - エラーの検出診断
    - システムの正常動作の継続不能
    - フェイル・セーフまたは復帰へのステータス移行
  - 補償（HFT > 0）（ハードウェアフォールトトレランス）
    - 診断機能による故障部分の検出と識別
    - 次の正常データは維持
    - 不具合検出跡のシステムの継続性
- 不可欠なもの – 冗長性
  - 診断、 比較、 識別、 投票





life.augmented

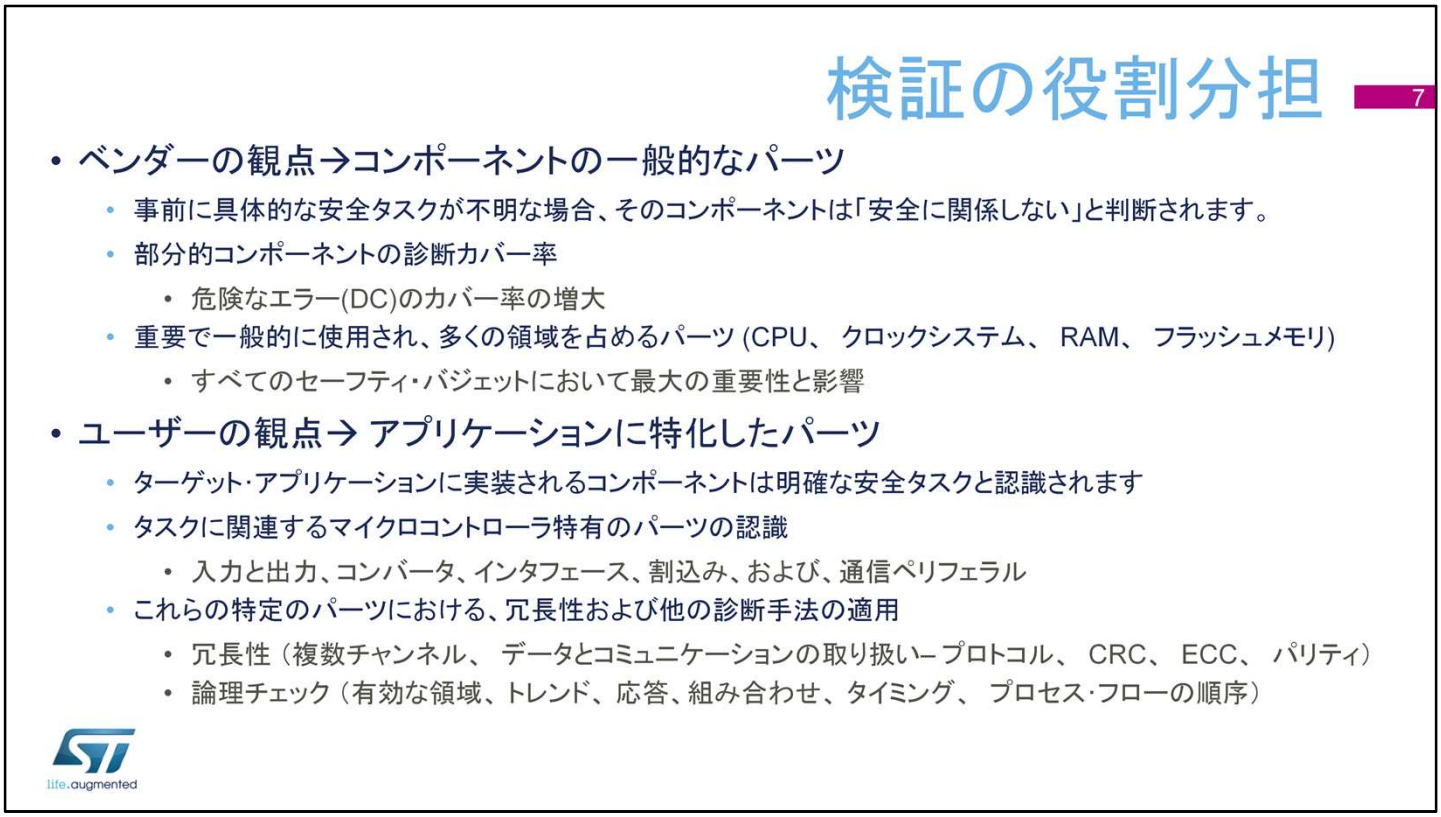
偶発故障が検出されて、それが補償できない時 (特に危険なエラーを検出後)は、 システムを停止し安全ステートに移行するか、リセット、ロールバック、または、特別なチェック機能のような復帰プロセスを実行する必要があります。
補償方法では通常、エラー訂正、安定化またはマスクの機能を使用中に、システムの通常処理を継続できます。 一般的に、確かな投票処理はダメージを受けた部分、または、不正データを識別するために使用され、正しいデータに修正されます。 規格は、正常動作を継続しつつ、ハードウェアフォールトトレランスまたはシステムが取り込めるエラーの最大数を認識します。
特別な機能テストに加え、冗長性は診断の基本原則になります。 検出と補償の両方技術は、効率のため、確実なレベルの冗長性を常に要求します。 不一致だけでなく正しいステートも同様に識別する必要があるため、補償は検出よりかなり多く要求されます。 そのため、専用の比較と投票メカニズムを、追加で適用する必要があります。

偶発故障について（3）

- 冗長性の技術
  - 構造面
    - デュアル・レジスタ、メモリ、ハードウェアのコンパレータや投票機能付きのCPUやMCUのようなパラレルの同一構造になります。
  - 機能面
    - シングル・タスク向けにパラレルの非対称のハードウェア構造または異なるソフトウェア手法が適用され、これらの出力は比較されます。
  - 時間面
    - 同じ手法が同じハードウェアまたはソフトウェアを使って異なるタイムスロットに何度も実装され、孫結果が比較されます。
  - 情報
    - 追加された情報はデータレベルで実装され、検証のためにハードウェアまたはソフトウェアによって評価されます。（パリティ、ECC、CRC、データ・プロトコルまたはコピー）

life.augmented

要求される冗長性のレベルは、使用する広範囲の異なるソフトウェアもしくはハードウェアの手法と技術を使用して達成できます。 それらのいくつかはここに列記されていますが、その他については、本プレゼンテーションの以降にて取り上げています。 本技術は、通常、ハードウェアまたはソフトウェアのいずれか、もしくは両方で対応されます。



安全の視点から、マイクロコントローラは適応する規格で決定される特殊要求を満たす必要のある、比較的複雑なプログラム可能な電子コンポーネントです。 ベンダーの視点では、マイクロコントローラの安全対応に関して、コンポーネントが最終的なアプリケーションの目的と安全タスクが事前に不明な場合、「安全に関係しない」と判断します。 そういうわけで、私たちは安全タスクの定められた共通レベルでコンポーネントが、”レディ”または”適切”などと話すことができます。 コンポーネント全体の信頼性をカバーし、最終的アプリケーションで要求されるセーフティ実装レベルに関する規格により定義された診断カバレッジ全体のバジェットを満足するために努力します。 マイクロコントローラのような複雑なコンポーネントは、さまざまな安全タスク（それぞれのタスクは診断カバレッジおよびコンポーネントのセーフティバジェット全体の重みが異なります）に関連する部分的コンポーネントの集合としてみなすことができます。 要求された全体のセーフティバジェットを確実に守るための効果的な方法は、重要で、ほとんどのア

プリケーションで一般的に使用されるマイクロコントローラのパートに特に集中することです。 設計のこれらの基本的かつ重要なパーツの安全性のどんな小さな改善でも、常にコンポーネントの全体のセーフティ・バジェットに最大の効果をもたらし、各アプリケーションに対して有益です。
一度マイクロコントローラがアプリケーションの設計に含まれて安全タスクが特定されると、セーフティ・サポートはより効率的に展開され、要求されたセーフティ・ケースに関連するマイクロコントローラの重要なパーツのみをカバーすることができます。 アプリケーション要求、設計、プロセス、および、使用機材の詳細な知識に基き、数多くの効果的な方法を適用することができます。 冗長性とシステム動作の知識は、別々に、または、合わせて適用される重要な原理です。 入力および出力は、論理ステート、値、またはトレンドやタイムインターバルの期待される応答のためにテストされるフィードバックと乗算またはチェックが実施されます。 正しいタイミングおよびフローの順序のためにプロセスを監視することができます。 冗長および独立フロー、分析、計算、または、データからくる結果の比較に基き正しい判断が行えます。

ハードウェア安全機能（1）

- 偶発故障検出のための特別なハードウェア機能
  - 標準 ARM Cortex®-M4 コア システム例外
    - 目的 – 予測できないソフトウェアまたはシステムの動作、または、不具合のキャプチャ
    - 方法 – システム割込みのハンドリング（HardFault、 MemManage、 BusFault、 UsageFault、 NMI）
  - 独立型およびウィンドウ型ウォッチドッグ
    - 目的– 正しいソフトウェアのタイミングとフローの監視
    - 方法 – ウォッチドッグ・タイムアウト時の正しいハンドリング技術を適用 – アプリケーション・ノート参照
  - フラッシュメモリのECC（SEC/DED）
    - 目的 – 不揮発性メモリの内容の正しい保護
    - 方法 – ワード読み出し時の追加ビットセットのチェックにより 32bitワード 毎に保護
      - 32bit ワード向けシングル・ビット・エラー訂正とマルチ・ビット・エラー検出
      - フラッシュメモリ保護のステータス情報を特定のECCステータス・レジスタに保持

life.augmented

STM32L4マイクロコントローラは、効率のよい診断テストと、幅広い低レベルセーフティアプリケーションをカバーするための即座に故障に反応するハードウェアを内蔵しています。
ハードウェアテストは、最小限のソフトウェア制御またはソフトウェア制御なしで自立制御可能です。 これは特に過渡エラー検出に便利で、セーフティプロセスにかかる全体の時間のほんの少しの時間のみ消費します。

ハードウェア安全機能（2）

- SRAMのパリティ・ビット
  - 目的 – 揮発性メモリの正しい内容の保護
  - 方法 – バイト読み出し時のシングルビットチェックにより、各バイトを保護
    - 8bitワードのシングルビットと複数の奇数ビットエラーの検出
    - 論理セルに集められたビットの物理的に拡散されたハードウェア設計は、局所的な放射線障害時の保護されたセルでの同時点での複数ビットエラーの発生を低減します。
- HW CRC 計算モジュール
  - 目的 – 与えられたデータの高速CRCチェックサム計算（ソフトウェアの手法で対応）
  - 方法 – データの上に追加の冗長性を構築（コミュニケーション、 メモリ）
- 外部クロックのためのクロックセキュリティシステム
  - 目的 – 外部クロックの不具合の検出
  - 方法 – 内部クロックへの自動切換え、NMI割込み生成
    - HSEとLSEのそれぞれに用意されたCSSブロック
- クロックのクロスリファレンス測定（2つの周波数差の監視）
  - 目的 – クロックシステムの不具合検出（ソフトウェアの手法で対応）
  - 方法 – リファレンス周波数入力は別の専用タイマーで取り込みます。

life.augmented

ここに列記したすべてのテスト(ECCを除く)は、完全に故障検出に特化されています。 そういうわけで、例えば、高いレベルでのSILを達成する場合のように補償または追加検証が必要な場合、ソフトウェアによるテストを追加する必要があります。 この場合、ユーザーは、ソフトウェアのテスト期間を考える際、確実にセーフティ·プロセスのための時間を考慮する必要があります。

ハードウェア安全機能（3）

- 電源の監視（POR、 PDR、 BOR）
  - 目的– 総てのシステムパーツが確実に正常動作するための安全スレッショルド
  - 方法 –緊急シャットダウンタスクをコールするための割込み、または、デバイスをリセット状態に維持
- 設定レジスタのロック機能
  - 目的 –重要な設定の不測の変化を防止（ペリフェラル、システム）
  - 方法 – ロックレジスタとビットの制御、特定の条件下でのみ設定
- 通信ペリフェラルにおけるプロトコルの取り扱い
  - 目的 –ハードウェアによる高速計算と、与えられたデータのCRCチェックサム確認
  - 方法 –通信データ上に追加の冗長性を構築
- タイマで収集された選択されたシステムエラーのブレーク入力
  - 目的 – タイマ出力の高速制御によりタイミング信号を生成
  - 方法 – すべてのタイマ出力をあらかじめ定めたステートに入れます
- アナログ・コンパレータによるウィンドウ・ウォッチドッグ（+ アナログ・リファレンス & 温度測定）
  - 目的 – アナログ値の正しい測定（ソフトウェアの手法で対応）
  - 方法 –有効な範囲、レベルおよびトレンドの高速比較

life.augmented

このスライドはアプリケーションに特化した安全機能を列記しています。
もし、専用の資料に記載されている特定の条件および制限が守られている場合、STM32L4マイクロコントローラで確実に安全水準を達成することができます。

追加のファームウェア・セーフティ・チェック

11

- ソフトウェアチェックによる偶発故障検出能力の改善
  - Flashメモリ – メモリ内容のCRCチェックサムコントロールの周期的な実行
    - ECC検出は32bitワードのダブルエラーまでの検出とシングルエラーの訂正を実施
    - 保護されたワードの読み出し時のみ不具合が検出されます
    - ECC ステータスチェック
  - SRAM2 (ハードウェア・パリティ) -周期的な内容のスクラビング
    - パリティビットは8bitバイトのシングルと複数の奇数ビットを検出します
    - 保護されたバイトの読み出し時のみ不具合が検出されます
    - シングルビットエラーの累積発生防止 (RAM領域の局所的な放射線障害など)
  - SRAM1 (パリティビットなし) – 周期的なマーチXアルゴリズムテスト
    - データ破壊
    - すべてのRAMのイニシャル・スタートアップテストに最適
    - アドレスおよびデータバスのチェック
    - ランタイム時にパフォーマンスに影響を与えない

life.augmented

このスライドはSTセルフ·テスト·ファームウェア·ソリューションに含まれるソフトウェア·チェックについて適応可能な理由の概要とともに列記されています。 一般的に、ファームウェアは、設計の詳細な知識に基くマイコンの汎用部分にフォーカスしているのに対し、SIL規格を満足する為の専用パッケージは効率化のための特別な手法により証明されている、より広範な試験方法を採用しています。 パッケージは無償でダウンロードできません。 ファームウェアに関しては、お近くのSTの窓口までお問合せ下さい。
フラッシュメモリはエラー訂正コード(ECC)を使用して内容が保護されますが、追加のCRCテストは特に早期に隠れた複数のビットエラー検出に役立ちます。 ECCステータスは並行してチェックされるべきです。 通常のテストは例外処理で使われるメモリ部分の問題を検出できます。 事前に計算されたCRCパターンの比較により、ファームウェアイメージ全体の検証が可能となります。 組み込みRAMの一部はハードウェアパリティチェックにより対応されます。 この方法により、シングル·

ビット･エラーを確実に検出します。 適用されている設計により、シングルバイトにおいて同時に挙がる複数エラーの確率は大変低いです。複数のシングルビットエラーを防止するためには、ユーザーは一定の間隔で全体のメモリ領域が読み出される時にスクラビングの方法が使えます。 これは潜在エラーを防ぐ事も可能です。
もしパリティビットが適用されないメモリに安全が重要な情報を保存する必要がある場合、マーチXアルゴリズムの機能テストを適用する必要があります。 これは、データとアドレスバスの診断を行なう追加テストですが、メモリの内容は破壊されます。 これはすべてのRAMスペースの初期機能テストに適しています。 プログラム実行時には、テストはパート毎に実施し、他に影響を与えない形で実際のメモリの内容の破壊を防止する仕組みが必要になります。

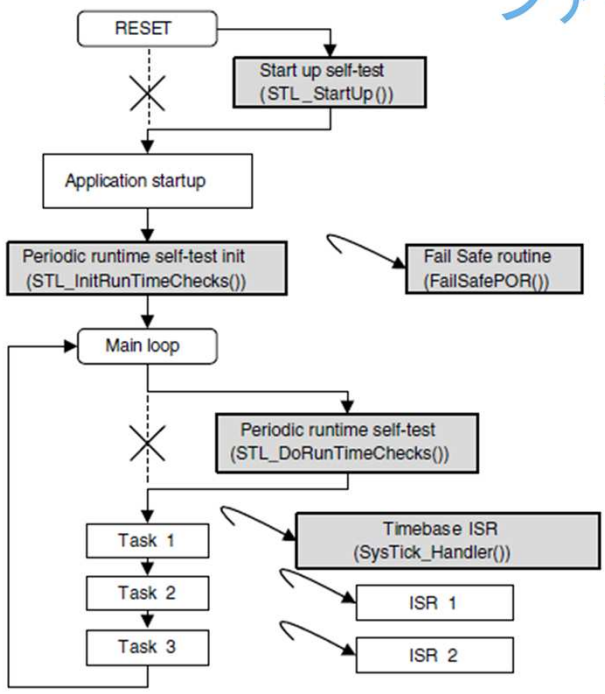
ファームウェア・アクセサリ・セーフティ・チェック

- ソフトウェアチェック（続き）
  - クロック – クロスリファレンス測定（特定のハードウェアタイマの相互接続を使用)
    - 外部発振の、高調波、副高調波、無発信は特に検出される必要があります
  - CPU – コアチェック
    - 機能性テスト（CPU レジスタ、 フラグ、 算術演算、 など）
  - ペリフェラル – 定期的に設定レジスタを確認
    - ロック設定が有効

life.augmented

クロックのクロスリファレンス測定は専用タイマの相互接続を使うことができます。 2つの独立したクロック·ソースの比率は期待された範囲内に収まる必要があります。 1つの周波数はタイマ入力として使われ、その他はタイマ入力をゲートし、タイマのキャプチャイベントを生成します。 命令の特別なシーケンスはCPUのユニットとレジスタを検証します。
ペリフェラルは、定期的に正しい設定を検証することが推奨されます。

ファームウェア実装例



5つの基本ファームウェアブロック:

- スタートアップ セルフテスト
  オプショナル、初期の1回動作の全体テスト
- 実行時 セルフテスト初期化
- 実行時 セルフテスト
  周期的、メインループ、メモリの部分テスト
- タイムベース割込み
  同期、クロック測定
- フェイルセーフの手順
  検出、復帰

原則として、セルフテストはシステムスタートアップのアプリケーションのメインループ初期化時に追加されるタスクです。この実行時のセルフテストのタスクはCPU、クロックシステム、スタック境界、プログラム･フロー、および揮発/不揮発メモリの周期的なテストを実行します。 ウォッチドッグのタイム･アウトはすべてが正常動作した場合にリフレッシュされます。メモリ領域はタスク内でパート毎にステップ･バイ･ステップでテストが実施されます。 テストはタイマ割込みに基くタイムベース･ティックによって同期されます。 テストを終了するために要求される間隔は、主に、テスト、タスクコールの頻度、およびシングルステップでテストされるブロックサイズのメモリサイズに依存します。 オプションとして、パワー･オン時またはアプリケーション･リセット後に、全体のセルフテストの一度のイニシャル･スタートアップを、追加で実装可能です。 不具合や不一致がこれらのテストで見つかった場合、いつでもフェイルセーフルーチンがコールされます。 それはアプリケーションをセーフ･ステートに遷移させ、可能性のある対策

を決める必要があります。

ST セーフティ サポート

- IEC 60730 および IEC 60335 (Class B)
  - 資料
    - 専門のアプリケーション・ノートとファームウェア実装ガイド
  - ソフトウェア
    - VDE-認証 STLソフトウェア·セルフテスト·ライブラリ（ST標準ペリフェラル·ライブラリに基く）
    - UL 認証 STLソフトウェア·セルフテスト·ライブラリ（Cube HAL ドライバに基く – 認証取得中）
- IEC 61508 (SIL)
  - 資料
    - セーフティ・マニュアル – 使用条件、 制限
    - FMEA/FMEDA分析の結果 – 診断カバー率のエビデンス
  - ソフトウェア
    - TÜV 認証 fRSTL ソフトウェア·セルフテスト·ライブラリ (サードパーティによる組込みソフトウェア)

life.augmented

STは安全が要求されるアプリケーションを開発されるお客様にサポートを提供します。 世界中で認可された安全検査の協会で認証済みの特別なセルフ·テスト·ライブラリは、ご要求に応じて複数の製品にて利用可能です。 ソフトウェアが実装されたときの特定の条件と制約事項は、資料に詳しく記載されています。 設計開始時から認証製品完成時までの複雑なコンサルティング業務とサポートサービスを提供する目的のために、STは外部の専門会社と協力しています。

参考資料

- 詳しくは、セーフティにフォーカスしたペリフェラル関連の以下の情報、または資料を参照ください。
  - AN3307 Guidelines for obtaining IEC 60335 Class B certification in STM32Fxxx applications
  - AN4435 Guidelines for obtaining UL/CSA/IEC 60335 Class B certification in any STM32 application *
  - STM32L4 Safety manual **
  - STM32-SafeSIL - 3rd-party embedded software **

*) *関連するファームウェアとドキュメントは UL 認取得中です。*
**)*関連するファームウェアとドキュメントは開発中です。*

life.augmented

詳細に関しましては、専用の資料をご参照下さい。 また、ファームウェアと資料の発行時期、ステータス、及び入手性に関しては、STマイクロエレクトロニクスの窓口までお問い合わせください。