STM32 安全サポートのプレゼンテーションへようこそ。ここでは、安全規格に準拠するための要件と自社プロジェクトで安全性をターゲットとしているお客様を STマイクロエレクトロニクスが支援する方法について説明します。

概要

- 幅広い電子アプリケーションが基本的な安全要件に準拠し、以下のような重大な危険を防ぐ必要がある。
  - 人または動物の死亡または負傷
  - 環境への被害
  - プロセスの破壊や劣化
  - 二次的要因
    - 電子デバイスの信頼性や誤作動
    - 顧客の不満
- 安全規格
  - 策定 – 国家および国際的な立法および行政機関
  - 適用 – 国際的に認知されている試験研究機関

アプリケーション側の利点

- ユーザのソフトウェア開発と認証プロセスを加速
- 安全規格への準拠を確保

life.augmented

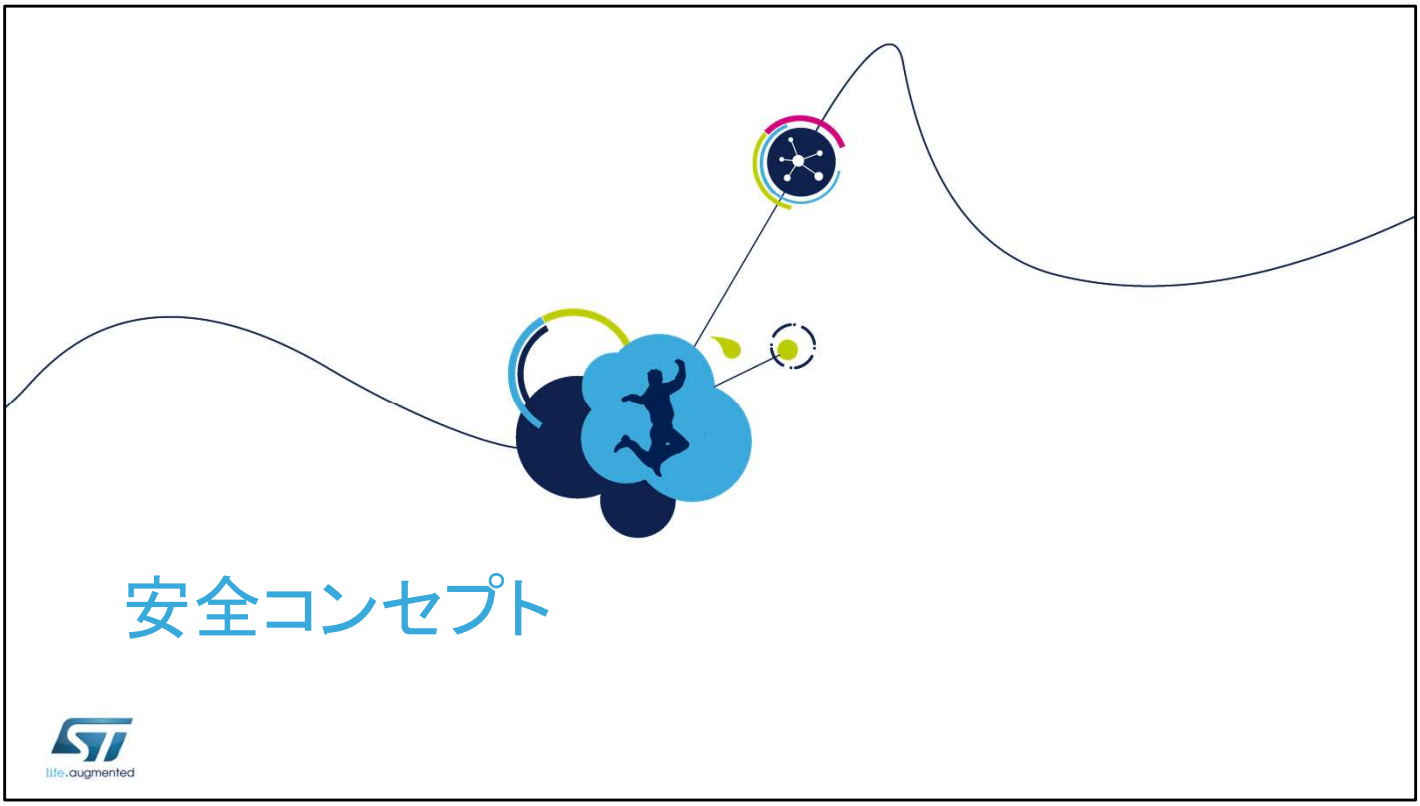
電子制御システムの使用が膨大な人間の活動範囲にまで拡大していることから、電子デバイスに対する安全要件は常に増え続けています。こうしたデバイスの使用の大幅な拡大に伴い、個々の安全規格に準拠する必要があります。
その主な目的は人の死亡や負傷ならびに環境破壊を防止することですが、それ以外にもより低いレベルとして、重要なデータや接続、電源、制御、その他多くの喪失をはじめとする産業プロセスの価値低下など、数多くの重要な要素があります。国家レベルと国際レベル両方での統一規格を策定するプロセスはかなり複雑であり、正反対の作業（例：ローカル市場の保護とグローバル化）が含まれることもあります。いずれにしても、主に影響を与える要因は現場経験、市場要件、保険問題、取引とビジネスのグローバル化に起因します。特定の立法府と行政府によって規格が作られる一方で、世界的に認知された特定の試験機関が、必要なすべての製品の検査と検証を行って、それらの適合性を保証します。
安全性をターゲットとしたアプリケーションは、ソフトウェア開発の迅速化による恩恵を受けることができます。特定のハードウェア機能を適切なハードウェア手法およびソフトウェア手法と組み合わせて使用し、効率的に早期診断を行うことにより、起こり得るコンポーネントの誤動作によって危険な事象が発生する可能性を低減します。特定のハードウェア設計と製造方法を適用することで、コンポーネントの信頼性が一層向上します。

STの視点

- STのサポート
  - 家電製品の安全性 – IEC 60730およびIEC 60335（Class B レベル）
  - 工業製品の安全性 – IEC 61508（SIL～SIL3 のソリューション）
- 決定論的原因故障に対する完全性（ハードウェア／ソフトウェア・ライフサイクルの保守）
  - 適切な内部プロセスおよび手順の設定
    - STの品質マニュアル、SOP、特定のツールおよび分析（製造、運用手順、設計、材料、生産試験、品質管理、ソフトウェア開発、ドキュメント、現場のフィードバック、問題の追跡など）に収集された共通ルール
  - すべてのルールや手順の適切な適用と規格への準拠
    - 定期的な監査と認証によって確認
- ランダム故障（ハードウェア）に対する完全性
  - 予測不可能な故障に対処する特定のハードウェア手法とソフトウェア手法
    - 標準診断ソフトウェア・ライブラリの提供
    - 安全性に関連するドキュメント（STM32G0安全性マニュアルなど）

life.augmented

ST は 2 つの基本的な一般安全規格に対応しています。1 つは、「Class B」または「Class C」規格と呼ばれる生活家電を対象としたものであり、もう 1 つは、「SIL」と呼ばれる安全度水準を対象としたより一般的な産業用規格です。
後者は汎用規格であり、さまざまな分野のアプリケーション専用の数多くの派生規格がそこから作られています。
ST は、こうした規格に準拠し、決定論的原因故障とランダム故障の両方に対応しています。決定論的原因故障は予測可能で、その回避および監視は業界で得られた実践的経験に基づいて行われます。決定論的原因故障は、主に、適切な内部プロセスを製品のライフサイクル全体に適用することで、回避できます。こうした要件は特定の内部品質ドキュメントに定義されます。定期的な検査と監査により、これらの内部ルールが適用されており、認知されている規格に準拠していることが保証されます。
ランダム故障に対する完全性を保証するには、以降のスライドで説明する特定のソフトウェア手法とハードウェア設計手法を適用する必要があります。

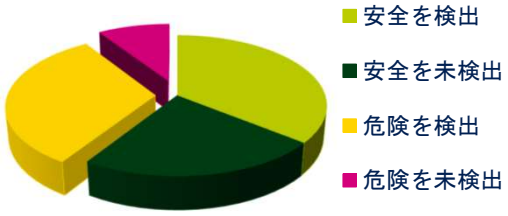


次のスライドでは、マイクロコントローラを使用する際に考慮すべき主な安全コンセプトの概要を説明します。

ランダム故障に対する技法 (1)

- ランダム故障の特定
  - 安全と危険
  - 検出と未検出
- ランダム故障のタイプ
  - 恒久的 - コンポーネントが恒久的に損傷
  - 一時的 - リカバリ可能
    - ソフトエラー - SWまたはHWのテストや診断によって特定可能
    - 一時的 - 迅速なHWテストまたは診断によってのみ特定可能
  - 製品相互間故障の基準
    - 単一点障害(SPF) – 即座に影響
    - 潜在故障(LF) – 休止中、別の故障と集計可能
    - 共通原因故障(CCF) – 即座に影響、複数のコンポーネントに影響し、複雑な安全構造(電源、クロック、温度、タイミング)が破壊される可能性あり

故障率円グラフ



life.augmented

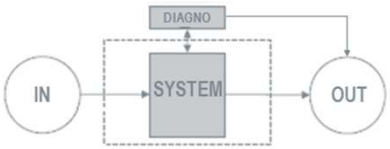
ランダム故障のすべてが危険な事象を引き起こすわけではありません。また、安全性の観点から安全と見なされることさえもあります。基本的に、安全規格では、直接的または間接的に安全性に関連し、危険な状況を招く可能性がある危険な故障を監視し、検出することを必要としています。安全なエラーと危険なエラーのどちらも、検出されることもあれば、隠れていて検出されないままとなることもあります。危険なエラーが発見され、防止が間に合う頻度が増すほど、故障が危険な事象に伝播する確率が下がります。危険なエラーを検出して危険事象を防止するのに必要な時間は、システム(センサ、アクチュエータなど)に起こり得る遅延と反応時間がすべて含まれている、利用可能な総プロセスセーフティタイム(PST)に収まっている必要があります。定量化の目的で、安全規格では、安全側故障割合と診断カバー率が評価されています。安全側故障割合(SFF)は、総故障率(安全側故障ならびに検出済みおよび未検出の危険側故障)に対する、検出された危険側故障率を含む安全側故障率の比率です。診断カバー率(DC)は、すべての危険側故障の確率に対する、検出された危険側故障の確率を比率で示したものです。ラムダム故障によって、恒久的エラーが起こることも、リカバリ可能なエラーが起こることもあります。ハード故障によって、コンポーネントには物理的損傷が恒久的に生じ、システムは正常に動作できなくなります。補正が不可能な場合は、修理するまで、システムを安全状態(アクチュエータへの電源切断など)にしておく必要があります。

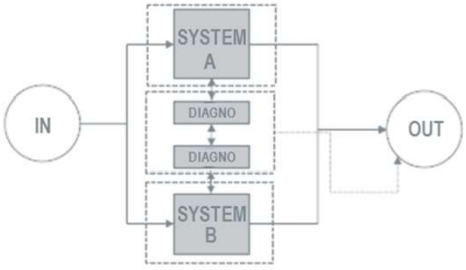
ランダムな一時的エラーやソフトエラーは修正可能であり、何らかのリカバリプロセスが適用可能です。ある特定の場合には、これらの故障は検出に加えて補正も可能となります。ソフトエラー故障は、ハードウェアとソフトウェア両方で管理可能ですが、一時的故障には高速なハードウェア手法のみが必要です。ソフトウェアテストはかなり遅い速度で行われ、実行時間が限られているため、このような一時的で短寿命のエラーを効率的に補正することは絶対にできません。

ISO 26262 の用語を使って製品相互間の観点から、単一点型、潜在型、共通型の故障原因を認識できます。かなり複雑な安全構造すら破壊する可能性が潜在的にあるため、共通原因故障には特に注目する必要があります。

ランダム故障の技法 (2)

- ランダム故障制御テクニック
  - 検出
    - 診断でエラーを認識
    - システムは正常な動作を継続不能
    - フェイルセーフ状態にするか、回復する必要あり
  - 補正（ハードフォールト許容度（HFT）> 0）
    - 診断により、問題のある部分を検出して特定可能
    - 次の正常部分が使用可能であるまま
    - システムは正常動作を継続可能
- 基本原則 - 冗長性
    - 診断、比較、特定、多数決





life.augmented

ランダム故障が検出されたものの補正できない場合、特に危険なエラーが検出された後には、システムを停止して安全な状態にするか、リセット、ロールバック、固有のチェック機能など、リカバリプロセスを実行する必要があります。
補正手法によってシステムが通常動作を継続可能になることが一般的ですが、その際にはエラー訂正、不活性化またはマスキング機能が使用されます。通常は確実な多数決プロセスが使用され、損傷を受けた部分や不正なデータが特定されて正常なものと交換されます。規格では、システムが通常動作を継続可能なまま耐えることができる最大エラー数である、ハードフォールト許容度（HFT）が評価されています。
固有の機能テストに加えて、ここでは冗長性も基本的な診断原則となります。検出手法と補正手法のどちらも、常に確実なレベルの冗長性が効率的であることが必要です。相違点だけではなく正しい状態についても特定する必要があるため、補正は検出よりも遥かに大変です。そのためには、比較と多数決の具体的なメカニズムを追加で適用する必要があります。

ランダム故障の技法 (3)

- 冗長技術
  - 構造
    - ハードウェア·コンパレータおよびボータ等の自己診断機能を組み込んだデュアル·レジスタ、メモリ、CPU、またはマイクロコントローラなどの並列同一構造
  - 機能
    - 並列非対称ハードウェア構造または各種のソフトウェア手法を単一タスクに適用して、その出力を比較
  - 時間
    - 異なる時間スロットで同一のハードウェアまたはソフトウェアを使用して、同一手法を数回実施して結果を比較
  - 情報
    - データ·レベルで追加情報を組み込んで、ハードウェアまたはソフトウェア（パリティ、ECC、CRC、データ·プロトコル、コピー）を使用してコンプライアンスを評価

life.augmented

必要なレベルの冗長性は、さまざまなソフトウェアまたはハードウェアの手法とテクニックを使用することで達成可能です。ここにはその一部がリストアップされており、それ以外については、このプレゼンテーションの中で後ほど説明します。テクニックは、一般的に、ハードウェア、ソフトウェア、もしくはその両方の組み合わせによって実現できます。

診断の責任

- ベンダ側重点項目 → コンポーネントの汎用部品
  - コンポーネントは、具体的な安全タスクが事前には知られていなかった場合、「無関係」と見なされる
  - ローカル・コンポーネントの診断カバー率
    - 検出可能な危険なエラーの比率（DC）を増加
  - 幅広くよく使用される重要な部品（CPU、クロック系、RAM、Flashメモリ）
    - 安全性バジェット全体に対する最大の重要度と影響
- ユーザ側重点項目 → アプリケーション固有の部品
  - ターゲット・アプリケーションに組み込まれたコンポーネントは、具体的安全タスクにより特定される
  - タスクに関係するマイクロコントローラ固有部品の特定
    - 入出力、コンバータ、インタフェース、割込み、通信ペリフェラル
  - これらの特定の部品にのみ冗長性とその他の診断手法を適用
    - 冗長性（複数チャネル、データおよび通信処理 - プロトコル、CRC、ECC、パリティ）
    - 論理チェック（有効範囲、傾向、応答、組合せ、タイミング、プロセス・フローの順序）

life.augmented

安全性の観点から、マイクロコントローラは、比較的複雑でプログラム可能な電子コンポーネントであり、該当する規格により定められている特定の要件に準拠している必要があります。マイクロコントローラに対する安全性への対応については、事前にその最終的なアプリケーションの目的と安全タスクがわかっていない場合、ベンダはその製品を「無関係」なコンポーネントと見なします。

私たちが、所定の共通水準の安全タスクに対して、コンポーネントが「対応可能」あるいは「適する」と表現することがある理由はここにあります。この取り組みは、常にコンポーネントの信頼性全体をカバーし、最終的なアプリケーションで必須とされる指定の安全度水準の規格で定義される診断カバー率のバジェット全体を満たすためのものです。マイクロコントローラのように複雑なコンポーネントは、全体的なコンポーネントの安全性バジェットにおいて、それぞれに異なった診断カバー率と重みを持つ、各種の安全タスクに関係する部分的コンポーネントの集合と見なすことができます。求められる全体的な安全性バジェットを保証する効果的な方法として、マイクロコントローラの重要な汎用部品（特に、多くのアプリケーションで共通に使用されるもの）に重点を置く必要があります。これらの基本的で重要な設計部分の安全性の小幅な向上であっても、常にコンポーネントの全体的な安全性バジェットに最大の利益がもたらされ、各アプリケーションにとって有益になります。

ひとたびマイクロコントローラがアプリケーション設計の中に取り入れられて安全タスクが規定されると、安全性対応の導入は大幅に効率的となり、求められるセーフティケースに関連するマイクロコントローラの非常に具体的な部品のみがその対象になります。そこで、アプリケーション要件、その設計、プロセス、制御対象装置に対する詳しい知識に基づいて、多くの効率的手法が適用できるようになります。冗長性とシステム動作に対する知識は、個別にもまとめても適用される重要な原則です。入出力は、多重化したり、フィードバックによるチェックを行って、傾向または時間間隔による論理的状態、値、期待される応答についてテストできます。これらのプロセスは、正しいタイミングやフロー順であるか監視できます。冗長で独立したフロー、分析、計算、データから得られる結果の比較に基づいて、正しい決定を行うことができます。

以下のスライドでは、安全性対応専用の機能を説明します。

ハードウェアの安全機能 (1)

- ランダム故障検出専用のハードウェア機能
  - 標準の Arm® Cortex®-M0+ コアシステムの例外
    - 目的 – ソフトウェアまたはシステムの予測不可能な動作または誤動作のキャプチャ
    - 方法 – システム割込みの処理（HardFault、MemManage、BusFault、UsageFault、NMI）
  - 標準の Arm® Cortex®-M0+ メモリ保護ユニット（MPU）
    - 目的 – ソフトウェア・バグによる予測不可能なソフトウェアの動作または誤動作のキャプチャ
    - 方法 – 特権ルールの適用、ソフトウェアプロセスの分離、メモリ・マップ・リソースに対するアクセス規則の適用を行うように MPUゾーンをプログラミング
  - 独立型ウォッチドッグとウィンドウ型ウォッチドッグ
    - 目的 – ソフトウェアのタイミングとフローが正しいか監視
    - 方法 – ウォッチドッグ・タイムアウトを処理する正しいテクニックの適用（専用のアプリケーションノート参照）

life.augmented

STM32G0 マイクロコントローラは、効率的に診断テストを実施し、幅広い低レベルの安全アプリケーションにまで及ぶ可能性がある故障に迅速に対処するための専用ハードウェアを備えています。ハードウェアテストは、ソフトウェア制御が最小限で済むか、不要であるように自動化されています。これは、一時的エラーの検出に特に便利であり、プロセス安全時間全体のごくわずかしか消費しません。
STM32G0 は安全アプリケーション専用として特別に設計されているわけではないため、上記の診断機能によるマイクロコントローラの負担軽減に対する全体的な寄与は不十分であることに注意してください。

ハードウェアの安全機能 (2)

- 完全性故障検出専用のハードウェア機能
  - FlashメモリのECC
    - 目的 – Flashの各256バイトワードに対するシングル･エラーの訂正とダブル･エラーの検出
    - 方法 – FlashバンクにSECDEDスキームを実装し、エラー検出時に割込みを生成
  - SRAMメモリのパリティ
    - 目的 – SRAMでのシングル･エラーの検出
    - 方法 – SRAMにパリティ･スキーム（8個ごとに1ビット）を実装し、エラー検出時に割込みを生成

life.augmented

エラー訂正コード（ECC）は、メモリデバイス上のデータ破壊の検出に使用されている最も一般的なテクニックです。完全性故障は、予測できない結果になることがあります。これは、内部ハードウェアブロックに基づいており、SECDED（シングルエラー訂正、ダブルエラー検出）として知られる拡張ハミングコードを使用する場合があります。この最後のケースでは、エラー検出時に、割込みが生成されます。

ハードウェアの安全機能 (3)

- HW CRC計算モジュール
  - 目的 – 所定のデータセットに対するCRCチェックサムの高速計算（ソフトウェア手法のサポート）
  - 方法 - データセット上への追加の冗長性（通信、メモリ）の構築
- 外部クロックに対するクロック・セキュリティ・システム
  - 目的 – 外部クロックの誤動作の検出
  - 方法 – 内部クロックへの自動切替え、NMI割込みの発生
  - HSEには独立したCSSブロックが使用可能
- クロック相互参照測定（2つの周波数間の差の監視）
  - 目的 – クロック・システムの誤動作の検出（ソフトウェア手法のサポート）
  - 方法 – リファレンス周波数入力を専用タイマの別周波数でキャプチャ

life.augmented

このスライドには、巡回冗長コード（CRC）計算とクロック制御専用のその他の安全機能がリストアップされています。

ハードウェアの安全機能 (4)

- 電源供給スーパーバイザ（パワーオン·リセット、パワーダウン·リセット、プログラム可能な電圧検出器）
  - 目的 – システムの全部品の正常動作を保証する安全しきい値
  - 方法 – 緊急停止処理のコールやデバイスをリセット状態に維持するための割込み
- 設定レジスタのロック·メカニズム
  - 目的 – 重要な設定（ペリフェラル、システム）の偶発的な変更の防止
  - 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処理
  - 目的 – 所定のデータセットに対するCRCチェックサムの高速ハードウェア計算と検証
  - 方法 - 通信データ上への追加の冗長性の構築
- 選択されたシステムエラーを収集するタイマのブレーク入力
  - 目的 – タイミング信号を生成するタイマ出力の高速制御
  - 方法 – すべてのタイマ出力を事前定義された状態にする

life.augmented

ここにリストアップされた ECC を除くすべてのテストは、故障検出専用です。そのため、さらに高いレベルの SIL を獲得するなど、補正や追加チェックが必要な場合に、別のソフトウェアテストを追加する必要があります。この場合、ユーザは、ソフトウェアテスト期間にプロセス安全時間が考慮されていることを確認する必要があります。

ファームウェア安全性アクセサリ·チェック

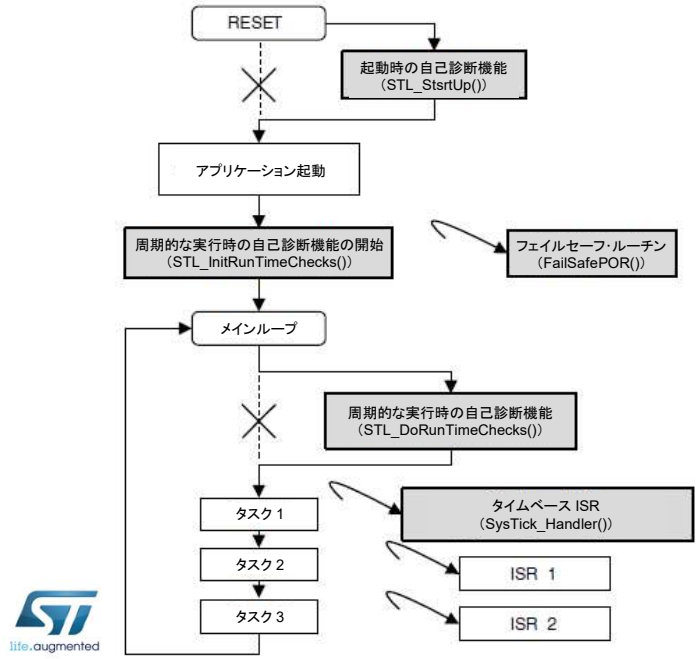
- ランダム故障の検出能力を向上するソフトウェア·チェック
  - STによる検証済みの標準的なソフトウェア·チェックを活用して安全関連プロジェクトに対応するため、複数のソフトウェア·ソリューションがst.com Webサイトから入手可能
    - X-CUBE-STL：SIL2までのIEC61508互換性を達成するためのソフトウェア·ソリューション
    - X-CUBE-CLASSB / STM32-CLASSB-SPL：IEC61730/IEC60335-1 Class B認証を獲得するためのソフトウェア·ソリューション

エンドユーザは、st.com Webサイトにアクセスするか、最寄りの ST 販売代理店に問い合わせて、特定のSTM32シリーズ／部品番号に対するソフトウェア·ソリューションを入手できるかどうか確認することが必要

life.augmented

このスライドでは、ST の自己診断機能ファームウェアソリューションに含まれているソフトウェアチェックが、適用可能である理由の簡単な説明とともにリストアップされています。一般的には、ファームウェアは、設計の詳細な知識に基づいてマイクロコントローラの汎用部品に重点を置いている一方で、SIL 規格の準拠に特化したパッケージは、効率のために、特定技法により証明されたより大規模な試験法を採用しています。このパッケージは無償ダウンロードの対象ではありません。ファームウェアについては、最寄りの ST 販売代理店までお問合わせください。

ファームウェア統合例



- 5つの基本ファームウェア・ブロック:
  - 起動時自己診断機能
    オプション、初回の1回の実行で全体をテスト
  - ランタイム自己診断機能の初期化
  - ランタイム自己診断機能
    周期的、メインループ内、メモリの部分的テスト
  - タイムベース割込み
  - 同期、クロック測定
  - フェイルセーフ手順
    検出、リカバリ

原則として、自己診断機能手順はシステム起動時のアプリケーションメインループを初期化する際の追加タスクとして含まれています。このランタイム自己診断機能タスクにより、CPU、クロック系、スタック境界、プログラムフロー、揮発性と不揮発性両方のメモリが周期的にテストされます。完了時には、すべてが正常に動作していれば、ウォッチドッグのタイムアウトがリフレッシュされます。メモリ領域は、タスク内で部分ごとに段階的にテストされます。テストは、タイマ割込みにより生成されるタイムベースティックを使用して同期されます。テストの完了に必要となる時間は、試験対象のメモリ領域のサイズ、タスクがコールされる頻度、1 つのステップの中でテストされるブロックのサイズに主に依存します。オプションで、1 回限りの初回起動時全体自己診断機能を、パワーオンリセット時またはアプリケーションリセット後に追加で実装できます。これらのテストの間に誤動作や不一致が検出されると、フェイルセーフルーチンが必ずコールされます。このルーチンがアプリケーションを安全な状態にし、次のリカバリの可能性を決定するはずです。

関連ペリフェラル

- 安全に関するトピックに関連した以下のトレーニングを参照
  - リセットおよびクロック制御（RCC）
  - Arm Cortex-M0+（コア）
  - 電源制御（PWR）
  - Flashメモリ（FLASH）
  - 巡回冗長検査（CRC）
  - 独立型ウォッチドッグ（IWDG）
  - システムウィンドウ型ウォッチドッグ（WWDG）

安全性は STM32G0 全製品シリーズに共通のものです。これまでに説明した機能の詳細な説明は、各種ペリフェラルの章に記載されています。

参照

- 詳細については、安全性に重点を置いたペリフェラルに関する次の参考文献およびその他のプレゼンテーションを参照：
  - アプリケーションノート AN3307：STM32アプリケーションでのIEC 60335 Class B認定を取得するためのガイドライン（Guidelines for obtaining IEC 60335 Class B certification in any STM32 applications）
  - アプリケーションノート AN4435：STM32アプリケーションでのUL/CSA/IEC 60335 Class B認定を取得するためのガイドライン（Guidelines for obtaining UL/CSA/IEC 60335 Class B certification in any STM32 application）*
  - UM2455 STM32G0マイクロコントローラ·シリーズの安全マニュアル（IEC 61508 およびその他の安全規格のフレームワークにおけるSTM32G0の使用に関する説明を含む）

（*）関連ファームウェアと関連資料は認証プロセス段階

life.augmented

ファームウェアと関連資料の入手、状況、配布可能性の詳細については、専用の関連資料を参照するか、最寄りの ST 販売代理店までお問合わせください。