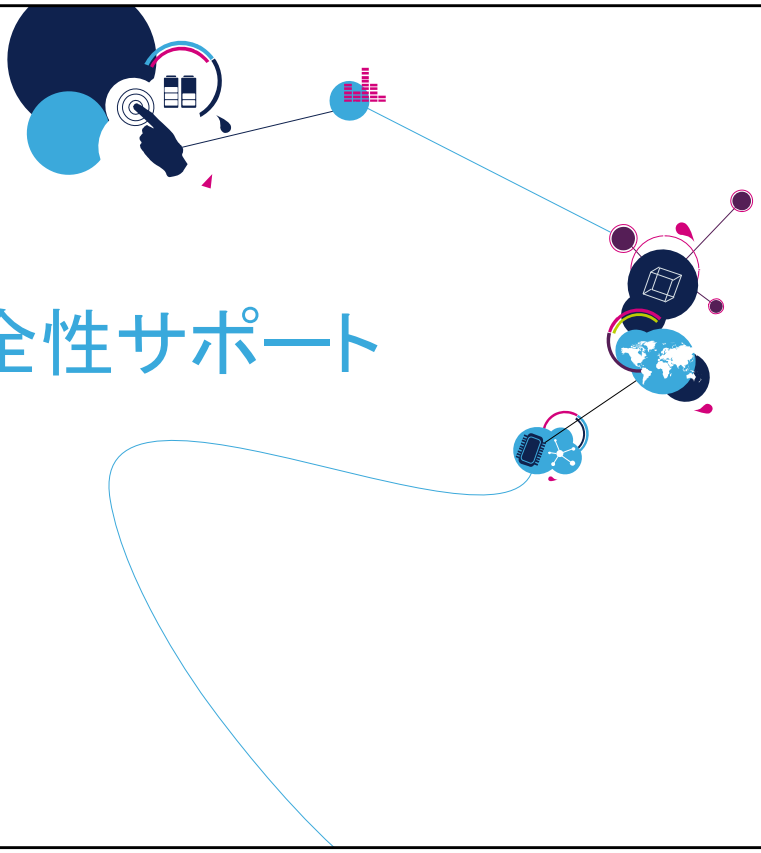


STM32MP1 – 安全性サポート

1.0 版

life.augmented

STM32 安全性サポートのプレゼンテーションにようこそ。ここでは、安全性基準の準拠に関する要件および顧客のプロジェクトの安全性を対象とした STMicroelectronics のサポート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は、基本的な安全性要件に準拠して、次のような重大な危険を防ぐ必要があります。
  - 人または動物の死亡やケガ
  - 環境への被害
  - 処理の崩壊や劣化
  - 二次的要因
    - 電子デバイスの信頼性や誤動作
    - 顧客の不満
- 安全性基準
  - 開発 – 正当かつ重要な国家機関および国際機関
  - 電気製品 – 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定のプロセスを加速させます。
- 安全性基準に準拠していることを保証します。

life.augmented

電子デバイスに関する安全性要件は、電子機器制御システムの使用が膨大な人間活動の範囲まで拡大するにつれて永続的に増加していきます。これらのデバイスが拡大していくことによって、特定の安全性基準に準拠する必要があります。主な目的は、人の死亡やケガ、環境への被害を防ぐことですが、重要データ、接続、電力、制御の損失などを含む産業的処理の劣化といったさらに低いレベルでの重要な要因がその他数多く存在します。国家水準および国際水準両方での統一基準を開発するプロセスは複雑です。正反対の作業が含まれることもあります（例：現地市場の保護とグローバル化）。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から発生します。この基準は、正当かつ重要な機関が提供し、世界で認知されている特定の試験施設がすべての必要な電気製品を検査および検証して基準に準拠していることを保証します。

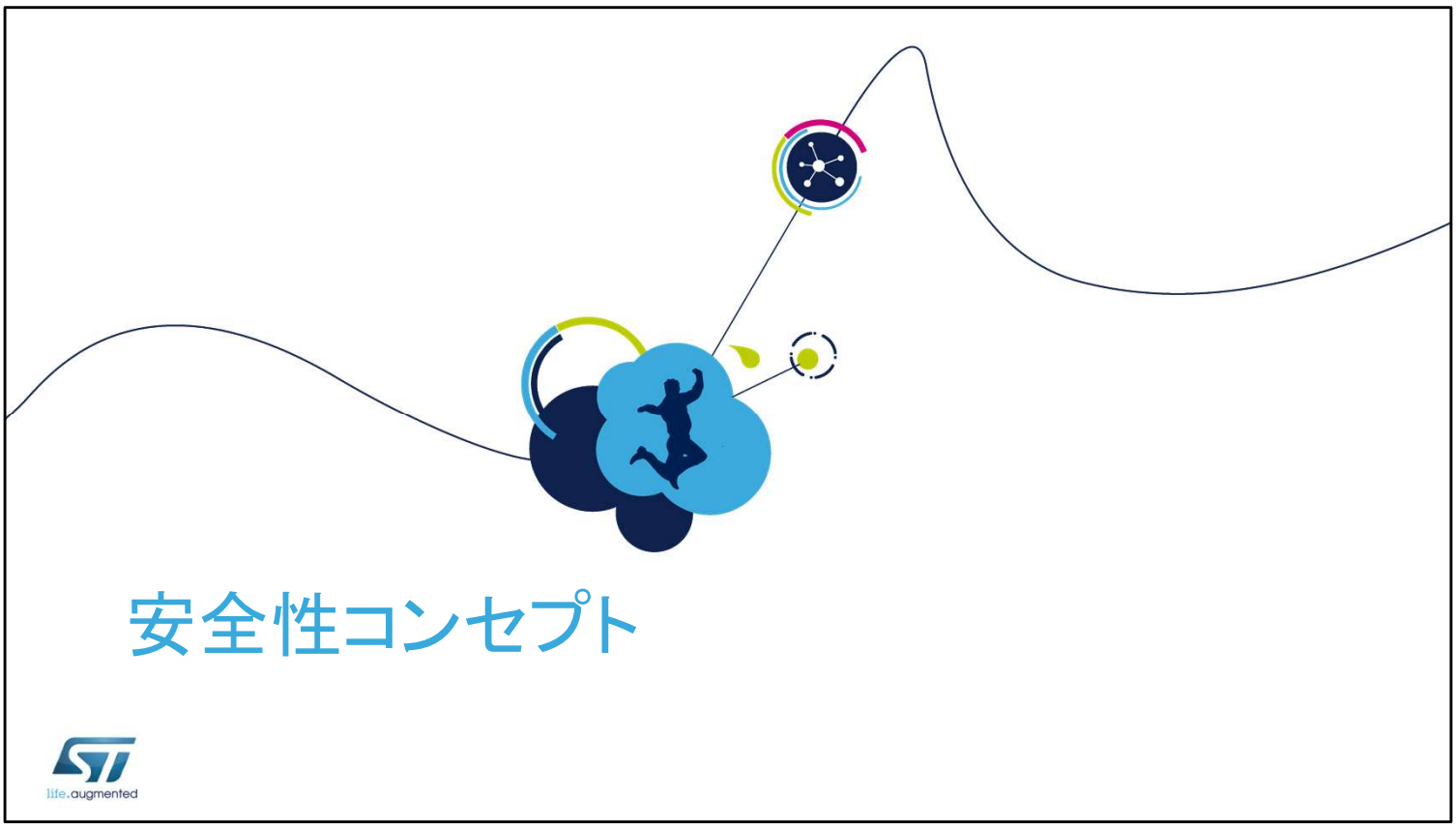
アプリケーションで安全性に注目することは、ソフトウェア開発を加速させるというメリットがあります。適切なハードウェア方式およびソフトウェア方式のアプリケーションとともに特定のハードウェア機能を使用し、効率的に早い段階での診断を行うことによって、想定できるコンポーネントの誤作動によって危険なイベントが発生する可能性を低減させます。特定のハードウェア設計や製造方式を適用すれば、さらにコンポーネントの信頼性を高めることができます。

ST の視点

- ST のサポート
  - 家庭電気製品の安全性 – IEC 60730 および IEC 60335（クラス B レベル）
  - 産業的安全性 – IEC 61508（SIL – 安全度水準 – SIL3 までのソリューション）
- 体系的障害の完全性（ハードウェア／ソフトウェアのライフサイクルメンテナンス）
  - 正しい内部プロセスおよび手順のセットアップ
    - ST の品質マニュアルにまとめられた共通ルール、SOP、特定のツールおよび分析（製造、操作手順、設計、素材、生産テスト、品質管理、ソフトウェア開発、資料、現場のフィードバック、問題追跡など）
  - すべてのルールや手順の正しい適用および基準の準拠
    - 定期的な監査および認定による確認
- ランダム障害に対する完全性（ハードウェア）
  - 予測不能な障害に対処する特定のハードウェア方式およびソフトウェア方式
    - 標準的な診断ソフトウェアのライブラリ提供
    - 安全性に関する関連資料（例：STM32MP1 安全性マニュアル）

life.augmented

ST は、「クラス B」や「クラス C」として知られている家庭用電気製品を対象とした基準と、「SIL」と呼ばれる安全度水準を対象とした共通の産業用基準の 2 つの基本的な安全性基準をサポートします。後者は、適用現場ごとに特化した非常に多岐にわたる基準を提供する汎用的な基準です。
ST はこれらの基準に準拠して、体系的障害とランダム障害の両方を考慮しています。体系的障害は予測可能で、回避方法と監視は業界で得た実践経験に基づきます。体系的障害は、主に製品のライフサイクルを通じて正しい内部処理を適用することで回避できます。これらの要件は、特定の内部品質関連資料で定義されています。定期的な点検と監査によって、これらの内部ルールが適用され、認知された基準に準拠していることが保証されます。
ランダム障害に対する完全性を保証するには、次のスライドに記載されているとおりに、特定のソフトウェア方式およびハードウェア設計技術を適用する必要があります。



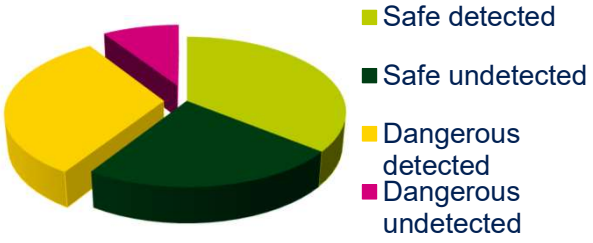
次のスライドには、マイクロコントローラでの作業時に考慮すべき主な安全性コンセプトの概要を示しています。

ランダム障害の方法論(1)

5

- ランダム障害の識別
  - 安全と危険
  - 検出と未検出
- ランダム障害のタイプ
  - 永続 - コンポーネントが永続的に損傷
  - 一時 - リカバリが可能
    - ソフトエラー – ソフトウェアテストやハードウェアテスト、診断で識別可能
    - 一時 - 高速ハードウェアテストや診断のみで識別可能
  - クロス製品障害の基準
    - 単一点障害(SPF) – 即時効果
    - 潜在障害(LF) – 休眠状態、他の障害と統合する可能性あり
    - 障害の共通発生(CCF) – 即時効果、複数コンポーネントに影響、複雑な安全性構造(電力、クロック、温度、タイミング)が崩壊する可能性あり

障害率円グラフ



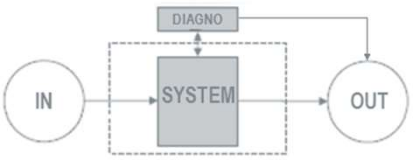
life.augmented

すべてのランダム障害が危険なイベントにつながるというわけではなく、安全性の観点から安全であるとみなされる場合もあります。基本的に、安全性基準では、安全性に直接的または間接的に関連する危険な障害を検出して、危険な状況が発生する可能性があることを把握するために監視が必要となります。安全なエラーと危険なエラーの両方が、システムによって検出、非表示、未検出のいずれかになります。危険なエラーが頻繁に発見されて時間内に防がれるほど、障害が危険なイベントに広がる可能性が低くなります。危険なエラーを検出して危険なイベントを防ぐために必要な時間は、システム(センサやアクチュエータなど)に関わるすべての遅延や反応時間を含む全体処理安全時間(PST)内に収める必要があります。数量化目的で、安全性基準では安全障害割合と診断カバー率について認知しておきます。安全障害割合(SFF)は、合計の障害割合(安全な障害と、検出済みおよび未検出の危険な障害)に対して、検出された危険な障害の割合を含む安全な障害の割合です。診断カバー率(DC)は、想定されるすべての危険な障害に対して、検出された危険な障害の可能性の割合です。ランダム障害は、永続エラーとリカバリ可能エラーを引き起こします。ハード障害は、コンポーネントに対して永続的な物理的損傷を引き起こし、システムが正常に動作できなくなります。補正できない場合、修理できるまでシステムを安全な状態(アクチュエータへの電源の切断など)にする必要があります。

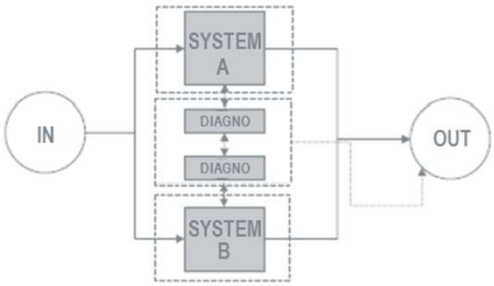
ランダム一時またはソフトエラーは訂正でき、数種類のリカバリプロセスを適用できます。検出に加えて、これらの障害は特定の場合において補正もできます。ソフトエラー障害はハードウェアとソフトウェアの両方で管理できますが、一時障害は高速ハードウェア方式のみ必要になります。ソフトウェアテストはかなり遅く、実行時間で制限されるため、これらの一時的なエラーや短期的なエラーに対する補正が一切できません。ISO 26262 を使用して、クロス製品の観点から、単一点、潜在、共通といった障害発生のタイプを認知できます。障害の共通発生は複雑な安全性構造も崩壊させる可能性があるため、特別に取り上げる必要があります。

ランダム障害の方法論(2)

- ランダム障害の制御技法
  - 検出
    - 診断でエラーを認知します。
    - システムが通常動作を続行できなくなります。
    - フェイル・セーフ状態またはリカバリ対象に設定する必要があります。



  - 補正(ハードフォルト許容値(HFT) > 0)
    - 診断で不良部品を検出して識別できます。
    - 次の正常な部品はそのまま使用できます。
    - システムはそのまま通常動作を続行できます。



- 基本原則 – 冗長性
  - 診断、比較、識別、投票

life.augmented

ランダム障害が検出されて補正できない場合、特に危険なエラーが検出された後、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、特定の検査機能のようなリカバリ処理を実行する必要があります。
通常、補正方式によってシステムはエラー訂正、パッシベーション、マスキングの機能を使用しつつ、正常な動作を続行できます。
一般的に、確実な投票処理は、破損した部品や後から正しいデータに置き換えられる誤ったデータを識別するために使用します。基準では、ハードフォルト許容値(HFT)、つまりシステムが対応でき、通常動作を続行できるエラーの最大数を認知しておきます。
特定の機能テストに加えて、ここでは冗長性が基本的な診断原理です。検出と補正の技法では、ともに確実な冗長性のレベルを常に効率的なものにしておく必要があります。補正では、矛盾点だけでなく正常な状態も識別する必要があるため、検出よりもかなり厳しい条件が求められます。これを行うには、特定の比較および投票のメカニズムをさらに適用する必要があります。

ランダム障害の方法論(3)

- 冗長性の技法
  - 構造
    - デュアルレジスタ、メモリ、CPU、ハードウェアコンパレータとボータのある MCU など並列識別構造にします。
  - 機能
    - 並列非対称ハードウェア構造または異なるソフトウェア方式を単一タスクに適用し、それらの出力を比較します。
  - 一時
    - 異なるタイムスロットで同じハードウェアやソフトウェアを使用して同じ方式を複数回実行し、結果を比較します。
  - 情報
    - 情報追加をデータレベルで実行し、ハードウェアやソフトウェアで準拠状況を評価します(パリティ、ECC、CRC、データプロトコル、コピー)。

life.augmented

必要な冗長性水準は、幅広いさまざまなソフトウェアやハードウェアの方式および技法を使用して達成できます。ここでは一部を列挙し、その他は後ほどこのプレゼンテーションでハイライトする予定です。この技法は、通常ハードウェア、ソフトウェア、またはその両方の組み合わせで実行できます。

診断責任

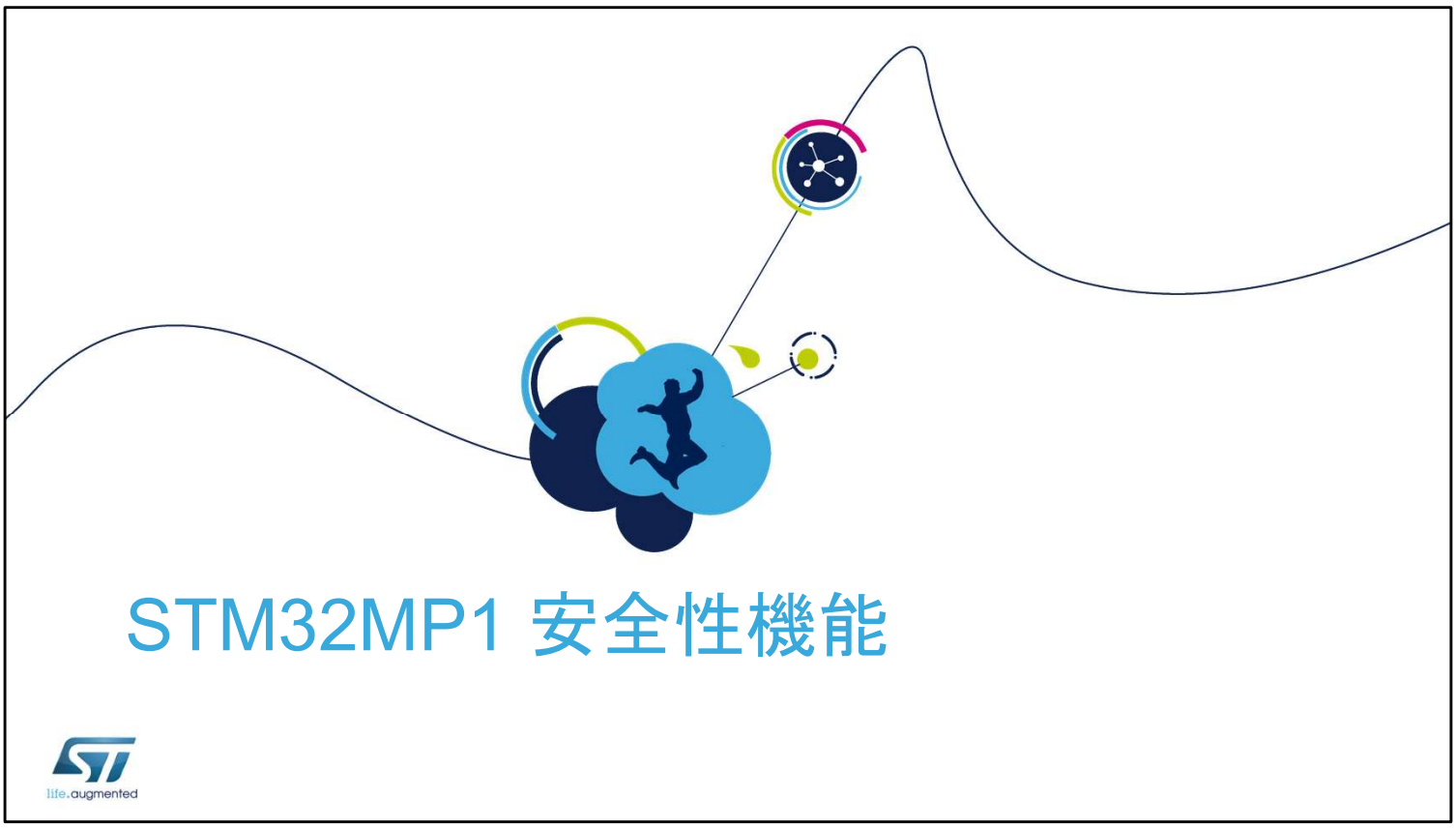
8

- ベンダの視点 → コンポーネントの汎用部品
  - 具体的な安全性タスクが前もってわかっていない場合、コンポーネントは「対象外」
  - ローカルコンポーネントの診断カバー率
    - 検出される危険なエラー(DC)の想定割合が増加します。
  - 重要部品、よく使用される部品、エリアが重要となる部品(CPU、クロックシステム、RAM、Flash メモリ)
    - 安全性全体において最も重要で影響が大きい部分です。
- ユーザの視点 → 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で統合されたコンポーネントを具体的な安全性タスクで識別
  - タスクに関係するマイクロコントローラ固有の部品の識別
    - 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
  - これら特定の部品だけの冗長性およびその他診断方式の電気製品
    - 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)
    - 論理検査(有効範囲、トレンド、応答、組み合わせ、タイミング、プロセスフローの順番)

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なプログラム可能電子コンポーネントであり、該当する基準で決まった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の安全性のサポートに関して、製品の最終的なアプリケーション目的と安全性タスクが前もってわかっていない場合、ベンダはその製品を「対象外」のコンポーネントとみなします。これは、決まった共通レベルの安全性タスクに対して「準備完了」または「適切」なコンポーネントについて話しているためです。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基準で定義される診断カバー率全体を満たすことです。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、さまざまな安全性タスクに関係する部分コンポーネントの一式とみなすことができ、それぞれに異なる診断カバー率とコンポーネントの安全性全体での重みがあります。必須となる安全性全体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部品および汎用部品、特にほとんどのアプリケーションでよく使用されているものに集中させる必要があります。これらの設計上で基本的かつ重要な部品の安全性がわずかに改善されると、必ずコンポーネントの安全性全体において最大の改善となり、これが各アプリケーションで有益なものとなります。

マイクロコントローラがアプリケーション設計に含まれており、安全性タスクが指定されていると、安全性サポートをもっと効率的に配置して、必要な安全性ケースに関係するマイクロコントローラの特定の部品だけをカバーできます。そして、アプリケーション要件、設計、制御下でのプロセスや設備の詳細な知識に基づいて数多くの効率的な方式を適用できるようになります。システム動作の冗長性と知識は個別またはともに適用される重要な原則となります。入出力は複数に増やしたり、フィードバックをチェックしたりして、トレンドや時間の範囲で論理状態、値、期待される応答をテストできます。そのプロセスが、正しいタイミングやフローの順番であることを監視できます。冗長性および独立型のフロー、分析、計算、データから導き出した結果の比較に基づいて、正しく判断できます。



次のスライドは安全性サポート専用の機能に特化しています。

ハードウェア安全性機能(1)

- 完全性障害を検出するための特定のハードウェア機能
  - 標準 Arm® Cortex®-M4 コアシステムの例外
    - 目的 – 予測できないソフトウェアやシステムの動作や誤動作をキャプチャします。
    - 方式 – システム割込みを処理します(HardFault、MemManage、BusFault、UsageFault、NMI)。
  - 標準 Arm Cortex-M4 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できないソフトウェアの動作や誤動作をキャプチャします。
    - 方式 – MPU ゾーンをプログラムして、特権ルールの強制、ソフトウェアプロセスの分離、メモリマップドリソースへのアクセスルールの強制を行います。

life.augmented

STM32MP1 マイクロプロセッサには、診断テストを行い、低レベルの安全性アプリケーションをカバーして障害にすぐ反応するためのハードウェアソリューションが備わっています。ハードウェアテストはソフトウェアによる制御が最小限に抑えられているか存在しておらず、自律しています。これは、特に一時的なエラーを検出するのに役立ち、安全性処理にかかる合計時間が最低限になります。
STM32MP1 は明示的に安全性アプリケーションでの特定の用途向けに設計されているわけではないため、上記の診断による MCU 軽減に対する全体的な貢献度は最低限のものであることに注意してください。

ハードウェア安全性機能(2)

- 完全性障害を検出するための特定のハードウェア機能
  - Arm Cortex-M4 専用ウィンドウ型ウォッチドッグ(WWDG1)
    - 目的 – 正しいソフトウェアのタイミングとフローを監視します。
    - 方式 – ウォッチドッグタイムアウトを処理するための正しい技法を適用します(指定のアプリケーションノートを参照)。
  - Arm Cortex-A7 専用独立型ウォッチドッグ(IWDG1 および IWDG2)
    - 目的 – 正しいソフトウェアのタイミングとフローを監視します。
    - 方式 – ウォッチドッグタイムアウトを処理するための正しい技法を適用します(指定のアプリケーションノートを参照)。

life.augmented

STM32MP1 マイクロコントローラには、診断テストを行い、低レベルの安全性アプリケーションをカバーして障害にすぐ反応するためのハードウェアソリューションが備わっています。ハードウェアテストはソフトウェアによる制御が最小限に抑えられているか存在しておらず、自律しています。これは、特に一時的なエラーを検出するのに役立ち、安全性処理にかかる合計時間が最低限になります。
STM32MP1 は明示的に安全性アプリケーションでの特定の用途向けに設計されているわけではないため、上記の診断による MCU 軽減に対する全体的な貢献度は最低限のものであることに注意してください。

ハードウェア安全性機能(3)

- 完全性障害を検出するための特定のハードウェア機能
  - 標準 Arm Cortex-M7 メモリ管理ユニット(MMU)
    - 目的 – ソフトウェアバグによる予測できないソフトウェアの動作や誤動作を検出します。
    - 方式 – MMU ゾーンをプログラムして、特権ルールの強制、ソフトウェアプロセスの分離、メモリマップドリソースへのアクセスルールの強制を行います。
  - 拡張信頼保護コントローラ(eTPZC)
    - 目的 – ペリフェラルへの TrustZone アクセス権を設定します。
    - 方式 – eTPZC ゾーンをプログラムして、Arm A7 専用ペリフェラルと Arm M4 専用ペリフェラルの隔離スキームを実装します。この隔離スキームによって、A7 CPU での安全性に関連しないアプリケーションソフトウェアの実行と、M4 CPU での安全性に関連するアプリケーションソフトウェアの実行が共存できます。

life.augmented

上記のハードウェア診断は、STM32MP1 で実行されるソフトウェアソリューションの体系的な安全度を向上させる関連の方法に役立ちます。

ハードウェア安全性機能(4)

- ハードウェア CRC 計算モジュール
  - 目的 – 指定のデータセットで CRC チェックサムを高速計算します(ソフトウェア方式のサポート)。
  - 方式 - データセットの上に追加の冗長性(通信、メモリ)を構築します。
- 外部クロックの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を検出します。
  - 方式 – 内部クロックに自動的に切り替えて、NMI 割込みを発生させます。
  - 個別の CSS ブロックは HSE に使用できます。
- クロック相互参照測定(2 つの周波数の違いを監視)
  - 目的 – クロックシステムの誤動作を検出します(ソフトウェア方式のサポート)。
  - 方式 – 参照周波数入力が専用タイマの別の入力でキャプチャされます。

life.augmented

このスライドでは、チェックサム冗長コード(CRC)の計算とクロック制御に特化した追加の安全性機能を列挙しています。

ハードウェア安全性機能(5)

- 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 – 安全閾値でシステムの全部品が正常に機能していることを確認します。
  - 方式 – 緊急停止処理を呼び出すための割込みを発生させたり、デバイスをリセット状態で保持したりします。
- 通信ペリフェラルでの処理プロトコル
  - 目的 – 指定のデータセットで CRC チェックサムを高速ハードウェアで計算および検証します。
  - 方式 – 通信データの上に追加の冗長性を構築します。
- 選択し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を高速制御します。
  - 方式 – すべてのタイマ出力を事前定義された状態にします。

life.augmented

さらに高いレベルの SIL を達成する場合など、補正や追加の検査が必要な場合はソフトウェアテストを追加する必要があることに注意してください。その場合、ソフトウェアによるテスト時間が処理安全時間を考慮していることをユーザは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検査

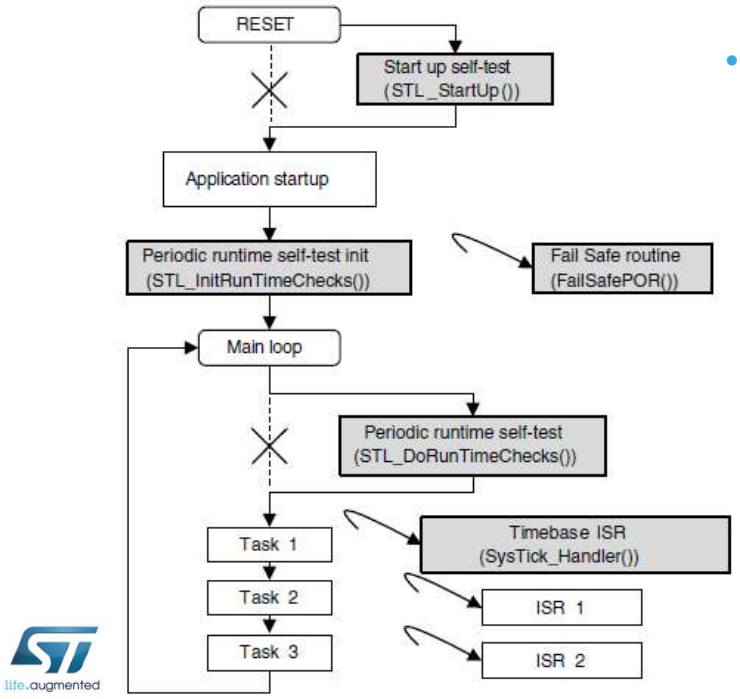
- ランダム障害を検出する機能を改善するソフトウェア検査
  - 基準を活用して安全性に関連するプロジェクトに対応するために、複数のソフトウェアソリューションが st.com ウェブサイトで使用できます。ST 認証ソフトウェア検査には次のものがあります。
    - X-CUBE-STL：SIL2 までの IEC61508 の互換性に対応したソフトウェアソリューション
    - X-CUBE-CLASSB/STM32-CLASSB-SPL：IEC61730/IEC60335-1 クラス B 認定に対応したソフトウェアソリューション

エンドユーザは、st.com ウェブサイトにアクセスしたり、お近くの ST 販売代理店に連絡して、特定の STM32 シリーズ／部品番号に使用できるソフトウェアソリューションを確認する必要があります。

life.augmented

このスライドでは、ST の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検査を、簡単な適用理由とともに列挙しています。一般的に、ファームウェアは設計に関する深い知識に基づいたマイクロコントローラの汎用部品を中心としていますが、SIL 基準の対応に特化したパッケージでは効率性を求める特定の方法論によって証明されたさらに拡張性のあるテスト方式を使用します。このパッケージは無料でダウンロードできません。ファームウェアについては、お近くの ST 販売代理店にお尋ねください。

ファームウェア統合例



- 5 個の基本的なファームウェアブロック:
  - 起動時セルフテスト
    オプション、初回 1 回の実行で全体テスト
  - ランタイム時セルフテスト初期化
  - ランタイム時セルフテスト
    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・セーフ手順
    検出、リカバリ

原則として、セルフテスト手順はシステム起動中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。このランタイム時セルフテストタスクには、CPU、クロックシステム、スタック境界、プログラムフロー、揮発性および不揮発性メモリの周期的テストがあります。ウォッチドッグタイムアウトは正常に完了した場合にリフレッシュされます。メモリ領域は、タスク内の部品ごとにステップごとにテストされます。このテストは、タイマ割込みから導かれるタイムベースティックによって同期されます。テストの完了に必要な間隔は、主に 1 回のステップでテストされる対象のメモリ領域のサイズ、タスク呼び出しの頻度、ブロックのサイズに依存します。オプションとして、1 回きりの初期起動時全体セルフテストはパワーオン・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行できます。このテスト中に誤動作や矛盾点が見つかった場合、必ずフェイル・セーフルーチンが呼び出されます。これは、アプリケーションを安全な状態にして、次のリカバリ可能性を決定する必要があります。

関連するペリフェラル

- 次の安全性項目に関するトレーニングを参照してください。
  - リセットおよびクロック制御（RCC）
  - Arm Cortex-M4（コア）
  - Arm Cortex-A7（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）

life.augmented

安全性は STM32MP1 全製品範囲に影響しています。前述の機能の詳細については、それぞれのペリフェラルの章で確認できます。

参照

- 詳細については、次の資料および安全性に特化したペリフェラルに関連するその他のプレゼンテーションを参照してください。
  - アプリケーションノート AN3307：Guidelines for obtaining IEC 60335 Class B certification in any STM32 applications
  - アプリケーションノート AN4435：Guidelines for obtaining UL/CSA/IEC 60335 Class B certification in any STM32 application *

(*) 関連するファームウェアおよび関連資料が、現在も認定プロセス中である場合があります。

使用可不可、ステータス、ファームウェアや関連資料の提供の詳細については、専用の関連資料を参照するか、お近くの ST 販売代理店にお問い合わせください。