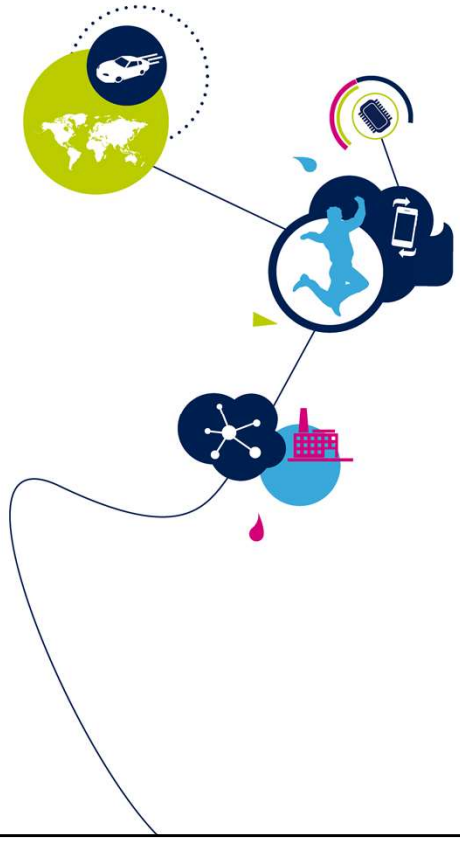
STM32WB – セーフティ

セーフティについて

1.0 版



life.augmented

STM32 セーフティについてのプレゼンテーションにようこそ。ここでは、安全規格への適合要件と、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STMicroelectronics が支援する方法について説明を行います。

概要

- 広範囲な電子アプリケーションは、以下のような重大なハザードの防止のために、基本的な安全要件に適合する必要があります。
  - 人または動物の死亡または負傷
  - 環境破壊
  - プロセスの破壊または価値の低下
  - 二次的要因
    - 電子デバイスの信頼性や誤動作
    - お客様の不満
- 安全規格
  - 策定 – 国家・国際立法府 & 行政府
  - 装置 – 世界的に認知された試験機関

アプリケーション側の利点

- ユーザソフトウェアの開発プロセスと認証プロセスの迅速化
- 安全規格に対する適合の保証

life.augmented

電子制御システムの利用が広範な人間活動に拡大していることから、電子デバイスに対する安全性要求は常に増加を続けています。これらのデバイスが大幅に拡大することにより、特定の安全規格に対する適合が必要となります。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には、重要データや接続、電源、制御、その他多くの喪失を含む産業プロセスの価値低下のような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の両方で整合規格を策定するプロセスはかなり複雑であり、正反対の活動（地域市場の保護とそのグローバライゼーションなど）が必要となることもあります。いずれにせよ、主に影響を及ぼす要因は、現場の経験、市場からの要求、保険問題、貿易とビジネスのグローバライゼーションに起因します。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、すべての必要装置すべての検査と検証を行って、それらの適合性を保証しています。

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可能性があります。適切なハードウェア手法とソフトウェア手法とともに特定のハードウェア機能が用いられた効率的で早期の診断により、起こり得るコンポーネントの誤動作による危険事象の確率が下がります。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 がフォーカスするもの

- ST によるサポート
  - 家庭用器具向け安全性 – IEC 60730 & IEC 60335（クラス B レベル）
  - 産業向け機能安全 – IEC 61508（SIL – SIL3 ソリューションまで）
- 系統的故障の完全性（ハードウェア／ソフトウェアのライフサイクル保守）
  - 正しい内部プロセスと手順の策定
    - ST の品質マニュアル、SOP、専用ツール & 分析（製造、操作手順、設計、材料、生産テスト、品質管理、ソフトウェア開発、文書化、市場フィードバック、問題追跡など）に収集されている共通ルール
  - すべてのルールと手順の正しい適用と、規格に対する適合性
    - 定期監査と認証により確認
- ランダム故障に対する完全性（ハードウェア）
  - 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
    - 完全関連資料（STM32WB 安全性マニュアルなど）

life.augmented

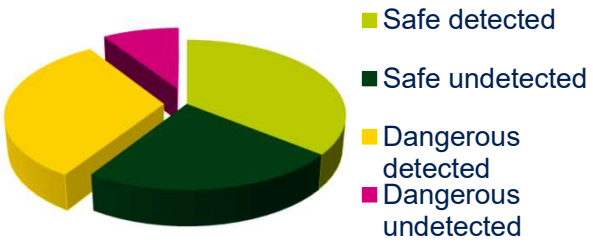
ST は 2 つの基本的安全規格に対応しています。1 つは、「クラス B」または「クラス C」規格と呼ばれる家庭用器具を対象としたものであり、もう 1 つは、「SIL」と呼ばれる安全度水準を対象としたより共通な産業用規格です。後者は汎用規格であり、さまざまな分野のアプリケーション専用の数多くの派生規格がそこから作られています。
これらの規格を遵守する ST は、系統的故障とランダム故障の両方に注意を払っています。系統的故障は予測可能であり、その回避と監視は、業界で得られた実践的経験に基づくものです。系統的故障は、主として正しい内部プロセスをある製品のライフサイクル全体に適用することで回避可能です。これらの要件は、特定の内部品質関連資料の中に定義されます。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、一般に認められた規格に適合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、以下のスライドに記載されているように、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。

セーフティ コンセプト

次のスライドには、マイクロコントローラを使用するにあたって考慮すべき主なセーフティコンセプトの概要が記載されています。

ランダム故障に対する技法(1)

- ランダム故障の特定
  - 安全 & 危険
  - 検出可能 & 検出不可能
- ランダム故障のタイプ
  - 恒久的 - コンポーネントは恒久的に損傷
  - 過渡的 - 回復の可能性
    - ソフトエラー – SW もしくは HW のテストまたは診断により特定可能
    - 過渡的 - 高速 HW テストまたは診断により排他的に特定可能
  - 製品相互間故障の基準
    - 単一点故障(SPF) – 即座に影響
    - 潜在故障(LF) – 休眠中であり、別の故障と一体化する可能性あり
    - 共通原因故障(CCF) – 即座に影響し、複数のコンポーネントが影響を受けます。
      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があります。

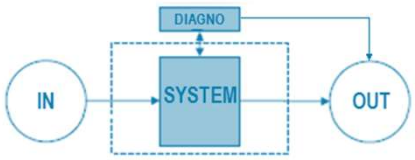


life.augmented

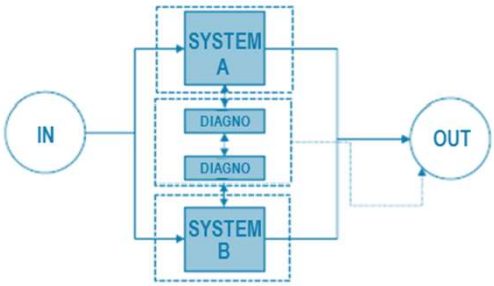
すべてのランダム故障が危険事象を招くわけではなく、安全性の観点から安全と見なされることすらあります。基本的に、安全規格には、直接的または間接的に安全性との関連性があり、危険な状況を招く潜在的可能性がある危険側故障を検出するための監視が必要です。安全なエラーと危険なエラーのどちらも、検出されることもあれば、隠れていてシステムによって検出されないままとなることもあります。危険なエラーが発見され、防止が間に合う頻度が増すほどに、故障が危険事象に伝播する確率が下がることが多くなります。危険なエラーを検出して危険事象を防止するのに必要な時間は、システム(センサー、アクチュエータなど)に起こり得る遅延と応答時間がすべて含まれている、利用可能なプロセス安全時間(PST)全体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高く評価されています。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の比率です。ラムダム故障によって、恒久的エラーが起こることも、回復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することができなくなります。補正を行えない場合には、システムは修理されるまで安全状態とする(アクチュエータへの電源遮断など)必要があります。
ランダムな過渡的エラーやソフトエラーは修正可能であり、何らかの回復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、過渡的故障には高速なハードウェア手法が専用で必要となります。ソフトウェアテストは大幅に遅く、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潜在的可能性があるため、共通原因故障には特に注目する必要があります。

ランダム故障に対する技法(2)

- ランダム故障制御手法
  - 検出
    - 診断によりエラーを認識
    - システムは正常動作を継続不可
    - システムはフェイル・セーフ状態となるか回復する必要あり



  - 補正(ハードフォルト許容度(HFT) > 0)
    - 診断により問題のある部分の検出と特定が可能
    - 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



- 基本原理 – 冗長化
  - 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状態とするか、リセット、ロールバック、専用のチェック機能のような回復プロセスを通過させる必要があります。
補正手法によってシステムが通常動作を継続可能と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用いられます。通常は確実な多数決プロセスが用いられ、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でありながら耐えることの可能な最大エラー数のことである、ハードフォルト許容度(HFT)が高く評価されています。
専用の機能テストに加えて、ここでは冗長化も基本的な診断原理となります。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果的であることを必要とします。相違点だけではなく正しい状態についても特定の必要があるため、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。

ランダム故障に対する技法(3)

- 冗長化手法
  - 構造
    - 二重化されたレジスタ、メモリ、CPU、ハードウェアコンパレータと多数決回路付きのMCUのような並列同一構造
  - 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用い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)を用いて適合性を評価

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用い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、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されることが一般的です。

診断の責任

- ベンダ側重点項目 → コンポーネントの汎用部分
  - 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
  - 共通使用される重要な大面積部品(CPU、クロック系、RAM、Flash メモリ)
    - 全体の安全バジェットに対して最大の重要度と影響
- ユーザ側重点項目 → アプリケーション専用部品
  - 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、具体的安全タスクを用いて特定される
  - タスクに関係するマイクロコントローラ専用部品の特定
    - 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化とその他の診断手法を適用
    - 冗長化(複数チャネル、データと通信処理 - 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、組み合わせ、タイミング、プロセスフロー順)

life.augmented

安全性の観点からは、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適合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、事前にはその最終用途の目的と安全タスクがわからないことから、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、どんな場合でもコンポーネントの全体的な信頼性を対象としており、最終用途から求められる所定の安全度水準に対する規格で定義される診断カバー率の全体バジェットを満足するためのものです。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率的な方法は、マイクロコントローラの重要な汎用部分(特に、多くのアプリケーションで共通に使用されるもの)に焦点を合わせることである必要があります。これらの基本的で重要な設計部分の安全性における小幅の向上であっても、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得られ、各アプリケーションにとっては有益です。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、求められる安全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分のみがその対象となります。そうすると、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可能となります。冗長化とシステム動作に対する知識は、個別にも一緒にも適用される極めて重要な原理です。入出力は、多重化かフィードバックによるチェックを行い、傾向または時間間隔による論理的状態、値、期待される応答に対するテストが可能です。これらのプロセスは、タイミングとフロー順が正しいかの監視が行えます。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。

STM32WB 安全機能

以下のスライドでは、安全性対応のための機能を説明します。

ハードウェア安全機能(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+ および Cortex-M4 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捕獲
    - 方法 – システム割込み(HardFault、MemManage、BusFault、UsageFault、NMI)の処理
  - 標準の 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ソフトウェアの予測不可能な動作または誤動作のキャプチャ
    - 方法 – 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に対するアクセス規則の強制を行うようにMPU ゾーンのプログラミング
  - 独立ウォッチドッグと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

STM32WB マイクロコントローラは、効率的診断テストのためと、広範囲な低レベル安全アプリケーションが対象となる潜在的可能性の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、過渡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。
STM32WB はセーフティアプリケーション専用として特別に設計されたものではないため、上記の診断機能による MCU 緩和への全体的な寄与は十分とは言えないことに注意してください。

ハードウェア安全機能(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 64bit ワードに対する単一エラーの修正と二重エラーの検出
    - 方法 – Flash バンクに対する SECDED スキーム、エラー検出時の割り込み生成の実装
  - SRAM2 メモリのパリティ
    - 目的 – 単一エラーの検出
    - 方法 – SRAM2 に対するパリティスキーム、エラー検出時の割り込み生成の実装

誤り訂正符号(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(単一誤り訂正二重誤り検出)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。この最後の場合には、エラー検出時に割込みが生成されます。

ハードウェア安全機能(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(通信、メモリ)に対する追加の冗長性の構築
- 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 – 基準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。

ハードウェア安全機能(4)

- 供給電源の監視機能(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閾値
  - 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
- 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 - 通信データに対する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既定の状態とする

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、故障検出専用となっています。より高いレベルの SIL を獲得するなど、補正や追加チェックが必要である場合に、別のソフトウェアテストを追加する必要がある理由はここにあります。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

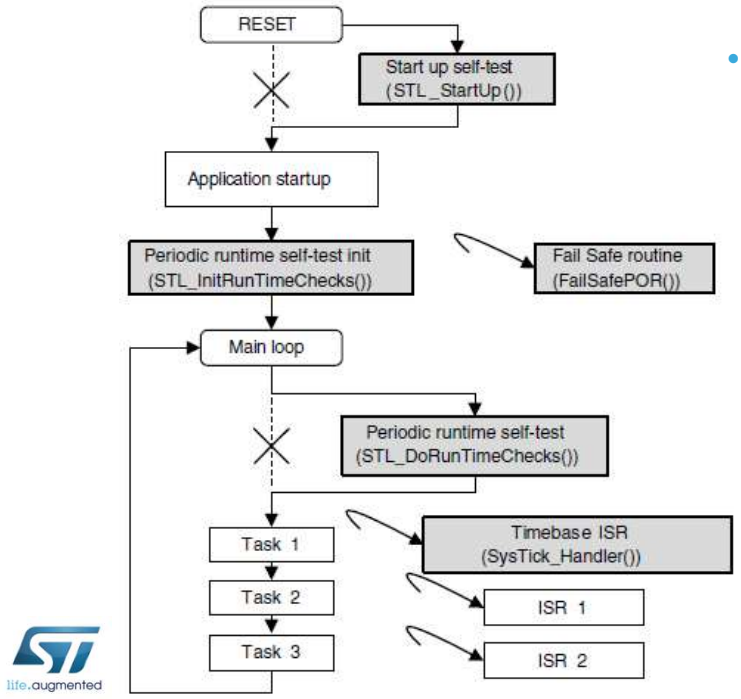
- ランダム故障の検出能力を向上するソフトウェアチェック
  - ST による検証済みの標準的なソフトウェアチェックを活用して安全関連プロジェクトに対応するため、複数のソフトウェアソリューションが st.com ウェブサイトから入手可能:
    - X-CUBE-STL:SIL2 までの IEC61508 互換性を達成するためのソフトウェアソリューション
    - X-CUBE-CLASSB/ STM32-CLASSB-SPL:IEC61730/IEC60335-1 クラス B 認証を獲得するためのソフトウェアソリューション

エンドユーザは、st.com ウェブサイトにアクセスするか、お近くの STM32 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が入手可能であるか確認する必要があります。

life.augmented

このスライドには、適用可能である理由の簡単な概要とともに、ST 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分に焦点を合わせている一方で、SIL 規格達成用のパッケージは、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用いています。パッケージは無償ダウンロードの対象ではありません。ユーザは、ファームウェアについてお近くの ST 代理店までお問い合わせください。

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、最初に 1 回だけ実行、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、回復

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の初期化時における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、クロックシステム、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用いて同期されます。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、パワーオン時またはアプリケーションリセット後に、1 回限りの初回起動時全体自己診断機能を追加実装できます。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とし、次の回復の可能性を決定するはずです。

関連ペリフェラル

- セーフティのトピックに関連した以下の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-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）

life.augmented

セーフティは STM32WB 製品群全体に共通のものです。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項目に記載されています。

参照

- 詳細については、安全性を焦点としたペリフェラルに関する以下の資料と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*
  - UM2456 STM32WB マイクロコントローラシリーズの安全性マニュアル（IEC 61508 その他の安全規格のフレームワークにおける STM32WB 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ドキュメントの入手、状況、配布可能性の詳細については、専用関連資料を参照するか、お近くの ST 代理店までお問い合わせください。