life.augmented

AN5698

アプリケーション・ノート

STM32 用 X-CUBE-STL 機能安全パッケージ（IEC 61508 準拠）の他の安全標準への適合

概要

STM32 マイクロコントローラ / マイクロプロセッサ安全マニュアルで報告されている安全解析は、安全基準 IEC 61508 に準拠して実行されます。この文書では、さまざまな安全規格に関する変更影響分析の結果を報告します。取り上げられる新しい安全規格ごとに、次の項目が考慮されます。

- 推奨ハードウェアアーキテクチャ（アーキテクチャカテゴリ）の違い、および IEC 61508 の安全アーキテクチャへのマッピング方法。
- 安全度水準の定義と測定基準の計算方法の違い、および新しい規格に従ったデバイスの安全性能の再計算と判断の方法。

この変更影響分析で検証された安全標準は次のとおりです。

- ISO 13849-1:2015、ISO13849-2:2012： Safety of machinery and Safety, related parts of control systems
- IEC 61800-5-2:2016: Adjustable speed electrical power drive systems (related parts Safety requirements, functional).

1 本書について

1.1 目的と適用範囲

STM32 マイクロコントローラ / マイクロプロセッサ安全マニュアルで報告されている安全解析は、IEC 61508 安全基準に従って実行されます。

この文書には、STM32 マイクロコントローラ / マイクロプロセッサの IEC61508 準拠の安全解析に適用され、関連する安全マニュアルに含まれている、さまざまな安全標準に関する変更影響解析の結果が含まれています。

この文書は、Arm® ベースのデバイスである STM32 マイクロコントローラおよびマイクロプロセッサを対象としています。

注 Arm は、米国内およびその他の地域にある Arm Limited（またはその子会社）の登録商標です。

1.2 用語と略語

表 1. 用語と略語

項目（略称）	定義
CoU	使用条件
CPU	中央処理装置
DC	診断範囲
FIT	故障率の単位
FMEA	故障モード影響解析
FMEDA	故障モードの影響診断解析
ITRS	国際半導体技術ロードマップ
MCU	マイクロコントローラユニット
MPU	マイクロプロセッサユニット
SFF	安全側故障割合
SIL	安全度水準

1.3 参照安全規格

[1] ISO 13849-1:2015, ISO13849-2:2012 – Safety of machinery and Safety-related parts of control systems,

[2] IEC 61800-5-2:2016 –Adjustable speed electrical power drive systems – Part 5-2: 安全要件 – 機能

[3] IEC61508:1-7© IEC:2010 - Functional safety of electrical/electronic/programmable electronic safety-related systems

2 ISO 13849-1:2015、ISO 13849-2:2012

ISO 13849-1 は、タイプ B1 規格です。プログラマブル電子回路、ハードウェア、およびソフトウェアを含む、機械制御システムの安全関連部品（SRP/CS）の開発のためのガイドラインを提供します。

2.1 ISO 13849 アーキテクチャカテゴリ

標準的な安全機能の図による表記は、ISO 13849-1:2015, [4.4] で報告されています。マイクロコントローラ安全マニュアルの関連したセクションで定義されている Compliant item（準拠項目）がブロック b（ロジック）の実装のために使用されているという仮定のもと、ISO 13849 の表記と安全マニュアルの表記とが同等であることは明白です。したがって、ISO 13849 アーキテクチャを Compliant item（準拠項目）の定義のためにマイクロコントローラ安全マニュアルに示されているものへマッピングすることが可能です。

セクション 2 ISO 13849-1:2015、ISO 13849-2:2012 の ISO 13849-1:2015 では、5 つの異なるカテゴリを詳細に定義しています。次の表に、マイクロコントローラ安全マニュアルの関連するセクションで説明されている、IEC 61508 に準拠したアーキテクチャの 1 つによって可能な実装をカテゴリごとに示します。各カテゴリに対して、達成可能な PL は診断範囲 $(DC)_{avg}$ の特定の値および危険側故障発生までの平均時間（MTTFd）によって決定されることに注意が必要です。（計算の詳細については ISO 13849 安全指標の計算 を参照してください。）。

表 2. ISO 13849 アーキテクチャカテゴリ

ISO13849-1:2015		IEC61508 準拠の安全アーキテクチャへのリンク	注記/制約事項
カテゴリ	条項		
B	6.2.3	1oo1 アーキテクチャで可能	MTTFd の要件はなく、$(DC)_{avg}$ はカテゴリ B に対して与えられていますが、いずれにしてもマイクロコントローラ安全マニュアルの推奨に従うことを推奨します。
1	6.2.4	推奨せず	推奨されないカテゴリー（IEC13849-1 を参照）。
2	6.2.5	1oo1 アーキテクチャで可能（外部 WDT は必須）	TE として機能する外部 WDT（CPU_SM_5）の採用は必須です。 $(DC)_{avg}$ および MTTFd の制約を満足することができますが、計算が必要です。(1) CCF の制約を満足しています。(2)
3	6.2.6	1oo2 アーキテクチャ + DUAL_SM_0 で可能	DC_{avg} および MTTFd の制約を満足することができますが、計算が必要です。(1) CCF の制約を満足しています。(2)
4	6.2.7	1oo2 アーキテクチャ + DUAL_SM_0 で可能	故障の蓄積を軽減するには、DUAL_SM_0 方式の実装が必須です。 DC_{avg} および MTTFd の制約を満足することができますが、計算が必要です。(1) CCF の制約を満足しています。(2)

1. DC_{avg} と MTTFd に関する計算は、安全機能の実装で使用されるので、デバイス以外の構成部品（センサ、アクチュエータなど）を含むこともあります。したがって、これらの数値はシステムレベルで評価する必要があります。
2. ISO13849-1 の附属書 F、表 F.1 に示されている CCF の追加要件は、基本的にシステム実装を強制するものであるため、マイクロコントローラ安全マニュアルの範囲外です。IEC61508 準拠活動（マイクロコントローラ安全マニュアル）のアウトプットとして得られる完全な安全解析が、表 F.1 の項目 #4 のスコアを求めるのに役立つことに注目が必要です。

2.2 ISO13849 安全指標の計算

ISO 13849 の付録 C に、さまざまな電気または電子部品の標準化した危険側故障発生までの平均時間（MTTFd）の表が示されています。ただし、ISO 13849 の表 C.3 は、プログラマブル IC の MTTFd を分類しようとする中で、IC メーカーのデータを参照しています。その結果、マイクロコントローラ安全マニュアルの安全解析結果は、ISO 13849 のドメインに再マッピングすることができます。IEC 61508 用に計算されたものでさえ、危険側故障の特定の定義においてますます正確になっているからです。

あるコンポーネントに対して PFH << 1 の場合、MTTFd = 1 / PFH と見なすことができます。

ST の方法論によると、FMEDA データには、潜在的な部分的な安全性についての仮定を持たない一時的故障に関連する故障率が含まれることには注意が必要です。この仮定のため、Device FMEDA の PFH 値は、非常に保守的な MTTFd の計算値を導き出します。

ISO 13849-1 では、各単一コンポーネントの DC は IEC 61508 の指標と同じ意味を持ちます。したがって、マイクロコントローラ安全マニュアルと関連する FMEA/FMEDA の結果を再利用できます。ただし、この標準では、コントロールシステムの各部分の寄与がチャネルのさまざまなサブシステムの MTTFd に対して重み付けされている、付属書 E の式 E.1 で定義されている式の形で、SRP/CS 全体に適用できる DC_{avg} のコンセプトを規定しています。したがって、全体の DC_{avg} の計算の責任はエンドユーザーにあります。

この規格では、DC_{avg} の計算中に故障除外の可能性を否定しています（ISO13849-2 表 D.21 例外は認めない）。これは、マイクロコントローラ安全マニュアルに記載されているデバイス解析の前提でもあります。

注　STM32 マイクロコントローラ安全マニュアルで分析された各アーキテクチャのソリューションにより、PFH 値が高い MTTFd を生み出すことになります。

3 IEC 61800-5-2:2016

この規格の適用範囲は、可変速電気駆動システムの機能安全です。

3.1 IEC 61800 アーキテクチャカテゴリ

HFT およびアーキテクチャに関する IEC 61800 の定義は IEC61508 のものと同等なので、再マッピングは簡単です。

STM32xx マイクロコントローラは、マイクロコントローラ安全マニュアルで報告されている考慮事項でタイプ B と見なされます（前提条件のセクションを参照）。

3.2 IEC 61800 安全指標の計算

PDS（SR）によって実行される安全機能の PFH は、IEC 61508-2 のアプリケーションによって評価されます。規格 IEC 61508 との強い連係は、同じ関連する指標 PFH および SFF の IEC 61800-5-2 での採用にも反映されています。したがって、マイクロコントローラ安全マニュアル（および関連する FMEA と FMEDA）の結果は、IEC 61800 ドメインに再マッピングできます。

改版履歴

表 3. 文書改版履歴

日付	版	変更内容
2021 年 10 月 12 日	1	初版発行

目次

表一覧