

# ISO 26262 機能安全準拠/対応 dsPIC33 DSC





## ISO 26262 機能安全準拠/対応 dsPIC33C DSC

セーフティクリティカルな車載アプリケーションは信頼性の高い動作を必要とし、かつユーザーの安全を確保する必要があるため、その設計には困難が伴います。Microchip 社の dsPIC33C DSC(デジタルシグナルコントローラ)は、ISO 26262 ASIL-B に準拠した車載市場のセーフティクリティカルな高性能組み込み、センサインターフェイス、デジタル電源、モータ制御アプリケーションに最適です。

ISO 26262 機能安全に関するユーザーの知識と経験の多寡に関わらず、Microchip 社はコスト、リスク、開発期間を低減し、機能安全要件を満たした設計の認証に役立つソリューションを提供できます。Microchip 社の機能安全準拠/対応 dsPIC33C DSC は車載設計の ISO 26262 ASIL-B 認証を支援するため以下のリソースを提供しています。



## 機能安全ソリューション

1. 「機能安全準拠」デバイスの要件を満たす一部の dsPIC33C DSC は、ISO 26262 に準拠した開発プロセスによって設計されています。
2. FMEDA(故障モード影響診断解析) レポート
3. FSM(機能安全マニュアル)
4. 機能安全リファレンス アプリケーション
5. アプリケーションノート - 『ISO 26262 Functional Safety: Implementation of a Safety Element out of Context』 (AN3864)
6. TÜV Rheinland 社認証済み機能安全診断ライブラリ
7. 開発エコシステム
8. ピン FMEA および DFA(従属故障解析) を含む安全関連の補足資料
9. FMEA、ユーザーマニュアル、確認レビューファイルを備えた機能安全準拠の協調スケジュール

セーフティクリティカル アプリケーションの開発を支援するため、Microchip 社は以下を提供しています。

1. 機能安全ベーシック パッケージ
2. 機能安全スタータ パッケージ
3. 機能安全フルパッケージ

## FMEDA(故障モード影響診断解析) レポート

機能安全準拠/対応 dsPIC33C DSC に関する FMEDA レポートでは、そのデバイスの故障モード、FIT (Failure-In-Time) 分布、検出方法が定量化されており、カバレッジプラン作成に役立ちます。

Note: ASIL-C の準拠には、ASIL デコンポジションにより Microchip 社の認証済み診断ライブラリと FMEDA を一緒に使う必要があります。

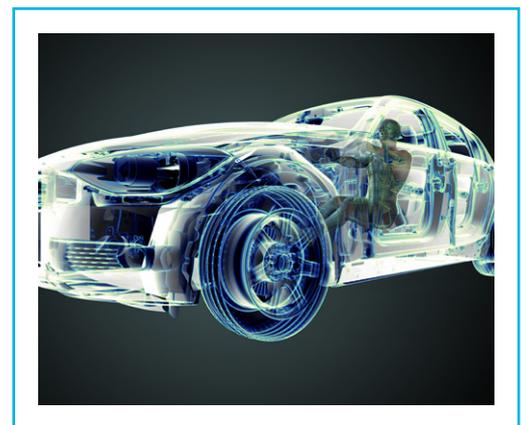
## FSM(機能安全マニュアル)

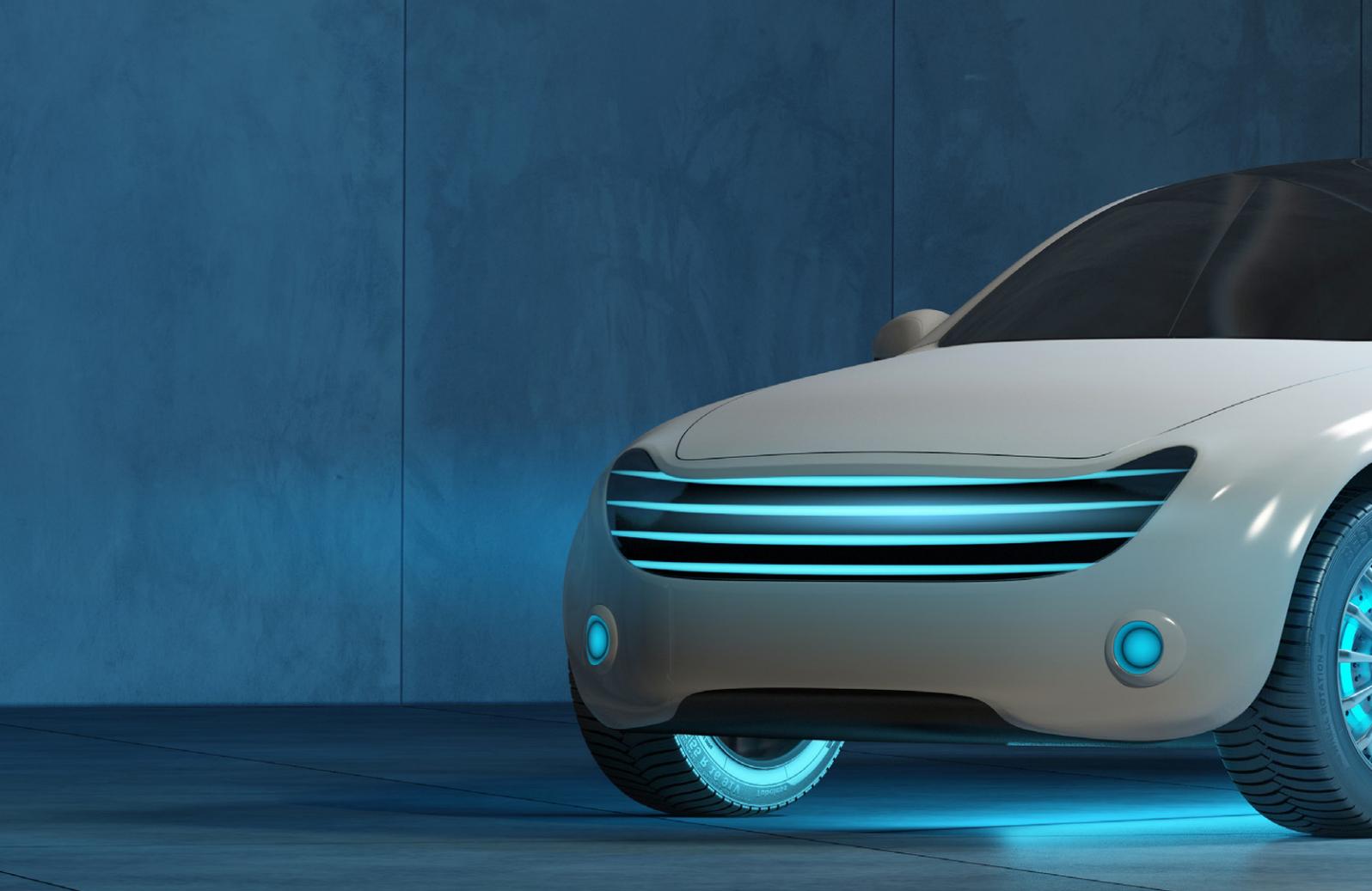
機能安全準拠/対応 dsPIC33C DSC に関する機能安全マニュアルには、FMEDA レポートに記載された故障検出方法の詳細とデバイスの安全動作に関する推奨事項が記載されています。FSM には従属故障と系統的故障を検出するためのハードウェア機能の説明が含まれ、これらは診断ライブラリの開発に役立ちます。

Note: ASIL-C の準拠には、ASIL デコンポジションにより Microchip 社の認証済み診断ライブラリと FSM を一緒に使う必要があります。

## 機能安全リファレンス アプリケーション

ISO 26262 機能安全規格に関する経験がなく FMEDA レポート、機能安全マニュアル、機能安全診断ライブラリ、新しいセーフティ クリティカル アプリケーションの関連ツールの使い方をこれから覚えようという場合、機能安全リファレンス アプリケーションが役に立ちます。このデータ監視リファレンス アプリケーションは dsPIC33CH512MP508 プラグイン モジュール (MA330046) を使った Explorer 16/32 開発ボード (DM240001-3) に実装されており、サンプルプロジェクトとして使うことができます。





## アプリケーションノート: 『ISO 26262 Functional Safety: Implementation of a Safety Element out of Context』 (AN3864)

この ISO 26262 機能安全アプリケーションノート (AN3864) では ISO 26262 安全規格の概念を紹介すると共に SEooC (Safety Element out of Context) の実装に焦点を当て、安全という視点から見たハードウェアとソフトウェアを取り扱っています。本アプリケーションノートは以下の点で役に立ちます。

- ISO 26262 規格の概要、特に SEooC に関する基本の理解を支援します。
- 機能安全リファレンス アプリケーションを使ったシステム開発の指針を提供します。
- ISO 26262 規格に準拠した開発に必要な手順と、準拠に必要な情報と成果物を示します。

### より高い安全レベルの達成

より高い安全レベルは、通常は冗長性によって達成されます。これは複数の dsPIC33 を使う事で実装できます。

例:

ASIL-C または ASIL-D では、ASIL デコンポジションにより複数の ASIL デバイス構成を利用可能です。

ASIL-C = ASIL-B(C) + ASIL-A(C)

ASIL-D = ASIL-B(D) + ASIL-B(D): ASIL-C または ASIL-D 安全目標は複数の DSC を組み合わせる事で達成できます。



## TÜV Rheinland 社認証済み機能安全診断ライブラリ

Microchip 社は、ランダムシステム故障を検出でき機能安全目標の達成を支援する機能安全ソフトウェア メカニズムを複数のモジュール \* に対して提供しています。

- フォルト条件でのシステム応答をテストするためのフォルト注入ルーチン
- 安全機能の要件、実現、検証の間の一貫性を追跡および達成するための静的および動的コード解析およびトレーサビリティレポート
- FMEDA と安全マニュアルで推奨された診断との緊密な統合
- 安全規格に対するライブラリの適合性を検証するためのテストベンチとプロジェクト ファイルをご要望に応じて提供

Note:

1. 機能安全フルパッケージの一部として診断ライブラリの最新版を提供します。この最新版は TÜV-Rheinland 社認証済みのものより新しい場合も、同じものである場合もあります。診断ライブラリの最新版は更新とバグ修正が含まれます。
2. \* サポートされるモジュールの一覧と ISO 26262 機能安全スタータ パッケージとフルパッケージのライブラリに含まれる診断機能の一覧は NDA の下で共有されます。
3. 認証済み診断ライブラリはデコンポジション手法により ASIL-C までの設計に使えます。





## 機能安全向けの開発エコシステム

Microchip 社は機能安全準拠/対応 dsPIC33 DSC に対応した TÜV SÜD 社認証済み設計ツールパッケージを提供し、ツール認定取得を支援します。MPLAB® XC16 コンパイラの機能安全ライセンスには ISO 26262 認定の開発環境に必要な全ての文書とレポートが含まれます。この文書パッケージには以下に示す TÜV SÜD 社の証明書、機能安全マニュアル、安全計画、ツール区分、弊社ツールの認定報告書が含まれます。

- TÜV SÜD 社認証済み MPLAB XC16 機能安全コンパイラ (SW006022-FS)
- MPLAB X IDE(統合開発環境)、MPLAB デバッガ/プログラマ、安全認定を容易にする関連文書
- MPLAB 解析ツールスイートのワークステーションライセンス (SW006027-2)

## サードパーティ ツールのサポート

LDRA (Liverpool Data Research Associates) ツールスイート等、ベンダーによるサードパーティ ツールをサポートしています。

詳細は [www.microchip.com/mplab-development-ecosystem-for-functional-safety](http://www.microchip.com/mplab-development-ecosystem-for-functional-safety) を参照してください。



## dsPIC33C DSC 用 ISO 26262 機能安全パッケージ

Microchip 社の dsPIC33C DSC 用 ISO 26262 機能安全パッケージを利用してセーフティクリティカルアプリケーションの設計を始めましょう。Microchip 社は以下を提供しています。

- **dsPIC33C DSC 用 ISO 26262 機能安全ベーシックパッケージ**：機能安全アプリケーションの設計を始めるための基本的なリソース
- **dsPIC33C DSC 用 ISO 26262 機能安全スタータパッケージ**：開発に必要な全ての手順を理解できるようにする事で、セーフティクリティカルアプリケーションの設計を支援
- **dsPIC33C DSC 用 ISO 26262 機能安全フルパッケージ**：初心者からベテランまで、セーフティクリティカルアプリケーションの設計と認定を支援するフルパッケージ
- **年次更新**：購入日から1年後に dsPIC33C DSC 用 ISO 26262 機能安全フルパッケージを更新できる年次更新パッケージ

dsPIC33C DSC 向け 機能安全ソリューション	ISO 26262 機能安全 ベーシック パッケージ	ISO 26262 機能安全 スタータ パッケージ	ISO 26262 機能安全 フルパッケージ
FMEDA レポート	✓	✓	✓
FSM(機能安全マニュアル)	✓	✓	✓
機能安全リファレンス アプリケーション - ソースコードとユーザーガイド	-	✓	✓
機能安全リファレンス アプリケーション ノート (AN3864)	-	✓	✓
機能安全診断概要文書	-	✓	✓
機能安全診断	-	ASIL-C 準拠診断ライブラリ と一部のモジュール*の ソースコード	ASIL-C 対応設計向けの TÜV Rheinland 社認証済み 診断ライブラリ (デコンポジションによる)。ライブラリには 一部のモジュール*について完全なソースコードを含む
診断ライブラリの FMEA と FSM	-	✓	✓
協調スケジューラ	-	✓	✓
診断ライブラリに対する TÜV- Rheinland 社証明書	-	-	✓
機能安全解析レポート	-	-	✓

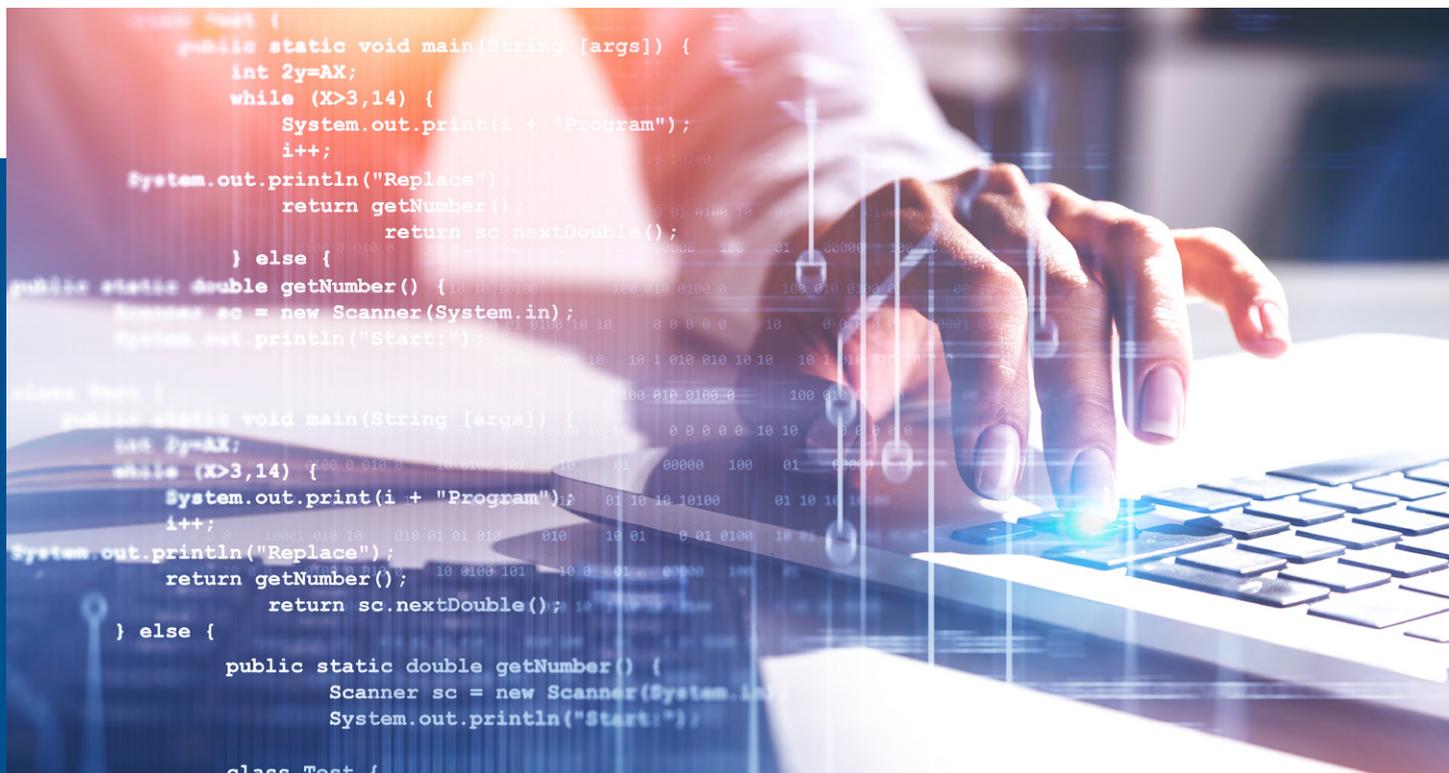
Note: ベーシックパッケージ、スタータパッケージ、フルパッケージ、年次更新、推奨開発ツールの詳細は Microchip 社正規代理店にお問い合わせください。スタータパッケージとフルパッケージは対応する機能安全コンパイラのバージョンに依存します。

\* サポートされるモジュールの一覧と ISO 26262 機能安全スタータ パッケージとフルパッケージのライブラリに含まれる診断機能の一覧は NDA の下で共有されます。



## ISO 26262 機能安全準拠/対応 dsPIC33 DSC – 対応状況

ISO 26262 機能安全準拠/ 対応 dsPIC33 DSC	説明	主なアプリケーション	FMEDA レポート	機能安全 マニュアル	診断ライブラリ
dsPIC33CH512MP508 (デュアルコア)	90 + 100 MHz、 最大 512 KB のフラッシュ AEC Q100 Grade 0 (150 °C)	高性能リアルタイム制御、 モータ制御、デジタル電源、 静電容量式センシング、 センサ インターフェイス、 計測制御	Now	Now	Now
dsPIC33CH128MP508 (デュアルコア)	90 + 100 MHz、 最大 128 KB のフラッシュ AEC Q100 Grade 0 (150 °C)		Now	Now	Future
dsPIC33CK1024MP710	100 MHz、最大 1024 KB のフラッシュ AEC Q100 Grade 0 (150 °C)		Now	Now	Now
dsPIC33CK512MPT608	100 MHz、最大 512 KB のフラッシュ AEC Q100 Grade 1 (125 °C) セキュア DSC		Now	Now	Now
dsPIC33CK512MP608	100 MHz、最大 512 KB のフラッシュ AEC Q100 Grade 0 (150 °C)		Now	Now	Now
dsPIC33CK256MP508	100 MHz、最大 256 KB のフラッシュ AEC Q100 Grade 0 (150 °C)		Now	Now	Now
dsPIC33CK64MP105	100 MHz、最大 64 KB のフラッシュ AEC Q100 Grade 0 (150 °C)		Now	Now	Now
dsPIC33CK256MC506	100 MHz、最大 256 KB のフラッシュ AEC Q100 Grade 0 (150 °C)	高性能リアルタイム制御、 モータ制御、 静電容量式センシング、 センサ インターフェイス、 計測制御	Now	Now	Now
dsPIC33CK64MC105	100 MHz、最大 64 KB のフラッシュ AEC Q100 Grade 0 (150 °C)		Now	Now	Now
dsPIC33EP128GS808 dsPIC33EP64GS506 dsPIC33EP32GS202	70 MHz、最大 128 KB のフラッシュ AEC Q100 Grade 1 (125 °C)	高性能リアルタイム制御、 デジタル電源、 センサ インターフェイス、 計測制御	Now	Now	-
dsPIC33EV256GM106 dsPIC33EV128GM106	70 MHz、5 V 最大 256 KB のフラッシュ AEC Q100 Grade 0 (150 °C)	5 V 高信頼性設計、モータ制御、 高性能リアルタイム制御、 静電容量式センシング、 センサ インターフェイス、 計測制御	Now	Now	-



詳細は [Microchip 社正規代理店](#) にお問い合わせください。

または [dsPIC33.functionalsafety@microchip.com](mailto:dsPIC33.functionalsafety@microchip.com) にお問い合わせください。





SMART | CONNECTED | SECURE

Microchip Technology Inc. | 2355 W. Chandler Blvd. | Chandler AZ, 85224-6199 | [microchip.com](http://microchip.com)