TASKING®

TASKING Compiler Qualification Kit
製品概要

概要

TASKING Compiler Qualification Kitは、開発部門がISO 26262などの安全規格に準拠している証明文書を提供します。このキットはソフトウェアツールの適格性検証の工程に対応し、TASKINGのツールセットが安全マニュアルどおりに使用された場合に、ASIL（自動車の安全要求レベル）で最も高いレベルであるASIL-Dにまで対応するセーフティクリティカルソフトウェアを開発できることを立証できます。

機能安全

機能安全規格であるISO 26262は、3,500kg未満の自動車に搭載される電気電子（E/E）システムを対象としています。自動車のOEMやサプライヤーは、この基準に準拠することが義務付けられていますが、それを証明するためには、規格に規定されるすべての条件が満たされていることを示す一連の証明書を作成する必要があります。

複雑なアプリケーションが増加するなか、「電気電子（E/E）システムの誤作動の原因となる不当なリスク因子が存在しないこと」と定義される機能安全は、特別な要件から当然の要件へとシフトしています。とはいえ、機能安全は今もなお複雑な問題で、ライフサイクルのすべての工程に影響を及ぼします。また、特殊なツールを導入して使用する必要もあるうえ、開発にかかる時間とコストも増加します。安全規格を厳格に遵守することは、安全に関する問題が発生したときに効果を発揮し、ISO 26262をはじめとする産業部門に固有の最新の安全規格に従ってシステム開発が行われた場合、通常は法的な説明責任が免除されます。

責務

E/Eシステムのサプライヤーには、認定を取得する義務があります。TASKINGのツールセットは、自動車、産業機器、鉄道、医療など、さまざまな市場で使用される安全関連のアプリケーションで長年にわたって利用されています。安全性が証明されるシステムの開発と認定を簡素化して加速させるために、TASKINGでは下記が提供されています。

- MISRAとCERTのガイドラインへの準拠を実証するための、コンパイラに組み込まれた静的コード解析機能
- Safety CheckerはASILの各レベルでソフトウェアの要素間のアクセスを検出
- ASPICE CL2に準拠する工程を用いて開発されたコンパイラ
- Safety Kitはツールセットの適格性に関して、信頼性のある書類を提供
- 安全マニュアルから逸脱したユースケースを修正し、認証取得をサポートするサービス

MISRAとCERTの静的コード解析

静的コード解析は、ソフトウェアのプログラムで考え得るすべての経路が正しく機能することを検証するために使用される手法です。ここでは、実際にプログラムを実行する必要はありません。この解析では、動的テストや相互評価で見落とされた不具合が効率的に検出されます。

European Motor Industry Software Reliability Association（MISRA）では、組み込みシステム向けのコードの安全性、セキュリティ、移植性、信頼性を確保するためのソフトウェア開発ガイドラインであるMISRA Cが策定されています。また、サイバー脅威に対処するために米国政府が設立したSoftware Engineering InstituteのCERT部門では、CERT Cコーディングスタンダードが策定されています。どちらの規格も、自動車、鉄道、航空宇宙、軍隊、医療など、さまざまな産業部門やアプリケーションで活用されています。

ISO 26262などの安全規格では、TASKING VXツールセットなどで提供されている静的解析の自動化ツールを使用して、MISRA CやCERT Cコーディングスタンダードへの違反を検出することが推奨されています。

SAFETY CHECKER

Safety Checkerでは、シングル/マルチコアのシステムのメモリに対するアクセス制限を設定することで、ASILの各レベルでソフトウェアの要素間のアクセスが自動的に検出されます。

これは、ASILが異なる複数の機能が1つのドメインコントローラーに統合される現在の自動車システムの設計において非常に重要になります。というのも、セーフティクリティカルでないソフトウェアのコンポーネントで発生したエラーが、セーフティクリティカルソフトウェアのコンポーネントで不具合を引き起こす恐れがあるからです。ISO 26262などの安全規格では、こうしたアクセスを確実に除外することが規定されています。Safety CheckerはASILの各レベルを認識する唯一の静的解析ツールで、アクセスの発生を確実に排除するための適切な解析を行うことができます。

最高レベルのASIL-Dについては、専用のハードウェアとメモリ保護ユニットを使用して、アクセス違反の発生を確実に排除することが規定されていますが、これについてはSafety Checkerが威力を発揮します。というのも、メモリ保護ユニットでは、システムの実行時に発生する干渉の影響が軽減されるのみで、顧客の手元にシステムがわたってから問題が発生する可能性がある一方、Safety Checkerではソフトウェアの構築時にアクセス違反が検出され、問題が発生する可能性が完全に排除されるからです。

ASPICE CL2に準拠する工程を用いて開発されたTASKINGツールセット

Automotive SPICE®（ASPICE）は、ソフトウェアの工程評価を対象とする国際規格のISO 15504から派生した成熟度モデルであり、工程の客観的な評価と改善に向けて準拠することがサプライヤーや（欧州の）自動車業界に義務付けられています。この規格は、米国やアジアで広く活用されているCMMIモデルに相当します。

TASKING VX Compilerは、ASPICE CL2に準拠する工程を用いて開発されています。このツールセットを使用すると、システムでの認証取得の簡素化と加速化が実現します。また、ASIL-Bまでのレベルについては、適格性に関して他の対応を行う必要はありません。

ID	工程	PA 1.1	PA 2.1	PA 2.2	CL（準拠レベル）
MAN.3	プロジェクト管理	F	F	F	2
ENG.4	ソフトウェア要件の解析	F	F	F	2
ENG.5	ソフトウェアの設計	F	F	F	2
ENG.6	ソフトウェアの構築	F	F	F	2
ENG.7	ソフトウェアの統合テスト	F	F	F	2
ENG.8	ソフトウェアのテスト	F	F	F	2
SUP.1	品質保証	F	F	F	2
SUP.8	構成管理	F	F	F	2
SUP.9	問題の解消	F	F	F	2
SUP.10	変更依頼管理	F	F	F	2

TASKINGの工程は、ASPICE CL2で評価されている（「F」は完全に達成されていることを示す）

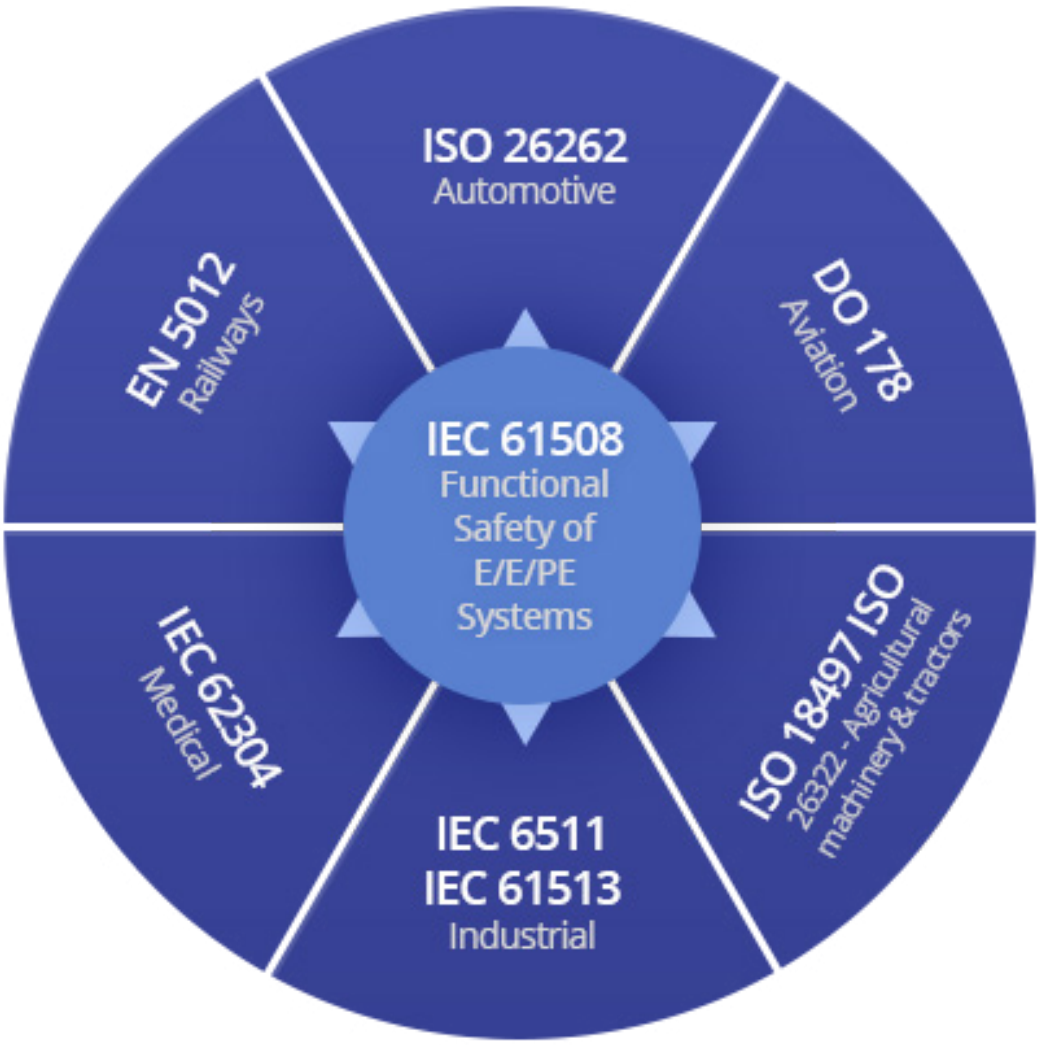
高いレベルのASILには、適格性に関する追加の証明が必要になりますが、これについてはTASKING Compiler Qualification Kitでサポートされています。

TASKING COMPILER QUALIFICATION KIT

TASKING Compiler Qualification Kitでは、コンパイラが安全マニュアルの記載どおりに使用された場合に、安全性に関連するソフトウェアをASIL-Dまでのレベルで開発できることを立証する証明文書が提供されます。Safety Kitには下記が含まれています。

- 安全性に関連する開発でのツールセットの使用方法についてのガイダンスが記載されているほか、低いレベルのASILに対応する「Evaluation of the tool development process（ツール開発工程の評価）」と高いレベルのASILに対応する「Validation of the software tool（ソフトウェアツールの検証」の検証方法を裏付ける証明が含まれた安全マニュアル
- TASKINGとユーザーから報告されたすべての既知の問題が含まれるTASKINGの障害レポートと対策のデータベースのすべての最新情報にアクセスするための権利
- 安全マニュアルに記載されているユースケースとは異なるツールを使用する場合に必要になる「Validation of the software（ソフトウェアツールの検証）」の実行に関するスクリプトと説明書

Safety Kitは、正式な認証を受ける必要があるセーフティクリティカルソフトウェアを開発する場合に役立ちます。このキットでは、コンパイラとその使用方法がシステムの安全要件を満たしていることを証明する文書が提供されます。



ISO 26262に準拠するTASKINGのサービス

これらのサービスは、ASIL-CとASIL-Dに対応する必要があり、**かつ**ツールの使用が安全マニュアルに記載されているユースケースと一致しないお客様に提供されています。

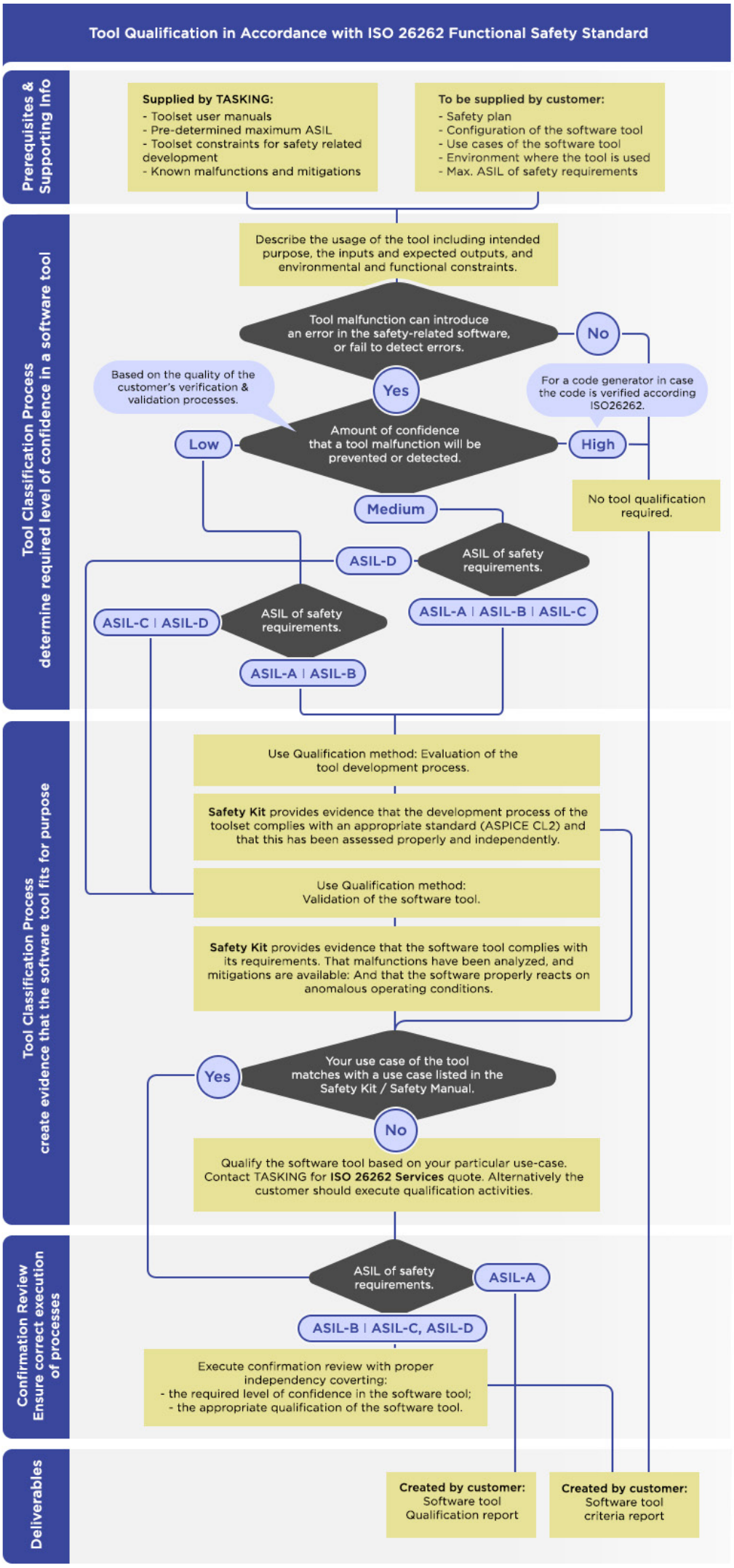
こうしたお客様には、自社でツールを検証していただくか、お客様のユースケースに基づいてTASKINGがSafety Kitを更新するかを選択していただけます。ISO 26262に準拠するTASKINGのサービスのメリットは下記のとおりです。

- 必要なコンパイラテストツールにコストをかける必要がありません。
- 必要なテストインフラストラクチャにかかるコストをカットする、またはゼロにすることができます。
- 必要なトレーニングにかかるコストをカットする、またはゼロにすることができます。
- 作業は、ツールに関して豊富な知識を備える専門家によって行われます。

対象となる規格

TASKING VX Compilerを使用することで、ISO 26262、EN 50128、ISO 25119に従って開発ツールの要件を満たすことができます。ツールセットは、安全関連の項目がそれぞれの要件に従って開発される限り、すべてのASILを対象に使用できます。

他の安全規格にも対応しているものの、現在のところSafety Kitの機能と他の規格の要件を相互に参照できる具体的な文書は作成されていません。


Tool Qualification in Accordance with ISO 26262 Functional Safety Standard
Prerequisites & Supporting Info
Supplied by TASKING:
- Toolset user manuals
- Pre-determined maximum ASIL
- Toolset constraints for safety related development
- Known malfunctions and mitigations
To be supplied by customer:
- Safety plan
- Configuration of the software tool
- Use cases of the software tool
- Environment where the tool is used
- Max. ASIL of safety requirements
Tool Classification Process
determine required level of confidence in a software tool
Describe the usage of the tool including intended purpose, the inputs and expected outputs, and environmental and functional constraints.
Tool malfunction can introduce an error in the safety-related software, or fail to detect errors.
No
Yes
Based on the quality of the customer's verification & validation processes.
For a code generator in case the code is verified according ISO26262.
Amount of confidence that a tool malfunction will be prevented or detected.
Low
High
Medium
No tool qualification required.
ASIL-D
ASIL of safety requirements.
ASIL-A | ASIL-B | ASIL-C
ASIL-C | ASIL-D
ASIL of safety requirements.
ASIL-A | ASIL-B
Tool Classification Process
create evidence that the software tool fits for purpose
Use Qualification method: Evaluation of the tool development process.
Safety Kit provides evidence that the development process of the toolset complies with an appropriate standard (ASPICE CL2) and that this has been assessed properly and independently.
Use Qualification method:
Validation of the software tool.
Safety Kit provides evidence that the software tool complies with its requirements. That malfunctions have been analyzed, and mitigations are available: And that the software properly reacts on anomalous operating conditions.
Yes
Your use case of the tool matches with a use case listed in the Safety Kit / Safety Manual.
No
Qualify the software tool based on your particular use-case. Contact TASKING for ISO 26262 Services quote. Alternatively the customer should execute qualification activities.
Confirmation Review
Ensure correct execution of processes
ASIL of safety requirements.
ASIL-A
ASIL-B | ASIL-C, ASIL-D
Execute confirmation review with proper independency coverting:
- the required level of confidence in the software tool;
- the appropriate qualification of the software tool.
Deliverables
Created by customer:
Software tool Qualification report
Created by customer:
Software tool criteria report