ISO 26262 Tool Qualification

ISO 26262 や IEC 61508 などの機能安全規格で要求されるプロセスの自動化に使用するソフトウェアツールは、その品質が安全性の観点から妥当であるかを利用者が検証し、認定することが求められます。開発対象の安全レベルとツールの用途に応じて認定方法を選定し、その活動の証拠を作成する必要があります。テストツールの場合は、TUV 等に事前に発行された資格証明書とレポートを利用できますが、最も厳しい安全レベルの場合は、ソフトウェアツールの妥当性確認をする必要があります。

ISO 26262-8.11：ソフトウェアツールの使用に対する信頼性

システムの開発に使用されるソフトウェアツールが、ISO 26262 で要求されるアクティビティとタスクをサポートする場合、以下の目標を効果的に達成するという確信が必要です。

a）ツールの誤動作に起因する誤った出力による、開発された製品の決定論的原因故障のリスクが最小限に抑えられる。
b）ISO 26262 で要求されるアクティビティやタスクが使用するツールの正しい動作に依存する場合、ISO 26262 への準拠に関して開発プロセスは適切である。

このようなソフトウェアツールの使用に対する信頼性は、次の基準で評価されます。

・ソフトウェアツールの誤動作とそれによる誤出力により、開発中の安全関連項目または要素にエラーを発生させる、あるいはエラーの検出ができない可能性がある（Tool Impact）
・誤動作による誤出力を防止あるいは検出する手段の信頼性（Tool error Detection）

評価は、ツールの役割、ツールの障害に関連するリスク、開発アイテムまたは要素の最大 ASIL に依存します。そしてユーザー固有の環境下で、ツールの開発時に意図された用途で、適正に使用されることを確認します。以下、ツールの信頼レベルと ASIL に応じて求められるツール認定について紹介します。

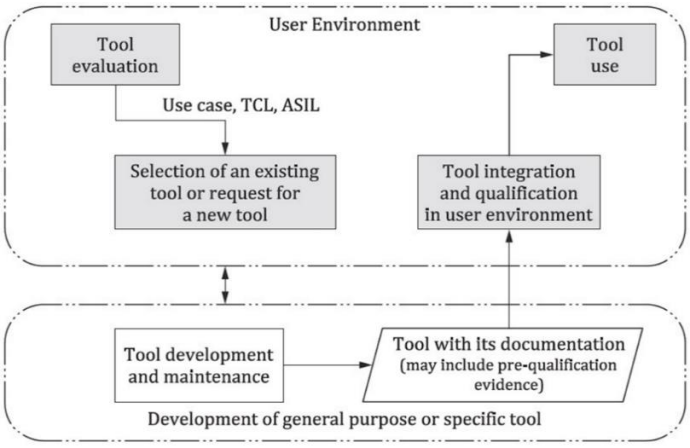


Figure 3 - Overview of Tool Confidence activities

ツール信頼レベルについて

ソフトウェアツールの使用に対する信頼性を示す**ツール信頼レベル（Tool Confidence Level：TCL）**が、**ツールの影響（Tool Impact）**と**ツールエラー検出（Tool Error Detection）**から、次の表にしたがって決定されます。

Table 3 - Determination of the tool confidence level (TCL)

		Tool Error Detection		
		TD1	**TD2**	**TD3**
Tool Impact	TI1	TCL1	TCL1	TCL1
	TI2	TCL1	TCL2	TCL3

ツールの影響（Tool Impact：TI）は、特定のソフトウェアツールの使用目的を分析および評価して、その誤動作が、開発中の安全関連アイテムまたは要素にエラーを導入することや、エラーの検出に失敗する可能性を判断します。TI1 は、そのような可能性がないと主張される場合に選択され、それ以外の場合は TI2 が選択されます。

TI1 に属するツールの例

- ➢ 要件管理ツール、ソースコード管理ツール、課題トラッカー

TI2 に属するツールの例

- ➢ コードジェネレータ　エラーを導入しないことを保証できない
- ➢ コンパイラ　エラーを導入しないことを保証できない
- ➢ 静的解析ツール　エラーを導入しないが、エラーの検出に失敗しないことを保証できない
- ➢ テストツール　エラーを導入しないが、エラーの検出に失敗しないことを保証できない

ツールエラー検出（Tool Error Detection：TD）は、ソフトウェアツールの誤動作に伴う誤った出力を生成するのを防ぐ対策、または誤動作に伴って誤った出力を生成したことを検出する対策の信頼性を以下のクラスに分類します。これはツールを使用するユーザーが認証機関と協議して決定しますが、一般に商用ツールは TD1、TD2 のいずれかです。そして新規に採用する場合や、同じツールでも環境やユースケースが異なるなら TD2 に分類されます。

- ➢ **TD1**：誤動作とそれに伴う誤った出力が防止または検出される高い信頼レベル
- ➢ **TD2**：誤動作とそれに伴う誤った出力が防止または検出される中程度の信頼レベル
- ➢ **TD3**：TD1、２以外。通常、開発プロセスに利用可能な体系的な対策がない場合に適用され、ソフトウェアツールの誤動作とそれに伴う誤った出力は、ランダムにしか検出できない

➢ TD1 を選択する場合、使用するソフトウェアツールに対する高い信頼性を示す必要があります。

- 特定のプロジェクト環境に適用されるユースケースを特定して文書化する
- 特定のプロジェクト環境で使用されるツールの特定の機能に適用されるユースケース
- ツールの運用要件（Tool Operational Requirements=TOR）を定義する必要がある
- ツールの運用要件からテストケースを実装する
- ツールに適切なテストケースを適用する
- ツールが必要なすべての TOR を満たしていることを実証するために、テスト結果を確認および文書化する

➢ TD2 が TI2 のツールに選択される場合、ツール信頼レベルは TCL2 になります。

- TCL2 の場合、下表により ASIL のレベルに応じてツールの使用に対する信頼性を示す必要がある
- 1a と 1b は、ASIL A、ASIL B、ASIL C に強く推奨される（+：推奨、++：強く推奨）

Table 5 - Qualification of software tools classified TCL2

Methods		ASIL			
		A	B	C	D
1a	Increased confidence from use in accordance with 11.4.7	++	++	++	+
1b	Evaluation of the tool development process in accordance with 11.4.8	++	++	++	+
1c	Validation of the software tool in accordance with 11.4.9	+	+	+	++
1d	Development in accordance with a safety standard[a]	+	+	+	+

➢ TD3 が TI2 のツールに選択される場合、ツール信頼レベルは TCL3 になります。

- TCL3 の場合、下表により ASIL のレベルに応じてツールの使用に対する信頼性を示す必要がある
- 1a と 1b は ASIL A と ASIL B に強く推奨される
- 1c および 1d は ASIL C および ASIL D に強く推奨される

Table 4 - Qualification of software tools classified TCL3

Methods		ASIL			
		A	B	C	D
1a	Increased confidence from use in accordance with 11.4.7	++	++	+	+
1b	Evaluation of the tool development process in accordance with 11.4.8	++	++	+	+
1c	Validation of the software tool in accordance with 11.4.9	+	+	++	++
1d	Development in accordance with a safety standard[a]	+	+	++	++

1a：11.4.7 に従った使用による信頼性の増加

- 以前認定されたツールを再利用するなど、使用実績による信頼性の向上
  - ・同じ目的/環境/バージョン/構成/回避策/ユースケース/機能的制約/プロセス等
  - ・変更が生じた場合は、それが影響しないことを正当化する必要がある
- エラーと誤動作の情報は体系的に蓄積されていること
- 使用実績がない場合、ツールベンダーは「ツール認定サポートパッケージ」としてデータを提供できる

1b：11.4.8 に従ったツール開発プロセスの評価

- ソフトウェアツールの開発に適用された開発プロセスは、適切な基準に準拠している必要がある
- 国際標準などに基づく評価
- ツールベンダーは、証明書と関連するテストレポートを提供する必要がある

1c：11.4.9 に従ったソフトウェアツールの妥当性確認

- ASIL D に強く推奨
- 検証プロセスは、ソフトウェアツールがその運用要件を備えることを実証する必要がある
- 誤動作やエラーを分析し、それらを回避または検出するための対策を講じる必要がある
- 異常な動作条件に対するソフトウェアツールの動作を調査する必要がある
- ツールベンダーは、要件、テスト計画、テストケース（ユースケース）、およびレポートを含むツール認定サポートパッケージを提供できる

1d：安全規格に従った開発

- ISO 26262-8:2011 – ASIL D に強く推奨されていた
- ISO 26262-8:2018 – 現在推奨されている
- ツールベンダーが提供できる

テストツールの Tool Qualification について

ツール認定は、ツールの使用に関する所定のまたは想定される情報に基づいて実行されます。

➢ 例： ユースケース、ユーザー要件、TCL、ASIL

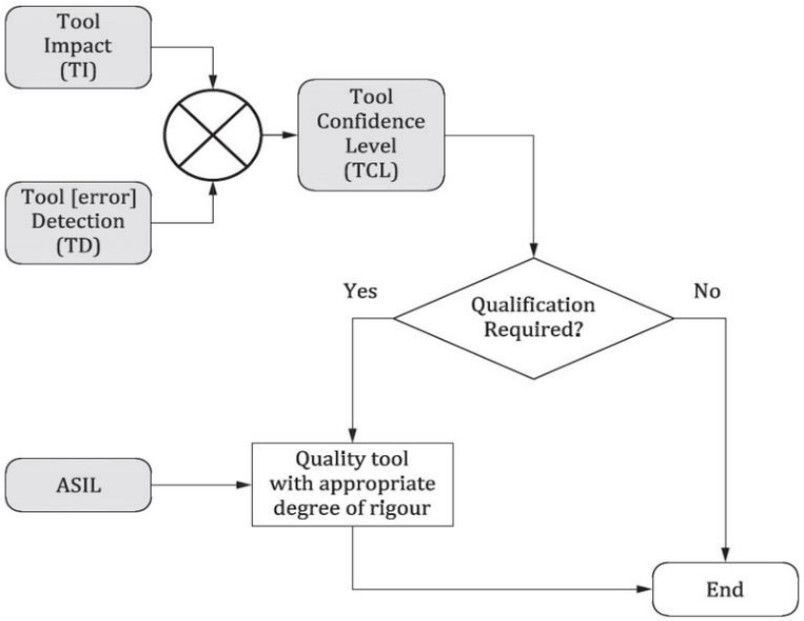


Figure 4 - Tool evaluation and qualification flow

Figure 4 の手順にしたがって、LDRA テストツールを使用する場合の例を説明します。

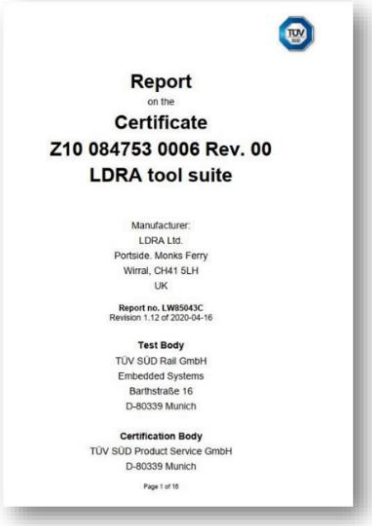
Tool Impact (TI)：LDRA のテストツールは TI2 に分類されます。

- TUV SUD レポートでは、「4.4 ツール分類」セクションにこれが記載される
- TD はツールを使用するユーザーが認定機関と協議して決定する

> The tool impact for the LDRA tool suite is TI2, because a verification tool can fail to detect existing errors in the source code to be analysed although it may not introduce errors into an application.
>
> TI2 requires an estimation of the tool error detection TD on customer side.

➢ TD2 を選択する場合

- アプリケーションが ASIL A、ASIL B、ASIL C の場合は、LDRA のツール資格証明書とレポートを認証目的に使用できます。



- アプリケーションが ASIL D の場合は、11.4.9 に従ったソフトウェアツールの妥当性確認をする必要があります。LDRA は、それをサポートするツール認定サポートパッケージを提供します。

Table 5 - Qualification of software tools classified TCL2

Methods		ASIL			
		A	B	C	D
1a	Increased confidence from use in accordance with 11.4.7	++	++	++	+
1b	Evaluation of the tool development process in accordance with 11.4.8	++	++	++	+
1c	Validation of the software tool in accordance with 11.4.9	+	+	+	++
1d	Development in accordance with a safety standard[a]	+	+	+	+

➢ TD1 を選択する場合

- ソフトウェアツールに対する高い信頼性を示す必要があります。(p.2)

LDRA は、それをサポートするツール認定サポートパッケージを提供します。

TD3 の選択について

LDRA 社テストの開発プロセスでは、すべての体系的な対策に従っており、ツール内にランダムな障害はなく、ツールに関する既知の問題または制限が文書化されています。そして障害がランダムになることは決してなく、TD3 は通常適用されません。もし、TD3 を選択する場合、そうするための適切な正当化が必要です。

LDRA のツール認定パッケージについて

LDRA のツール認定パッケージは、開発プロジェクトに固有の環境（コンパイラ/ IDE、ホスト/シミュレータ/ターゲット）で実行した結果をツール認定レポートに入力して、ツールの妥当性を証明します。

- 以下の機能をツール認定サポートパッケージ（Tool Qualification Support Pack：TQSP）でサポート
  - プログラミングルールチェック
  - 構造カバレッジ分析
  - ダイナミックデータフローカバレッジ
  - アセンブラカバレッジ分析
  - 単体テスト/ローレベルテスト

- ツール認定パッケージには、ツールの使用例とドキュメントが含まれます
  - ツール基準評価レポート（Tool Criteria Evaluation Report =TCER）ドキュメント
    - ツールの資格分析(Tool Qualification Analysis)
    - ツール認定(Tool Qualification)
    - 実行される活動
    - ツール認定データ
  - ツール検証計画（TVP）ドキュメント
    - 計画フェーズの活動
    - ツール検証アクティビティ
    - ツール認定レポートアクティビティ
  - ツール運用要件（TOR）ドキュメント
    - 通常の動作条件
    - ツールの操作要件
  - ツール認定レポート（TQR）ドキュメント
    - ツール構成の識別
    - インストールレポート
    - 認定試験結果
    - TOR カバレッジマトリックス
    - ツールのステータス
    - コンプライアンスステートメント

LDRA TQSP Documents

Sl.no.	Document	Source	Description
1	TCER： Tool Criteria Evaluation Report	LDRA	この LDRA 提供のツール基準評価レポートは、TVP の指示に従って、サプライヤー/カスタマーによってカスタマイズされます。この TCER には、ツールとそのアーキテクチャの説明、求められる認定資格の詳細、実行するツール認定アクティビティの識別、作成するツール認定データの要約が含まれています。
2	TOR： Tool Operational Requirements	LDRA	LDRA ツールの運用要件は、この TCER に基づく資格の対象となる運用要件を識別します。サプライヤー/顧客は、TCER および SVR で認定される特定の要件を特定する必要があります。
3	TVP： Tool Verification Plan	LDRA	ツール検証計画は、LDRA ツールスイートの検証用に LDRA が提供する説明用スクリプトです。TVP は TVCP を参照して、各 TOR に関連付けられたテストケースを識別します。
4	TVCP： Tool Verification Cases and Procedures	LDRA	LDRA が提供するツール検証のケースと手順には、すべてのソースコード、ソースコードに対して実行されるテストケース、および LDRA ツールスイートのインストールの検証に使用する期待される結果が含まれています。サプライヤー/顧客は、TVCP に含まれるテストケースが、プロジェクトで使用されているすべてのソースコード構成要素をカバーするのに十分であることを確認する責任があります。
5	TVR： Tool Verification Results	Project	ツール検証結果は、インストール環境でテストソースコードに対して TVCP を実行することによって生成された実際の結果です。これらの実際の結果は、TVCP に含まれている期待される結果と比較され、ツールが通常の動作条件下で適切に動作していることが示されます。
6	TQR： Tool Qualification Report	LDRA	LDRA が提供するソフトウェアツール認定レポートは、TVP に含まれる指示に従ってサプライヤー/顧客によってカスタマイズされ、ツール検証の結果を要約します。これにより、プロジェクトで定義されたプロセス内での LDRA ツールスイートの認定を受け入れるために必要なデータを証明機関に提供します。 このドキュメントは、通常の動作条件下での認定ツールの正しい動作を示すための主要なデータです。

Tool qualification objective matrix

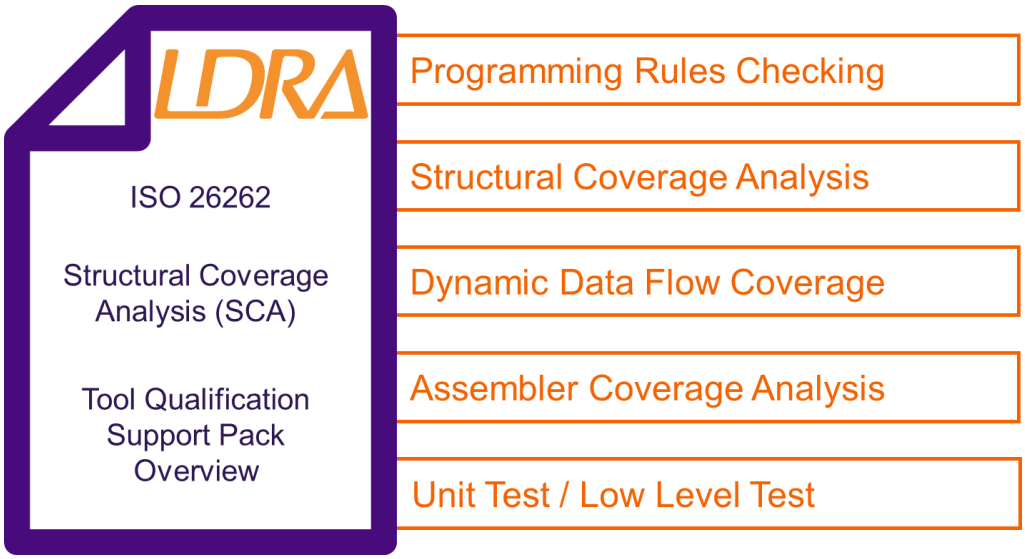
SN	Part No	Section Number	Description	Document / Life Cycle Data Reference	Section Number	Verified	Comment
1	ISO 26262 Part 8	11.4.3	コンプライアンスチェック	TCER		✓	
2		11.4.4	ソフトウェアツール使用の計画	SVP, TCER, TVP		✓	
3		11.4.4.1(a),(b) and (d)	ツールの特定、環境、設定	TCER, TVP, TQR		✓	
4		11.4.4.1(c)	ユースケース	TCER, TOR		✓	
5		11.4.4.2(a)	ツールの特徴と機能	TCER, TVP		✓	
6		11.4.4.2(b)	ユーザーマニュアル	TVP		✓	
7		11.4.4.2(d),(e) and (c)	異常状態、故障（検出と予防を含む）	TCER, TOR		✓	
8		11.4.5	ツール評価	TCER		✓	
9		11.4.6	ツール認定	TCER		✓	
10		11.4.2	ツールの信頼レベルと認定の妥当性チェック	TCER		✓	
11		11.4.9	ソフトウェアツールの妥当性確認	TCER, TVP, TVCP, TVR		✓	
12		11.4.9.2	テストケースと手順	TVCP		✓	
13		11.4.9.2	テスト検証結果	TVR		✓	
14		11.4.10	確認レビュー	TCER, TQR		✓	
15		11.5.1	ソフトウェアツール基準評価レポート	TCER		✓	
16		11.5.2	ソフトウェアツール認定レポート	TQR		✓	
17	ISO 26262 Part 6	9.4.5 Table 12 and 9.4.6	ソフトウェア単体レベルとテスト環境での構造カバレッジメトリック	TCER, TVP, TVCP, TVR, TQR		✓	
18	ISO 26262 Part 2	6.4.7 Table 1	ソフトウェアツール基準評価レポートとソフトウェアツール認定レポートの確認レビュー	レビュー記録		✓	
19		6.4.7 Table 1	項目とプロジェクトマネジメントの開発者に関する独立性 I1：確認は異なる担当者によって行わねばならない	レビュー記録		✓	

まとめ

- TD の選択に基づいて、TCL を導出できる
- ASIL D の場合、ソフトウェアツールの検証を実行する必要がある
- LDRA ツールスイート認定の場合：
  - TD1 で ASIL A から ASIL D：
    - ツール認定のユースケースをプロジェクト環境で実行できる
  - TD2 で ASIL A から ASIL C：
    - TUV レポートと TUV 証明書で十分
  - TD2 で ASIL D：
    - ツール認定のユースケースをプロジェクト環境で実行できる
  - TD3 は LDRA ツールスイートには適用されない

LDRA Solution - Tool Qualification

- 規制当局に広く認められている 20 年以上のツール認定の血統
- ツール認定パッケージ：プログラミングルールチェック、構造カバレッジ分析、
  ダイナミックデータフローカバレッジ、アセンブラカバレッジ分析、単体テスト/ローレベルテスト
- LDRA TQSP は、ツール認定プロセスを完全にサポートし、ツール認定の負担を軽減する



FUJI SETSUBI

富士設備工業株式会社 電子機器事業部　www.fuji-setsu.co.jp