DO-330 ソフトウェアツール認定に関する考慮事項: いつ、どこで、どのように適用されるか

DO-330 Software tool qualification considerations: When, where, and how it applies

https://ldra.com/do-330/

今日の複雑でセーフティクリティカルなシステムは、自動化と効率化のためのツールに依存しています。ツール認定により、開発に使用されるツールが、それらによって発生する可能性のある障害やエラーに関連するリスクに見合った程度まで信頼できることが保証されます。DO-330/ED-215 は、ソフトウェア開発を含む、ソフトウェアツールが関与するすべてのセーフティクリティカルな開発活動に関連します。

DO-330/ED-215 は主に、DO-178C/ED-12C および DO-278A/ED-209 に代表される民間航空規格をサポートするための技術補遺として作成されました。ただし、「自動車、宇宙、システム、電子ハードウェア、航空データベース、安全性評価プロセスなどの他の分野でも使用される可能性がある」とも主張しています。

RTCA DO-330 および EUROCAE ED-215 とは何ですか?

RTCA DO-330 と EUROCAE ED-215 は事実上同じ文書であり、RTCA/EUROCAE 合同委員会によって共同執筆されました。DO-330/ED-215 は、DO-178B を DO-178C に置き換えたときに導入された 4 つの技術補遺 (または DO-200 を含む 5 つ) のうちの 1 つです。

DO-330 の「ソフトウェアツール認定に関する考慮事項(Software Tool Qualification Considerations)」には、次のように記載されています。「ソフトウェアツールは、他のソフトウェアの開発、検証、制御を支援するために、多様なドメインで広く使用されています。 … 例としては、自動コードジェネレーター、コンパイラ、テストツール、変更管理ツールなどがあります。この文書では、ツールを認定するためのプロセスと目標について説明します。」

DO-330/ED-215 は、ドメインに依存しないスタンドアロンの文書です。DO-178C がリリースされる前は、DO-178C で説明されている目標は DO-178 文書の不可欠な部分として含まれていました。現在の形式では、DO-330/ED-215 は、航空分野での DO-178C/ED-12C、DO-278/ED-109、DO-254/ED-80、および DO-200 のサポートとしてだけでなく、その他のセーフティクリティカルなドメインでの使用も想定されています。

DO-330 はなぜ開発されたのですか？

この文書によると、DO-330/ED-215 の開発の動機は以下の3つでした。

- ツール開発者とツールユーザーにツール固有のガイダンスを提供する
- アプリケーションソフトウェアではなくツールに特化した文書を提供し、「混乱と誤解」を回避する
- 航空機搭載および地上のソフトウェアシステム、および潜在的には「自動車、宇宙、システム、電子ハードウェア、航空データベース、安全性評価プロセスなどの他の領域」にガイダンスを提供する

DO-330 に関連する他の規格やガイダンス文書は何ですか?

DO-330 and DO-178C

DO-178C/ED-12C「航空機搭載システムおよび機器の認証におけるソフトウェアの考慮事項(Software Considerations in Airborne Systems and Equipment Certification)」は、すべての商用ソフトウェアベースの航空宇宙システムを承認するために、認証機関(FAA, EASA, TCCA, ANAC…) によって参照される主要な文書です。これは、民間航空機アプリケーションのソフトウェアシステムの正確性と堅牢性を確保するために、ソフトウェアライフサイクル全体をカバーする正式なプロセス規格です。

DO-178C §12.2.3 には、「各ツール認定レベルに必要な目標、ガイダンス、およびライフサイクルは、DO-330/ED-215「ソフトウェアツール認定に関する考慮事項 (Software Tool Qualification Considerations) 」に記載されています」とあります。

DO-330 and DO-278A

DO-278A/ED-190A「通信、ナビゲーション、監視および航空交通管理 (CNS/ATM) システムのソフトウェア完全性保証に関する考慮事項(Software Integrity Assurance Considerations for Communication, Navigation, Surveillance and Air Traffic Management (CNS/ATM) Systems) 」は、DO-178C/ED-12C の姉妹文書であり、CNS/ATM アプリケーション用のソフトウェアシステムの正確性と堅牢性を確保するために同様の原則に準拠しています。

DO-278A §12.2.3 には、「各ツール認定レベルに必要な目標、ガイダンス、およびライフサイクルは、DO-330「ソフトウェアツール認定に関する考慮事項(Software Tool Qualification Considerations)」に記載されています」 とあります。

DO-330 and DO-254

DO-254/ED-80 「航空機搭載電子ハードウェアの設計保証ガイダンス(Design Assurance Guidance for Airborne Electronic Hardware)」では、DO-330/ED-215 に記載されている原則を、ハードウェアの設計と開発をサポートするために使用されるソフトウェアツールに適用することを要求しています。

DO-330 and DO-200A

DO-200A「航空データ処理規格(Standards for Processing Aeronautical Data)」は、品質保証や QMS など、航空データの処理に適用されるデータ処理のすべての段階の最小要件を規定しています。DO-200A は、これらのプロセスのサポートに使用されるソフトウェアツールの前提条件として DO-330/ED-215 の適用を挙げています。

DO-330 and DO-331

DO-331/ED-216 「モデルベースの開発と検証(Model Based Development and Verification)」では、モデルベースデザインを使用する場合に適用される、DO-178C に記載されている原則の調整について説明しています。

DO-331/ED-216 は DO-330/ED-215 と同様、DO-178B を DO-178C に置き換えたときに導入された技術補遺の 1 つです。ただし、DO-331/ED-216 は航空以外の分野には適用されません。

DO-330 and DO-332

DO-332/ED-217「オブジェクト指向技術および関連技術(Object Oriented Technology and related technologies)」には、オブジェクト指向プログラミングおよび補完的な実践に適用できる追加の目標とアドバイスが含まれています。DO-332/ED-217 は DO-330/ED-215 と同様、 DO-178B を DO-178C に置き換えたときに導入された技術補遺の 1 つですが、航空以外の分野には適用されません。

DO-330 and DO-333

DO-333/ED-218「DO-178C および DO-278A に対する形式手法の補遺 (Formal Methods Supplement to DO-178C and DO-278A)」では、準拠アプリケーションにおける形式手法の使用に関連する追加の目標とアドバイスが特定されています。DO-330/ED-215 と同様、DO-333/ED-218 は DO-178B を DO-178C に置き換えたときに導入された技術補遺の 1 つですが、航空以外の分野には適用されません。

ツール認定とは何ですか?

ツール認定とは、ツールのエラーがシステムの安全性に影響を与えるリスクが許容できるほど低い(エラーが少ない、または安全性に影響を与えることがない)ことを保証するために設計されたプロセスを表す一般的な用語です。多くの規格では、ツールの用途とツールが導入される環境を考慮して、ツール認定を達成するためのプロセスが定義されています。

アプリケーションに関する考慮事項は、潜在的なエラーが回避または検出されるような方法でツールが使用されることを保証するように設計されています。環境の観点では、インストールされたツールに対して、ツールとその使用に対する確信と信頼を構築して、そのツールが貢献する広範なツールチェーンの一部として機能することを保証します。

ツール認定には、1 つ以上の規格で推奨されている 4 つの主要なアプローチがあります。

- 使用実績による証明
- ツール開発プロセスの評価
- 安全規格に沿った開発
- ツール検証

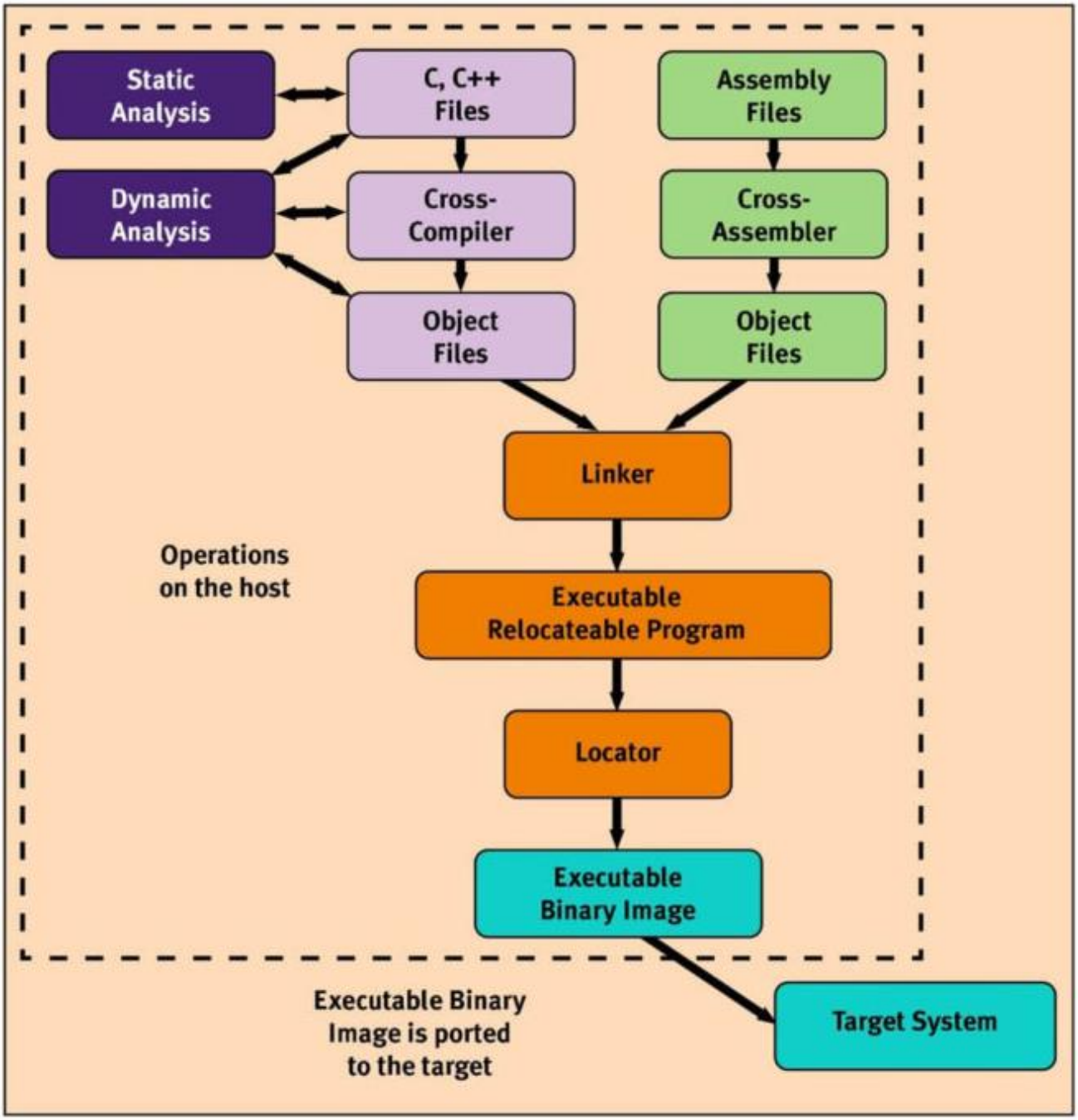
DO-330 に関係するのはツール検証のみです。

ツール検証とは何ですか?

ツールの検証は、ツール認定のための最も徹底的なアプローチですが、最も時間がかかります。これは民間航空プロジェクトに許可されている唯一のアプローチであり、DO-330/ED-215 で議論されている唯一のアプローチです。他の分野の最もクリティカルなアプリケーションでも、これが唯一実行可能なアプローチであることがよくあります。

ツールの各機能は、ツールが導入される環境を使用して解析され、結果が文書化されます (多くの場合、ベンダー検証スイートを使用します)。

静的解析の場合、これは、エンディアンや整数のサイズなどの機能が正しく構成されていることを確認することを意味します。動的解析には、ターゲット上でインスツルメントされたコードの構築と実行が含まれるため、ツールチェーンへの依存度が高くなります (下図)。



製品の安全性に影響を与える可能性のあるこれらの機能での潜在的なエラーは、プロセス内で検出または回避される確率を決定するためにさらに評価されます。

DO-330 は民間航空用途にどのように適用されますか?

DO-330/ED-215 は民間航空以外の分野にも適用できるように書かれていますが、その主な焦点は依然として民間航空です。この規格で説明されている原則は新しいものではありませんが、DO-178C バージョンの登場に伴い、DO-178 から分離されました。したがって、民間航空アプリケーションでの使用は十分に証明されており、DO-330/ED-215 はその分野の専門家にとって馴染みのある用語で構成されています。

DO-330 では、ツール開発者が実行するツール認定アクティビティがいくつか定義されていますが、ツールがアプリケーションにとって適切で十分な信頼性があることを示す主たる責任はツールのユーザーにあります。詳細については、こちらをご覧ください。

DO-330 は他の安全性が重要な分野のアプリケーションにどのように適用されますか?

民間航空分野以外のセーフティクリティカルアプリケーションの多くでは、ツール認定に対する要求がそれほど厳しくないアプローチの 1 つが活用されており、多くの場合、許容可能な評価の証拠を引用し、それを達成するために TÜV から事前認証を受けたツールを活用しています。ただし、ほとんどの機能安全規格では、最もクリティカルなアプリケーションクラスのツール検証レベルの認定が必要です。

これらの機能安全規格 (IEC 61508、EN 50128、IEC 62304 など) の多くは、何を行う必要があるのかについて詳しく説明していません。このような場合に DO-330 の原則を適用することは、その空白に対処する 1 つの方法です。

一部の DO-330 ツール認定アクティビティは、ツール開発者が実行する必要があります。ただし、アプリケーションの重要性を考慮して、ツールが適切で十分に信頼できることを示す主たる責任はツールのユーザーにあります。詳細については、こちらをご覧ください。

DO-330 ツール認定レベルとは何ですか?

ツール認定は、DO-330/ED-215「ソフトウェアツールの認定に関する考慮事項(Software Tool Qualification Considerations)」に記載されているように、航空機搭載システムおよび機器の認証プロセスの重要な部分です。DO-330/ED-215 では、次の 3 つの基準に従って割り当てられるツール認定レベル (TQL) の概念が導入されています。

Criterion 1

出力が航空機搭載ソフトウェアの一部であるため、エラーが挿入される可能性があるツール

Criterion 2

検証プロセスを自動化するため、エラーの検出に失敗する可能性があり、その出力が以下の排除または削減を正当化するために使用されるツール:

1. ツールによって自動化されたもの以外の検証プロセス、または
2. 航空機搭載ソフトウェアに影響を与える可能性のある開発プロセス。

Criterion 3

意図された用途の範囲内で、エラーの検出に失敗する可能性があるツール。

したがって、認定されていないコンパイラや、UML ツールからの自動コードジェネレーターは、Criterion 1 に適合します。同じ UML ツールの認定バージョンは、コード検証プロセスのオーバーヘッドを削減するように設計されているため、Criterion 2 に適合します。LDRA ツールスイートは検証ツールであり、Criterion 3 のツールです。

アプリケーションのソフトウェアレベル (DO-178C の場合は、設計保証レベル(Design Assurance Level) DAL を参照) に関係なく、このような検証ツールには、下記 5 つのレベルの中で最も要求の少ないツール認定レベル 5 が常に割り当てられます。

Software Level (DAL)	Criterion 1	Criterion 2	Criterion 3
A	TQL-1	TQL-4	TQL-5
B	TQL-2	TQL-4	TQL-5
C	TQL-3	TQL-5	TQL-5
D	TQL-4	TQL-5	TQL-5

民間航空認証局は、プロジェクトごとにツールの認定を要求します。ツールの適合性を示す責任は、民間航空アプリケーションを開発する組織にあります。ただし、ベンダーが提供するツール認定サポートパック (Tool Qualification Support Pack: TQSP) を利用することはできます。

ツール認定サポートパック（ツール認定キット）を使用した DO-330 認定

DO-330/ED-215 の条件では、すべてのプロジェクトにツールの認定が必要です。TÜV や同様の認証は、DO-330/ED-215 が適用されるプロジェクトとは関係ありません。

多くのベンダーは、期待される結果とレポートプロセスや、テストケースを含む文書を提供しています。通常、ツール認定キット(Tool Qualification Kit) または ツール認定サポートパック として知られるこれらの成果物は、ツールが展開されるツールチェーン内で正しい結果を提供するようにツールが適切に構成されているかどうかを示すために使用できます。

LDRA ツールスイートを例にとると、DO-330/ED-215 ツール認定サポートパック (TQSP) は 次の 5 つのサブパックで構成されており、それぞれが関連する開発プロジェクトの「運用要件」として指定できます。

- コーディング規約チェック
- 構造カバレッジ解析
- データ結合と制御結合解析
- アセンブラコードレベルカバレッジ解析
- 単体テスト/ローレベルテスト

TQSP には、検証プロセスを通じてユーザーをガイドするように設計された 4 つの主要な文書が含まれています。これらの文書によって定義されたプロセスにより、証拠となる成果物の作成と、規格に適した形式で調査結果を要約するように設計されたレポートの編集が保証されます。

その 4 つのドキュメントは以下のとおりです。

ツール検証計画 (Tool Verification Plan：TVP)

アプリケーションに適した構成のために LDRA が提供するツール検証計画には、ソースコード、テストケース、および期待される結果が含まれており、関連するインストール環境でのツールの有効性を検証するために使用します。

ツール達成概要 (Tool Accomplishment Summary：TAS)

LDRA は、TVP の指示に従ってユーザーがカスタマイズできるように、汎用のツール達成概要(Tool Accomplishment Summary)を提供します。TAS は、ツールとそのアーキテクチャを説明し、ツールチェーンとそれが動作するその他の環境条件を詳細にし、PRC および TVP 文書に関連する実施結果を提供します。DO-330/ED-215 TQSP で提供されている LDRA ツール達成概要からの抜粋を以下に示します。

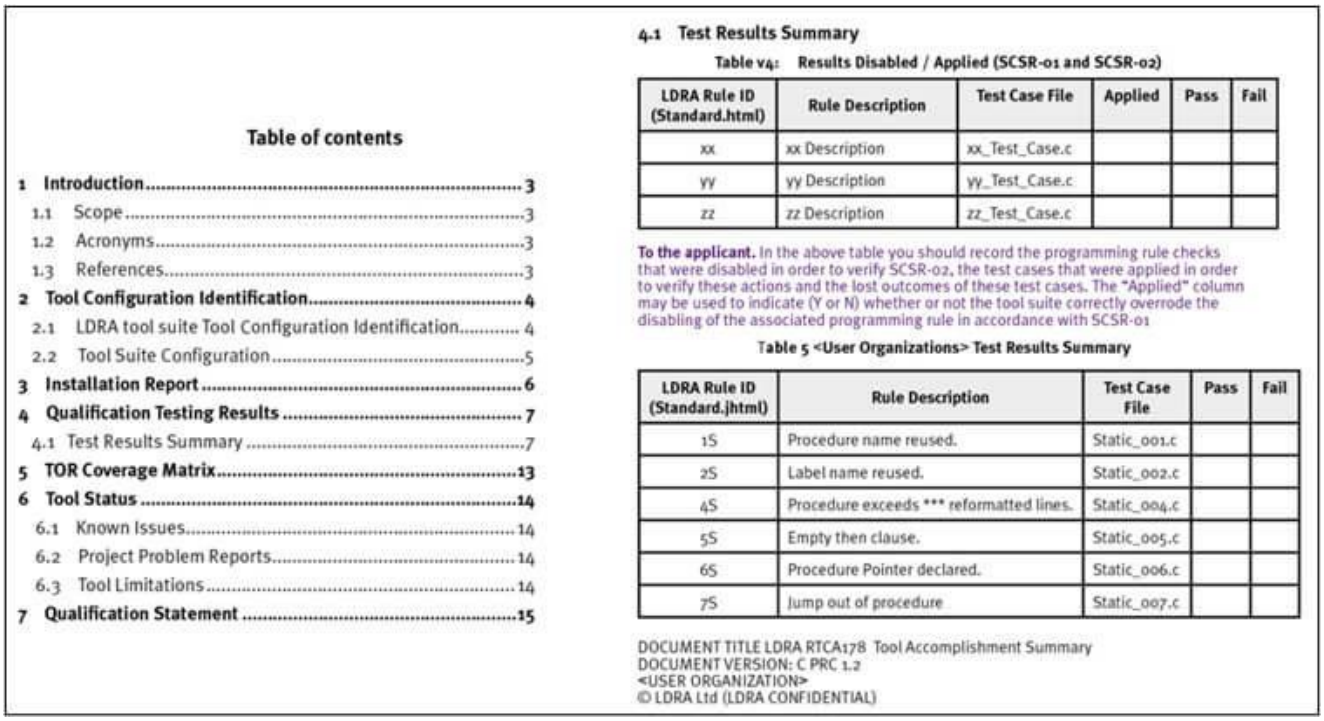


Table of contents

4.1 Test Results Summary

Table v4: Results Disabled / Applied (SCSR-01 and SCSR-02)

LDRA Rule ID (Standard.html)	Rule Description	Test Case File	Applied	Pass	Fail
xx	xx Description	xx_Test_Case.c			
yy	yy Description	yy_Test_Case.c			
zz	zz Description	zz_Test_Case.c			

To the applicant. In the above table you should record the programming rule checks that were disabled in order to verify SCSR-02, the test cases that were applied in order to verify these actions and the lost outcomes of these test cases. The "Applied" column may be used to indicate (Y or N) whether or not the tool suite correctly overrode the disabling of the associated programming rule in accordance with SCSR-01

Table 5 <User Organizations> Test Results Summary

LDRA Rule ID (Standard.jhtml)	Rule Description	Test Case File	Pass	Fail
1S	Procedure name reused.	Static_001.c		
2S	Label name reused.	Static_002.c		
4S	Procedure exceeds *** reformatted lines.	Static_004.c		
5S	Empty then clause.	Static_005.c		
6S	Procedure Pointer declared.	Static_006.c		
7S	Jump out of procedure	Static_007.c		

DOCUMENT TITLE LDRA RTCA178 Tool Accomplishment Summary
DOCUMENT VERSION: C PRC 1.2
<USER ORGANIZATION>
© LDRA Ltd (LDRA CONFIDENTIAL)

ツールの運用要件 (Tool Operational Requirement：TOR)

ツールが RTCA DO-330 / EUROCAE ED-215 に従って認定されるためには、ツールの運用要件 (TOR) を定義する必要があります。準拠を達成するには、TOR は検証可能で一貫性があり、ツールの機能とその結果として得られる出力がツールによって置き換えられるアクティビティに対応していることを示すのに十分な詳細が含まれている必要があります。TQSP の一部として提供される TOR の文書テンプレートからの抜粋を以下に示します。

3 Tool Operational Requirements

3.1 Application of specified Coding Standars and Rules

[SCSR-02] If the coding standard model is selected to be applied as a whole, LDRA tool suite *shall* only apply, and report against, the subset of the available programming rules checks indicated in section 3.1.1 of this TOR

[SCSR-02] LDRA tool suite *shall* apply all of the programming standard rule checks indicated as applicable in section 3.1.1 of this TOR irrespective of whether any of these checks have been disabled in the CPEN.DAT file that is being applied at the time of the analysis

The selection of additional rules, external to the selected coding standard, is addressed in section 3.1.2 of this TOR.

3.1.1 Coding Standard Rules

[CSR-0.1] LDRA tool suite *shall* apply each <User Organization> rule below.

LDRA Rule ID (Standard.html)	Rule Description	Test Case File
1 S	Procedure name reused.	Static_001.c
2 S	Label name reused.	Static_002.c
4 S	Procedure exceeds *** reformatted lines.	Static_004.c
5 S	Empty then clause.	Static_005.c
6 S	Procedure pointer declared.	Static_006.c
7 S	Jump out of procedure.	Static_007.c
8 S	Empty else clause	Static_008.c
9 S	Assignment operation in expression	Static_009.c
11 S	No brackets to loop body (added by LDRA tool suite).	Static_011.c
12 S	No brackets to then/else (added by LDRA tool suite).	Static_012.c
13 S	goto detected.	Static_013.c
20 S	Parameter not declared explicitly.	Static_020.c

ツール認定プラン (Tool Qualification Plan TQP)

ツール認定計画文書には、ツール検証計画 (下記) で特定されたプロジェクト固有の情報が含まれています。DO-330 は通常、航空アプリケーション開発に適用され、その場合、ソフトウェア認証計画 (Plan for Software Aspects of Certification：PSAC) で指定されているすべての要件も取り込まれます。

7 Tool Qualification Data to be Produced

The following tool qualification data will be produced or otherwise used under this TQP

Item	ID	Source	Description	CC	Submit
1	PSAC	Project	The Plan for Software Aspects of Certification is the primary means used by the certification authority for determining whether an applicant is proposing a software life cycle that is commensurate with the rigour required for the level of software being developed. The PSAC is required to contain specific information regarding the intent to qualify the LDRA tool suite, and should reference this TQP. The PSAC should identify the specific certification credit sought, which may be identified by reference to specific sections in the TQP.	CC1	Yes
2	TQP	LDRA①	This LDRA provided Tool Qualification Plan is customised by the applicant in accordance with the instructions in the TVP for the LDRA tool suite. This TQP contains a description of the tool and its architecture, details of the certification credit sought, identifies the tool qualification activities to be performed, and summarises the tool qualification data to be produced.	CC1	Yes
3	TOR	LDRA	The LDRA Tool Operational Requirements identifies the operational requirements eligible for qualification under this TQP. The applicant should identify the specific requirements being qualified in the TAS and SAS. As the TOR is referenced by submitted data, it should be controlled as CC1 data by the applicant.	CC1	Avail
4	TVP	LDRA	The Tool Verification Plan is an LDRA provided instructional script for verification of the LDRA tool suite. The TVP refers to the TVCP to identify the test cases associated with each TOR. The applicant should be prepared to provide this document to the certification authority upon request.	CC2	Avail

結論

DO-330/ED-215「ソフトウェアツール認定に関する考慮事項」は、民間航空プロジェクトに推奨されるソフトウェアツール認定の原則を説明する自己完結型の文書です。DO-178C のリリース前は、これらの原則は DO-178 の不可欠な部分として説明されていました。

DO-330/ED-215 は、当時リリースされた 4 つの補遺のうちの 1 つですが、航空分野での DO-178C/ED12C、DO-278/ED-109、DO-254/ED-80、DO-200 のサポートだけでなく、他のセーフティクリティカルな分野での使用も意図しているという点でユニークです。

追加情報

DO-330 PDFs – free download

Technical briefing – DO-330 test tool qualification for aerospace applications
Technical briefing – Leveraging DO-330 and ISO 26262 tool verification techniques for developments compliant with other functional safety standards
Technical white paper – Test tool qualification for functional safety

DO-330 – further information

Certification and Regulatory Support page
LDRA Resource Centre

FUJI SETSUBI

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

www.ldra.com
LDRA
LDRA UK & Worldwide
Portside, Monks Ferry,
Wirral, CH41 5LH
Tel: +44 (0)151 649 9300
e-mail: info@ldra.com

LDRA Technology Inc.
2540 King Arthur Blvd, Suite 228,
Lewisville, Texas 75056
United States
Tel: +1 (855) 855 5372
e-mail: info@ldra.com

LDRA Technology Pvt. Ltd.
Unit No B-3, 3rd Floor Tower B,
Golden Enclave, HAL Airport Road,
Bengaluru
560017
India
Tel: +91 80 4080 8707
e-mail: india@ldra.com