LDRA tool suite®
IEC 61508 に対するテスト支援機能

Implementing IEC 61508 with the LDRA tool suite®

Prof. M. A. Hennell Technical Director LDRA Ltd

www.ldra.com

Introduction

IEC 61508 は、電気・電子・プログラマブル電子部品で構成される安全関連システムに対する国際規格である。これはアプリケーション領域ごとの標準を用意するためのフレームワークとして、独立した標準を意図している。

この資料では、LDRA ツールスイートにより寄与できる、IEC 61508 スタンダードの要件を紹介する。IEC 61508 スタンダードには、多数の表がある:

- Annex A 技法、手段に関する選択指針
- Annex B ソフトウエアライフサイクルの各フェーズの検証活動に適切な手法のリスト
- Annex C この資料の対象外

この資料では、各表の要件を満たすために、LDRA ツールスイートを活用する方法について解説する。そして各表内の要件を満たす LDRA ツールスイートの機能について、簡単に説明する。

参考までに各表にある列 'ref' は、スタンダードの別部分への参照であり、この資料内では直接関係しないが、解り易くするために残している。表内の R、HR、NRは、推奨、強く推奨、推奨しないの意味。--- 箇所は、助言無し。スタンダードに準拠するうえで、推奨される手法を取らない場合は、その根拠・理由が求められる。もし HR されている手法であれば、より強い理由が必要となる。この資料では、LDRA ツールスイートにより少ないコストで各手法が提供されること、そしてこれらの採用・不採用に関わる論争・課題を軽減できることを紹介する。

障害検出手法の選択をする場合、次の点に留意すると良い。一般に静的解析手法はテクニカルな障害（言語上の欠陥、配列境界エラー、ありがちなプログラミング上の誤り、ゼロ割、などに起因するもの）を検出し、アプリケーションの障害は動的テストとその解析、一部のフォーマルメソッド（形式手法）など、要件に基づいた手法により検出される。

この資料中フォーマルメソッド（形式手法）とは、数学を基盤とした手法であり定義済みの意味論をベースとするもの。

The Annex A Tables

以下、スタンダードから各表を引用し、LDRA ツールスイートで該当する機能を説明する。各表内の列は、それらの番号で参照する。

Table A.1 – Software safety requirements specification

Technique/Measure	Ref.	SIL1	SIL2	SIL3	SIL4
1 Computer-aided specification tools	B.2.4	R	R	HR	HR
2a Semi-formal methods	Table B.7	R	R	HR	HR
2b Formal methods including for example,CCS, CSP, HOL, LOTOS, OBJ, temporal logic, VDM and Z	C.2.4		R	R	HR

TBreq （LDRA ツールの要件トレーサビリティ機能）は、記載されたソフトウエアの要件に対し、トレーサビリティ技術を用いて、テストケースやコードとの関連を取ることから、項１に該当する。

安全要求を満たすテストデータを生成させる方法次第で、それは TBrun （LDRA ツール の自動ユニットテスト機能）と相まって、項 2a, 2b に該当する。既にサードパーティの提供するフォーマルメソッド（形式手法）を基盤としたテストベクタ生成ツールが、TBrun に統合されている。

Table A.2 – Software design and development: software architecture design

Technique/Measure	Ref	SIL1	SIL2	SIL3	SIL4
1 Fault detection and diagnosis	C.3.1		R	HR	HR
2 Error detecting and correcting codes	C.3.2	R	R	R	HR
3a Failure assertion programming	C.3.3	R	R	R	HR
3b Safety bag techniques	C.3.4		R	R	R
3c Diverse programming	C.3.5	R	R	R	HR
3d Recovery block	C.3.6	R	R	R	R
3e Backward recovery	C.3.7	R	R	R	R
3f Forward recovery	C.3.8	R	R	R	R
3g Re-try fault recovery mechanisms	C.3.9	R	R	R	HR
3h Memorising executed cases	C.3.10		R	R	HR
4 Graceful degradation	C.3.11	R	R	HR	HR
5 Artificial intelligence - fault correction	C.3.12		NR	NR	NR
6 Dynamic reconfiguration	C.3.13		NR	NR	NR

7a Structured methods including for example, JSD, MASCOT, SADT and Yourdon	C.2.1	HR	HR	HR	HR
7b Semi-formal methods	Table B.7	R	R	HR	HR
7c Formal methods including for example, CCS, CSP, HOL, LOTOS, OBJ, temporal logic, VDM and Z	C.2.4		R	R	HR
8 Computer-aided specification tools	B.2.4	R	R	HR	HR

このテーブルはデザイン構造についてのリストであるが、LDRA ツールスイートで寄与できる部分がある。例えば項 3h は、TBrun の TCF の仕組みでカバーされ、またシステムが構造化されていること（項 7a）をツールで確認できる。TBreq は項 8 に相当な貢献ができる。LDRA ツールスイートを用いて、デザインを基に生成されたコードを解析して、関連する欠陥がソフトウエア内で起こり得ないことから、アーキテクチャ上の特定機能に対する要件が存在しないことを証明する。C++の全ての例外が処理されることのチェック､全てのファイル I/O 動作が正常であることのチェック、下限境界に欠陥のある配列が存在しないことのチェック（C, C++）、そして殆どの配列に対して上限境界の欠陥の検出など。

Table A.3 – Software design and development: Support tools and programming language

Technique/Measure	**Ref**	**SIL1**	**SIL2**	**SIL3**	**SIL4**
1 Suitable programming language	C.4.6	HR	HR	HR	HR
2 Strongly typed programming language	C.4.1	HR	HR	HR	HR
3 Language subset	C.4.2			HR	HR
4a Certificated tools	C.4.3	R	HR	HR	HR
4b Tools: increased confidence from use	C.4.4	HR	HR	HR	HR
5a Certificated translator	C.4.3	R	HR	HR	HR
5b Translator: increased confidence from use	C.4.4	HR	HR	HR	HR
6 Library of trusted/verified software modules and components	C.4.5	R	HR	HR	HR

LDRA ツールスイートを用いて、C のような強い型付けではない言語を、強い型付けに格上げすることができる（項 2）。そして適正なサブセット使用（項 3）の施行を強化する。

LDRA ツールスイートは認証可能（certifiable）である（DO-178B の用語では qualified ）（項 4）。航空電子システムの標準である DO-178B に認証された、非常に多くの実績がある。

ツールの使用による自動化の結果、コードの品質への信頼性が大いに増大する。TBreq により提供されるトレーサビリティにより、ソフトウエアの再利用、インパクト解析が促進される。

TBrun で行えるオブジェクトコードレベルの検証は、ソースコードとオブジェクトが構造的にも機能的にも一致することを確認する。これは認証されていないコンパイラや、他のツールチェインのコンポーネント、などの問題に対する標準的なソリューションである。

ここでは殆ど全てのレベルで HR が求められているので、SIL のレベルに対する考察はそれほど重要ではない。また、他の項目の追加にかかるコストも大きくはならない。

Table A.4 – Software design and development: detailed design

Technique/Measure	**Ref**	**SIL1**	**SIL2**	**SIL3**	**SIL4**
1a Structured methods including for example, JSD, MASCOT, SADT and Yourdon	C.2.1	HR	HR	HR	HR
1b Semi-formal methods	Table B.7	R	HR	HR	HR
1c Formal methods including for example, CCS, CSP, HOL, LOTOS, OBJ, temporal logic, VDM and Z	C.2.4		R	R	HR
2 Computer-aided design tools	B.3.5	R	R	HR	HR
3 Defensive programming	C.2.5		R	HR	HR
4 Modular approach	Table B.9	HR	HR	HR	HR
5 Design and coding standards	Table B.1	R	HR	HR	HR
6 Structured programming	C.2.7	HR	HR	HR	HR
7 Use of trusted/verified software modules and components (if available)	C.2.10 C.4.5	R	HR	HR	HR

項 2 は TBreq で、コンピュータ支援デザインツールの成果物に対するトレーサビリティを提供できる。

項 3 は、TBvision （LDRA のプログラミングスタンダードのレポート機能）と、公開済みのスタンダード、あるいはユーザ個々に規定された、ディフェンシブなプログラミングの履行によりサポートされる。項 4 は、プロシジャ、及びファイルの視野に立った適正なメトリクスによって満たされ得る。不適切、あるいは過度のモジュール化は、メトリクスから判定される。項 5 は、TBvision を用いてソースコードに対するデザインとコーディングスタンダードを実施することで満たされる。

項 6 は、SPV(the Structured Programming Verification) 機能で確認できる。実証済みのコンポーネントの利用（項 7）は、それらコンポーネントが LDRA ツールの機能で十分に検証済みであれば正当化できる。デザインの品質の一部はコードレベルに遡って検証できる。ファイルハンドリング、インターフェイスの検証、構造化の確認、複雑度解析など。この場合もやはり、SIL のレベルは LDRA ツールスイートの適用には関与しない。なぜなら得られる効果によってかかるコストに大差が無いため。

Table A.5 – Software design and development: software module testing and integration

Technique/Measure	**Ref**	**SIL1**	**SIL2**	**SIL3**	**SIL4**
1 Probabilistic testing	C.5.1		R	R	HR
2 Dynamic analysis and testing	B.6.5 Table B.2	R	HR	HR	HR
3 Data recording and analysis	C.5.2	HR	HR	HR	HR
4 Functional and black box testing	B.5.1 B.5.2 Table B.3	HR	HR	HR	HR
5 Performance testing	C.5.20 Table B.6	R	R	HR	HR
6 Interface testing	C.5.3	R	R	HR	HR

項 1 は、TBreq と TBextreme によるデータ駆動型テスト選出手法の統合を TBrun 環境で実行させることで満たされる。

項 2 は、LDRA Testbed のコアなる機能でカバーされる。LDRA ツールスイートは、ステートメントカバレッジ、ブランチ/デシジョンカバレッジ、LCSAJ カバレッジ、データフロー、MC/DC カバレッジをサポートしている。動的な解析は、アプリケーション障害の検出に非常に効果的である。

項 3 は、全てのテストに関わる情報を記録する LDRA ツールスイートの TCF ファイルにて満たされる。このファイルはテストのプロセスを実行する中で自動生成され、認証期間に対する記録となるようにデザインされている。

項 4 は、LDRA ツールスイートの動的解析機能と、TBreq を介してマップ（トレーサビリティ）されたコンポーネントとそのプロシジャに対して、実施されるファンクショナルテストにより満たされる。

項 5 パフォーマンステストは、TBrun とパフォーマンス・インスツルメントの仕組みによって満たされる。インターフェイスのテストは、データフロー解析か、TBrun のホスト環境でのテストによって実現される。

項 6 は、フォーマルメソッド（形式手法）のアルゴリズムで、宣言されたインターフェイスと実際のインターフェイスの一致を確かめることでカバーされる。

動的テストのカバレッジ解析のレベルは SIL のレベルに応じて選択される。SIL のレベルに関わらず、ブランチ/デシジョンレベルのテストが、産業界で標準的に採用されている。MC/DC、LCSAJ レベルのテストで更なる障害が検出されうるので、高いレベルの SIL では考慮に入れるべき。

Table A.6 – Programmable electronics integration (hardware and software)

Technique/Measure	**Ref**	**SIL1**	**SIL2**	**SIL3**	**SIL4**
1 Functional and black box testing	B.5.1 B.5.2 Table B.3	HR	HR	HR	HR
2 Performance testing	C.5.20 Table B.6	R	R	HR	HR

項 1 は、TBrun から機能テストやブラックボックステストなど、様々なターゲットテスト実行とその動的解析によりカバーされる。さらに TBreq を介してマップ（トレーサビリティ）されたコンポーネントとそのプロシジャに対して、実施されるファンクショナルテストにより満たされる。

項 2 パフォーマンステストは、TBrun とパフォーマンス・インスツルメントの仕組みによって満たされる。インターフェイスのテストは、データフロー解析か、TBrun のターゲット環境でのテストによって実現される。

SIL のレベルに応じたカバレッジレベルの達成が求められる。

Table A.7 – Software safety validation

Technique/Measure	Ref	SIL1	SIL2	SIL3	SIL4
1 Probabilistic testing	C.5.1		R	R	HR
2 Simulation/modelling	Table B.5	R	R	HR	HR
3 Functional and black-box testing	B.5.1 B.5.2 Table B.3	HR	R	R	R

TBrun によるターゲットのテスト実行と、適正に生成されるテストデータにより項 1、2 はカバーされる。

項 2 には、LDRA によるコントロールフローモデリング、データフローモデリングから、システムが望ましい特性であることの確認もできる。

項 3 は、TBrun の様々な動的解析を機能テストやブラックボックステストへの使用で持たされる。さらに項 3 は、TBreq を介してマップ（トレーサビリティ）されたコンポーネントとそのプロシジャに対して、実施されるファンクショナルテストにより満たされる。

SIL のレベルに応じた、満たされるべきカバレッジのレベルがある。

Table A.8 – Modification

Technique/Measure	Ref	SIL1	SIL2	SIL3	SIL4
1 Impact analysis	C.5.23	R	R	R	R
2 Reverify changed software module	C.5.23	R	R	R	R
3 Reverify affected software modules	C.5.23	R	HR	HR	R
4 Revalidate complete system	C.5.23		R	HR	HR
5 Software configuration management	C.5.24	HR	HR	HR	HR
6 Data recording and analysis	C.5.2	HR	HR	HR	HR

一般に項 1 から 5 は、TBreq を介してマップ（トレーサビリティ）されたコンポーネントとそのプロシジャに対して、実施されるファンクショナルテストにより満たされる。更に、TBevolve （コード変更によるインパクトを観測できる LDRA ツールの機能）は、TBrun のリグレッションテスト機

能と相まって、項 1 に対応する。LDRA Testbed をプロジェクトに対して用いることで、全ての機能バージョンの比較対照となる、最初のベースラインを形成できる。

TBrun により再検証プロセスは全体的に支援され実施できる。リグレッションテストのプロセス全体が TBrun により完全に自動化される。LDRA ツールスイートにより生成されるクロスリファレンスは、影響を受けるモジュールに適応できる。また、LDRA ツールスイートと構成管理ツールの統合により、項 5 を満たすことが簡素化できる。項 6 データの記録と解析は、TBrun と TCF ファイルにより執り行える。再検証活動のコストは深刻な課題であるが、ここでも TBrun による自動化の支援によってこれらコストを飛躍的に軽減できる。これらコストは、SIL のレベルを問わない。

Table A.9 – Software verification

Technique/Measure	**Ref**	**SIL1**	**SIL2**	**SIL3**	**SIL4**
1 Formal proof	C.5.13		R	R	HR
2 Probabilistic testing	C.5.1		R	R	HR
3 Static analysis	B.6.4 Table B.8	R	HR	HR	HR
4 Dynamic analysis and testing	B.6.5 Table B.2	R	HR	HR	HR
5 Software complexity metrics	C.5.14	R	R	R	R

項 1 は、ツールに組込まれているフォーマルメソッド（形式手法）によって満たされる。12 種もの数学を基盤としたアルゴリズムでシステムや、その一部に特定の障害が無いことを証明する（I/O の障害、変数用法の障害など、）

項 2 は、テストデータ生成アルゴリズムと TBrun によって満たされる。項 3 は、LDRA ツールスイートにより包括的に実施できる。項 4 の動的テストとその解析も、同様である。また LDAR ツールスイートは、多くのソフトウエア複雑性のメトリクスを生成できる（項 5）。そして複雑度解析結果を統合した全体像、各種品質特性を管理者が把握できるので、プロジェクト管理が支援される。

項 1, 3, 5 の実施コストは、全 SIL のレベルで変わらない。そして相対的に少ないコストで済み、高い効果が期待できる。項 4 は、実施されるべきカバレッジ解析のレベルの選択が必要。

Table A.10 – Functional safety assessment

Assessment/Technique	Ref	SIL1	SIL2	SIL3	SIL4
1 Checklists	B.2.5	R	R	R	R
2 Decision/truth tables	C.6.1	R	R	R	R
3 Software complexity metrics	C.5.14	R	R	R	R
4 Failure analysis	Table B.4		R	HR	HR
5 Common cause failure analysis of diverse software (if diverse software is actually used)	C.6.3		R	HR	HR
6 Reliability block diagram	C.6.5	R	R	R	R

ツールにより非常に多くの安全性、保全性に関するチェックが行われ、クオリティレポートに表示される（項 1）。そしてツールでチェックできない面に限って、人によるチェックを実施する。項 2 decision/truth テーブルは、MC/DC や、LCSAJ テストケースプランナーにより生成される。クオリティレポートは、複雑度に関する多くの側面のメトリクスを生成する。項 4, 5, 6 は、LDRA ツールスイートでは満たされない。

The Annex B Tables

Table B.1 – Design and coding standards

Technique/Measure*	Ref	SIL1	SIL2	SIL3	SIL4
1 Use of coding standard	C.2.6.2	HR	HR	HR	HR
2 No dynamic objects	C.2.6.3	R	HR	HR	HR
3a No dynamic variables	C.2.6.3		R	HR	HR
3b Online checking of the installation of dynamic variables	C.2.6.4		R	HR	HR
4 Limited use of interrupts	C.2.6.5	R	R	HR	HR
5 Limited use of pointers	C.2.6.6		R	HR	HR
6 Limited use of recursion	C.2.6.7		R	HR	HR
7 No unconditional jumps in programs in higher level Languages	C.2.6.2	R	HR	HR	HR

デザインとコーディングスタンダードの項 1 は、LDRA ツールスイートで完全に満たされる。LDRA ツールスイートでは広く業界で採用される多数のプログラミングスタンダードをサポートしているので、それらを補完させることで追加のチェックとなる。詳細情報は、www.ldra.com/standards.asp

ダイナミックオブジェクトの使用は、包括的に検出可能（項 2）。

動的変数の使用は検出可能で（項 3）、適切な初期化が実装されているかの検証するチェックが実施される。動的変数のインストールのオンラインチェック（項 3b）は、フォーマルメソッド（形式手法）の機能により正しく格納されることを確認できる。

インタラプト・ハンドラの使用は検出し、レポートできる（項 4）。ポインタの使用とそれに関わる障害はレポートされる（項 5）。再起呼出の使用は、個別プロシジャ、複数プロシジャともにレポートされる（項 6）。goto などの使用により生じる条件無しジャンプはレポートされる（項 7）。このテーブルに該当する、全ての LDRA ツールスイートの解析機能は、その基本解析の一環として得られるので、SIL のレベルに関わることは無い。

Table B.2 – Dynamic analysis and testing

Technique/Measure	**Ref**	**SIL1**	**SIL2**	**SIL3**	**SIL4**
1 Test case execution from boundary value analysis	C.5.4	R	HR	HR	HR
2 Test case execution from error guessing	C.5.5	R	R	R	R
3 Test case execution from error seeding	C.5.6		R	R	R
4 Performance modelling	C.5.20	R	R	R	HR
5 Equivalence classes and input partition testing	C.5.7	R	R	R	HR
6 Structure-based testing	C.5.8	R	R	HR	HR

項 1 は TBrun により実行されカバレッジ解析により支援される。項 2 は、潜在する障害を判定はできないが、TBrun により支援される。

項 3 は、TBrun で対処できる。オリジナルのプロシジャーとエラーを含むプロシジャーに対し、エラーを露呈するテストデータを実行することで。項 4 は、パフォーマンスプロファイルを生成するためにインスツルメンテーションが利用できる。

項 5 は、特定のテストデータ生成アルゴリズムで得られる。構造化ベースのテストは、動的解析の標準的な機能で満たされる。項 6 は、LDRA ツールスイートの動的解析の標準的な機能で満たされる。SIL のレベルに応じた、カバレッジ測定のレベル選択がある。

Table B.3 – Functional and black-box testing

Technique/Measure	**Ref**	**SIL1**	**SIL2**	**SIL3**	**SIL4**
1 Test case execution from cause consequence diagrams	B.6.6.2			R	R
2 Prototyping/animation	C.5.17			R	R
3 Boundary value analysis	C.5.4	R	HR	HR	HR
4 Equivalence classes and input partition testing	C.5.7	R	HR	HR	HR
5 Process simulation	C.5.18	R	R	R	R

TBrun は、とりわけ TBreq を介して要件から直接テストデータを生成し実行すること、あるいは特定の手法（統計的なランダム生成など）によりテストデータを生成することで、項 1 と 4 を満たす。これらはテストデータ生成手法に依存する。TBrun は、境界値解析も実施できる。

項 3 は、TBrun によって満たされる。項 2、5 は、LDRA ツールスイートの対象外。SIL のレベルに応じたカバレッジ解析のレベル選択がある。

Table B.4 – Failure analysis

Technique/Measure	**Ref**	**SIL1**	**SIL2**	**SIL3**	**SIL4**
1a Cause consequence diagrams	B.6.6.2	R	R	R	R
1b Event tree analysis	B.6.6.3	R	R	R	R
2 Fault tree analysis	B.6.6.5	R	R	HR	HR

3 Failure modes, effects and criticality analysis	B.6.6.4	R	R	HR	HR
4 Monte-Carlo simulation	C.6.6	R	R	R	R

LDRA ツールスイートは、これらのアイテムを直接的には満たさない。しかしながら、これら作業の結果得られる成果物のトレーサビリティを取って、管理することが TBreq で行える。

Table B.5 – Modelling

Technique/Measure	**Ref**	**SIL1**	**SIL2**	**SIL3**	**SIL4**
1 Data flow diagrams	C.2.2	R	R	R	R
2 Finite state machines	B.2.3.2		R	HR	HR
3 Formal methods	C.2.4		R	R	HR
4 Performance modelling	C.5.20	R	HR	HR	HR
5 Time Petri nets	B.2.3.3		R	HR	HR
6 Prototyping/animation	C.5.17	R	R	R	R
7 Structure diagrams	C.2.3	R	R	R	HR

項 1 に対して LDRA ツールスイートは、コントロールフロー/データフローのグラフィカルモデルをシステムから生成する。それらの図は、ハードコピーなどに利用できる。

LDRA ツールスイートでは、特定タイプの障害が無いことを確証するために、多数のフォーマルメソッド（形式手法）をコントロールフローモデル、データフローモデルをベースにして実施している（項 3）これらのプロセスによって生成される成果物のトレーサビリティを取って、管理することが TBreq で行える。
これらモデルは LDRA ツールスイートの基本機能の一部として生成されるので、SIL のレベルとの関わりは無い。

Table B.6 – Performance testing

Technique/Measure	Ref	SIL1	SIL2	SIL3	SIL4
1 Avalanche/stress testing	C.5.21	R	R	HR	HR
2 Response timings and memory constraints	C.5.22	HR	HR	HR	HR
3 Performance requirements	C.5.19	HR	HR	HR	HR

LDRA ツールスイートは、性能の尺度を生成できる。Ada 版の LDRA ツールスイートはスタック解析が行える。また一方、項 2、3 からの成果物のトレーサビリティを取って、管理することが TBreq で行える。

Table B.7 – Semi-formal methods

Technique/Measure	Ref	SIL1	SIL2	SIL3	SIL4
1 Logic/function block diagrams		R	R	HR	HR
2 Sequence diagrams		R	R	HR	HR
3 Data flow diagrams	C.2.2	R	R	R	R
4 Finite state machines/state transition diagrams	B.2.3.2	R	R	HR	HR
5 Time Petri nets	B.2.3.3	R	R	HR	HR
6 Decision/truth tables	C.6.1	R	R	HR	HR

LDRA ツールスイートは、機能構造をドキュメント化するブロックダイアグラムである、システムの完全なコントロールフローグラフを生成する。 あるいは、個々のプロシジャーをグラフ表示できる。これらグラフには注釈が付加され、デシジョン決定構造を表現できる（項 1）

プロシジャー内の関連は、コールツリー（コールグラフ）で表示できる。実行不可能なコードなどは、LCSAJ で表示可能。包括的なメトリクスのセットにより、複雑度はコントロール可能となる。

これらのプロセスにより得られる成果物のトレーサビリティを取って、管理することが TBreq で行える。LDRA ツールスイートでは、これらを基本機能の一環として生成するので、SIL のレベルとの関わりは無い。

Table B.8 – Static analysis

Technique/Measure	Ref	SIL1	SIL2	SIL3	SIL4
1 Boundary value analysis	C.5.4	R	R	HR	HR
2 Checklists	B.2.5	R	R	R	R
3 Control flow analysis	C.5.9	R	HR	HR	HR
4 Data flow analysis	C.5.10	R	HR	HR	HR
5 Error guessing	C.5.5	R	R	R	R
6 Fagan inspections	C.5.15		R	R	HR
7 Sneak circuit analysis	C.5.11			R	R
8 Symbolic execution	C.5.12	R	R	HR	HR
9 Walk-throughs/design reviews	C.5.16	HR	HR	HR	HR

LDRA ツールスイートは、包括的に静的解析を実施する。この静的解析機能は、潜在的な問題に対するチェックリスト（プログラミングガイドラインを代表とした）に対する自動評価。コントロールフロー解析は、異常なループ制御構造、ループのネスティング、反復などを検出できる。データフロー解析は、異常な振舞いを検出するために広範に渡って活用される。

境界値の解析は、まず静的解析で実行可能性のコンディションがチェックされる。そして TBrun によるテストデータの実行を加えることで（二重化策）、障害が存在する可能性が、相当に削減される。

広範に渡るチェック機能により、ウォークスルー、Fagan 流検査（Fagan inspection)、その他のレビューを軽減できる。これらレビューは、ツールでチェックできない部分のみに限ることができる。

LDRA ツールスイートは、これら解析を基本機能の一環として行うので、SIL のレベルに依存しない。

Table B.9 – Modular approach

Technique/Measure	Ref	SIL1	SIL2	SIL3	SIL4
1 Software module size limit	C.2.9	HR	HR	HR	HR
2 Information hiding/encapsulation	C.2.8	R	HR	HR	HR
3 Parameter number limit	C.2.9	R	R	R	R
4 One entry/one exit point in subroutines and functions	C.2.9	HR	HR	HR	HR
5 Fully defined interface	C.2.9	HR	HR	HR	HR

LDRA ツールスイートは、項 1 に対するメトリクスを生成する。

データアイテムの範囲は、LDRA ツールスイートで表示される（項 2）。データフロー解析レポートの情報により、インフォメーション隠蔽の適切なレベルを得ることができる。

項 3 について、LDRA ツールスイートはパラメータ数、既定リミット超過数のレポートを生成する。

LDRA ツールスイートによる全関数の複数エントリーポイントのチェックは、項 4 に相当する。

LDRA ツールスイートのプロシジャーインターフェイスをコントロールするためのスタンダードの実施は、項 5 に相当する。プロシジャー内インターフェイスは詳細に渡ってチェックされ、ユーザインターフェイスは特定の障害に対してのみチェックされる。

例）

```
' More than *** parameters in procedure.
' Parameter not declared explicitly.
' No parameters declared in proc specification.
' Procedure Parameter has a type but no identifier.
' Ellipsis used in procedure parameter list.
' Empty parameter list to procedure/function.
' Function and prototype return inconsistent.
' Function and prototype param inconsistent.
' Call by value parameter not const.
' Default parameter use.
' Array passed as actual parameter.
```

ここに関わる情報は、LDRA ツールスイートの基本的な機能の一部として生成されるので、SIL のレベルに依存しない。

Summary

この資料で明らかなのは、LDRA ツールスイートは、広範に渡って IEC61508 スタンダードの認証取得に貢献できるということ。あらゆる SIL のレベルに適切であり、またツールの成熟性、長年に渡る実績は他に類を見ない。

LDRA ツールスイートは世界的に採用され、IEC 61508 など多くの国際的なスタンダードの認証取得を支えている。

References

1 ..... European Organisation for Civil Aviation Equipment, Software Considerations in Airborne Systems and Equipment Certification (ED-12B/DO-178B), EUROCAE, 17 rue Hamelin, F-75783 Paris Cedex 16, France, 1992. Available at http://www.eurocae.org.

2..... International Electrotechnical Commission, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (IEC 61508), International Electrotechnical Commission, 3 rue de Varembé, Geneva, Switzerland, 1998. Available at http://www.iec.org.ch

LDRA Ltd. Portside, Monks Ferry, Wirral, CH41 5LH, UK.

t : +44 (0)151 649 9300 f : +44 (0)151 649 9666

w : www.ldra.com e : info@ldra.com

富士設備工業株式会社 電子機器事業部

〒591-8025 大阪府堺市北区長曽根町1928-1

Tel: 072-252-2128 www.fuji-setsu.co.jp