



LDRA



Andrew Banks
IEng MIET FBCS CITP

LDRA Software Technology

June 2023

Andrew BanksさんはLDRAの社員でもありますので、始めに、弊社とLDRAについて簡単に紹介します。

スタンダード認証支援テストツール

C/C++コンパイラの妥当性を検証

ドメイン固有モデリングと自動生成

プロダクトライン開発のバリエーション管理

JTAG バウンダリスキャンテスト

JTAGデバッグの世界標準 Lauterbach

JTAGデバッグ Ashling

C/C++コンパイラ 欧州車載品質

IEC 61508, ISO 26262, DO-178B/C, IEC 62304, EN 50128, MISRA, CERT など、国際スタンダード実績No1の LDRA社テストツールは、静的解析・単体テスト・システムレベルテスト・カバレッジ解析を、あらゆる実行環境下で、要件トレーサビリティに統合することで、認証プロセスの工数と費用を軽減します。



まず富士設備は、世界最高峰の革新的な開発支援ツールの代理店として、LDRA社テストツールの販売とサポートを、およそ20年近く承っています。



1975年設立 => 45年以上の実績とブランド

ISO 9001 認証取得

スタンダード認証プロセスを支援する

ソフトウェアテスト、管理支援ツールを提供

IEC 61508, IEC 62304, EN 50128,

ISO 26262, IEC 60880 のツール認定取得

各種スタンダード委員会にも貢献

DO-178C, ISO 26262

MISRA C/C++, CERT,



このLDRAは設立45年以上の実績と経験のもと、スタンダード認証プロセスを支援するテストツールを提供し、IECやISOのツール認定もされています。また各種スタンダードにも貢献しています。

LDRA Standards Experience & Pedigree

LDRA



Professor Mike Hennell

Member of SC-205 /
WG-71 (DO-178C) formal
methods subgroup

Member of MISRA C committee
and MISRA C++ committee

Member of the working group
drafting a proposed secureC
annex for the C language
definition
(SC 22 / WG14)



Chris Tapp

Chairman of MISRA
C++ committee

Member of MISRA C committee
language definition

<https://ldra.com/misra/#misra3>



Andrew Banks

MISRA Committee Chair

Committee Member for Second
Edition of ISO 26262

UK Head of Delegation
to ISO/IEC JTC1/SC7

MISRA representative to BSI
IST/15 for Software and
Systems Engineering

設立者であるMike Hennellさんは、航空業界のDO-178やMISRAの委員会、およびISOやIECに関わり、今日の主役であるAndrew BanksさんはMISRA Cの議長やISOの委員も務めています。ちょうど先週、ISOの委員会が岡山であり、それに合わせて来日しました。真ん中のChris Tappさんは、MISRA C++の議長です。この二人は以前、IPAの招待でMISRAの代表としてセミナーもしました。

コーディング規約
チェック

構造化カバレッジ
解析

データフロー
コントロールフロー
解析

単体テストの
自動化支援

あらゆるターゲット
環境をサポート

要件～検証結果
のトレーサビリティ

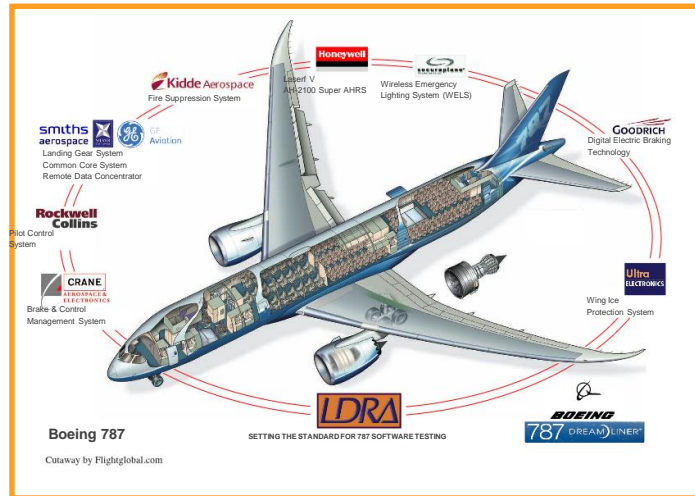
ツール認定

認証機関への
エビデンス提示



- 検証作業を自動化
- 認証プロセスを支援
- 検証と認証作業を加速

このLDRA社が提供するテストツールは、とりわけ厳しい航空業界で標準的に採用されるなか進化を続けています



ANAが世界初運行させたボーイング787にも採用され、



自衛隊の主力戦闘機でもあるF35は、主契約のロッキードマーチンと全サプライヤーが採用しました。このプロジェクト当時、C++の良いコーディング規約が無かったため、ロッキードとC++の開発者（Bjarne Stroustrup）、そしてLDRAが一緒になって、JSF C++スタンダードを作りました。これは後にMISRA C++の基になったと言われています。



またユーロファイター・タイフーンにも採用されました。
日・英・伊の共同開発が始まる次期戦闘機は、この後継機と言
われています。
このプロジェクトでは、LCSAJというコードのパス密度解析と、
そのカバレッジ尺度が採用されたことは少し興味深いです。



宇宙分野では、NASAのアртеミス計画の公式検証ツールとして、宇宙船「オリオン」にも活用されています。アルテミス計画には日本のJAXAと欧州のESAも参画していますので、今後採用領域が増えることが期待されます。



他にも、あらゆる市場で採用されています。

MISRA、CERT 等の各種コーディング規約をサポート



- CAST
- CERT
- CMSE
- CONFORM
- CWE
- Customer Sample
- DERA
- EADS
- FSB582-C
- GJB
- HIS
- JPL
- Legacy
- MISRA-AC
- MISRA-C:1998
- MISRA-C:2004
- MISRA-C:2012
- NETRINO
- RUNTIME
- SEC-C
- Standard
- TBrun Requires
- UML
- VSOS
- No Standards Model

Rule Number	Default Strength	Description	CAST	CERT	CWE	HIS	JPL	MISRA-AC	MISRA	MISRA-C 2004	MISRA-C 2012	NETRINO	SEC-C
1	C	Procedure name reused.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2	M	Label name reused.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	M	More than *** executable reformatted lines in file.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	M	Procedure exceeds *** reformatted lines.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	C	Empty then clause.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
6	O	Procedure pointer declared.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	C	Jump out of procedure.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	C	Empty else clause.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

https://www.fuji-setsu.co.jp/files/Implementing_ISO_26262_second_edition_white_paper_v2.0JP.pdf#page=15

11

このLDRA社テストツールは、今日の本題であるMISRAなどの各種コーディング規約をサポートするルールチェックのスーパーセットが搭載されています。例えばMISRAやCERTをベースに取捨選択して、独自のルール集を編集できるということです。

- 静的解析の一環としてMISRA等のコーディング規約と同時に解析される

	Value	Lower Limit	Upper Limit
castregister			
↳ TesteC			
↳ Clarity	78% Metrics Successful		
↳ Maintainability	90% Metrics Successful		
↳ Testability	93% Metrics Successful		
↳ Metric Groupings			
↳ Clarity	50% Metrics Successful		
↳ Depth of Loop Nesting	0	0	2
↳ Average Length of Basic Blocks	3%	1%	6%
↳ Code Comments/Exe. Lines	0 ; (Fail)	5	200
↳ Declaration Comments/Exe. Lines	0 ; (Fail)	1	100
↳ Total Comments/Exe. Lines	66	10	200
↳ Blank Lines	0	0	100
↳ Comments in Executable Code	0 ; (Fail)	1	100
↳ Comments in Declarations	0	0	100
↳ Comments in Headers	2 ; (Fail)	5	50
↳ Total Comments	2 ; (Fail)	10	200
↳ Maintainability	100% Metrics Successful		
↳ Testability	100% Metrics Successful		
↳ Metric Groupings			
↳ Procedure Information	100% Metrics Successful		
↳ Comments Associated with Procedures (% of total)	40% Metrics Successful		
↳ Ratio of Comments to Executable lines (%)	60% Metrics Successful		
↳ Complexity Metrics	100% Metrics Successful		
↳ Loop/Interval Analysis	100% Metrics Successful		
↳ Unreachable Information	100% Metrics Successful		
↳ randomShopping			
↳ Clarity	80% Metrics Successful		
↳ Maintainability	100% Metrics Successful		
↳ Testability	87% Metrics Successful		

Zone.cpp	
↳ Clarity	100%
↳ Executable ref. Lines	147
↳ Depth of Loop Nesting	1
↳ Total LCSAJs	46
↳ Unique Operands	105
↳ Average Length of Basic Blocks	4.03%
↳ Comments in Headers	53
↳ Maintainability	100%
↳ Unreachable Branches	0
↳ Unreachable Lines	0
↳ Maximum LCSAJ Density	4
↳ Unreachable LCSAJs	0
↳ Total LCSAJs	46
↳ Vocabulary	119
↳ Cyclomatic Complexity	9
↳ Knots	23
↳ Essential Cyclomatic Complexity	1
↳ Essential Knots	0
↳ Testability	100%
↳ Fan Out	7
↳ File Fan In	0
↳ Number of Procedures	7
↳ Procedure Exit Points	11
↳ Number of Loops	5
↳ Unreachable Branches	0
↳ Unreachable Lines	0
↳ Maximum LCSAJ Density	0
↳ Unreachable LCSAJs	0
↳ Total LCSAJs	46
↳ Total Operands	286
↳ Number of Basic Blocks	36
↳ Executable reformatted Lines	145
↳ Cyclomatic Complexity	9
↳ Knots	23

また複雑度などのメトリクスは、コーディング規約と同時に解析され、「可読性」、「保守性」、「テスト容易性」といった、コード品質の尺度で評価されます。

Requirement based Test case

Value	Name	Type
I	CALCULATE_CMD	command
I	*** Value Retained ***	airspeed
O	0	airspeed

Unexecuted code for the given test case

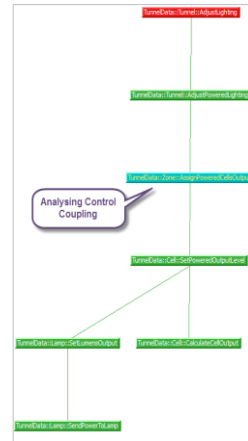
```

31 void runAirspeedCommand (S_T16 command) {
32   if (command == CALCULATE_CMD) {
33     calculateAirspeed (&airspeed);
34     break;
35   }
36   if (command == DISPLAY_CMD) {
37     displayAirspeed (&airspeed);
38     break;
39   }
40 }
    
```

Unexecuted data reference for the given test case

Variable Name	File	Procedure	Type Code	Attribute Code	Used on lines...
airspeed	AirspeedCommands.cpp	runAirspeedCommand	O	R	36, 38, 39, 40
command	AirspeedCommands.cpp	runAirspeedCommand	I	R	31, 32, 33, 34, 35, 36, 37, 38, 39, 40
testcase	AirspeedCommands.cpp	calculateAirspeed	I	R	31, 32, 33, 34, 35, 36, 37, 38, 39, 40

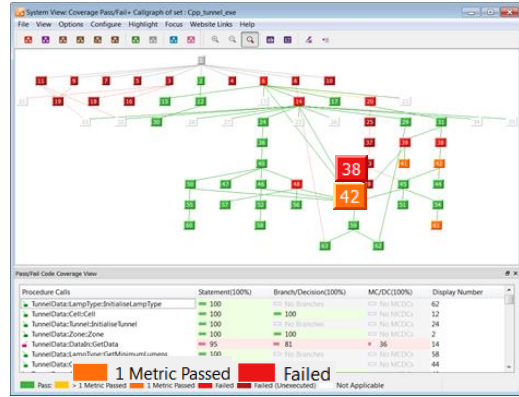
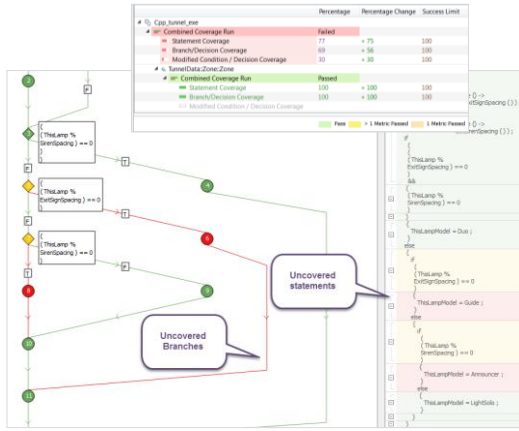
On line 39 the reference to airspeed by displayAirspeed is not executed with this test case



Dramatically reduce the effort required to achieve data and control coupling objectives

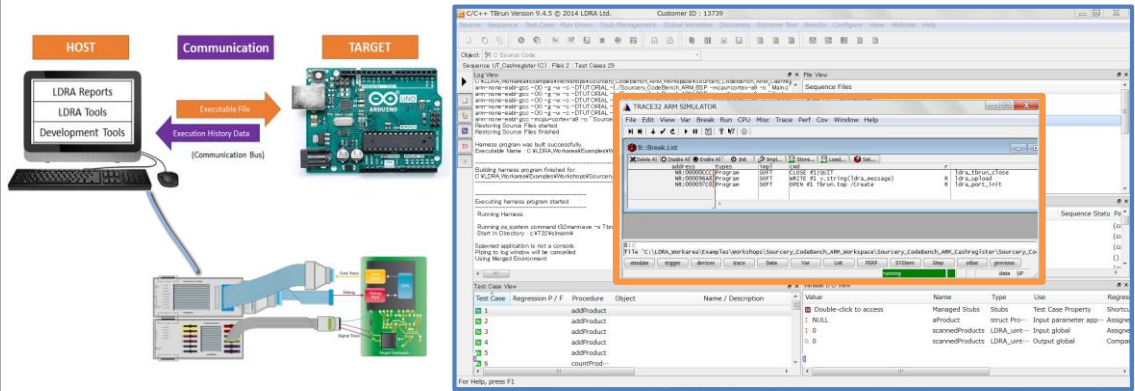
更にデータカップリングとコントロールカップリングの静的および動的解析や、

動的テストをカバレッジ解析で評価



出荷されて初めて実行されるようなコードを無くし、不要なコードは削除する

MCDCなどのテストのカバレッジ解析、



あらゆるターゲット環境で実行

また単体テストの自動化支援などを、あらゆるターゲット環境でサポートします。



機能安全規格のベストプラクティスを支援

MISRA やCERTなどコーディング規約

複雑性のメトリクスの測定

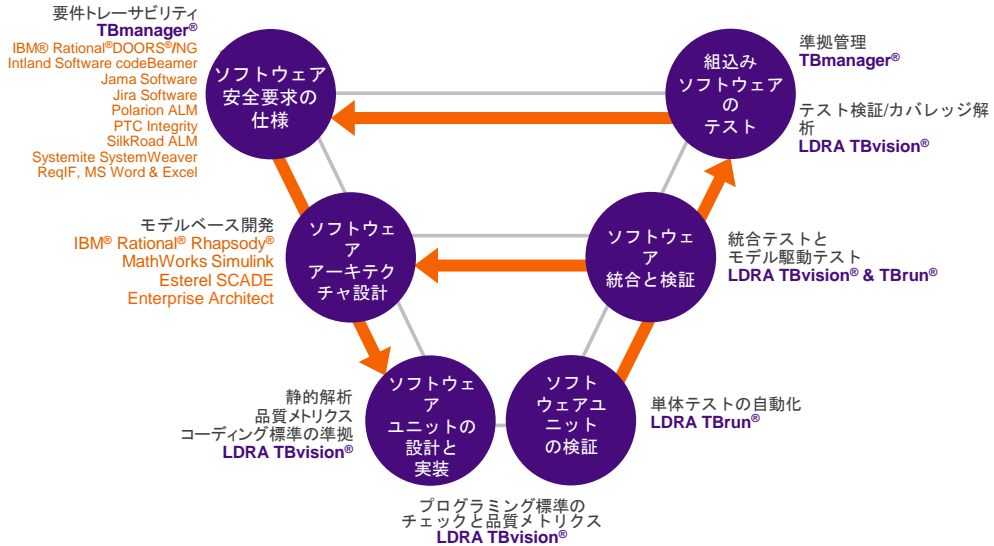
単体テスト、動的テストのカバレッジ解析

あらゆるターゲット環境をサポート

静的～動的解析を単一ツールで効率化

16

以上を纏めると、航空業界で標準的に採用されるなか進化を続けるLDRA社テストツールは、機能安全規格で実証されたベストプラクティスを支援するために、MISRA やCERTなどコーディング規約、複雑性のメトリクスの測定、単体テストや動的テストのカバレッジ解析を、あらゆるターゲット環境でサポートします。そして、静的解析で得られた結果が単体テストやカバレッジ解析にも活用されるので、複数のツールを管理・運用する苦勞から解放されて、開発の早期段階から活用することで、開発期間の削減にも貢献します。



今日、ツールの詳しい紹介はしませんが、興味頂ける方は評価版やデモを依頼頂けると幸いです。

Need more information?

 **FUJI SETSUBI**
www.fuji-setsu.co.jp

