



LDRA社単体テストツールのデモ/紹介 (HighTec社TriCoreコンパイラと ローターバッハ社デバッグとの連携例)



Delivering Software Quality and Security through
Test, Analysis & Requirements Traceability

LDR

ISO 9001認証取得

1975年設立 => 40年以上の実績とブランド

IEC 61508, IEC 62304, EN 50128,

ISO 26262, IEC 60880 のツール認定取得

スタンダード認証プロセスを支援する

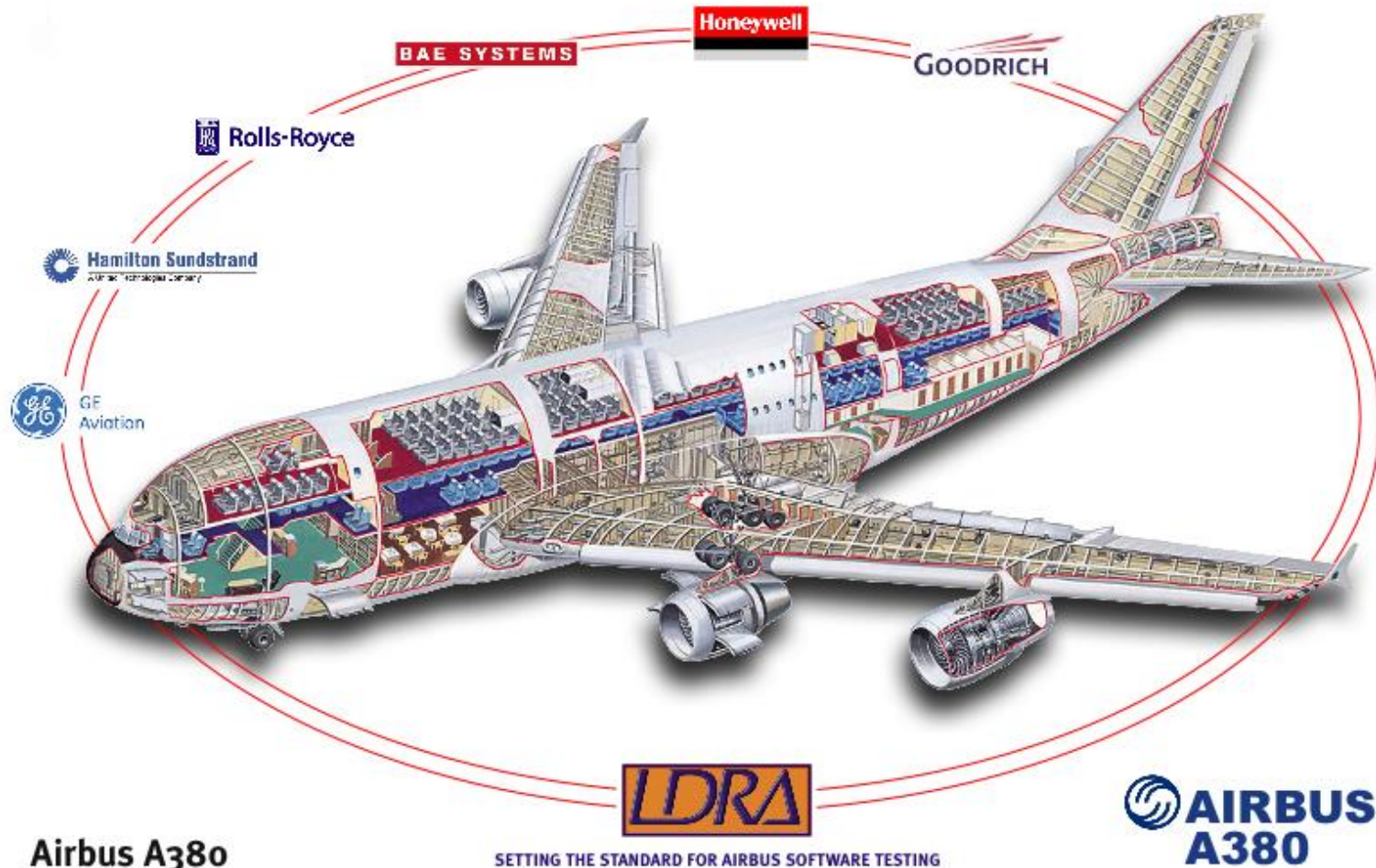
ソフトウェアテスト、管理支援ツールを提供



特徴: 航空業界で標準的に採用



Customer: Airbus A380



Cutaway illustration reprinted from Popular Mechanics. Copyright The Hearst Corporation. All rights reserved

From an original painting by John Batchelor

Customer: F-35

www.ldra.com



F-35 Lightning II

SETTING THE STANDARD FOR JSF SOFTWARE TESTING

Cutaway illustration reprinted from Popular Mechanics, May 2002. Copyright The Hearst Corporation. All rights reserved

From an original painting by John Batchelor



**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)



Bill St Clair

Member of SC-205 /
WG-71 (DO-178C) Object
Oriented
Technology subgroup



Andrew Banks

MISRA Committee Chair
Committee Member for
Second Edition of ISO 26262

Chair of BSI IST/15/-/26
for Software Testing

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

Member of BSI IST/15-/20 for
Bodies of Knowledge and
Professionalization



Dr Clive Pygott

Member of ISO software
vulnerabilities working
group (SC 22 / WG 23)

Member of MISRA
C++ committee

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



Liz Whiting

Member of MISRA C
committee language
definition



Chris Tapp

Chairman of MISRA
C++ committee

Member of MISRA C
committee language
definition

航空業界標準:LDRA社ツール

コーディングスタン
ダードチェック

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

あらゆるターゲット
環境でサポート

要件～検証結果
のトレーサビリティ

ツール認定

オブジェクティブ
の追跡・管理

認証機関への
エビデンス提示



検証作業を自動化

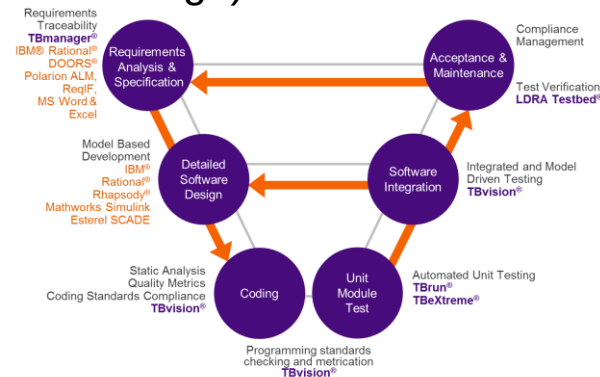
認証プロセスを支援

検証と認証作業を軽減

1975年設立～航空業界の顧客の知恵を組み込み進化を続ける

各機能が有機的につながる

- 静的解析:コーディングスタンダード準拠、コード品質のメトリクス
 - MISRA、CERT C、IPA/SEC ESCR 等各種サポート。ユーザ定義ルール集も編集できる
 - コードの視覚化(コールグラフ、フローグラフ、クロスリファレンス)
- 動的解析:構造化カバレッジ
 - 関数コール、ステートメント、ブランチ、MC/DC、LCSAJ (path coverage).
 - アセンブラレベルカバレッジ (DO-178C Level A)
 - あらゆる組込みコンパイラ、実行環境をサポート
- 単体テスト(Unit/low-level testing)
 - テストハーネス、スタブ、グローバル宣言などの自動生成
 - 堅牢性テストのためのテストケース自動生成
- データフロー・コントロールフローの静的・動的解析
 - DO-178C で認定可能な唯一の汎用ツール
- 要件トレーサビリティに検証実行・オブジェクト管理を統合
- ツール認定キットを提供(DO-178Cに必要)
- TUVの事前認定





航空システム



防衛システム



医療機器



産業機器
電カプラント



鉄道システム



車載システム



LDRA テストツールの概要

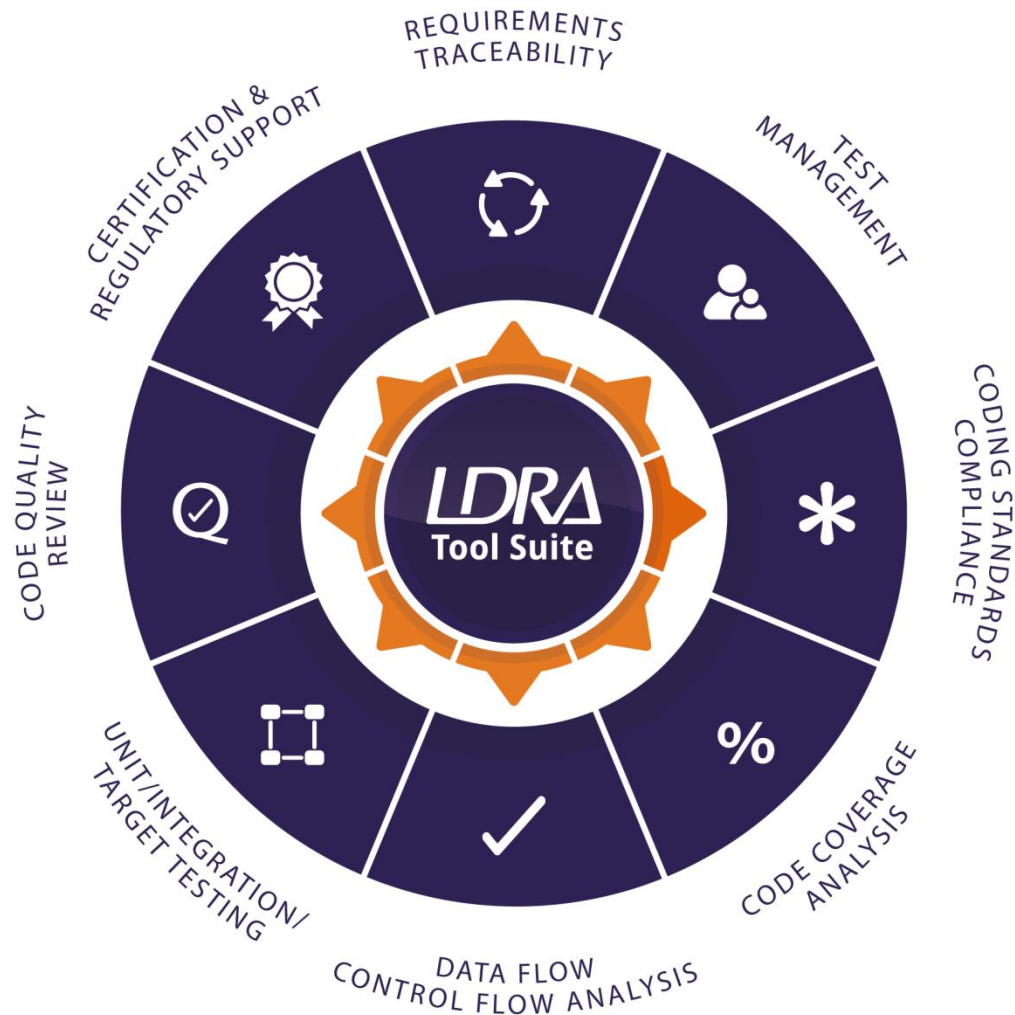


Delivering Software Quality and Security through
Test, Analysis & Requirements Traceability

The LDRA Tool Suite® 構成



LDRA Solution



コーディング
スタンダード
チェック

コード品質の
尺度

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
統合テスト

要件トレーサ
ビリティ

テストの管理

認証プロセス
の支援

コーディングスタンダードへの準拠

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
 TBrn Requires
 UML
 VSOS
 No Standards Model

- ✖ ISO 26262 - Road Vehicles Safety Standard - Unfulfilled
 - ✖ Part 6: - Product Development : Software Level - Unfulfilled
 - ✖ Section 5 - Initiation of product development at the software level - Unfulfilled
 - ✖ Table 1 - Topics to be covered by modelling and coding guidelines - Unfulfilled
 - ⚠ 1a - Enforcement of low complexity - Partial - 4 artifacts
 - 📄 Design and coding guidelines Document fulfilled by 1 item
 - Misra c 2012.pdf
 - 📄 Metric Threshold File fulfilled by 1 item

LDRA Report File Editor - C:\LDRA_Toolsuite\c\creport.dat*

File Edit View Help

Static	Complexity	Data Flow	Cross Ref	Info Flow	Qual Report	Qualsys	LCSAJ	Hungarian Notation	User Def	Section 3	Section 4	PDTMCSFVA	
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.	☒	☐	☐	☒	☐	☒	☒	☒	☒	☐	☒
2	M	Label name reused.	☒	☐	☐	☐	☐	☒	☒	☒	☐	☐	☐
3	M	More than *** executable reformatted lines in file.	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
4	M	Procedure exceeds *** reformatted lines.	☒	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
5	C	Empty then clause.	☒	☒	☒	☐	☐	☐	☐	☐	☐	☐	☒
6	O	Procedure pointer declared.	☒	☐	☐	☐	☒	☐	☐	☐	☐	☐	☐
7	C	Jump out of procedure.	☒	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
8	C	Empty else clause.	☒	☐	☐	☐	☐	☐	☐	☐	☐	☐	☒

Report File (PC): Section 1 read (24 Models)(24 Modifiers)...Section 2 read (866 Rules)...Section 3 read...Section 4 read...Penalty File (PC): read

Automate coding standards compliance to eliminate defects early in the lifecycle
 MISRA-C:1998 ,2004, 2012, MISRA-C++:2008, CERT C, IPA/SEC ESCR

MISRA C:2012 Addendum 2

ISO/IEC TS 17961:2013 の「Cセキュアコーディング」に対する
MISRA C:2012のカバレッジ

x46 の C SecureルールのとれがMISRA C:2012のガイドライン
の対象であるかを示す

MISRA C:2012 Amendment 1

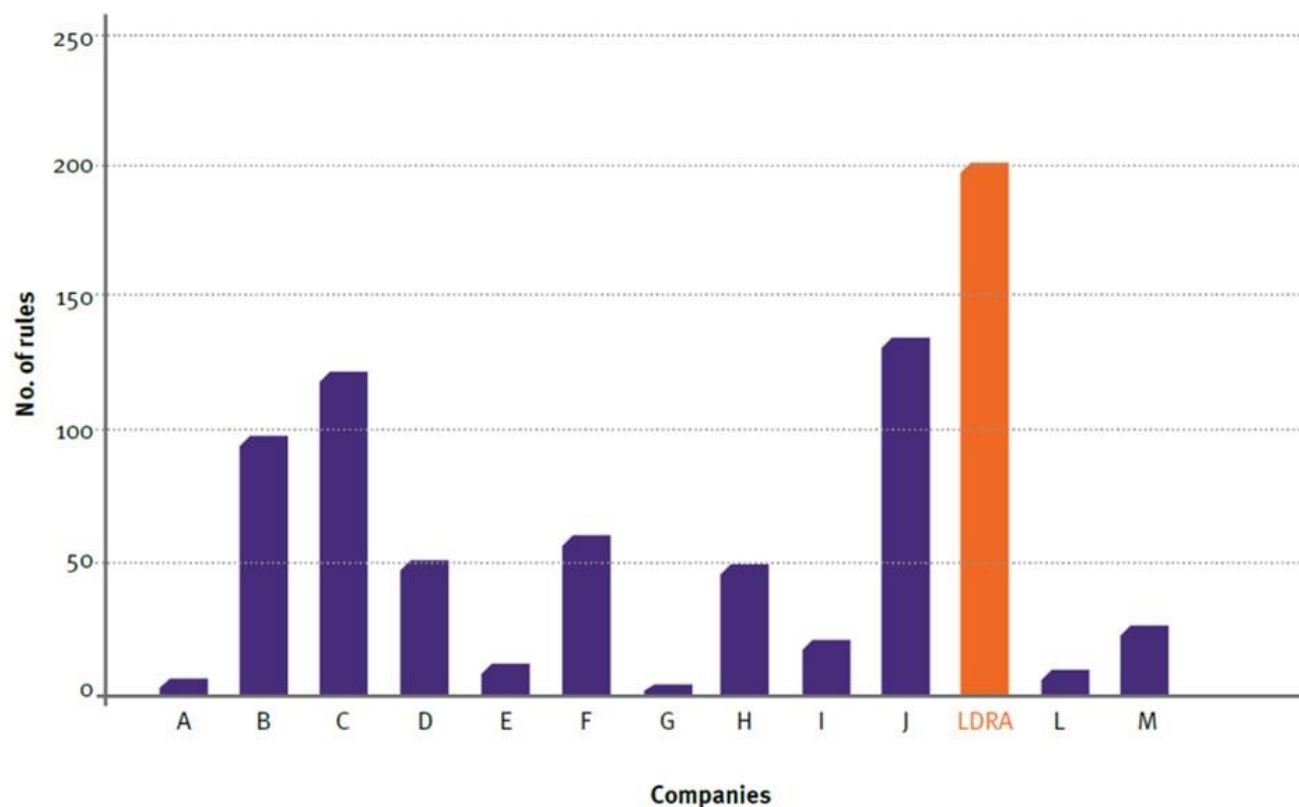
ISO C セキュアガイドラインへのカバレッジを強化する
14の新しいCコーディングルール

特に「信頼されていないデータの使用」というセキュリティ上の脆弱
性に付き物の具体的な問題へ取り組む

セキュアでないコーディングの例

https://www.fuji-setsu.co.jp/files/MISRA_C_2012_AMD1.pdf

CERT 対応で他を圧倒！



Tool	No. of rules
A	7
B	96
C	122
D	50
E	11
F	63
G	3
H	48
I	21
J	135
LDRA tool suite	201
L	10
M	26

LDRAはシステムワイドにコントロールフローとデータフローを解析できることが優位性のひとつ

複雑度解析やコード品質の尺度

- ✖ 1a - Enforcement of low complexity
 - Input Artifacts
 - Design and coding guidelines Document fulfilled by 1 item
 - Software Design & Code Standards(SDCS).docx
 - Output Artifacts
 - Quality Review Report fulfilled by 1 item

Code Quality View (Maintainability)		
Procedure Calls	Cyclomatic Complexity	Knots
GetOptimum	98 : (Fail)	114 : (Fail)
LzmaDec_DecodeReal	82 : (Fail)	76 : (Fail)
LzmaDec_TryDummy	61 : (Fail)	94 : (Fail)
GetOptimumFast	41 : (Fail)	38 : (Fail)
LzmaDec_DecodeToDic	30 : (Fail)	57 : (Fail)
LzmaEnc_CodeOneBlock	30 : (Fail)	32 : (Fail)
main2	23 : (Fail)	28 : (Fail)
LzmaEncProps_Normalize	20 : (Fail)	7 : (Fail)
Decode2	14 : (Fail)	15 : (Fail)
Hc4_MatchFinder_GetMatches	14 : (Fail)	9 : (Fail)
Bt4_MatchFinder_GetMatches	14 : (Fail)	9 : (Fail)
MatchFinder_Create	14 : (Fail)	8 : (Fail)
GetMatchesSpec1	13 : (Fail)	14 : (Fail)
LzmaEnc_Alloc	13 : (Fail)	8 : (Fail)
BtGetMatches	11 : (Fail)	11 : (Fail)
LzmaEnc_SetProps	11 : (Fail)	2
SkipMatchesSpec	10	13 : (Fail)
MatchFinder_ReadBlock	10	12 : (Fail)
Hc_GetMatchesSpec	10	12 : (Fail)

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%
Number of Procedures	7
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	1
Number of Loops	5
Unreachable Branches	0
Unreachable Lines	0
Maximum LCSAJ Density	4
Unreachable LCSAJs	0
Total LCSAJs	46
Total Operands	286
Number of Basic Blocks	36
Executable reformatted Lines	145
Cyclomatic Complexity	9

Quickly assess code quality to reduce cost of development and verification

データカップリング、コントロールカップリング

1e - Control flow analysis

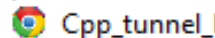
Output Artifacts

- Code Coverage Flowgraphs fulfilled by 1 item
 - Callgraph - Pass/Fail Coverage for Lampmodel....
- Code Coverage Callgraphs fulfilled by 1 item
 - Callgraph - Pass/Fail Coverage for Lampmodel....

Input Assets

1f - Data flow analysis

Output Artifacts



Variable I/O View		
Value	Name	Type
⊞ CALCULATE_CMD	command	S_U16
⊞ *** Value Retained ***	airspeed	S_U32
⊞ 0	airspeed	S_U32

```

31 void runAirspeedCommand (S_U16 command) {
32     switch (command)
33     {
34     case CALCULATE_CMD:
35         calculateAirspeed (airspeed);
36         break;
37     case DISPLAY_CMD:
38         displayAirspeed (airspeed);
39         break;
40     }
41 }
42

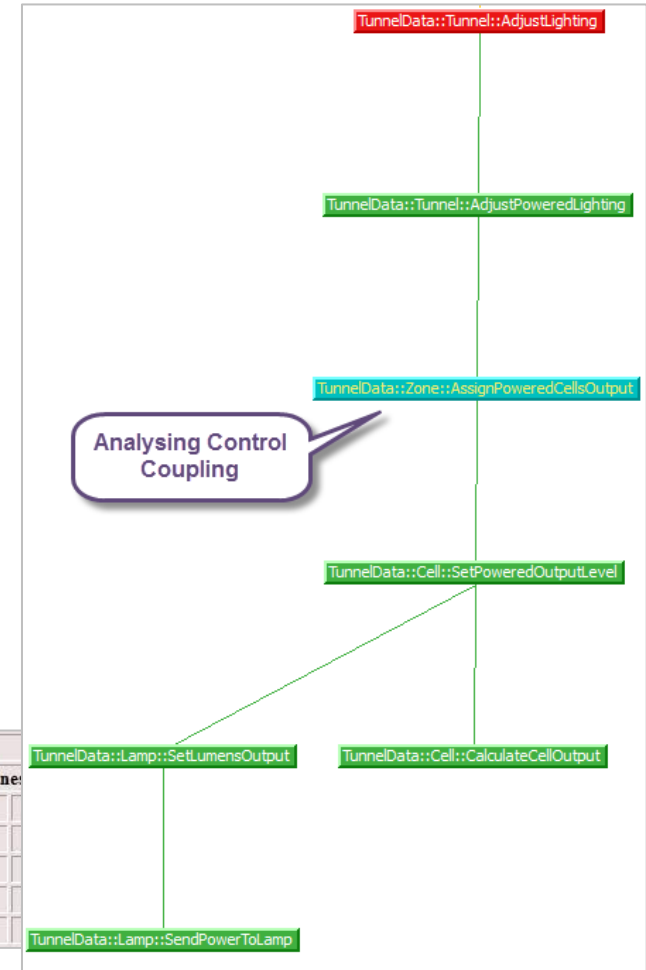
```

Unexecuted code for the given test case

Unexecuted data reference for the given test case

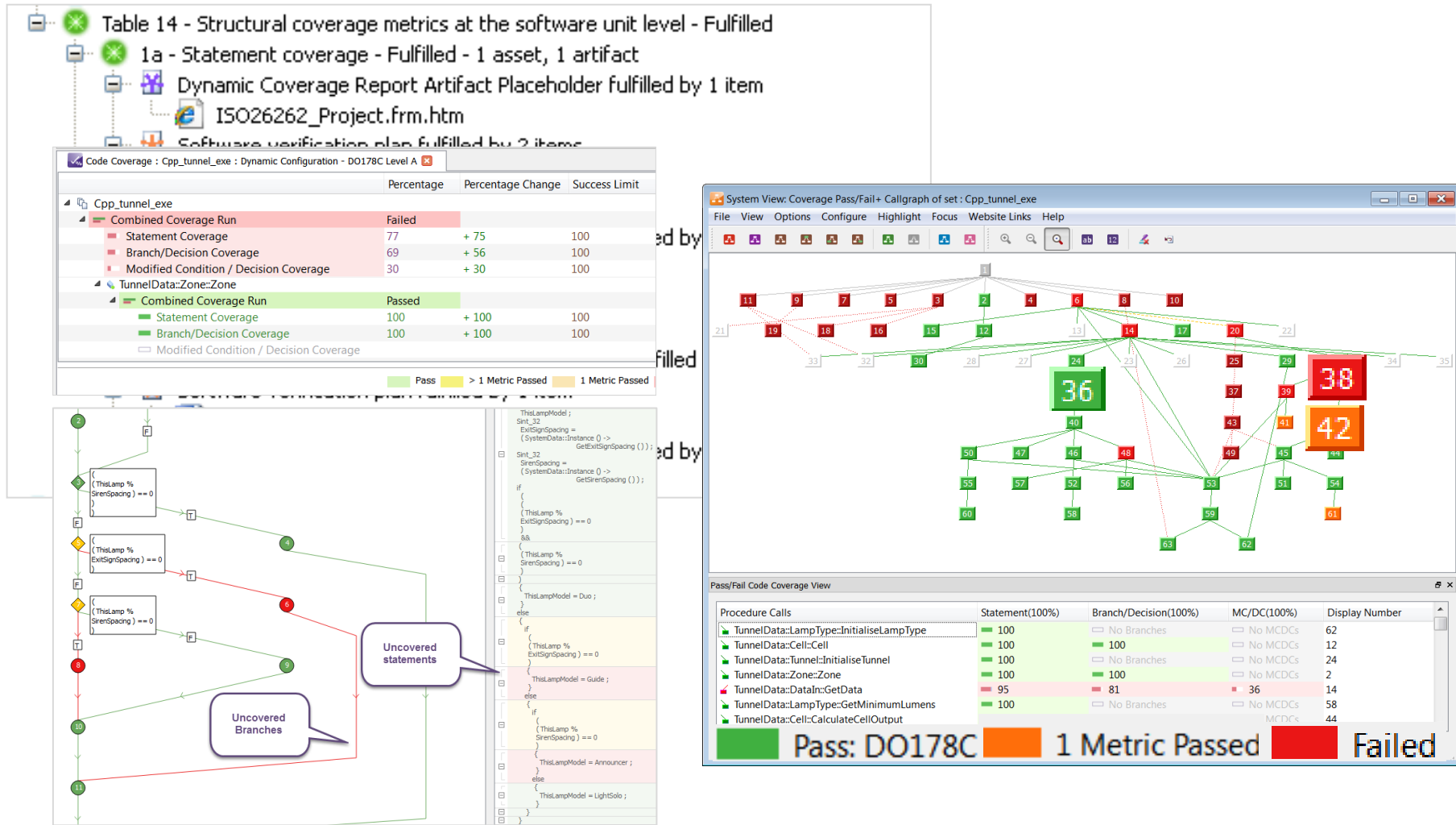
Variable Name	File	Procedure	Type Code	Attribute Code	Used on line
airspeed	AirspeedCommands.cpp	runAirspeedCommand	G	R	39 *****
command	AirspeedCommands.cpp	runAirspeedCommand			36
					31
					33
factor	AirspeedCalculate.cpp	calculateAirspeed			16

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

構造化カバレッジ解析



Automate all levels of code coverage across a wide array of embedded environments

あらゆるターゲット環境で実行

- Section 8 - Software unit design and implementation - Unfulfilled
- Table 9 - Design principles for software unit design and implementation - Unfulfilled
- 1a - One entry and one exit point in subprograms and functions - Fulfilled - 2 assets, 1 artifact
- Code Review Report Artifact Placeholder fulfilled by 1 item
- ISO26262_Project.frm.htm

HighTec_TriCore_Workspace - HighTec_TriCore_Dice/src/dice.c - HighTec Development Platform

File Edit Source Refactor Navigate Search Project LDRA Run Window Help

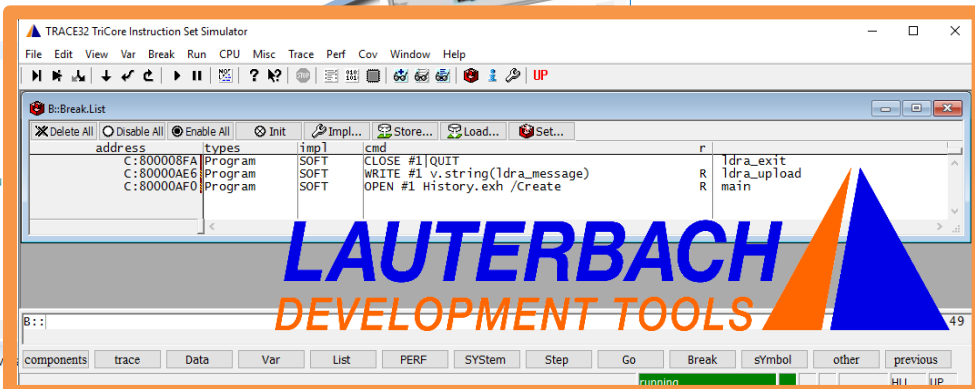
C:\... Na... main.c dice.c

```
1 #include "types.h"
2 #include "dice.h"
3
4 const u32 TABLE[]={1,2,3,5,6,
5 u16 table_index=0;
6
7 /* Forward declarations */
8 static u32 rollDice (void);
9
10 /*
11 * Roll a dice and get a value
12 */
13 static u32 rollDice (void) {
14     table_index++;
15     table_index %= 16;
16     return TABLE[table_index];
17 }
18
```

LDRA Code Violations LDRA Code Cov

Double click a Function to Open in Editor.

C:\LDRA_Workarea\Examples\TIPS\Lauterbach\HighTec_TriC
Combined Coverage Run
Statement Coverage 100 100
Branch/Decision Coverage 100 100
Modified Condition / Decision Coverage 100 100
integer_to_ascii
Combined Coverage Run
Statement Coverage 100 100



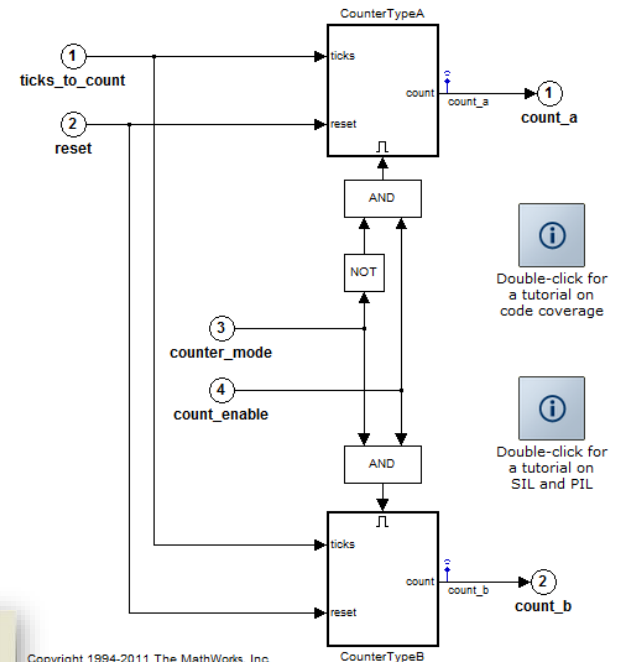
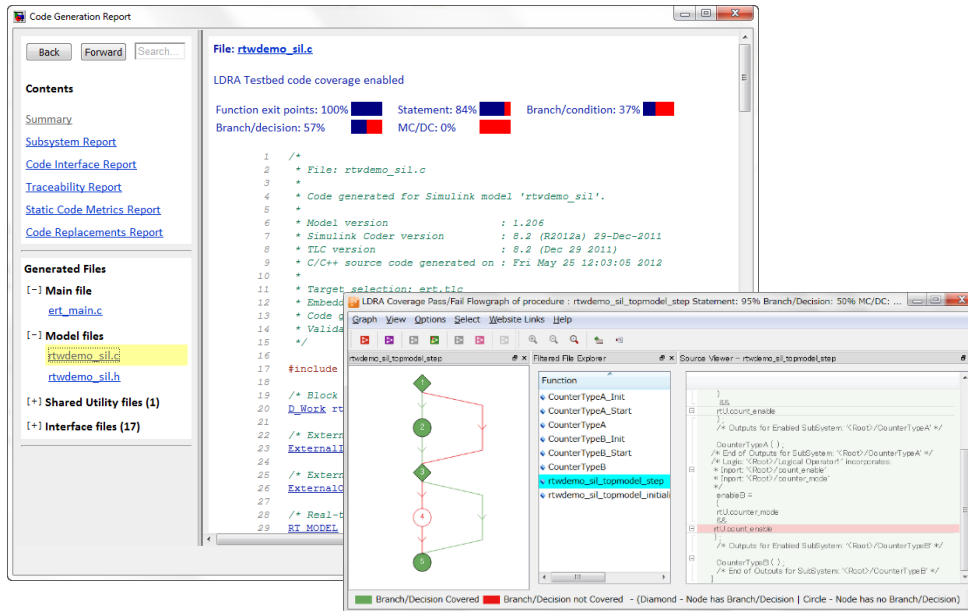
TriCore用HighTecコンパイラとローターバツハ社デバッガ動画デモ

静的解析～単体テスト : https://www.fuji-setsu.co.jp/demo/Tricore_HighTec_Lauterbach_LDRA.wmv

要件トレーサビリティ : https://www.fuji-setsu.co.jp/demo/TBmanager_Tricore_HighTec_Lauterbach.wmv

19

Simulink® 統合: SIL, PIL をサポート



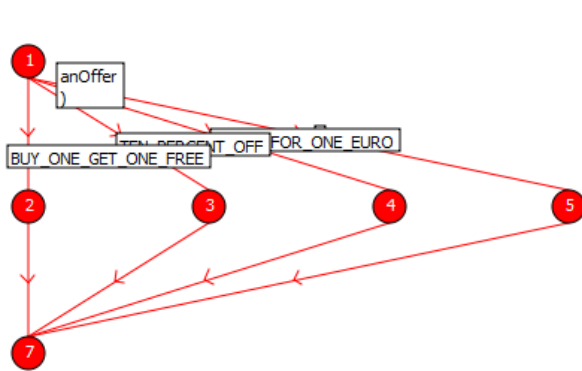
Copyright 1994-2011 The MathWorks, Inc.



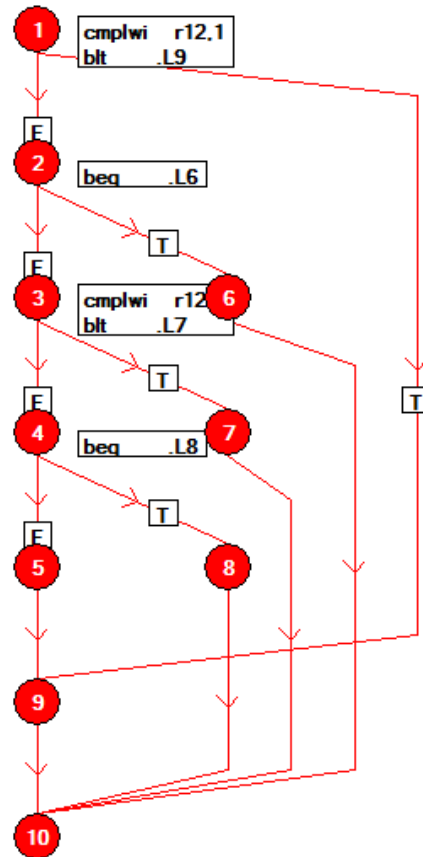
<https://www.fuji-setsu.co.jp/products/LDRA/Simulink.html>

**LDRA tool with Simulink to provide independent verification of model-generated code.
Bidirectional traceability ensures coverage from requirements through test.**

オブジェクトコードレベルの検証



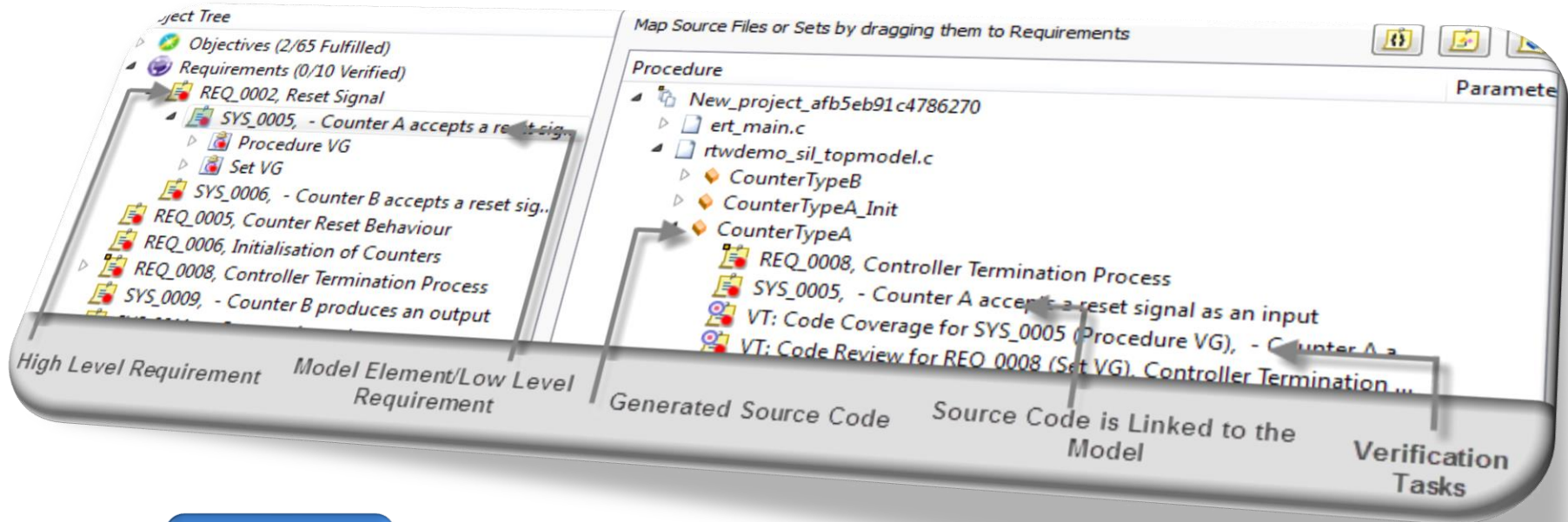
Standard	DO-178C
Standard Level	A - SI, B - , C - , D -
References	6.4.4.2.b

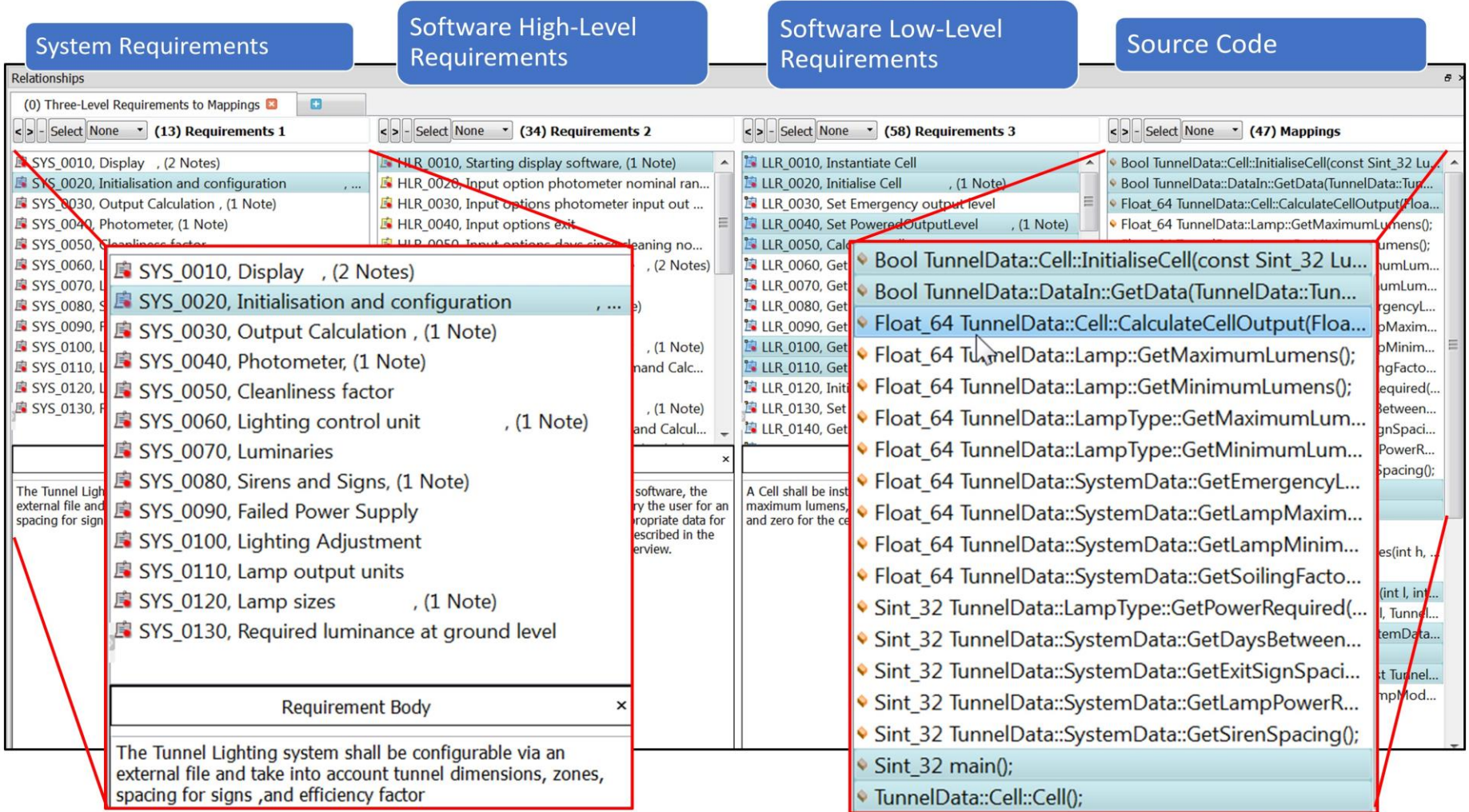


- 6.4.4.2 - Structural Coverage Analysis - Partial
 - 6.4.4.2a - MC/DC, Statement and Branch Coverage - Fulfilled - 20 artifacts
 - 6.4.4.2b - Object Code Coverage - Fulfilled - 20 artifacts
 - Test Case Sequence File fulfilled by 10 items
 - UnitTest_specialoffer.tcf
 - Scenario_Filling_The_Basket.tcf
 - Scenario_Cancelling_Products.tcf
 - UnitTest_main.tcf
 - UnitTest_cashregister.tcf
 - Scenario_Ignoring_Erroneous_Commands.tcf
 - UnitTest_tester.tcf
 - UnitTest_productdatabase.tcf
 - Scenario_Adding_Products.tcf
 - Scenario_Manually_Entering_A_Barcode.tcf
 - Assembler Code Dynamic Review Report fulfilled by 5 items
 - productdatabase_3.dyn.htm
 - main_2.dyn.htm
 - specialoffer_4.dyn.htm
 - tester_5.dyn.htm
 - cashregister_1.dyn.htm
 - Test Case Regression Report fulfilled by 5 items
 - tester.thr.htm
 - productdatabase.thr.htm
 - specialoffer.thr.htm
 - main.thr.htm
 - cashregister.thr.htm
 - 6.4.4.2c - Data Coupling and Control Coupling - Unfulfilled

Efficiently meet the DO-178C objective by ensuring traceability from source code to executable object code

要件からテストに至るトレーサビリティ







ISO 26262

Structural Coverage
Analysis (SCA)

Tool Qualification
Support Pack
Overview

Programming Rules Checking

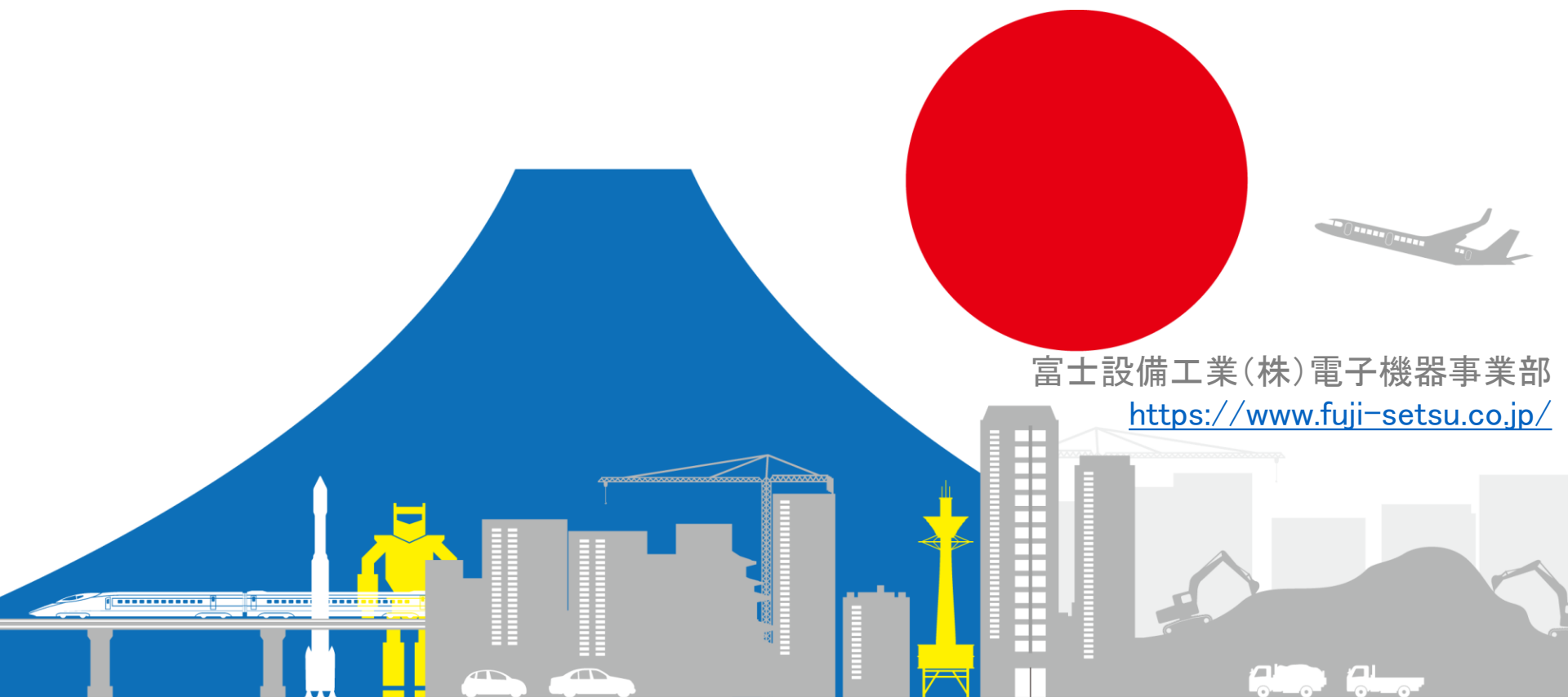
Structural Coverage Analysis

Dynamic Data Flow Coverage

Assembler Coverage Analysis

Unit Test / Low Level Test

Over 20 years of tool qualification pedigree widely recognised by regulators



富士設備工業(株)電子機器事業部

<https://www.fuji-setsu.co.jp/>