# Ensuring Safety and Security of Next Generation Automotive Software

Stephen Di Camillo, stephen.dicamillo@ldra-usa.com

Technical Marketing and Business Development Manager

# Speaker

## Technical Marketing and Business Development Manager, LDRA

Stephen Di Camillo

As Technical Marketing and Business Development Manager at LDRA, he works with customers worldwide in industries including automotive, aerospace, railway, medical, communications, energy, and industrial equipment. He has over 30 years of experience in embedded systems and software development, with a focus on model-based engineering and standards compliance, helping engineering organizations adopt new processes, tools, and technologies to improve the efficiency and effectiveness of system and software development and testing while maintaining compliance with new and evolving technical standards. He holds a Bachelor of Science degree from Cornell University.

https://avionicsandtesting-innovations.com/speaker/steve-di-camillo/

https://ldra.wistia.com/medias/4xj5ibs6lz

https://ldra.wistia.com/medias/3cmh3vj9yl

# Agenda

LDRA introduction

Automotive software trends and challenges

The LDRA solution

Summary

# LDRA overview

Provider of Software Quality, Compliance Management & Testing Solutions

Established 1975

ISO 9001 certified company

Certified for use in safety related software development according to IEC 61508, EN 50128, ISO 26262, IEC 62304 & IEC 60880

Active participants in standards e.g. DO-178C, MISRA C/C++, CERT & ISO 26262

MISRA C & Secure C Training Courses

CERTIFICATE NO FS/71/220/15/0105 PAGE 1/1

LICENCE HOLDER
LDRA LTD
PORTSIDE, MONKS FERRY,
WIRRAL, CH41 5LH,
UNITED KINGDOM

MANUFACTURING PLANT
LDRA LTD
PORTSIDE, MONKS FERRY,
WIRRAL, CH41 5LH,
UNITED KINGDOM

PROJECT NO-ID: K1C2-AU01
LICENSED TEST MARK
CERT. REPORT NO.: K1C20003

Tested according to: IEC 61508:2010 Ed. 2.0, ISO 26262:2011, EN 50128:2011, IEC 60880:2006, IEC 62304:2006

Certified product(s): LDRA tool suite, LDRAunit, LDRArules, LDRAcover, LDRAlite

Model(s): Version 9.5

Technical Data and Parameter: Usable in development of safety related software acc. to:
- ISO 26262 up to ASIL D, TCL1 can be reached
- IEC 61508 up to SIL 4, class T2 tool
- EN 50128 up to SW-SIL 4, class T2 tool
- IEC 62304 up to SW safety Class C
- IEC 60880

Specific Requirements: The certificate is based on voluntarily tests. Any changes to the design, components or processing may require repetition of some parts of the qualification in order to retain the certification. The certificate report is an integral part of this certificate. The safety related application guidelines (refer to K1C20003) shall be maintained.

Certification Body for Functional Safety SGS-TÜV Saar GmbH
Munich, 04.11.2015
Gudrun Neumann

CERTIFICATE
No. Z10 16 09 84753 003

Holder of Factory(ies): LDRA Ltd., Portside, Monks Ferry, Wirral, Merseyside CH41 5LH, UNITED KINGDOM
Factory(ies): 84753
Certification Mark:
Product: Software Tool for Safety Related Development
Model(s): LDRA tool suite, LDRArules, LDRAcover, LDRAunit, LDRAlite
Parameters: The certified tools, classified T2, fulfil the requirements for support tools according to IEC 61508-3 and EN 50128. The tools are qualified to be used in safety-related software development according to IEC 61508, EN 50128 and ISO 26262. It is suitably validated for use in safety-related development according to IEC 62304(ed.1)
The test report is a mandatory part of this certificate.
Tested according to: IEC 61508-3(ed.2), ISO 26262-8:2011, EN 50128:2011
The product was tested on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition the certification holder must not transfer the certificate to third parties. See also notes overleaf.
Test report no.: LW85043C
Valid until: 2021-10-03
Date, 2016-10-04
(Guido Neumann)
Page 1 of 1

ZERTIFIKAT ◆ CERTIFICATE ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

TÜV SÜD Product Service GmbH · Zertifizierstelle · Ridlerstraße 65 · 80339 München · Germany

https://www.fuji-setsu.co.jp/products/LDRA/

# LDRA Standards Experience & Pedigree

## 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

Holds U.S. patents for a portable storage system and LDRA's embedded requirements verification system

## 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

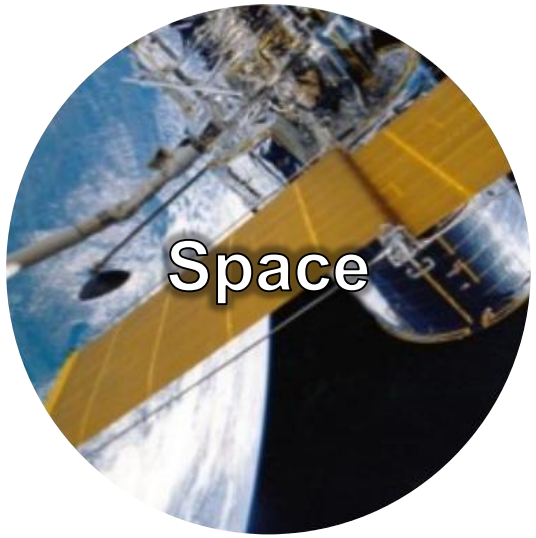
Member of BSI IST/15-/20 for Bodies of Knowledge and Professionalization

# Where we help









# Automotive software trends and challenges

# Automotive industry trends

**Innovation is causing market disruption**

- Increasingly, a vehicle's DNA is its software
- Requires learning fast, deciding fast, delivering fast

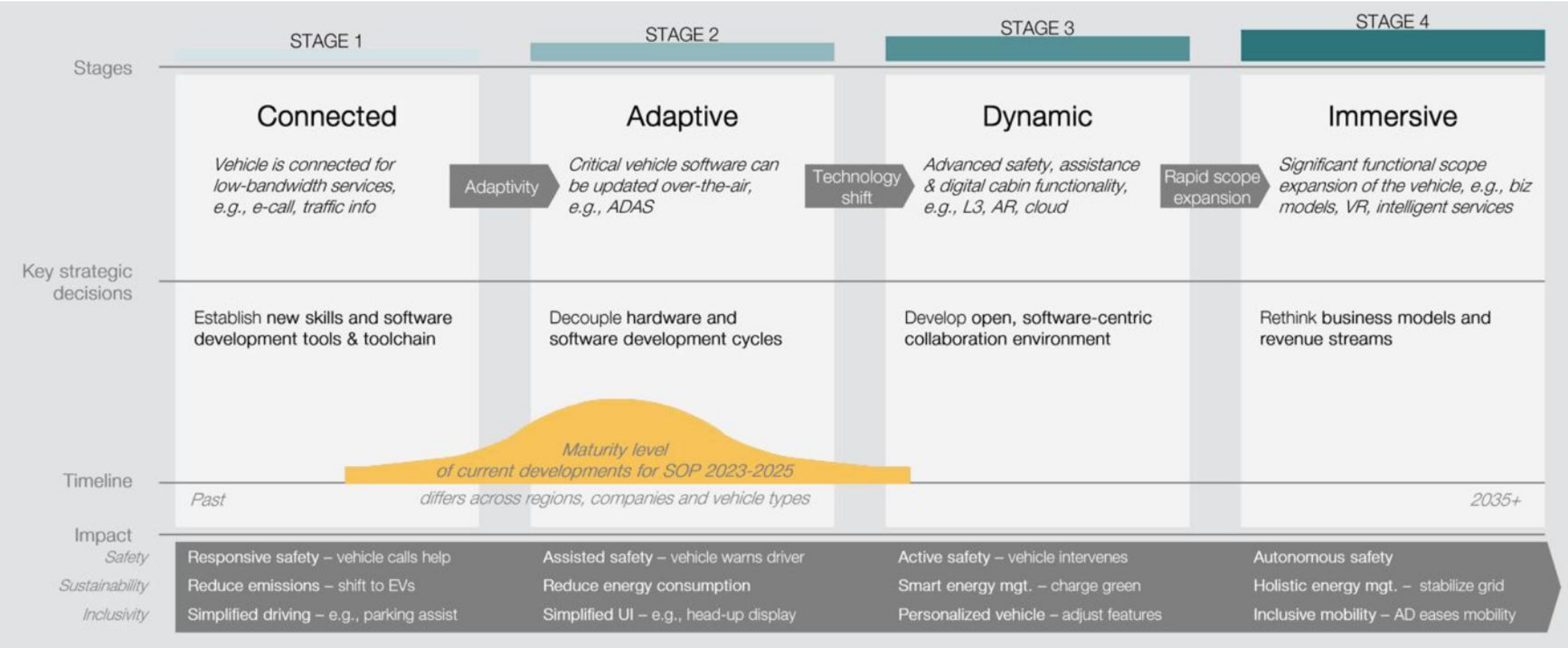
**Vehicles are becoming part of connected IoT solutions**

- More partners, more standards, more interfaces
- Inherently more complexity and failure modes

**Vehicles are becoming autonomous**

- More software, more technology, more 'intelligent'
- ADS and ADAS

# Software defined vehicle journey

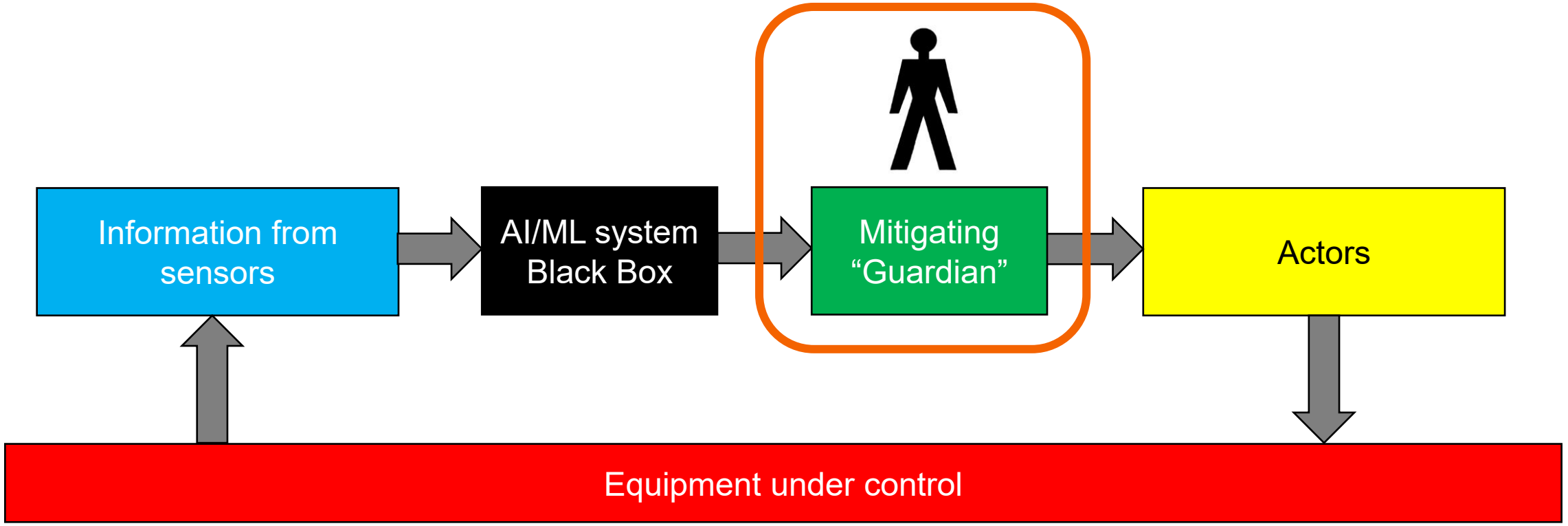



https://initiatives.weforum.org/drive-a/sdv

# Safety for AI/ML systems

Most approvals to date include some level of human intervention to provide mitigation

Human guardians can be replaced by conventional, deterministic applications developed in accordance with functional safety standards



# SAE Levels of driving automation

| Level | Name | DDT | Monitor Driving Environment | DDT Fallback Performance | ODD |
|---|---|---|---|---|---|
| 0 | No Automation | Driver | Driver | Driver | N/A |
| 1 | Driver Assistance | Driver and System | Driver | Driver | Limited |
| 2 | Partial Driving Automation | System | Driver | Driver | Limited |
| 3 | Conditional Driving Automation | System | System | Fallback Ready User becomes driver | Limited |
| 2 | High Driving Automation | System | System | System | Limited |
| 5 | Full Driving Automation | System | System | System | Unlimited |

Level 3 and higher are significantly more complicated and include many more safety and security requirements

Driver Performs Part or All of the DDT

ADS (“System”) Performs the Entire DDT (While Engaged)

# Safe automotive software – ISO 26262

Functional safety is:

The absence of unreasonable risk due to hazards caused by malfunctioning behaviour of electrical and/or electronic system systems

In other words, a functionally safe system must work correctly and fail in a predictable (safe) way


Safety by Nick Youngson CC BY-SA 3.0 Pix4free.org

https://www.fuji-setsu.co.jp/products/LDRA/Safety.html

# Secure automotive software – ISO/SAE 21434

Cybersecurity is:

The condition in which assets are sufficiently protected against threat scenarios to items of road vehicles, their functions and their electrical or electronic components

In other words, a secure system must work correctly and ensure vulnerabilities are mitigated

*Security threats can have safety implications*

https://www.fuji-setsu.co.jp/products/LDRA/CyberSecurity.html

# Business implications of safety and security

Compliance with safety and security standards for
Next Generation Automotive Software is a difficult challenge!

**Safe and secure systems and software design**

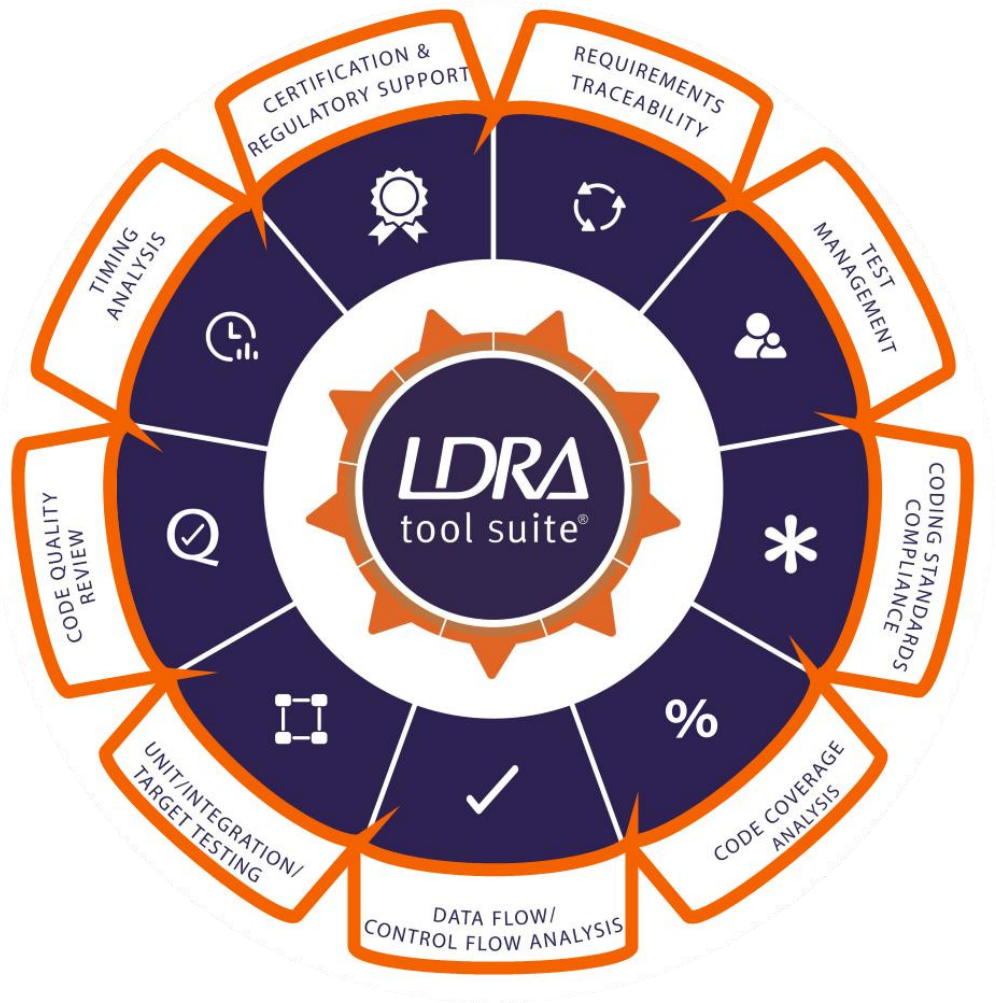
**HARA/TARA, safety/security analysis and traceability**

**Validation & verification management**

**Traceable change management**

# The LDRA solution

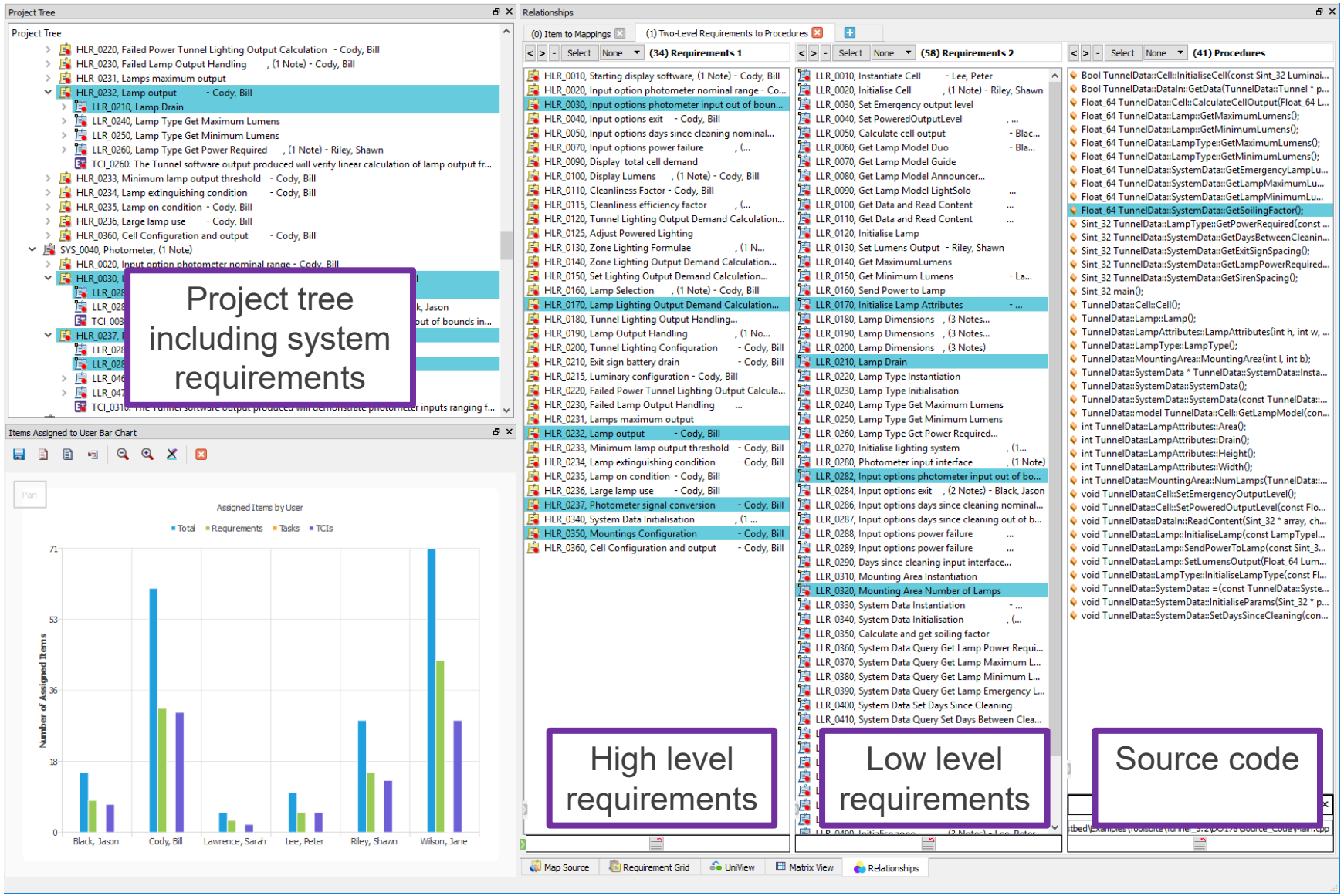
# Meeting the Challenges of ISO 26262 & ISO 21434 Compliance




https://www.fuji-setsu.co.jp/products/LDRA/#LDRA_options

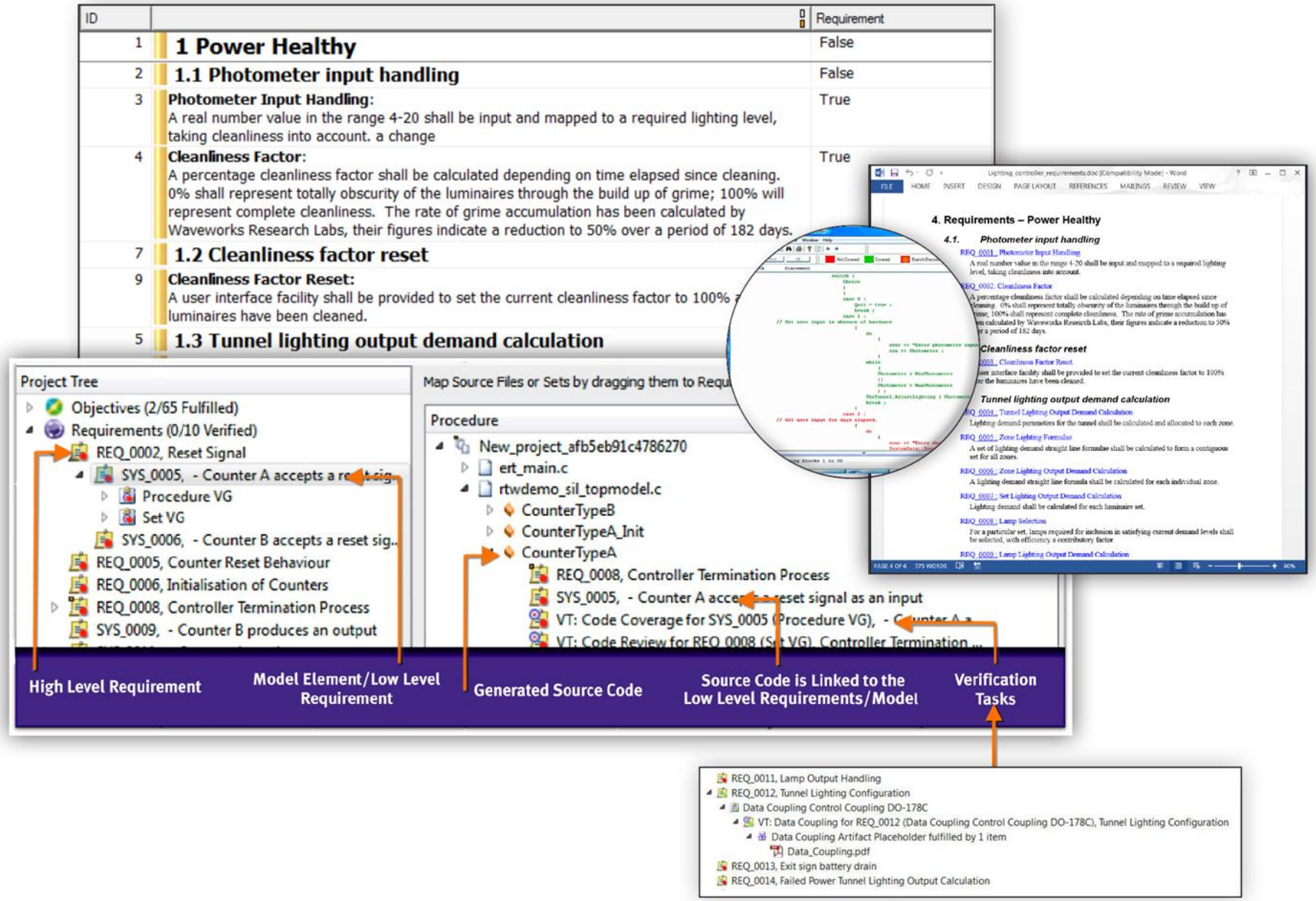
- Objectives tracking
- Requirements traceability
- Coding standards compliance & vulnerability analysis
- Data flow & control flow analysis
- Data & control coupling analysis, and Taint analysis
- Unit, Integration, Target testing
- Object Code Verification (OCV)
- Structural coverage, and Robustness & Fuzz testing
- Timing analysis
- Tool qualification
- Compliance management & reporting

# Requirements Traceability and Impact Analysis




Improve decision making and reduce costs using traceability and impact analysis

# Verification of requirements



# Change impact analysis

Assess impact of design changes

Manage the implementation of a design change

### 3.4.1. Exit Sign

Requirement Updated

HLR_0210: Exit sign battery drain

The system shall provide data to summarize emergency battery drain imposed by each individual siren & exit sign, and by all such provision in the system as a whole. The battery voltage needs to be verified before exit sign.

Links: SYS_0080

New Requirement

HLR_0211: Update Exit sign battery drain

The exit sign should be updated with an indicator. The exit LED shall be made ON.

Links: SYS_0080

| Number | Name | Body |
|---|---|---|
| HLR_0210 | Exit sign battery drain | The system shall provide data to summarize emergency battery drain imposed by each individual siren & exit sign, and by all such provision in the system as a whole. The battery voltage needs to be verified before exit sign. |

**Upstream Impact**

| Number | Name | Body |
|---|---|---|
| SYS_0080 | Sirens and Signs | The Tunnel lighting system shall include facilities for the handling of emergency exit signs and sirens. These should include provision to allow the basic configuration of the system itself, in particular: 1. the number of lamps which can be positioned in a particular ceiling section, and 2. the current drain placed on emergency battery provision by each model of lamp, and by the system as a whole |

**Downstream Impact**

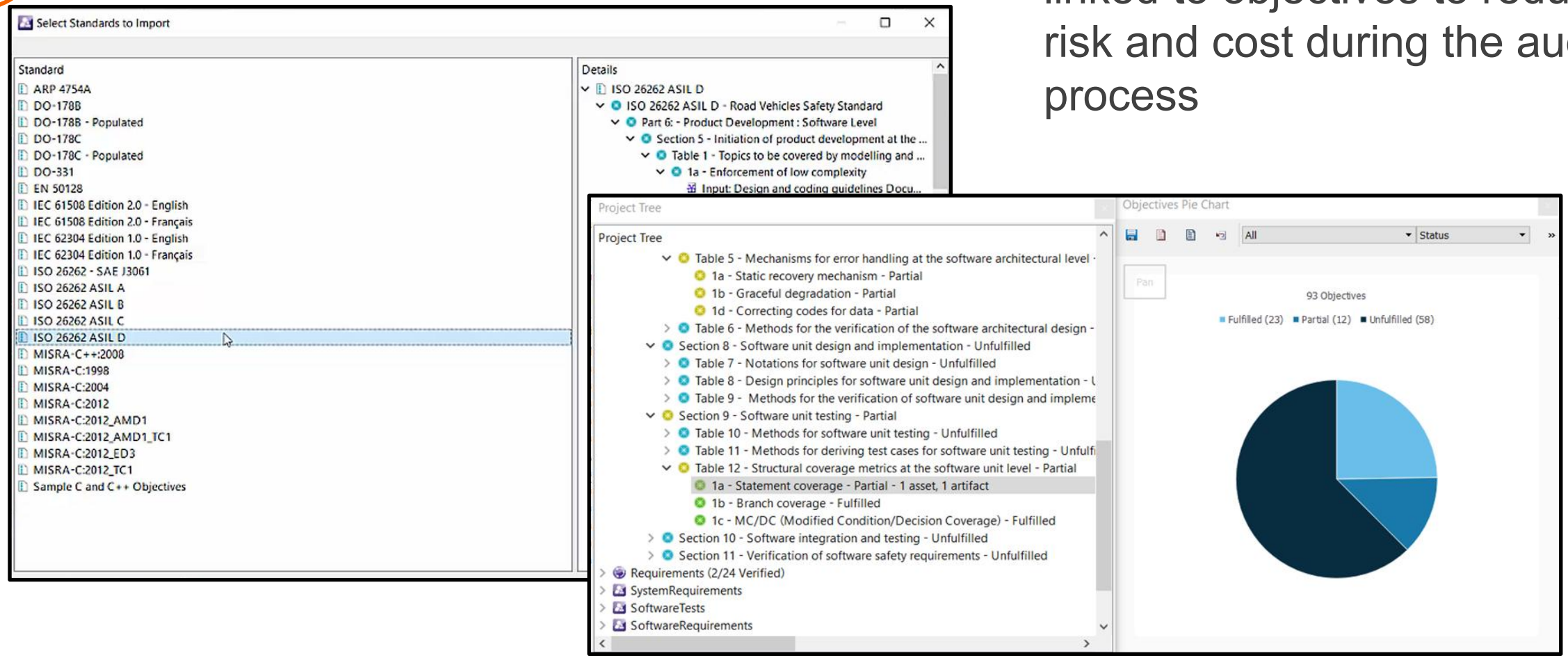
| Number | Name | Body |
|---|---|---|
| LLR_0380 | System Data Query Get Lamp Minimum Lumens | For each lamp type minimum lamp lumens shall be returned upon query |
| LLR_0390 | System Data Query Get Lamp Emergency Lumens | Emergency lamp lumens shall be returned upon query |
| LLR_0420 | System Data Query Get Exit Sign Spacing | Exit sign spacing shall be returned upon query |
| LLR_0430 | System Data Query Get Siren Spacing | Siren spacing shall be returned upon query |
| LLR_0530 | Zone assign emergency cell output | The zone class shall assign the emergency cell output levels to conserve emergency power supplies |
| LLR_0360 | System Data Query Get Lamp Power Required | For each lamp type power required shall be returned upon query |
| LLR_0370 | System Data Query Get Lamp Maximum Lumens | For each lamp type maximum lamp lumens shall be returned upon query |

**Modification**

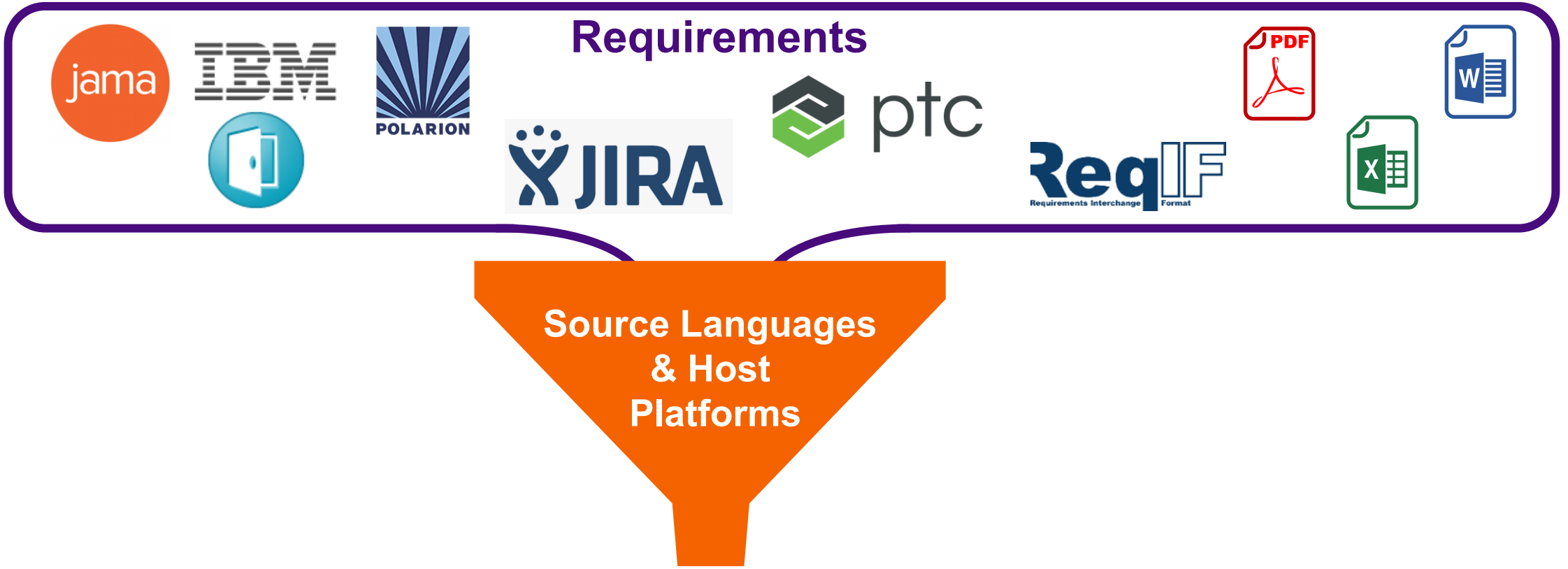
| Content Changed | Source Mapping Changed | Upstream/Downstream Changed | Status Changed |
|---|---|---|---|
| Yes | No | No | No |

# Objectives Tracking

Artifacts and assets can be linked to objectives to reduce risk and cost during the audit process



# Lifecycle Development Support

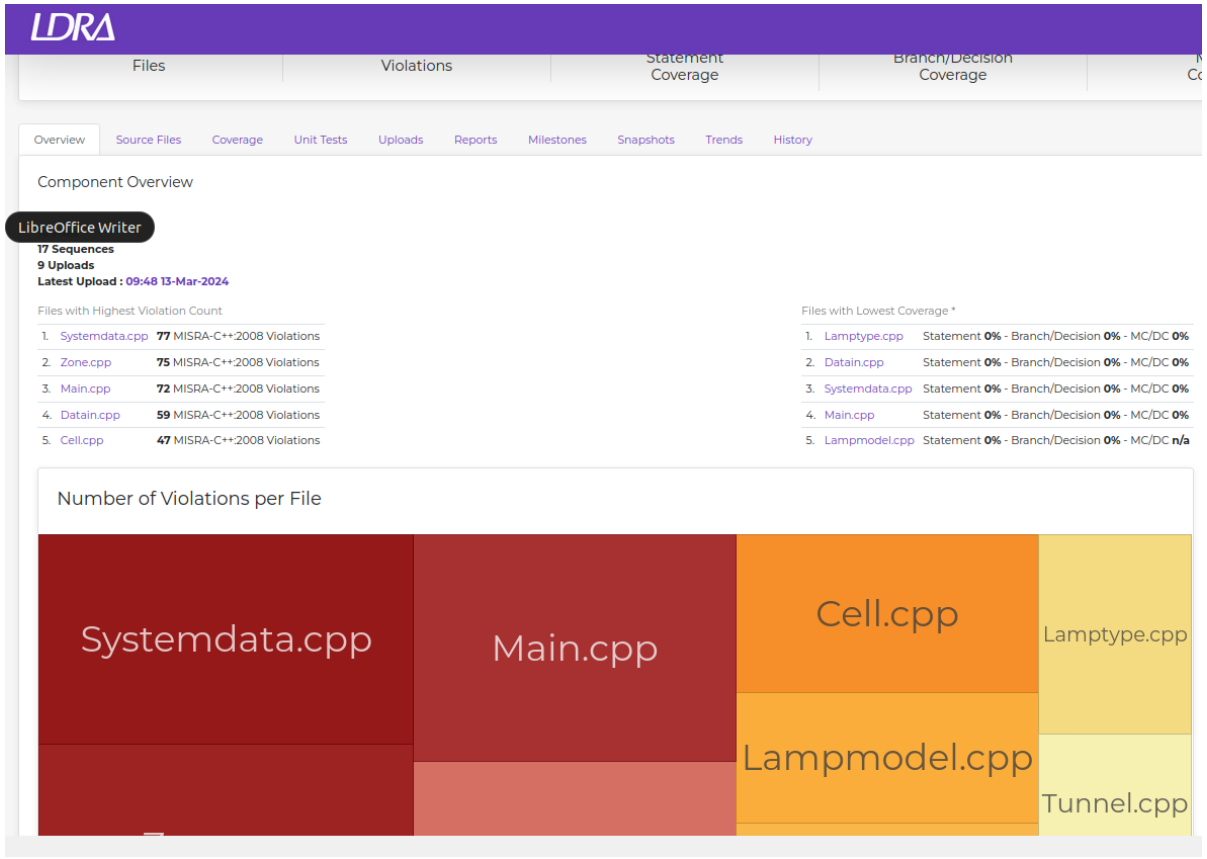


# Importance of static analysis

Static analysis plays a crucial role in ensuring the safety and security of software systems

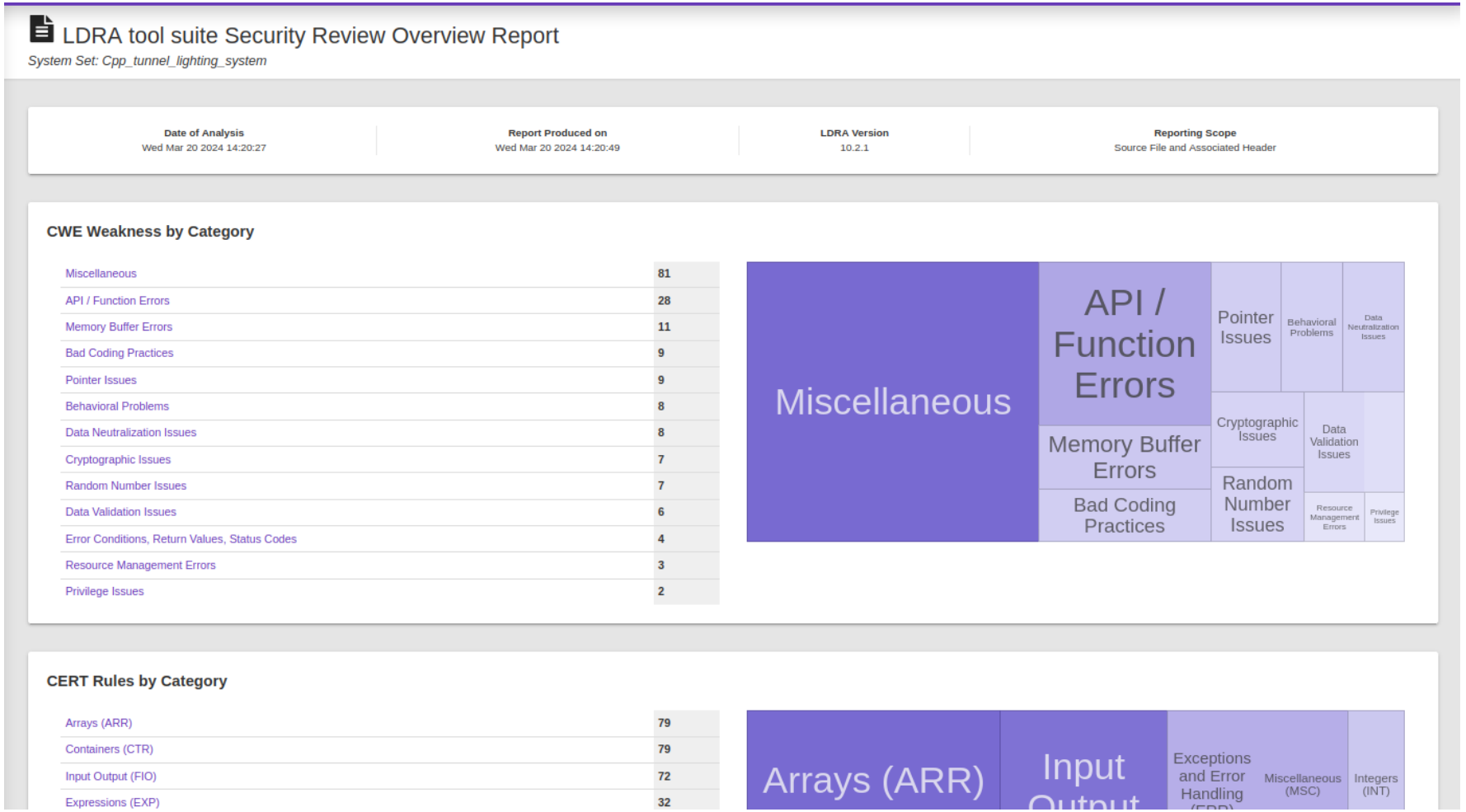
Objectives of Static Analysis:

- Early Detection of Vulnerabilities
- Comprehensive Code Review
- Identification of Code Smells and Anti-Patterns
- Enforcement of Coding Standard
- Integration with CI/CD
- Scalability and Efficiency
- Regulatory Compliance



# Static analysis identifies security vulnerabilities

Major Security Standards such as ISO/SAE 21434 recommend static analysis execution prior to any type of testing



LDRA tool suite Security Review Overview Report

*System Set: Cpp_tunnel_lighting_system*

| Date of Analysis | Report Produced on | LDRA Version | Reporting Scope |
|---|---|---|---|
| Wed Mar 20 2024 14:20:27 | Wed Mar 20 2024 14:20:49 | 10.2.1 | Source File and Associated Header |

**CWE Weakness by Category**

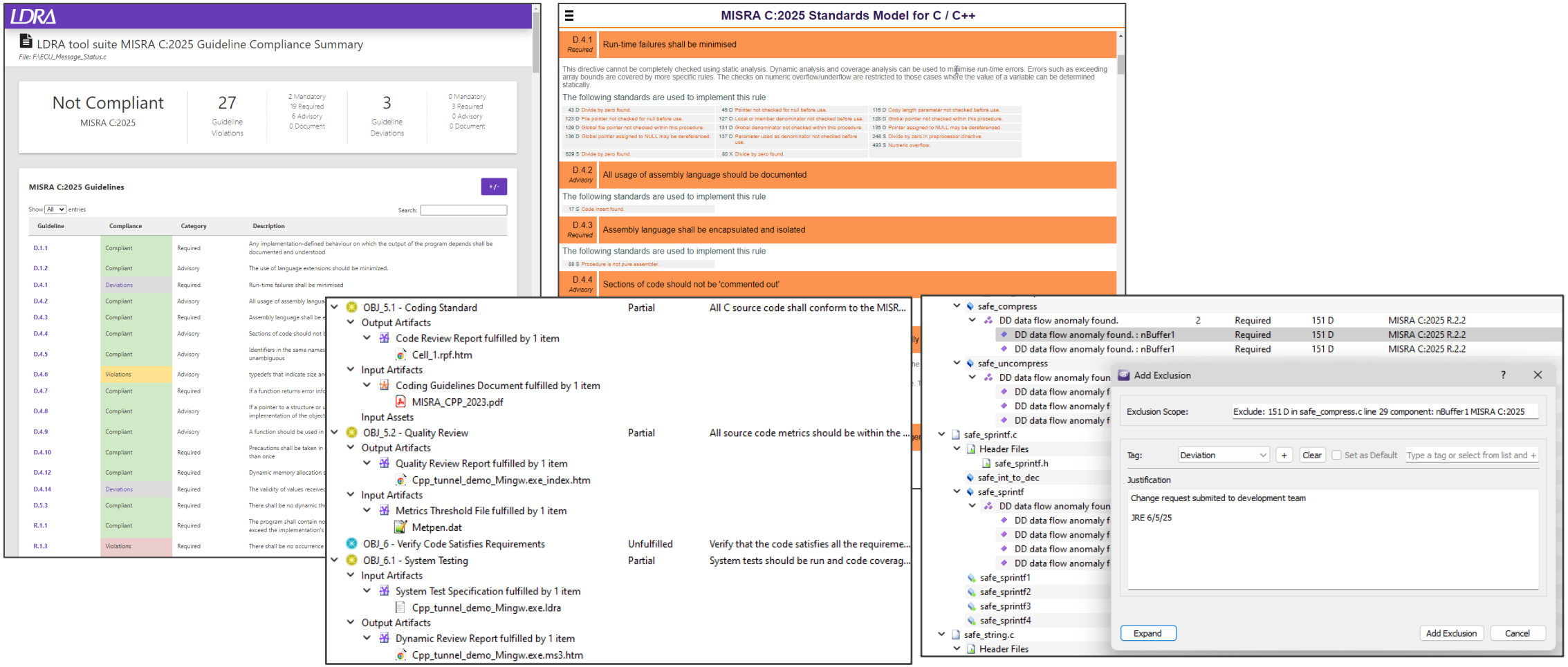
| | |
|---|---|
| Miscellaneous | 81 |
| API / Function Errors | 28 |
| Memory Buffer Errors | 11 |
| Bad Coding Practices | 9 |
| Pointer Issues | 9 |
| Behavioral Problems | 8 |
| Data Neutralization Issues | 8 |
| Cryptographic Issues | 7 |
| Random Number Issues | 7 |
| Data Validation Issues | 6 |
| Error Conditions, Return Values, Status Codes | 4 |
| Resource Management Errors | 3 |
| Privilege Issues | 2 |



**CERT Rules by Category**

| | |
|---|---|
| Arrays (ARR) | 79 |
| Containers (CTR) | 79 |
| Input Output (FIO) | 72 |
| Expressions (EXP) | 32 |

# Safety and security coding standards compliance




Manage deviation, removal, justification and documentation of rules

# Code complexity and quality metrics

- Table A.12 8 - Limited size and complexity of Functions, Subroutines and Methods - Fulfilled - 1 asset, 1 artifact
  - Code review report fulfilled by 1 item
    - Mingw_c_cashregister.frm.htm
  - Design and coding guidelines document fulfilled by 1 item
    - Complexity_Guidelines from Acme_coding_standard.doc

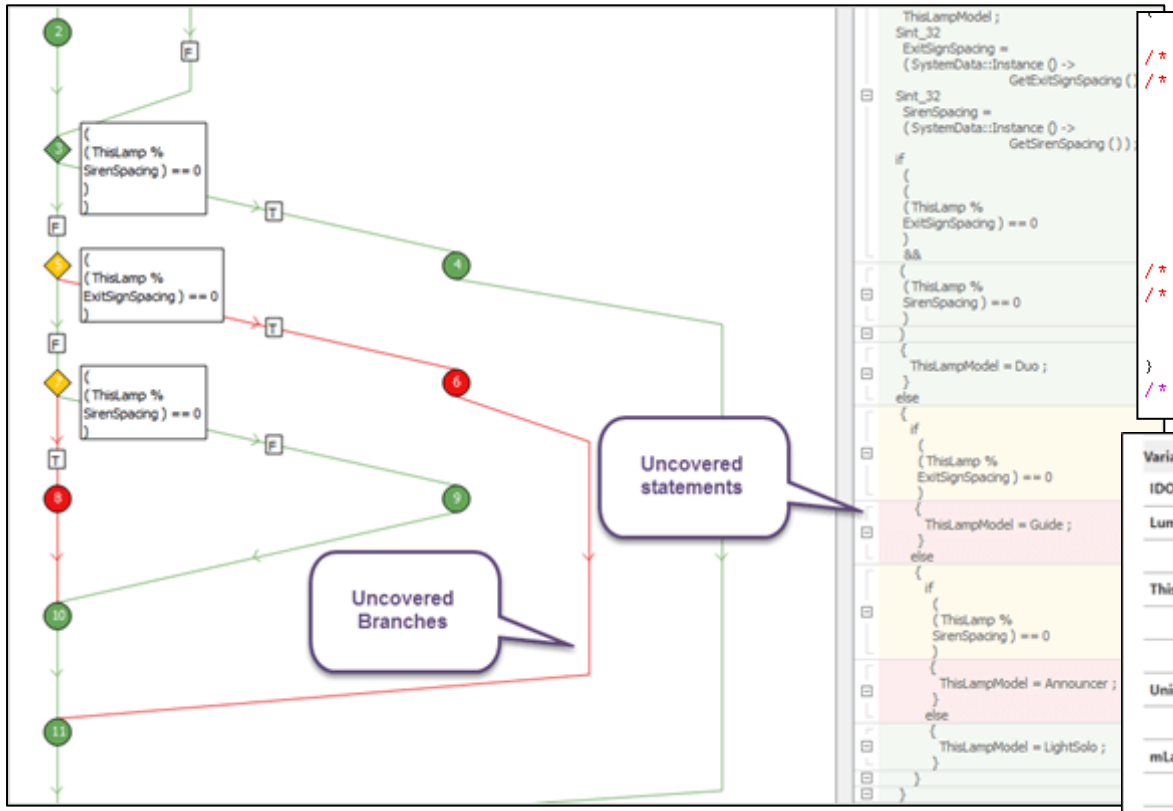
Code Quality View (Maintainability)

| 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) |
| LzmaEnc_Init | 9 | 32 : (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% |
| 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 |
| 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 |
| Knots | 23 |

# Data & control flow visualization and analysis




Control flow graph

```
   uint32_t pulse=0U;
/* (M) DATAFLOW VIOLATION    : 70 D : DU anomaly, variable value is not used. : pulse :      40F
/*    See also line 17 DataFlow.c(DATAFLOW) */
   uint32_t iter;

   if ( cycles > 0U )
   {
      for ( iter=0U; iter<cycles; iter++ )
      {
         pulse++;
/* (M) DATAFLOW VIOLATION    : 70 D : DU anomaly, variable value is not used. : pulse :      57T
/*    See also line 17 DataFlow.c(DATAFLOW) */
      }
   }
}
/* (O) DATAFLOW VIOLATION    :  7 D : DU  data flow anomalies found. */
```

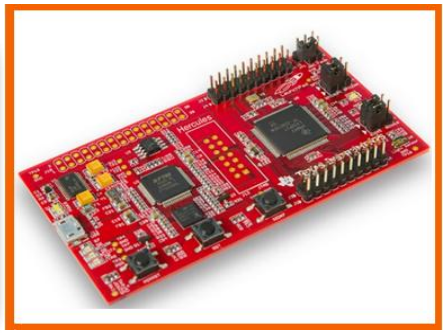
*pulse* is Defined but Unused

| Variable Name | File | Procedure | Type Code | Attribute Code | Used on lines... |
|---|---|---|---|---|---|
| IDOffset | Cell.cpp | TunnelData::Cell::InitialiseCell | Global | Reference | 55 |
| LuminaireSetSize | Cell.cpp | TunnelData::Cell::InitialiseCell | Parameter | Declaration | 32 |
| | | | Parameter | Reference | 40 |
| ThisLamp | Cell.cpp | TunnelData::Cell::InitialiseCell | Local | Declaration | 48 |
| | | | Local | Reference | 54 55 55 55 56 |
| | | | Local | Definition | 48 56 |
| UniqueCellID | Cell.cpp | TunnelData::Cell::InitialiseCell | Parameter | Declaration | 32 |
| | | | Parameter | Reference | 55 78 |
| mLampTypeID | Cell.cpp | TunnelData::Cell::InitialiseCell | Member | Reference | 55 63 |
| | | | Member | Definition | 54 |
| pLampTypeIDs | Cell.cpp | TunnelData::Cell::InitialiseCell | Parameter | Declaration | 32 |
| | | | Parameter | Reference | 54 |

Data flow reporting

# Unit and integration testing on host/target

- 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
    - System Design Specification fulfilled by 1 item
      - Software_Design_Document.doc
    - Design and coding guidelines Document fulfilled by 1 item
      - C_C++_Coding_Standards_and_Guidelines.pdf



Automated test case generation of Requirements-Based Tests and Robustness Tests

Test Case View

| Test Case | Regression P / F | Procedure |
|---|---|---|
| Tc 1 | PASS | integer_to_ascii |
| Tc 2 | PASS | integer_to_ascii |
| Tc 3 | PASS | integer_to_ascii |
| Tc 4 | PASS | integer_to_ascii |
| Tc 5 | PASS | integer_to_ascii |
| Tc 6 | PASS | integer_to_ascii |
| Tc 7 | PASS | integer_to_ascii |
| Tc 8 | PASS | integer_to_ascii |
| Tc 9 | PASS | integer_to_ascii |

Variable I/O View

| Value | Name | Type | Use | Regression Analysis |
|---|---|---|---|---|
| I 123 | value | u32 | Input parameter applied through local | Assigned |
| I 5 | digits | u8 | Input parameter applied through local | Assigned |
| I 0 | blanks | u8 | Input parameter applied through local | Assigned |
| O '0' | itoa_str[0] | s8 | Output global | Compare + Write |
| O '0' | itoa_str[1] | s8 | Output global | Compare + Write |
| O '1' | itoa_str[2] | s8 | Output global | Compare + Write |
| O '2' | itoa_str[3] | s8 | Output global | Compare + Write |
| O '3' | itoa_str[4] | s8 | Output global | Compare + Write |
| O '0' | itoa_str[5] | s8 | Output global | Compare + Write |
| O '0' | itoa_str[6] | s8 | Output global | Compare + Write |
| O 0 | itoa_str[7] | s8 | Output global | Compare + Write |

# Target license package

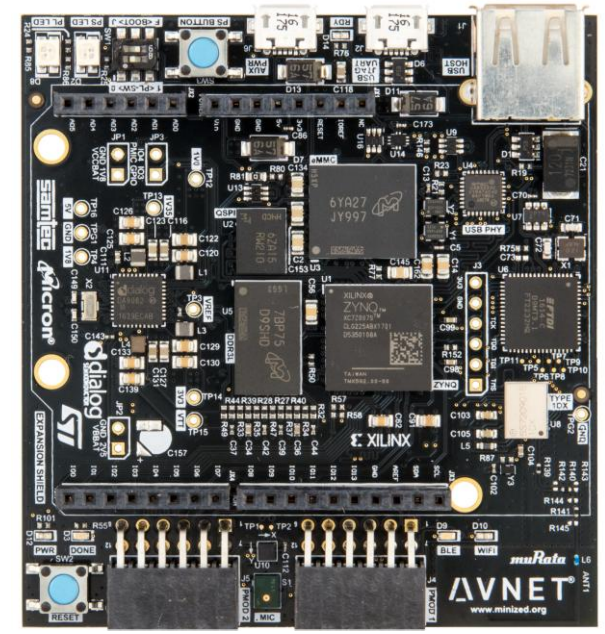
Pre-configured files to use LDRA tools with a specific compiler and target out of the box

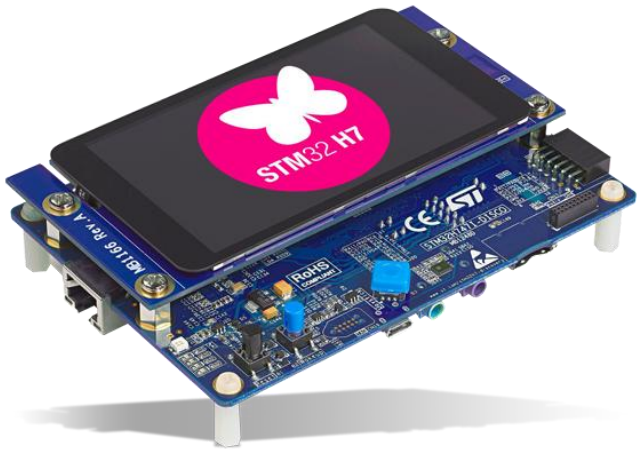
Consistent and professional look and feel

- Fully automated
- Getting Started Tutorial
- Example projects
- TBmanager project

Hundreds of combinations of compiler/target available

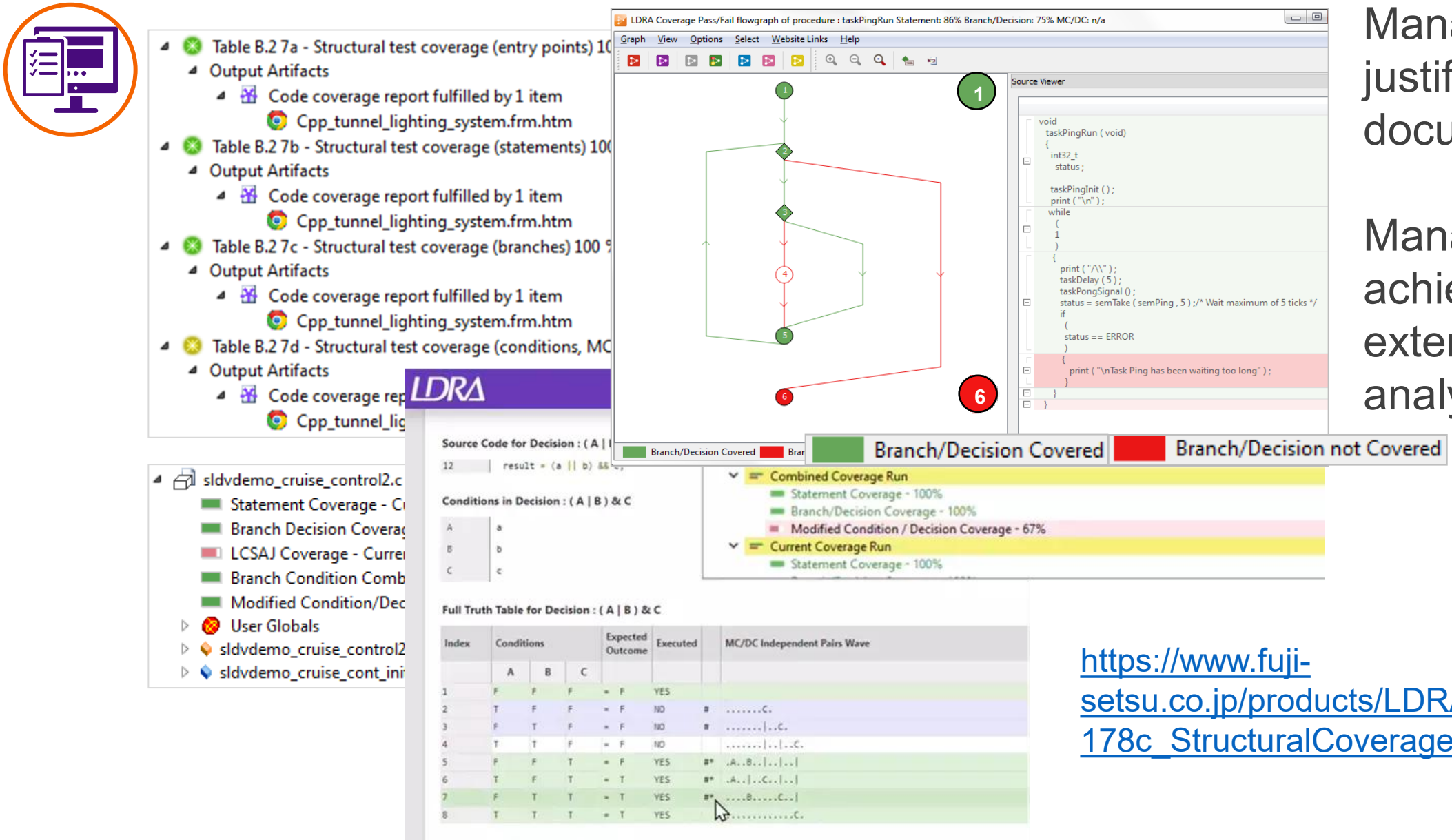
- New configurations can be quickly and easily created




https://ldra.com/products/target-licence-packages-tlp/#TLP2

# Measuring structural coverage




Manage coverage justifications and documentation

Manage coverage achieved through external coverage analysis

https://www.fuji-setsu.co.jp/products/LDRA/do-178c_StructuralCoverageAnalysis.html

# Data & control coupling analysis and coverage

**Data Coupling (Out from Procedure)**

| Variable | Line | Type | | Coupled To Parameter (Alias) | Procedure | Line | File |
|---|---|---|---|---|---|---|---|
| LampTypeID **mThisLampTypeID** | 41 | Member | --> | const LampTypeID **ThisLampTypeID** | TunnelData::SystemData::GetLampPowerRequired | 92 | Systemdata.cpp |
| Float_64 **LumensRequired** | 41 | Parameter | --> | const Float_64 **LumensRequired** | TunnelData::SystemData::GetLampPowerRequired | 92 | Systemdata.cpp |

**Data Coupling (In to Procedure)**

| Variable | Procedure | Line | File | Type | | Coupled To Parameter (Alias) | Line |
|---|---|---|---|---|---|---|---|
| Float_64 **LumensDemand** | TunnelData::Cell::SetPoweredOutputLevel | 159 | Cell.cpp | Array Index of Local | --> | Float_64 **LumensRequired** | 33 |

**Dynamic Data Flow Coverage for Data Coupling Variables**

data access not exercised

| Variable Name | File | Procedure | Type Code | Attribute Code | Used on lines... |
|---|---|---|---|---|---|
| **LumensRequired** | Lamp.cpp | TunnelData::Lamp::SetLumensOutput | Parameter | Declaration | 33 |
| | | | Parameter | Reference | 36 39 ***** 41 |
| **mThisLampTypeID** | Lamp.cpp | TunnelData::Lamp::SetLumensOutput | Member | Reference | 41 |

US 20230048792A1

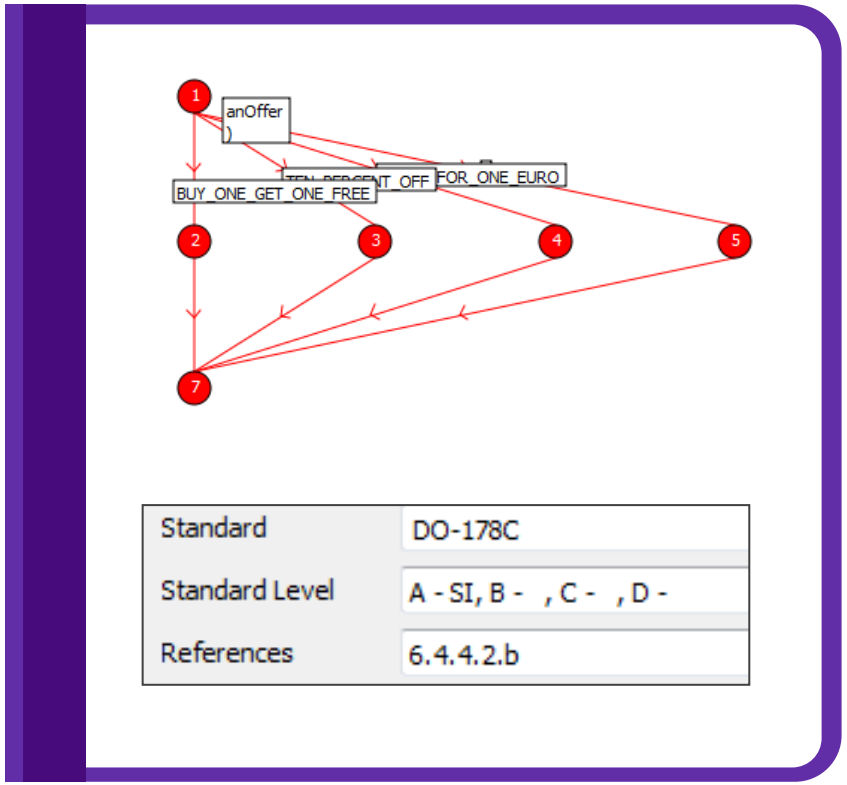
(10) International Publication Number

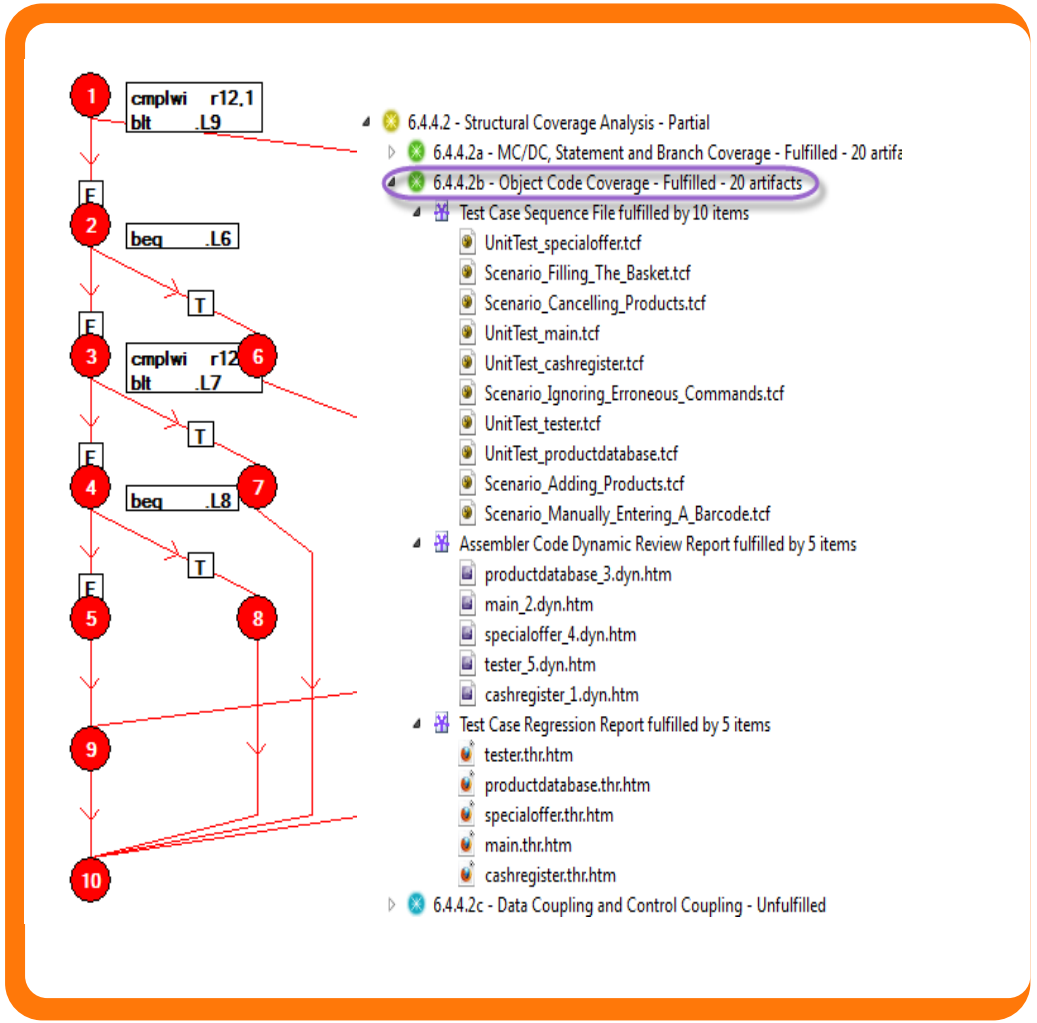
WO 2022/256103 A1

US011474927B1

https://www.fuji-setsu.co.jp/products/LDRA/resources.html#DCCC

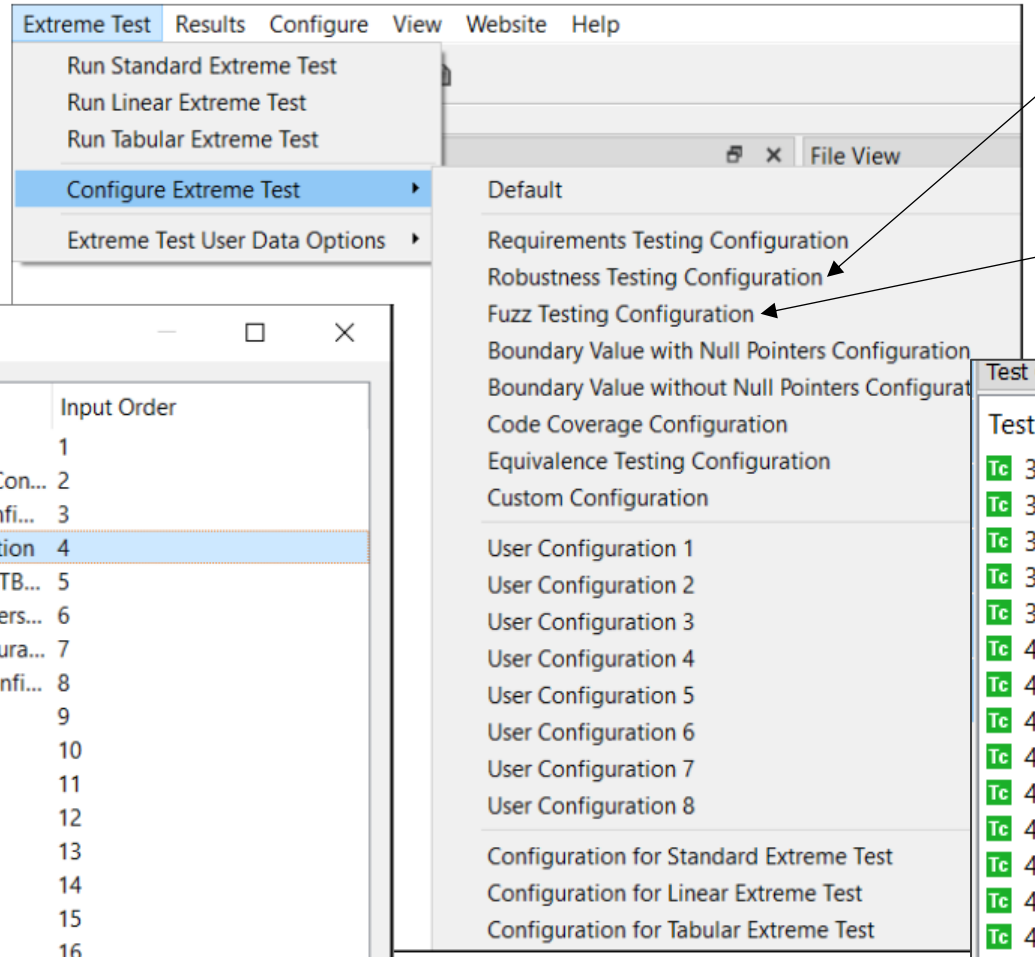
# Object code verification

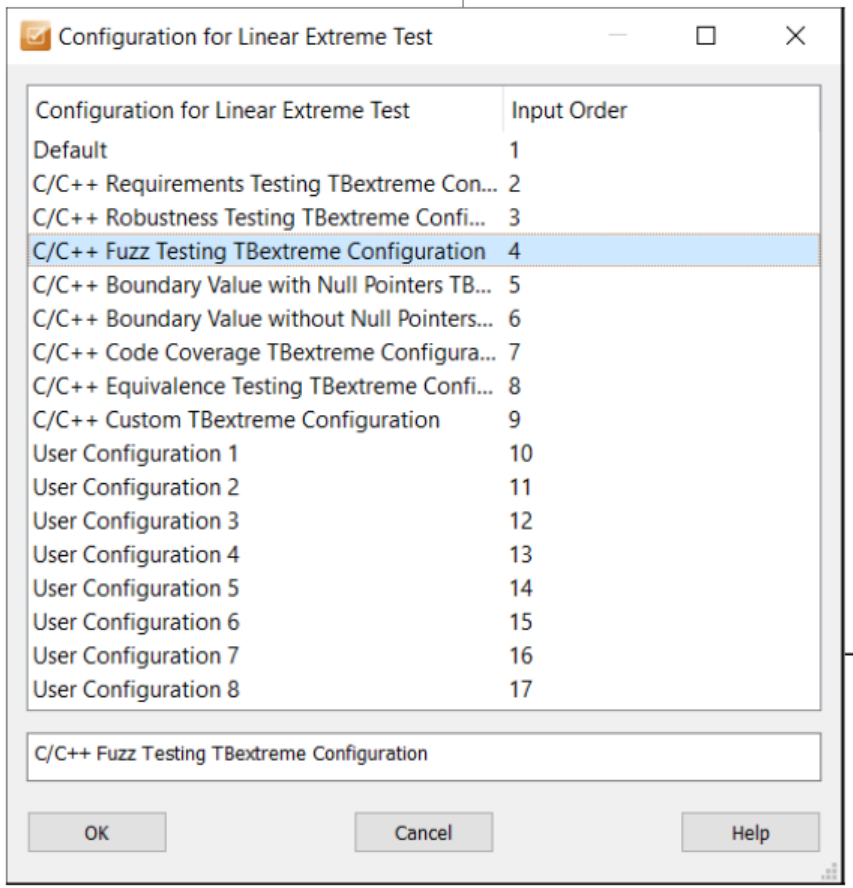


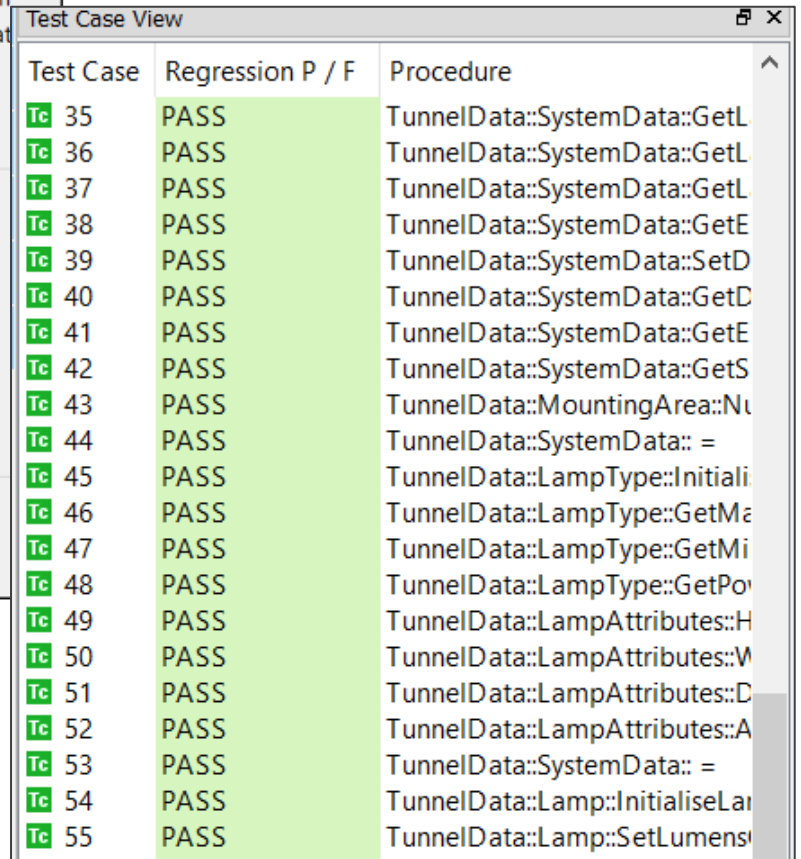




https://www.fuji-setsu.co.jp/products/LDRA/resources.html#OCV

# Automatic test case generation/robustness & fuzz testing



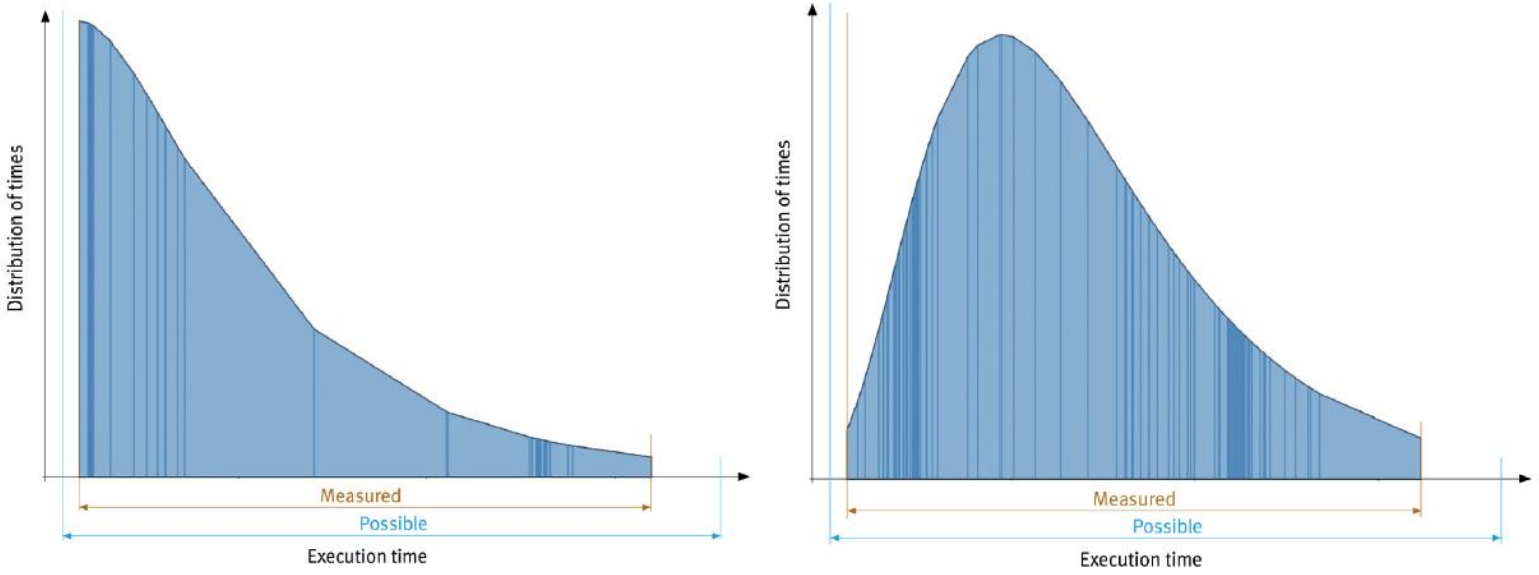




Automates robustness testing to verify system resilience against unexpected inputs and boundary values.

Performs fuzz testing by injecting malformed data to expose vulnerabilities and bugs.

# Timing analysis including WCET




**Timing Summary**

| | |
|---|---|
| Number of Tests | 100 |
| Best-Case Execution Time | 57321953.100000 |
| Worst-Case Execution Time | 338863903.400000 |
| Minimal Observed Execution Time | 63691059 - Test Case 1 (Rep 1) |
| Maximal Observed Execution Time | 308058094 - Test Case 1 (Rep 2) |
| Mean Observed Execution Time | 115596348 |

**Timing Summary**

| | |
|---|---|
| Number of Tests | 100 |
| Best-Case Execution Time | 59658020.100000 |
| Worst-Case Execution Time | 495044356.400000 |
| Minimal Observed Execution Time | 66286689 - Test Case 1 (Rep 63) |
| Maximal Observed Execution Time | 450040324 - Test Case 1 (Rep 38) |
| Mean Observed Execution Time | 228836793 |

Run many unit/Integration test cycles

Generate interference across shared resources

Visualize the distribution of execution times

https://www.fuji-setsu.co.jp/products/LDRA/resources.html#WCET

# Parallel security and safety objectives compliance

Static analysis can be used to satisfy code review objectives for both safety and security in  parallel

Dynamic analysis such as structural coverage, robustness testing, data coupling analysis, and WCET measurements can also satisfy objectives for safety and security

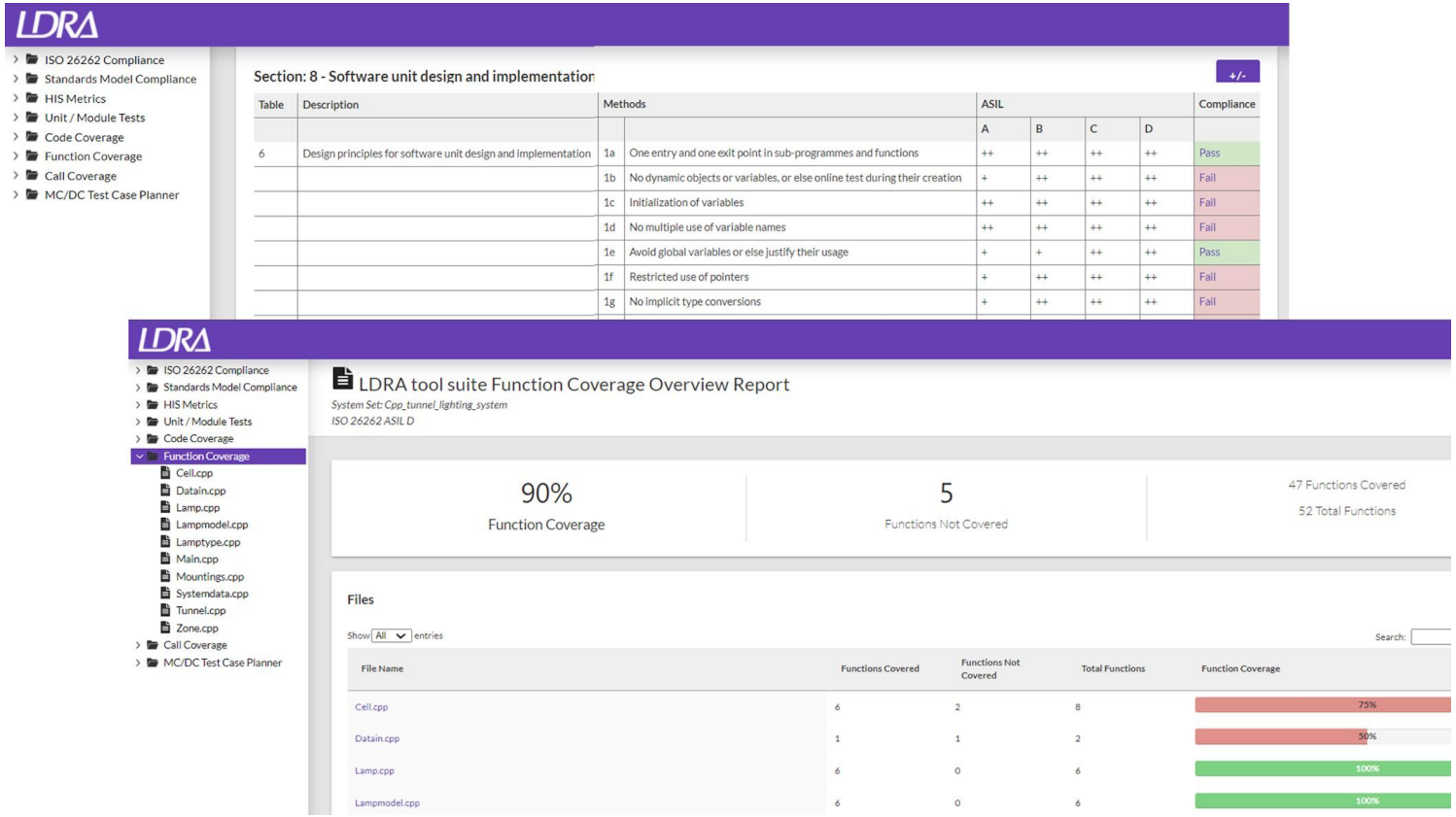
| | | | | | |
|---|---|---|---|---|---|
| TunnelData::Cell::GetLampModel | | | | | |
| Local or member denominator not checked before use. | 3 | | Rule | 127 D | CWE-3.4 129,369 |
| Local or member denominator not checked before use. : SirenSpacing | | | Rule | 127 D | CWE-3.4 129,369 |
| Local or member denominator not checked before use. : SirenSpacing | | | Rule | 127 D | CWE-3.4 129,369 |
| Local or member denominator not checked before use. : ExitSignSpacing | | | Rule | 127 D | CWE-3.4 129,369 |

| | | | | |
|---|---|---|---|---|
| TunnelData::Cell::GetLampModel | | | | |
| Remainder of % op could be negative. | 4 | Document | 584 S | MISRA C:2023 D.1.1 |
| Local or member denominator not checked before use. | 3 | Required | 127 D | MISRA C:2023 D.4.1,D.4.14 |
| No brackets to then/else. (analysed w. MISRA-C++:2008) | 4 | Required | 12 S | MISRA C:2023 R.15.6 |

# Certification reporting

Publish analysis and test results as indexed reports

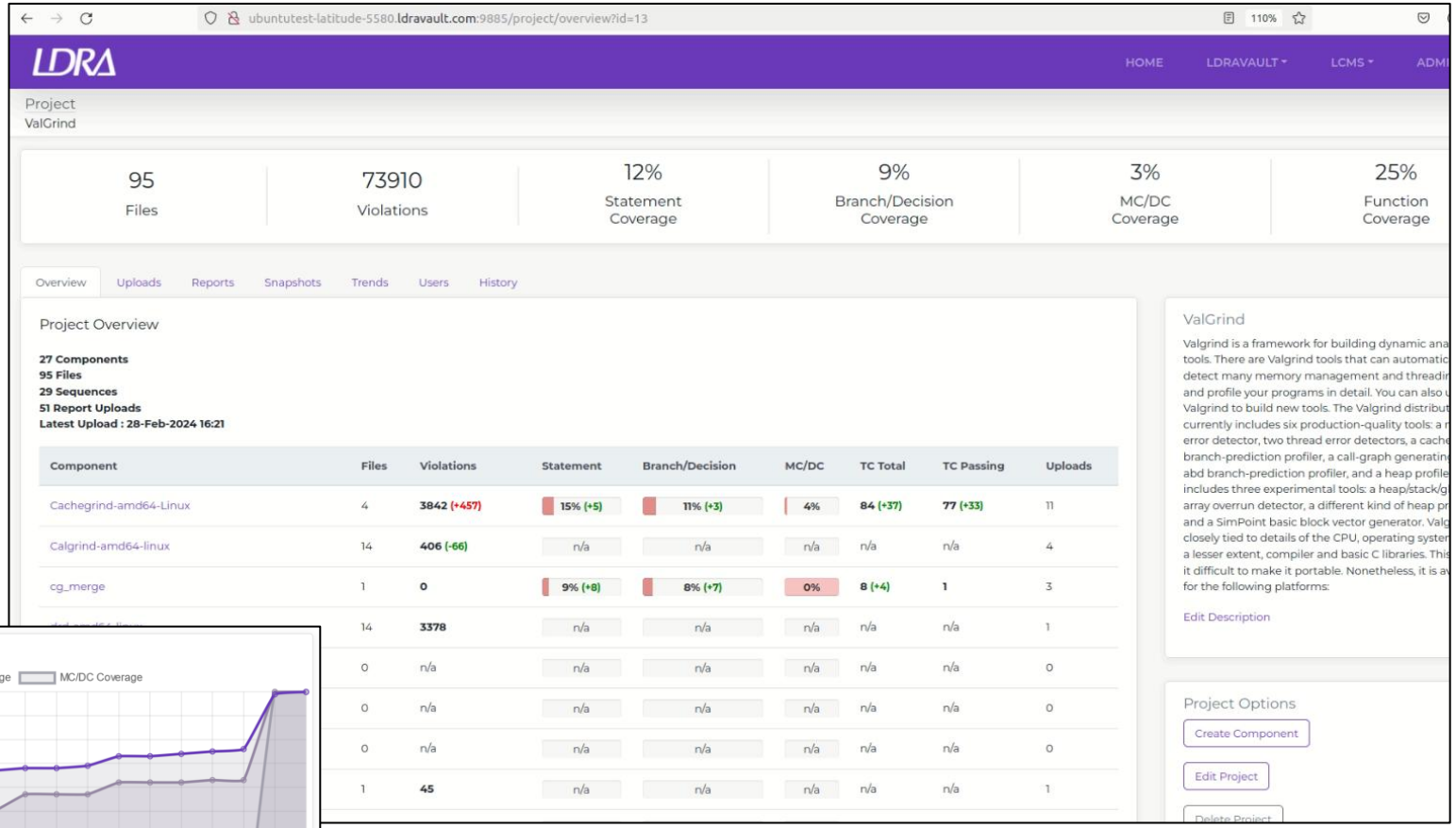
Reports fulfill safety and security standards objectives

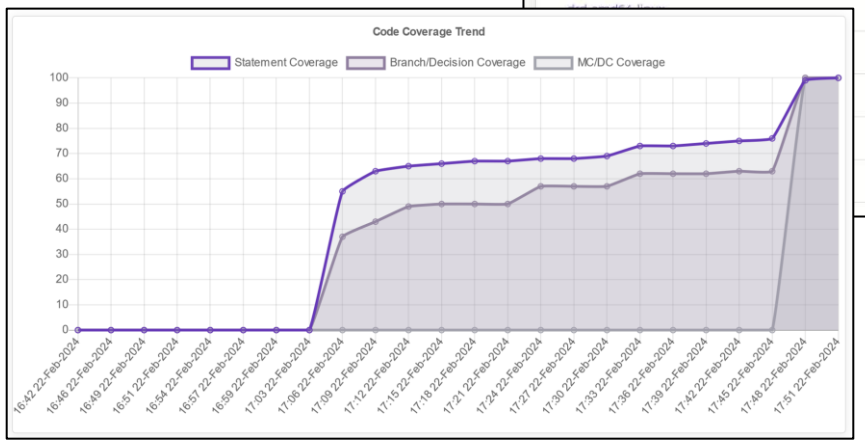


# Scalable software certification

Efficiently manage large sets of software certification artifacts

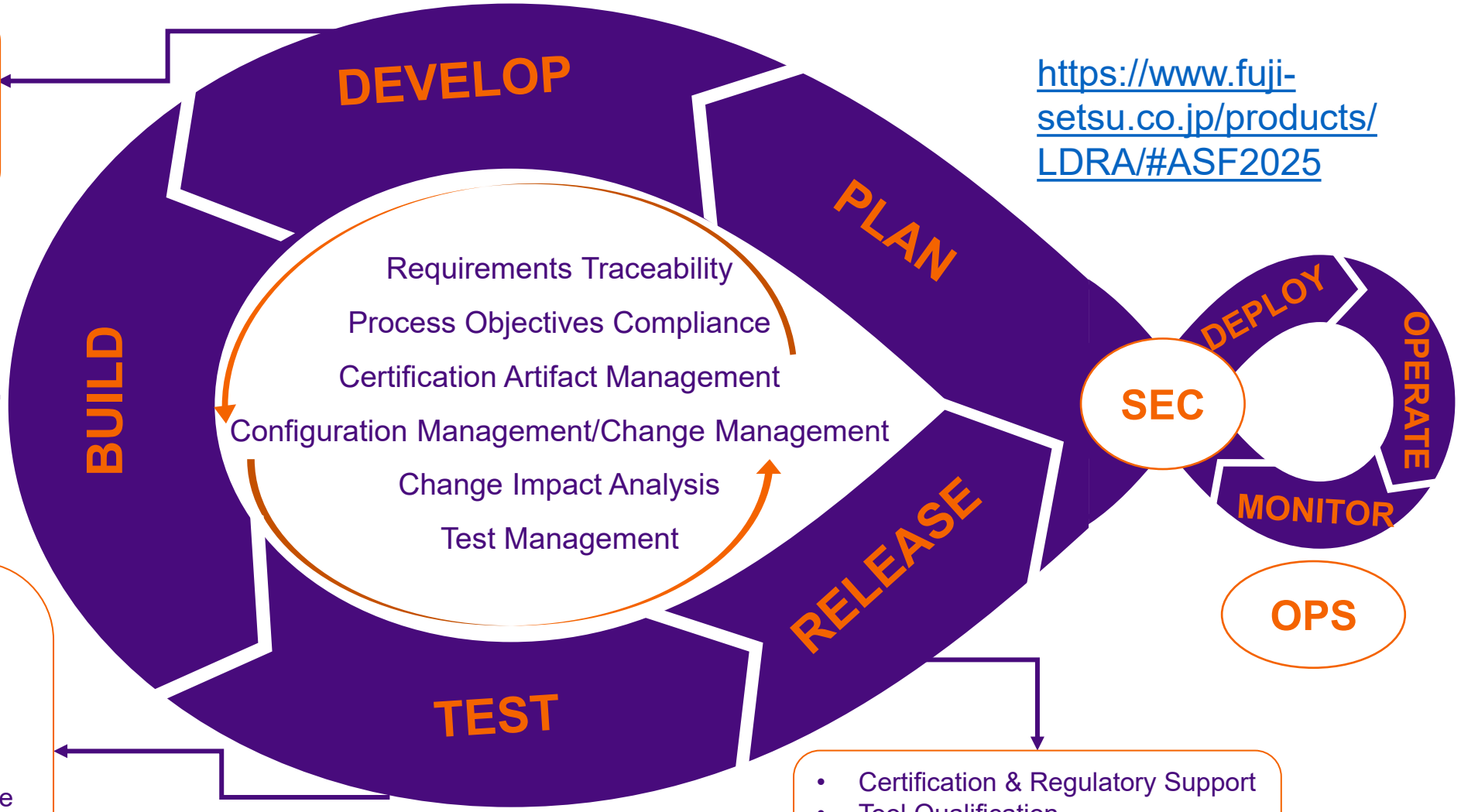
Leverage LDRA's proven analysis capabilities



# CI/CD and DevSecOps

- Coding Standards Compliance
- Code Quality Analysis
- Taint/Vulnerability Analysis
- Data & Control Flow Analysis
- Software Quality Reporting




https://www.fuji-setsu.co.jp/products/LDRA/#ASF2025

- Target Testing
- Robustness Testing/Fuzzing
- Requirements-Based Testing
- Timing Analysis
- Structural Coverage Analysis
- Source/Object Code Coverage
- Function Coverage & Call Coverage
- Dynamic Data Flow & Control Flow Coverage
- Software Verification Reporting

- Certification & Regulatory Support
- Tool Qualification
- Industry Standards Compliance Reporting

# ISO 26262 QM & ASIL A to C

ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

Product Service

**CERTIFICATE**

**No. Z10 084753 0006 Rev. 01**

**Holder of Certificate:** LDRA Ltd.
Portside, Monks Ferry
Wirral, Merseyside CH41 5LH
UNITED KINGDOM

**Certification Mark:**

**Product:** Software Tool for Safety Related Development

**Model(s):** LDRA tool suite
LDRArules
LDRAcover
LDRAunit
LDRAlite

**Parameters:** The certified tools fulfills the requirements for support tools classified T2 according to IEC 61508-3 and EN 50128. The tools are qualified to be used in safety-related software development according to IEC 61508, EN 50128 and ISO 26262. It is suitably validated for use in safety-related development according to IEC 62304. The test report is a mandatory part of this certificate.

**Tested according to:**
IEC 61508-3:2010
IEC 62304:2006
IEC 62304:2006/AMD1:2015
ISO 26262-8:2018
EN 50128:2011/AMD2:2020

The product was tested on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition the certification holder must not transfer the certificate to third parties. This certificate is valid until the listed date, unless it is cancelled earlier. All applicable requirements of the Testing, Certification, Validation and Verification Regulations of TÜV SÜD Group have to be complied. For details see: www.tuvsud.com/ps-cert

**Test report no.:** LW85043C

**Valid until:** 2029-04-18

**Date,** 2024-04-23

( Christian Dirmeier )

Page 1 of 1
TÜV SÜD Product Service GmbH • Certification Body • Ridlerstraße 65 • 80339 Munich • Germany

TÜV®

SGS TÜV SAAR

**CERTIFICATE NO** FS/71/220/23/1048 **PAGE 1/1**

**LICENCE HOLDER & MANUFACTURER**

LDRA Ltd
Portside, Monks Ferry,
Wirral, CH41 5LH,
United Kingdom

| PROJECT NO/-ID | LICENSED TEST MARK | CERT. REPORT NO. |
|---|---|---|
| M15F-AU05 | SGS TÜV SAAR FUNCTIONAL SAFETY APPROVED | M15F0010 is an integral part of this certificate. |

**Certified product(s)** LDRA tool suite
LDRAunit
LDRArules
LDRAcover
LDRAlite

Version 10.0.3 and 10.1.0

**Tested according to** IEC 61508-3:2010; clause 7.4.4
ISO 26262-8:2018; clause 11.4.9
EN 50128:2011
IEC 60880:2006
IEC 62304:2015

**Technical Data and Parameter** Suitable for development of safety-related software acc. to:

- ISO 26262 up to ASIL D,
- IEC 61508 up to SIL 4, class T2 tool
- EN 50128 up to SIL 4, class T2 tool
- IEC 62304 up to SW safety Class C
- IEC 60880 for category A functions

Certification Body
for Functional Safety &
Cyber Security
SGS-TÜV Saar GmbH

Munich, Mar 08, 2023
Gudrun Neumann

CERTIFICATE

https://www.fuji-setsu.co.jp/products/LDRA/resources.html#iso26262ToolQualification

# Conclusion

## Challenges of certifying next-generation automotive software

- Rapid evolution of SDV technology
- Safety and security concerns
- Growth in software content, including safety and security functions

## Overcoming the challenges with LDRA

- Flexible and scalable proven in use solutions
- Designed to meet the highest safety and security standards
- Supports DevSecOps and continuous integration platforms

# Contact Us

ldra.com

info@ldra.com

# Follow Us

LDRA Limited

LDRA

FUJI SETSUBI

FUJI SETSUBI

# LDRA　スタンダード認証支援テストツール

https://www.fuji-setsu.co.jp/products/LDRA/

富士設備工業(株)電子機器事業部
https://www.fuji-setsu.co.jp