Verifying Security in a Safety Context

Airworthiness and DO-326A/DO-356A

Cary Bryczek

Jama Software

Director of A&D Solutions

Ehsan Salehi

LDRA

Senior Field Application Engineer

jama software

LDRA

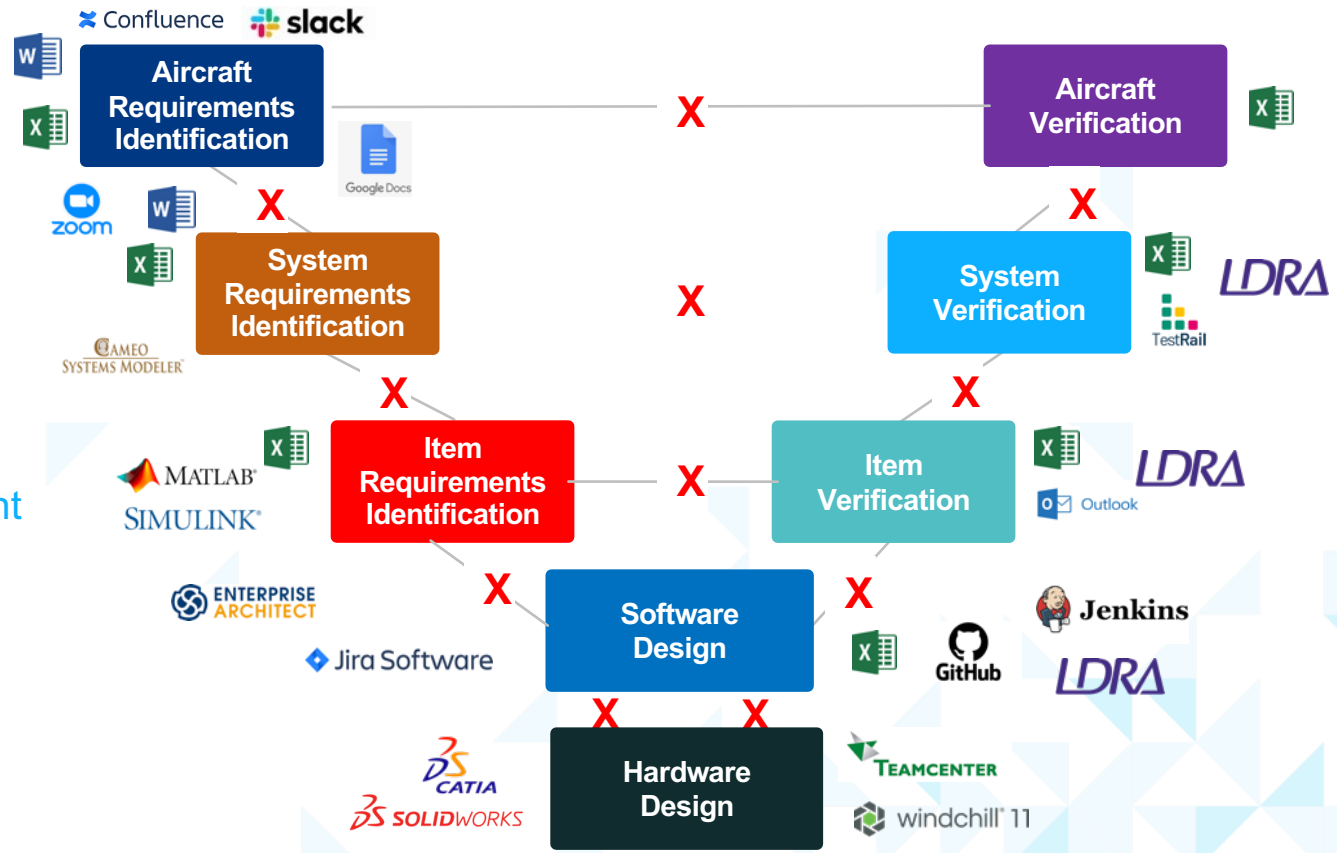
Sample airborne systems customers

Partnering for Cybersecurity by Design

PREVENTING NEGATIVE PRODUCT OUTCOMES & COMPLIANCE ISSUES

#1 Cause of Product Delays, Defects, Cost Overruns, Audit Failures, Product Failures

- Late identification of defects/coverage gaps due to lack of visibility through the development process
- Poor requirement coordination and change management between hardware/software
- Lack of ongoing risk assessment and change management
- Highly manual, after the fact traceability effort to satisfy contract requirements and standards (ex: ARP4754, DO-178C, DO-254, DO-326/356, ARP4761)
- No way to integrate desktop tools and Excel files



jama software® LDRA

Live Traceability™

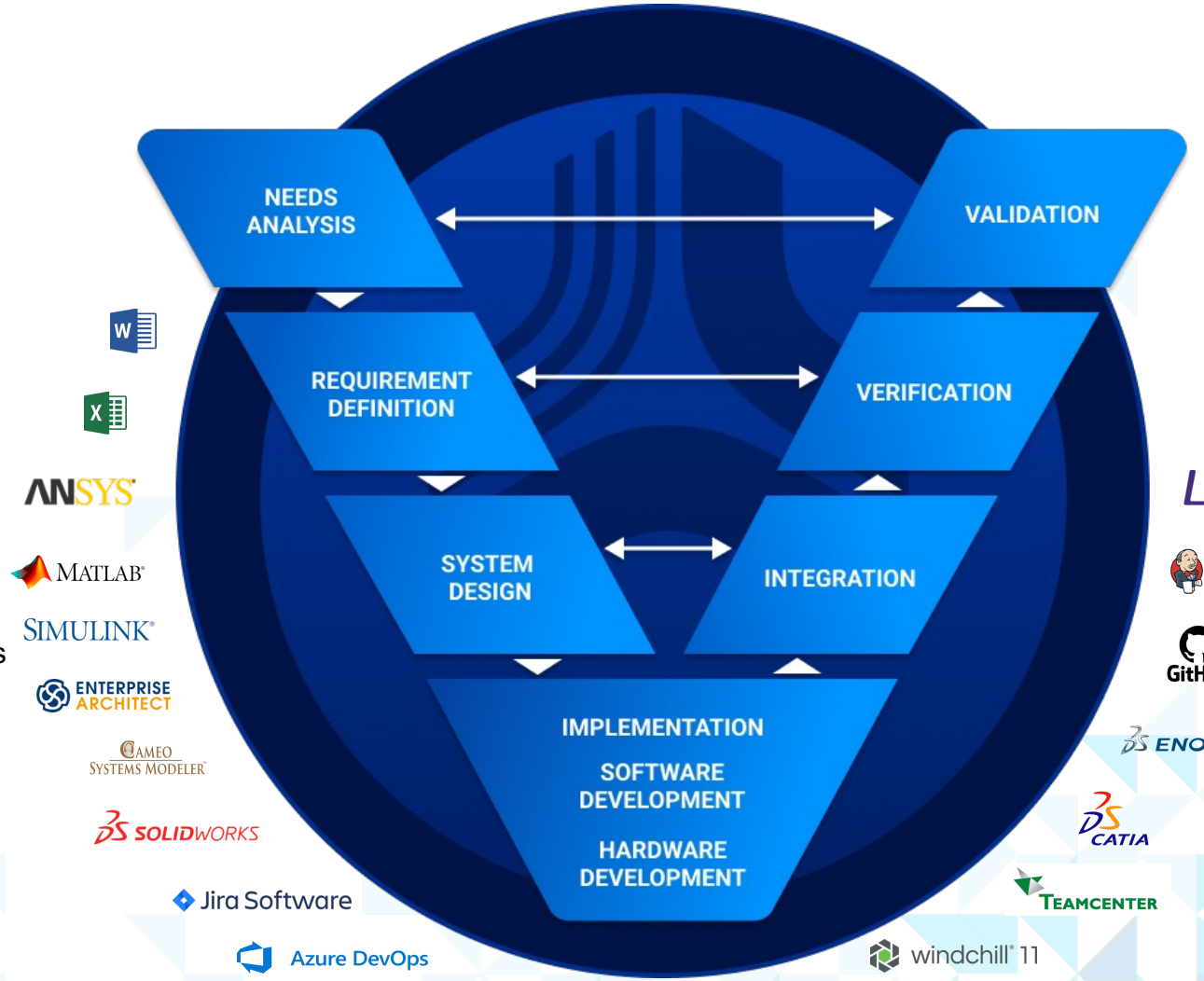
RESOLVES NEGATIVE PRODUCT OUTCOMES & COMPLIANCE ISSUES

WHAT IT IS

Live requirements traceability is the ability for any engineer at any time to see the most up to date and complete upstream and downstream information for any requirement—no matter the stage of systems development or how many siloed tools and teams it spans. This enables the engineering process to be managed through data, and its performance improved in real time.

WHY IT'S IMPORTANT

Live Traceability of system requirements is required by industry standards to ensure product safety and forms the foundation for digital engineering and model-based systems engineering. It delivers significant productivity improvements, and dramatically reduces the risk of product delays, cost overruns, defects, rework, and recalls resulting in faster time to market.



Advantages to Using Jama Connect & LDRA Together

- SINGLE METHOD TO MANAGE SECURITY ASSURANCE (NOT WORK IN OFFLINE SPREADSHEETS AND TOOLS)

- A single system to manage assets, architecture, vulnerabilities, security threats, security requirements and the verification tests.
- Relationships between cyber security items to security requirements and verification test cases
- Built-in Version control capabilities at the atomic item level and overall Security Assurance level
- Leverage Live Traceability to understand coverage, context, and impact
- Manage item lifecycle – Draft -> Review -> Approved
- Built-in and custom reports available for export need

The “DO-326/ED-202 Set”

AVIATION CYBERSECURITY

The DO-326/ED-202 set of standards, jointly developed by RTCA (U.S.) and EUROCAE (Europe) since 2006 includes, at its core, the following standards:

- DO-326A/ED-202A: “Airworthiness Security Process Specification,” with the original edition issued in 2010, and its revision A in 2014. This is the “header” standard, from which all the others evolve, and which defines the cyber-security process for aircraft and systems development, including the actions to be taken for certification per-se.
- DO-356A/ED-203A: “Airworthiness Security Methods & Considerations,” with the original editions issued in 2014 and 2015 (respectively), and its revision A in 2018. This is a detailed, practical, guide for the implementation of DO-326A/ED-202A, and could be as well considered its “part B.”DO-355/ED-204: “Information Security Guidance for Continuing Airworthiness,” issued in 2014. This is an “in-service” guide for airworthiness cybersecurity, versus the previous two standards, aiming at the development stage, and as such is already in relatively wide use by developers as well as operator

What is Airworthiness Security

AVIATION CYBERSECURITY

- RTCA DO-326A. *“Airworthiness security is the protection of the airworthiness of an aircraft from intentional unauthorized electronic interaction. Existing safety processes have not had to consider intentional disruption. Intentional unauthorized electronic interaction (also known as ”unauthorized interaction”) is defined as human-initiated actions with the potential to affect the aircraft due to unauthorized access, use, disclosure, denial, disruption, modification, or destruction of electronic information or electronic aircraft system interfaces. This definition includes the effects of malware on infected devices and the logical effects of external systems on aircraft systems, but does not include physical attacks or electromagnetic jamming.”*

- DO-326A: “The purpose of the Airworthiness Security Process (AWSP) is to establish that, when subjected to unauthorized interaction, the aircraft will remain in a condition for safe operation (using the regulatory airworthiness criteria)”

Applying the Airworthiness Security Assurance Process

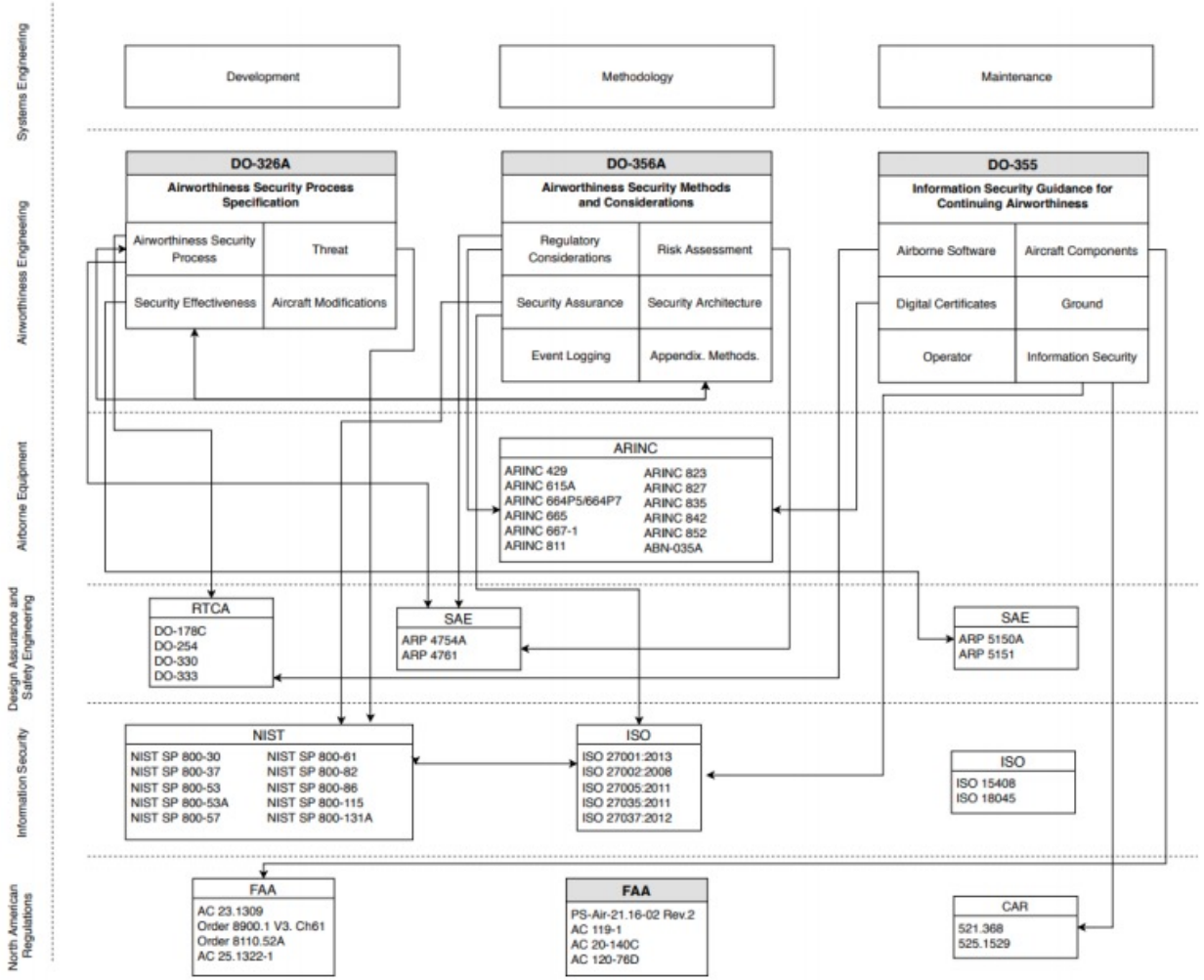
WHAT IT IS AND HOW YOU DO IT

The What

DO-326A	
Airworthiness Security Process Specification	
Airworthiness Security Process	Threat
Security Effectiveness	Aircraft Modifications

The How

DO-356A	
Airworthiness Security Methods and Considerations	
Regulatory Considerations	Risk Assessment
Security Assurance	Security Architecture
Event Logging	Appendix Methods



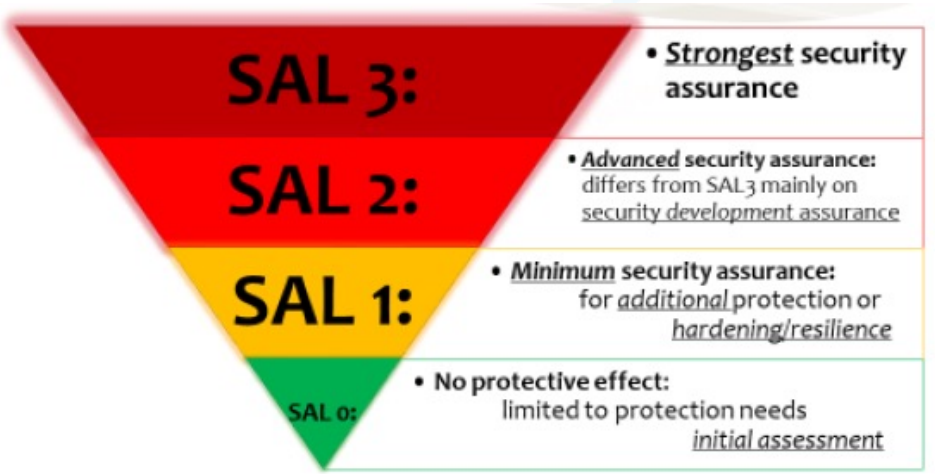
Airworthiness Security Process (AWSP)

DO-326A/ED-202A & DO-356A/ED-203A

Airworthiness security is the protection of the airworthiness of an aircraft from intentional unauthorized electronic interaction

Basic Process

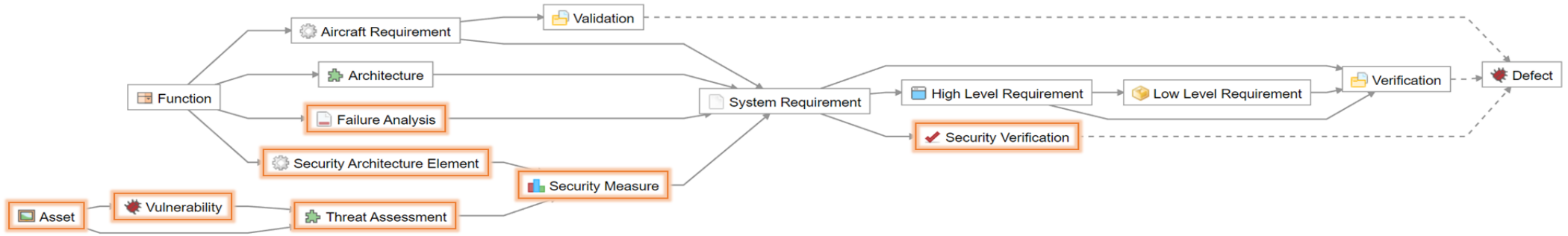
1. Identify System Assets & Perimeters
2. Identify Threats for each Asset
3. Identify Risks for each threat
4. Create Controls/Mitigations for each risk

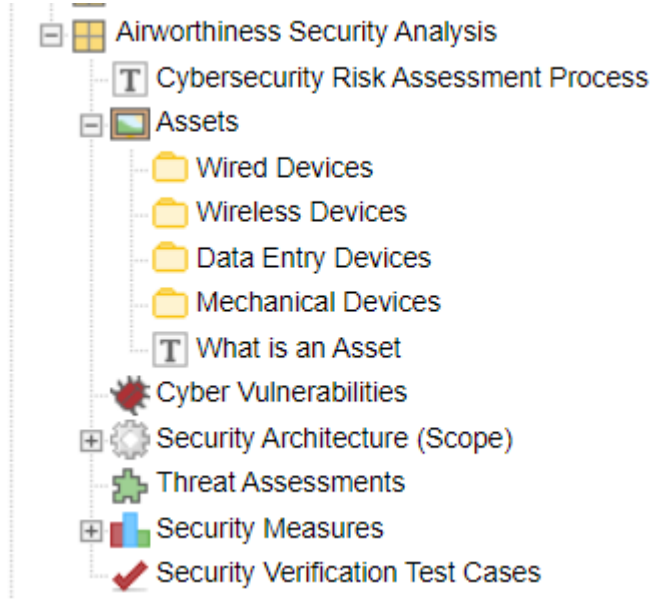


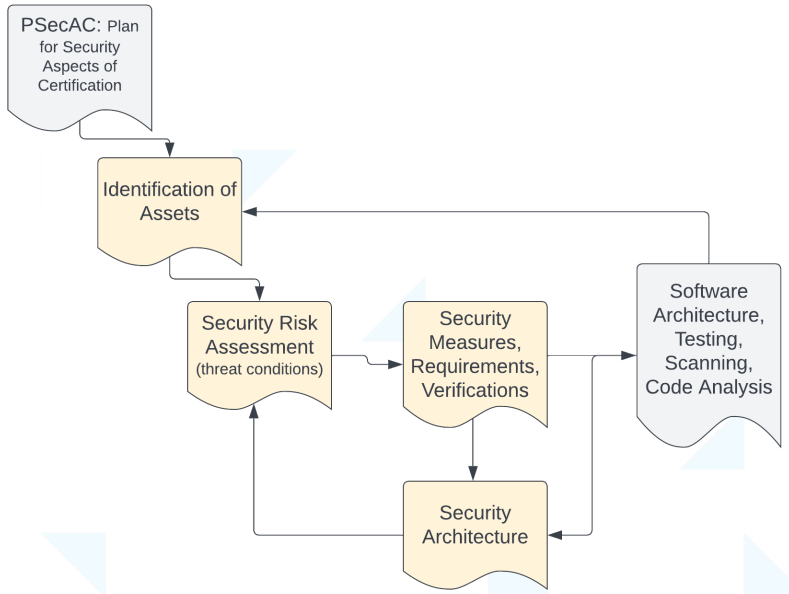
DO-326A Cybersecurity

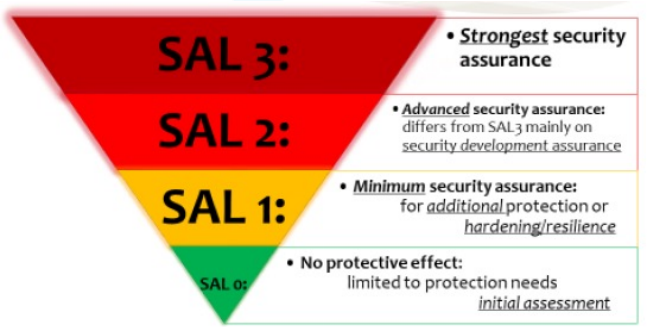
AIRWORTHINESS SECURITY PROCESS

DO-326A









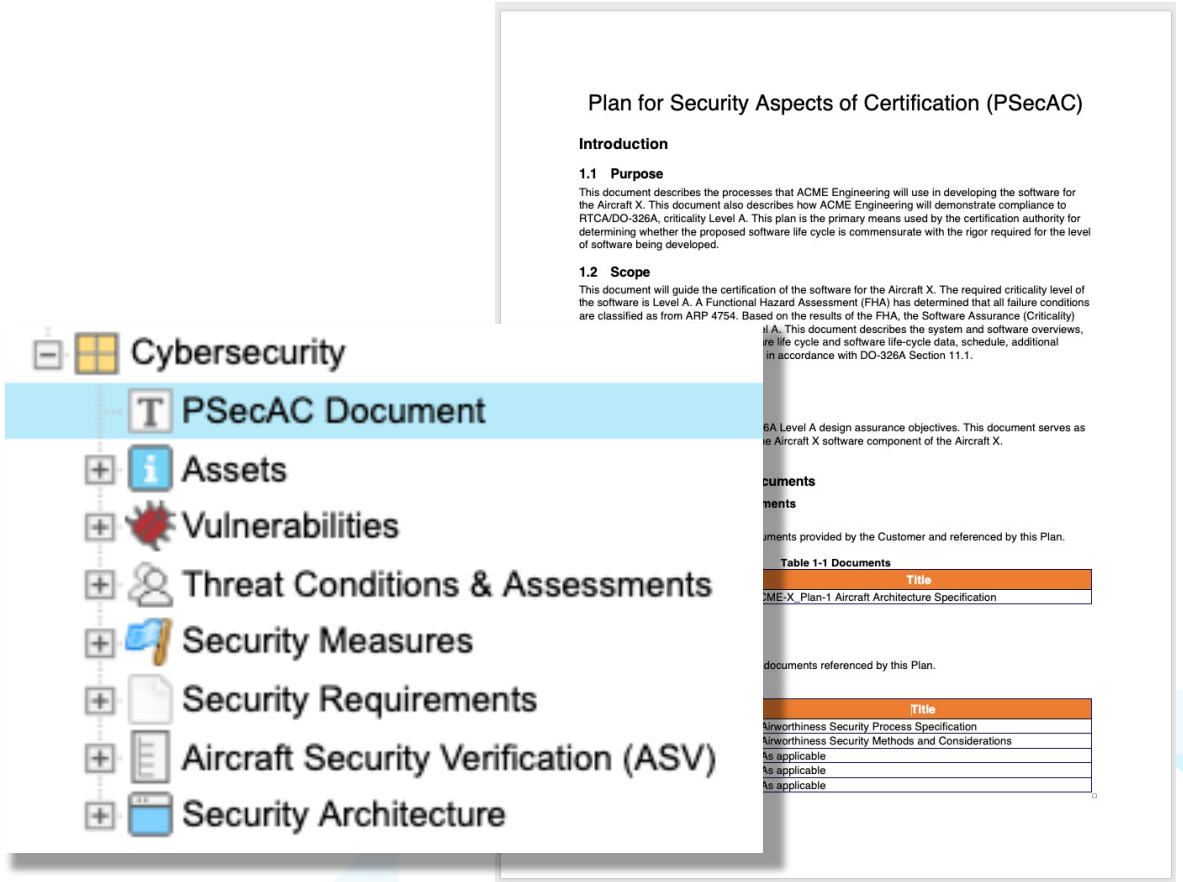
jama software® LDRA

DO-326A Airworthiness Security Process - 7 Steps

2.0 Step 1: Plan for Security Aspects of Certification	**Aircraft Level Planning / System Level Planning**
2.0 Step 2: Security Scope Definition	Threat Assessment Process
2.0 Step 3: Security Risk Assessment	Threat Assessment Process
2.0 Step 4: Decision Gate	Threat Assessment Process
2.0 Step 5: Security Development	Definition of Security Measures & Requirements
2.0 Step 6: Security Effectiveness Assurance	Verification and Validation of Security Measures and Requirements
2.0 Step 7: Communication of Evidence	PSecAC Summary Reporting

Step 1 - Develop Plan for Security Aspects of Certification document (PSecAC)

- Use Plan item type in Jama Connect to author or import PSecAC document.
- Alternatively, use Plan item type to reference released documents in a document management system using Document Control ID or URL.

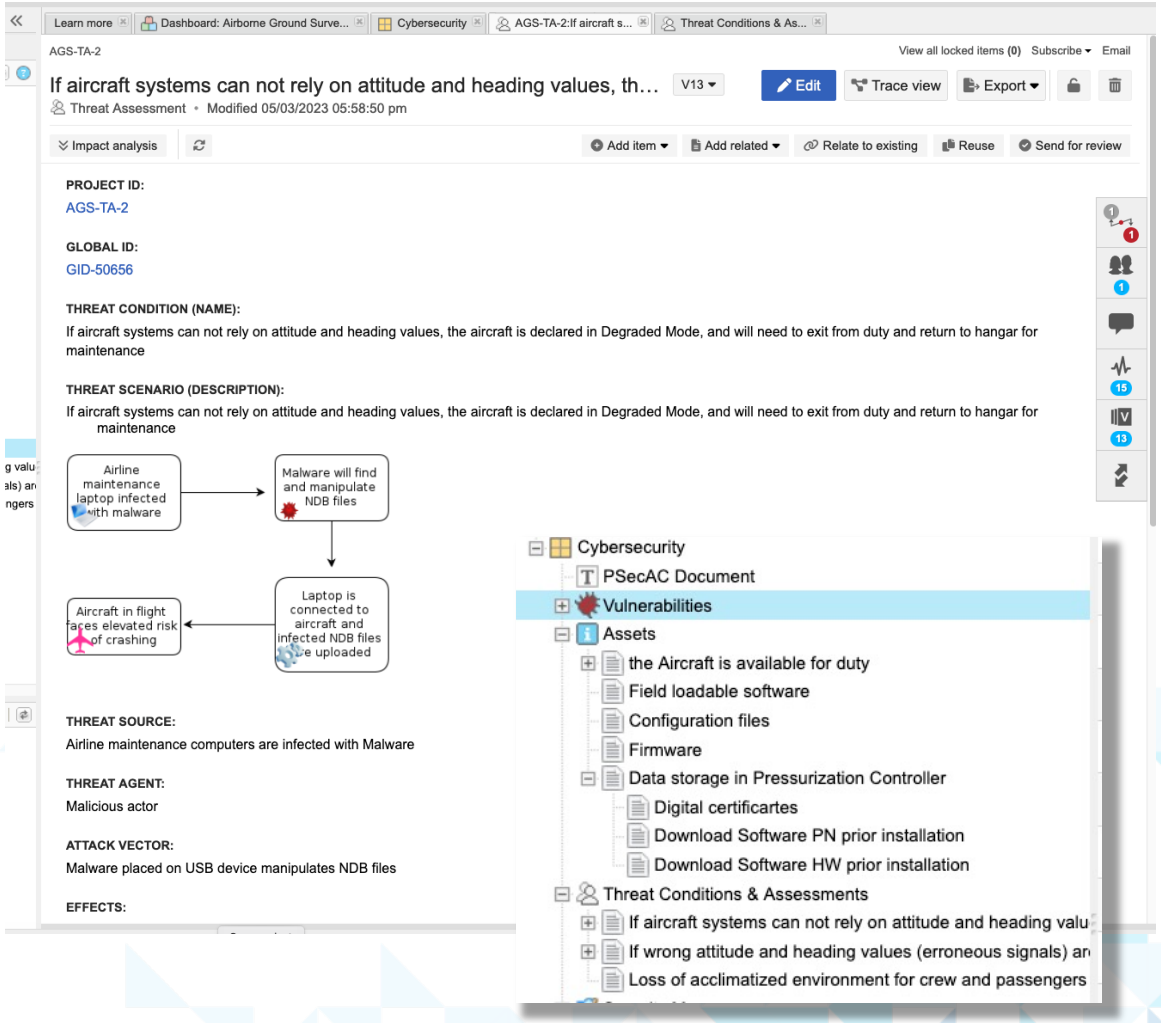


Step 2 - Identify Security Scope, Perimeter, and Assets

- Security scope and security perimeter will inform the creation of Asset items in Jama.
- It is often helpful to create diagrams using Jama's diagram editor for helpful reference of the scope and perimeter in relation to the assets.

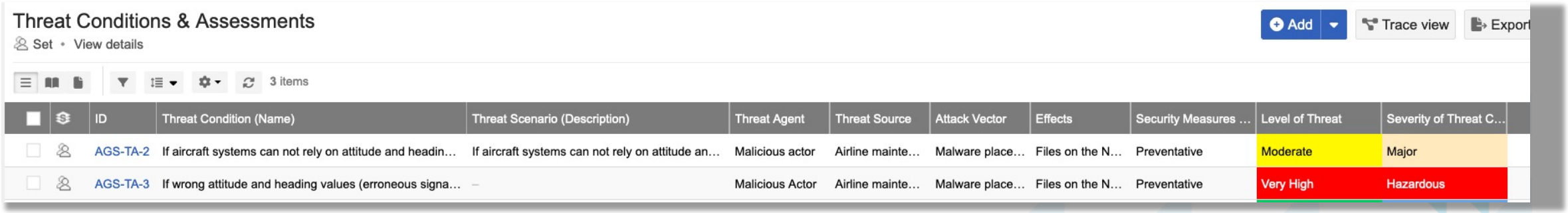
Step 3 - Identify Threats for Each Asset

- For each Asset, create one or more Threat Assessment items.
- Create trace relationships between the Asset items and Threat Assessment items.
- For each threat record the analyzed threat conditions.
- For each threat assessment, record the threat scenarios.



Step 4 - Identify Risks for Each Threat

For each threat assessment record the severity of threat condition and the level of the threat. Jama Connect will automatically generate the Acceptability (Unacceptable or Acceptable).



Threat Conditions & Assessments

Set • View details

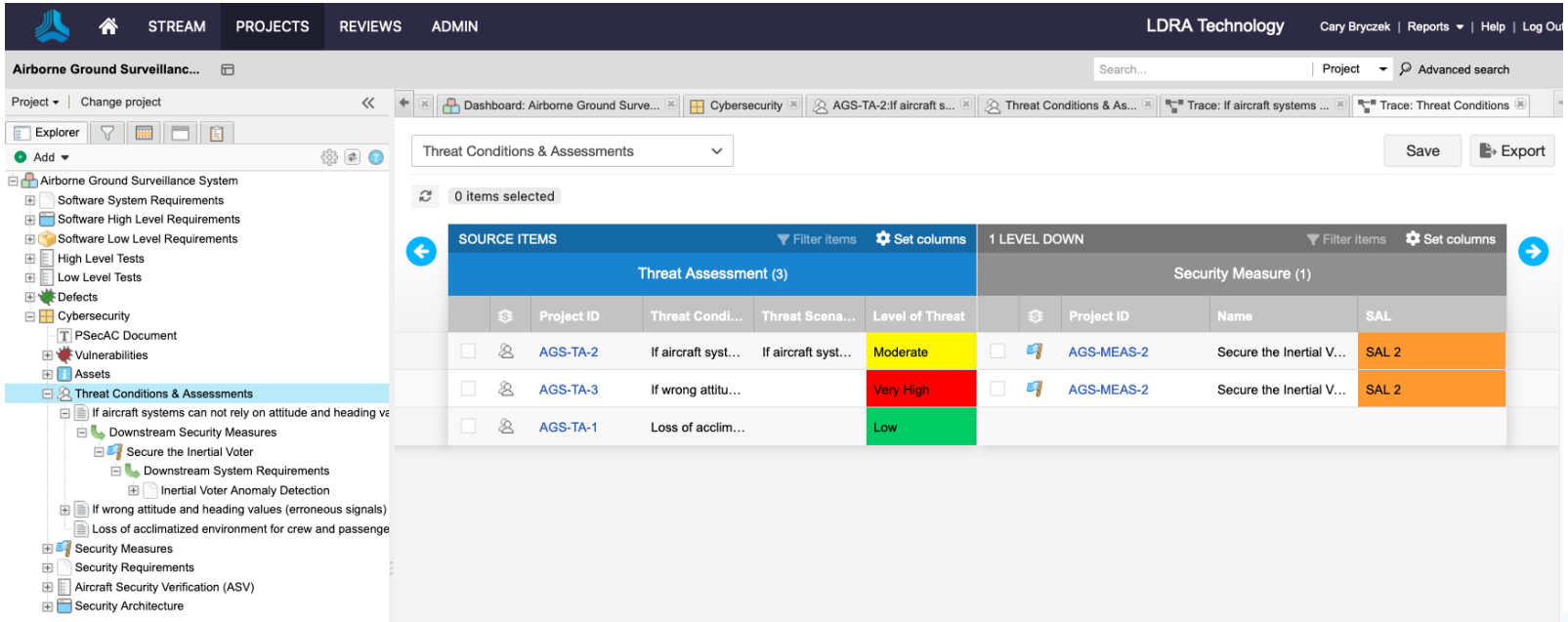
Add | Trace view | Export

3 items

ID	Threat Condition (Name)	Threat Scenario (Description)	Threat Agent	Threat Source	Attack Vector	Effects	Security Measures …	Level of Threat	Severity of Threat C…
AGS-TA-2	If aircraft systems can not rely on attitude and headin…	If aircraft systems can not rely on attitude an…	Malicious actor	Airline mainte…	Malware place…	Files on the N…	Preventative	Moderate	Major
AGS-TA-3	If wrong attitude and heading values (erroneous signa…	–	Malicious Actor	Airline mainte…	Malware place…	Files on the N…	Preventative	Very High	Hazardous

Step 5 - Create Controls/Mitigations for Each Risk

- For each Threat Assessment create a trace relationships to a Security Measure item. Create a new security measure if necessary.



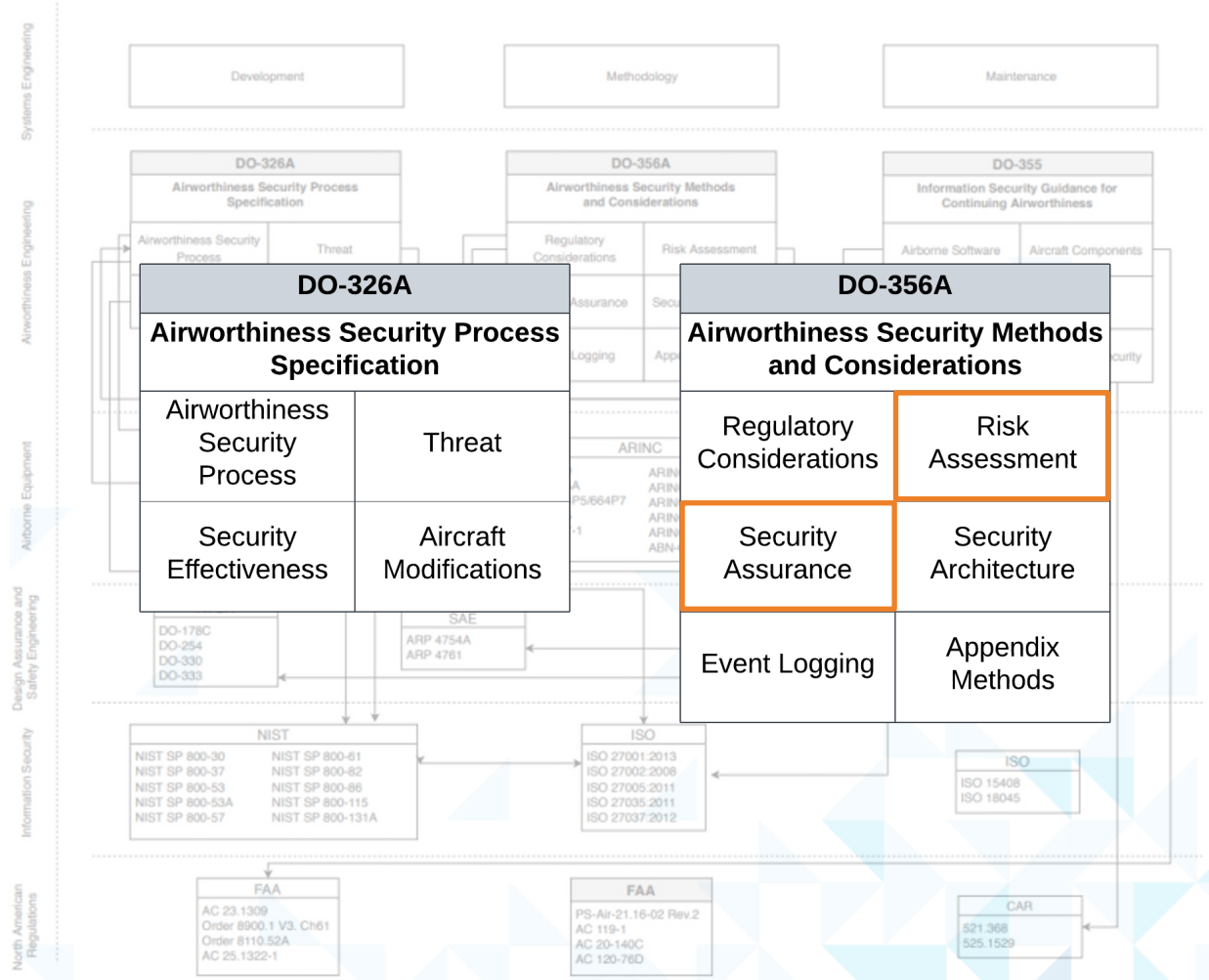
- Perform Security Measure characterization documenting a control/mitigation by relating it to a System Requirement. Create a new requirement(s) at the System Requirement level as necessary.

Step 6 - Communication of Evidence

- Use the filters in Jama to identify Threat Assessments whose Acceptability is Unacceptable. For these Assessments, create a trace report (live trace in the UI or traceability export) to analyze and report on risk assessment activities.
- Update the PSecAC document as necessary with compliance demonstration evidence.

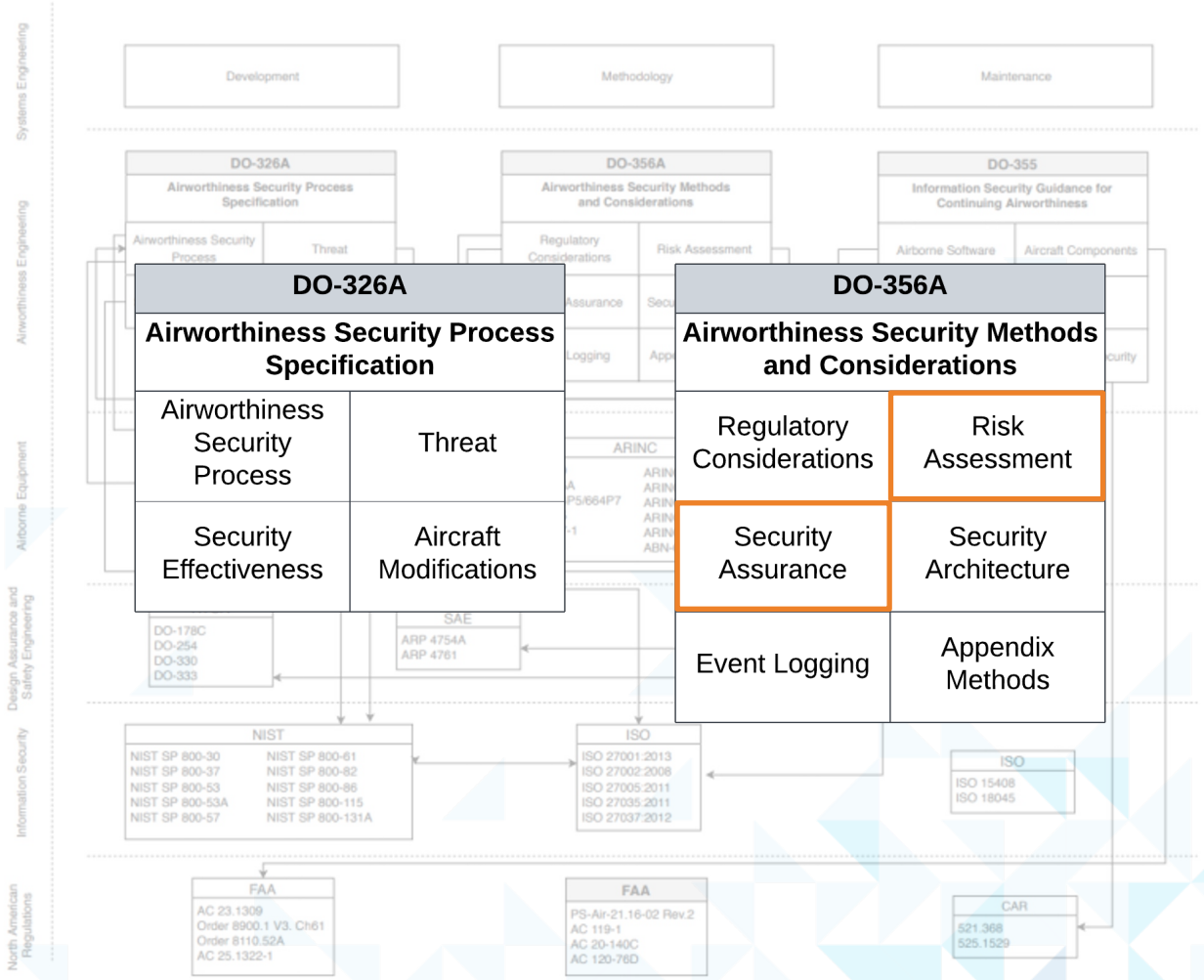
Risk Assessment Objectives

Ref.	Objective	Jama Supporting Capability
O1.1	The security scope is established and validated.	**Security Assessment and Review Center**
O1.2	The Threat Condition Identification and Evaluation is complete and validated.	**Security Assessment and Review Center**
O1.3	The Preliminary Aircraft/System Security Risk Assessments and Aircraft/System Security Risk Assessments are performed and consistent with related aircraft/system safety assessments.	**Risk Assessment Process**
O1.4	Preliminary Aircraft/System Security Risk Assessment results have been processed to define aircraft/system security architecture and identify the need for security measures.	**PSecAC Summary Reporting**
O1.5	Aircraft/System Security Risk Assessment is consistent and complete with respect to security scope, security guidance, security requirements, security verification, security refutation and vulnerability identification.	**Security Assessments, Review Center, & Coverage Analysis**



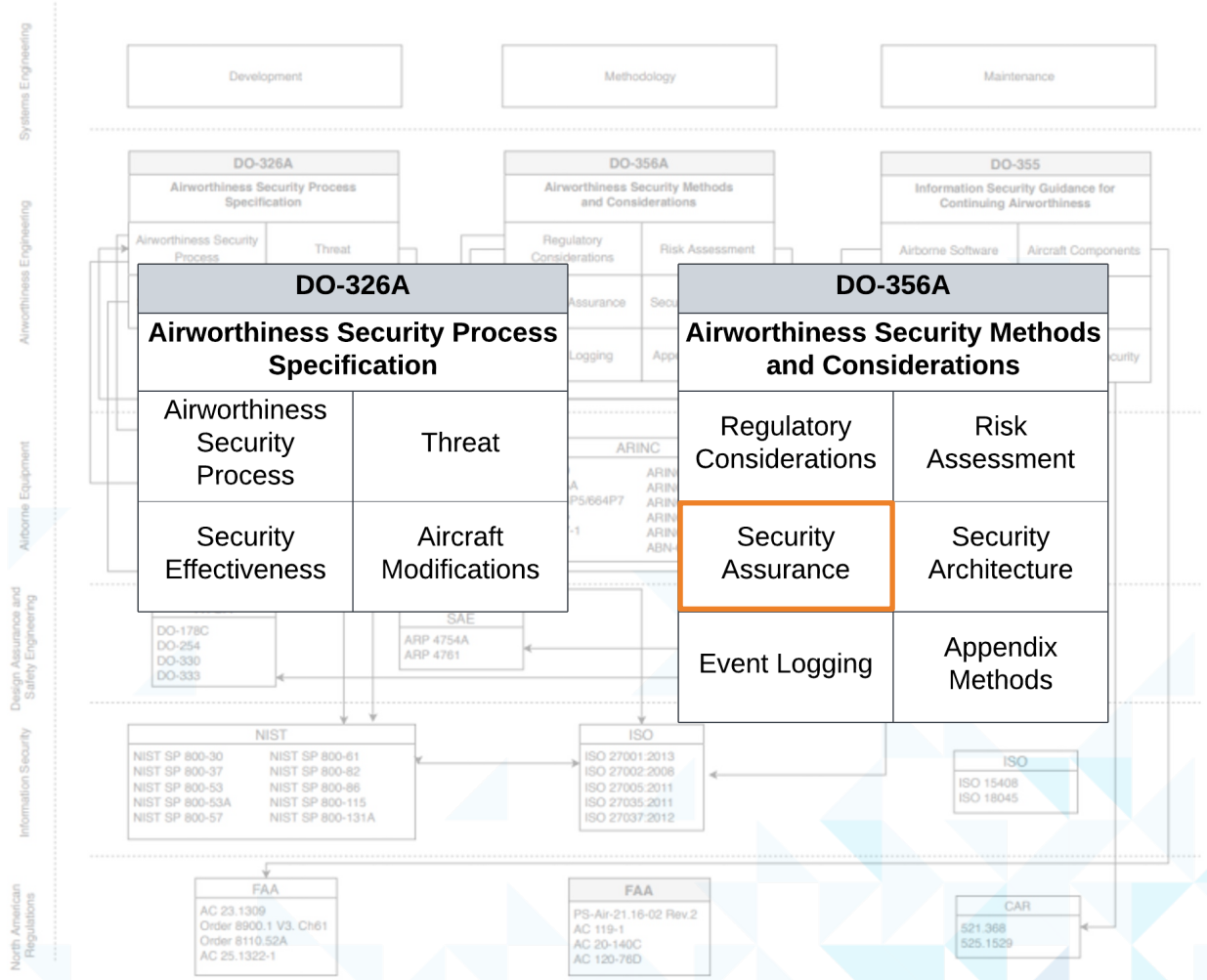
Vulnerability Identification Objectives

Ref.	Objective	Jama Supporting Capability
O2.1	Vulnerabilities in security measures and assets (including COTS) are identified and evaluated for their potential impact on safety.	**Vulnerability and Threat Assessment Process**
O2.2	Vulnerabilities are treated according to their evaluation.	**Vulnerability and Threat Assessment Process**



Security Refutation Objectives

Ref.	Objective	LDRA Supporting Capability
O3.1	Refutation analyses are performed to identify new vulnerabilities.	
O3.2	Refutation tests are performed to evaluate the exposure of vulnerabilities in the security environment and to challenge the vulnerability evaluation.	**TBrun with TBextreme tests**
O3.3	Refutation test plans are available. Refutation test results cover refutation test plans and performed tests. Refutation test results are analyzed and discrepancies are justified and traced.	**TBmanager and TBreports**



Refutation

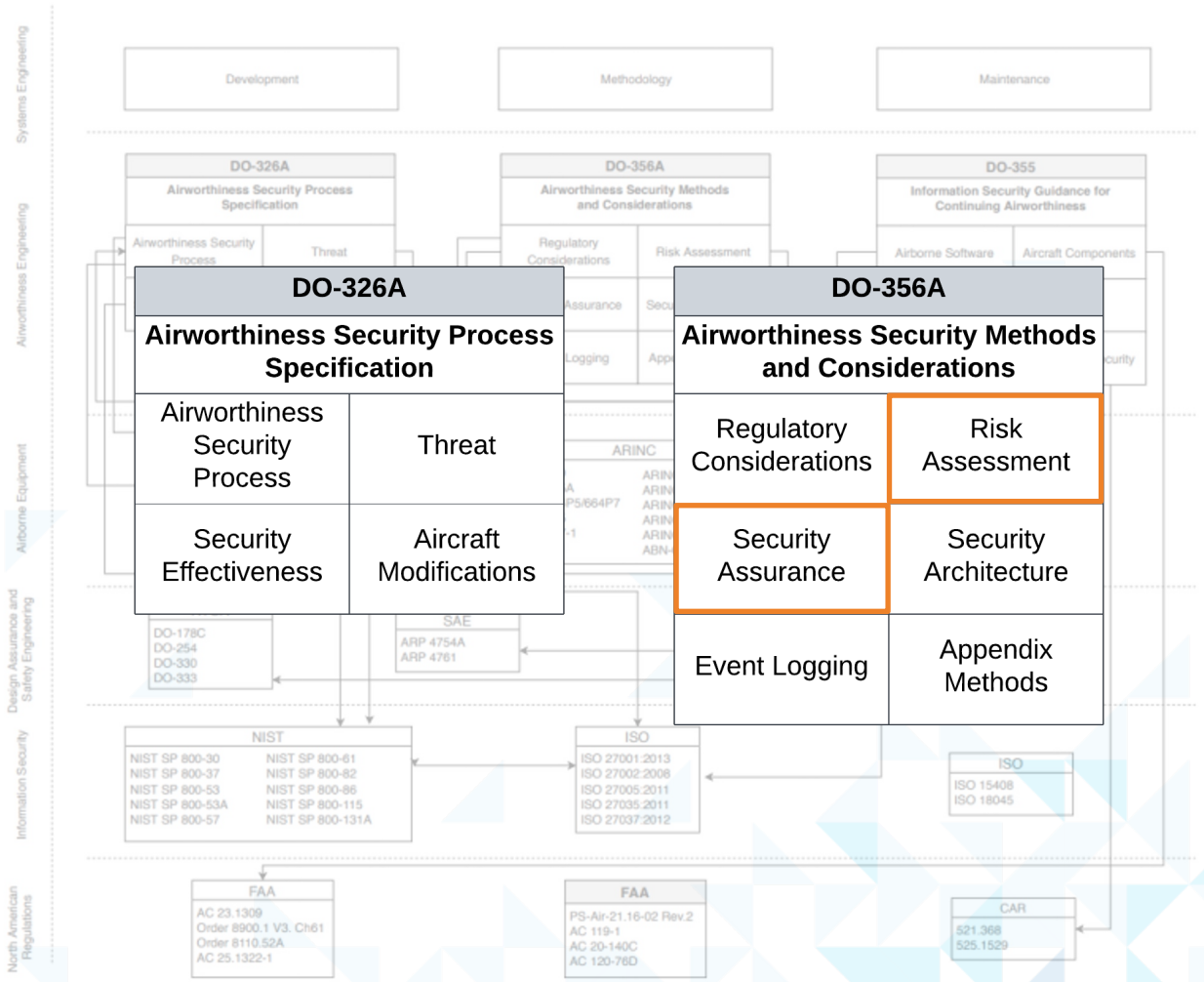
ED-203A / DO-356A

“Refutation acts as an independent set of assurance activities beyond analysis and requirements. As an alternative to exhaustive testing, refutation can be used to provide evidence that an unwanted behavior has been precluded to an acceptable level of confidence.

NOTE: Refutation is also known as Security Evaluation in some contexts.”

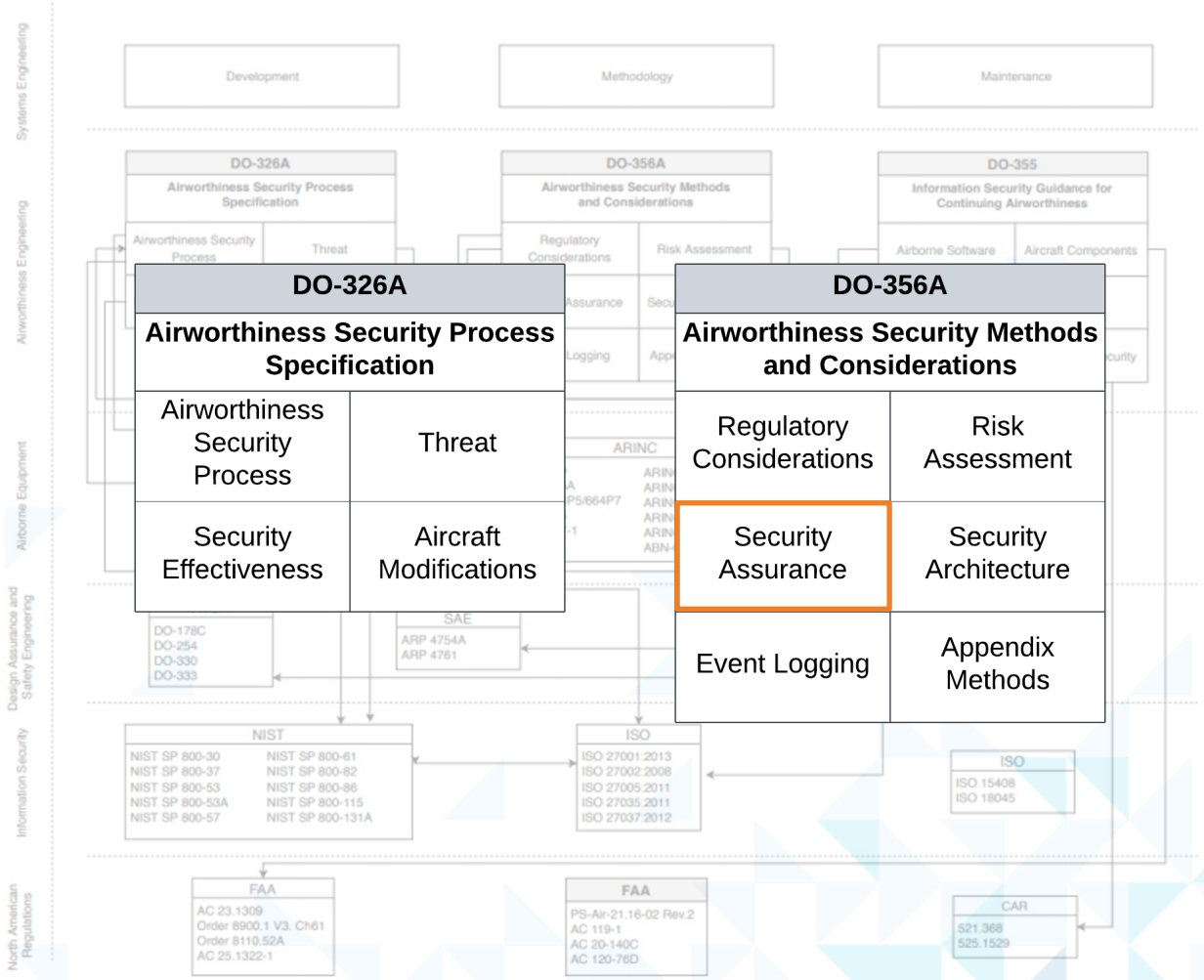
Security Deployment Objectives

Ref.	Objective	Jama Supporting Capability
O4.1	Security guidance is correct, complete and validated against technical and operational security measures and requirements.	**Traceability** **Analysis &** **Reports**



Security Implementation Objectives

Ref.	Objective	LDRA Supporting Capability
O8.1	Source code and/or hardware description complies with security requirements.	**TBmanager**
O8.2	Source code and/or hardware description conforms to security coding standards.	**TBvision, TBsecure, and TBreports**
O8.3	Source code and/or hardware description complies with item security architecture.	**TBmanager**

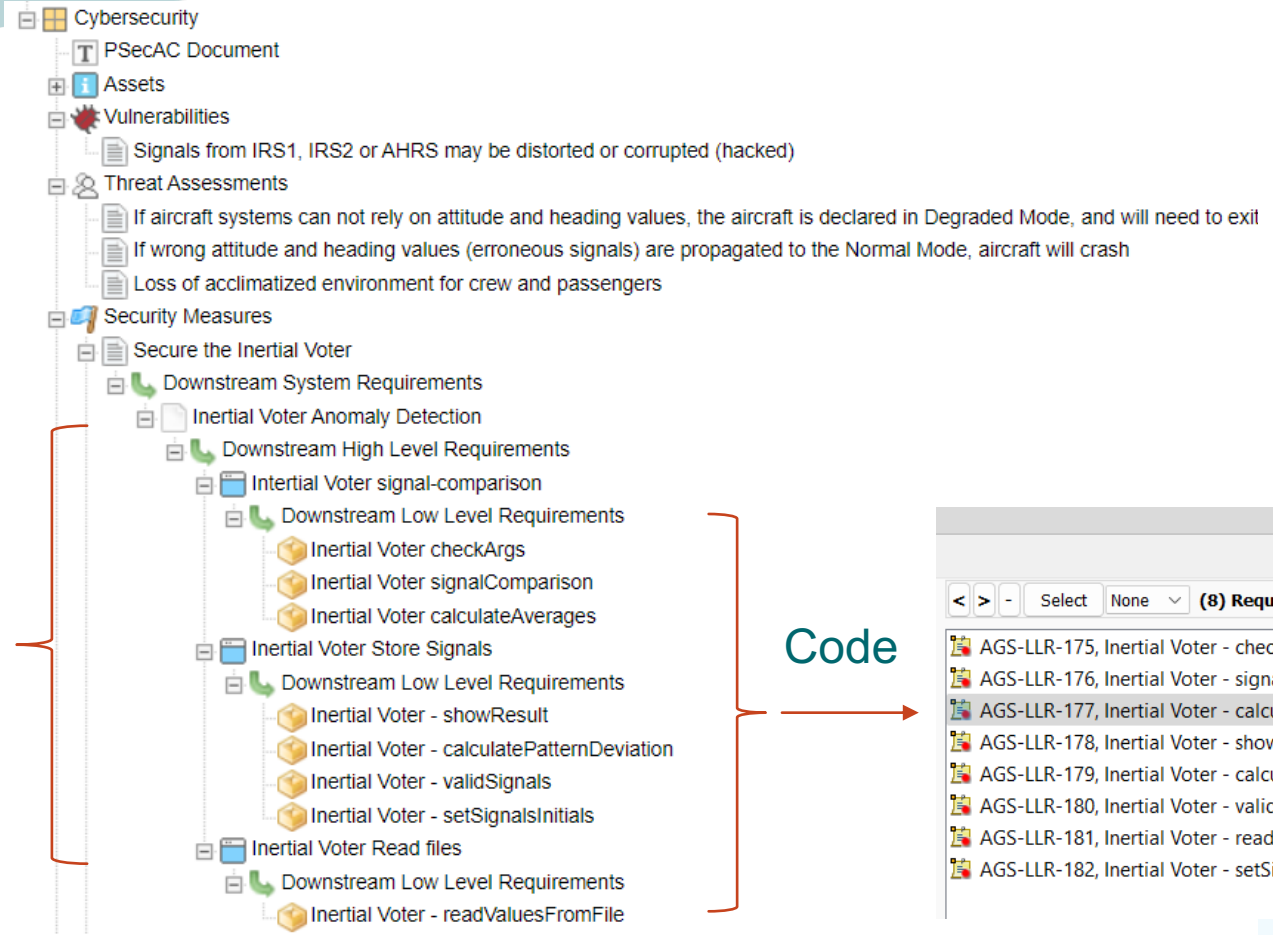


Source Code Complies with Security Requirements

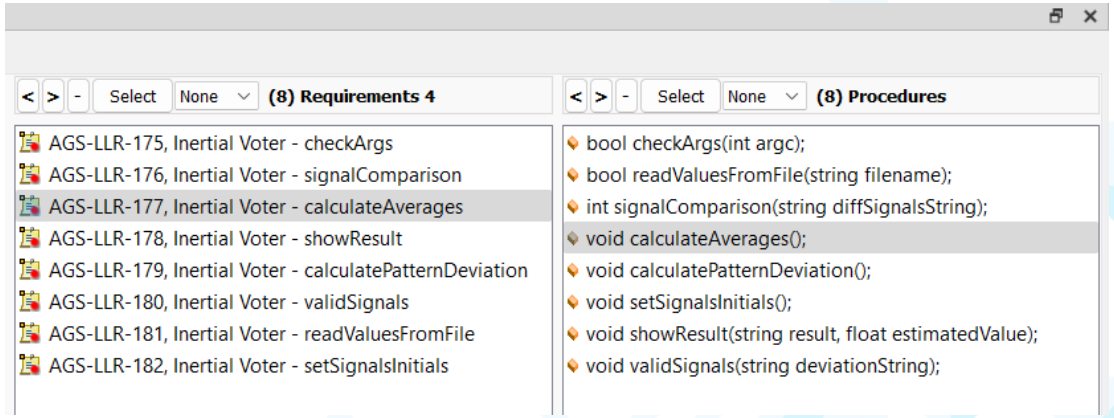
Threats

Security Measures

Security Requirements

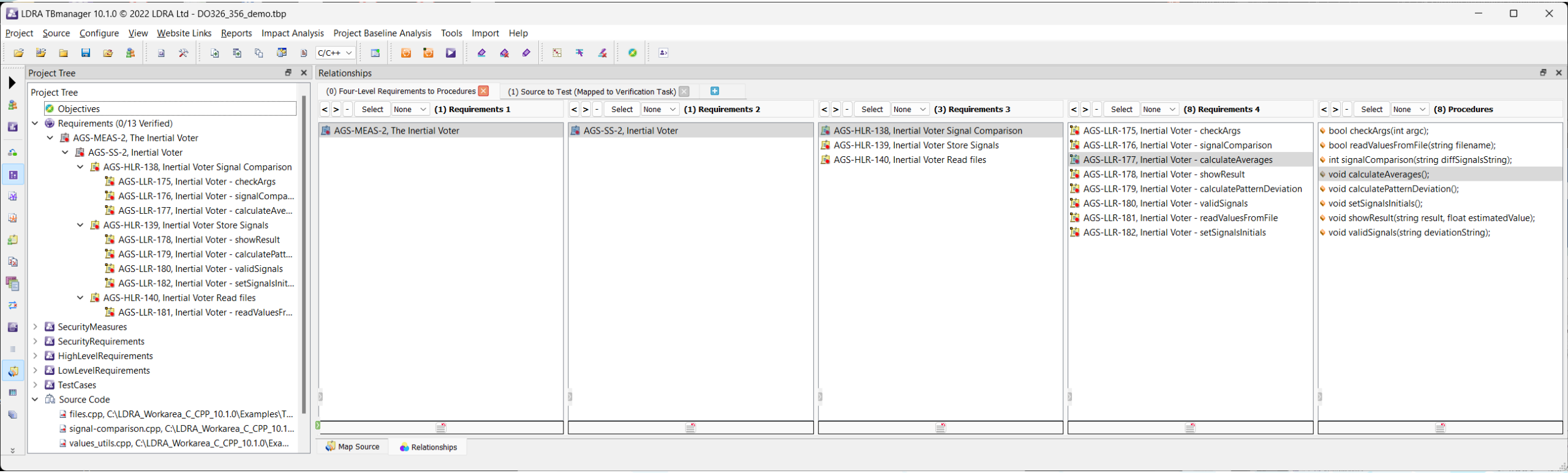


Code



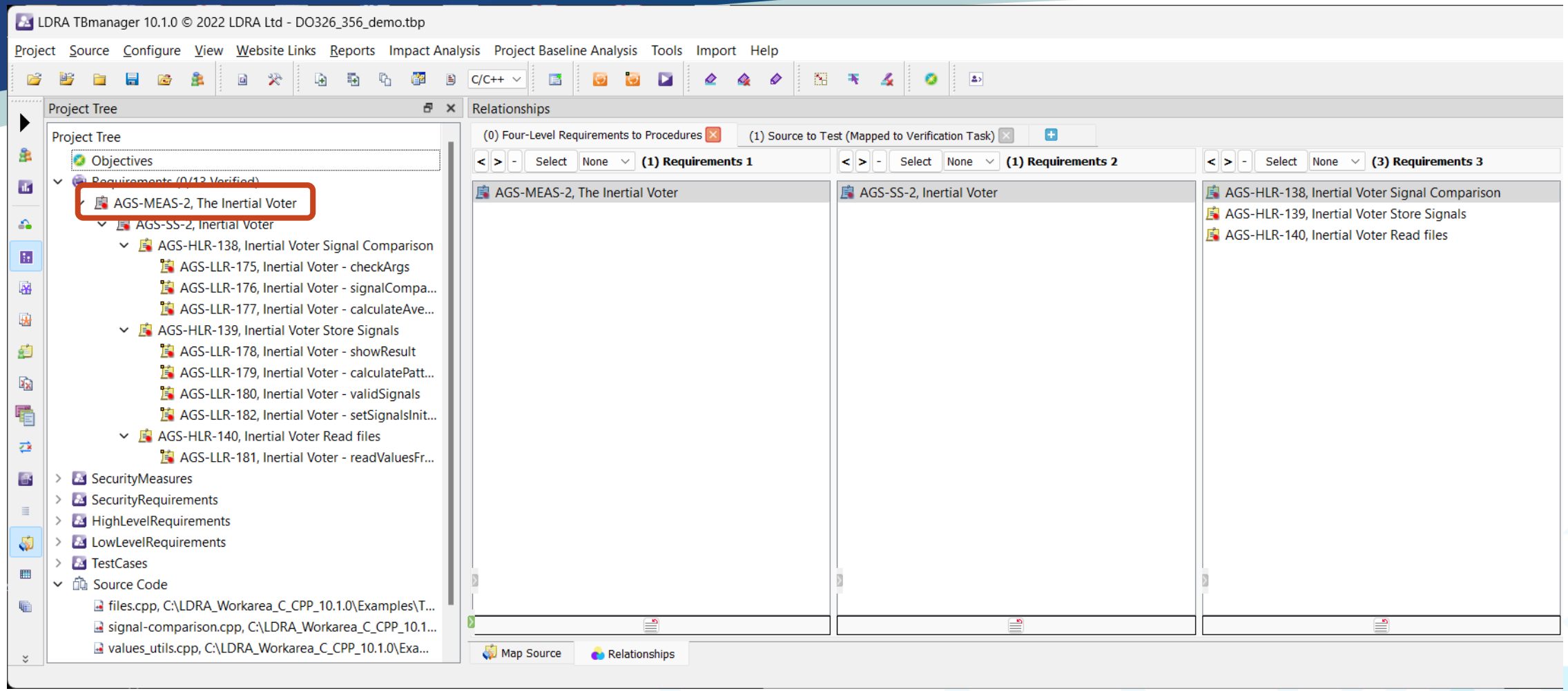
Source Code Complies with Security Requirements

SECURITY MEASURE -> SECURITY REQUIREMENTS -> CODE



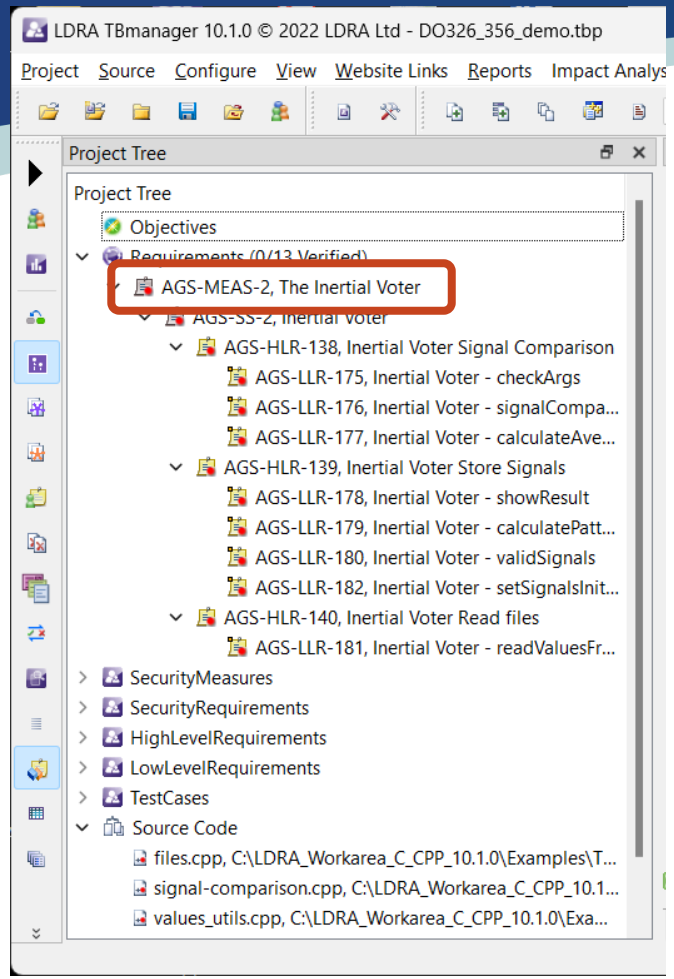
Source Code Complies with Security Requirements

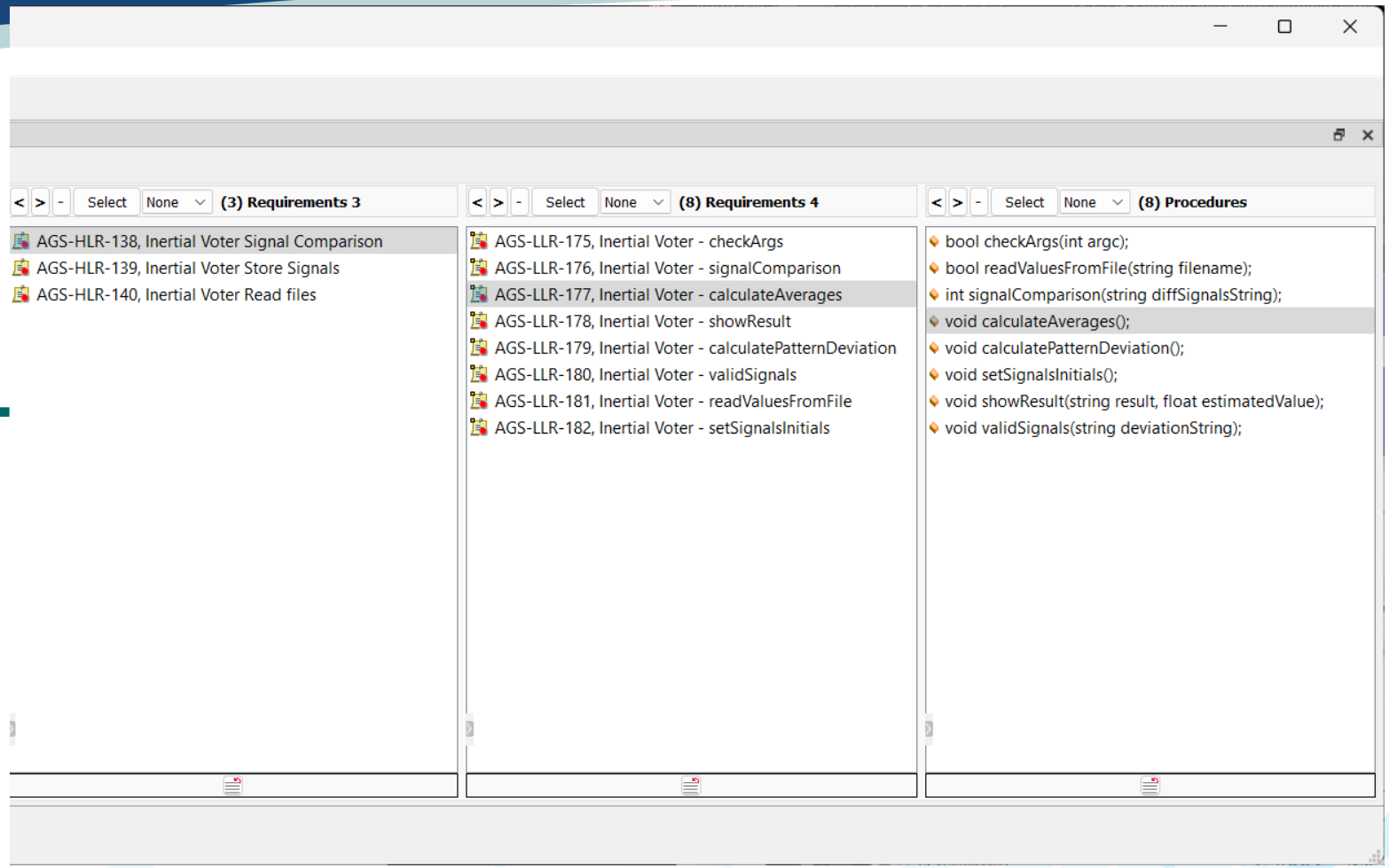
SECURITY MEASURE -> SECURITY REQUIREMENTS -> HIGH LEVEL REQUIREMENTS



Source Code Complies with Security Requirements

HIGH LEVEL REQUIREMENTS -> LOW LEVEL REQUIREMENTS -> CODE





Source Code Conforms to Security Coding Standards

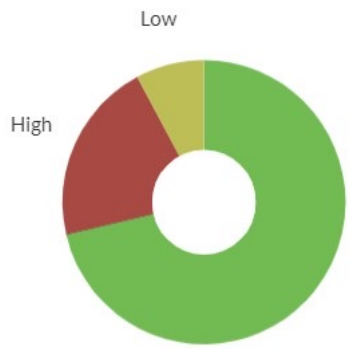
- Security Report
  - MISRA-C++:2008
  - CERT-C++:2016
  - CWE

LDRA tool suite Security Report

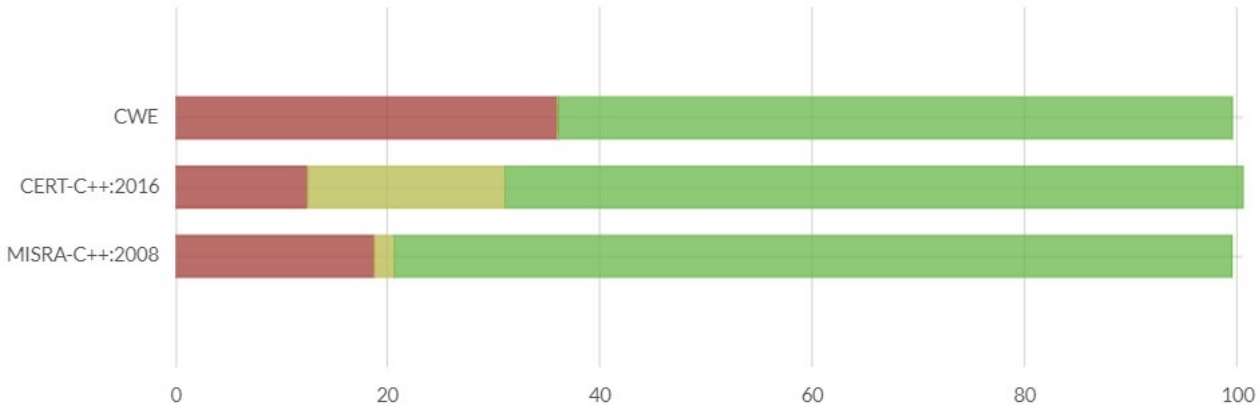
File: C:\LDRA_Workarea_C_CPP_10.1.0\Examples\Toolsuite\DO326_356_demo\Source\signal-comparison.cpp

Date of Analysis	Report Produced on	LDRA Version
Wed May 3 2023 13:27:26	Wed May 3 2023 13:28:42	10.1.0

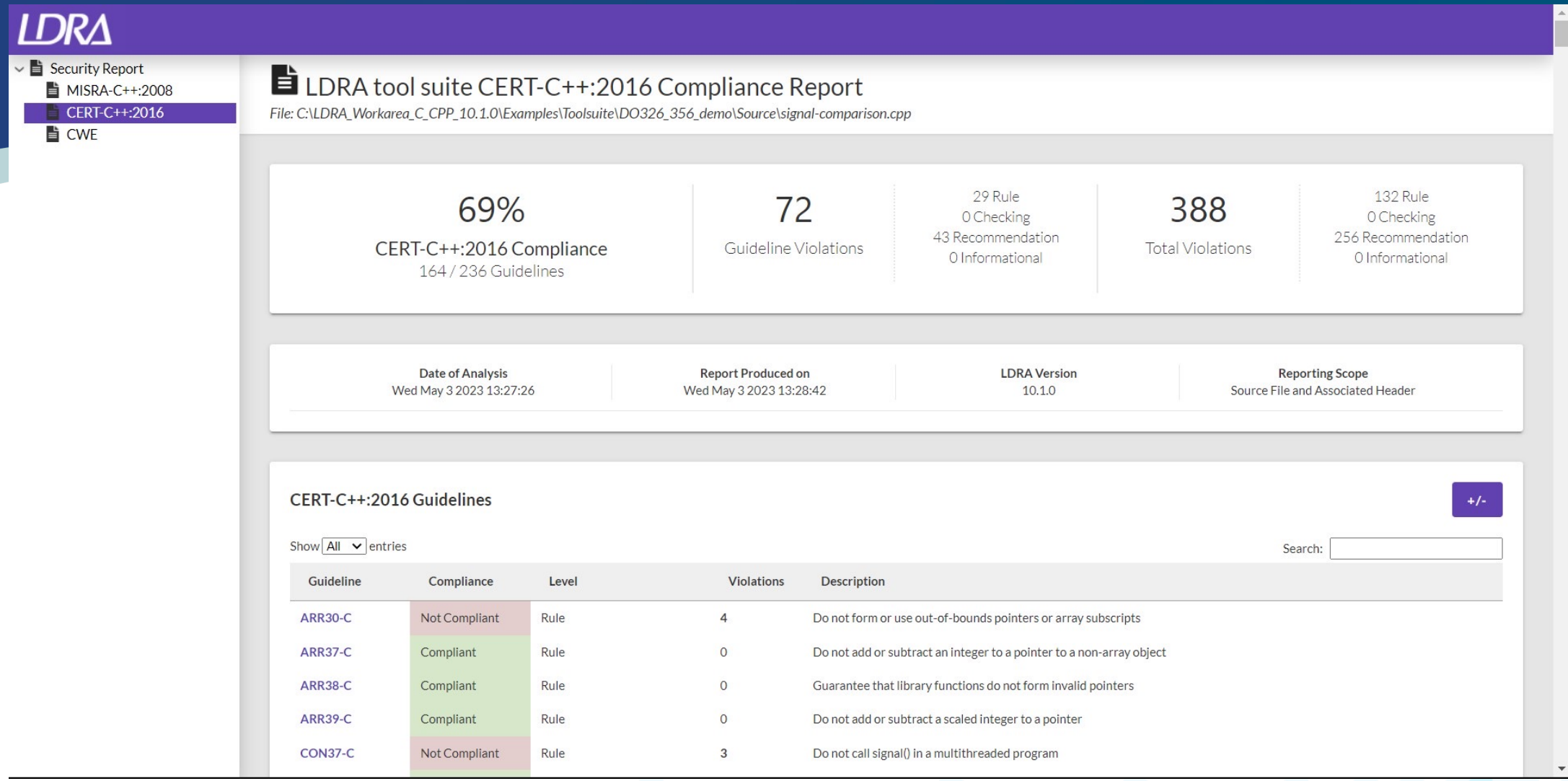
Security Summary



Security Distribution



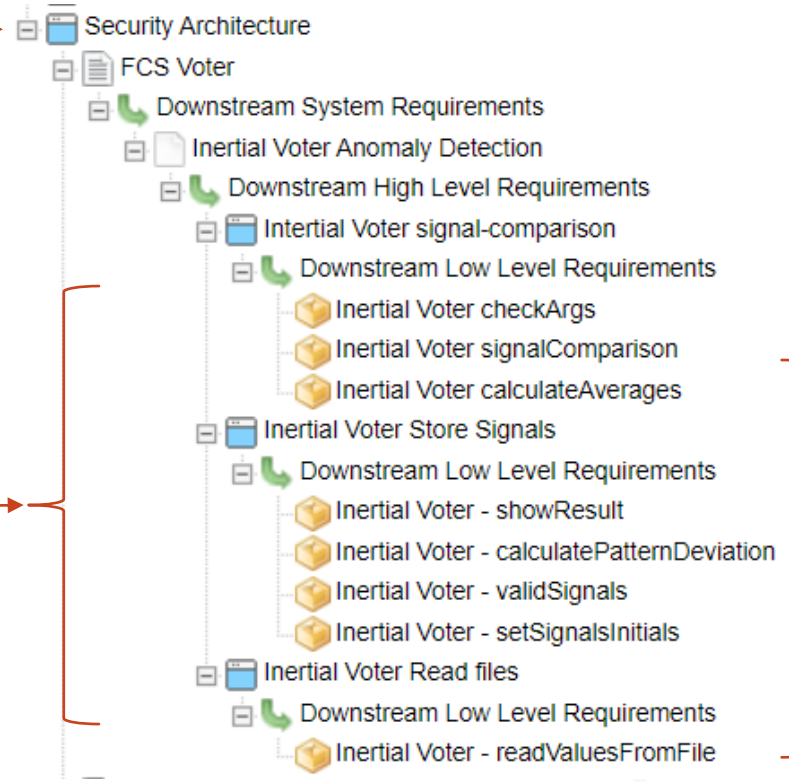
Source Code Conforms to Security Coding Standards



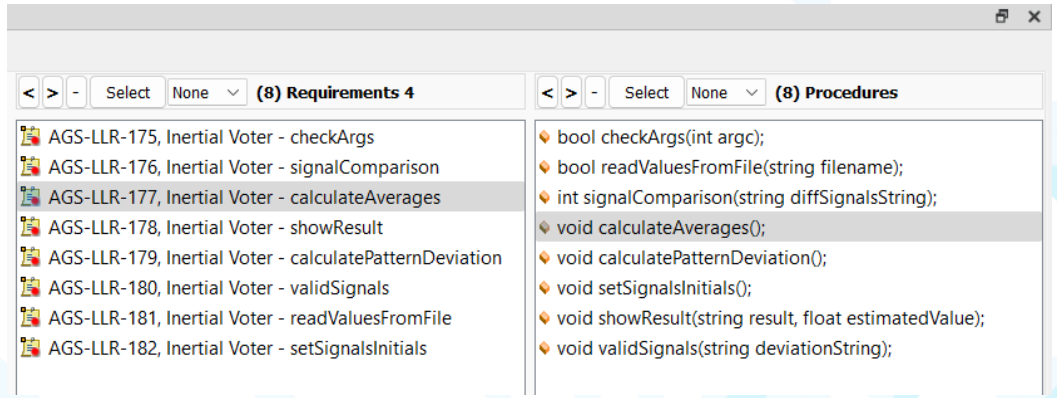
Source Code Complies with Security Architecture

Security Architecture

Security Requirements

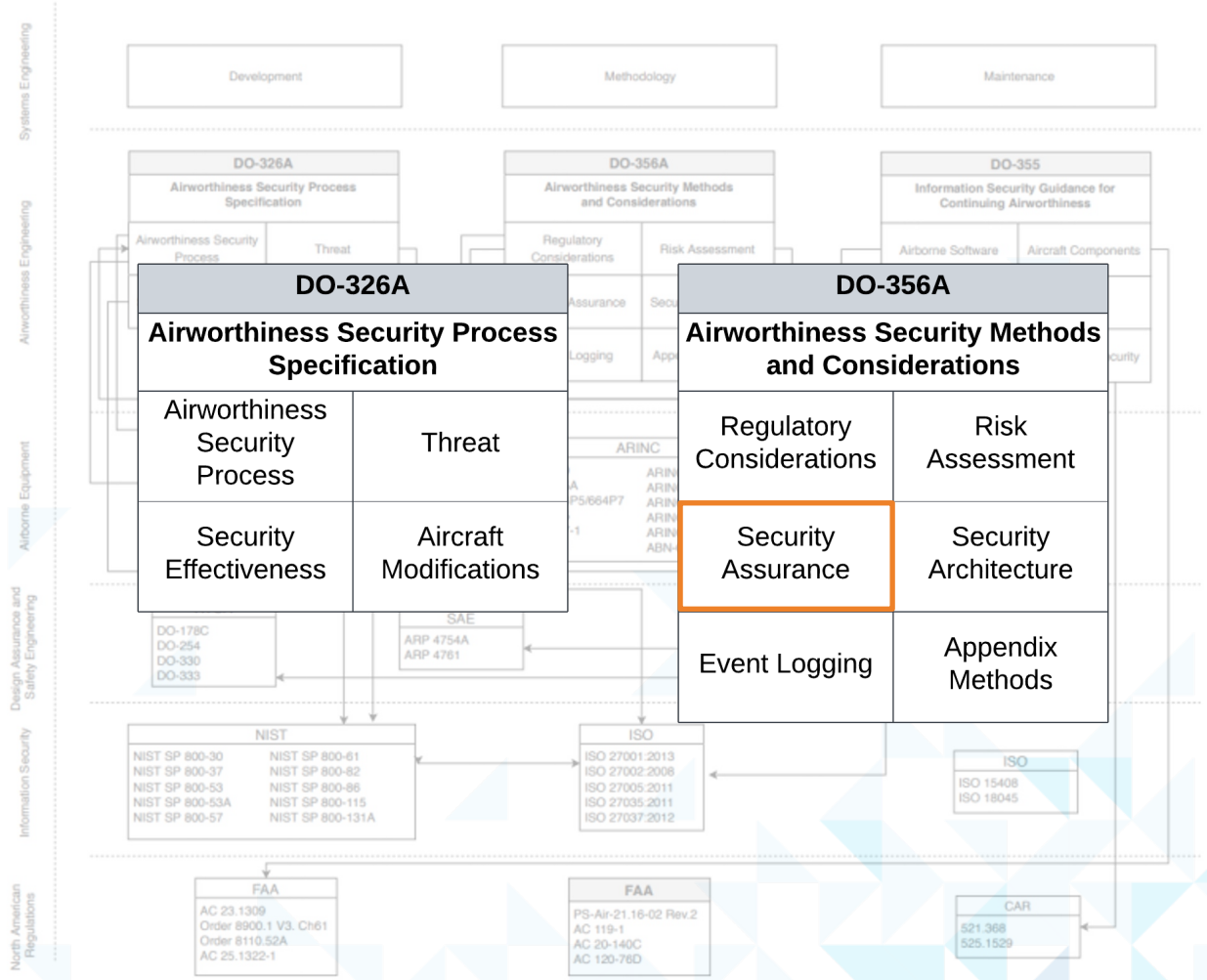


Code



Security Verification Objectives

Ref.	Objective	LDRA Supporting Capability
O9.1	Security functional and robustness verification elements are developed, validated and performed.	**TBrun**
O9.2	Security functional and robustness verification results are complete and correct, and discrepancies are justified and traced.	**TBreports, TBsecure, TBjustify**
O9.3	Test coverage of software and/or hardware implementation is achieved.	**TBmanager**



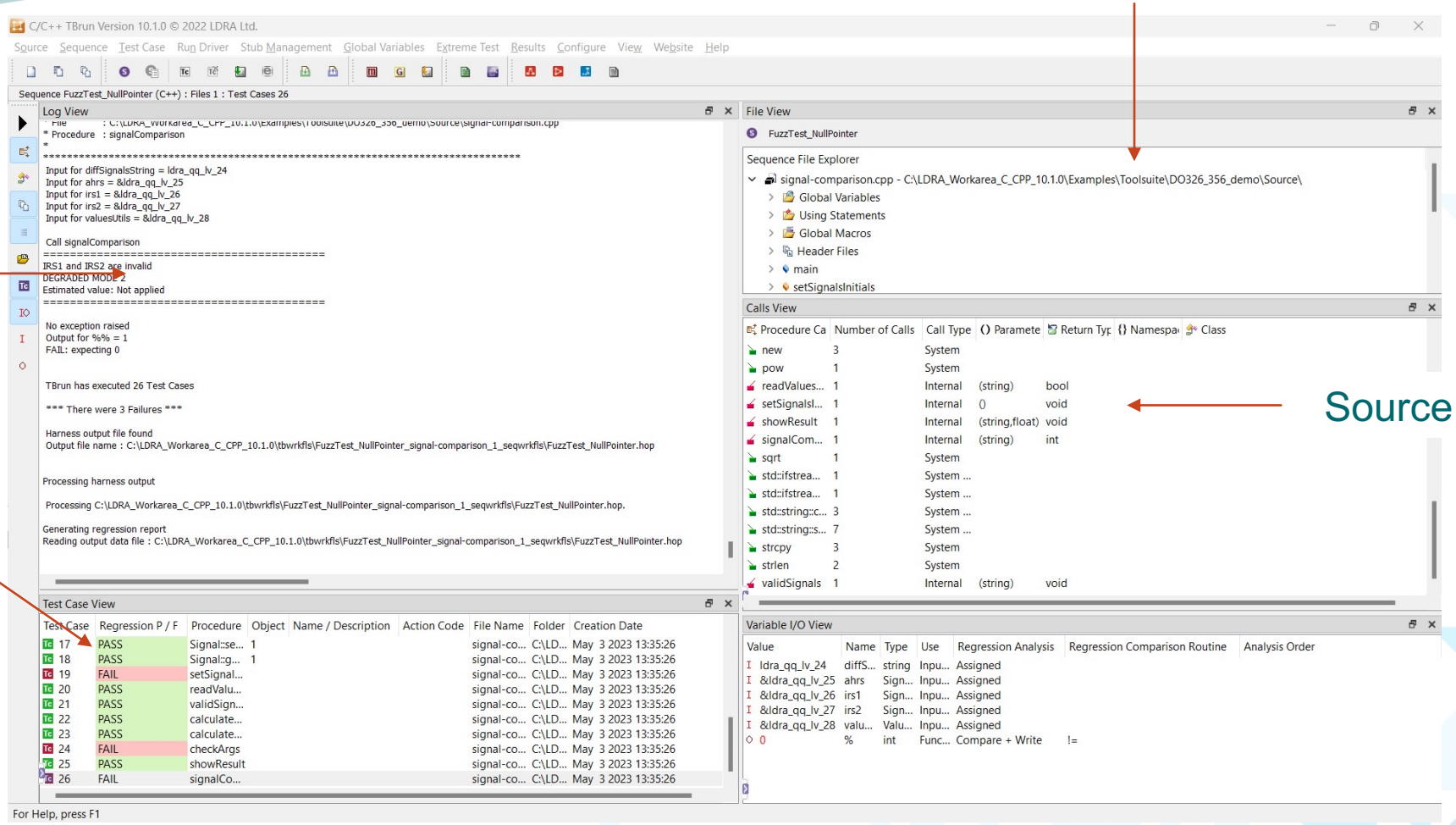
Security functional and robustness verification elements are developed, validated and performed

Source Code

Test Case Logs

Source Code Calls

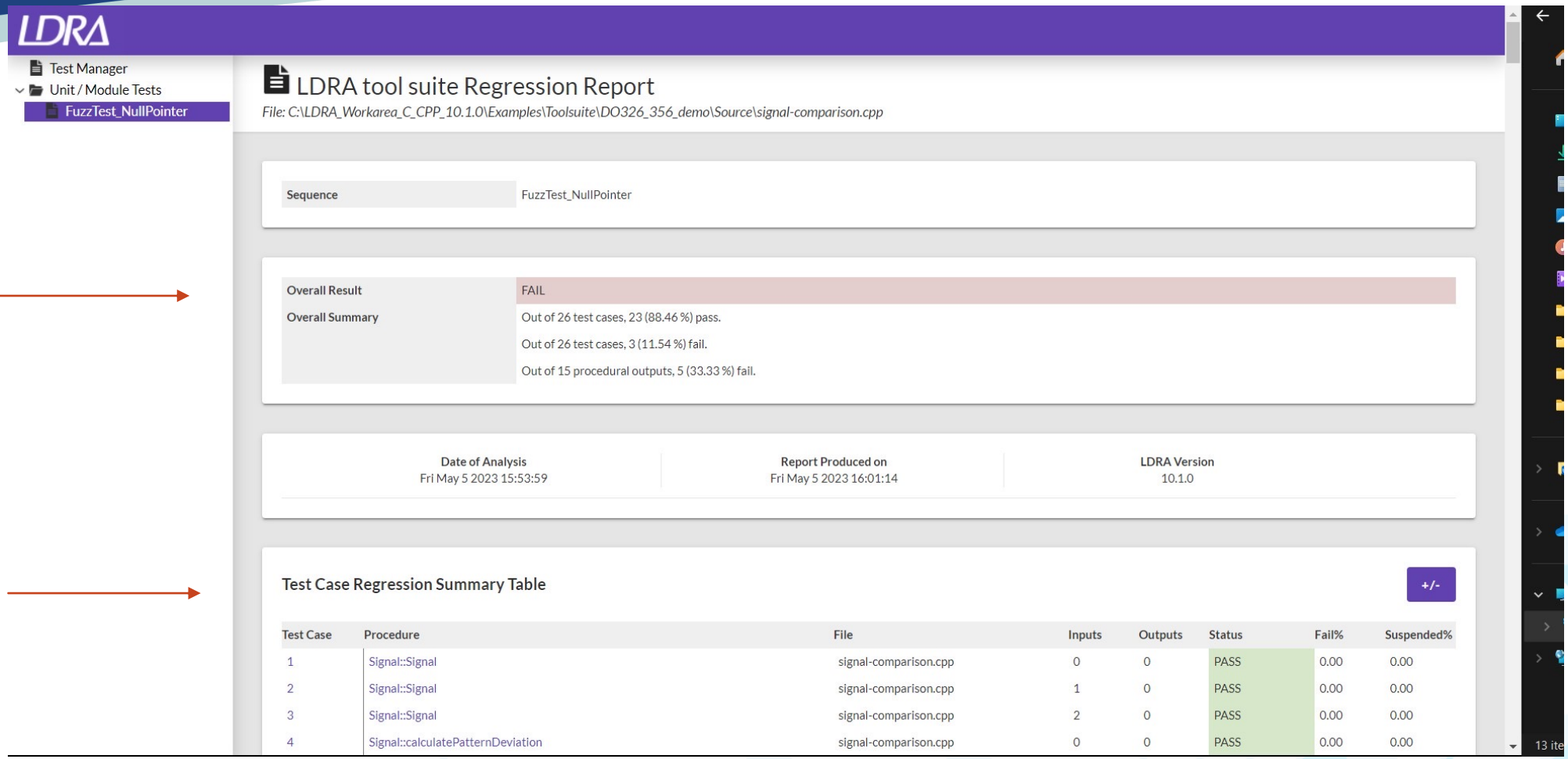
Pass/Fail Results



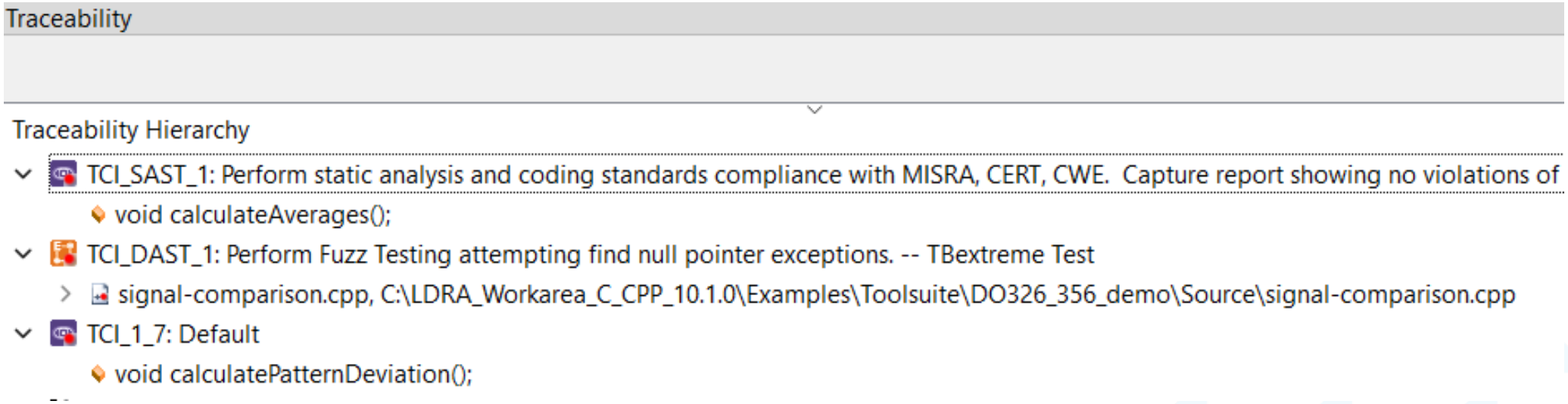
Security functional and robustness verification results are complete and correct

Report Summary →

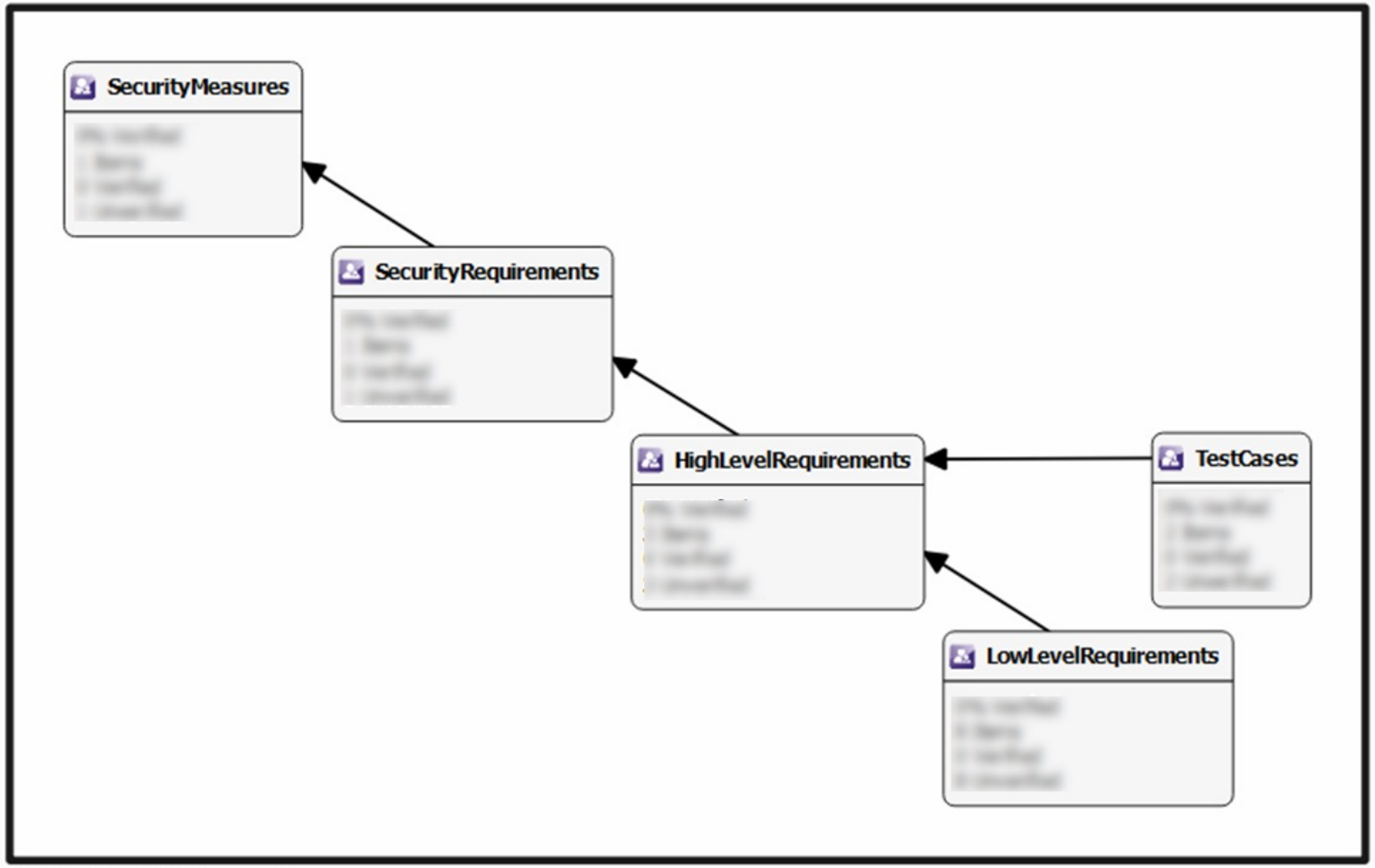
Report Details →



Test Coverage of Software is Achieved



Test Coverage of Software is Achieved



Summary

Important capabilities for Verifying Security in a Safety Context include:

- Applying the Airworthiness Security Process
- Tracing Security Measures to Requirements and Tests
- Using SAST and DAST to Identify and Mitigate Security Vulnerabilities
- Improving Assurance through Refutation Testing

Using Jama Connect with the LDRA tool suite provides a comprehensive solution to manage assets, architecture, vulnerabilities, security threats, security requirements and the verification tests, reducing the time, cost, and risks of compliance with DO-326A/DO-356A and achieving airworthiness

Q&A

Jama software®

LDRA

Thank You

Jama software®

LDRA