June 13 , 2012

High-Integrity Programming: Reviews and Tests

José F. Ruiz

Senior Software Engineer
AdaCore

Ada-Europe 2012, Stockholm

T

Products

AdaCore Offering at a Glance

Development Tools

- All-in-one IDE
- Compiler
- Debugger
- Multilanguage support

Verification Tools

- Testing
- Static Analysis
- Formal Proof

Certification Evidence

- Run-time certification
- Tool qualification
- Traceability analysis

Training

- Language
- Toolset

Support

- Online Support
- Online Consulting

Development

- Enhancements
- Tools
- Run-times
- Ports

Supported Platforms

Native

- Windows
- Linux
- Mac OS X
- Other UNIX (Solaris, AIX, HP-UX, Tru64…)
- OpenVMS

Cross

- VxWorks 5
- VxWorks 6
- VxWorks 653
- VxWorks 6 Cert
- VxWorks MILS
- ELinOS
- LynxOS
- .Net

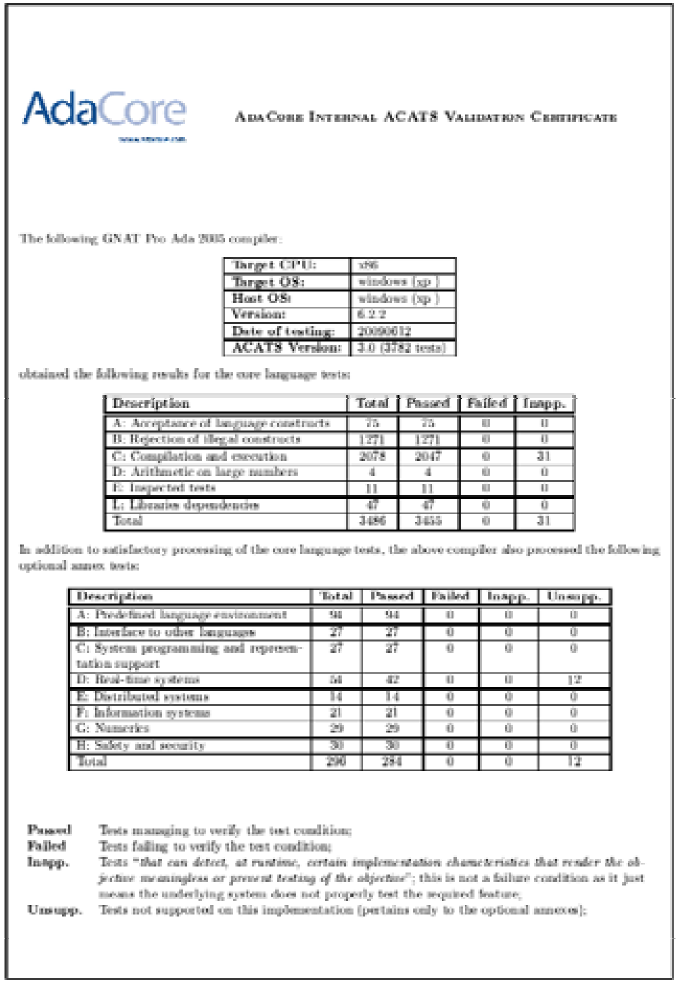
Bareboard

- PowerPC
- ERC32
- LEON2/3
- AVR

Processors

- x86
- x86-64
- SPARC (32 & 64 bit)
- PowerPC
- MIPS
- Itanium
- Alpha
- PA-RISC
- AVR

All Annexes Supported – e.g. Windows



AdaCore

www.adacore.com

ADACORE INTERNAL ACATS VALIDATION CERTIFICATE

The following GNAT Pro Ada 2005 compiler:

Target CPU:	x86
Target OS:	windows (xp)
Host OS:	windows (xp)
Version:	6.2.2
Date of testing:	20090612
ACATS Version:	3.0 (3782 tests)

obtained the following results for the core language tests:

Description	**Total**	**Passed**	**Failed**	**Inapp.**
A: Acceptance of language constructs	75	75	0	0
B: Rejection of illegal constructs	1271	1271	0	0
C: Compilation and execution	2078	2047	0	31
D: Arithmetic on large numbers	4	4	0	0
E: Inspected tests	11	11	0	0
L: Libraries dependencies	47	47	0	0
Total	3486	3455	0	31

In addition to satisfactory processing of the core language tests, the above compiler also processed the following optional annex tests:

Description	**Total**	**Passed**	**Failed**	**Inapp.**	**Unsupp.**
A: Predefined language environment	94	94	0	0	0
B: Interface to other languages	27	27	0	0	0
C: System programming and representation support	27	27	0	0	0
D: Real-time systems	54	42	0	0	12
E: Distributed systems	14	14	0	0	0
F: Information systems	21	21	0	0	0
G: Numerics	29	29	0	0	0
H: Safety and security	30	30	0	0	0
Total	296	284	0	0	12

Passed Tests managing to verify the test condition;

Failed Tests failing to verify the test condition;

Inapp. Tests "*that can detect, at runtime, certain implementation characteristics that render the objective meaningless or prevent testing of the objective*"; this is not a failure condition as it just means the underlying system does not properly test the required feature;

Unsupp. Tests not supported on this implementation (pertains only to the optional annexes);

AdaCore Products for Software Development

Development Environment

GNAT PRO

Core Package

- GPS
- Compiler
- Debugger
- Multilanguage support

Static Analysis Package

- GNATmetric
- GNATcheck
- GNATstack

Code Quality & Testing Package

- Code Coverage (native)
- Code Profiling (native)
- Auto doc generator
- Unit testing framework

Service

- Customer web account
- Support
- Online consulting
- Access to intermediate releases

AdaCore Products

Development Environment

Static Analysis

QA & Testing for Embedded

AdaCore Products for Certification

Tool Qualification

- Coding Standard Checker (GNATcheck)
- Code Coverage (GNATcoverage)
- Static Stack Size Analyzer (GNATstack)

Structural Code Coverage for DO-178B/C Level A

- Traceability Study

Certification Material

- For GNAT Pro Ada run-times
  - Ravenscar
  - Cert

DO-178C Training

- Object Oriented Techniques for the development of certified software (DO-332)

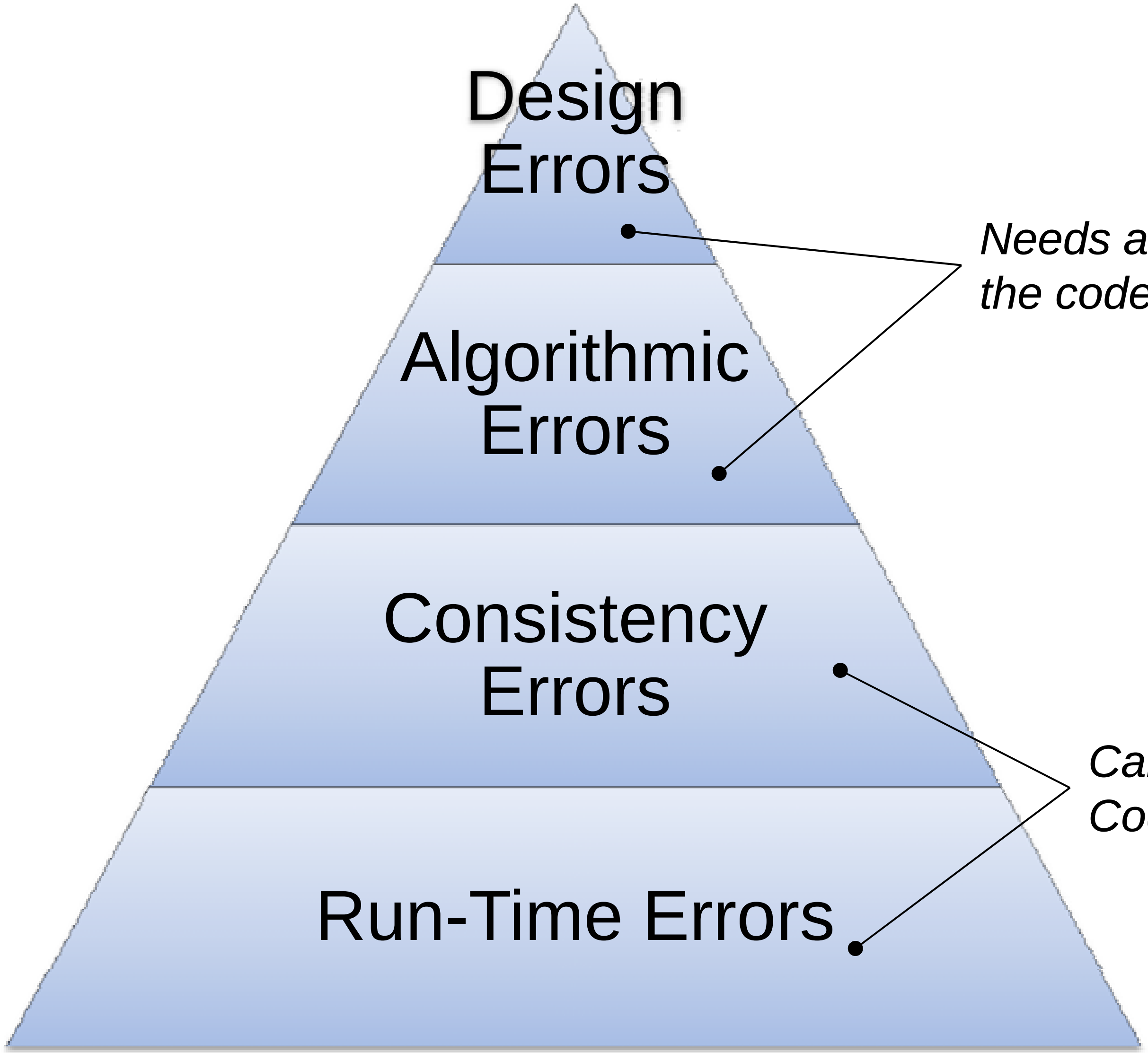
GNAT Pro Add-Ons

- **Portable Graphical User Interface - GtkAda**
  - Object-Oriented GUI Programming
  - Portable and Efficient Implementation (Windows, Linux, Solaris, and others)
- **Web Interface to Ada Applications - AWS**
  - Web Browser to Monitor/Control Ada Applications
  - No Extra Web Server Needed
  - Available on Native Platforms, VxWorks 5.5 & VxWorks 6
- **Distributed Systems Development - PolyORB**
  - CORBA Support
  - Ada Distributed Systems Annex Support
- **Semantic Ada Source Code Analyzer - ASIS**
  - Easy Development of Semantic Analysis Tools

CodePeer

Automated Code Review and Validation

Error Classification



Needs additional information than the code (specification, models…)

Can be deduced from the code
CodePeer will work on these

Peer Review

- Best practice in Extreme and Agile programming
- Improve code quality
- Reduce errors

But…

- Requires initial effort to setup infrastructure
- Needs to sustain project pressure
- Often bypassed

Alleviating Peer Review Process

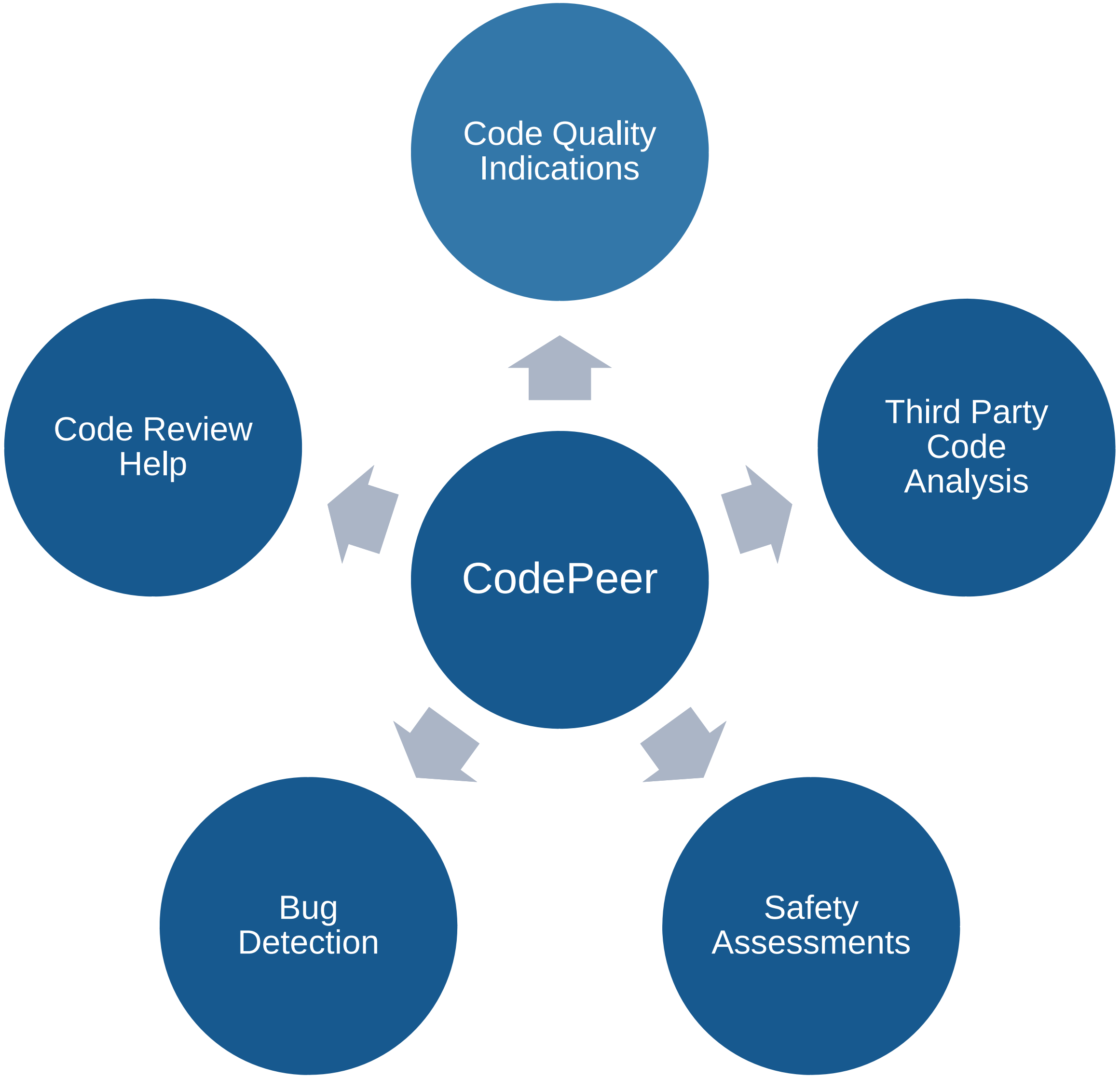
Certain categories of verifications

- Can be automated
- Are better handled by tools

CodePeer provides:

- Static analysis
- Symbolic program interpretation
- Incremental & modular analysis

CodePeer Usage



CodePeer

Code Quality Indications

Third Party Code Analysis

Safety Assessments

Bug Detection

Code Review Help

CodePeer in Action

CodePeer

- Static run-time errors detection
- Test vectors generation
- Pre/post conditions generation
- Analysis results consolidation

Day-to-day development

- compile-time analysis
- local analysis

Software maintenance

- global change impact analysis

Project quality assurance

- global analysis
- test vectors leverage

CodePeer Area of Action

Ada Run-Time Checks

- out-of-bound indexing
- numeric overflow/out of range
- division by zero

User Checks

- Assert statements
- if … then … raise … control flow

Programming Errors

- Uninitialized variables
- Never ending subps/loops
- Race conditions
- Dead code

T

GNATtest

Unit Testing Development

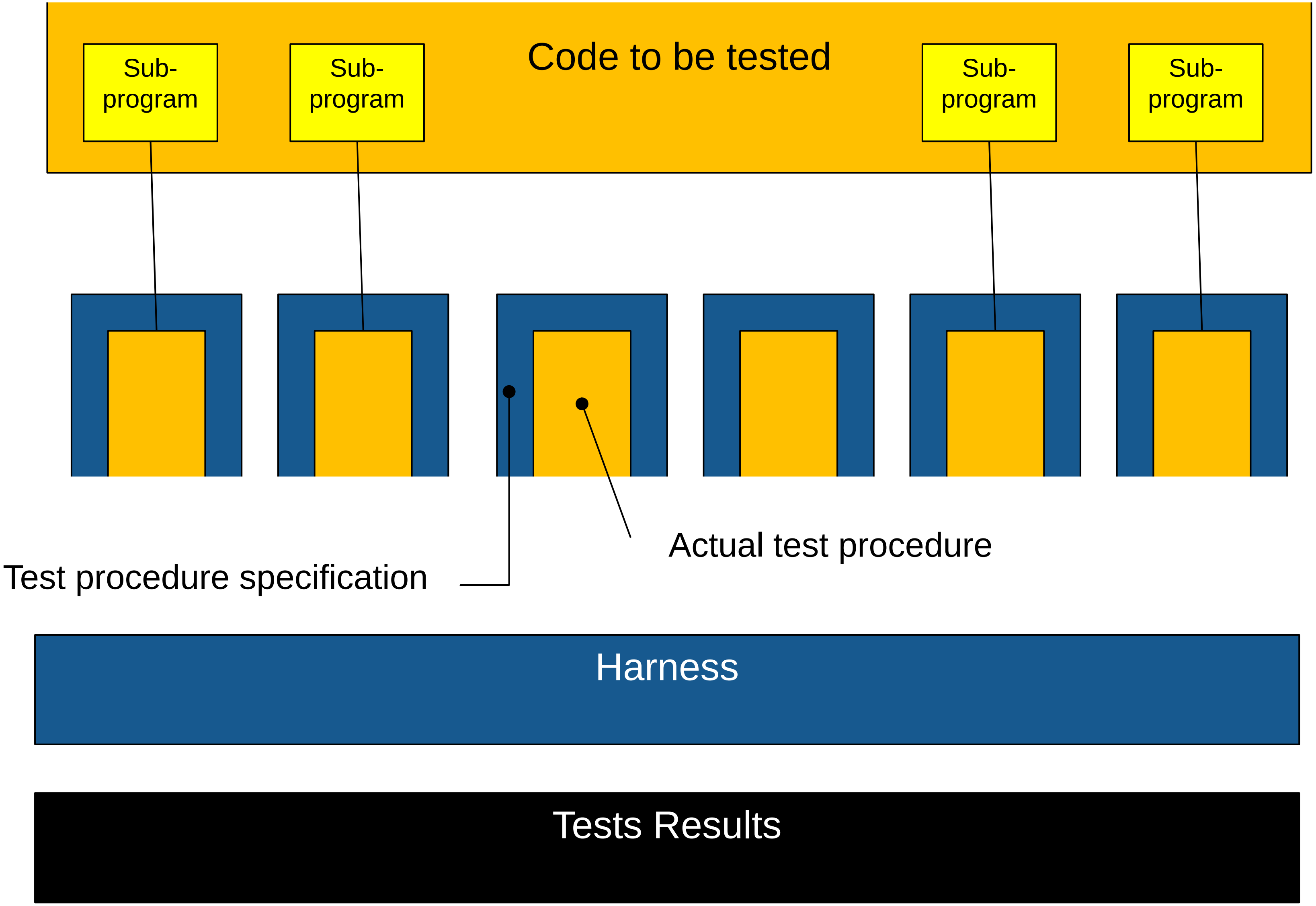
- **Developing unit testing is cumbersome**

- **There’s a lot of work involved in task of little value**
  - Framework and rules specification (for generics, classes…)
  - Harness development
  - Maintenance and update when new subprograms are added

- **Ideally, developers should concentrate only on test procedure development**

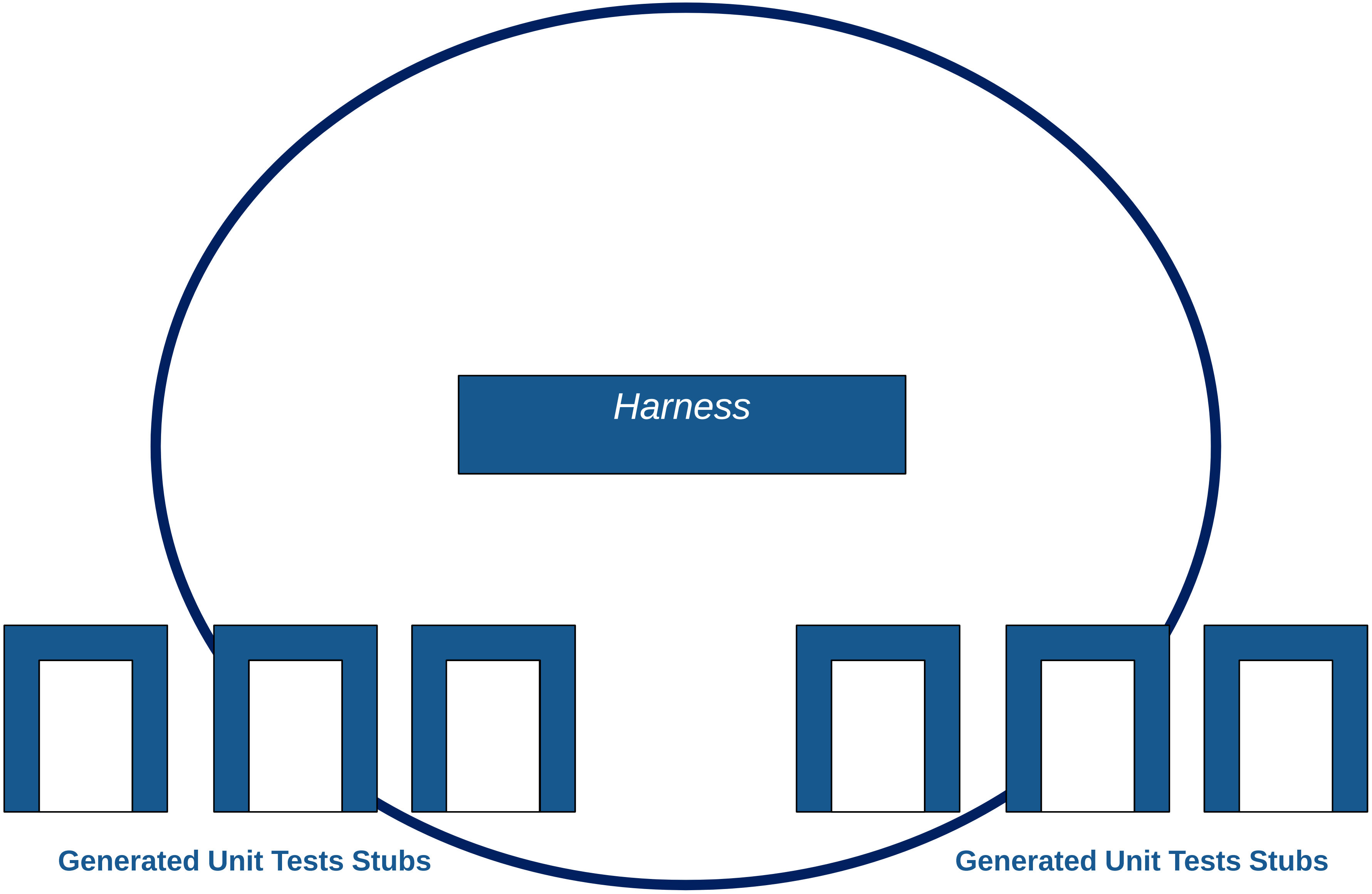
Automatic Generation of Test Harness

What Can Be Automated?



Maintenance of Unit Tests

Maintenance of Unit Tests

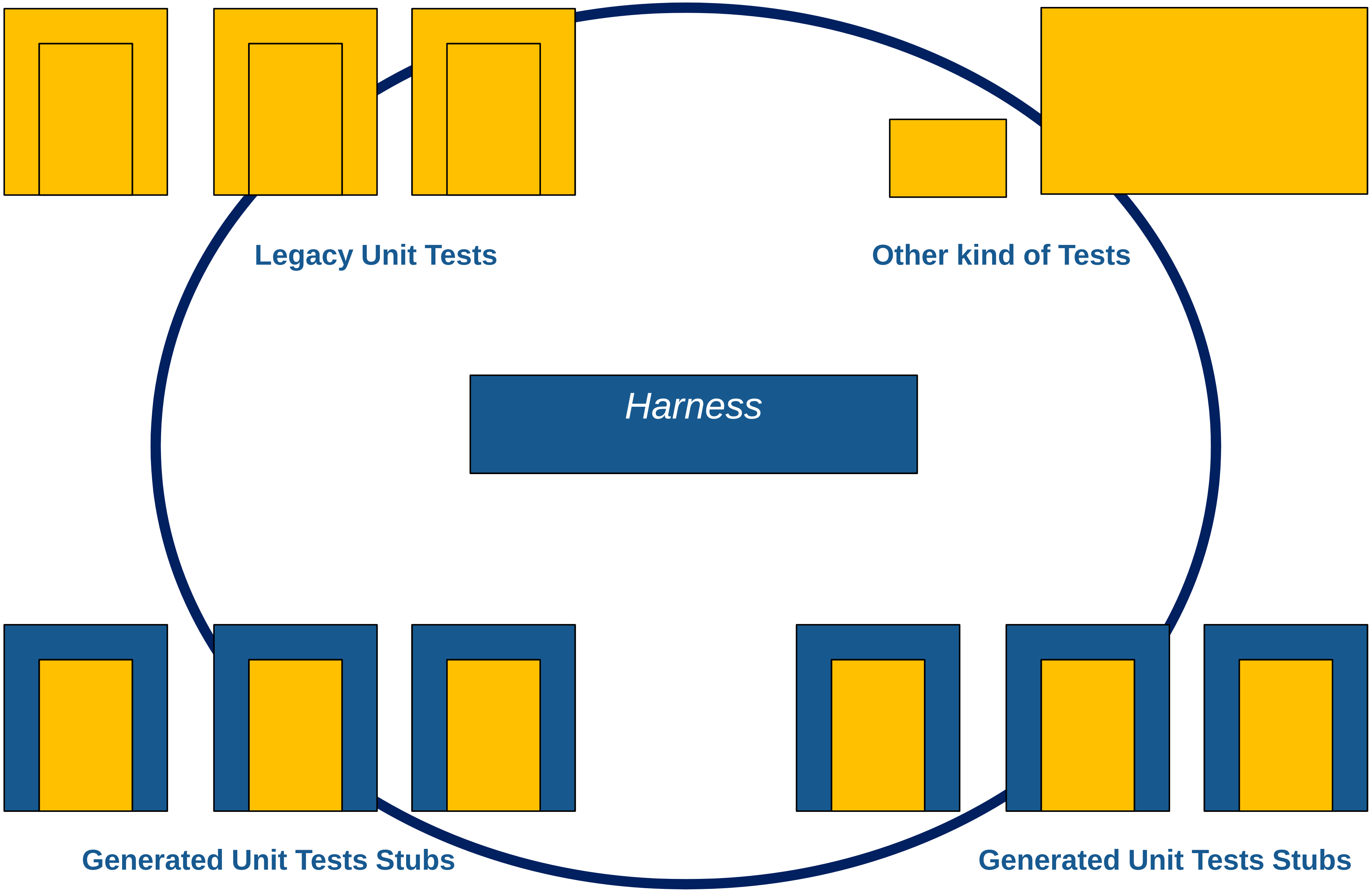


Generated Unit Tests Stubs

Generated Unit Tests Stubs

Integration of Independent Tests

Integration of Independent Unit Tests



Legacy Unit Tests

Other kind of Tests

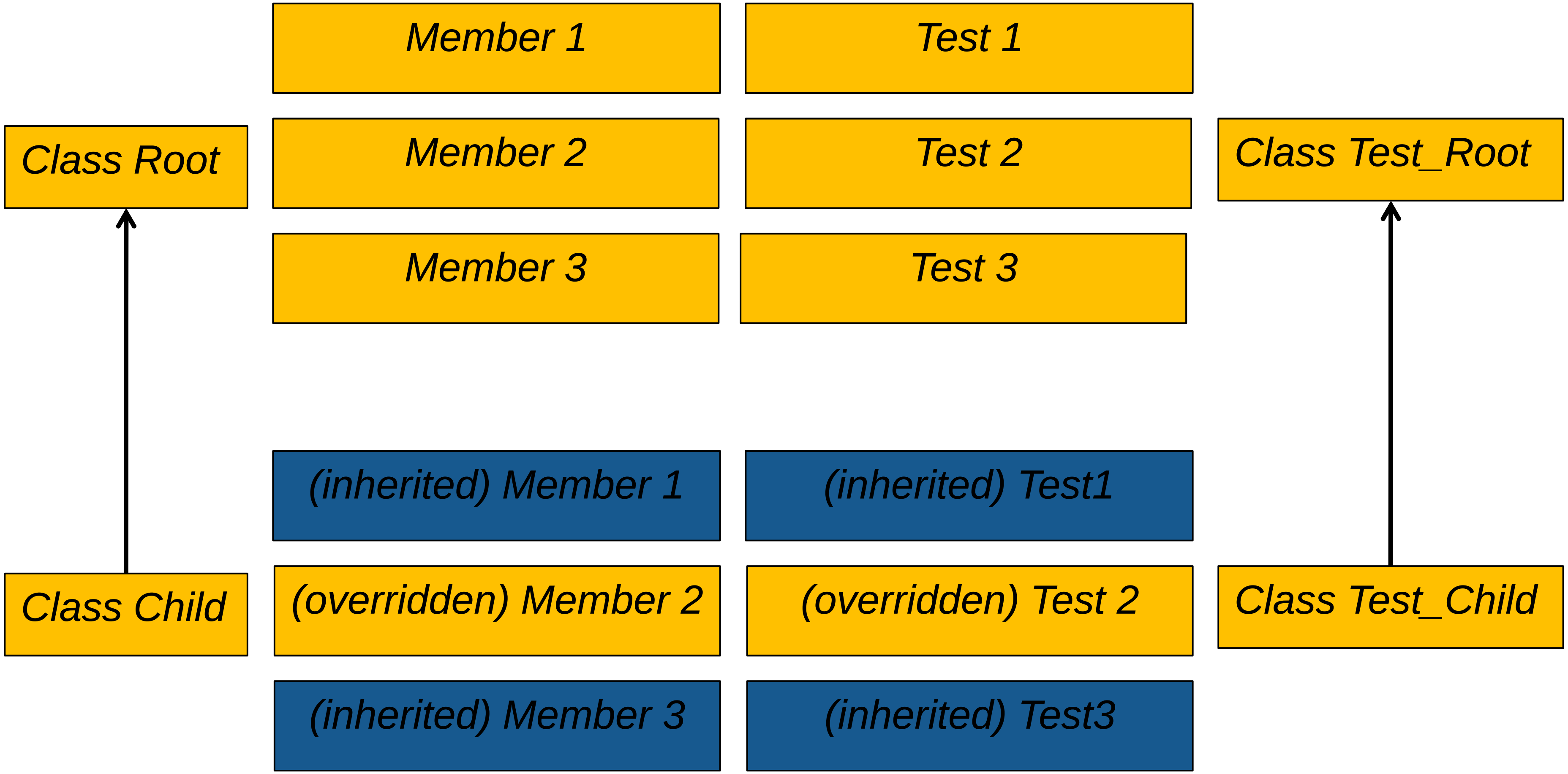
Harness

Generated Unit Tests Stubs

Generated Unit Tests Stubs

Dedicated support for Object Orientation

Dedicated Support for Object Orientation



Class Root

Member 1

Member 2

Member 3

Test 1

Test 2

Test 3

Class Test_Root

Class Child

(inherited) Member 1

(overridden) Member 2

(inherited) Member 3

(inherited) Test1

(overridden) Test 2

(inherited) Test3

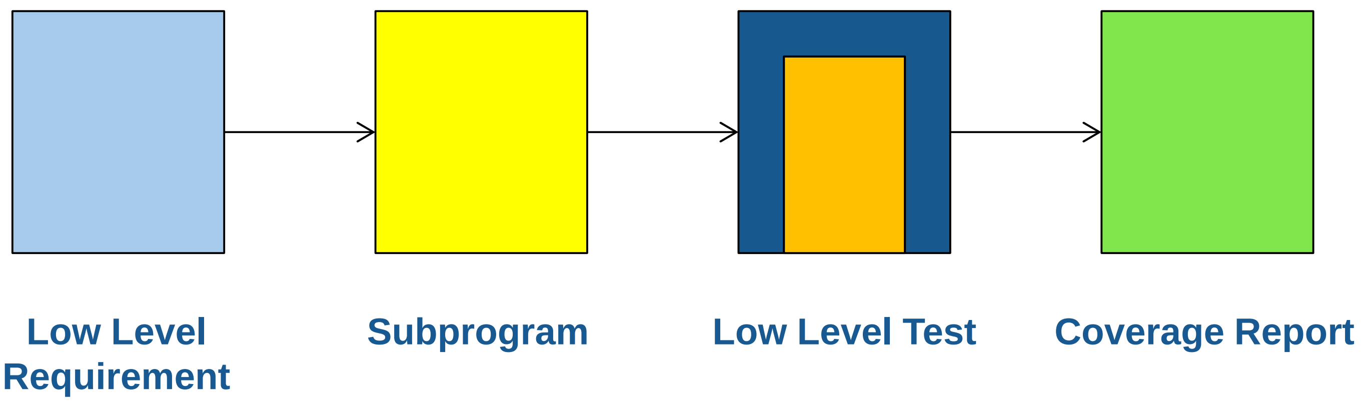
Class Test_Child

Integrated with GPS

DO-178C-Ready

DO-178C-Ready

- **Natural path from DO-178 low level requirements to structural coverage**



- **Liskov substitution verification implemented, to support OOP supplement of DO-178C**

Ada 2012-Ready

Ada 2012-Ready

```
function Sqrt (X : Integer) return Integer with
   Test_Case => (Requires => X = 100,
                 Ensures  => Sqrt’Result = 10),
   Test_Case => (Requires => X < 0,
                 Ensures  => Sqrt’Result = 0);

procedure Sqrt_Test_1;

procedure Sqrt_Test_2;
```

Available for Native, Cross and High-Integrity Platforms