VALIDATION

Version 1.0
8 May 1989

presented by

DONALD G. FIRESMITH

President
Advanced Software Technology Specialists
3418 Broadway
Fort Wayne, IN 46807
U.S.A.

- Validation is the official DoD testing process used to demonstrate that a candidate Ada compiler conforms with the Ada language standards as defined in ANSI/MIL-STD-1815A-1983.

- The goal of Ada validation is to:
  - Ensure compliance to ANSI/MIL-STD-1815A-1983.
  - Prevent the proliferation of subsets, supersets, and dialects of the Ada programming language.

- Policy regarding validation is documented in "Ada Compiler Validation Procedures and Guidelines" Version 1.1 (NTIS accession number AD-A178154) published by the AJPO on 1 January 1987. This document is in the process of being updated.

- Validation means having passed ALL applicable tests in the Ada Compiler Validation Capability (ACVC) test suite.

- Ada Compilers must be validated by an Ada Validation Facility (AVF) managed by the Ada Validation Organization (AVO) of the Ada Joint Program Office (AJPO). These organizations make up the Ada Certification Body.

- The ACVC test suite consists of the following six classes of tests:

  A) Legal tests that must be compiled without error.
  B) Illegal tests that must be detected at compile time.
  C) Legal tests that must execute correctly.
  D) Capacity tests.
  E) Tests of Implementation-dependent features.
  L) Illegal tests that must be detected at link time.

- ACVC test suite tends to test simple capabilities rather than capacity or synergistic issues.

- New tests are being rapidly added to the ACVC test suite (approximately 20% to 30% per year):

- As of October 1988, ACVC test suites last 18 months and validation certificates now expire one year after the relevant test suites expire.

- A Validation Certificate may now be valid as long as 2.5 years.

- The Ada Compiler Validation Capability Implementers Guide (AIG) by John Goodenough (NTIS accession number AD-A189647) describes the conditions to be checked by validation tests.

- ACVC version 1.10 covers 76.4% of the test objectives of the AIG, and ACVC version 1.11 is expected to cover the rest.

- New tests in ACVC 1.10 will concentrate on generics (LRM Chapter 12) and Representation Clauses and Implementation-Dependent Features (LRM Chapter 13):

- Although NO compiler implements 100% of the Ada language, compiler vendors often falsely advertise that their compilers "comply fully with the Department of Defense ANSI/MIL-STD-1815A specifications."

  What these exagerated claims really mean is that the compilers have passed the current validation test suite.

- Validation is for a specific configuration (i.e., host/OS and target/OS combination).

- There are three types of validated Ada compilers:
  - Base compiler:

    An Ada compiler that:

    * Has passed the applicable ACVC tests at an Ada Validation Facility (AVF) or at a vendor site under witness of AVF personnel.
    * Therefore has been judged to minimally conform to the Ada programming language standard.
    * Has a current validation certificate.

- Derived compiler:

  A base compiler used on an equivalent configuration or a slight modification of a base compiler used on a an equivalent or closely-related configuration that:

  * Has been successfully tested BY THE VENDOR.
  * Has been registered with the AJPO.
  * Has been certified by the vendor to conform to the Ada programming language in every respect and by the same measure as does the base compiler from which it was derived.

  No validation certificate is issued.

- Project-validated compiler:

  A validated compiler that is project baselined and that is considered validated for the duration of the project even if the associated base compiler's validation lapses.

  A project-validated compiler may be derived when the developer customizes the runtime library for a specific project.

  A project-validated compiler need not be capable of running all ACVC tests so long as it supports all mandatory Ada features that the restricted target can support.

  The vendor need not continue to support project-validated compilers.

- A list of the current validated compilers and their associated host/target configurations can be obtained from the Ada Information Clearinghouse (AdaIC).

- To obtain more information about a specific compiler, ask the vendor or AVF for a copy of the Validation Summary Report (VSR). Note that the AVFs have a history of being late in delivery of the VSR to the vendor.

- According to SofTech, validated compilers may be ranked in order of increasing risk as follows:

  1. Validated base compilers (for base configuration).
  2. Unmodified derived compilers (for new configuration).
  3. Modified derived compilers (for new configuration).
  4. Unmodified project-validated compilers (for generic target).
  5. Modified project-validated compilers (for generic or restricted target).

- Validation is lost if:
  - The validation certificate expires.
  - The ACVC is updated and the base or derived compiler no longer passes all tests.
  - The compiler is modified (e.g., RTS customization).
  - The configuration is modified (e.g., new OS version, new target board).
  - A derived compiler is found to fail an ACVC test.
- Although compiler maintenance may introduce changes that violate ANSI/MIL-STD-1815A and would cause the maintained compiler to fail a relevant ACVC test, maintenance (by itself) does not cause a compiler to lose its validation status so long as new version(s) of the compiler are:
  - Clearly distinguished and
  - Not known to fail any ACVC tests.

  Retesting is NOT required.

- According to the Federal Software Testing Center in Virginia, "Even with the relative immaturity of the Ada language, the stringency of the Ada validation test suite assures a more complete compliance with the language standard than does any other programming language."

- Although validation ensures that Ada compilers are very reliable, all complex software contains bugs.

- During the development of the 11th Missile Application of the Common Ada Missile Packages (CAMP) Program, 57 software errors were found in the CAMP-developed software and 96 compiler errors were found.

- Ada compilers have even been known to report errors in error-free code.

- Lack of reliability is most often due to the immaturity of most Ada compilers and language features not covered by the ACVC.

- Because the ACVC test programs are relatively small, they do not saturate symbol tables or library files used by Ada compilers. Therefore, stress tests are necessary to determine if the compiler will handle a large enough application.

- Validation does not replace the "trial by fire" provided by many users.

Validation does NOT mean:

- Absolutely compatible with the LRM.
- Totally bug-free, reliable, or robust.
- High capacity.
- Efficient on the host computer:
  - Fast compiler installation time.
  - Fast compilation speed.
  - Fast link/load speed.
  - Small compiler size.
- Efficient on the target computer:
  - Fast object code.
  - Small object code.
  - Small runtime system.

Validation also does NOT mean:

- User-friendly compiler services (e.g., error messages).
- Adequately supported by the vendor.
- Tested on real (or similar) projects.
- Suitable for all (or most) applications (e.g., support of embedded real-time features).

- Validation does not test:
  - Optional or implementation-dependent features (e.g., pragmas, order of evaluation). Thus ACVC Test Suite 1.10 only tests approximately half of the requirements of LRM Chapter 13.
  - Support tools other than the compiler.

    Except for the CAIS Implementation Validation Capability (CIVC) test suite scheduled for completion by SofTech by June 1989, there are no AJPO-sanctioned validation test suites for validating APSE software other than the compiler (and optimizer and RTS).
  - All features of the Ada runtime system.

- Validation is therefore a minimum, but NOT sufficient, requirement.

- According to the AJPO policy as defined in "Ada Compiler Validation Procedures and Guidelines", compiler users are responsible for understanding the scope and limitation of the validation process:

  "Users are cautioned that validation does not imply or warrent the use of an Ada compiler for any application, nor does it provide an evaluation of compiler efficiency or performance."

- Because the AJPO let the Ada trademark lapse on 1 December 1987, ensure that all validated compiler products and documentation display the Ada Certification Mark: