Extended Abstract

Software Conformance – extending the meaning of I V & V[1]

S. Parthasarathy
Algologic Research & Solutions
78 Sancharpuri Colony
Bowenpally P.O.
Secunderabad – 500 011 – INDIA

drpartha@gmail.com

Keywords *:* automation, software, formal methods, railways, safety, verification, validation, proof, abstraction.

Preamble

This paper gives an overview of "software conformance", a concept promoted by Algologic Reserarch & Solutions. Traditionally, I V&V has been concerned only with "operational correctness" of prpgrams, seen as adherence to specifications. In the case of safety critical systems, this view is not enough. Many more techno-legal issues are involved. One such issue is that of conformance to standards.

Software Conformance Services

The IEEE Standard ANSI / IEEE Std. 729-1983 defines verification and validation as:

validation:

- the process of evaluating the software at the end of the software development process to ensure compliance with software requirements

verification:

- the process of determining whether or not the products of a given phase of the software development cycle fulfil the requirements established during the previous phase
- formal proof of program correctness

The seminal book [2] by Stephen J Andriole explicits that:

- **validation** determines the correctness of the end product
- **verification** is performed at each phase and between each phase of the development life cycle

We notice the emphasis on "operational" correctness, as highlighted by the software complying to the expectations. In addition to the "correctness" of the product and processes, compliance to appropriate standards is an indispensable part of software development for mission-critical applications. Mission-critical software may be expected to comply with domain-specific standards (e.g. CENELEC), or domain-independent standards (e.g. IEC 61508), or process standards (e.g.

1Paper proposed for : 2nd International Workshop on Education and Training for Quality Software Engineering, October, 2006, Beijing, CHINA

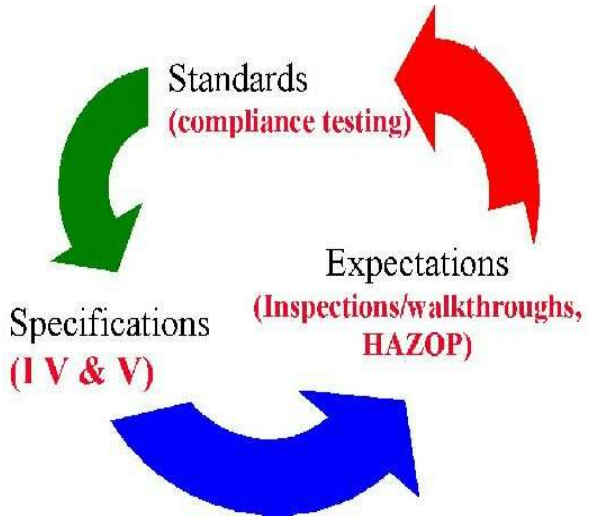
SEI/CMM, ISO900x). In all cases, a rigorous approach is needed for assessing the level of standards compliance.

So, we add "standards compliance" to the above:

- **standards compliance** is the act of identifying appropriate standards for a given software and verifying the adherence of the software to the standards.

This paper therefore includes this important dimension to V & V -- that of conformance to standards -- and has launched its Conformance Services Division which can be a one-stop source for a wide range of services related to verification, validation and standards compliance.

- **Conformance Services** may be defined as an integrated approach to verification, validation and standards compliance.



This paper proposes a holistic and integrated approach, to software conformance. The approach would rely heavily on sound mathematical principles which also take into account human attitudes and cultural background of the developers and end-users.

The literature on V & V strongly recommends that V & V should be always done by an agency which is managerially and financially independent of the software design and development team. This gives rise to the "independent" suffix for V&V, making it IV&V.

In this document, IV&V should be understood as conformance services, as defined above. These conformance services involve assistance in the following areas:

- development of formal specifications
- review of existing specifications
- vulnerability and hazards analysis
- design reviews
- verification services
- product validation
- program flow analysis
- documentation audit
- usability analysis
- design of test plans
- coding guidelines and style reviews
- test coverage analysis
- selection and evaluation of applicable standards
- configuration management
- standards conformance assessment
- training
- Consultancy, and contracted research

IV&V including conformance services is subject to several practical constraints:

1. In this document, IV&V should be understood as a service consisting of an integrated approach to : verification, validation and standards conformance.

2. An IV&V report does not amount to any confirmation of the product being defect-free. This is because formal IV&V is itself still a matter of research and discovery. Moreover, by its very nature, mission-critical software is a complex entity. The tools and technologies used are still subject to debate and controversies.

3. The dependability of an IV&V investigation is subject to several imponderables. IV&V of software will depend on the form in which the specifications and design are available. To be able to perform a formal IV&V, the specifications and the design should be in a formally verifiable form. English language specifications or design will first have to be converted into a formally verifiable framework. This translation itself could be erroneous or defective.

4. The conclusions of an IV&V depend largely on the honesty, cooperation and and transparency of the developing agency whose product is being verified.

5. IV&V is a time consuming activity. Please do NOT impose unreasonable time schedules to complete and IV&V.

6. IV&V does not include prescription or suggestion of any remedial measures. The developing agency must take all necessary steps, to repair or mitigate the flaws discovered by the IV&V process.

7. Although there are industry/domain specific standards on how a mission-critical software should be developed, there is still no consensus or standard as to how the conformance to standards should itself be verified. In case any such standard exists for performing IV&V, the client is free to suggest the standard for performing IV&V.

8. The IV&V auditor does not accept any responsibility or liability for the consequences of using a software on which IV&V has been done.

Conclusions :

This paper extends the concept of IV&V, to include confirmation of conformance to standards. There is a great need for such an extension, in cases which inlvove safety, particularly of a large number of people, like in the case of railways automation. Some of the constraints encountered in safety critical systems is also discussed briefly.

References :

1. Stephen J Andriole "*Software validation, verification, testing and documentation*" Pub. Petrocelli Books, NJ. USA
2. IEEE IEEE Standard Glossary of Software Engineering Terminology, ANSI / IEEE Std. 729-1983 , Pub.: IEEE Press
3. S. Parthasarathy *The burden of proof* Technical Report (on formal proof of program correctness), Pub.: Algologic Research & Solutions, Secunderabad, India, Sept. 2001
4. *S. Parthasarathy Notation, method, tool: A conceptual framework for the application of formal methods.* IFAC Symp. Control in Transportation Systems 2000, Braunschweig, Germany, June 2000.

5. *S. Parthasarathy The explication problem: Achille's heel of formal methods.* Entwicklung und Betrieb komplexer Automatisierungssysteme (EKA´99), Braunschweig, Germany, May 1999.

****