V&V Measurement Management Tool for Safety-Critical Software

Edgardo Palza, Alain Abran*, Christopher Fuhrman*, Eduardo Miranda***

**École de Technologie Supérieure – ETS*
1100 Notre-Dame Ouest, H3C 1K3 Montréal, Québec, Canada.

*** Ericsson Research Canada*

8500 Blvd. Decarie H4P 2N2, Montréal Québec, Canada

edgardo.palza-vargas.1@ens.etsmtl.ca,

aabran@ele.etsmtl.ca,

christopher.fuhrman@etsmtl.ca

eduardo.miranda@ericsson.com

Abstract:

This paper presents a V&V Measurement Management Tool (V&V MMT) to support the Management of V&V activities in the context of safety-critical software. We illustrate how V&V MMT can facilitate the quantification of the V&V processes, activities and tasks in projects recommended in the IEEE Standard for Software Verification and Validation (IEEE Std. 1012-1998) for facilitating the establishment of V&V measurement indicators: (1) Software Verification and Validation Plan (SVVP), (2) Baseline change assessment, (3) Management Review of V&V, (4) Management and Technical Review Support, (5) Interface with Organizational and Supporting Process.

Keywords

Verification and Validation, Safety Critical Software, Measurement Repository, Measurement Meta-model, Measurement Management.

1 Introduction

Today's software is becoming increasingly more complex: heterogeneous composition on a diversity of platforms, distributed execution, complexity in calculation algorithms, multiplicity of contractors with diverse development methodologies, etc. The result of such complexity is increased risk and higher costs in software projects.

The type of software that, directly or indirectly, ensures the safety of human life or significant financial investments is referred to as safety-critical software. This type of software is required to meet very high levels of safety and reliability and

to meet demanding quality standards. Therefore, the related development process must be tightly managed, because of the very high level of quality required. Indeed, many accidents caused by deficient quality of critical software have been reported in the software engineering literature (Therac 25 [1], Ariane 5 [2], *etc.).*

Software Verification and Validation (V&V) is a set of activities whose goal is to foster software quality during the development life cycle. V&V can represent up to fifty percent of the budget in software/system critical projects [3]. For safety-critical software, risk mitigation is very important [4]. Many software projects, for instance within NASA and elsewhere, involve software V&V activities to mitigate certain software development risks.

In this paper we propose a V&V Measurement Management Tool (V&V MMT) for safety-critical software. This tool is based on a measurement meta-model repository [5], [6]. It is important to note that the proposed V&V MMT supports the IEEE Standard for Software Verification and Validation (IEEE Std. 1012-1998) [7]. The software processes described in [7] include: management, acquisition, supply, development, operation, and maintenance. This IEEE standard is also recommended for use in software-intensive projects: for instance, the NASA[1] IV&V Facility's "Program Manager Handbook" [8] makes clear the usefulness of the IEEE Std 1012-1998 [7] and IEEE Std 1059-1993 [9] for the planning and execution of V&V activities in their projects.

The effectiveness of V&V depends on the timeliness of the development processes and on the quality of the deliverables. In this proposal, we discuss how the V&V MMT can help to support measurements activities for Management V&V processes in organizations. Our approach is described in terms of activities, processes and tasks recommended in IEEE 1012, section 5.1. This should facilitate measurements in terms of:

(1) Software Verification and Validation Plan (SVVP).

(2) Baseline change assessment.

(3) Management Review of V&V.

(4) Management and Technical Review Support.

(5) Interface with Organizational and Supporting Process.

[1] - National Aeronautics and Space Administration

2 Safety Critical Software and V&V

Since software has become an important component of critical systems (e.g., in aeronautics/aerospace, power plants, medical devices, chemical plants, automobiles, military weapons, etc.) the impact of software on systems safety has been demanding greater attention in organizations dedicated to the production of this critical software.

For safety-critical software, risk mitigation must be taken very seriously. Many software projects, within NASA and elsewhere, require software verification and validation (V&V) activities to mitigate certain software development risks. Some NASA projects may even require *independent* V&V (IV&V) activities, in which an organization independent from the one developing the software performs the V&V activities during the lifecycle.

Software V&V is a set of activities aimed at attaining software quality during the development life cycle. Although there are several approaches (or models) to planning the life cycle for software development, there are clearly certain disciplines that exist in phases within *any* life cycle. These disciplines include requirements engineering, analysis, design, implementation and testing. At each step along the development life cycle, mistakes can be made, which in turn can affect the quality of the final software product. *Verification* strives to detect and correct mistakes made within each step of the software life cycle—to determine whether the products of a life-cycle activity satisfy the requirements of that activity. These verification activities are not sufficient, however, to assure that the final software product fulfills its intended purpose and meets its users' needs. Therefore, *validation* determines if the software meets the needs for its intended use.

The IEEE Standard for Software Verification and Validation (IEEE Std. 1012-1998) [7]is a process standard that addresses V&V processes with respect to the life cycle processes for software. This standard was designed to be applicable to all life-cycle models, even though not all of these models include the processes contained in the standard. IEEE 1012 has been used by several private and government organizations to structure the V&V activities performed on various projects; for instance, NASA's Independent Verification and Validation Facility (IV&V) uses the IEEE 1012 for the its software IV&V plans.

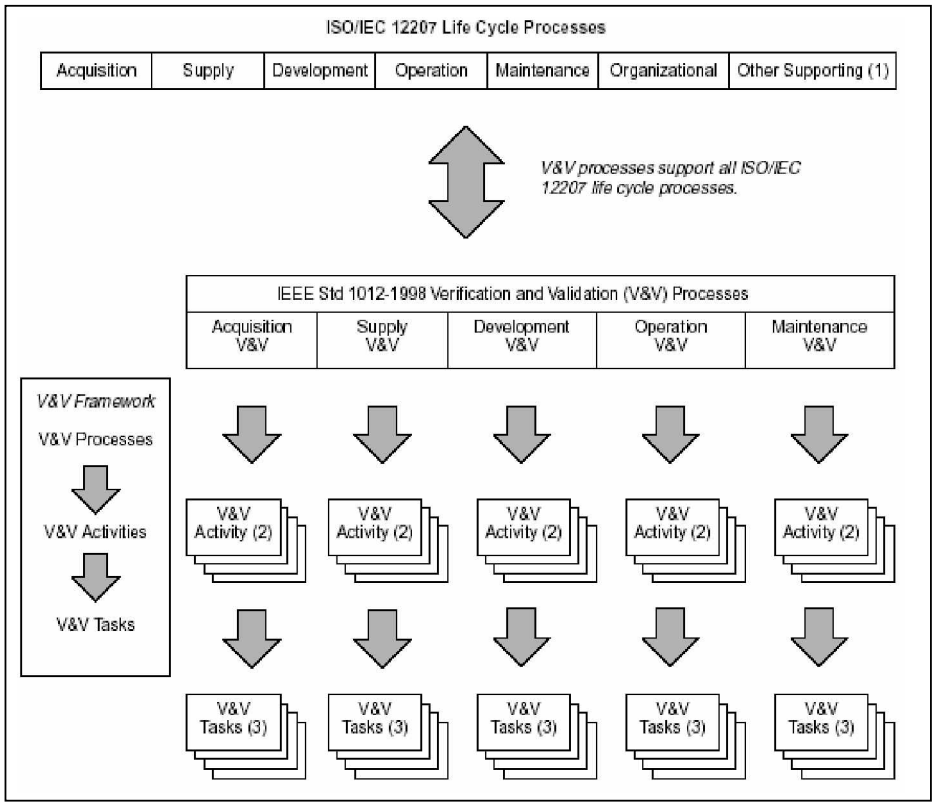

Figure 1: V&V Framework (IEEE 1012)

Figure 1 shows how the IEEE 1012 defines a V&V framework at three levels: processes, activities and tasks. A top-level *process*, such as Development V&V, is comprised of *activities*, such as Concept V&V, Requirements V&V, etc. These are, in turn, comprised of *tasks*, such as Traceability Analysis, Software Design Evaluation, etc. These tasks provide the highest level of detail, including the specific nature of the V&V work to be performed, the required inputs and the required outputs.

A key artefact of the IEEE 1012 is the Software V&V Plan (SVVP), which includes a mandatory section to describe the roles and responsibilities for organizational elements or individuals involved with the software V&V. IEEE 1012 was designed to integrate with the IEEE/EIA 12207.0, a broader standard providing a framework for managing and developing software [10]. Such integration is described in an appendix of IEEE 1012, to facilitate conformance between both IEEE 1012 and IEEE/EIA 12207.0 in development projects where

both standards must be used. The goal of this integration is to avoid unnecessary duplication of documentation or processes resulting from the application of distinct standards.

3 V&V Measurement Meta-model Repository Tool

In this section, we present the basics characteristics of the V&V MMT. The V&V MMT is based on a meta-model repository whose design is documented in [5]. The core of the V&V MMT contains a database structure that does not presuppose any particular measures or relationship between them; the measures themselves are treated as data. These data are referred to as *metadata* -- data that represent measurement data of V&V products and processes.

To meet the constraints of a dynamic measurement environment, the V&V MMT must have a generic database repository with a high level of flexibility. This requires then that the definitions of the V&V measures and their relationships be stored in the repository as a metadata entity. The metadata are a level of abstraction of the V&V measurements rather than the measurements themselves. The metadata entity can then provide the flexibility required by the ever-changing information needs of the organization.

The V&V MMT allows specifying and tracking V&V measures based on ‘base measures’ and ‘derived measures’ as documented in “Practical Software Measurement – PSM” [11] and ISO 15939 [12]. This can be done for all V&V processes defined in IEEE 1012. The data collection and storage mechanisms are next implemented through a database system. The data analysis and reporting indicators are based on Structured Query Language (SQL) and Online Analytical Process (OLAP) cubes. The V&V MMT was constructed, as ISO 15939 requires, following the principle that the Software measurement process be flexible, tailorable and adaptable to the needs of particular users.

The V&V MMT is also designed to facilitate the integration of the concepts of a Measurement Information Model and a Measurement Process Model defined in 15939 [12]. The Measurement Information Model in particular is a structure linking the documented information needs to the relevant entities and attributes of concern. In the case of V&V, those entities include V&V processes, V&V products, V&V plans and resources associates. The Measurement Information Model describes how the relevant V&V attributes are quantified and converted to *indicators* that provide a basis for a V&V decision-making..

4 V&V Measurement Management

The V&V MMT provides support to management of V&V activities described in IEEE 1012. This support is expressed in terms of the facilitation of the following tasks: (1) monitor the execution of the SVVP, (2) analyze problems discovered during the execution of the SVVP, (3) report progress of the process, (4) ensure products satisfy requirements, (5) assess evaluation results, (6) determine whether a task is complete and check the results for completeness.

Figure 2 shows how the V&V MMT interacts with processes, activities and tasks established in IEEE 1012. The management of V&V activities monitoring and evaluate all the V&V outputs. Through the V&V MMT we can identify trend data and potential risks in the management of V&V.

In the following paragraphs we present some characteristics of the V&V MMT that are directly related to implementation of an efficient V&V management in safety-critical software.

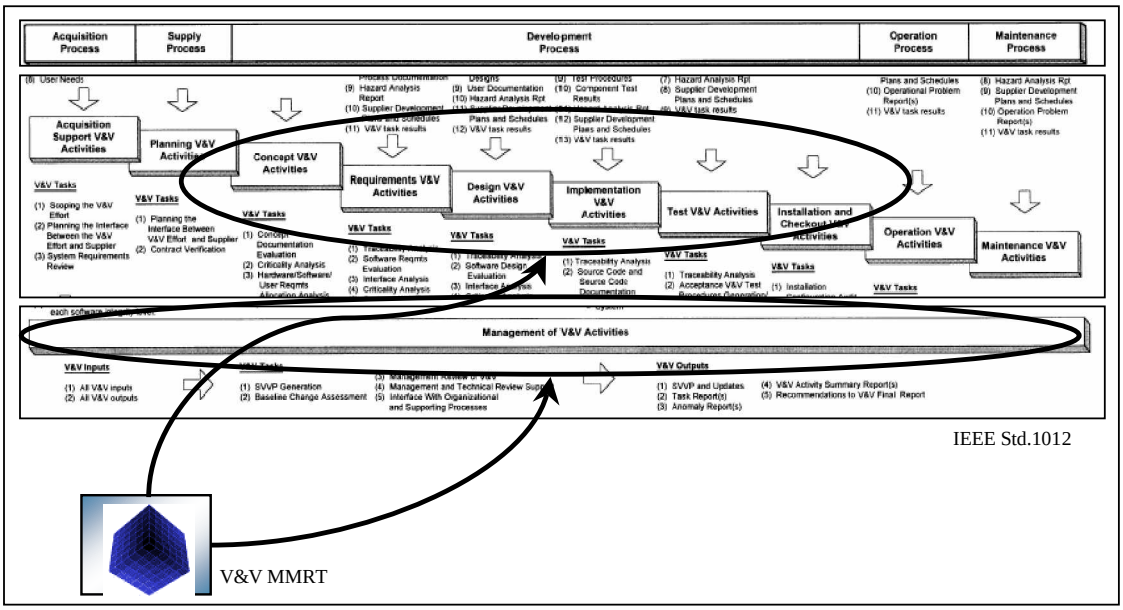

Figure 2: Support of V&V MMT to IEEE 1012

4.1 V&V Measurement quality and effectiveness

The V&V MMT provides a quantitative understanding of the effectiveness of V&V in terms of the quality, reliability and maintenance of software projects. The V&V MMT facilitates evaluation of quality performance of the processes,

activities and tasks, through the establishment of the relevant measures. The V&V MMT facilitates the monitoring of the identified milestones established in the SVVP according to IEEE 1012 (5.5.1 task 1).

Examples of measures in process performance that the V&V MMT could implement are as follows: effectiveness of process activities, percentage of defects removed by product verification activities, percentage of rework time, mean time between failures, number and severity of defects in the released product, etc.

4.2 Measurement V&V baseline

The V&V MMT allows the collection and storage of measurement data directly related to the information needs of V&V tasks (IEEE 1012, 5.5.1 task 2). The V&V MMT set these measurement data in a flexible and tailorable hierarchy. This hierarchy is composed of an association's levels to facilitate the evaluation of software changes for V&V tasks (e.g., anomaly corrections and requirements changes). It is important to note that the V&V MMT has been built according to a set of related measures that are generally applicable in several circumstances, regardless of the specific information needs of any particular situation.

The V&V MMT collects measurement data from several V&V tasks and allows analyzing them to establish a process performance baseline for quality and process performance in the project. The V&V MMT offers the possibility of establishing estimations based on historical measurement V&V data, as well as providing an understanding of the nature and extent of variation experienced in process performance.

4.3 V&V Measurement improvement

The V&V MMT can facilitate summarization of the V&V effort to define changes to V&V tasks or redirect V&V effort (IEEE 1012, 5.5.1 task 3). The V&V MMT can contribute to establish measures to determine the value of each process improvement with respect to the organization's quality and process-performance objectives. Examples of pertinent measurement include: the ratio of the number of software modules verified and validated to the total number of modules, the ratio of the number of defects identified by V&V to the number of defect missed, etc. The V&V MMT facilitates the measurement of actual V&V cost vs. planned V&V cost, V&V effort on tasks, and schedule for deploying V&V on each processes and products. Additionally, it is possibly establish a measure of the progress toward achieving the organization's quality and process-

performance objectives, as well as the number and severity of customer complaints concerning the provided service.

4.4 Measurement V&V indicators

The V&V MMT incorporates the possibility to establish indicators based on hierarchical measurement data stored in the meta-model database system. The tool is designed to accept a customized definition of the parameters, e.g., the definition of a trigger alerts when a maximum value is reached.

The repository tool can quantitatively determine the status of the processes; it can monitor and detect changes in the performance and then decision-makers can implement corrective actions as necessary. The V&V MMT offers the possibility of verifying the timely delivery according to the approved schedule of all software products (IEEE 1012, 5.5.1 task 4). The V&V MMT offers the option of establishing both process measurements (e.g., efforts, cycle time, and defect removal effectiveness) and product measurements (e.g., reliability, defect density).

4.5 Interface with Organizational and Supporting Process

The V&V MMT offers the possibility of exporting the V&V data in different file formats to facilitate the exchange with other processes implemented in the organization (IEEE 1012, 5.5.1 task 5).

5 Conclusion

In this paper we have presented our solution for implementing a measurement management repository for the monitoring and evaluation of V&V processes and products in safety critical software. We have illustrated the characteristics of an integrated, generic and flexible V&V measurement meta-model based on an OLAP approach. As well, we have presented how the V&V MMT can support and facilitate the implementation of IEEE 1012 in organizations dedicated to the production of safety critical software.

Such a V&V MMT can help organizations dedicated to the production of the critical software (e.g., NASA) to improve monitoring and to control trend indicators in safety and reliability of their products as well as quality and coverage of V&V tasks. Thus, the use of our proposed V&V MMT could contribute to minimizing risks and optimizing investments in safety-critical software.

REFERENCES

[1] N. G. Leveson and C. S. Turner, "An investigation of the Therac-25 accidents," *Computer*, vol. 26, pp. 18-41, 1993.

[2] P. J. L. LIONS, "Ariane 5: Flight 501 Failure - Report by the Inquiry Board," vol. Access date 04-09-2004, URL: http://sunnyday.mit.edu/accidents/Ariane5accidentreport.html, 1996.

[3] E. Kit, *Software Testing in the Real World*: Addison-Wesley, 1995.

[4] D. R. Wallace and R. U. Fujii, "Software Verification and Validation: An Overview," *IEEE Software*, vol. 6, pp. 10, 1989.

[5] A. Abran and E. Palza, "Design of a Generic Performance Measurement Repository in Industry," *The 13th IWSM2003, International Workshop on Software Measurement is coming to Montreal, Canada, On September 23-25, 2003*, 2003.

[6] E. Palza, C. Fuhrman, and A. Abran, "Establishing a Generic and Multidimensional Measurement Repository in CMMI context," *28th Annual IEEE/NASA Software Engineering Workshop, Greenbelt, MD, USA*, 2003.

[7] IEEE Std 1012-1998, "IEEE Standard for Software Verification and Validation," 1998.

[8] NASA Software IV&V Facility, "Software Independent Verification and Validation: Program manager handbook," vol. 2003: Goddard Space Flight Center, 2000.

[9] IEEE Std 1059-1993, "IEEE Guide for Software Verification and Validation Plans," 1993.

[10] IEEE, "IEEE/EIA 12207.0-1996 Industry Implementation of International Standard ISO/IEC 12207: 1995 (ISO/IEC 12207) Standard for Information Technology Software Life Cycle Processes," in *IEEE/EIA 12207.0-1996*, 1998, pp. i-75.

[11] J. McGarry, "PSM - Practical Software Measurement: Objective Information for Decision Makers," Addison Wesley, 2001.

[12] International ISO/IEC Standard 15939, "Information Technology - Software Engineering - Software Measurement Process," 2001.