V & V : TOWARDS A SYSTEM ENGINEERING FRAMEWORK

A.E.K Sahraoui LAAS du CNRS Toulouse, France E-mail sahraoui@laas.fr
D. Jones Raytheon systems company Dallas TX 75243 djones@raytheon.com

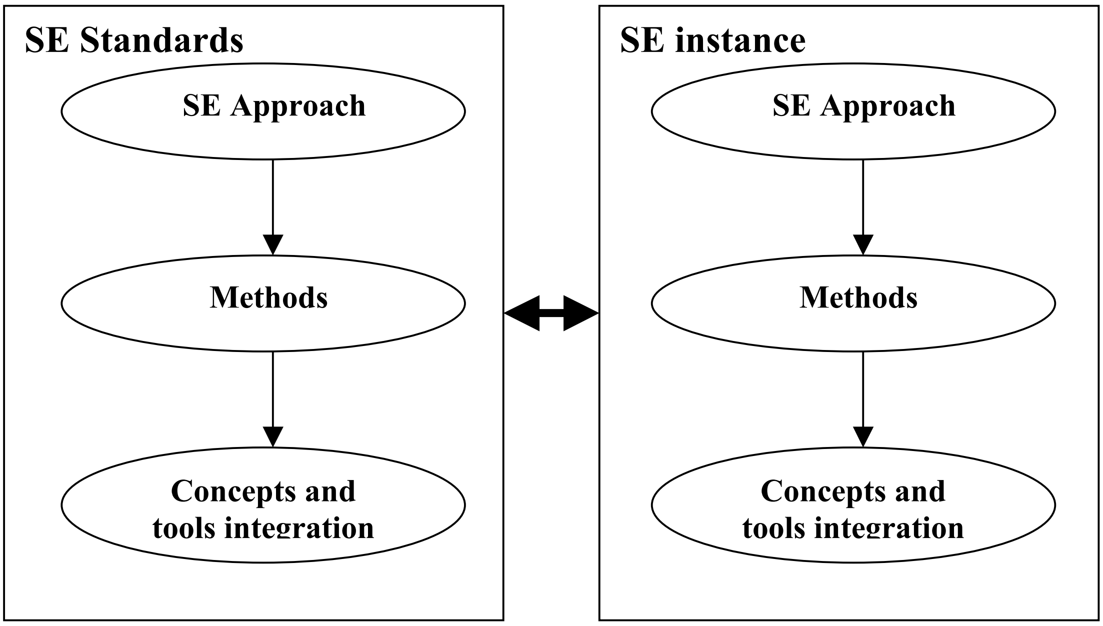
Abstract

In this paper we describe a research project for a study of verification and validation processes within a system engineering framework : inconsistency checking, traceability issues and all requirements related in SE standards as EIA-632. Three key challenges for making such work successful are (1) consider system engineering concepts as a guide, (2) use integrate V&V in a an advanced requirement management/acquisition model, and (3) integrate an approach for formalizing requirements.

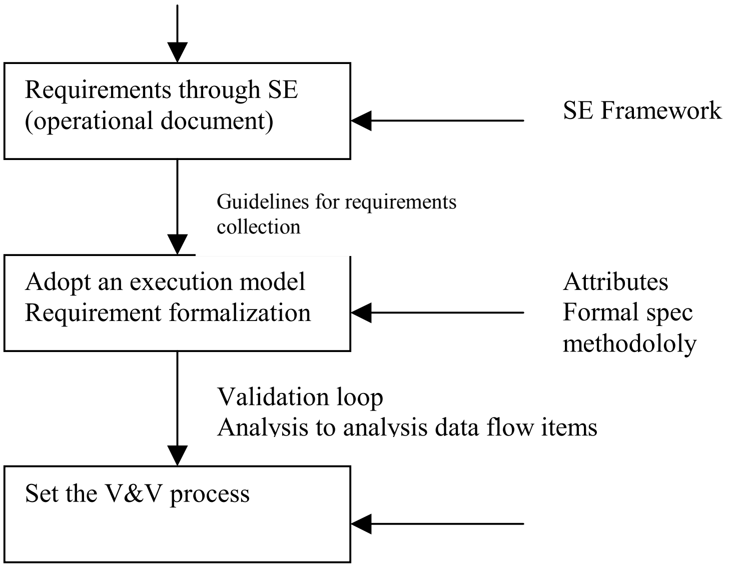
Introduction and problematics

The purpose of the requirement process is to develop requirements to satisfy needs, analyze the system, to derive a more detailed and precise set of requirements and to manage those requirements throughout the development cycle.

The SE framework may vary either with respect to the system developed or/also depending of company policy; for such principle we propose that any SE framework must be defined; we resume our approach for such item as illustrated by the following figure


SE Standards
SE Approach
Methods
Concepts and tools integration
SE instance
SE Approach
Methods
Concepts and tools integration

The left part corresponds to a general framework based on standards, recommendations which we consider as generic. The right part corresponds to an instance based on company policies or product type (avionics, transportation, manufacturing, etc …)
The approach is illustrated by the following figure



The general approach is based on three aspects

- Define the SE Framework and guidelines for requirements in order to stick to the reality.
- Use an information model (defined by Jones and INCOSE WG on req. Eng.) as an experimental architecture. This can be extended to other existing models proposed in the literature or used in some industries as the European space agency etc ..
- Propose an integrated approach to the V & V process

On Verification and Validation

We present here the main items related to the V & V process, its complexity and main related techniques. There is a large influence from the software engineering technology. Our aim is therefore clear, we must work on procedures to reduce the V &V efforts or to reduce its complexity. This is achieved in this work by developing a framework.
In V & V , we have many views and aspects. We give the sequel the various views, each view is as important as the other. These views do correspond to the steps/phases encountered in DoD 2167A and the ED-79/ARP 4754 of the european organisation for civil aviation equipment (EUROCAE) IEEE-P1220 . We are interested by consistency relationships; the following types of consistency relationships

Requirements <-> Requirements : The challenge for consistency verification is to use standard approaches that have been experimented with the integration of automated V & V. In our work , we are more concerned with such specific phase;. Other following phases are more mature in their respective domain. General objectives and requirements at this stage in system development are the most keen to errors and inconsistencies. Our approach is to translate informal requirements into semi-formal or formal requirements. Candidate methods are statecharts/activitycharts for the semi-formal specification and VDM for formal specification. Tool support is available for both software specification in particular and for system specification in general; we make use of extensions and interfaces of support tools through exchange format as STEP.

Requirements <-> Design : Requirements define the functional behavior of a system while design models define the internal structure of a system. Consistency between design models and requirements is concerned with whether the design model exhibits the required behavior and satisfies all the constraints.

Design <-> Implementation : During the development, the system must not only implement behavior as implemented by the design model, but models themselves may need to change based on discovered limitations of an implementation environment.

Inconsistency management : The framework is method independent. Approaches used in the software industry and developed at NASA (IV&V lab) are based on the viewpoints paradigm. Global consistency is achieved though a series of pair-wise consistency checks between viewpoints.

State of the art in SE standards : We look here at the V&V issue through SE standard views. The definition concerning validation and verification varies from standards to another; we will not consider the terminology aspect in this paper.

Requirements validation in IEEE : Validation consists of two types of activities: (1) evaluation of the requirements baseline to ensure that it represents identified customer expectations and project, enterprise, and external constraints and (2) assessment of the requirements baseline to determine whether the full spectrum of possible system operations and system life-cycle support concepts has been adequately addressed.

EIA 632 : There are eight requirements for V&V in this standard, we used such standard in our study

- Val1 : Requirements statements validation
- Val2 : Acquirer requirements validation
- Val3 : Other stackholder requirement validation
- Val4 : System technical requirements validation
- Val5 : Logical solution representations validation
- Ver1 : Design solution verification
- Ver2 : End product verification
- Ver3 : Enabling product readiness

Requirement execution model

We integrate such V&V issues in the execution model proposed by the INCOSE requirement engineering working group. The model is defined as follows

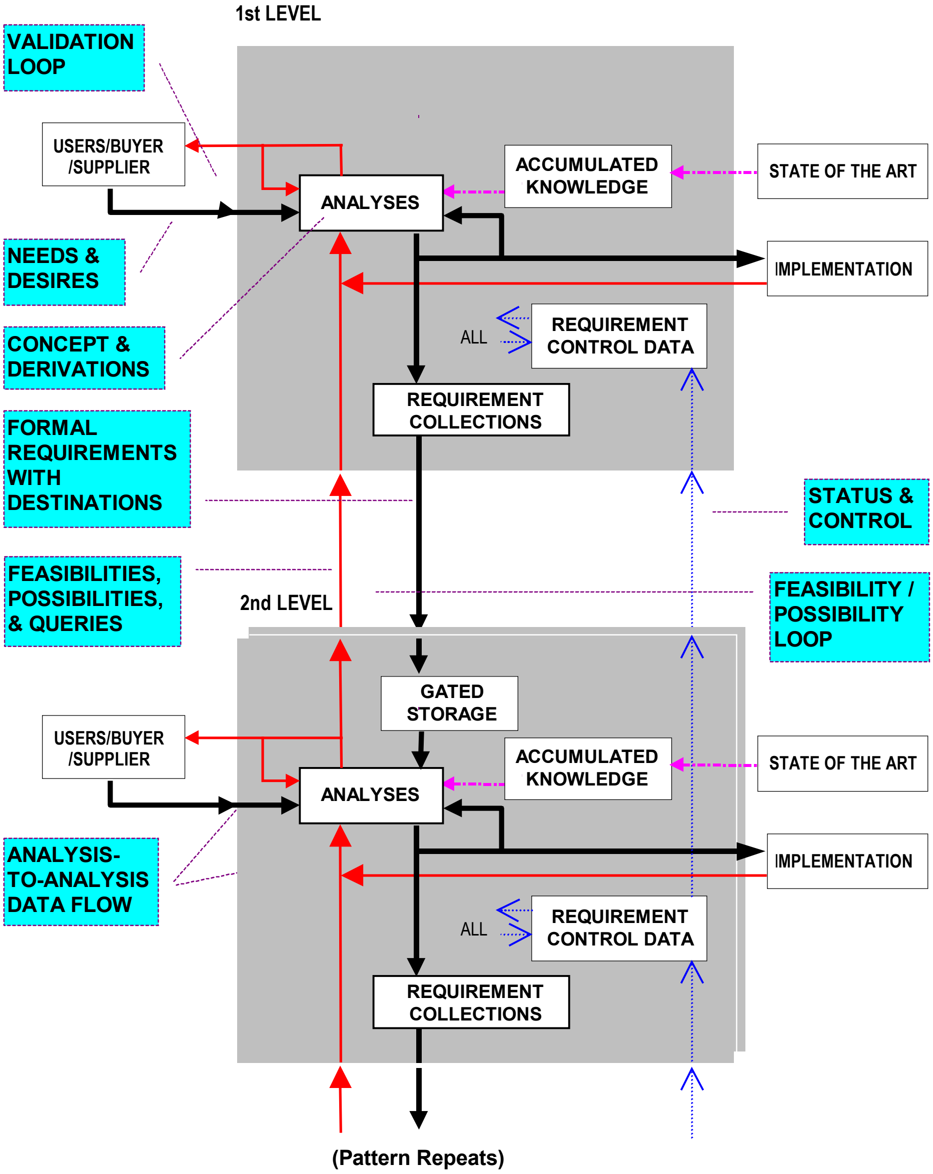
- A resulting hierarchy of requirements composed of collections of requirements that correspond to the various parts of the system or product being engineered and the people who work on them. The archetypal example of a requirement collection is a specification.
- Wherever a derived requirement exists some analysis was involved. Such analysis makes use of accumulated knowledge, both that stored in databases and that stored in the minds of men and women.
- Any particular requirement in a requirement collection in the hierarchy comes either from another collection, from an analysis, or an external source variously called the “customer”, “users / buyer / suppliers”, or “stakeholders”.
- As requirements are generated or revised the flow of requirements to collections must be done in an orderly, gated manner. Generally the responsible people must

agree to accept the requirements involved. This is an important feature in man based V & V.

- Some requirements in collections do not pass to other collections or analyses but instead are implemented. That is, for example, a part is built or tested, or assembled from lower level components.
- In addition to requirements themselves, the systems engineering process deals with a hierarchy of feasibilities, possibilities, and queries that are associated with the requirements. If the requirements are considered to flow "downward" then these items flow "upward".
- Finally, the requirement management process and tool must maintain control data for the requirement hierarchy and facilitate operator control of the process.

Model Blocks

Resulting from the foregoing is the following figure:



This figure is similar to Figure 1 of (Jones et al 1997) with some interface additions. The analysis blocks of this figure may contain a number of separate analyses blocks as was shown in Figure 2 of the cited reference. The feedback loops shown on the Analyses blocks indicate requirement flow from one analysis to another. Similarly, the requirements collections blocks may contain more than one collections. Generally there will be at least as many requirements collections as there are layers at the next level.

As was pointed out in that reference, a single analysis, for example a mechanical structural analysis or an electrical circuit model, can be present at more than one level. Thus this concept can handle the situation where a system simulation or model covers many levels of subassemblies of a system. Similarly, the same Users / Buyer / Supplier at more than one level on this diagram.

Although simple, this model is complete in the sense that all interface information flows are included. This completeness is the reason for the State Of The Art and Accumulated Knowledge blocks.

The multi-layer structure of the second level is retained. There are multiple Analyses and Requirement Collections at the second level.

The Implementation blocks still exist, but there is no feedback of queries from them. (These blocks, like the Output block, are essentially "bit buckets" in the simulation.)

We emphasize that this is a data flow model under specific assumptions and is not one of process steps. Considering that the system design process is NP-complete (**Moody et al 1997**), a complete solution probably is not possible.

The approach

The project being conducted has as a main objective to integrate formal and semi-formal methods for describing requirements as to make V&V processes less complex.

The attribute annotations for requirements

We define a syntax approach to requirement specification using a stimulus response notation (or Input/Output). The syntax is [input, condition, Output]; this notation is consistent with methodology in standard industry practice. While documents as DO178B, DOD-Std2167A, ANSI/IEEE 829-1983, and Mil-Std 498 provide some general guidelines for requirements V&V, they do not provide specific required details.

We extend such notation with items proposed in the execution model; these added items focus on other aspects of a requirement (priority, reliability/criticality); we are concerned with these two items for the corresponding reasons : the priority is an important issue for requirement management when considering options corresponding cost, the criticality is set in order to use appropriate formal methods for V&V.

Traceability issues

Tracking items from requirement to implementation in forward and backward direction is a main issue in V&V cycle (requirement <-> design <-> implementation). Safety requirements traceability approach has been proposed in [Pearson, 1998] for complex avionics systems. Few tools did overcome this aspect. However a formal notation for requirement enables to propose a preliminary approach to such issue. The execution model proposed in (3) will be used for requirement traceability partially.

Formalizing requirements for V&V

V&V automation is a "dream" among the test community. Most V&V are actually man based. We cannot automate all the process but, there are possibility through the use of specific methods in requirements. Two alternatives are proposed for formalizing requirements. The semi-formal approach is carried out with RDD100 and Statemate based on the precedent notation. However, for critical systems, the use of formal method is the adequate alternative that is proposed; ,we use for trial the VDM method (Vienna Design Method).

The statecharts based semi-formal approach

Statecharts is an approach for specifying embedded systems, a powerful method that has been used in many applications (avionics, transportation, automotive, etc ..)

The VDM based formal approach

The Vienna Design Method if a formal model oriented approach. The two approaches will be illustrated on a railway Interlocking system. The V&V process carried out using these types of methods.

The combined statecharts-VDM approach

The Stm-VDM approach has been developed at LAAS-CNRS in order to integrate semi-formal and formal method.

Conclusion

Issues on V&V has been discussed; V&V remain the main aspect in SE approach to engineer a system; standards, requirement execution model and corresponding methods are possible to be integrated for such purpose.

References

Beshore, David G., W. F. Vietinghoff, and J. C. Kiser, “Improving Requirements Processes Through Modeling and Data to Achieve Level 5 Capability Maturity” *Proceedings of the 8th Annual International Symposium of the INCOSE - Volume I*, 1998.

Carson, Ron,”Requirements completeness : a deterministic approach” *Proceedings of the 8th Annual International Symposium of the INCOSE - Volume I*, 1998

Jones, David A., Pradip C. Kar, James R. van Gaasbeek, Frank Hollenbach, Marty Bell, and Dr. “Executable requirements management model-Interim Report, ” *Proceedings of the 8th Annual International Symposium of the INCOSE - Volume II,* 1998

Donat, R.M, Joyce J.J “Applying test description tool to test system level requirements” *Proceedings of the 8th Annual International Symposium of the INCOSE - Volume I*, 1998

Moody, Jay Alan, William L. Chapman, F. David Van Voorhees, and A. Terry Bahill, *Metrics and Case Studies for Evaluating Engineering Designs*, 1997. (Prentice Hall PTR)

Ramesh, Fala, Timoth Powers, Curtis Tubbs, and Michael Edwards, “A Study of Current Practices of Requirements Traceability in Systems Development”, September, 1993. (Technical Report NPS-AS-93-018, Naval Postgraduate School, Monterey, CA)

Rechtin, Eberhardt, *Systems Architecting,* 1991. (Prentice-Hall)

Sahraoui, A.E.K et al “ An experience with a multi-formalism specification of an avionics system” *Proceedings of the 8th Annual International Symposium of the INCOSE - Volume I*, 1998

Sahraoui, A.E.K “from state transition to DFD extended methods for requirements expression” Ed. MC.Zhou, Kluwer Academic Publishers, N°ISBN N.0-7923-9557-3, 1995, pp.305-336