ESA ISVV Handbook :: Evolution of the ISVV Guide

Authors: Nuno Silva, José Miguel Borges and Xavier Ferreira (Critical Software), Jesper Troelsen (Rovsing)

TEC-ED & TEC-SW Final Presentation Days

Presentation Date: 01/12/2022

CRITICALSOFTWARE.COM

Information Classification: Public

1

Outline

- Introduction

- ISVV Handbook Generation Process

- ISVV Handbook Contents Definition

- ISVV Handbook Workshops

- ISVV Handbook Public Reviews

- Conclusions and Future Work

- Acknowledgements

Information Classification: Public
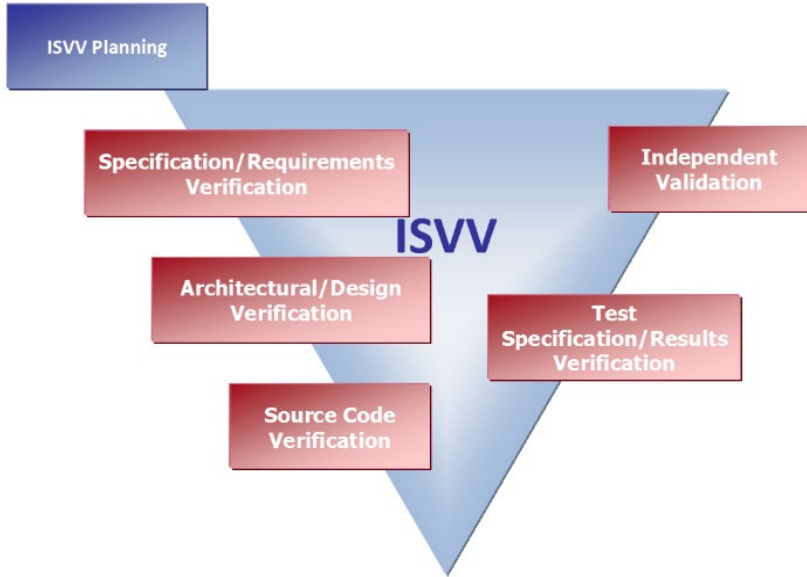
Introduction

Introduction

- GSTP Project name: "**ISVV for Evolutions in Software Developments and Processes"**, ESA Contract: 4000127073/19/NL/AF

- The ISVV Guide, was released in December 2008 and since then, it was the main driver for ISVV activities in European space industry.

- In the past 14 years, the software development evolved dramatically and so did the space software industry.

- The project was guided based on an initial set of requirements reflecting the experience gathered in over a decade of application of the ISVV Guide along with observations upon the evolution of software engineering in general.

Introduction

- Feedback was collected from a large set of stakeholders representing the industry, agencies and other users, and the change proposals were later discussed and agreed with the same stakeholders.

- After redaction, the ISVV Guide became the ISVV Handbook, prepared for ECSS adoption as an official Handbook.

- It was later reviewed by many representatives from industry and ESA.

- Now, the new ISVV Handbook is ready to be published and used, and it will hopefully bring a more streamlined and flexible way of applying ISVV on software in European space projects.

- This presentation will guide the attendees through the whole ISVV Handbook updates process, by highlighting the main novelties and providing a status of the recent public reviews' implementations.

Main Phases

- Stakeholders Questionnaire outcome:
  - TN1: IVV Collection Improvements Technical Note
- Handbook Contents Drafted:
  - TN2: IVV Assessment Improvement Technical Notes (16)
- Handbook related Workshops:
  - ADCSS2020 (October 2020) + ESA/ESTEC Workshop (November 2020)
- Handbook Drafting and Public Review

ISVV Handbook Generation Process

- Collect feedback from stakeholders/participants
- Analyse and extract the most relevant information from the answers to the checklists.
- Prepare individual technical notes per topic.
- Prepare, present and discuss this information with stakeholders in a dedicated workshop.
- Produce the handbook and support ESA on its promotion.

ISVV Handbook Generation Process

- Initial stakeholders selection:
  - All the companies involved as ISVV customer or supplier (particularly in Europe)
  - Agencies (NASA, JAXA, INPE, DLR, CNES …)
  - Other institutions working in space/astronomy
  - Additional participants that showed up after the word spread out

ISVV Handbook Generation Process

- ## Active Participants in Questionnaire

    - ESA / Critical Software / Rovsing
    - Airbus DS
    - OHB
    - Thales Alenia Space
    - TERMA
    - HULD
    - CAPTEC
    - GMV
    - Everis
    - Leonardo
    - NASA
    - JAXA
    - DLR
    - INPE

→ 86 Specific Proposed Changes stated as questions inside the former ISVV Guide.

→ Almost 1500 questions answered!

Information Classification: Public

ISVV Handbook Generation Process

- **MAN.PM.T1.S5: Estimate ISVV scope and budget (ISVV Supplier)**

  The ISVV Supplier should do an independent estimation of the ISVV budget. See section 4.1.

- **MAN.PM.T1.S6: Develop ISVV plan (ISVV Supplier)**

  The ISVV Supplier must define an ISVV plan (a draft could be part of the proposal). The plan should be approved by the ISVV Customer. The developer's software development plan, software product assurance plan, and software verification and validation plan should be taken into account if available (overall coordination planning data is to be provided by the ISVV Customer). An outline of a sample ISVV plan is found in Annex B.1.

- **MAN.PM.T1.S7: Approve ISVV Plan (ISVV Customer)**

  The ISVV Customer should approve the ISVV plan developed by the ISVV Supplier. An outline of a sample ISVV plan is found in Annex B.1.

- **MAN.PM.T1.S8: Determine confidentiality issues and prepare NDAs (ISVV Customer)**

  It is the responsibility of the ISVV Customer to clarify confidentiality requirements and ensure these are kept throughout the project through the signing of Non-Disclosure Agreement with the ISVV Supplier and any of its sub-contractors (see Section 2.4).

- **MAN.PM.T1.S9: Approve scope definition resulting from ISVV level definition (ISVV Customer)**

  All ISVV level definition results must be approved by the ISVV Customer. See also section 3.2.1.

Outputs:
- ISVV plan (ISVV Supplier)

3.5.2 ISVV Process Execution, Monitoring and Control.

TASK DESCRIPTION		
Title: ISVV Process monitoring and control	**Task ID:**	MAN.PM.T2

Sticky Note — rbarbosa — 06/09/2019 12:00:46 — Options ▾

Q-15: Do you see any of the listed subtasks as non-essential for the proper management an ISVV project?
(Note: You can propose tasks or subtask candidates which were not efficient in ISVV projects you participated or which could be removed). Specify.
R:

Sticky Note — rbarbosa — 06/09/2019 12:00:55 — Options ▾

Q-16: Would any additional tasks or subtasks be here specified to complement or improve the ISVV management? Exemplify.
R:

Information Classification: Public

ISVV Handbook Contents Definition

- Group 1: Incorporate experience from using the ISVV
- Group 2: Alignment to latest development standards
- Group 3: Modern software development practices and methods

The groups, areas of improvement/topics, were requirements from the SoW meant for guidance. They drove the categories of changes/updates

- Solve contradictions
- Propose Handbook Specific Contents
- Draft it and get it publicly reviewed

ISVV Handbook Contents Definition

- Group 1: Incorporate experience from using the ISVV

Topic ID	Topic Title
R-1.1	Verification of software requirement baseline and concept documentation
R-1.2	Improvement of the Independent Validation Activity (IVA)
R-1.3	ISVV Level re-assessment
R-1.4	ISVV metrics definition and collection framework
R-1.5	ISVV statement of work template
R-1.6	Verification of the unit test specification
R-1.7	Clarification of ISVV activity outputs
R-1.8	Revisit current ISVV tasks regarding their effectiveness
R-1.9	Lessons learned collection framework
R-1.10	Independent verification and validation of software dependability and safety activities
R-1.11	Continuous ISVV process
R-1.12	Reassess the ISVV industrial context (optional)
R-1.13	Complementarity of ISVV activities (optional)
R-1.14	Miscellaneous inputs on ISVV processes
R-1.15	Level 2 description improvements (optional)

ISVV Handbook Contents Definition

- Group 2: Alignment to latest development standards

Topic ID	Topic Title
R-2.1	ECSS-E40C and ECSS-Q80C impact on ISVV processes
R-2.2	Align the document structure with the ECSS Handbook documentation format
R-2.3	Traceability between ESA ISVV Handbook and International Standards (optional)
R-2.4	Independent verification and validation from other space domains (optional)
R-2.5	Independent verification and validation from non-space domains (optional)

ISVV Handbook Contents Definition

- Group 3: Modern software development practices and methods

Topic ID	Topic Title
R-3.1	Independent verification and validation of reused software
R-3.2	Independent verification and validation of data
R-3.3	Independent verification and validation of complex electronics (ASIC/FPGA-based designs) (optional)
R-3.4	Independent verification and validation of auto generated code
R-3.5	Independent verification and validation when using Model Based Techniques
R-3.6	Independent verification and validation of SW developed following an iterative model
R-3.7	Independent verification and validation of agile developed systems
R-3.8	Modern and alternative methods & techniques to perform independent verification and validation

ISVV Handbook Contents Definition

- Examples of Open Points
  - Complementary ISVV activities for System, Engineering, Operations and Maintenance phases;
  - ISVV level definition activity and alternatives;
  - Key properties of software which affect the ISVV scope;
  - Test cases from the nominal development validation activities should be provided to the ISVV team?

- Decisions Workshop and Handbook Drafting

ISVV Handbook Contents Definition

- All TNs included:
  - ISVV Handbook Topic Assessment → From SoW + Questionnaire → **16 Technical Notes**
  - Summary of Improvements → **120 Changes in total**
  - Impact on ISVV Processes & Methods
  - Open Points → **20 Open Points in total**
  - Proposed Updates

  - Delivered for 16 dedicated workshops

ISVV Handbook Contents Definition

- Examples of significant changes
  - ISVV level re-assessment / tailoring (1 slide)
  - ISVV Metrics / Lessons Learned (1 slide)
  - ISVV of Requirements Baseline (1 slide)

ISVV level re-assessment / tailoring

I.4 Influencing factors

This section lists the main factors, which might influence the tailoring process and scope definition.

Software factors:

a. Software criticality and mission criticality.

   1. The ISVV supplier may also perform the criticality analysis by using a simplified FMECA method – see annex F.2.27.2.

b. Software characteristics:

   1. Complexity (language, models, algorithms).

   2. Size (lines of codes, number of requirements).

   3. Reusability (is the software component reused from previous project, will it be reused for future projects).

   4. Possibility to update in flight.

   5. Performance requirements.

   6. Type of code to be analysed: E.g., the programming language in which the code is developed, if code is auto generated; particularly, the inspection of auto generated code using custom code generators is an important factor.

c. The software development life cycle.

Experience and lessons learned:

a. Lessons learned from previous ISVV projects.

b. Experience and knowledge gained from this ISVV project (relevant for update of tailoring throughout the ISVV project).

Feasibility factors:

a. Experience and capabilities of the ISVV supplier

b. Access to tools and experience using tools

c. ISVV budget

d. Project risk register

e. External dependencies (e.g. access to SVF)

I.6 Prioritisation score

…

The following score can be applied to these elements:

a. Software Criticality (Crit), Score: A->10, B->7, C->4, D->0

b. Software Complexity (Comp), Score: 1-3

c. Software Reusability (Reus), Score: 1-3

The Prioritisation Score for the software component is calculated by:

$$\text{Prioritisation Score} = (\text{Crit}) + (\text{Comp}) + (\text{Reus})$$

Some general rules based on the Prioritisation Score:

Prioritisation Score of >= 10: This software component has **"High"** priority for ISVV. All the tasks should be performed, and a broad variety of methods and tools should be used for verification and validation.

Prioritisation Score of 7-9: This software component has **"Medium"** priority for ISVV. Prioritisation between the tasks can be applied, but a broad variety of methods and tools should be used for verification and validation.

Prioritisation Score of <= 6: This software component has **"Low"** priority for ISVV. Certain task might be skipped for this component or only a few methods and tools could be selected for the verification and validation. The complete ISVV could also be skipped for this component in favour of software components with a higher prioritisation score.

Information Classification: Public

ISVV Metrics / Lessons Learned

Table A-2: Catalogue of simple metrics

1. Metric

1.1. # RIDs per criticality (major, minor, comment).

1.2. # RIDs per type (external consistency, internal consistency, correctness, technical feasibility, readability & maintainability, completeness).

1.3. # RIDs per status (reported, accepted, rejected, corrected).

1.4. # RIDs per status per criticality.

1.5. # RIDs per criticality per ISVV subtask and task.

1.6. # RIDs per status per ISVV subtask and task.

1.7. # RIDs per type per status.

1.8. # RIDs per type per ISVV activity.

1.9. # RIDs that result in document modifications.

1.10. # RIDs that result in source code modifications.

1.11. # RIDs that result in behavioural changes in source code.

1.12. # physical lines of code, excluding comments (LOC).

1.13. # requirements.

1.14. # iterations of ISVV deliverables.

1.15. Range of hours spent on ISVV.

1.16. Range of hours spent on IVA activity.

1.17. IVA proposed tests metrics:

- # tests proposed.
- # tests executed.
- # tests failed resulting in accepted RIDs.
- # tests failed resulting in rejected RIDs (issue with SVF, out of scope, etc.).

Table A-5: Lessons learned questionnaire

4. Lessons learned

4.1. Questions to the ISVV supplier:

- What was the type of the software under ISVV (AOCS, CSW, etc.)?
- Did you experience any problems during the project and how were the problems dealt with? This could be problems related to:
  - Immature deliverables
  - Increase in scope
  - Estimations exceeded
  - Items in the risk register
  - CCNs
  - RIDs handling process
- Did you apply any good practices that brought visible benefits to the project?
- What methods used were found most efficient?
- Were any methods used, which turned out to be less efficient than planned?
- What lessons learned can be derived from the applied tailoring for the project?

4.2. Questions to the ISVV supplier (for IVA only):

- What was the type of Independent Validation (who runs the tests – ISVV supplier or SW supplier)?
- What was the efficiency of IVA activity? (High | Medium | Low)
- Have you encountered any problems during validation activity? And how were the problems dealt with? This could be problems related to:
  - SVF stability, installation and usability
  - SVF training
  - Execution of test cases
  - Issues found during test
  - Own SVF enhancement
  - Tests results ambiguity
  - Partly done ISVV
  - Possible CCN
- Did you apply any good practices that brought visible benefits to the project?

4.3. Questions to the end customer/ISVV customer/SW supplier:

- What is your general feedback about value created and efficiency of the ISVV project?
- What good practices, tasks, improvements have brought a significant added value to the ISVV project?
- Are there any areas that should be improved?
- Was the tailoring appropriate for the ISVV project?

Information Classification: Public

ISVV of Requirements Baseline
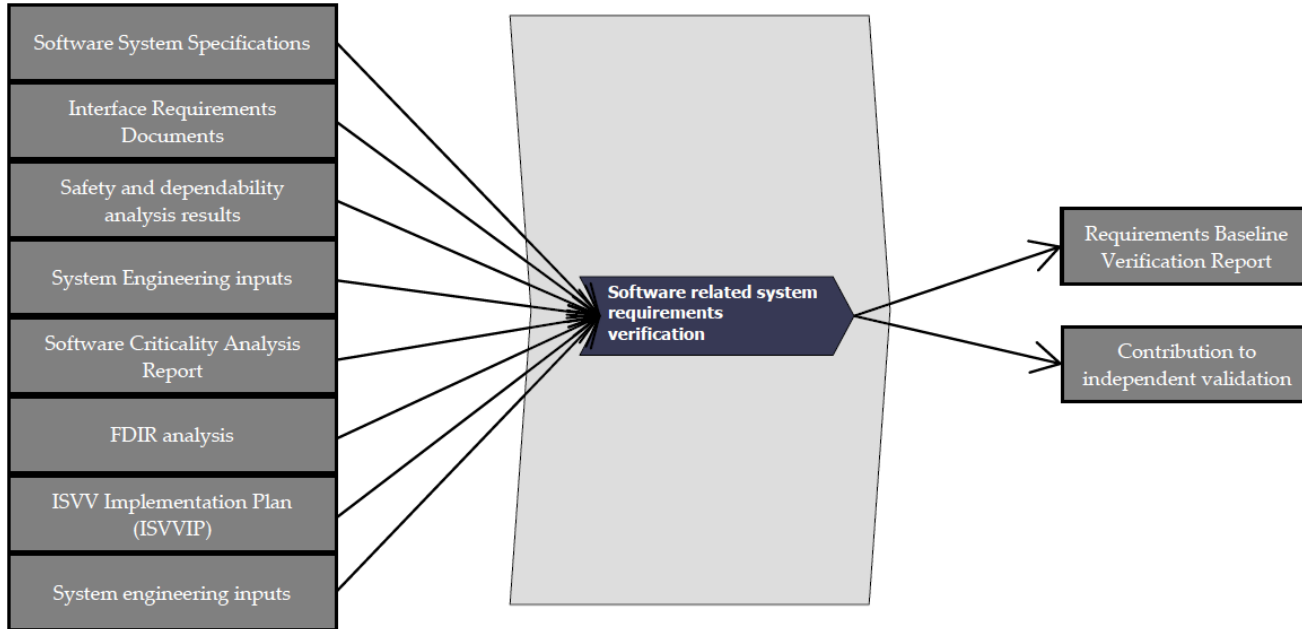
Figure 6-1: Requirements Baseline Analysis

ISVV Handbook Workshops

- 16 Dedicated Workshops have been held during November 2020

Day	Time	Morning Workshop	Time	Afternoon Workshop
17	10:00-12:00	ISVV for Agile projects	14:00-16:00	ECSS Updates / Security Requirements
18	10:00-12:00	ISVV for Iterative / Incremental projects	14:00-16:00	Continuous ISVV
19	10:00-12:00	ISVV for Reused SW	14:00-16:00	Verification of Unit Test Specifications
20	10:00-12:00	ISVV for Model Based Development	14:00-16:00	Reserved
21				
22				
23	10:00-12:00	ISVV Metrics / Lessons Learned	14:00-16:00	Safety & Dependability
24	10:00-12:00	ISVV Level reassessment	14:00-16:00	Independent Validation Analysis Improvements
25	10:00-12:00	ISVV for Autogenerated Code	14:00-16:00	Modern Methods and Techniques for ISVV
26	10:00-12:00	Requirements Baseline ISVV	14:00-16:00	ISVV of Data
27	10:00-12:00	ISVV for ASIC/FPGA	14:00-16:00	Reserved

ISVV Handbook Workshops

- Participation according to topic interest
- More than 20 participants from European Industry, Agencies and Japan
- 85 total Actions raised during the workshops

Information Classification: Public

ISVV Handbook Public Reviews

- Drafted Handbook delivered for public review at the end of July 2022.

- Besides ESA internal delivery, 14 other stakeholders got the drafted Handbook.

- Up to end of September, besides ESA, 5 companies had provided public review comments (8 reviewers).

- ESA collected internal comments from 10 internal reviewers.

ISVV Handbook Public Reviews

- Industry reviewers selection: all stakeholders who expressed interest in the workshops (largest pool of industry partners) have been invited (excluding agencies).

Information Classification: Public   24

ISVV Handbook Public Reviews

- Industry comments: 84
  - Trivial: 24 (28.6%)
  - Simple: 51 (60.7%)
  - Complex: 9 (10.7%)

- ESA comments: 205
  - Trivial: 46 (22.4%)
  - Simple: 125 (61.0%)
  - Complex: 34 (16.6%)

- Total comments: 289
  - Trivial: 70 (24.2%)
  - Simple: 176 (60.9%)
  - Complex: 43 (14.9%)

- Reviewers Severity
  - Major: 45 (15.6%)
  - Minor: 211 (73.0%)
  - Comment/Editorial: 33 (11.4%)

Information Classification: Public

ISVV Handbook Public Reviews

- Implementation status
  - Rejected: 66 (22.8%)
  - Agreed: 202 (69.9%)
  - Postponed: 21 (7.3%)

- Postponed issues are the ones that require significant changes or feedback from the handbook application

Conclusions and Future Work

- Handbook Ready after Public Review

- List of Postponed issues (some might lead to changes, some not)

- Feedback on its applicability will be requested/collected, namely for the significant changes (RB ISVV, Metrics collection, applicability to new lifecycles, ISVV tailoring…)

Conclusions and Future Work

- Gathering statistics in a more consistent way through means of metrics and lessons learned.

- In the future an ECSS Working Group will take over the ESA ISVV Handbook:

  – Analysis of the compliance to ECSS Handbook

  – Consideration of the applicability of the postponed issues

Conclusions and Future Work

- The ISVV Guide was initially converted into an ECSS handbook, but that work could not be finalized:
  - The overloaded agenda of ECSS members
  - Working group postponed for 2023
  - Contributed to the delays in the HB release (review, update, release)
  - We decided to release it outside ECSS not to delay the availability of the handbook further
  - ECSS WG work will have an impact in the next release (this is why there are postponed improvements / changes also)

Information Classification: Public

Conclusions and Future Work

- ESA will distribute/make available the new ISVV Handbook (on demand/as part of SoWs …):
  - ESA POC: Andrei-Mihai Buzgan (Andrei-Mihai.Buzgan@esa.int)
  - Technical: Nuno Silva (nsilva@criticalsoftware.com), and Jesper Troelsen (jtr@rovsing.dk)
  - Handbook will be available for download by mid-December at:
    - https://criticalsoftware.com/en/news/new-isvv-guide-for-space-in-the-works
    - ESA Alfresco platform for the participating stakeholders

Aknowledgements

- All stakeholders participating in the initial questionnaire, the ISVV Workshops and the public review

- ESA Reviewers

Information Classification: Public

31

Thank You!
Q&A

Nuno Silva, PhD

nsilva@criticalsoftware.com

Jesper Troelsen

jtr@rovsing.dk

TEC-ED & TEC-SW Final Presentation Days

Information Classification: Public