ECSS updates on software standards (PA & ENG & ISVV)

Fabian Frost

ESA ESTEC

25/09/2023

Agenda

1. **Evolution of ECSS-E-ST-40C (now Rev.1)**
   - Highlight of Main Changes
   - Change Details
2. **Evolution of ECSS-Q-ST-80C-Rev.1 (now Rev. 2)**
   - Highlight of Main Changes
   - Change Details
3. **Evolution of ESA ISVV Guide issue 2.0 (now CSW-ESAISVV-2022-GBK-02897 issue 1.0)**
   - History, Motivation and Approach
   - Project, Timeline and Results
   - Overview of the new handbook
   - New additions / Updates / Changes
   - Way forward
4. **Way forward**

PART 1

Evolution of ECSS-E-ST-40C (now Rev. 1)

Highlight of Main Changes

- Revisit of definitions, including new definition of “software”
- Introduction of security aspects
- Make the standard less waterfall
- Reinforce the verification of code
- Address impact of Hardware-Software co-engineering process and ensure consistency with ECSS-E-ST-20-40C standard
- Consider the outcomes of ISVV guidelines update
- Introduce the Software Delivery Review Board and Software validation specification review
- Introduce the Software Validation Control

Change Details

1. Followed ECSS process for revisions including that no modification of existing numbering is allowed
2. 68 Change Requests have been processed
3. Additional modifications have been implemented to correct existing issues
4. Working Group was composed of 22 persons for agencies and industries

ESA	8
Airbus Defence and Space SAS	1
ArianeGroup	2
CNES	3
DLR	2
ESA	1
INTECS	1
OHB	1
Thales Alenia Space	3

Definitions

1. Definitions agreed with ECSS-E-ST-20-40C (ASIC, FPGA and IP Core engineering standard)

3.2.20 processing unit

function which is defined to execute software.

NOTE 1 The term covers the hardware functions such as processing core included in Central Processing Unit (CPU), Graphical Processing Unit (GPU), Vision Processing Unit (VPU), Tensor Processing Unit (TPU), Neural Processing Unit (NPU), Physics Processing Unit (PPU), Digital Signal Processor (DSP), Image Signal Processor (ISP).

NOTE 2 In the context of SW engineering, it also covers the software processing units such as interpreters, emulators and virtual machines.

3.2.29 software

set of instructions and data executed on a processing unit

NOTE 1: See 3.2.20 for the definition of processing unit.

NOTE 2: Some processing units only require data, e.g. configuration of state machines or configuration data of a neural network.

NOTE 3 Files using Hardware Description Languages (e.g. VHDL, Verilog, System-C) used to model ASICs or bit stream files used to programme FPGAs are not software.

Security

1. Around 200 modifications are linked to the related change request
    a. Introduction of a new definition (threat) and abbreviations.
    b. A full section has been added to cover the Software security process (5.11).
    c. Many requirements (5.x) have been added or updated to introduce the consideration of security in the complete development process.
    d. Introduction of a new file (Security File) and related documents
        - Software security management plan (SSMP)
        - Software security analysis report (SSAR)
        - Security risk treatment plan (SRTP)

Improve life-cycle independence

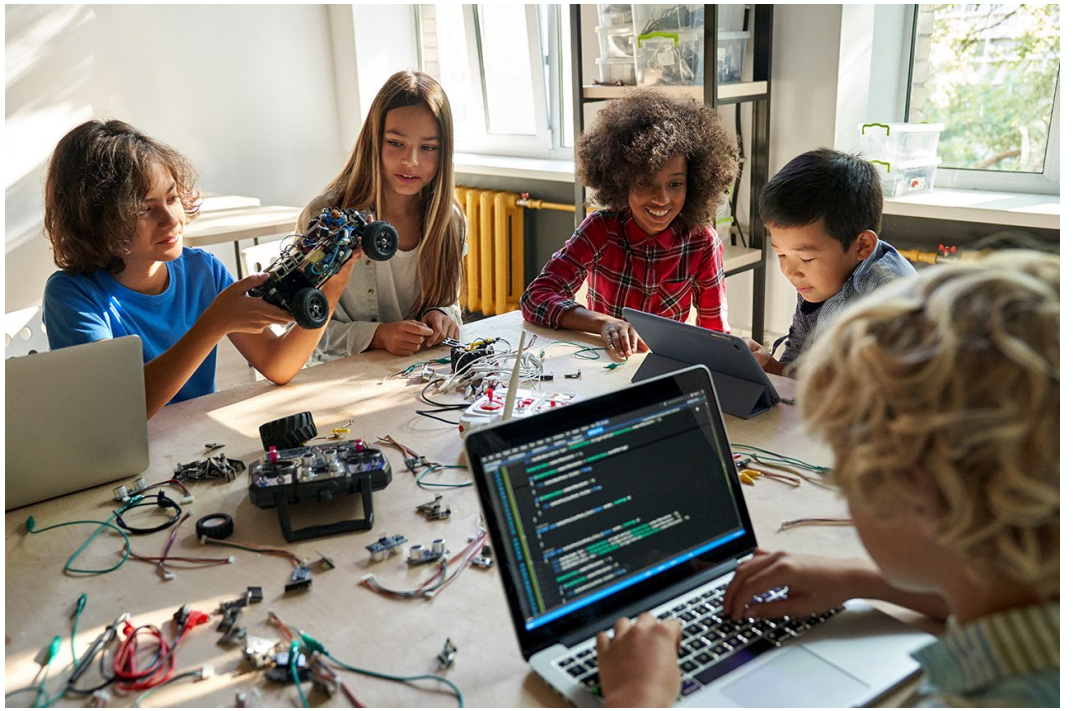
1. Current version of the standard is considered too oriented to waterfall life cycle even if it is clearly required that the Supplier must define and follow a software life cycle (5.3.2.1a).
2. Rev1 reduces the reference to waterfall life cycle and to remove any bias.
3. 16 modifications are linked to this change request.

Reinforce the verification of code

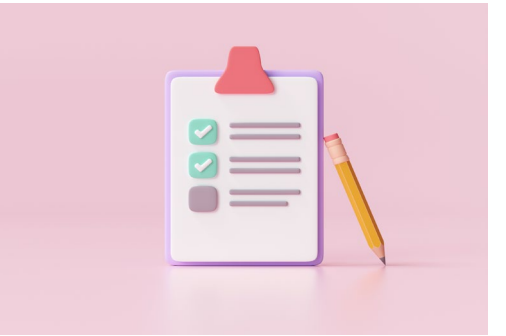
1. The requirements of section 5.8.3.5 have been consolidated.
    a. Requirement a. code verifications have been moved to a dedicated annex and extended.
        - Annex U (informative) - Software code verification identifies 14 code checks. Most of the checks are supported by static analysis tools.
    b. Requirement b. the “AM” abbreviation has been replaced by “TBA” – To Be Agreed
    c. Requirement c. has been updated to ensure that a code coverage measure is always provided, whatever the criticality category of the software.

Hardware-Software co-engineering

1. Introduce the concept of Hardware/Software co-design/co-engineering to cover the development of functions deployed partly on a general-purpose processor and hardwired logic (ASIC or FPGA).
2. The partitioning being a System activity, few updates are linked to this change request thanks to the existing process.
    a. Requirement related to Software have to be provided in the SSS and IRD
    b. SDP must identify all the exchange of information between hardware and software development teams (e.g. models and simulators).



Reviews and Software VCD



1. Introduce the Software Delivery Review Board
    a. The SW DRB is formalizing a good practice of large projects.
    b. It is a technical review and then is not mandatory
2. Introduce the Software Validation Specification Review
    a. The SVSR is an anticipation of the TRR that has been identified by lessons learnt from projects. TRR is covering two objectives that are to agree on the validation specification and to ensure that test can start. Any disagreement on the validation specification will lead to fail or postpone the TRR.
3. The Software VCD has been introduced to map the System VCD at software level without requesting a specific document but only evidences (e.g. through development platforms).

PART 2

Evolution of ECSS-Q-ST-80C-Rev.1 (now Rev. 2)

Highlight of Main Changes

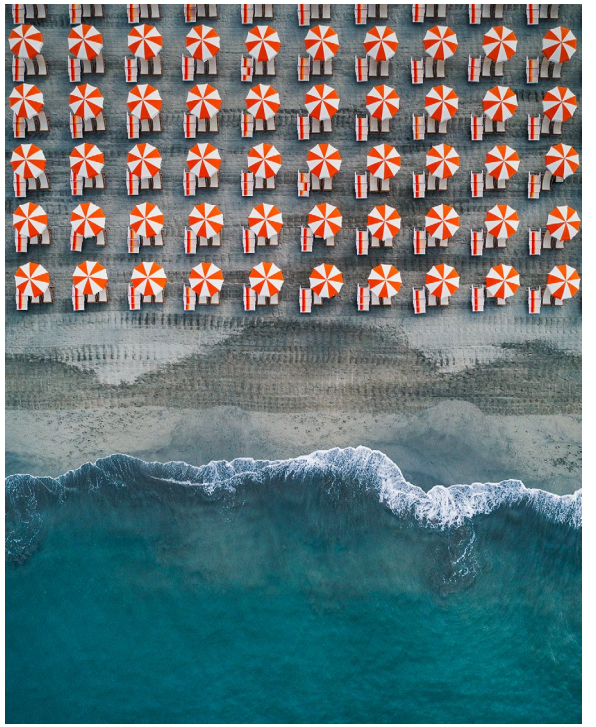
- Alignment to ECSS-E-ST-40C Rev.1
- Software Security Assurance requirements
- Lessons learnt and external change request

Change Details

1. 69 Change Requests have been processed
2. Additional modifications have been implemented to correct existing issues or Lessons Learnt
3. Several working groups were created (including industry partners)
4. Inputs came from new / updated:
    a. standards e.g. E40 / ESSB / ISO 25010
    b. ISVV Handbook
    c. Lessons learnt database

Alignment to ECSS-E-ST-40C Rev.1

- Terms and Definitions
  - Update and addition of definitions
- **Software Validation Control**
  - 6.3.5.33 added **new requirement** requesting provision of validation test result matrix (like a SW VCD)
- Delivery Review Board (DRB)
  - 6.3.6 new requirements added to introduce SW DRB and related PA aspect
- **Security**
  - throughout Q80 rev. 2 added **new requirements** -> see next slides

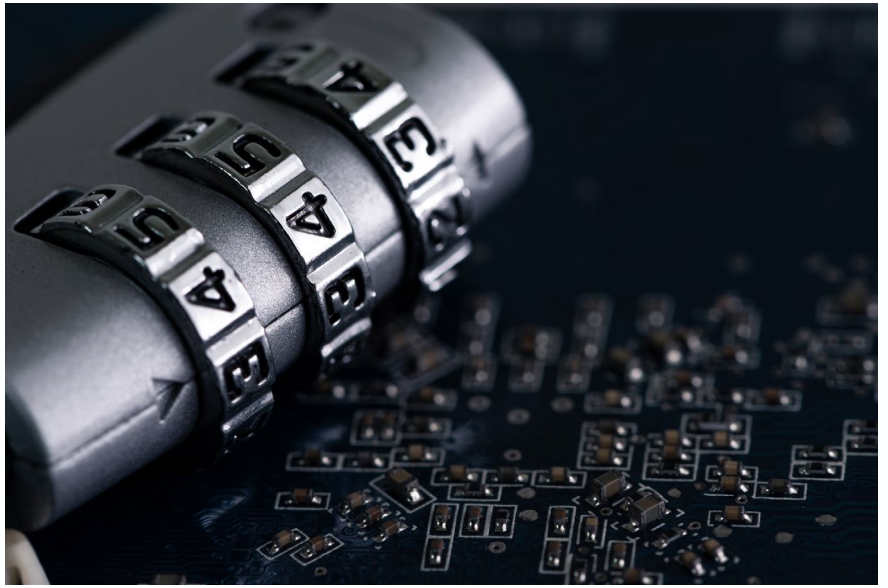


Software Security Assurance requirements

- Training
  - 5.1.5.4 b. added for security aspects
- Software Problems
  - 5.2.5.1 a. removed security as covered by E40 rev 1
- NCRs
  - 5.2.6.1 d. added to include security representative in NRB
- Sensitivity Classification
  - 5.4.5 added based on security analysis at higher level
- Procurement
  - 5.5.3 and 5.5.6 security related import/export constraints/information
- Tools and Methods
  - 5.6.1.2 added to take security into account for selection of these
- Development Environment
  - 5.6.2.1 point 13/14 added to assess security aspects

Software Security Assurance requirements

- Life cycle
  - 6.1.3 and 6.1.4 updated to included security
- Documentation process
  - 6.2.1.1 added security management
- HSIA
  - 6.2.2.8 added note to include HW security related failures
- Configuration Managment
  - 6.2.4.7 (i) added regarding disposal of sensitive documentation
  - 6.2.4.8 b. added to ensure SW protection
  - 6.2.4.9 b. added to ensure SW authenticity
  - 6.2.4.11 rewritten to also include security aspect
- ISVV
  - 6.2.6.13 updated reflecting security aspect



Software Security Assurance requirements

- Reuse of SW
  - 6.2.7.3/4/8 updated reflecting security aspect
- **SW security**
  - 6.2.9 added entire **new chapter** with **new requirements** for security
- **Handling of security sensitive software**
  - 6.2.10 added entire **new chapter** with **new requirements** for security
- SW Engineering process
  - 6.3 added throughout many sub-sections security aspects
- SW product quality assurance
  - 7.1.1/7.4.4/7.5.2 added security aspects

Lessons learnt and external change request

- Process assessment
  - 5.7.2 updated regarding process assessment
    - Added ECSS-Q-HB-80-02 reference
    - Updated to new ISO/IEC 33001 reference
    - added for Very Small Entity (VSE) alternative ISO/IEC 29110-6-1
    - Updated assessment of Assessor competence
- TRR
  - 6.1.5 changed to make it explicit and mandatory for SW
- ISVV
  - 6.2.6.13 updated reflecting changes due to new ISVV handbook (ECSS guideline replacement) as well as chapter 6.3.5.28

PART 3

Evolution of ESA ISVV Guide issue 2.0

(now CSW-ESAISVV-2022-GBK-02897 issue 1.0)

ISVV Handbook – Updates Overview

Andrei Buzgan

ESA ESTEC

25/09/2023

Contents

1. History, Motivation and Approach

- ESA ISVV Guide was release in December 2008
- It was the main driver for the ISVV activities for the past 15 years
  - Still in used by active projects which were defined before the release of the new Handbook
- It became outdated and out of synch with the latest versions of the ECSS standards
  - It references the E40B and Q80B from 2003
  - ECSS Software Development and Agile Handbooks were not available at that time
- The long-time usage of the Guide highlighted its strength and weaknesses
- The Handbook aims to rectify those weaknesses and bring the ISVV process definition inline with modern technologies, methods and practices used in software development today.

Terminology:

“The (ISVV) Guide” refers to the old ESA ISVV Guide from 2008; “The (ISVV) Handbook refers to the updated new version of the Guide, released in January 2023, draft candidate for the official ECSS ISVV Handbook.

2. Project, Timeline and Results

- The ISVV Handbook was the result of a GSTP project, with the participation of Portugal (Critical Software) and Denmark (Rovsing)
- Project started in 2019 (Kick-Off meeting was held on 21-June-2019)
- Stakeholders were surveyed and data was gathered in the beginning of 2020
- Throughout 2020, assessment technical notes were produced for every identified improvement/change area of the old Guide and they were discussed with the stakeholders in a chain of virtual workshops held over 2 weeks in November 2020
- The feedback received during the workshops was processed in the following months and the edit of the new Handbook began in early 2021
- The first draft (ECSS ready) was completed in June 2021
- An internal ESA review took place beween July and September 2021 and the result was the first ECSS ISVV Handbook draft

2. Project, Timeline and Results

- The Handbook draft could not be submitted to ECSS for a public review due to limited ECSS resources for new projects and working groups for 2022
- In order not to further delay the release of the Handbook, the document was stripped off any ECSS badges (structure and content remained untouched) and submitted to a (non-ECSS) public review in June/July 2022 where all stakeholders were invited
- The final version of the ESA ISVV Handbook was completed in December 2022 and published in 2023 via ESSR, under SAVOIR documents licence.

https://essr.esa.int/project/independent-software-verification-and-validation-handbook

(ESSR registration is needed – straightforward and simple from any member state with a corporate email address)

3. Overview of the new handbook

- The handbook updates cover 28 topics which were individually analysed and detailed in dedicated technical notes (available for download together with the Handbook)
- These 28 topics generated ~148 changes with various degrees of impact on the old Guide (from editorials, notes and clarifications to addition of new activities and tasks and new chapters)
- For this presentation, these changes will be grouped in 3 categories and the most relevant will summarized in the next slides

- New additions – this category contains the topics added to the old Guide in which they were never approached
- Updates – this category is the most extended in terms of impact and it contains fine tunings, rephrasings, corrections and clarifications of existing subjects (mostly changes spread all over the document)
- Changes – removal of obsolete subjects or practices and their replacement with more up-to-date alternatives (the most significant is the removal of ISVV levels and their replacement with the conceot of ISVV tailoring

4. New to the ISVV process

- Verification of the software requirements baseline and concept documentation
  - This is a higher level activity compared with the old ISVV process, which started with the Technical Specification review
- Verification and validation of software systems developed following an Agile methodology or an iterative process
  - Agile development raises various challenges in relation with ECSS standards and implicitly to ISVV – the new Handbook provides guidance on how to adapt the ISVV process to match the Agile Software development.
  - Iterative software development is a simplier case of similar challenges, to which ISVV was adapted before, but never formalized in a coherent set of guidelines until now
- Continuous ISVV is not a completely new concept and it is somehow linked to Agile and Iterative development paradigms since it is based on continuous feedback from the development project towards ISVV project – now, the ISVV Handbook contains a separate section dedicated only to Continuous ISVV

4. New to the ISVV process

- Independent Verification and Validation of configuration data – this new part of the ISVV process refers to the following major aspects of data used by software:
  - Identification of critical data sets
  - How data sets are used in testing
  - How these data sets are produced and controlled
  - What subsets of data within predefined range are relevant for testing
  - What combinations of various data sets are more relevant, etc.

5. Updates to the ISVV process descriptions

- The Guide document structure was aligned with the ECSS handbook redacting guidelines
- Key terms and definitions were aligned with the latest ECSS standards
- The entire body of the Guide was revisited in order to simplify the text, remove ambiguities, correct mistakes, improve diagrams and tables and the overall readability of the document
- A significant number of modern methods and techniques used to perform ISVV were added
  - Annex F now contains ~20 newly added of such methods and techniques, with descriptions
- The ISVV tasks dedicated to Unit Testing were corrected, refined and expanded
- Overall improvement of ISVV tasks
  - alignement of task outputs, unused questionnaires were removed, contents of ISVV reports was clarified
- Overall optimization of ISVV tasks
  - the analysis of task effectiveness lead to merging of some tasks or complete removal of others

5. Updates to the ISVV process descriptions

- The independent verification of dependability and safety artefacts was extended
  - New tasks were added to cover the review of dependability and safety
  - The old Guide was covering the dependability and safety only as they were flown down into requirements, design and tests.
- The ISVV for reused software was improved
  - The Handbook now contains clear tasks to be applied for different tyopes of reused software, including reused software previously subjected to ISVV
- The tasks related to generated code were improved and extended
  - In addition, now, also models and tools used for code generation are covered, in different scenarios
- Several tasks covering the IVV of model-based software development were clarified
- The roles involved in an ISVV project were clarified and detailed, including the description of possible interactions
- ESA has now a recommended role defined in the new Handbook.

6. Changes to the ISVV process

The ISVV Handbook contains also the following major changes to the process:

- Now, the ISVV process has a clear set of metrics defined and a set of guidelines on how these metrics can be gathered
- Similar to the ISVV metrics, a framework for gathering the lessons learned from an ISVV project is defined
- To help the ISVV customers and ISVV providers, the Handbook now contains a template for ISVV statement of work
- To fill the gap between the ISVV Guide and ECSS standards (E80), now the Handbook defines 2 types of ISVV plans: the old ISVV plan required by E80 and the ISVV Implementation Plan which is the plan created by the ISVV supplier with the support of ISVV customer
    - Annex A.4 contains the template for the newly introduced ISVVIP.

6. Changes to the ISVV process

- The ISVV Levels reassessment lead to the removal of ISVV Levels from the management part of ISVV projects
  - The ISVV Handbook now defines the process of ISVV project tailoring
  - This concept should be seen for now as experimental, since there is no practical ecxperience yet on how efficient it is
  - The ISVV tailoring should be seen as a fully configurable set of activties and tasks to be performed in order to achieve the goals of the ISVV project
  - The Handbook defines some guidelines on how this tailoring process should be performed and it also defines some restrictions based on several parameters
  - The ISVV tailoring uses a system of priorities for every task and subtask which in conjunction with a set of influencing factors and the predefined budget, by applying the defined guidelines, will lead to a clear definition of the ISVV scope
  - The ISVV scope will be documented and contained in the ISVV plans and it will drive the ISVV activities

6. The way forward

- Some of the changes and concepts introduced by the new ISVV Handbook need validation by being applied in real projects
- The feedback from the first projects to use the new Handbook will be extremely valuable for the next iteration of the document
- To support this feedback collection, the metrics and lessons learned frameworks will play an important role (the final reports request for a summary of this information to be provided)
  - The major issue here is that the ISVV final reports cannot be centralized by a single entity (except ESA, maybe)
  - An efficient solution to collect all this information in an anonymized way still needs to be found
  - The new projects using the new Handbook are invited to provide willingly this information in a form that suits their internal restrictions
  - You may use the generic email address isvv@esa.int for any inquiry regarding the new Handbook or ISVV topics in general (the email will reach TEC-SWF, the section responsible for ISVV topics at ESA/ESTEC)

Way forward

Way forward

- **ECSS-Q-ST-80C-Rev.2 release**
  - **Expected** Q1 of 2024 and will be available to ECSS account holders via: Active Standards (ecss.nl)
- **ECSS-E-ST-40C-Rev.1 release**
  - **Expected** Q1 of 2024 and will be available to ECSS account holders via: Active Standards (ecss.nl)
  - **ECSS-E-HB-40 update ongoing** (aligning to rev.1, model-based SW engineering, …)
- **CSW-ESAISVV-2022-GBK-02897 issue 1.0**
  - **Released 12/12/2022** and is available to ESSR account holders via: Independent Software Verification and Validation Handbook (essr.esa.int)
- A new **system security standard** is being created -> currently called ECSS-Q-ST-80-10C (name will change)

Way forward

- We need **you** to improve further
- First hand project feedback for ECSS standards and ISVV guide
- Consider also the ECSS Handbooks

- Provide your feedback via: https://ecss.nl/standards/cr-form/
- Feedback is evaluated by committee (Industry and Space Agencies)
- Ask for ECSS training and support