

IEEE Standard for System, Software, and Hardware Verification and Validation

IEEE Computer Society

Developed by the
Software and Systems Engineering Standards Committee

IEEE Std 1012™-2024

STANDARDS

IEEE Standard for System, Software, and Hardware Verification and Validation

Developed by the

Software and Systems Engineering Standards Committee
of the
IEEE Computer Society

Approved 12 November 2024

IEEE SA Standards Board

Abstract: The Verification and Validation (V&V) processes are used to determine whether the development products of a given activity conform to the requirements of that activity and whether the product satisfies its intended use and user needs. V&V life cycle process requirements are specified for different integrity levels. The scope of V&V processes encompasses systems, software, and hardware, and it includes their interfaces. Systems, software, and hardware being developed, maintained, or reused [legacy, commercial off-the-shelf (COTS), non-developmental items] can be the system of interest to which this standard is applied. The term software also includes firmware and microcode, and each of the terms system, software, and hardware includes related information or documentation. V&V processes include the analysis, evaluation, review, inspection, assessment, and testing of products.

Keywords: acceptance testing, adaptive, Agile, AI, architecture evaluation, artificial intelligence, component testing, concept documentation evaluation, COTS, criticality, criticality analysis, design evaluation, disposal plan evaluation, environmental Verification and Validation (V&V) factors, field programmable gate array, firmware, FPGA, hardware life cycle, hardware V&V, hardware Verification and Validation, hazard analysis, IEEE 1012™, implementation evaluation, independent V&V, integration testing, integrity level, interface analysis, IV&V, machine learning, microcode, minimum V&V tasks, ML, nth of a kind, objective evidence, operating procedure evaluation, qualification testing, quality assurance, regression analysis, regression testing, requirements allocation analysis, requirements evaluation, reuse software, risk analysis, security analysis, SaaS software life cycle, software as a service, software quality assurance, software V&V, software Verification and Validation, source code documentation evaluation, source code evaluation, SQA, stakeholder needs and requirements evaluation, system element interaction analysis, system life cycle, system maintenance strategy assessment, system of interest, system requirements evaluation, system V&V, system Verification and Validation, testing, traceability analysis, V&V, V&V measures, Validation, Verification, vignette

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

Copyright © 2025 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 22 August 2025. Printed in the United States of America.

IEEE is a registered trademark in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

PDF: ISBN 979-8-8557-1683-2 STD27623
Print: ISBN 979-8-8557-1684-9 STDPD27623

IEEE prohibits discrimination, harassment, and bullying.

For more information, visit <https://www.ieee.org/about/corporate/governance/p9-26.html>

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE Standards documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page (<https://standards.ieee.org/ipr/disclaimers.html>), appear in all IEEE standards and may be found under the heading “Important Notices and Disclaimers Concerning IEEE Standards Documents.”

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents are developed within IEEE Societies and subcommittees of IEEE Standards Association (IEEE SA) Board of Governors. IEEE develops its standards through an accredited consensus development process, which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE standards are documents developed by volunteers with scientific, academic, and industry-based expertise in technical working groups. Volunteers involved in technical working groups are not necessarily members of IEEE or IEEE SA and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE makes no warranties or representations concerning its standards, and expressly disclaims all warranties, express or implied, concerning all standards, including but not limited to the warranties of merchantability, fitness for a particular purpose and non-infringement. IEEE Standards documents do not guarantee safety, security, health, or environmental protection, or compliance with law, or guarantee against interference with or from other devices or networks. In addition, IEEE does not warrant or represent that the use of the material contained in its standards is free from patent infringement. IEEE Standards documents are supplied “AS IS” and “WITH ALL FAULTS.”

Use of an IEEE standard is wholly voluntary. The existence of an IEEE standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity, nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document should rely upon their own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: THE NEED TO PROCURE SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus balloting process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English language version published by IEEE is the approved IEEE standard.

Use by artificial intelligence systems

In no event shall material in any IEEE Standards documents be used for the purpose of creating, training, enhancing, developing, maintaining, or contributing to any artificial intelligence systems without the express, written consent of IEEE SA in advance. “Artificial intelligence” refers to any software, application, or other system that uses artificial intelligence, machine learning, or similar technologies, to analyze, train, process, or generate content. Requests for consent can be submitted using the Contact Us form.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE SA Standards Board Operations Manual is not, and shall not be considered or inferred to be, the official position of IEEE or any of its committees and shall not be considered to be, or be relied upon as, a formal position of IEEE or IEEE SA. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that the presenter’s views should be considered the personal views of that individual rather than the formal position of IEEE, IEEE SA, the Standards Committee, or the Working Group. Statements made by volunteers may not represent the formal position of their employer(s) or affiliation(s). News releases about IEEE standards issued by entities other than IEEE SA should be considered the view of the entity issuing the release rather than the formal position of IEEE or IEEE SA.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE or IEEE SA. However, **IEEE does not provide interpretations, consulting information, or advice pertaining to IEEE Standards documents.**

Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its Societies and subcommittees of the IEEE SA Board of Governors are not able to provide an instant response to comments or questions, except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in evaluating comments or revisions to an IEEE standard is welcome to join the relevant IEEE SA working group. You can indicate interest in a working group using the Interests tab in the Manage Profile & Interests area of the [IEEE SA myProject system](#).¹ An IEEE Account is needed to access the application.

Comments on standards should be submitted using the [Contact Us](#) form.²

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not constitute compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

¹ Available at: <https://development.standards.ieee.org/myproject-web/public/view.html#landing>.

² Available at: <https://standards.ieee.org/about/contact/>.

Data privacy

Users of IEEE Standards documents should evaluate the standards for considerations of data privacy and data ownership in the context of assessing and using the standards in compliance with applicable laws and regulations.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under U.S. and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, neither IEEE nor its licensors waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate licensing fees, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400; <https://www.copyright.com/>. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every 10 years. When a document is more than 10 years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit [IEEE Xplore](#) or [contact IEEE](#).³ For more information about the IEEE SA or IEEE's standards development process, visit the IEEE SA Website.

Errata

Errata, if any, for all IEEE standards can be accessed on the [IEEE SA Website](#).⁴ Search for standard number and year of approval to access the web page of the published standard. Errata links are located under the Additional Resources Details section. Errata are also available in [IEEE Xplore](#). Users are encouraged to periodically check for errata.

³ Available at: <https://ieeexplore.ieee.org/browse/standards/collection/ieee>.

⁴ Available at: <https://standards.ieee.org/standard/index.html>.

Patents

IEEE standards are developed in compliance with the [IEEE SA Patent Policy](#).⁵

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE SA Website at <https://standards.ieee.org/about/sasb/patcom/patents.html>. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

IMPORTANT NOTICE

Technologies, application of technologies, and recommended procedures in various industries evolve over time. The IEEE standards development process allows participants to review developments in industries, technologies, and practices, and to determine what, if any, updates should be made to the IEEE standard. During this evolution, the technologies and recommendations in IEEE standards may be implemented in ways not foreseen during the standard's development. IEEE standards development activities consider research and information presented to the standards development group in developing any safety recommendations. Other information about safety practices, changes in technology or technology implementation, or impact by peripheral systems also may be pertinent to safety considerations during implementation of the standard. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, data privacy, and interference protection practices and all applicable laws and regulations.

⁵ Available at: <https://standards.ieee.org/about/sasb/patcom/materials.html>.

Participants

At the time this standard was completed, the P1012 Working Group had the following membership:

Edward A. Addy, *Chair*
Roger U. Fujii, *Vice Chair*
David P. Hooten, *Secretary*

Rossnyev Alvarado
Xu Baisong
Arde Bedjanian
Yegor Bugayenko
Susan Burgess
William Burgess
Marc Canellas
Larry Chi
Darrell Cooksey
Ken Costello
Michael Cox
Michael Crerar
John Davis
Yvonne De la Rosa
Ronald Dean
Honghan Deng
Harpal Dhama
Sunjay Dhama
Nathaniel Drechsler
Dale Dzielski

Delden Fane
Eva Freund
Ben Frisk
Dirk Guijt
Yin Guo
Jon Hagar
Sheri Harshberger
Paul Heininger
George Hughes
David Jarosh
John Kay
Tom Kurihara
He Libing
Andrew Lodge
Baofu Lu
Paul Lusardi
Kris Marshall
Collin McMahon
M. R. Nayak
Charles Nielsen
Al Pangelinan

Chandra Patel
Laura Pullum
Bill Roggenbrodt
Barbara Scalia
Taylor Schalmo
Scott Schield
William Schoenhals
Steve Schwarm
Tricia Shaffer
Li Shi
Carl Singer
Ryan Stone
Gerald Stueve
Serdar Uyar
Murat Uzman
Wes Weiner
Yichun Wu
Zhu Xihu
Steve Yang
Bin Zhang

The following members of the individual balloting committee voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

Edward A. Addy
Johann Amsenga
Butch Anton
Juris Borzovs
Pieter Botman
Marc Canellas
Paul Cardinal
Lynn Carter
Lawrence Catchpole
Zhiman Chen
CarlEric Codere
Ronald Dean
Dale Dzielski
Luisandrey Fajardofajardo
Roger U. Fujii
David Fuschi
Jon Hagar

Sheri Harshberger
David Herrell
Werner Hoelzl
David P. Hooten
Piotr Karocki
John Kay
Daozhuang Lin
Claire Lohr
Edward McCall
Roberto Moreno
Joanna Olszewska
Moradeke Olumogba
Thomas Owens
Cam Posani
R. K. Rannow
Annette Reilly

Robert Schaaf
Jhony Sembiring
Raymond Senechal
Thomas Starai
Eugene Stoudenmire
Walter Struppler
Maryna Tyrpak
Hasan Uyar
Murat Uzman
John Vergis
Stephen Webb
Peter Wishart
M. Woolf
Weiping Wu
Yichun Wu
Janusz Zalewski
Bin Zhang

When the IEEE SA Standards Board approved this standard on 12 November 2024, it had the following membership:

David J. Law, *Chair*
Jon W. Rosdahl, *Vice Chair*
Gary Hoffman, *Past Chair*
Alpesh Shah, *Secretary*

Sara Biyabani
Ted Burse
Stephen Dukes
Doug Edwards
J. Travis Griffith
Guido R. Hiertz
Ronald W. Hotchkiss

Hao Hu
Yousef Kimiagar
Joseph L. Koepfinger*
Howard Li
Xiaohui Liu
John Haiying Lu
Kevin W. Lu
Hiroshi Mano

Paul Nikolich
Robby Robson
Lei Wang
F. Keith Waters
Sha Wei
Philip B. Winston
Don Wright

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 1012-2024, IEEE Standard for System, Software, and Hardware Verification and Validation.

The Verification and Validation (V&V) processes are technical processes of systems, software and hardware engineering. The Verification process and the Validation process are interrelated and complementary processes, and are referenced together as Verification and Validation. The purpose of V&V is to help the organization build quality into the system during the life cycle. V&V processes provide an objective assessment of products and processes throughout the life cycle. This assessment demonstrates whether the requirements are correct, complete, accurate, consistent, and testable. The V&V processes determine whether the development products of a given activity conform to the requirements of that activity and whether the product satisfies its intended use and user needs. The determination includes the assessment, analysis, evaluation, review, inspection, and testing of products and processes. V&V is performed in parallel with all life cycle stages, not at their conclusion.

V&V is an extension of program management and systems, software, and hardware engineering that employs a rigorous methodology to identify objective data and conclusions to provide feedback about quality, performance, and schedule to the supplier. This feedback consists of anomaly resolutions, performance improvements, and quality improvements not only for expected operating conditions but also across the full spectrum of the system and its interfaces. Early feedback results allow the organization to modify the products in a timely fashion and thereby reduce overall project and schedule impacts. Without a proactive approach, the anomalies and associated system changes are typically delayed to later in the program schedule, resulting in greater program costs and schedule delays.

IEEE Std 1012TM is a process standard that defines the V&V processes in terms of specific activities and related tasks. The standard also defines the contents of the V&V plan (VVP), including example formats.

V&V may be performed at the level of the system, software element, or hardware element, or on any combination of these. V&V may also be performed on an element of a system, including a subordinate system (i.e., subsystem). Throughout this standard, the term hardware means an electronic or mechanical hardware element. In each case, the V&V processes are invoked, either in parallel or recursively, across the full life cycle of the system or element.

This version of the standard is a revision to IEEE Std 1012TM-2016/Cor1-2017 [B19].⁶ The earliest version of this standard (1986) described the content of a software V&V plan, with subsequent versions (1998 and 2004) changing the focus from the software V&V plan to software V&V processes. The 2012 revision expanded the scope of the V&V processes to include systems and hardware as well as software. The 2016 revision aligned the system V&V process more completely with the terminology and structure of ISO/IEC/IEEE 15288:2023(E) [B41]. This revision aligns the software and hardware V&V processes with the terminology and structure of ISO/IEC/IEEE 12207:2017(E) [B40] and adds several new annexes, including a set of vignettes to provide examples of applying this standard under various scenarios. The following is a summary of the changes made in this version:

- No new V&V activities or tasks have been added; however, some activities and tasks have been rearranged to align with the new or modified processes from ISO/IEC/IEEE 12207:2017(E) [B40]. Some V&V activities and tasks have been rearranged to facilitate understanding and ease of use.
- The terminology and structure were revised to be consistent with ISO/IEC/IEEE 12207:2017(E) [B40].
- Annexes were added on the topics of test concepts for V&V, V&V for artificial intelligence/machine learning systems, V&V of field programmable gate arrays, and guidance on V&V in an adaptive development environment such as Agile.

⁶ The numbers in brackets correspond to those of the bibliography in Annex P.

- Revisions were made to the annexes on independence and reuse.
- An annex was added to provide vignettes that illustrate the application of this standard in various scenarios, with special consideration of criticality analysis and its impact.

The following key concepts are emphasized in this standard:

- Integrity levels: Defines four integrity levels to describe the importance of the system, software, and hardware, varying from high integrity to low integrity, to the user.
- Minimum V&V tasks for each integrity level: Defines the minimum V&V tasks required for each of the four integrity levels.
- Optional V&V tasks: Includes a table of optional V&V tasks for tailoring the V&V effort to address the project needs and application-specific characteristics.
- Intensity and rigor applied to V&V tasks: Includes the concept that the intensity and rigor applied to the V&V tasks vary according to the integrity level. Higher integrity levels require the application of greater intensity and rigor to the V&V task. Intensity includes a greater scope of analysis across all normal and abnormal system operating conditions. Rigor includes more formal techniques and recording procedures.
- Detailed criteria for V&V tasks: Defines specific criteria for each V&V task, including minimum criteria for correctness, consistency, completeness, accuracy, readability, and testability. The V&V task descriptions include a list of the required task inputs and outputs.
- Systems viewpoints: Includes minimum software and hardware V&V tasks to address system issues. These tasks include hazard analysis, security analysis, risk analysis, migration assessment, and retirement assessment. Specific system issues are contained in individual V&V task criteria.
- Conformance to international and IEEE standards: Defines the V&V processes to conform to life cycle process standards such as ISO/IEC/IEEE 15288:2023(E) [B41] and ISO/IEC/IEEE 12207:2017(E) [B40], as well as the family of IEEE systems and software engineering standards. This standard addresses all system and software life cycle processes, including those in the Agreement, Organizational Project-Enabling, Technical Management, and Technical process groups. This standard is compatible with all life cycle models; however, not all life cycle models use all of the life cycle processes described in this standard.

Acknowledgements

The IEEE P1012 Working Group would like to acknowledge the strong contribution by Dr. Michael J. Cox in the development of this revision of IEEE Std 1012. Dr. Cox passed away on March 2, 2020, and his commitment to improving professionalism in systems engineering and V&V is reflected in this standard.

Contents

1. Overview	15
1.1 Scope	15
1.2 Purpose	16
1.3 Word usage.....	16
1.4 Field of application.....	17
1.5 V&V objectives.....	18
1.6 Organization of the standard.....	18
1.7 Audience.....	21
1.8 Conformance	21
1.9 Disclaimer.....	21
2. Normative references.....	21
3. Definitions and acronyms.....	22
3.1 Definitions	22
3.2 Acronyms	27
4. Relationships between V&V and life cycle processes.....	28
5. Integrity levels.....	32
6. Overview of V&V processes.....	34
6.1 General	34
6.2 V&V team characteristics.....	35
6.3 V&V testing.....	36
7. Common V&V processes.....	37
7.1 V&V Management Process	37
7.2 Acquisition Support V&V Process	39
7.3 Supply Planning V&V Process.....	39
7.4 Project Planning V&V Process.....	40
7.5 Configuration Management V&V Process	40
8. System V&V processes.....	51
8.1 Business or Mission Analysis V&V Process	51
8.2 Stakeholder Needs and Requirements Definition V&V Process	51
8.3 System Requirements Definition V&V Process	52
8.4 Architecture Definition V&V Process.....	53
8.5 Design Definition V&V Process.....	54
8.6 System Analysis V&V Process.....	55
8.7 Implementation V&V Process	55
8.8 Integration V&V Process.....	56
8.9 Verification Process.....	57
8.10 Transition V&V Process.....	58
8.11 Validation Process	58
8.12 Operation V&V Process	59
8.13 Maintenance V&V Process.....	60
8.14 Disposal V&V Process	61
9. Software V&V processes.....	96
9.1 Business or Mission Analysis V&V Process	96
9.2 Stakeholder Needs and Requirements Definition V&V Process	97

9.3 System/Software Requirements Definition V&V Process.....	97
9.4 Architecture Definition V&V Process.....	98
9.5 Design Definition V&V Process.....	99
9.6 System Analysis V&V Process.....	100
9.7 Implementation V&V Process.....	101
9.8 Integration V&V Process.....	102
9.9 Verification Process.....	103
9.10 Transition V&V Process.....	103
9.11 Validation Process.....	104
9.12 Operation V&V Process.....	105
9.13 Maintenance V&V Process.....	105
9.14 Disposal V&V Process.....	107
10. Hardware V&V processes.....	148
10.1 Business or Mission Analysis V&V Process.....	148
10.2 Stakeholder Needs and Requirements Definition V&V Process.....	149
10.3 System/Hardware Requirements Definition V&V Process.....	149
10.4 Architecture Definition V&V Process.....	150
10.5 Design Definition V&V Process.....	151
10.6 System Analysis V&V Process.....	152
10.7 Implementation V&V Process.....	153
10.8 Integration V&V Process.....	154
10.9 Verification Process.....	155
10.10 Transition V&V Process.....	155
10.11 Validation Process.....	156
10.12 Operation V&V Process.....	157
10.13 Maintenance V&V Process.....	157
10.14 Disposal V&V Process.....	158
11. V&V reporting, administrative, and documentation requirements.....	192
11.1 V&V reporting requirements.....	192
11.2 V&V administrative requirements.....	195
11.3 V&V documentation requirements.....	195
12. V&V plan.....	196
12.1 Overview.....	196
12.2 VVP section 1: Purpose.....	197
12.3 VVP section 2: Referenced documents.....	197
12.4 VVP section 3: Definitions.....	197
12.5 VVP section 4: V&V overview.....	197
12.6 VVP section 5: V&V processes.....	199
12.7 VVP section 6: V&V reporting requirements.....	199
12.8 VVP section 7: V&V administrative requirements.....	199
12.9 VVP section 8: V&V test documentation requirements.....	200
Annex A (informative) V&V test concepts.....	201
Annex B (informative) A risk-based integrity level schema.....	210
Annex C (informative) Definition of independent V&V (IV&V).....	212
C.1 Independence parameters.....	212
C.2 Forms of independence.....	212
Annex D (informative) V&V of reuse software and hardware, including COTS.....	215
D.1 Purpose.....	215
D.2 V&V of software developed in a reuse process.....	216

D.3 V&V of software developed and reused outside of a reuse process	216
Annex E (informative) V&V measures	221
E.1 Introduction	221
E.2 Measures for evaluating anomaly density	221
E.3 Measures for evaluating V&V effectiveness.....	222
E.4 Measures for evaluating V&V efficiency.....	222
Annex F (informative) Example of V&V relationships to other project responsibilities	224
Annex G (informative) Optional V&V tasks.....	225
Annex H (informative) Environmental factors consideration	231
H.1 Introduction	231
H.2 In the agreement processes	231
H.3 In the organizational project-enabling processes	231
H.4 In the project processes.....	232
H.5 In the technical processes	232
Annex I (informative) V&V of system, software, and hardware integration	234
I.1 Introduction	234
I.2 Examples of system failures caused by integration issues	234
Annex J (informative) Hazard, security, and risk analyses	239
J.1 Introduction.....	239
J.2 Hazard analysis	240
J.3 Security analysis	241
J.4 Risk analysis	249
Annex K (informative) Example of assigning and changing the system integrity level of “supporting system functions”	251
Annex L (informative) Verification and Validation of n th of a kind systems.....	253
Annex M (informative) Guidance for applying IEEE 1012 in an adaptive environment.....	255
M.1 Introduction.....	255
M.2 Background.....	256
M.3 V&V for adaptive (agile) activities.....	257
Annex N (informative) Verification and Validation considerations for machine learning and artificial intelligence	260
N.1 Introduction	260
N.2 Requirements V&V	260
N.3 Hazard analysis.....	262
N.4 Testing V&V	264
N.5 Approaches to the V&V of AI/ML	267
N.6 Model evaluation	267
N.7 Operation V&V	268
Annex O (informative) Vignettes to illustrate application of IEEE 1012.....	269
O.1 Introduction	269
O.2 Integrity level assignment of nuclear power system	270
O.3 Determining the integrity level for a CCTV monitoring system onboard a rail vehicle.....	280
O.4 Application of IEEE Std 1012 to a Non-defense government system	287
O.5 Determining integrity level for training simulators	293

O.6 V&V of field programmable gate array (FPGA) based systems.....	298
Annex P (informative) Bibliography	304

IEEE Standard for System, Software and Hardware Verification and Validation

1. Overview

1.1 Scope

This Verification and Validation (V&V) standard is a process standard that addresses all system, software, and hardware life cycle processes, including the Agreement, Organizational Project-Enabling, Technical Management, and Technical Process Groups. This standard is compatible with all life cycle models (e.g., system, software, and hardware); however, not all life cycle models use all of the processes listed in this standard.

V&V processes determine whether the development products of a given activity conform to the requirements of that activity and whether the product satisfies its intended use and user needs. This determination may include the analysis, evaluation, review, inspection, assessment, and testing of products and processes.

The user of this standard invokes the V&V processes associated with the life cycle processes used by the project. A description of system life cycle processes may be found in ISO/IEC/IEEE 15288:2023(E) [\[B41\]](#), and a description of software life cycle processes may be found in ISO/IEC/IEEE 12207:2017(E) [\[B40\]](#).

This standard defines the Verification and Validation Processes that are applied to the system, software, and hardware development throughout the life cycle, including acquisition, supply, development, operations, maintenance, and retirement. This standard applies to the system, software, and hardware being acquired, developed, maintained, or reused. The term software also includes firmware and microcode (e.g., field programmable gate arrays and programmable logic devices). Each of the terms system, software, and hardware includes its associated documentation.

The Verification Process provides objective evidence for whether the products:

- Conform to requirements (e.g., for correctness, completeness, consistency, and accuracy) for all activities during each life cycle process.
- Satisfy the standards, practices, and conventions during life cycle processes.
- Successfully complete each life cycle activity and satisfy all the criteria for initiating succeeding life cycle activities (i.e., builds the product correctly).

The Validation Process provides objective evidence for whether the products:

- Satisfy system requirements allocated to the products at the end of each life cycle activity.
- Solve the right problem (e.g., correctly model physical laws, implement business rules, and use the proper system assumptions).

— Satisfy intended use and user needs in the operational environment (i.e., builds the correct product). The Verification Process and the Validation Process are interrelated and complementary processes that use each other's process results to establish better completion criteria and analysis, evaluation, review, inspection, assessment, and test V&V tasks for each life cycle activity. The V&V task criteria described in [Table 1a](#) through [Table 1d](#) explicitly define the conformance requirements for V&V processes.

The development of a sufficient body of evidence requires a trade-off between the amount of time spent and a finite set of system conditions and assumptions against which to perform the V&V tasks. Each project should define criteria for a sufficient body of evidence (e.g., selecting an integrity level), the schedule, and the scope of the V&V analysis and test tasks.

This standard does not assign the responsibility for performing the V&V tasks to any specific organization. The analysis, evaluation, and test activities may be performed by multiple organizations; however, the methods and purpose will differ for each organization's functional objectives.

ISO/IEC/IEEE 15288:2023(E) [\[B41\]](#) and ISO/IEC/IEEE 12207:2017(E) [\[B40\]](#) include tasks for the supplier to execute the agreement according to established project plans and to deliver the product or service in accordance with the agreement criteria. The techniques described in this standard are useful in performing the supplier's tests and evaluations. Therefore, whenever this standard mentions the supplier's performance of a Verification or Validation activity, it is to be understood that the reference applies to the test and evaluation tasks of system development.

1.2 Purpose

The purpose of this standard is to achieve the following:

- Establish a common framework of the V&V processes, activities, and tasks in support of all system, software, and hardware life cycle processes.
- Define the V&V tasks, required inputs, and required outputs in each life cycle process.
- Identify the minimum V&V tasks corresponding to a four-level integrity schema.
- Define the content of the V&V plan.

1.3 Word usage

The word *shall* indicates mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (*shall equals is required to*).^{7,8}

The word *should* indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required (*should equals is recommended that*).

The word *may* is used to indicate a course of action permissible within the limits of the standard (*may equals is permitted to*).

The word *can* is used for statements of possibility and capability, whether material, physical, or causal (*can equals is able to*).

⁷ The use of the word *must* is deprecated and cannot be used when stating mandatory requirements; *must* is used only to describe unavoidable situations.

⁸ The use of *will* is deprecated and cannot be used when stating mandatory requirements; *will* is only used in statements of fact.

1.4 Field of application

This standard applies to all applications of systems. When conducting V&V of a system, software, or hardware element, it is important to examine the interactions with the system of which the element is a part. This standard identifies the important system considerations that V&V processes, activities and tasks address in determining correctness and other V&V attributes (e.g., completeness, accuracy, consistency, and testability).

The dynamics of complex systems and the multitude of different logic paths available within the system in response to varying stimuli and conditions demand that the V&V effort examines the correctness of the system for each possible variation in conditions. The ability to model complex, real-world conditions will be limited, and thus, the V&V effort examines whether the limits of the modeling are realistic and reasonable for the desired solution. The unlimited combination of system conditions presents the V&V effort with the challenge of using a finite set of analytical, test, simulation, and demonstration techniques to establish a reasonable body of evidence that the system is correct.

A system provides the capability to satisfy a stated need or objective by combining one or more of the following: processes, hardware, software, facilities, and people. These relationships require that V&V processes consider interactions among all system elements (software and hardware). The V&V processes address the following interactions with the system:

- Environment: Determines that the system correctly accounts for all conditions, natural phenomena, physical laws of nature, business rules, and physical properties and the full ranges of the system operating environment.
- Operators/users: Determines that the system communicates the proper status/condition of the system to the operator/user and correctly processes all operator/user inputs to produce the required results. For incorrect operator/user inputs, assures that the system is protected from entering into a dangerous or uncontrolled state. Validates that operator/user policies and procedures (e.g., security, interface protocols, data representations, and system assumptions) are consistently applied and used across each component interface.
- Other software, hardware, and systems: Determines that the software or hardware component interfaces correctly with other components in the system of interest in accordance with requirements and that errors are not propagated between components of the system of interest.

The scope of V&V processes includes the operational environment, operators and users, hardware, software, data processes (e.g., processes for providing service to users), procedures (e.g., operator instructions), and facilities. The user of this standard should consider V&V as part of the life cycle processes defined by industry standards, such as ISO/IEC/IEEE 12207:2017(E) [\[B40\]](#) or ISO/IEC/IEEE 15288:2023(E) [\[B41\]](#).

To address the systems perspective, the system, software, and hardware V&V efforts should provide an integrated analysis where the V&V tasks are interrelated, providing input and insight into other V&V tasks. The results from completed life cycle processes provide valuable and necessary inputs to V&V tasks in other life cycle processes. The results and findings from one V&V task may cause previously completed V&V tasks to be analyzed again with the new data. This relationship among V&V tasks (including feedback to the technical and software/hardware specific processes) employing rigorous systems engineering techniques is a key approach to an integrated systems, software, and hardware V&V. The V&V results provide the other ISO/IEC/IEEE 15288:2023(E) [\[B41\]](#) and ISO/IEC/IEEE 12207:2017(E) [\[B40\]](#) life cycle processes (agreement, organizational project-enabling, technical management, and technical) with early detection of anomalies and potential process trends that may be used for process improvement. The V&V processes and tasks described in this standard may be used in conjunction with systems engineering and process improvement models, such as the CMU/SEI-2010-TR-033 [\[B6\]](#).

1.5 V&V objectives

V&V processes provide an objective assessment of products and processes throughout the life cycle. This assessment demonstrates whether the requirements are correct, complete, accurate, consistent, and testable. The V&V processes determine whether the products of a given activity conform to the requirements of that activity and whether the product satisfies its intended use and user needs. The determination includes assessment, analysis, evaluation, review, inspection, and testing of products and processes. V&V tasks are performed in parallel with all life cycle stages, not at their conclusion.

The results of V&V provide the following benefits to the program:

- Facilitate early detection and correction of anomalies
- Enhance management insight into process and product risks
- Support the life cycle processes to assure conformance to program performance, schedule, and budget
- Provide an early assessment of performance
- Provide objective evidence of conformance to support a formal certification process
- Improve the products from the acquisition, supply, development, and maintenance processes
- Support process improvement activities

1.6 Organization of the standard

The V&V processes described in this standard are constructed to be consistent with ISO/IEC/IEEE 15288:2023(E) [B41] and ISO/IEC Std 12207:2008(E) [B40].

This standard is organized into clauses (Clause 1 through Clause 12), tables [Table 1 through Table 3, and their respective subparts a) through d)], figures [Figure 1 and Figure 2, and their respective subparts a) through d)], and annexes (Annex A through Annex P). Clause 2 through Clause 12, [Table 1a](#) through [Table 1d](#), and [Table 2a](#) through [Table 2d](#) provide the mandatory V&V requirements for this standard. [Table 1a](#) through [Table 1d](#) and [Table 2a](#) through [Table 2d](#) are the focal points of this standard, containing detailed V&V activity and task requirements. [Table 1a](#) through [Table 1d](#) and [Table 2a](#) through [Table 2d](#) address the following:

- Common V&V tasks in [Table 1a](#) and [Table 2a](#)
- System V&V tasks in [Table 1b](#) and [Table 2b](#)
- Software V&V tasks in [Table 1c](#) and [Table 2c](#)
- Hardware V&V tasks in [Table 1d](#) and [Table 2d](#)

Each clause listed below contains V&V activities and tasks and has the subset of [Table 1a](#) through [Table 1d](#) and [Table 2a](#) through [Table 2d](#) associated with the V&V requirements for that clause. [Figure 1a](#) through [Figure 1d](#), [Figure 2a](#) through [Figure 2d](#), and [Table 3a](#) through [Table 3d](#) contain informative material that provide examples of V&V processes and guidance for using this standard, and they are similarly organized.

- [Clause 1](#) provides guidance for using this standard.
- [Clause 2](#) is reserved for normative references; however, this standard does not prescribe any normative references.
- [Clause 3](#) provides a definition of terms, abbreviations, and conventions.
- [Clause 4](#) describes the relationships between the V&V processes and the life cycle processes from ISO/IEC/IEEE 15288:2023(E) and ISO/IEC/IEEE 12207:2017(E) [B40], and it describes how the V&V standard is applied recursively within the concept of a system of systems and from system to software or hardware components.
- [Clause 5](#) describes the use of integrity levels to determine the scope and rigor of V&V processes.

- [Clause 6](#) explains how V&V tasks are described within this standard.
- [Clause 7](#) describes common V&V tasks. The common V&V tasks are invoked for any V&V that is performed (system, software, or hardware).
 - 1) [Table 1a](#) contains the V&V tasks and activities and their criteria for common V&V tasks and activities.
 - 2) [Table 2a](#) contains the minimum tasks for each integrity level for common V&V tasks.
 - 3) [Table 3a](#) contains the optional common V&V tasks.
 - 4) [Figure 1a](#) depicts a summary of common V&V activities and tasks.
 - 5) [Figure 2a](#) depicts a summary of V&V test products and tasks.
- [Clause 8](#) describes system V&V tasks.
 - 1) [Table 1b](#) contains the V&V tasks and activities and their criteria for system V&V tasks and activities.
 - 2) [Table 2b](#) contains the minimum tasks for each integrity level for system V&V tasks.
 - 3) [Table 3b](#) contains the optional system V&V tasks.
 - 4) [Figure 1b](#) depicts a summary of system V&V activities and tasks.
 - 5) [Figure 2b](#) depicts a summary of system V&V test products and tasks.
- [Clause 9](#) describes software V&V tasks.
 - 1) [Table 1c](#) contains the V&V tasks and activities and their criteria for software V&V tasks and activities.
 - 2) [Table 2c](#) contains the minimum tasks for each integrity level for software V&V tasks.
 - 3) [Table 3c](#) contains the optional software V&V tasks.
 - 4) [Figure 1c](#) depicts a summary of software V&V activities and tasks.
 - 5) [Figure 2c](#) depicts a summary of software V&V test products and tasks.
- [Clause 10](#) describes hardware V&V tasks.
 - 1) [Table 1d](#) contains the V&V tasks and activities and their criteria for hardware V&V tasks and activities.
 - 2) [Table 2d](#) contains the minimum tasks for each integrity level for hardware V&V tasks.
 - 3) [Table 3d](#) contains the optional hardware V&V tasks.
 - 4) [Figure 1d](#) depicts a summary of hardware V&V activities and tasks.
 - 5) [Figure 2d](#) depicts a summary of hardware V&V test products and tasks.
- [Clause 11](#) describes V&V reporting, administrative, and documentation requirements.
- [Clause 12](#) describes the content of a V&V plan.

This standard is organized so that the V&V processes (system, software, or hardware) may be invoked separately or in any combination. V&V processes may be accomplished in any of the following combinations: system V&V ([Clause 8](#)), software V&V ([Clause 9](#)), hardware V&V ([Clause 10](#)), system/software V&V ([Clause 8](#) and [Clause 9](#)), system/hardware V&V ([Clause 8](#) and [Clause 10](#)), software/hardware V&V ([Clause 9](#) and [Clause 10](#)), and system/software/hardware V&V ([Clause 8](#) through [Clause 10](#)). Some V&V tasks are common to systems, software, and hardware V&V; in order not to repeat these V&V tasks in each part, the common V&V tasks are listed once in [Clause 7](#). The common V&V tasks are invoked for any V&V that is performed. These combinations are illustrated in [Figure 3](#).

V&V Scope	Common Clause 7	System Clause 8	Software Clause 9	Hardware Clause 10
System only	X	X		
Software only	X		X	
Hardware only	X			X
System and software	X	X	X	
System and hardware	X	X		X
Software and hardware	X		X	X
System, software, and hardware	X	X	X	X

Figure 3—V&V effort combination

NOTE—References to Table 1 and Table 2 without a suffix a, b, c, or d are understood to include those parts of the table that correspond to the parts of the V&V scope being invoked (i.e., Common, System, Software, or Hardware). References to Figure 1 and Figure 2 that do not have a suffix a, b, c, or d are similarly understood to include those parts of the figure that correspond to the parts of the V&V scope being invoked.⁹

[Clause 4](#) through [Clause 6](#) contain guidance that is applicable to all combinations of the V&V scope. [Clause 11](#) contains reporting requirements for all combinations of V&V scope. [Clause 12](#) describes the content of the V&V plan and provides a sample V&V plan outline.

[Table 1a](#) through [Table 1d](#) provide V&V task descriptions, inputs, and outputs for each life cycle process. [Table 2a](#) through [Table 2d](#) list minimum V&V tasks required for different integrity levels. [Table 3a](#) through [Table 3d](#) provide a list of optional V&V tasks and their suggested applications in the system life cycle. These optional V&V tasks may be added to the minimum V&V tasks to tailor the V&V effort to project needs.

[Figure 1a](#) through [Figure 1d](#) provide an example of an overview of the V&V inputs, outputs, and minimum V&V tasks for integrity level 4. [Figure 2a](#) through [Figure 2d](#) provide guidelines for scheduling V&V test planning, execution, and Verification activities. An example of a phased life cycle model was used in [Figure 1a](#) through [Figure 1d](#) and [Figure 2a](#) through [Figure 2d](#) to illustrate a mapping of the ISO/IEC/IEEE 12207:2017(E) [\[B40\]](#) life cycle processes to the V&V activities and tasks described in this standard.

All annexes are informative. [Annex A](#) discusses concepts related to V&V testing. [Annex B](#) provides an example of a risk-based, four-level integrity schema. [Annex C](#) describes the degrees of independence in V&V. [Annex D](#) provides guidelines for conducting V&V of reuse software. [Annex E](#) describes V&V measures. [Annex F](#) illustrates an example of the V&V organizational relationship to other project responsibilities. [Annex G](#) describes optional V&V tasks. [Annex H](#) describes environmental factors that should be considered when conducting V&V. [Annex I](#) discusses potential issues with interactions among systems, software, and hardware. [Annex J](#) describes hazard analysis, security analysis, and risk analysis and their role in V&V. [Annex K](#) provides an example of assigning and changing the integrity level of supporting system functions. [Annex L](#) describes V&V for n^{th} of a kind systems. [Annex M](#) provides guidance for conducting V&V in an adaptive environment, such as Agile. [Annex N](#) discusses V&V considerations for machine learning and artificial intelligence (AI). [Annex O](#) contains vignettes (Integrity level assignment of nuclear power system, Determining the integrity level for a CCTV monitoring system onboard a rail vehicle, Application of IEEE Std 1012 to a non-defense government system, Determining integrity level for training simulators, and V&V of field programmable gate array (FPGA) based systems) to provide examples and considerations in determining criticality levels and applying V&V within varied scenarios. [Annex P](#) provides a bibliography of the informative standards referenced in this standard.

⁹ Notes in text, tables, and figures are given for information only and do not contain requirements needed to implement the standard.

1.7 Audience

The audience for this standard includes system, software, and hardware suppliers, acquirers, developers, maintainers, V&V practitioners, operators, users, and managers in both the supplier and acquirer organizations.

1.8 Conformance

The word *shall* identifies the mandatory requirements to be followed to conform to this standard. The words *should* and *may* indicate optional tasks that are not required to claim conformance to this standard.

Not all V&V efforts are initiated at the start of the life cycle process of Acquisition and continued through the Maintenance Process. If a project uses only selected life cycle processes, then conformance to this standard is achieved if the minimum V&V tasks are implemented for all of the associated life cycle processes selected for the project. A claim of conformance to this standard includes identification of the applicable life cycle processes. As in all cases, the minimum V&V tasks are defined by the integrity level assigned to the system, software, or hardware.

For life cycle processes that are not used by the project, the V&V requirements and tasks for those life cycle processes are optional V&V tasks invoked as needed at the discretion of the project. Specific development methods and technologies (such as automated code generation from detailed design) may eliminate development steps or combine several development steps into one; therefore, a corresponding adaptation of the minimum V&V tasks is permitted and is documented in any claim of conformance to this standard.

When this standard is invoked for existing systems, software, or hardware and the required V&V inputs are not available, then the V&V tasks may use other available project input sources or may reconstruct the needed inputs to achieve conformance to this standard.

[Clause 2](#) through [Clause 12](#), [Table 1a](#) through [Table 1d](#) and [Table 2a](#) through [Table 2d](#) provide the mandatory V&V requirements for this standard. System, software, or hardware conformance to this standard can be achieved by demonstrating that all the “shall” requirements in the specified clauses are met as defined by the following:

- System V&V conformance: [Clause 7](#) and [Clause 8](#)
- Software V&V conformance: [Clause 7](#) and [Clause 9](#)
- Hardware V&V conformance: [Clause 7](#) and [Clause 10](#)

All conformance waivers need to be approved by the acquiring organization and described in the Verification and Validation plan (VVP). The information required for deviations and waivers includes the task identification, rationale, and the effect on quality.

1.9 Disclaimer

This standard establishes minimum criteria for V&V processes, activities, and tasks. However, implementing these criteria does not automatically ensure conformance to system or mission objectives, or prevent adverse consequences (e.g., loss of life, mission failure, loss of system safety or security, or financial or social loss). Conformance to this standard does not absolve any party from any social, moral, financial, or legal obligations.

2. Normative references

This standard does not require the use of any normative references.

3. Definitions and acronyms

3.1 Definitions

For the purposes of this document, the following terms and definitions apply. The *IEEE Standards Dictionary Online* [B16] or the IEEE Standards Dictionary [B15] should be consulted for terms not defined in this clause.¹⁰

acceptance testing: (A) Testing conducted to determine whether a system satisfies its acceptance criteria and to enable the customer to determine whether to accept the system. **(B)** Formal testing conducted to enable a user, customer, or other authorized entity to determine whether to accept a system or component.

NOTE—See ISO/IEC/IEEE 24765:2017 [B43].

acquirer: Stakeholder that acquires or procures a product or service from a supplier. Other terms commonly used for an acquirer are buyer, customer, owner, or purchaser.

NOTE—See ISO/IEC/IEEE 24765:2017 [B43].

anomaly: Anything observed in the documentation or operation of a system that deviates from expectations based on previously verified system, software, or hardware products or reference documents.

NOTE—See ISO/IEC/IEEE 24765:2017 [B43].

artificial intelligence (AI): <discipline> research and development of mechanisms and applications of AI systems.

NOTE 1—AI systems are designed to operate with varying levels of automation.

NOTE 2—Predictions can refer to various kinds of data analysis or production (including translating text, creating synthetic images, or diagnosing a previous power failure). It does not imply anteriority.

NOTE 3—See ISO 22989-2021 [B38].

artificial intelligence system (AIS): Engineered system that generates outputs such as content, forecasts, recommendations, or decisions for a given set of human-defined objectives.

NOTE—See ISO 22989-2021 [B38].

asset: An item (e.g., design, specifications, source code, documentation, test suites, or manual procedures) that has been designed for use in multiple contexts.

NOTE—See IEEE Std 1517™-2010 [B24].

baseline: Any agreement or result designated and fixed at a given time, from which changes require justification and approval.

NOTE—See ISO/IEC/IEEE 24765:2017 [B43].

commercial off the shelf (COTS): Software and/or hardware product available for purchase and use without the need to conduct development activities.

¹⁰IEEE Standards Dictionary Online is available at: <http://dictionary.ieee.org>. An IEEE account is required for access to the dictionary, and one can be created at no charge on the *dictionary sign-in page*.

NOTE 1—COTS software product includes the product description (including all cover information, data sheet, web site information, etc.), the user documentation (necessary to install and use the software), the software contained on a computer sensible media (disk, CD-ROM, internet downloadable, etc.). Software is mainly composed of programs and data. This definition applies also to product descriptions, user documentation and software which are produced and supported as separate manufactured goods, but for which typical commercial fees and licensing considerations do not apply.

NOTE 2—See ISO/IEC/IEEE 24765:2017 [B43].

component: One part that makes up a system. A component may be hardware or software and may be subdivided into other components.

NOTE 1—The terms module, component, and unit are often used interchangeably or defined to be subelements of one another in different ways depending on the context. The relationship of these terms is not yet standardized.

NOTE 2—See ISO/IEC/IEEE 24765:2017 [B43].

component testing: Testing of individual hardware or software components.

NOTE—See ISO/IEC/IEEE 24765:2017 [B43].

criticality: The degree of impact that a requirement, module, error, fault, failure, or other item has on the development or operation of a system.

NOTE—See ISO/IEC/IEEE 24765:2017 [B43].

documentation: A record (e.g., report, calculation, specification) or other similar product that provides an evidentiary basis of a single or series of activities, tasks, or events and their associated plans, results, or outcomes that may support a larger product, process, or program. Documentation may be printed, electronic, or presented in another suitable media that allows the viewer to confirm that specific activities or tasks occurred and that any associated plans, outcomes, or results have been accurately recorded.

NOTE—This standard uses the term ‘documentation’ in an equivalent manner to the term document that may serve as a single information item or may be a part of a larger information item.

domain: A problem space.

NOTE—See IEEE Std 1517-2010 [B24].

domain analysis: (A) The analysis of systems within a domain to discover commonalities and differences among them. (B) The process by which information used in developing software systems is identified, captured, and organized so that it can be reused to create new systems, within a domain. (C) The result of the process in (A) and (B).

NOTE—See IEEE Std 1517-2010 [B24].

domain engineering: A reuse-based approach to defining the scope (i.e., domain definition), specifying the structure (i.e., domain architecture), and building the assets (e.g., requirements, designs, software code, and documentation) for a class of systems, subsystems, or applications. Domain engineering may include the following activities: domain definition, domain analysis, developing the domain architecture, and domain implementation.

NOTE—See IEEE Std 1517-2010 [B24].

firmware: The combination of a hardware device and computer instructions and data that reside as read-only software on that device.

NOTE 1—This term is sometimes used to refer only to the hardware device or only to the computer instructions or data, but these meanings are deprecated.

NOTE 2—The confusion surrounding this term has led some to suggest that it be avoided altogether.

NOTE 3—See ISO/IEC/IEEE 24765:2017 [B43].

government off the shelf (GOTS): software and/or hardware product supplied by the government for reuse in another project.

NOTE—See ISO/IEC/IEEE 24765:2017 [B43].

hazard: **(A)** An intrinsic property or condition that has the potential to cause harm or damage. **(B)** A source of potential harm or a situation with a potential for harm in terms of human injury, damage to health, property, or the environment, or some combination of these.

NOTE—See ISO/IEC/IEEE 24765:2017 [B43].

hazard identification: The process of recognizing that a hazard exists and defining its characteristics.

NOTE—See ISO/IEC/IEEE 24765:2017 [B43].

independent Verification and Validation (IV&V): Verification and Validation (V&V) performed by an organization that is technically, managerially, and financially independent of the development organization.

NOTE 1—See Annex C for a description of the degrees of independence for V&V.

NOTE 2—See ISO/IEC/IEEE 24765:2017 [B43].

information item: Separately identifiable body of information that is produced, stored, and delivered for human use.

NOTE 1—An information item can be produced in several versions during a project or system life cycle.

NOTE 2—See ISO/IEC/IEEE 15289:2019 [B42].

integration testing: Testing in which software components, hardware components, or both are combined and tested to evaluate the interaction between them.

NOTE—See ISO/IEC/IEEE 24765:2017 [B43].

integrity level: A value representing project-unique characteristics (e.g., complexity, criticality, risk, safety, security, desired performance, and reliability) that define the importance of the system, software, or hardware to the user.

interface design document (IDD): Documentation that describes the architecture and design interfaces between the system and components. These descriptions include control algorithms, protocols, data contents and formats, and performance.

NOTE—See ISO/IEC/IEEE 24765:2017 [B43].

interface requirements specification (IRS): Documentation that specifies the requirements for the interfaces between systems and components. These requirements include constraints on formats and timing.

NOTE—See ISO/IEC/IEEE 24765:2017 [B43].

life cycle processes: A set of interrelated or interacting activities that result in the development or assessment of system, software, or hardware products. Each activity consists of tasks. The life cycle processes may overlap one another. For Verification and Validation (V&V) purposes, no life cycle process is concluded until its development products are verified and validated according to the defined tasks in the Verification and Validation plan (VVP).

NOTE—See ISO/IEC/IEEE 24765:2017 [\[B43\]](#).

machine learning (ML): Process of optimizing model parameters through computational techniques, such that the model's behavior reflects the data or experience.

NOTE— See ISO 22989-2021 [\[B38\]](#)

microcode: A collection of microinstructions, comprising part of, all of, or a set of microprograms.

NOTE—See ISO/IEC/IEEE 24765:2017 [\[B43\]](#).

microprogram: A sequence of instructions, called microinstructions, specifying the basic operations needed to carry out a machine language instruction.

NOTE—See ISO/IEC/IEEE 24765:2017 [\[B43\]](#).

minimum tasks: Verification and Validation (V&V) tasks required by the integrity level assigned to the system, software, or hardware to be verified and validated.

nth of a kind component/system: A re-manufacturing or re-installation of a previously verified and validated hardware and/or software design. The nth of a kind component/system is equivalent to the first application in all relevant aspects, including functional and performance requirements, design documentation, environment, and regulatory constraints.

NOTE—See Annex L for a discussion of Verification and Validation (V&V) of nth of a kind systems.

optional tasks: Verification and Validation (V&V) tasks that may be added to the minimum required V&V tasks to address specific application requirements.

qualification testing: Testing conducted on a hardware element, software element or system to evaluate conformance with specified requirements.

required inputs: The set of items necessary to perform the minimum Verification and Validation (V&V) tasks mandated within any life cycle activity.

required outputs: The set of items produced as a result of performing the minimum Verification and Validation (V&V) tasks mandated within any life cycle activity.

reusable product: A system, software, or hardware product developed for one use but having other uses, or one developed specifically to be usable on multiple projects or in multiple roles on one project. Examples include, but are not limited to, commercial off-the-shelf (COTS) software products, acquirer-furnished software products, software products in reuse libraries, and preexisting developer software products. Each use may include all or part of the software product and may involve its modification. This term can be applied to any software product (for example, requirements, or architectures), not just to software itself.

NOTE—See ISO/IEC/IEEE 24765:2017 [\[B43\]](#).

risk: (A) The combination of the likelihood of occurrence and the consequences of a given future undesirable event. Risk can be associated with products and/or projects. **(B)** The combination of the likelihood of an abnormal event or failure and the consequence(s) of that event or failure to a system's components, operators, users, or environment.

NOTE—See ISO/IEC 16085-2006 [\[B37\]](#). ISO/IEC 16085 Systems and software engineering—Life cycle processes—Risk management provides examples of risk categories, but does not provide a complete taxonomy. By its nature, V&V will typically identify risks that are technical, safety, or engineering, but may also identify other types, including legal, organizational, cost, or schedule risks.

security: (A) The protection of computer hardware or software from accidental or malicious access, use, modification, destruction, or disclosure. Security also pertains to personnel, data, communications, and the physical protection of computer installations. (B) The protection of information and data so that unauthorized persons or systems cannot read or modify them, and authorized persons or systems are not denied access to them.

NOTE—See ISO/IEC/IEEE 24765:2017 [B43].

software as a service (SaaS): Access to resources from client devices through a thin client interface or program interface.

NOTE 1—The level of control over the resource provided to the consumer can vary with the service provider. In DevOps, SaaS can be automated as part of the DevOps pipeline.

NOTE 2—See IEEE Standards Dictionary Online [B16].

software design description (SDD): A representation of software created to facilitate analysis, planning, implementation, and decision-making. The software design description is used as a medium for communicating software design information and may be thought of as a blueprint or model of the system.

NOTE—See ISO/IEC/IEEE 24765:2017 [B43].

software requirements specification (SRS): Documentation of the essential requirements (functions, performance, design constraints, and attributes) of the software and its external interfaces.

NOTE—See ISO/IEC/IEEE 24765:2017 [B43].

system of interest: System whose life cycle is under consideration in the application of one instance of this Verification and Validation (V&V) standard.

NOTE—See ISO/IEC/IEEE 15288:2023(E) [B41].

test case: (A) A set of test inputs, execution conditions, and expected results developed for a particular objective, such as to exercise a particular program path or to verify compliance with a specific requirement. (B) Documentation specifying inputs, predicted results, and a set of execution conditions for a test item.

NOTE—See ISO/IEC/IEEE 24765:2017 [B43].

test design: Documentation specifying the details of the test approach for a system, software, or hardware feature or combination of features and identifying the associated tests.

NOTE—See ISO/IEC/IEEE 24765:2017 [B43].

test plan: (A) A document describing the scope, approach, resources, and schedule of intended test activities. It identifies test items, the features to be tested, the testing tasks, who will do each task, and any risks requiring contingency planning. (B) A document that describes the technical and management approach to be followed for testing a system or component. Typical contents identify the items to be tested, tasks to be performed, responsibilities, schedules, and required resources for the testing activity.

NOTE—See ISO/IEC/IEEE 24765:2017 [B43].

test procedure: (A) Detailed instructions for the setup, execution, and evaluation of results for a given test case. (B) A document containing a set of associated instructions as in (A). (C) Documentation that specifies a sequence of actions for the execution of a test.

NOTE—See IEEE Std 982.1™-2005 [B18].

Validation: (A) The process of providing evidence that the system, software, or hardware and its associated products satisfy requirements allocated to it at the end of each life cycle activity, solve the right problem (e.g., correctly model physical laws, implement business rules, and use the proper system assumptions), and satisfy intended use and user needs. **(B)** confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled

NOTE—For (B), see ISO/IEC/IEEE 24765:2017 [B43].

Verification: (A) The process of evaluating a system or component to determine whether the products of a given development phase satisfy the conditions imposed at the start of that phase. **(B)** The process of providing objective evidence that the system, software, or hardware and its associated products conform to requirements (e.g., for correctness, completeness, consistency, and accuracy) for all life cycle activities during each life cycle process (acquisition, supply, development, operation, and maintenance); satisfy standards, practices, and conventions during life cycle processes; and successfully complete each life cycle activity and satisfy all the criteria for initiating succeeding life cycle activities. Verification of interim work products is essential for proper understanding and assessment of the life cycle phase product(s).

NOTE—For (A), see ISO/IEC/IEEE 24765:2017 [B38].

Verification and Validation (V&V) effort: The work associated with performing the V&V processes, activities, and tasks.

3.2 Acronyms

The following acronyms appear in this standard:

AI	artificial intelligence
AIS	artificial intelligence system
ATWS	anticipated transient without scram
AUC	area under the curve
BWR	boiling water reactor
CCTV	closed-circuit television
COOP	continuity of operations plan
COTS	commercial off-the-shelf
CPU	central processing unit
CRC	cyclic redundancy check
CSAS	containment spray actuation signal
DCS	digital computer system
DRP	disaster recovery plan
ECCS	emergency core cooling systems
ECFS	electronic contract filing system
EMC	electromagnetic compatibility
EMI/RFI	electromagnetic interference/radio frequency interference
ESF	engineered safety features
FEDRAMP	Federal Risk and Authorization Management Program
FMEA	failure modes and effects analysis
FNR	false negative rate
FPDS	Federal Procurement Data System
FPGA	field programmable gate array
FPR	false positive rate
GAN	generative adversarial networks
GOTS	government off-the-shelf
GPS	global positioning system
HAZOPS	hazards and operability studies
HILS	hardware in the loop simulation

HRS	hardware requirements specification
HW	hardware
I&C	instrumentation and control
IAEA	International Atomic Energy Agency
IDD	interface design document
I/O	input/output
IRS	interface requirements specification
IT	information technology
IV&V	independent Verification and Validation
LCL	local coincidence logic
LOCA	loss of coolant accident
ML	machine learning
MR	metamorphic relation
MVP	minimum viable product
NPP	nuclear power plant
N/R	not required
NVR	network video recorder
OCD	operational concept document
PIA	privacy impact assessment
PII	personally identifiable information
PLC	programmable logic controller
PRNM	power range neutron monitor
PWR	pressurized water reactor
QA	quality assurance
RC	radio control
RCS	reactor coolant system
RFP	request for proposal (tender)
ROC	receiver operating characteristic
RPS	reactor protection system
SaaS	software as a service
SDD	software design description
SILS	software in the loop simulation
SIS	safety injection signal
SRS	software requirements specification
SSE	subsystem element
SW	software
TNR	true negative rate
TPR	true positive rate
TRA	threat and risk assessment
UAT	user acceptance testing
VMS	video management software
VVP	Verification and Validation plan
V&V	Verification and Validation
WBS	work breakdown structure
XAI	explainable artificial intelligence

4. Relationships between V&V and life cycle processes

This standard is structured to enable a V&V practitioner to use [Clause 7](#) (common V&V) and any of [Clause 8](#) (system V&V), [Clause 9](#) (software V&V), or [Clause 10](#) (hardware V&V) in performing V&V for a particular product. V&V on a system is performed using [Clause 7](#) and [Clause 8](#) (common and system), on software using [Clause 7](#) and [Clause 9](#) (common and software), and on hardware using [Clause 7](#) and [Clause 10](#) (common and hardware).

Most systems consist of more than a single hardware or a single software element. A depiction of a more complex system with subsystems and system elements (i.e., software or hardware, shown as shaded boxes) is shown in [Figure 4](#). The system life cycle processes are applied recursively from the system of interest to the systems at the next level, with the recursion continuing until a system element is reached. For software system elements, the software life cycle processes are applied, and for hardware system elements, the hardware life cycle processes are applied. The life cycle processes at the system, software, or hardware levels may be conducted in parallel for systems or system elements at the same level. The full set of life cycle processes (system, software, or hardware, as appropriate) are applied to each product. In the same way, system V&V is applied recursively for each system of the system of interest, and software or hardware V&V is applied to each system element. For V&V purposes, no life cycle process is concluded until its development products are verified and validated according to the defined tasks in the VVP (see [Clause 12](#)).

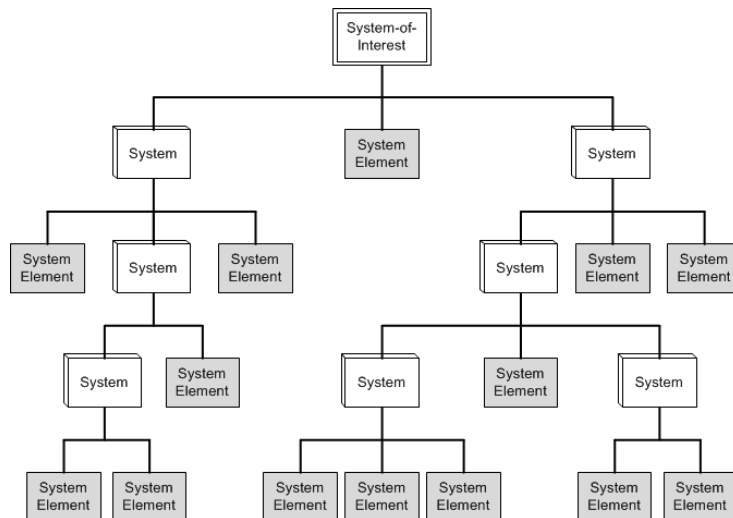
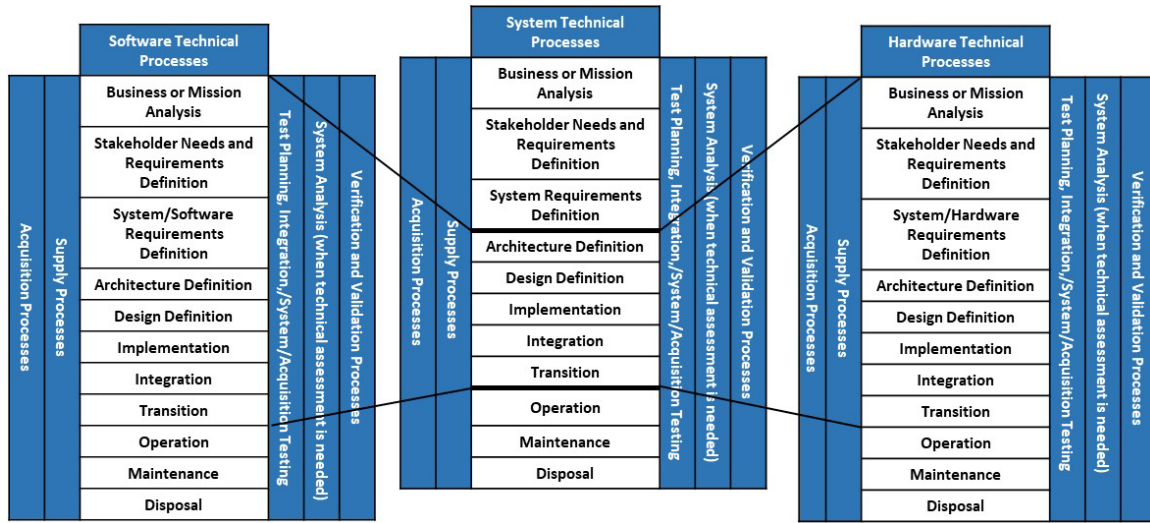


Figure 4—Example system-of-interest structure

The Verification Process and the Validation Process are two processes within the technical processes group of the system life cycle processes defined in ISO/IEC/IEEE 15288:2023(E) [B41]. System V&V, as described in this V&V standard, is a conforming instance of the V&V processes in ISO/IEC/IEEE 15288:2023(E) [B41] (i.e., conducting system V&V as described in this V&V standard enables the V&V practitioner to claim full conformance with those two system life cycle processes, although other approaches may also be in conformance). In a similar fashion, software V&V as described in this V&V standard is a conforming instance of the V&V processes within the technical processes group of the life cycle processes defined in ISO/IEC/IEEE 12207:2017(E) [B40].

The purpose of the system Implementation Process is to produce a specified system element implemented as a software and hardware product or service. Within the system Implementation Process, each software and hardware element is developed using the full software or hardware life cycle (requirements, design, implementation/construction, integration, and test). This concept is reflected in [Figure 5](#), which also illustrates that the Technical Processes for software and hardware overlap with the System Architecture Definition, Design Definition, System Analysis, Integration, and Transition processes. At the system element level, the implementation will be realized by the Implementation Process (described in [Clause 9](#)) or the Implementation process (described in [Clause 10](#)).



NOTE 1—The layout of the processes is not intended to specify an ordering of processes. V&V activities may be applied to any life cycle process.

NOTE 2—Management of V&V activity is concurrent with all V&V activities.

NOTE 3—The task description, inputs, and outputs of all V&V tasks are included in [Table 1a](#) through [Table 1d](#).

Figure 5—Relationship of system, software, and hardware processes

Not all life cycle processes from ISO/IEC/IEEE 15288:2023(E) [\[B41\]](#) and ISO/IEC/IEEE 12207:2017(E) [\[B40\]](#) have V&V tasks specified in this standard. Each Technical process has a corresponding V&V process, as do the Acquisition, Supply, Project Planning, and Configuration Management processes. The V&V processes also interact with the other system and software processes not included in this table, such as providing inputs and receiving outputs used in the V&V effort.

Each ISO/IEC/IEEE 12207 software-specific process is a specialization of its corresponding process in ISO/IEC/IEEE 15288:2023(E) [\[B41\]](#). Users may consider claiming conformance to the ISO/IEC/IEEE 15288 process rather than the ISO/IEC/IEEE 12207 process.

Each hardware process corresponding to an ISO/IEC/IEEE 12207 software-specific process is a specialization of its related process in ISO/IEC/IEEE 15288.

The life cycle model, including selected processes, defines the evolution of the system, software, and hardware elements throughout the life cycle stages. To achieve the outcomes of the V&V processes for each of the other life cycle process, this standard is organized by life cycle process, and within each life cycle process, the V&V activities and tasks for that life cycle process are identified. [Figure 6](#) illustrates that organization for system life cycle processes. The listing of all V&V activities and tasks to specific system, software, or hardware life cycle processes are depicted in [Figure 1a](#), [Figure 1b](#), [Figure 1c](#), and [Figure 1d](#).

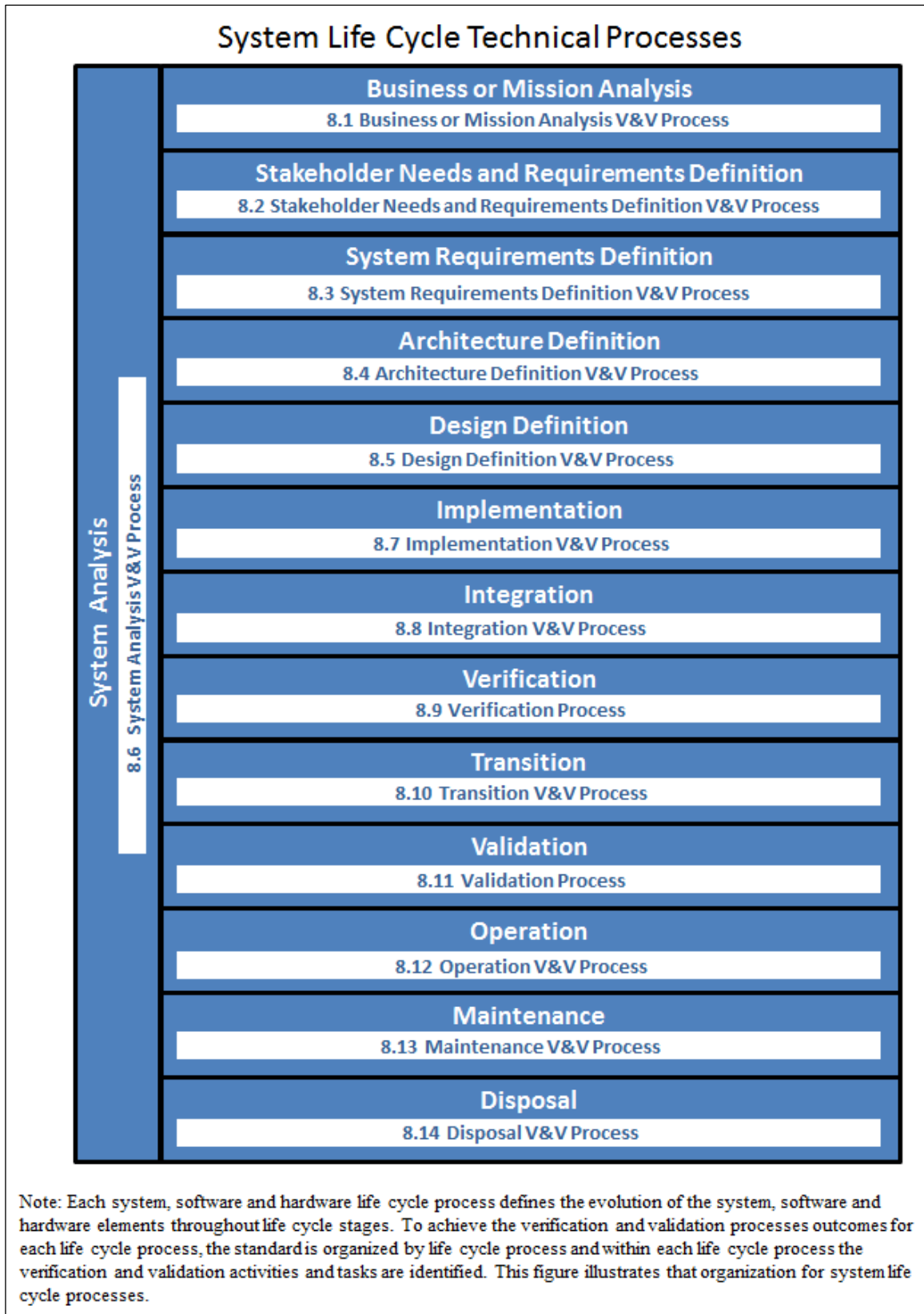


Figure 6—V&V processes align with other technical life cycle processes

5. Integrity levels

Integrity level determination establishes the importance of the system to the user and acquirer based on complexity, criticality, risk, safety, security, desired performance, reliability, or other system-unique characteristics. Integrity levels are used to determine the V&V tasks, activities, rigor, and the level of intensity of the V&V to be performed.

The following is a result of the integrity level determination:

- a) An integrity schema is defined.
- b) Integrity levels for all system elements are assigned.
- c) Integrity assignments are used to determine V&V activities and tasks using [Table 2a](#) through [Table 2d](#).
- d) A basis is established to review and revalidate the integrity levels throughout the V&V effort.

The degree of rigor and intensity in performing and documenting any V&V task associated with a system, software, or hardware work product shall be commensurate with the integrity level. As the integrity level decreases, so does the required scope, intensity, and degree of rigor associated with the V&V task. For example, system integration testing for integrity level 4 systems must be performed independently by the V&V organization, whereas for an integrity level 3 system, the V&V organization need only review the results from systems integration testing.

Use the integrity schema established for the system, software, or hardware, if one exists. An integrity level schema shall be specified if one is not already defined. Establish gradations of criticality or integrity to assure complete coverage of the risk classes from possible system behaviors from no risk to worst-case risk. The integrity levels established for a system element by the developer should result from agreements between the acquirer and the supplier and remain consistent with regulatory requirements.

This standard was developed with a four-level schema to explain the minimum normative V&V requirements. Other integrity schemas are acceptable. For any selected integrity schema, the selected integrity levels shall be mapped into this standard's four-level schema (and associated V&V criteria) to demonstrate that the minimum V&V requirements are satisfied. Because V&V is applied recursively from the system of interest down to each of the subsystems or elements at the next level, it is not necessary to use the same integrity level schema for all the subsystems or elements of the system of interest.

NOTE—A process for developing an integrity schema can be found in ISO/IEC 15026-3:2013 [\[B33\]](#).

The V&V criticality analysis task is used to classify the integrity level of every system (e.g., subsystem) or element in the system of interest. Integrity levels are assigned to requirements, functions, groups of functions, components, or subsystems. The integrity levels characterize and quantify the potential for undesirable effects and consequences resulting from integrity lapse, unintended effects, failure mode effects, and unverified performance effects. The characteristics that determine integrity level vary depending on the intended application and use of the system.

Integrity level assignments shall be applied recursively to the components of each system element. As the development stages progressively decompose the solution into more detail, the criticality analysis performed at each development stage assigns integrity levels to each function. By recursively assigning integrity levels to individual solution parts, greater rigor and intensity are applied to the higher integrity level elements. Progressive decomposition for criticality analysis and assignment of integrity levels shall be applied to segregate parts that warrant high-integrity V&V tasks from those parts that do not. This recursive assignment of integrity levels to solution parts keeps the V&V effort focused on the high-integrity elements, making the V&V effort cost-efficient and technically effective.

From the system perspective, during integrity level analysis, software and hardware are treated as functional elements. Subsystem components cannot have a higher criticality or integrity level than the parent subsystem. The system shall be assigned the same integrity level as the highest level assigned to any individual element.

The integrity level assigned to the parent shall be as high as the highest integrity level of the system elements. The system elements can have the integrity level of the system parent or lower, depending on the critical functions they support.

The integrity level assigned to reused, COTS, and government off-the-shelf (GOTS) components shall be in accordance with the integrity level schema adopted for the system element into which COTS or GOTS may be integrated for the project. The reused COTS or GOTS component shall be evaluated for use in the context of its application. The design, development, procedural, and technology features implemented in the system can raise or lower the assigned integrity levels.

The V&V criticality analysis task is used to classify the integrity level of enabling systems. Examples of enabling systems include tools that insert or translate code (e.g., optimizing compilers and auto-code generators). All enabling systems shall be assigned the same integrity level as the integrity level assigned to the software element that the tool affects. If the tool cannot be verified and validated, then the tool's output shall be subject to the same level of V&V as the software element.

The mapping of the integrity level schema and the associated minimum V&V tasks shall be documented in the VVP. The basis for assigning integrity levels to components shall be documented in a V&V task report and V&V final report. [Table 2a](#) through [Table 2d](#) of this standard identify the necessary and sufficient V&V activities and tasks to perform for each integrity level. Once the integrity levels have been determined, [Table 2a](#) through [Table 2d](#) are used to identify the activities and tasks to adapt and plan the V&V effort. High integrity requires a larger set of V&V processes and a more rigorous application of V&V tasks. The V&V processes should be tailored to specific system elements with a combination of the minimum V&V tasks and addition of optional V&V tasks.

The addition of optional V&V tasks allows the V&V effort to address application-specific characteristics. [Table 3a](#) through [Table 3d](#) provide a list of optional V&V tasks and their suggested applications in the life cycle of the system of interest. These optional V&V tasks may be added to the minimum V&V tasks, as necessary, to tailor the V&V effort to project needs to provide additional assurance and confidence in the operational use of the system.

The integrity level assignment shall be continually reviewed and updated by conducting the V&V criticality analysis task throughout the life cycle. Changes to assignments shall be used to reassess the V&V plan and performance for appropriate integrity assurance throughout the life cycle. If the integrity level of any component is revised, the effect of the revision on existing requirements shall be evaluated to identify additional activities and tasks to be performed on the system, software, and hardware. This includes adopting V&V tasks for the revised component integrity level and performing those V&V tasks for previous life cycle stages.

Critical functions are assigned a high system integrity level at the initiation of the project and shall not be lowered at any stage of the development process unless authorized by the system acquirer or governing regulatory organization. Other system functions may be assigned lower system integrity levels than the critical functions at the beginning stages. However, if any lower system integrity level functions can modify or alter critical data or can create an improper condition or system state to exist causing critical system functions to take incorrect actions, then those lower system functions shall be elevated to critical system integrity levels for V&V analysis and test. For discussion purposes, these system functions shall be designated "critical supporting system functions."

During the evolution of the system through requirements, design, implementation, and integration, the selection of technology or design/implementation techniques could mitigate or eliminate the impact that a "critical supporting system function" may have on critical system functions. In such cases and only with extreme care, the integrity level for a "critical supporting system function" may be lowered for V&V analysis and test purposes. In contrast, there may be means to obtain a higher integrity level by a combination of components having lower integrity levels (e.g., duplication or redundancy—see ISO/IEC 15026-3:2013 [\[B33\]](#)).

Annex K describes an example of how system integrity levels are assigned to “supporting system functions” and how system integrity levels may be changed during the system development stages for the “supporting system functions” as a result of the selection of design/implementation techniques.

6. Overview of V&V processes

6.1 General

V&V processes have activities and tasks defined for the processes in the Agreement processes and Technical processes group, the Project Planning Process, and the Configuration Management Process of ISO/IEC/IEEE 15288:2023(E) [B41]. V&V processes have activities and tasks defined for the processes in the Software Implementation Processes group and for the software Configuration Management Process of ISO/IEC/IEEE 12207:2017(E) [B40]. Although there is no corresponding IEEE standard that addresses the hardware life cycle, V&V activities and tasks are defined for processes analogous to those for the software life cycle. The minimum V&V activities and tasks supporting these processes are referenced in the following clauses and are defined in [Table 1a](#) through [Table 1d](#) of each part of this standard. The subclause titles in this clause are the same as the column headings in [Table 1a](#) through [Table 1d](#) to correlate the requirements of the following subclauses with [Table 1a](#) through [Table 1d](#) tasks. Not all projects include each of the life cycle processes listed. To conform to this standard, the V&V processes shall address all those life cycle processes used by the project.

V&V activities that are common across system, software, and hardware are in [Clause 7](#). These include the V&V Management activity, which is not specifically described by ISO/IEC/IEEE 15288:2023(E) [B41] or ISO/IEC/IEEE 12207:2017(E) [B40] but is essential to the implementation of V&V tasks. Other common V&V activities in [Clause 7](#) are associated with the Acquisition Process, the Supply Process, the Project Planning Process, and the Configuration Management Process.

V&V activities that are associated with system life cycle processes are in [Clause 8](#) (System V&V). The system processes are those in the technical processes group of ISO/IEC/IEEE 15288:2023(E) [B41].

V&V activities that are associated with software life cycle processes are in [Clause 9](#) (Software V&V). The software processes are those in the technical processes group of ISO/IEC/IEEE 12207:2017(E) [B40].

V&V activities that are associated with hardware life cycle processes are in [Clause 10](#) (Hardware V&V). The hardware processes are based on the technical processes group of ISO/IEC/IEEE 12207:2017(E) [B40].

The V&V effort shall conform to the task descriptions, inputs, and outputs as described in [Table 1a](#) through [Table 1d](#). The V&V effort shall include the minimum V&V tasks specified in [Table 2a](#) through [Table 2d](#) for the assigned integrity levels. If the user of this standard has selected a different integrity level schema, then this standard’s integrity level schema and associated minimum V&V tasks of [Table 2a](#) through [Table 2d](#) shall be mapped to their selected integrity level schema.

Optional V&V tasks may also be performed to augment the V&V effort to satisfy project needs. Optional V&V tasks are listed in [Table 3a](#) through [Table 3d](#) and described in [Annex G](#). The list in [Table 3a](#) through [Table 3d](#) is illustrative and not exhaustive.

Some V&V activities and tasks include analysis, evaluations, and tests that may be performed by multiple organizations (e.g., development, project management, quality assurance, and V&V). For example, risk analysis and hazard analysis may be performed by project management, the development organization, and the V&V effort. The V&V effort performs or uses the outputs from these tasks from other sources to develop the supporting basis of evidence showing whether the product satisfies its requirements and to mitigate risks to the project. These V&V analyses are complementary to other analyses and do not eliminate or replace the analyses performed by other organizations. The degree to which these analysis efforts will be coordinated with other organizations shall be documented in the organizational responsibility section of the VVP.

6.2 V&V team characteristics

This standard does not require that V&V be performed by any specific organization and even allows V&V activities to be performed by multiple organizations. However, V&V is often conducted by a well-defined organization, and even when not, the collection of individuals performing V&V activities may be considered to be a team. The term “V&V team” is used in this context.

The V&V team, as a combined group, should have the technical knowledge and expertise to enable the assessment of the system to the rigor and depth indicated by the integrity level of the system. In general, the team should have knowledge and expertise in the following:

- Domain of the system of interest
- Systems engineering
- V&V
- System perspective

The expertise of the team should include not only the engineering of the system itself, but also the overall environment in which the system is intended to operate: general business or mission area, functions and interactions with interfacing systems, support systems, physical environment, and regulatory constraints.

The V&V team needs systems engineering knowledge and expertise to enable assessment of the system's work products, system elements (e.g., software, hardware), interactions among the system elements, and interfaces with other systems and the environment. In this context, systems engineering includes requirements engineering, software engineering, hardware engineering, and systems, software and hardware architecture, design, implementation, and testing.

In addition, the V&V team needs to understand the V&V processes and corresponding life cycle processes (see ISO/IEC/IEEE 15288:2023(E) [\[B41\]](#) and ISO/IEC/IEEE 12207:2017(E) [\[B40\]](#)) and the tasks and activities that will be conducted during the V&V effort. This includes V&V planning, V&V management, and interfaces with other stakeholders. The V&V team, and particularly V&V team management, needs to be able to communicate information about the V&V results and about discrepancies discovered during the V&V effort, understanding that different stakeholders need different levels and methods of communication.

In addition to the technical knowledge and expertise regarding the domain of the system of interest, systems engineering, and V&V, the V&V team needs a perspective that allows an understanding of the complete system and an ability to conceptualize how the proposed system might behave in varied circumstances. While performing V&V tasks, the team will need to consider alternatives (e.g., think outside the box, conceive of missing conditions or actions, alternate or abnormal scenarios), perceive relationships and correlations (especially those not explicitly defined), and have a holistic view of the system.

While not each member of the V&V team has to have this complete body of knowledge, the team as a whole should have expertise and knowledge in all these areas. The team may include a mixture of experience, with more senior members giving guidance to more junior members. In the case of cutting-edge technologies, the V&V team might not start with a strong understanding of some of these aspects, since the technologies are still being developed. In this case, a deliberate effort should be conducted to gain expertise in the new technologies to enable assessment of the work products.

Some members of the V&V team may have specific expertise that is utilized only sporadically during the life cycle, and they will engage in the V&V effort at specific times during the life cycle. However, it is best if some members of the V&V team are engaged throughout the life cycle in order to form an understanding of the full system, its elements and their interactions, and the interactions of the system with its environment. As the V&V effort evolves, the members of the team will develop detailed system knowledge and expertise.

Other skills, such as the ability to communicate within the V&V team and with developers, development management, and the customer, are also important. Communication should be tailored to each recipient, and

should be based on factual findings from V&V tasks and directed at successful development of the system. The V&V team should display high ethical standards in both the performance of V&V tasks and in communication with all parties.

6.3 V&V testing

Testing is an activity that may be performed by various organizations within the development effort. This standard requires a minimum level of V&V testing dependent on the integrity level, as reflected in [Table 1a](#) (common V&V activities and tasks), [Table 1b](#) (system V&V activities and tasks), [Table 1c](#) (software V&V activities and tasks), and [Table 1d](#) (hardware V&V activities and tasks). [Figure 7](#) summarizes the minimum level for V&V testing for the types of testing and integrity level. The term perform means that the V&V effort specifies and creates its testing products (i.e., test plan, test design, test cases, and test procedures) and either conducts that testing or analyzes the results of that testing if it is conducted by another organization. The term review means that the V&V effort reviews the testing plans and analyzes the results of tests.

Software	V&V testing by integrity level			
	4	3	2	1
Software component testing V&V	Perform	Perform	Review	No action
Software integration testing V&V	Perform	Perform	Review	No action
Software qualification testing V&V	Perform	Perform	Review	No action
Software acceptance testing V&V	Perform	Perform	Review	No action

Hardware	V&V testing by integrity level			
	4	3	2	1
Hardware component testing V&V	Review	Review	Review	No action
Hardware integration testing V&V	Review	Review	Review	No action
Hardware qualification testing V&V	Perform	Perform	Review	No action
Hardware acceptance testing V&V	Perform	Perform	Review	No action

System	V&V testing by integrity level			
	4	3	2	1
System integration testing V&V	Perform	Review	Review	No action
System qualification testing V&V	Perform	Review	Review	No action
System acceptance testing V&V	Perform	Review	Review	No action

NOTE 1—The requirement to “perform” testing means that the V&V effort creates its testing criteria, confirms that the testing is conducted appropriately, and reviews the results. The term allows but does not require that the V&V effort conducts tests if the identical V&V criteria are already specified in other testing. Alternatives to conducting tests include methods such as witnessing a test conducted by the supplier or developer.

Having the V&V effort “perform” its own testing increases the detection of system/software/hardware errors, especially for high integrity levels, because V&V testing can provide the following benefits:

- Examines the stress, abnormal, and fault recovery scenarios that development testing often does not have sufficient time for such test case scenarios.
- Creates additional testing coverage of the system/software/hardware from the V&V perspective of how the system should perform with inputs and stimuli different from the development test scenarios such that those different inputs/stimuli may expose errors undetected in development test scenarios.

NOTE 2—For V&V testing, it is ideal for the V&V processes to have their own test drivers, test simulations, test models, and system test facility. It is not the intended purpose for V&V processes to repeat or duplicate the same or similar testing as accomplished by the development processes. Rather, V&V testing provides objective evidence that the high integrity level requirements perform as intended under all operational scenarios, including stress and abnormal conditions, error recovery situations, and high-risk hazardous situations. Having a separate V&V test capability allows for development testing to be uninterrupted (not shared); permits special test scenarios, error injection, and test monitoring capability to be integrated into the test facility; and provides for an independent test capability to investigate erroneous and unusual scenarios without interference with the development test schedule.

However, because of budgetary considerations, the development testing and V&V testing often share the same system test capabilities (e.g., resources or facilities). When sharing the same test capabilities with the development testing, the V&V effort shall establish the following procedures on common facility usage to maintain the integrity of both the V&V and development test processes:

- Maintain a controlled copy of system and hardware settings and software elements used in the test facility, such as test drivers, test simulations, interface drivers, and software items that are being tested and undergoing V&V; (These configured items and descriptions are required to allow V&V testing to set the test facility to a known state before beginning V&V testing since items could have been changed during the development testing period.)
- Initialize the test facility to the V&V test configuration at the start of V&V testing; (The test facility configuration may be restored to the prior test configuration at the conclusion of V&V testing.)
- Use V&V test procedures and V&V-provided system test database configurations and scenarios.
- Monitor and record the V&V test processes and results (although V&V testing may share the test facility operators used by development testing).

The V&V effort generates the input data and interfacing data inputs in accordance with the V&V test cases/procedures. The objectives of V&V testing are to identify the system/software/hardware element errors. Often, the small differences in test data and interface data inputs may cause the error source(s) to be evident. Testing system/software/hardware during key system transition states and at all boundary conditions is a method of exercising the key requirements of the system. Satisfactory V&V testing results and the absence of major errors constitute the objective evidence for verifying and validating the system.

NOTE 3—Hardware integration takes place at many levels. For electronics, this can range from the chip level and board level to a fully integrated computer system that can be integrated into a larger computer network. For a mechanical system, the levels of integration can range from a nut-and-bolt assembly to a complex multi-degree-of-freedom system. At the lowest level of integration, the issues are so elemental or the integration processes so standardized and well understood that V&V of the integration may not be required or applicable. In some cases, as in the assembly of a circuit board, the V&V activities may be carried out by the manufacturer during the integration of the assembled product.

Figure 7—Minimum level for V&V testing by integrity level

[Annex A](#) describes V&V testing concepts and methodology to verify and validate the system/software component(s) for correctness, completeness, safety, security, and accuracy of the entire system/software performance requirements through all phases of the operational environment. The V&V testing is complementary to the development testing rather than duplicative or redundant. The annex describes the variety of different testing strategies that can be used by V&V testing to expose any errors or deficiencies as the system/software evolves through the development life cycle. The V&V testing methodology begins early in a system/software life cycle where the first test planning strategies (e.g., test plan, test scenarios, test design, and test cases) are formulated by the analytic V&V tasks performed in life cycle stages, as early as system requirements definition. Often system/software errors or incomplete solutions are discovered during analysis of test strategies across all operating conditions, which may reveal a deficiency or incompleteness pertaining to the requirements or design solution. By testing against stress and boundary conditions and conducting a comprehensive testing strategy of attempting to surface errors or deficiencies across the full performance spectrum of conditions, the V&V testing provides a comprehensive and supportive testing approach to development testing.

7. Common V&V processes

7.1 V&V Management Process

7.1.1 Purpose

The purpose of the V&V Management Process is to develop and maintain the V&V plan, determine the status of the V&V effort, and direct the V&V effort to perform according to plans and satisfy technical objectives.

7.1.2 Outcomes

The following outcomes occur as a result of the successful implementation of the V&V Management Process:

- a) The VVP is developed.
- b) The V&V effort is continuously reviewed.
- c) Revisions of the VVP are made as necessary based on updated project schedules, development status, or changes in the V&V approach.
- d) V&V results are coordinated with other parties performing life cycle activities.
- e) V&V task results are reviewed for conformance to task requirements.
- f) Recommendations are made to program management regarding readiness to proceed to the next stage of the project life cycle, acceptance, and certification.
- g) Process improvement opportunities in the conduct of V&V are identified.

NOTE—V&V management is focused on management activities unique to V&V. Other project management activities that are common across all projects, such as cost management and human resource management, are not addressed by this standard.

The V&V Management Process monitors and evaluates all V&V outputs. Management of the V&V effort is performed for all life cycle V&V processes and activities. All the V&V reporting, administrative, and documentation requirements are defined in [Clause 11](#). The outline and content of the VVP are described in [Clause 12](#).

V&V management assesses each proposed change to the system, software, or hardware; identifies the requirements that are affected by the change; and plans V&V tasks to address the change. For each proposed change, management assesses whether any new hazards or risks are introduced in the development process and identifies the impact of the change on the assigned integrity levels. V&V task planning is revised by adding new V&V tasks or changing the scope or intensity of existing V&V tasks if integrity levels, hazards, or risks are changed. A baseline change results from changes allocated to releases in an incremental development process (e.g., planned baseline versions).

Through the use of V&V measures and other qualitative and quantitative measures, program trend data and possible risk issues are developed and provided to the developer and acquirer to effect timely notification and resolution. At key program milestones (e.g., requirements review, design review, and test readiness), V&V management consolidates the V&V results to establish supporting evidence of whether to proceed to the next stage of the project life cycle. V&V management determines whether a V&V task should be repeated as a result of changes in the program.

7.1.3 Activity and tasks

The V&V effort shall perform, as specified in [Table 2a](#) for the selected integrity level, the following V&V management activity and tasks described in [Table 1a, Activity 7.1](#):

- a) [V&V Management](#). This activity consists of the following tasks:
 - 1) [VVP generation](#)
 - 2) [Interface with other processes](#)
 - 3) [Proposed/baseline change assessment](#)
 - 4) [Management review of the V&V effort](#)
 - 5) [Management and technical review support](#)
 - 6) [Identify process improvement opportunities in the conduct of V&V](#)
 - 7) [V&V final report generation](#)

7.2 Acquisition Support V&V Process

7.2.1 Purpose

The purpose of the Acquisition Support V&V Process is to provide assurance that the outcomes of the Acquisition Process (ISO/IEC/IEEE 15288:2023(E) [B41] or ISO/IEC/IEEE 12207:2018(E) [B40]) have been achieved.

7.2.2 Outcomes

The following outcomes occur as a result of the successful implementation of the Acquisition Support V&V Process:

- a) Interfaces are planned with the supplier and acquirer.
- b) System requirements to be included in the request for proposal (RFP) are reviewed.
- c) V&V task results are provided to support the acquirer's acceptance of the system.

7.2.3 Activity and tasks

The V&V effort shall perform, as specified in [Table 2a](#) for the selected integrity level, the following acquisition support V&V activity and tasks described in [Table 1a, Activity 7.2](#):

- a) [Acquisition support V&V](#). This activity consists of the following tasks:
 - 1) [Scoping the V&V effort](#)
 - 2) [Planning the interface between the V&V effort and supplier](#)
 - 3) [System requirements review](#)
 - 4) [Acceptance support](#)

Acquirer acceptance of the system of interest culminates after acceptance testing and installation. The V&V acquisition acceptance support activities occur throughout the life cycle, in conjunction with other interrelated development and V&V tasks, inputs, and outputs.

The acquisition support V&V activity addresses project initiation, RFP, contract preparation, supplier monitoring, and acceptance and completion.

For a system of interest that is determined to be an identical copy of a system that has been previously verified and validated, and the environment is also identical, then no further V&V tasks are needed beyond those to provide the body of evidence that the system and environment are identical. This copy of a system is often referred to as an “nth of a kind system.” See [Annex L](#) for a more detailed discussion.

7.3 Supply Planning V&V Process

7.3.1 Purpose

The purpose of the Supply Planning V&V Process is to provide assurance that the outcomes of the Supply Planning Process (ISO/IEC/IEEE 15288:2023(E) [B41] or ISO/IEC/IEEE 12207:2018(E) [B40]) have been achieved.

7.3.2 Outcomes

The following outcomes occur as a result of the successful implementation of the Supply Planning V&V Process:

- a) Interfaces are planned with the supplier and acquirer.
- b) RFP requirements and contract requirements are determined to be consistent and satisfy user needs before the contract is finalized.

7.3.3 Activity and tasks

The V&V effort shall perform, as specified in [Table 2a](#) for the selected integrity level, the following supply planning V&V activity and tasks described in [Table 1a, Activity 7.3](#):

- a) [Supply planning V&V](#). This activity consists of the following tasks:
 - 1) [Planning the interface between the V&V effort and supplier](#)
 - 2) [Contract Verification](#)

The supply planning V&V activity addresses the initiation, preparation of response, contract, planning, execution and control, review, and evaluation, as well as delivery and completion activities.

7.4 Project Planning V&V Process

7.4.1 Purpose

The purpose of the Project Planning V&V Process is to provide assurance that the project scope is complete and that all activities are defined.

7.4.2 Outcomes

As a result of the successful implementation of the Project Planning V&V Process, the VVP is coordinated with the project plan.

7.4.3 Activity and task

The V&V effort shall perform, as specified in [Table 2a](#) for the selected integrity level, the following Project Planning Process V&V activity and task described in [Table 1a, Activity 7.4](#):

- a) [Project planning V&V](#). This activity consists of the following task:
 - 1) [Project planning strategy assessment](#)

7.5 Configuration Management V&V Process

7.5.1 Purpose

The purpose of the Configuration Management V&V Process is to provide assurance that the Configuration Management Process (ISO/IEC/IEEE 15288:2023(E) [\[B41\]](#) or ISO/IEC/IEEE 12207:2018(E) [\[B40\]](#)) supports the V&V processes.

7.5.2 Outcomes

The following outcomes occur as a result of the successful implementation of the Configuration Management V&V Process:

- a) A configuration management strategy is defined for the program that will assure configuration controls are in place to maintain and document configuration item baselines with unique identifiers. The strategy should include notification to the V&V effort for all changes made to the configuration item baselines.
- b) Items requiring configuration management are defined and documented. The items controlled should include enabling the systems, tools, and processes that are integral to system development and life cycle support that will be subject to V&V to demonstrate conformance to this standard.
- c) The status of items under configuration management is made available throughout the life cycle. Provisions should be included to assure that the V&V effort receives the current status for all configuration items.

7.5.3 Activity and task

The V&V effort shall perform, as specified in [Table 2a](#) for the selected system integrity level, the following Configuration Management Process V&V activity and task described in [Table 1a, Activity 7.5](#):

- a) [Configuration management V&V](#): This activity consists of the following task:
 - 1) [Configuration management assessment](#)

If configuration management issues are discovered during the V&V effort that indicate configuration baselines are not established or controlled, or if the configuration of released items is not controlled, the issues shall be documented and provided to the system developer and to the V&V customer for resolution.

Table 1a—V&V tasks, inputs, and outputs

7.1 Activity: V&V management (common)		
V&V tasks	Required inputs	Required outputs
(1) VVP generation a) Generate a VVP (see Clause 12) for all life cycle processes. The VVP may require updating throughout the life cycle. Outputs of other activities are inputs to the VVP. b) Establish a baseline VVP prior to the requirements V&V activities. c) Identify project milestones in the VVP. d) Schedule V&V tasks to support project management reviews and technical reviews. NOTE—The required input of concept documentation includes statement of need, advance planning report, project initiation memo, feasibility studies, system requirements, governing regulations, procedures, policies, customer acceptance criteria and requirements, acquisition documentation, business rules, and draft system architecture	VVP (previous update) Contract Concept documentation Supplier development plans and schedules	VVP and updates
(2) Interface with other processes a) Coordinate the V&V effort with organizational project-enabling processes and project processes. b) Identify the V&V data to be exchanged with these processes. c) Document the data exchange requirements in the VVP.	VVP Data identified in the VVP from the organizational project-enabling processes and project processes	Updated VVP
(3) Proposed/baseline change assessment a) Evaluate proposed changes (i.e., modifications, enhancements, and additions as a result of anomaly corrections or requirement changes) for effects on the system and previously completed V&V tasks. b) Plan iteration of affected tasks or initiate new tasks to address proposed changes or baseline changes associated with an iterative development process. c) Verify and validate that changes are consistent with requirements and do not adversely affect requirements directly or indirectly. An adverse effect is a change that could create new system hazards and risks or impact previously resolved hazards and risks.	VVP Proposed changes Hazard analysis results Risks identified by V&V tasks Supplier development plans and schedules Developer products (produced to date)	Task report(s)—Proposed/baseline change assessment Updated VVP Anomaly report(s)
(4) Management review of the V&V effort a) Review and summarize the V&V effort to define changes to V&V tasks or to redirect the V&V effort. b) Evaluate each anomaly for its criticality (e.g., IEEE Std 1044™-2009 [B21]). Assess anomalies and risks for trends and tendencies. The scope and application of V&V activities and tasks shall be revised to address the causes of these anomalies and risks. c) Recommend whether to proceed to the next stage of the project life cycle and provide task reports, anomaly reports, and V&V activity summary reports to the organizations identified in the VVP. d) Verify that all V&V tasks conform to task requirements defined in the VVP.	VVP and updates Supplier development plans and schedules Anomaly reports V&V task results [e.g., technical accomplishments, V&V reports, resource utilization, V&V measures (see Annex E), plans, and identified risks]	Task report(s)—Recommendations Updated VVP V&V activity summary reports Recommendations to the V&V final report

e) Verify that V&V task results have a basis of evidence supporting the results. f) Assess all V&V results and provide recommendations for program acceptance and certification as input to the V&V final report. g) Use the results of the review to identify process improvement opportunities in the conduct of V&V. h) Review the quality of the products and services to assure they meet customer requirements. i) Review the program risks and initiate actions to mitigate risks that exceed thresholds. j) Review program measures (e.g., V&V measures, test results, anomaly reports, timing, and capacity results) to assure the quality of products and processes. NOTE—For additional information and guidance on review methods, see IEEE Std 1028-2008 [B20].		
(5) <u>Management and technical review support</u> a) Support project management reviews and provide V&V results at project-defined technical reviews (e.g., preliminary design review and critical design review) by assessing the review materials, attending the reviews, and providing task reports and anomaly reports. Provide objective evidence on the status of development products (system, software, hardware) to project management authorities, including recommendations and assessment of positive trends and anomaly trends. This evidence can be used to determine whether the criteria of major program milestones have been achieved and whether to proceed to the next stage of the project life cycle. Provide an assessment of the positive trends and anomaly trends to allow greater focus toward the functional program requirements warranting more resources and additional analysis support or to require changes in V&V resources or tasks. b) Verify timely delivery according to the approved schedule of all products and documents.	V&V task results Materials for review (e.g., operational concept document [OCD], architectural and design documents, system requirements, SRS, IRS, SDD, IDD, and test documents)	Task report(s)— Review results Anomaly report(s)
(6) <u>Identify process improvement opportunities in the conduct of V&V</u> a) Gather and analyze the lessons learned. b) Gather and analyze the risks identified. c) Gather and analyze the V&V measures. d) Identify and analyze deficiencies in the V&V processes. e) Determine and implement corrective actions using best practices (e.g., repeat V&V tasks, conduct a new V&V task to address corrective actions, or use a different method/technique for executing a V&V task). f) Monitor the efficacy of the corrective actions.	V&V task results materials for review (e.g., OCD, architectural and design documents, system requirements, SRS, IRS, SDD, IDD, and test documents)	Task report(s)— Review results Anomaly report(s)
(7) <u>V&V final report generation</u> a) Summarize in the V&V final report the V&V activities, tasks, and results, including status and disposition of anomalies. b) Provide an assessment of the overall quality and provide recommendations. c) Document V&V process improvement opportunities.	V&V activity summary report(s)	Task report(s)—V&V final report

NOTE—The V&V final report is intended to be produced at the completion of V&V following development, operations, maintenance, or retirement.		
7.2 Activity: Acquisition support V&V (common, 15288—Acquisition Process)		
V&V tasks	Required inputs	Required outputs
(1) <u>Scoping the V&V effort</u> a) Determine the characteristics (e.g., complexity, criticality, risk, safety, security, desired performance, reliability, or other project-unique characteristics) that define the importance of the system of interest to the user. b) Adopt the system integrity schema assigned to the project. If no integrity level schema exists, then one is developed. c) Assign an integrity level to the system of interest. d) Establish the degree of independence (see Annex C), if any, required for the V&V. e) Determine the minimum V&V tasks for the integrity level using Table 2a through Table 2d and the selected integrity level schema. f) Determine the extent of V&V on reuse items selected for the program (see Annex D). g) Determine the extent of V&V on an n th of a kind system (see Annex M). h) Determine the extent of V&V for tools that insert or translate code (e.g., optimizing compilers and auto-code generators). i) Augment the minimum V&V tasks with optional V&V tasks, as necessary. j) Provide an estimate of the V&V budget, including test facilities, and tools as required.	Preliminary system description Statement of need RFP or tender System integrity level schema	VVP
(2) <u>Planning the interface between the V&V effort and supplier</u> (Preparing the preliminary data and processes for the interface with a supplier to be selected in the Supply Process.) a) Incorporate the project integrity level schema into the planning process. b) Plan the V&V schedule for each V&V task. c) Identify the preliminary list of development processes and products to be evaluated by the V&V processes. d) Describe V&V access rights to proprietary and classified information. e) Coordinate the plan with the acquirer.	VVP Draft RFP or tender Contract	Task report(s)— Recommendations for RFP or tender Updated VVP
(3) <u>System requirements review</u> a) Review the system requirements (e.g., system requirements specification, feasibility study report, business rules description) in the RFP or tender to perform the following: b) Verify the consistency of requirements to user needs. c) Validate whether the requirements can be satisfied by the defined technologies, methods, and algorithms defined for the project (feasibility). d) Verify whether objective information that can be demonstrated by testing is provided in the requirements (testability). e) Review other requirements, such as deliverable definitions, listing of appropriate compliance standards and regulations,	Preliminary system description Statement of need User needs Draft RFP or tender	Task report(s)— System requirements review Anomaly report(s)

performance, safety, security and quality attributes, and user needs for completeness, correctness, and accuracy.		
(4) <u>Acceptance support</u> (The following V&V activities support acceptance in the Acquisition Process. The activities are described in various V&V tasks across the life cycle where required inputs for the V&V activities are generated to aid the understanding of the activity flow.) a) System acceptance test plan V&V [8.3, Task 6]. b) System acceptance test design V&V [8.4, Task 8]. c) System acceptance test case V&V [8.5, Task 8]. d) System acceptance test procedure V&V [8.7, Task 7]. e) System acceptance test execution V&V [8.10, Task 3]. f) Software acceptance test plan V&V [9.3, Task 6]. g) Software acceptance test design V&V [9.4, Task 9]. h) Software acceptance test case V&V [9.5, Task 10]. i) Software acceptance test procedure V&V [9.7, Task 9]. j) Software acceptance test execution V&V [9.10, Task 3]. k) Hardware acceptance test plan V&V [10.3, Task 6]. l) Hardware acceptance test design V&V [10.4, Task 9]. m) Hardware acceptance test case V&V [10.5, Task 10]. n) Hardware acceptance test procedure V&V [10.7, Task 9]. o) Hardware acceptance test execution V&V [10.10, Task 3].	Concept documentation SDD IDD SRS IRS Source code Hardware items Executable code User documentation Test plans, designs, cases, procedures, results Acceptance test plan V&V task results	Task report(s)—Acceptance Support V&V Acceptance V&V test plan, design(s), cases, procedures, test results Anomaly report(s)
7.3 Activity: Supply planning V&V (common, 15288—Supply Process)		
V&V tasks	Required inputs	Required outputs
(1) <u>Planning the interface between the V&V effort and supplier</u> (Coordinating and documenting the interface data and processes with the selected supplier) a) Review the supplier development plans and schedules to coordinate the V&V effort with development activities. b) Establish procedures to exchange V&V data and results with the development effort. c) Coordinate the plan with the supplier.	VVP Contract Supplier development plans and schedules	Updated VVP
(2) <u>Contract Verification</u> Verify the following characteristics of the contract: a) System requirements (from RFP or tender, and contract) satisfy and are consistent with user needs. b) Procedures are documented for managing requirement changes and for identifying the management hierarchy to address problems. c) Procedures for interface and cooperation among the parties are documented, including ownership, warranty, copyright, and confidentiality. d) Acceptance criteria and procedures are documented in accordance with requirements.	VVP RFP or tender Contract User needs Supplier development plans and schedules	Task report(s)—Contract Verification Updated VVP Anomaly report(s)
7.4 Activity: Project planning V&V (common, 15288—Project Planning Process)		
V&V tasks	Required inputs	Required outputs
(1) <u>Project planning strategy assessment</u> a) Verify the project plan strategy, including objectives, and constraints.	Project plan strategy Schedules and tasks	Task report(s)—Project planning strategy assessment

b) Verify project scope includes all relevant activities. c) Verify life cycle model is defined.	Requirements Life cycle model Project scope	Anomaly report(s)
7.5 Activity: Configuration management V&V (common, 15288—Configuration Management Process)		
V&V tasks	Required inputs	Required outputs
(1) <u>Configuration management assessment</u> Verify that the Configuration Management Process is complete and adequate. The task criteria are as follows: a) Completeness Verify that there is a process for describing the system, software, and hardware product functionality, tracking program versions, generating baselines (including parameters and settings), and managing changes. b) Adequacy Verify that the Configuration Management Process is adequate for the development complexity, system size, integrity level, project plans, and user needs.	Configuration Management Process documentation	Task report(s)— Configuration management assessment Anomaly report(s)
NOTE (for Table 1a)—Other inputs may be used. For any V&V activity and task, all of the required inputs and outputs from preceding activities and tasks may be used, but for conciseness, only the primary inputs are listed.		

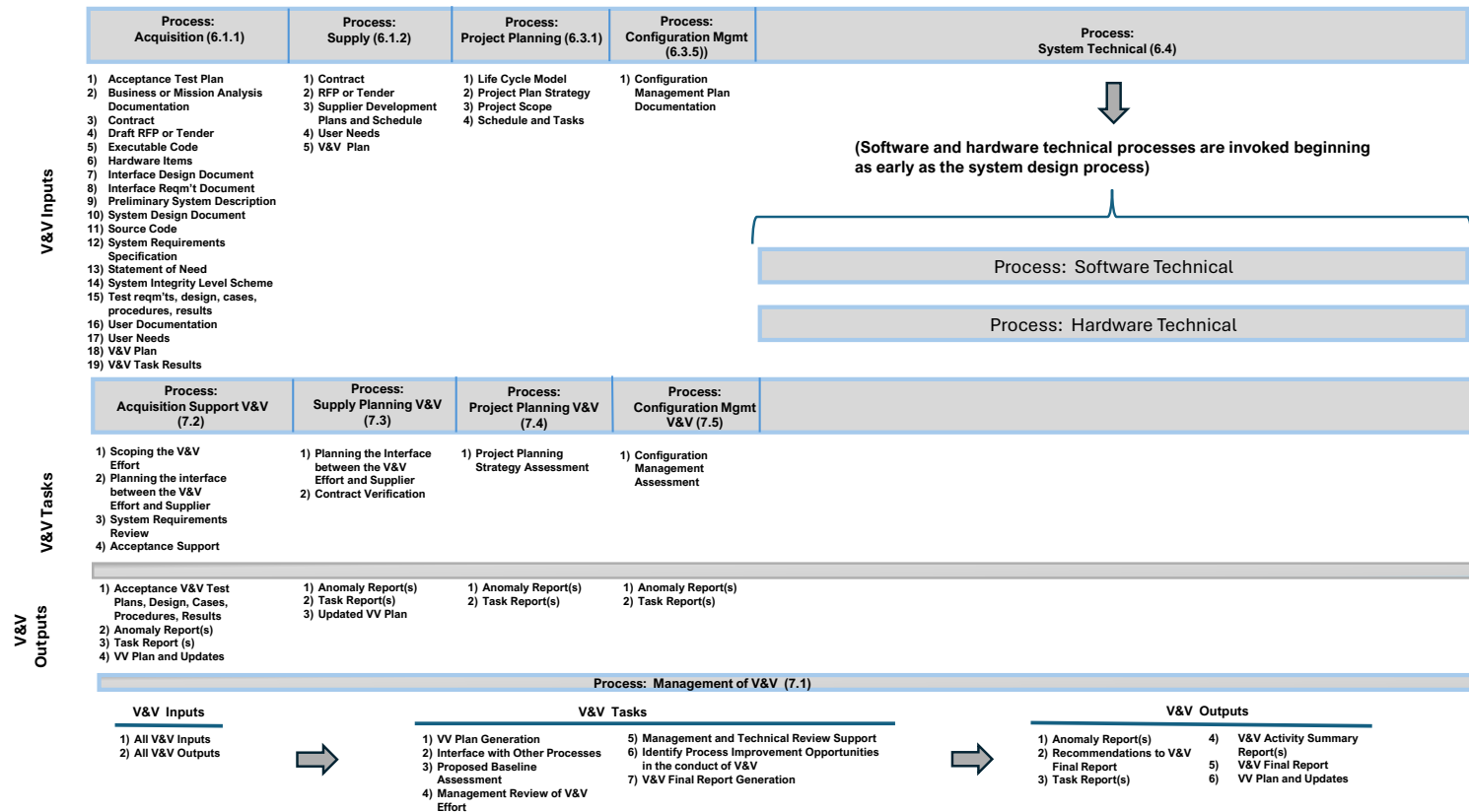
Table 2a—Minimum V&V tasks assigned to each integrity level for common V&V

V&V processes	V&V management (see 7.1)				Acquisition support V&V (see 7.2)				Supply planning V&V (see 7.3)				Project planning V&V (see 7.4)				Configuration management V&V (see 7.5)			
Integrity levels	Levels				Levels				Levels				Levels				Levels			
	4	3	2	1	4	3	2	1	4	3	2	1	4	3	2	1	4	3	2	1
Acceptance support	—	—	—	—	X	X	X	X	—	—	—	—	—	—	—	—	—	—	—	—
Configuration management assessment	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	X	X	X	X
Contract Verification	—	—	—	—	—	—	—	—	X	X	X	X	—	—	—	—	—	—	—	—
Identify process improvement opportunities in the conduct of V&V	X	X	X	X	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
Interface with other processes	X	X	X	X	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
Management and technical review support	X	X	X	X	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
Management review of the V&V effort	X	X	X	X	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
Planning the interface between the V&V effort and the supplier	—	—	—	—	X	X	X	X	X	X	X	X	—	—	—	—	—	—	—	—
Project planning strategy assessment	—	—	—	—	—	—	—	—	—	—	—	—	X	X	X	X	—	—	—	—
Proposed/baseline change assessment	X	X	X	X	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
Scoping the V&V effort	—	—	—	—	X	X	X	X	—	—	—	—	—	—	—	—	—	—	—	—
System requirements review	—	—	—	—	X	X	X	X	—	—	—	—	—	—	—	—	—	—	—	—
V&V final report generation	X	X	X	X	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
VVP generation	X	X	X	X	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
NOTE—Whenever a V&V task is selected as a mandatory requirement for multiple integrity levels, the V&V task implementation is dictated by the rigor, intensity, and depth of the analysis or test. A higher integrity level implementation requires greater rigor (e.g., formal methods or structured analysis methods), intensity (e.g., consideration of all system conditions and system environment states), and depth (e.g., abnormal cases, boundary conditions, or comprehensive fault and recovery scenarios) of the analysis or test than the lower integrity level implementation.																				

The recommended applicability of optional tasks to the common V&V processes described in [Clause 7](#) is shown in [Table 3a](#). [Annex G](#) provides a description of each of the optional V&V tasks.

Table 3a—Optional V&V tasks and suggested applications in System Agreement and Project processes

	Acquisition (7.2)	Supply (7.3)	Project planning (7.4)
Algorithm analysis	—	X	—
Audit performance	—	—	—
Audit support	—	—	X
Control flow analysis	—	—	—
Cost analysis	X	X	X
Database analysis	—	—	—
Data flow analysis	—	—	—
Disaster recovery plan assessment	—	—	X
Distributed architecture assessment	—	—	—
Exploratory Testing	—	—	—
Feasibility study evaluation	X	X	X
Independent risk assessment	—	—	—
Inspection	—	—	—
Inspection—Concept	—	—	—
Inspection—Requirements	—	—	—
Inspection—Design	—	—	—
Inspection—Source code	—	—	—
Inspection—Test plan	—	—	—
Inspection—Test design	—	—	—
Inspection—Test case	—	—	—
Operational evaluation	—	X	—
Performance monitoring	X	—	—
Post-installation Validation	—	—	—
Project management oversight support	X	X	X
Proposal evaluation support	X	—	—
Regression analysis and testing	—	—	—
Reusability analysis	X	X	X
Reuse analysis	X	X	X
Simulation analysis	—	X	—
Sizing and timing analysis	—	—	—
System software assessment	—	—	—
Test certification	—	—	—
Test evaluation	—	—	—
Test witnessing	—	—	—
Training documentation evaluation	—	—	—
Usability analysis	—	—	X
User documentation evaluation	—	—	X
User training	X	—	X
V&V tool plan generation	X	X	X
V&V tool qualification	—	—	—
Walkthrough	—	—	—
Walkthrough—Design	—	—	—
Walkthrough—Requirements	—	—	—
Walkthrough—Source code	—	—	—
Walkthrough—Test	—	—	X
Work breakdown structure (WBS) evaluation	—	—	X



NOTE 1—Clause references in the process definitions (top graphic bar) are ISO/IEC/IEEE 15288:2023(E) [B41] clause numbers.

NOTE 2—The V&V tasks may be performed concurrently. The sequential (waterfall) model is shown as an example of a life cycle model.

NOTE 3—V&V tasks listed in the figure are the minimum required for integrity level 4 (highest integrity level).

NOTE 4—Table 1a (common V&V tasks), Table 1b (system V&V tasks), Table 1c (software V&V tasks), and Table 1d (hardware V&V tasks) contain a complete list of minimum V&V tasks. Table 2a (common V&V tasks), Table 2b (system V&V tasks), Table 2c (software V&V tasks), and Table 2d (hardware V&V tasks) define the minimum V&V tasks for each integrity level.

NOTE 5—The clause numbers in the activity V&V graphic bar(s) correspond to Clause 7 of this standard, where the common V&V processes and activities can be found.

Figure 1a—Summary of common V&V activities and tasks