IEEE STANDARDS ASSOCIATION

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

IEEE Computer Society

Sponsored by the
Software and Systems Engineering Standards Committee

IEEE
3 Park Avenue
New York, NY 10016-5997
USA

**IEEE Std 1012™-2016**
(Revision of
IEEE Std 1012-2012/
Incorporates
IEEE Std 1012-2016/Cor1-2017)

**IEEE Std 1012™-2016**
(Revision of
IEEE Std 1012-2012/
Incorporates
IEEE Std 1012-2016/Cor1-2017)

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

Sponsor

**Software and Systems Engineering Standards Committee**
of the
**IEEE Computer Society**

Approved 28 September 2017

**IEEE-SA Standards Board**

**Abstract:** 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. This standard applies to systems, software, and hardware being developed, maintained, or reused (legacy, commercial off-the-shelf [COTS], non-developmental items). The term *software* also includes firmware and microcode, and each of the terms *system, software*, and *hardware* includes documentation. V&V processes include the analysis, evaluation, review, inspection, assessment, and testing of products.

**Keywords:** acceptance testing, architecture evaluation, component testing, concept documentation evaluation, criticality, criticality analysis, design evaluation, disposal plan evaluation, environmental verification and validation (V&V) factors, hardware life cycle, hardware V&V, hardware verification and validation, hazard analysis, IEEE 1012, implementation evaluation, independent verification and validation (IV&V), integration testing, integrity level, interface analysis, IV&V, minimum V&V tasks, 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, software life cycle, software quality assurance (SQA), 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

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



PDF: ISBN 978-1-5044-1812-6 STD20911
Print: ISBN 978-1-5044-1813-3 STDPD20911

## Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page, appear in all standards and may be found under the heading "Important Notices and Disclaimers Concerning IEEE Standards Documents." They can also be obtained on request from IEEE or viewed at http://standards.ieee.org/IPR/disclaimers.html.

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

IEEE Standards documents (standards, recommended practices, and guides), both full-use and trial-use, are developed within IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association ("IEEE-SA") Standards Board. IEEE ("the Institute") develops its standards through a consensus development process, approved by the American National Standards Institute ("ANSI"), which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE Standards are documents developed through scientific, academic, and industry-based technical working groups. Volunteers in IEEE working groups are not necessarily members of the Institute 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 Standards do not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

IEEE does not warrant or represent the accuracy or content of the material contained in its standards, and expressly disclaims all warranties (express, implied and statutory) not included in this or any other document relating to the standard, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; and quality, accuracy, effectiveness, currency, or completeness of material. In addition, IEEE disclaims any and all conditions relating to: results; and workmanlike effort. 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 his or her 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: PROCUREMENT OF 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 development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE should be considered the approved IEEE standard.

## Official statements

A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual 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. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position of IEEE.

## Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE. However, IEEE does not provide 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 Standards Coordinating Committees 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 revisions to an IEEE standard is welcome to join the relevant IEEE working group.

Comments on standards should be submitted to the following address:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
Piscataway, NJ 08854 USA

## 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 imply 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.

## 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, IEEE does not waive any rights in copyright to the documents.

## Photocopies

Subject to payment of the appropriate fee, 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. 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 ten years. When a document is more than ten 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 the IEEE-SA Website at http://ieeexplore.ieee.org/xpl/standards.jsp or contact IEEE at the address listed previously. For more information about the IEEE–SA or IEEE's standards development process, visit the IEEE-SA Website at http://standards.ieee.org.

## Errata

Errata, if any, for all IEEE standards can be accessed on the IEEE-SA Website at the following URL: http://standards.ieee.org/findstds/errata/index.html. Users are encouraged to check this URL for errata periodically.

## Patents

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 http://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.

## Participants

## IEEE Std 1012-2016

At the time IEEE Std 1012-2016 was completed, the P1012 Working Group had the following membership:

**Roger U. Fujii**, *Chair*
**Michael E. Waterman**, *Vice Chair*
**Edward A. Addy**, *Secretary*

Rossnyev Alvarado
Steven Baird, Jr.
Arde Bedjanian
Luis Betancourt
Susan M. Burgess
Tiffany Burgess
William Burgess
Norbert Carte
Lisa Castelli
Jiayu Chen
Larry Chi
Ivan Chow
Pong C. Chung
Darrell Cooksey
Ken Costello
David H. Daniel
Harpal Dhama
Ronald F. Dean, Sr.
Jun Ding
Stephen Driskell
Eva Freund
Jon D. Hagar
Libing He
Yanjun He
John W. Hefler
David Hooten
George R. Hughes
Yu-chih Ko
Thomas M. Kurihara
Lingpo Li
Gang Ma
Charles R. Martin
Robert R. Moniri
Owen Nelson
Adefeyike Odutayo
Stan Potoczny
William Roggenbrodt
Shirley A. Savarino
Scott W. Schield
Raymond R. Senechal
Li Shi
Maryna Y. Tyrpak
Murat S. Uzman
Yichun Wu
Steve Yang
Xiaobai Yu

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

Edward A. Addy
Robert Aiello
Johann Amsenga
T. Scott Ankrum
Lee Armstrong
Steven Baird, Jr.
Bakul Banerjee
Pieter Botman
Susan M. Burgess
Juan Carreon
Sue Carroll
Keith Chow
Raul Colcher
Paul Croll
Geoffrey Darnton
Ronald F. Dean, Sr.
Grazia D'Elia
Harpal Dhama
Teresa Doran
Sourav Dutta
Andrew Fieldsend
Eva Freund
David Friscia
Roger U. Fujii
David Fuschi
Gregg Giesler
Randall Groves
Jon D. Hagar
John Harauz
David Herrell
Werner Hoelzl
Bernard Homes
George R. Hughes
Theresa Hunt
Noriyuki Ikeuchi
Atsushi Ito
Mark Jaeger
Paul Joannou
Cheryl Jones
Piotr Karocki
Yuri Khersonsky
Thomas M. Kurihara
Susan Land
David Leciston
Edward McCall
James Moore
Michael Newman
Warren Odess-Gillett
James Pritchett
Iulian Profir
Laura Pullum
Annette Reilly
Robert Robinson
Terence Rout
Bartien Sayogo
Robert Schaaf
Hans Schaefer
Scott W. Schield
Maud Schlich
Stephen Schwarm
Carl Singer
James Sivak
Michael Smith
Thomas Starai
Walter Struppler
Gerald Stueve
Marcy Stutzman
Thomas Tullia
Maryna Y. Tyrpak
Mark-Rene Uchida
Murat S. Uzman
John Vergis
David Walden
Michael E. Waterman
Stephen Webb
Steve Yang
Jian Yu
Oren Yuen
Shuhui Zhang
Daidi Zhong

When the IEEE-SA Standards Board approved this standard on 15 May 2016, it had the following membership:

**Jean-Philippe Faure**, *Chair*
**Ted Burse**, *Vice Chair*
**John D. Kulick**, *Past Chair*
**Konstantinos Karachalios**, *Secretary*

Chuck Adams
Masayuki Ariyoshi
Stephen Dukes
Jianbin Fan
J. Travis Griffith
Gary Hoffman
Ronald W. Hotchkiss
Michael Janezic
Joseph L. Koepfinger*
Hung Ling
Kevin Lu
Annette D. Reilly
Gary Robinson
Mehmet Ulema
Yingli Wen
Philip Winston
Howard Wolfman
Don Wright
Yu Yuan
Daidi Zhong

*Member Emeritus

## Participants
## IEEE Std 1012-2016/Cor1-2017

At the time IEEE Std 1012-2016/Cor1-2017 was completed, the P1012 Working Group had the following membership:

**Roger U. Fujii**, *Chair*
**Michael E. Waterman**, *Vice Chair*
**Edward A. Addy**, *Secretary*

Rossnyev Alvarado
Steven Baird, Jr.
Arde Bedjanian
Luis Betancourt
Susan M. Burgess
Tiffany Burgess
William Burgess
Norbert Carte
Lisa Castelli
Jiayu Chen
Larry Chi
Ivan Chow
Pong C. Chung
Darrell Cooksey
Ken Costello
David H. Daniel
Harpal Dhama
Ronald F. Dean, Sr.
Jun Ding
Stephen Driskell
Eva Freund
Dirk Guijt
Jon D. Hagar
Libing He
Yanjun He
John W. Hefler
David Hooten
George R. Hughes
Yu-chih Ko
Thomas M. Kurihara
Lingpo Li
Gang Ma
Charles R. Martin
Robert R. Moniri
Owen Nelson
Adefeyike Odutayo
Stan Potoczny
William Roggenbrodt
Shirley A. Savarino
Scott W. Schield
Raymond R. Senechal
Li Shi
Maryna Y. Tyrpak
Murat S. Uzman
Yichun Wu
Steve Yang
Xiaobai Yu

The following members of the individual balloting committee voted on Corrigendum 1 of this standard. Balloters may have voted for approval, disapproval, or abstention.

Edward Addy
Robert Aiello
Johann Amsenga
Steven Baird, Jr.
Ulas Baloglu
Patti Brideson
Demetrio Bucaneg, Jr.
Paul Cardinal
Juan Carreon
Keith Chow
Paul Croll
Ronald F. Dean, Sr.
Sourav Dutta
Dale Dzielski
Eva Freund
David Friscia
Roger Fujii
David Fuschi
Randall Groves
Louis Gullo
Jon D. Hagar
John Harauz
Mark Henley
David Herrell
Frank Hill
Werner Hoelzl
Bernard Homes
Noriyuki Ikeuchi
Atsushi Ito
Cheryl Jones
Piotr Karocki
Thomas M. Kurihara
George Kyle
David Leciston
Claire Lohr
Ignacio Marin-Garcia
Edward McCall
Andrew Nack
Michael Newman
James Pritchett
Annette D. Reilly
Robert Robinson
Terence Rout
Robert Schaaf
Hans Schaefer
Scott W. Schield
Maud Schlich
Stephen Schwarm
Raymond R. Senechal
Carl Singer
Michael Smith
Kendall Southwick
Luca Spotorno
Thomas Starai
John Stevens
Walter Struppler
Vincent Tume
Maryna Y. Tyrpak
Mark-Rene Uchida
Murat S. Uzman
John Vergis
David Walden
Jian Yu
Oren Yuen
Shuhui Zhang

When the IEEE-SA Standards Board approved this standard on 28 September 2017, it had the following membership:

**Jean-Philippe Faure**, *Chair*
**Gary Hoffman**, *Vice Chair*
**John D. Kulick**, *Past Chair*
**Konstantinos Karachalios**, *Secretary*

Chuck Adams
Masayuki Ariyoshi
Ted Burse
Stephen Dukes
Doug Edwards
J. Travis Griffith
Michael Janezic
Thomas Koshy
Joseph L. Koepfinger*
Kevin Lu
Daleep Mohla
Damir Novosel
Ronald C. Petersen
Annette D. Reilly
Robby Robson
Dorothy Stanley
Adrian Stephens
Mehmet Ulema
Phil Wennblom
Howard Wolfman
Yu Yuan

*Member Emeritus

## Introduction

This introduction is not part of IEEE Std 1012™-2016, IEEE Standard for System, Software, and Hardware Verification and Validation.

The Verification and Validation 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 (V&V)*. 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 1012 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 1012-2012 [B5].[1] 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. This revision aligns more completely with the terminology and structure of ISO/IEC/IEEE 15288:2015(E) [B16] and ISO/IEC 12207:2008 [B11]. The following is a summary of the changes made in this version:

— No new V&V activities or tasks have been added other than to address the new or modified processes from ISO/IEC/IEEE 15288:2015(E) [B16], and conformance to this standard can be readily aligned with conformance to the V&V clauses of ISO/IEC/IEEE 15288. Some V&V activities and tasks have been rearranged to facilitate understanding and ease of use.

— The terminology, structure, and mappings were revised to be consistent with ISO/IEC/IEEE 15288:2015(E) [B16].

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.

[1] The numbers in brackets correspond to those of the bibliography in Annex N.

— 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 15288:2015(E) [B16] and ISO/IEC 12207:2008 [B11], as well as the entire family of IEEE software engineering standards. This standard addresses all system and software life cycle processes, including the Agreement, Organizational Project-Enabling, Project, Technical, Software Implementation, Software Support, and Software Reuse 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.

## Contents

# 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, Project, Technical, Software Implementation, Software Support, and Software Reuse 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 may invoke those life cycle processes and the associated V&V processes that apply to the project. A description of system life cycle processes may be found in ISO/IEC/IEEE 15288:2015(E) [B16],[1] and a description of software life cycle processes may be found in ISO/IEC 12207:2008 [B11]. Annex A maps ISO/IEC/IEEE 15288:2015(E) [B16] (Table A.1 and Table A.2) and ISO/IEC 12207:2008 [B11] (Table A.3 and Table A.4) to the V&V activities and tasks defined in this standard.

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,

[1] The numbers in brackets correspond to those of the bibliography in Annex N.

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.

V&V processes consist of the Verification process and the Validation process. 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 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 15288:2015(E) [B16] includes 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:

— 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 Verification and Validation Plan.

## 1.3 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 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 a 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 in accordance with requirements and that errors are not propagated between components of the system.

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 12207:2008 [B11] or ISO/IEC/IEEE 15288:2015(E) [B16].

To address the systems perspective, 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 15288:2015(E) [B16] life cycle processes (agreement, organizational project-enabling, technical management, and technical) with an 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 [B1].

## 1.4 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.

## 1.5 Organization of the standard

The Verification and Validation processes described in this standard are constructed to be consistent with ISO/IEC/IEEE 15288:2015(E) [B16] and ISO/IEC Std 12207:2008 [B11].

This standard is organized into clauses (Clause 1 through Clause 12), tables (Table 1 through Table 3, and their respective subparts a–d), figures (Figure 1 and Figure 2, and their respective subparts a–d), and annexes (Annex A through Annex N). Clause 2 through Clause 12 and 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 point 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 containing V&V activities and tasks 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 provides examples of V&V processes and provides guidance for using this standard, and they are similarly organized. All annexes are informative.

- 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 15288:2015(E) [B16] and ISO/IEC 12207:2008 [B11], 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, Clause 9, and 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 combinations**

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.[2]

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 12207:2008 [B11] life cycle processes to the V&V activities and tasks described in this standard.

Annex A describes the mapping of ISO/IEC 12207:2008 [B11] and ISO/IEC/IEEE 15288:2015(E) [B16] to this standard's V&V activities and tasks. Annex B provides an example of a risk-based, four-level integrity schema. Annex C describes the degrees of independence in verification and validation. 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 system, 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 maps the process outcomes from ISO/IEC 12207:2008 [B11] and ISO/IEC/IEEE 15288:2015(E) [B16] to associated V&V tasks. Annex M describes V&V for $n^{th}$ of a kind systems. Annex N provides a bibliography of the informative standards referenced in this standard.

[2] Notes in text, tables, and figures of a standard are given for information only and do not contain requirements needed to implement this standard.

## 1.6 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.

## 1.7 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 below:

- 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.

## 1.8 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. Standards useful for the implementation and interpretation of this standard are listed in Annex N, Bibliography.

## 3. Definitions and acronyms

### 3.1 Definitions

For the purposes of this document, the following terms and definitions apply. The *IEEE Standards Dictionary Online* [B2] should be consulted for terms not defined in this clause.[3]

**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 24765:2010 [B20].

**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 24765:2010 [B20].

**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 24765:2010 [B20].

**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 [B10].

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

NOTE—See ISO/IEC/IEEE 24765:2010 [B20].

**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 24765:2010 [B20].

**component testing:** Testing of individual hardware or software components.

NOTE—See ISO/IEC/IEEE 24765:2010 [B20].

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

[3] *IEEE Standards Dictionary Online* subscription is available at: http://www.ieee.org/portal/innovate/products/standard/standards_dictionary.html.

NOTE—See ISO/IEC/IEEE 24765:2010 [B20].

**domain:** A problem space.

NOTE—See IEEE Std 1517-2010 [B10].

**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 [B10].

**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 [B10].

**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 24765:2010 [B20].

**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 24765:2010 [B20].

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

NOTE—See ISO/IEC/IEEE 24765:2010 [B20].

**independent verification and validation (IV&V):** 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 24765:2010 [B20].

**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 24765:2010 [B20].

**integrity level:** A value representing project-unique characteristics (e.g., complexity, criticality, risk, safety level, security level, 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 system and components. These descriptions include control algorithms, protocols, data contents and formats, and performance.

NOTE—See ISO/IEC/IEEE 24765:2010 [B20].

**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 24765:2010 [B20].

**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 24765:2010 [B20].

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

NOTE—See ISO/IEC/IEEE 24765:2010 [B20].

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

NOTE—See ISO/IEC/IEEE 24765:2010 [B20].

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

**$n^{th}$ of a kind component/system:** a re-manufacturing or re-installation of a previously verified and validated hardware and/or software design. The $n^{th}$ 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 M for a discussion of V&V of $n^{th}$ of a kind systems.

**optional tasks:** Those 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.

NOTE—See ISO/IEC/IEEE 24765:2010 [B20].

**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, architectures), not just to software itself.

NOTE—See ISO/IEC/IEEE 24765:2010 [B20].

**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 [B19]. ISO/IEC 16085 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 24765:2010 [B20].

**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 24765:2010 [B20].

**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 24765:2010 [B20].

**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 15288:2015(E) [B16].

**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 24765:2010 [B20].

**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 24765:2010 [B20].

**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 24765:2010 [B20].

**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 [B4].

**validation: (A)** The process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements. **(B)** 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.

NOTE—For (A), see ISO/IEC/IEEE 24765:2010 [B20].

**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 24765:2010 [B20].

**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:

| | |
|---|---|
| COTS | commercial off-the-shelf |
| CPU | central processing unit |
| GOTS | government off-the-shelf |
| HDD | hardware design description |
| HRS | hardware requirements specification |
| HW | hardware |
| IDD | interface design document |
| IRS | interface requirements specification |
| IV&V | independent verification and validation |
| N/A | not applicable |
| N/R | not required |
| OCD | operational concept document |
| QA | quality assurance |
| RFP | request for proposal (tender) |
| SDD | software design description |
| SRS | software requirements specification |
| SW | software |

| | |
|---|---|
| TRA | threat and risk assessment |
| VVP | verification and validation plan |
| V&V | verification and validation |
| WBS | work breakdown structure |

## 4. Relationships between verification and validation (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 verification and validation plan (VVP).

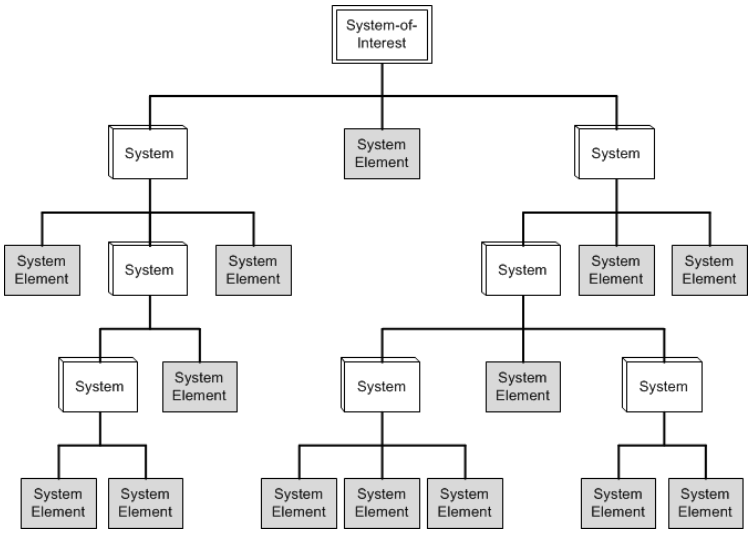
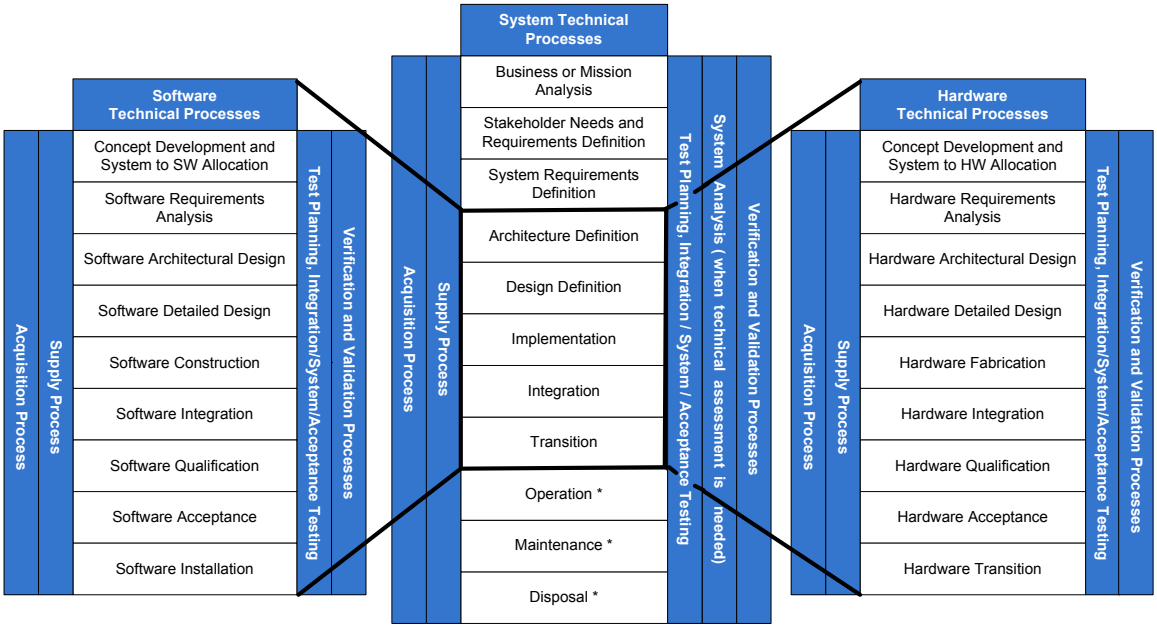



**Figure 4—Example system-of-interest structure**

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 15288:2015(E) [B16]. System V&V as described in this V&V standard is a conforming instance of the Verification and Validation processes in ISO/IEC/IEEE 15288:2015(E) [B16] (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 Software Verification and Software Validation processes within the Software Support processes group of the Life Cycle processes defined in ISO/IEC 12207:2008 [B11].

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 Software Construction process (described in Clause 9) or the Hardware Fabrication 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—The Operation, Maintenance, and Disposal processes within the System Technical processes are marked with an asterisk (*) to indicate that there are Software and Hardware V&V activities and tasks that support these System Technical processes but are not shown in Figure 5.

NOTE 3—Management of V&V activity is concurrent with all V&V activities.

NOTE 4—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**

Figure 6 maps the V&V activities to those processes for which this V&V standard calls out specific activities and tasks.

| V&V activity<br>IEEE 1012 | System processes<br>(ISO/IEC/IEEE 15288:2015(E) [B16]) | Software processes<br>(ISO/IEC 12207:2008 [B11]) | Hardware processes<br>(NOTE 4) |
|---|---|---|---|
| V&V Management | Verification, Validation | Software Verification, Software Validation | |
| Acquisition Support V&V | Acquisition | Acquisition | Acquisition |
| Supply Planning V&V | Supply | Supply | Supply |
| Project Planning V&V | Project Planning | Project Planning | Project Planning |
| Configuration Management V&V | Configuration Management | Software Configuration Management | Hardware Configuration Management |
| Business or Mission Analysis V&V | Business or Mission Analysis | | |
| Stakeholder Needs and Requirements Definition V&V | Stakeholder Needs and Requirements Definition | Stakeholder Requirements Definition | Stakeholders Requirements Definition |
| System Requirements Definition V&V | System Requirements Definition | System Requirements Analysis | System Requirements Analysis |
| Architecture Definition V&V | Architecture Definition | | |
| Design Definition V&V | Design Definition | | |
| System Analysis V&V | System Analysis | | |
| Implementation V&V<br>Software/Hardware V&V Activities<br>Software/Hardware Concept V&V<br>Software/Hardware Requirements Analysis V&V<br>Software/Hardware Design V&V<br>Software Construction/Hardware Fabrication V&V<br>Software/Hardware Integration V&V<br>Software/Hardware Qualification Testing V&V<br>Software/Hardware Acceptance Testing V&V | Implementation | Software Implementation | Hardware Implementation |
| Integration V&V | Integration | Support System Integration | Support System Integration |
| All verification activities of the IEEE 1012 life cycle | Verification | Software Verification | Hardware Verification |
| Transition V&V<br>Software Installation and Checkout V&V<br>Hardware Transition V&V | Transition | Software Installation | Hardware Transition |
| All validation activities of the IEEE 1012 life cycle | Validation | Software Validation | Hardware Validation |
| Operation V&V<br>Software Operation V&V<br>Hardware Operation V&V | Operation | Software Operation | Hardware Operation |
| Maintenance V&V<br>Software Maintenance V&V<br>Hardware Maintenance V&V | Maintenance | Software Maintenance | Hardware Maintenance |
| Disposal V&V<br>Software Disposal V&V<br>Hardware Disposal V&V | Disposal | Software Disposal | Hardware Disposal |

NOTE 1—Not all life cycle processes from ISO/IEC/IEEE 15288:2015(E) [B16] and ISO/IEC 12207:2008 [B11] have V&V tasks specified in this standard. 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 that are used in the V&V effort.

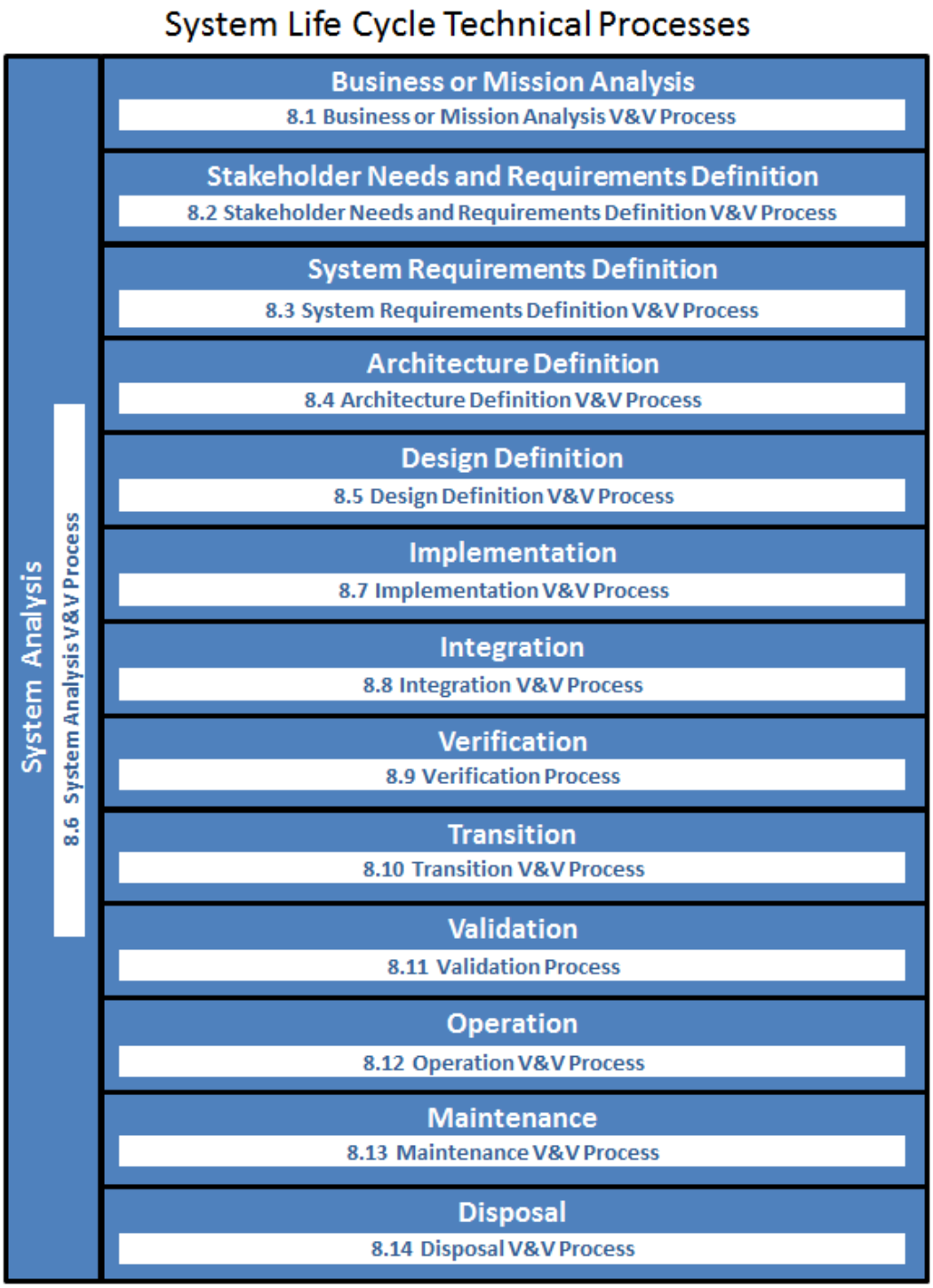
NOTE 2—V&V practitioners provide feedback on noted deficiencies or areas for improvement

NOTE 3—Each ISO/IEC 12207 software specific process is a specialization of its corresponding process in ISO/IEC/IEEE 15288:2015(E) [B16]. Users may consider claiming conformance to the ISO/IEC/IEEE 15288 process rather than the ISO/IEC 12207 process.

NOTE 4—Each hardware process that corresponds to an ISO/IEC 12207 software specific process is a specialization of its corresponding process in ISO/IEC/IEEE 15288.

**Figure 6—Mapping of V&V activities to system, software, and hardware processes**

The life cycle model, including selected processes, defines the evolution of the system, software, and hardware elements throughout life cycle stages. To achieve the verification and validation processes outcomes for each life cycle process, this standard is organized by life cycle process, and within each life cycle process the verification and validation activities and tasks for that life cycle process are identified. Figure 7 illustrates that organization for system life cycle processes. The listing of all verification and validation activities and tasks to specific system, software, or hardware life cycle processes are depicted in Figure 1a (Common V&V), Figure 1b (System V&V), Figure 1c (Software V&V), and Figure 1d (Hardware V&V). The mappings of ISO/IEC/IEEE 15288 processes and activities with IEEE Standard 1012 V&V activities and of ISO/IEC 12207 processes and activities with IEEE Standard 1012 V&V activities are shown in Annex A.




NOTE—Each system, software, and hardware life cycle process defines the evolution of the system, software, and hardware elements throughout life cycle stages. To achieve the verification and validation process outcomes for each life cycle process, the standard is organized by life cycle process and within each life cycle process the verification and validation activities and tasks are identified. This figure illustrates that organization for system life cycle processes.

**Figure 7 —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 level, security level, 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 entities 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 among 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 15026:2011 [B14].

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 details, 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 is 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 it supports.

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. The tools that insert or translate code (e.g., optimizing compilers and auto-code generators) 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 output of the tool 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 combination

of components having lower integrity levels (e.g., duplication or redundancy—see ISO/IEC 15026:2011 [B14]).

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. V&V process overview

## 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 15288:2015(E) [B16]. 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 12207:2008 [B11]. 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 15288:2015(E) [B16] or ISO/IEC 12207:2008 [B11] 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 15288:2015(E) [B16].

V&V activities that are associated with software life cycle processes are in Clause 9 (Software V&V). The software life cycle processes are the lower level processes under the Software Implementation process of ISO/IEC 12207:2008 [B11]. The Software Design V&V activity addresses both the Software Architectural Design process and the Software Detailed Design process. The Software Test V&V activity addresses testing in several of the software life cycle processes, including the Software Construction process, the Software Integration process, and the Software Qualification Testing process.

V&V activities that are associated with hardware life cycle processes are in Clause 10 (Hardware V&V).

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 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 8 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: 1) examines the stress, abnormal, and fault recovery scenarios that development testing often does not have sufficient time for such test case scenarios and 2) 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 verification and validation processes to repeat or duplicate the same or similar testing as accomplished by the development processes. Rather, V&V testing provides the 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 data base configurations and scenarios; and
- 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 absence of major errors constitute the objective evidence for verifying and validating the system.

NOTE 3—Hardware integr ation 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 8—Minimum level for V&V testing by integrity level**

# 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, and to determine the status of the V&V effort and to direct the V&V effort to perform according to plans and satisfy technical objectives.

### 7.1.2 Outcomes

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 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 those 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 Activities and tasks

The V&V effort shall perform, as specified in Table 2a for the selected integrity level, the following 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 15288:2015(E) [B16]) have been achieved.

### 7.2.2 Outcomes

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 acquirer acceptance of the system.

### 7.2.3 Activities 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 "$n^{th}$ of a kind system." See Annex M 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 process (ISO/IEC/IEEE 15288:2015(E) [B16]) have been achieved.

### 7.3.2 Outcomes

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 Activities 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 successful implementation of the Project Planning V&V process:

a) The VVP is coordinated with the project plan.

### 7.4.3 Activities and tasks

The V&V effort shall perform, as specified in Table 2a for the selected integrity level, the following Project Planning process V&V task and activity 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 supports the Verification and Validation processes.

### 7.5.2 Outcomes

As a result of successful implementation of the Configuration Management V&V process, objective evidence is documented assuring that:

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 Activities and tasks

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 should 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**<br>a) Generate a VVP for all life cycle processes. The VVP may require updating throughout the life cycle. Outputs of other activities are inputs to the VVP.<br>b) Establish a baseline VVP prior to the Requirements V&V activities.<br>c) Identify project milestones in the VVP.<br>d) Schedule V&V tasks to support project management reviews and technical reviews.<br>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)<br>Contract<br>Concept documentation<br>Supplier development plans and schedules | VVP and updates |

| 7.1 Activity: V&V Management (Common) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(2) Interface with Other Processes**<br>a) Coordinate the V&V effort with Organizational Project-Enabling processes and Project processes.<br>b) Identify the V&V data to be exchanged with these processes.<br>c) Document the data exchange requirements in the VVP. | VVP<br>Data identified in the VVP from the Organizational Project-Enabling processes and Project processes | Updated VVP |
| **(3) Proposed/Baseline Change Assessment**<br>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.<br>b) Plan iteration of affected tasks or initiate new tasks to address proposed changes or baseline changes associated with an iterative development process.<br>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<br>Proposed changes<br>Hazard analysis report<br>Risks identified by V&V tasks<br>Supplier development plans and schedules<br>Developer products (produced to date) | Task report(s)—Proposed/baseline change assessment<br>Updated VVP<br>Anomaly report(s) |
| **(4) Management Review of the V&V Effort**<br>a) Review and summarize the V&V effort to define changes to V&V tasks or to redirect the V&V effort.<br>b) Evaluate each anomaly for its criticality (e.g., IEEE Std 1044™-2009 [B7]). 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.<br>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.<br>d) Verify that all V&V tasks conform to task requirements defined in the VVP.<br>e) Verify that V&V task results have a basis of evidence supporting the results.<br>f) Assess all V&V results and provide recommendations for program acceptance and certification as input to the V&V final report.<br>g) Use results of review to identify process improvement opportunities in the conduct of V&V.<br>h) Review the quality of the products and services to assure they meet customer requirements.<br>i) Review the program risks and initiate actions to mitigate risks that exceed thresholds.<br>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.<br>NOTE—For additional information and guidance on review methods see IEEE Std 1028™-2008 [B6]. | VVP and updates<br>Supplier development plans and schedules<br>Anomaly reports<br>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<br>Updated VVP<br>V&V activity summary reports<br>Recommendations to the V&V final report |

| 7.1 Activity: V&V Management (Common) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(5) Management and Technical Review Support**<br>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.<br>b) Verify timely delivery according to the approved schedule of all products and documents. | V&V task results<br>Materials for review (e.g., operational concept document [OCD], architectural and design documents, system requirements, software requirements specification [SRS], interface requirements specification [IRS], software design description [SDD], interface design document [IDD], and test documents) | Task report(s)—Review results<br>Anomaly report(s) |
| **(6) Identify Process Improvement Opportunities in the Conduct of V&V**<br>a) Gather and analyze the lessons learned.<br>b) Gather and analyze the risks identified.<br>c) Gather and analyze the V&V measures.<br>d) Identify and analyze deficiencies in the V&V processes.<br>e) Determine and implement corrective actions using best practices (e.g., repeat V&V tasks or conduct a new V&V task to address corrective actions or use a different method/technique for executing a V&V task).<br>f) Monitor the efficacy of the corrective actions. | V&V task results<br>Materials for review (e.g., OCD, architectural and design documents, system requirements, SRS, IRS, SDD, IDD, and test documents) | Task report(s)—Review results<br>Anomaly report(s) |
| **(7) V&V Final Report Generation**<br>a) Summarize in the V&V final report the V&V activities, tasks, and results, including status and disposition of anomalies.<br>b) Provide an assessment of the overall quality and provide recommendations.<br>c) Document V&V process improvement opportunities.<br>NOTE—The V&V Final Report is intended to be produced at the completion of V&V following development, operations, maintenance, or retirement. | V&V Activity summary report(s) | Task report(s)—V&V final report |

| 7.2 Activity: Acquisition Support V&V (Common, 15288—Acquisition process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(1) Scoping the V&V Effort**<br>a) Determine the characteristics (e.g., complexity, criticality, risk, safety level, security level, desired performance, reliability, or other project-unique characteristics) that define the importance of the system of interest to the user.<br>b) Adopt the system integrity schema assigned to the project. If no integrity level schema exists, then one is developed.<br>c) Assign an integrity level to the system of interest.<br>d) Establish the degree of independence (see Annex C), if any, required for the V&V. | Preliminary system description<br>Statement of need<br>RFP or tender<br>System integrity level schema | VVP |

| 7.2 Activity: Acquisition Support V&V (Common, 15288—Acquisition process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| e) Determine the minimum V&V tasks for the integrity level using Table 2a through Table 2d and the selected integrity level schema.<br>f) Determine the extent of V&V on reuse items selected for the program (see Annex D).<br>g) Determine the extent of V&V on an $n^{th}$ of a kind system (see Annex M).<br>h) Determine the extent of V&V for tools that insert or translate code (e.g., optimizing compilers and auto-code generators).<br>i) Augment the minimum V&V tasks with optional V&V tasks, as necessary.<br>j) Provide an estimate of the V&V budget, including test facilities, and tools as required. | | |
| **(2) Planning the Interface between the V&V Effort and Supplier**<br>(Preparing the preliminary data and processes for the interface with a supplier to be selected in the supply process)<br>a) Incorporate the project integrity level schema into the planning process.<br>b) Plan the V&V schedule for each V&V task.<br>c) Identify the preliminary list of development processes and products to be evaluated by the V&V processes.<br>d) Describe V&V access rights to proprietary and classified information.<br>e) Coordinate the plan with the acquirer. | VVP<br>Draft RFP or tender<br>Contract | Task Report(s)—Recommendations for RFP or tender<br>Updated VVP |
| **(3) System Requirements Review**<br>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:<br>b) Verify the consistency of requirements to user needs.<br>c) Validate whether the requirements can be satisfied by the defined technologies, methods, and algorithms defined for the project (feasibility).<br>d) Verify whether objective information that can be demonstrated by testing is provided in the requirements (testability).<br>e) Review other requirements, such as deliverable definitions, listing of appropriate compliance standards and regulations, user needs, etc., for completeness, correctness, and accuracy. | Preliminary system description<br>Statement of need<br>User needs<br>Draft RFP or tender | Task report(s)—System requirements review<br>Anomaly report(s) |
| **(4) Acceptance Support**<br>(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.)<br>a) System Acceptance Test Plan V&V [8.3, Task 7].<br>b) System Acceptance Test Design V&V [8.4, Task 8].<br>c) System Acceptance Test Case V&V [8.5, Task 7].<br>d) System Acceptance Test Procedure V&V [8.7, Task 7].<br>e) System Acceptance Test Execution V&V [8.10, Task 3].<br>f) Software Acceptance Test Plan V&V [9.2, Task 6].<br>g) Software Acceptance Test Design V&V [9.3, Task 10]. | Concept documentation<br>SDD<br>IDD<br>SRS<br>IRS<br>Source code<br>Hardware items<br>Executable code<br>User documentation<br>Test plans, designs, cases, procedures, results | Task report(s)—Acceptance V&V<br>Acceptance V&V test plan, design(s), cases, procedures, test results<br>Anomaly report(s) |

| 7.2 Activity: Acquisition Support V&V (Common, 15288—Acquisition process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| h) Software Acceptance Test Case V&V [9.4, Task 8].<br>i) Software Acceptance Test Procedure V&V [9.7, Task 1].<br>j) Software Acceptance Test Execution V&V [9.7, Task 2].<br>k) Hardware Acceptance Test Plan V&V [10.2, Task 6].<br>l) Hardware Acceptance Test Design V&V [10.3, Task 10].<br>m) Hardware Acceptance Test Case V&V [10.4, Task 8].<br>n) Hardware Acceptance Test Procedure V&V [10.7, Task 1].<br>o) Hardware Acceptance Test Execution V&V [10.7, Task 2]. | Acceptance test plan<br>V&V task results | |

| 7.3 Activity: Supply Planning V&V (Common, 15288—Supply process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(1) Planning the Interface between the V&V Effort and Supplier**<br>(Coordinating and documenting the interface data and processes with the selected supplier)<br>a) Review the supplier development plans and schedules to coordinate the V&V effort with development activities.<br>b) Establish procedures to exchange V&V data and results with the development effort.<br>c) Coordinate the plan with the supplier. | VVP<br>Contract<br>Supplier development plans and schedules | Updated VVP |
| **(2) Contract Verification**<br>Verify the following characteristics of the contract:<br>a) System requirements (from RFP or tender, and contract) satisfy and are consistent with user needs.<br>b) Procedures are documented for managing requirement changes and for identifying the management hierarchy to address problems.<br>c) Procedures for interface and cooperation among the parties are documented, including ownership, warranty, copyright, and confidentiality.<br>d) Acceptance criteria and procedures are documented in accordance with requirements. | VVP<br>RFP or tender<br>Contract<br>User needs<br>Supplier development plans and schedules | Task Report(s)—Contract verification<br>Updated VVP<br>Anomaly report(s) |

| 7.4 Activity: Project Planning V&V (Common, 15288—Project planning process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(1) Project Planning Strategy Assessment**<br>a) Verify the project plan strategy, including objectives and constraints.<br>b) Verify project scope includes all relevant activities.<br>c) Verify life cycle model is defined. | Project plan strategy<br>Schedules and tasks<br>Requirements<br>Life cycle model<br>Project scope | Task report(s)—Project planning strategy assessment<br>Anomaly report(s) |

| 7.5 Activity: Configuration Management V&V (Common, 15288—Configuration management process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(1) Configuration Management Assessment**<br>Verify that the configuration management process is complete and adequate. The task criteria are as follows:<br>a) Completeness<br>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.<br>b) Adequacy<br>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<br>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**

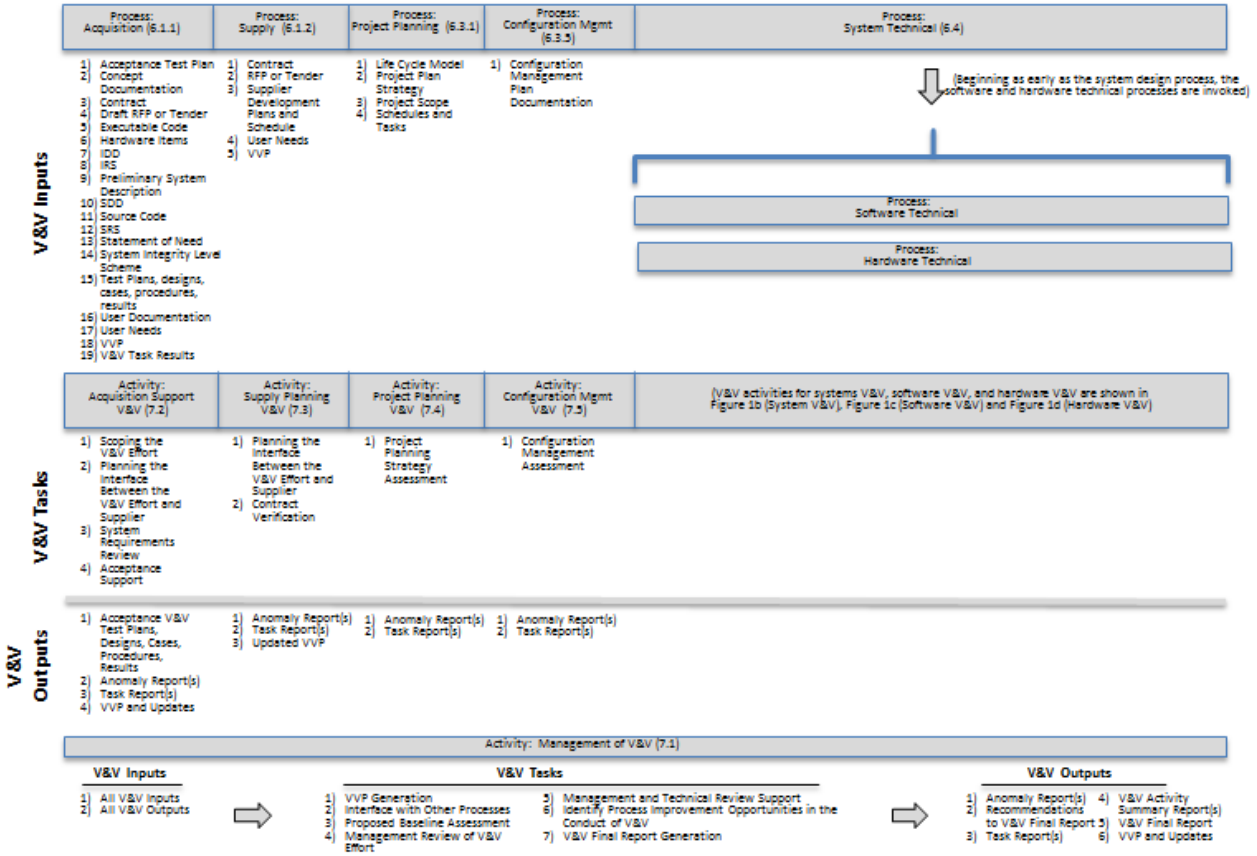
| V&V Activities | Activity: V&V Management (see 7.1) | | | | Activity: Acquisition Support V&V (see 7.2) | | | | Activity: Supply Planning V&V (see 7.3) | | | | Activity: Project Planning V&V (see 7.4) | | | | Activity: Configuration Management V&V (see 7.5) | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 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 | | |
| Qualification testing | | | |
| 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 15288:2015(E) [B16] clause numbers.

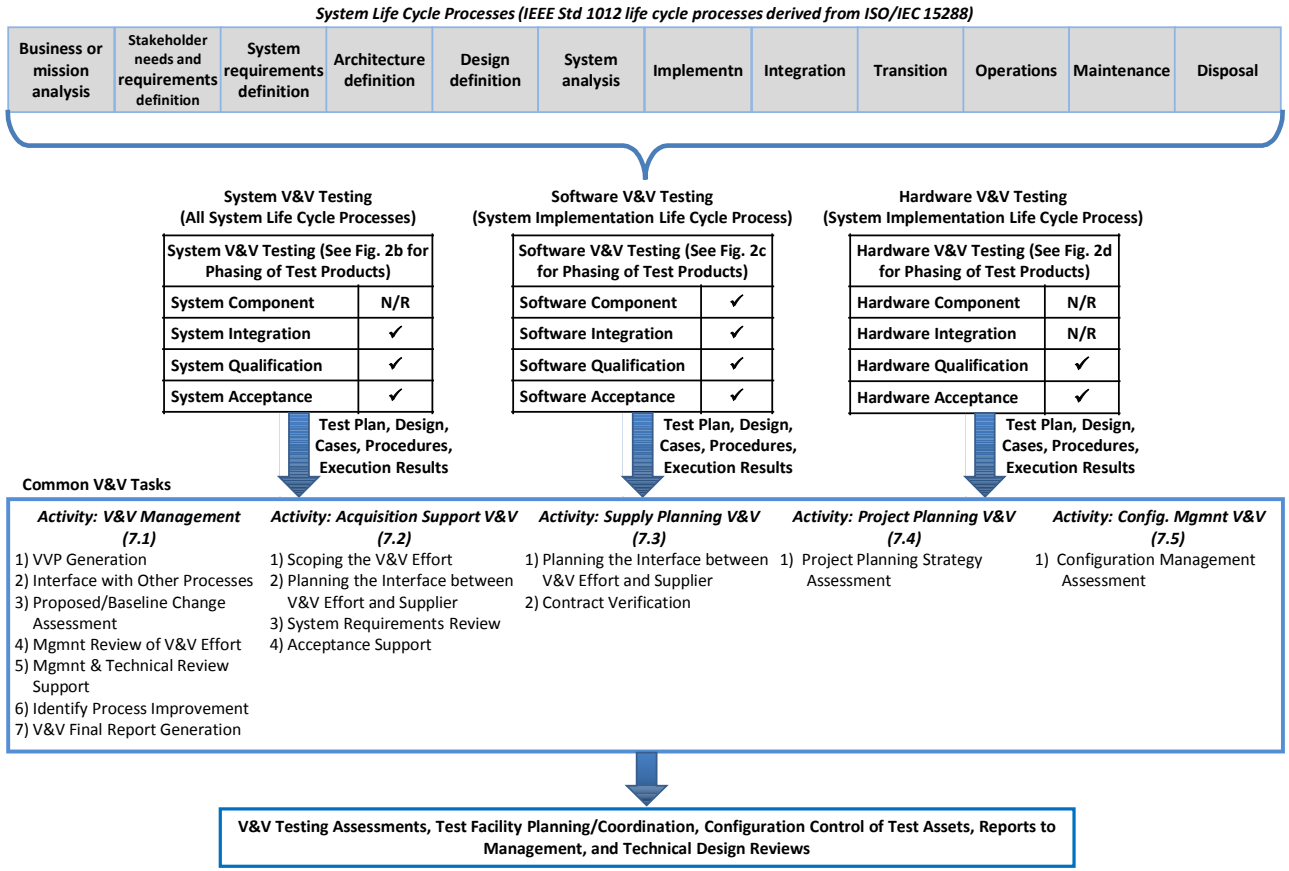
NOTE 2—The V&V tasks may be performed concurrently. The sequential (waterfall) model is shown as an example of a life cycle model.

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 the 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**




NOTE 1—N/R = not required for integrity level 4; ✓ = required for integrity level 4. Diagram illustrates integrity level 4 V&V testing tasks.

NOTE 2—System component consists of software or hardware elements. Because those are tested as part of software and hardware V&V testing, no system component V&V testing is specified.

NOTE 3—The V&V activity clauses shown in the diagram are IEEE Std 1012 clauses.

NOTE 4—System V&V testing covers test planning to execution (spanning system life cycle stages of system requirements definition through transition). Software/hardware V&V testing covers test planning to execution (spanning software/hardware life cycle stages of requirements analysis through transition). Software/hardware life cycle stages all occur within the system implementation life cycle stage.

**Figure 2a—Summary of V&V test products and tasks**

# 8. System V&V processes

## 8.1 Business or Mission Analysis V&V process

### 8.1.1 Purpose

The purpose of the Business or Mission Analysis V&V process is to provide assurance that the outcomes of the Business or Mission Analysis process (ISO/IEC/IEEE 15288:2015(E) [B16]) have been achieved.

### 8.1.2 Outcomes

As a result of the successful implementation of the Business or Mission Analysis V&V process, objective evidence is developed to assess whether:

a) The problem or opportunity space adheres to the organizational strategy.

b) The solution space is consistent with the problem or opportunity space.

c) Preliminary life cycle concepts are consistent with the solution space.

d) The preferred candidate solution alternative(s) are selected.

e) Any enabling systems or services needed for business or mission analysis are available.

f) The root of traceability is established, starting with the organization strategy and tracing to the problem or opportunity space to the solution space to the candidate solutions.

### 8.1.3 Activities and tasks

The V&V effort shall perform, as specified in Table 2b for the selected integrity level, the following Business or Mission Analysis V&V activity and tasks described in Table 1b, Activity 8.1:

a) Business or Mission Analysis V&V: This activity consists of the following tasks:

1) Business or Mission Analysis Results Evaluation

2) Traceability Analysis

3) Criticality Analysis

4) Hazard Analysis

5) Security Analysis

6) Risk Analysis

The Business or Mission Analysis V&V tasks listed shall be used to verify and validate the Business or Mission Analysis process outcomes described in ISO/IEC/IEEE 15288:2015(E) [B16]. The mappings of IEEE 1012 V&V tasks to ISO/IEC/IEEE 15288:2015(E) [B16] Business or Mission Analysis process outcomes are contained in Annex L.

## 8.2 Stakeholder Needs and Requirements Definition V&V process

### 8.2.1 Purpose

The purpose of the Stakeholder Needs and Requirements Definition V&V process is to provide assurance that the outcomes of the Stakeholder Needs and Requirements Definition process (ISO/IEC/IEEE 15288:2015(E) [B16]) have been achieved.

### 8.2.2 Outcomes

As a result of the successful implementation of the Stakeholder Needs and Requirements Definition V&V process, objective evidence is developed to assess whether the stakeholder requirements:

a) Specify the required characteristics and context of use of services and operational concepts.

b) Define all constraints on a system solution.

c) Are traceable to the originating stakeholders.

d) Are complete, unambiguous, correct, and accurate.

e) Can be validated by measurable analyses or tests.

### 8.2.3 Activities and tasks

The V&V effort shall perform, as specified in Table 2b for the selected integrity level, the following Stakeholder Needs and Requirements Definition V&V activity and tasks described in Table 1b, Activity 8.2:

a) Stakeholder Needs and Requirements Definition V&V: This activity consists of the following tasks:

   1) Stakeholder Needs and Requirements Evaluation

   2) Traceability Analysis

   3) Criticality Analysis

   4) Hazard Analysis

   5) Security Analysis

   6) Risk Analysis

The Stakeholder Needs and Requirements Definition V&V tasks listed shall be used to verify and validate the Stakeholder Needs and Requirements Definition process outcomes described in ISO/IEC/IEEE 15288:2015(E) [B16]. The mappings of IEEE 1012 V&V tasks to ISO/IEC/IEEE 15288:2015(E) [B16] Stakeholder Needs and Requirements Definition process outcomes are contained in Annex L.

## 8.3 System Requirements Definition V&V process

### 8.3.1 Purpose

The purpose of the System Requirements Definition V&V process is to provide assurance that the outcomes of the System Requirements Definition process (ISO/IEC/IEEE 15288:2015(E) [B16]) have been achieved.

### 8.3.2 Outcomes

As a result of the successful implementation of the System Requirements Definition V&V process, objective evidence is developed to assess whether the system requirements:

a) Specify all required characteristics, attributes, functional and performance requirements, interface requirements, and requirements for qualification, safety and security, human factors engineering, and user documentation for the system.

b) Specify all constraints that will affect the architecture of the system and the means to realize the system.

c) Are unique, complete, unambiguous, consistent with all other requirements, implementable, and verifiable.

d) Are traceable to the stakeholder requirements.

e) Provide a basis (through analysis or test planning) for verifying that each system requirement can be satisfied.

### 8.3.3 Activities and tasks

The V&V effort shall perform, as specified in Table 2b for the selected integrity level, the following System Requirements Definition V&V activity and tasks described in Table 1b, Activity 8.3:

a) System Requirements Definition V&V: This activity consists of the following tasks:

1) Requirements Evaluation
2) Interface Analysis
3) Traceability Analysis
4) Criticality Analysis
5) System Integration Test Plan V&V
6) System Qualification Test Plan V&V
7) System Acceptance Test Plan V&V
8) Hazard Analysis
9) Security Analysis
10) Risk Analysis

The System Requirements Definition V&V tasks listed shall be used to verify and validate the System Requirements Definition process outcomes described in ISO/IEC/IEEE 15288:2015(E) [B16]. The mappings of IEEE 1012 V&V tasks to ISO/IEC/IEEE 15288 System Requirements Definition process outcomes are contained in Annex L.

## 8.4 Architecture definition V&V process

### 8.4.1 Purpose

The purpose of the Architecture Definition V&V process is to provide assurance that the outcomes of the Architecture Definition process (ISO/IEC/IEEE 15288:2015(E) [B16]) have been achieved.

### 8.4.2 Outcomes

As a result of the successful implementation of the Architecture Definition V&V process, objective evidence is developed to assess whether:

a) The system architecture (i.e., hardware, software, interfaces, and communication) satisfies the system requirements.

b) The system architecture is realizable.

c) The system architecture is based on specified selection criteria.

d) The basis for verifying the system elements is defined.

e) The basis for integration of the system elements is established.

### 8.4.3 Activities and tasks

The V&V effort shall perform, as specified in Table 2b for the selected integrity level, the following Architecture Definition V&V activity and tasks described in Table1b, Activity 8.4:

a) Architecture Definition V&V: This activity consists of the following tasks:

1) Architecture Evaluation
2) Interface Analysis
3) Requirements Allocation Analysis
4) Traceability Analysis
5) Criticality Analysis
6) System Integration Test Design V&V
7) System Qualification Test Design V&V
8) System Acceptance Test Design V&V
9) Hazard Analysis
10) Security Analysis
11) Risk Analysis

The Architecture Definition V&V tasks listed above shall be used to verify and validate the Architecture Definition process outcomes described in ISO/IEC/IEEE 15288:2015(E) [B16]. The mappings of IEEE 1012 V&V tasks to ISO/IEC/IEEE 15288 Architecture Definition process outcomes are contained in Annex L.

## 8.5 Design Definition V&V process

### 8.5.1 Purpose

The purpose of the Design Definition V&V process is to provide assurance that the outcomes of the Design Definition process (ISO/IEC/IEEE 15288:2015(E) [B16]) have been achieved.

### 8.5.2 Outcomes

As a result of the successful implementation of the Design Definition V&V process, objective evidence is developed to assess whether:

a) The design characteristics of each system element are defined.

b) The design enablers necessary for design definition are selected or defined.

c) The interfaces between system elements composing the system are defined or consolidated.

d) The system design is established.

e) Inputs for requirements of any enabling systems or system elements that serve the design definition activities are identified.

f) Any enabling systems or services needed for design definition are available.

g) Traceability of the design characteristics to the architectural elements of the system architecture is established.

### 8.5.3 Activities and tasks

The V&V effort shall perform, as specified in Table 2b for the selected integrity level, the following Design Definition V&V activity and tasks described in Table 1b, Activity 8.5:

a) Design Definition V&V: This activity consists of the following tasks:

1) Design Evaluation
2) Interface Analysis
3) Traceability Analysis
4) Criticality Analysis
5) System Integration Test Case V&V
6) System Qualification Test Case V&V
7) System Acceptance Test Case V&V
8) Hazard Analysis
9) Security Analysis
10) Risk Analysis

Design definition V&V culminates in defining periodic assessment of the design for managing the design from evolution of the system architecture to obsolescence of components and technologies.

The Design Definition process arrives at a solution that satisfies system requirements by defining system element, design enablers and interfaces. Requirements for enabling systems are defined, the design is baselined and traceability of the design characteristics to the elements of the system architecture is established.

The Design Definition V&V activity analyzes the characteristics, elements, interfaces, baseline, and inputs as well as traceability activities for the system under review and enabling systems.

The Design Definition V&V tasks listed shall be used to verify and validate the Design Definition process outcomes described in ISO/IEC/IEEE 15288:2015(E) [B16]. The mappings of IEEE 1012 V&V tasks to ISO/IEC/IEEE 15288 Design Definition process outcomes are contained in Annex L.

## 8.6 System analysis V&V process

### 8.6.1 Purpose

The purpose of the System Analysis V&V process is to provide assurance that the outcomes of the System Analysis process (ISO/IEC/IEEE 15288:2015(E) [B16]) have been achieved.

### 8.6.2 Outcomes

As a result of the successful implementation of the System Analysis V&V process, objective evidence is developed to assess whether:

a) The strategy for the system analysis is complete and is appropriate for the importance of the analysis.

b) The results of the system analysis support its conclusions and recommendations.

### 8.6.3 Activities and tasks

The V&V effort shall perform, as specified in Table 2b for the selected integrity level, the following System Analysis V&V activity and tasks described in Table 1b, Activity 8.6:

a) System Analysis V&V: This activity consists of the following tasks:

   1) System Analysis Strategy Evaluation

   2) System Analysis Results Evaluation

The System Analysis V&V process shall be performed for any specific implementation of the System Analysis process where the associated decision could affect a system or system element of the integrity level indicated in Table 2b.

The System Analysis V&V tasks listed shall be used to verify and validate the System Analysis process outcomes described in ISO/IEC/IEEE 15288:2015(E) [B16]. The mappings of IEEE 1012 V&V tasks to ISO/IEC/IEEE 15288 System Analysis process outcomes are contained in Annex L.

## 8.7 Implementation V&V process

### 8.7.1 Purpose

The purpose of the Implementation V&V process is to provide assurance that the outcomes of the Implementation process (ISO/IEC/IEEE 15288:2015(E) [B16]) have been achieved.

### 8.7.2 Outcomes

As a result of the successful implementation of the Implementation V&V process, objective evidence is developed to assess whether:

a) The implementation activities performed produce a system element that conforms to the system requirements.

b) The implementation correctly implements the design definition.

c) The system element has been implemented within the defined constraints.

d) The recorded evidence of implementation is complete and correct.

e) The system element has been packaged and stored in accordance with defined requirements.

### 8.7.3 Activities and tasks

The V&V effort shall perform, as specified in Table 2b for the selected integrity level, the following Implementation V&V activity and tasks described in Table 1b, Activity 8.7:

a) Implementation V&V: This activity consists of the following tasks:

1) Implementation Strategy Assessment
2) System Element Implementation Analysis
3) System Element Interaction Analysis
4) Criticality Analysis
5) System Integration Test Procedure V&V
6) System Qualification Test Procedure V&V
7) System Acceptance Test Procedure V&V
8) Hazard Analysis
9) Security Analysis
10) Risk Analysis

The Implementation V&V tasks are to monitor, review, audit, and analyze hardware and software products. If a hardware or software V&V is being conducted, the system V&V activities will use those V&V results to perform, in part or in whole, the system V&V activities.

The behavior (e.g., performance, security, hazard, interfaces) of each element may impact the behavior (e.g., by realized performance or lack of performance, or through direct or indirect coupling) of other elements in the system. Therefore, as each system element undergoes its own V&V, the V&V results assessing the actual behavior of that system element should be used to assess the behavior of other coupled system elements.

The Implementation V&V process should monitor the V&V results of each system element to assess if the elements are meeting their requirements. If a given system element is determined not to be able to meet all of its allocated requirements, requirements may need to be reallocated to other elements as a part of the systems engineering function. This reallocation scenario includes situations when COTS and GOTS products are selected as system elements and fall short of meeting all requirements. When this occurs, V&V tasks must be reiterated (repeated, redone) or recursively applied to the affected elements.

The Implementation V&V tasks listed shall be used to verify and validate the Implementation process outcomes described in ISO/IEC/IEEE 15288:2015(E) [B16]. The mappings of IEEE 1012 V&V tasks to ISO/IEC/IEEE 15288 Implementation process outcomes are contained in Annex L.

## 8.8 Integration V&V process

### 8.8.1 Purpose

The purpose of the Integration V&V process is to provide assurance that the outcomes of the Integration process (ISO/IEC/IEEE 15288:2015(E) [B16]) have been achieved.

### 8.8.2 Outcomes

As a result of the successful implementation of the Integration V&V process, objective evidence is developed to assess whether:

a) The system elements as described by the architecture definition, design definition and implementation are integrated correctly.

b) The integrated system meets the system requirements.

c) The system integration strategy is consistent with the system architecture.

d) The integration test plan and procedures are traceable to the system architecture.

e) The unavoidable constraints of integration that influence requirements are addressed correctly.

f) The integration of human performance into systems and their operation is correct.

g) Nonconformances due to integration actions are recorded and addressed.

### 8.8.3 Activities and tasks

The V&V effort shall perform, as specified in Table 2b for the selected integrity level, the following Integration V&V activity and tasks described in Table 1b, Activity 8.8:

a) Integration V&V: This activity consists of the following tasks:

1) System Integration Strategy Assessment

2) System Integration Test Execution V&V

3) System Element Interaction Analysis

4) System Qualification Test Execution V&V

The Integration V&V process should monitor each system element through element V&V results to assess if the elements are meeting their requirements, in a manner similar to Implementation V&V.

The Integration V&V tasks listed shall be used to verify and validate the Integration process outcomes described in ISO/IEC/IEEE 15288:2015(E) [B16]. The mappings of IEEE 1012 V&V tasks to ISO/IEC/IEEE 15288 Integration process outcomes are contained in Annex L.

## 8.9 Verification process

### 8.9.1 Purpose

The purpose of the Verification process is to provide objective evidence for whether the outcomes achieve the following:

a) Conform to requirements (e.g., for correctness, completeness, consistency, and accuracy) for all activities during each life cycle process.

b) Satisfy the standards, practices, and conventions during life cycle processes.

c) Successfully complete each life cycle activity and satisfy all the criteria for initiating succeeding life cycle activities (i.e., the product is built correctly).

### 8.9.2 Outcomes

As a result of successful implementation of the Verification process:

a) A Verification and Validation Plan is developed and implemented.

b) The system of interest and all components of the system of interest are assigned integrity levels that are reevaluated throughout the life cycle of the system.

c) The system and each of its components are evaluated for requirements satisfaction based on assigned integrity levels.

d) Objective evidence is developed to determine whether the system and each of its components conform to requirements and satisfy all the criteria for each successive life cycle activity.

### 8.9.3 Activities and tasks

The activities and tasks for the Verification process applied to the Technical processes of the System life cycle processes from ISO/IEC/IEEE 15288:2015(E) [B16] are described in Clause 8.1 (Business or Mission Analysis V&V process), Clause 8.2 (Stakeholder Needs and Requirements Definition V&V process), Clause 8.3 (System Requirements Definition V&V process), Clause 8.4 (Architecture Definition V&V process), Clause 8.5 (Design Definition V&V process), Clause 8.6 (System Analysis V&V process), Clause 8.7 (Implementation V&V process), Clause 8.8 (Integration V&V process), Clause 8.10 (Transition V&V process), Clause 8.12 (Operation V&V process), Clause 8.13 (Maintenance V&V process), and Clause 8.14 (Disposal V&V process).

## 8.10 Transition V&V process

### 8.10.1 Purpose

The purpose of the Transition V&V process is to provide assurance that the outcomes of the Transition process (ISO/IEC/IEEE 15288:2015(E) [B16]) have been achieved.

### 8.10.2 Outcomes

As a result of the successful implementation of the Transition V&V process, objective evidence is developed to assess whether:

a) The system transition strategy is comprehensive and explicitly documented.

b) The system is installed in its operational location in accordance with the transition plan.

c) The system delivers all specified services per its governing requirements.

d) The system is sustainable by enabling systems.

### 8.10.3 Activities and tasks

The V&V effort shall perform, as specified in Table 2b for the selected integrity level, the following Transition V&V activity and tasks described in Table 1b, Activity 8.10:

a) Transition V&V: This activity consists of the following tasks:

1) Transition Strategy Evaluation

2) Transition Demonstration Assessment

3) System Acceptance Test Execution V&V

The Transition V&V tasks listed shall be used to verify and validate the Transition process outcomes described in ISO/IEC/IEEE 15288:2015(E) [B16]. The mappings of IEEE 1012 V&V tasks to ISO/IEC/IEEE 15288 Transition process outcomes are contained in Annex L.

## 8.11 Validation process

### 8.11.1 Purpose

The purpose of the Validation process is to provide objective evidence for whether the outcomes achieve the following:

a) Satisfy system requirements allocated to the products at the end of each life cycle activity.

b) Solve the right problem (e.g., correctly model physical laws, implement business rules, and use the proper system assumptions).

c) Satisfy intended use and user needs in the operational environment (i.e., the correct product is built).

### 8.11.2 Outcomes

As a result of successful implementation of the Validation process:

a) A Verification and Validation Plan is developed and implemented.

b) The system of interest and all components of the system of interest are assigned integrity levels that are maintained throughout the life cycle of the system.

c) The system and each of its components are evaluated for satisfaction of allocated system requirements and of intended use and user needs based on assigned integrity levels.

d) Objective evidence is developed to determine whether the system and each of its components satisfy all allocated system requirements and meet intended use and user needs.

### 8.11.3 Activities and tasks

The activities and tasks for the Validation process applied to the Technical processes of the System life cycle processes from ISO/IEC/IEEE 15288:2015(E) [B16] are described in Clause 8.1 (Business or Mission Analysis V&V process), Clause 8.2 (Stakeholder Needs and Requirements Definition V&V process), Clause 8.3 (System Requirements Definition V&V process), Clause 8.4 (Architecture Definition V&V process), Clause 8.5 (Design Definition V&V process), Clause 8.6 (System Analysis V&V process), Clause 8.7 (Implementation V&V process), Clause 8.8 (Integration V&V process), Clause 8.10 (Transition V&V process), Clause 8.12 (Operation V&V process), Clause 8.13 (Maintenance V&V process), and Clause 8.14 (Disposal V&V process).

## 8.12 Operation V&V process

### 8.12.1 Purpose

The purpose of the Operation V&V process is to provide assurance that the outcomes of the Operation process (ISO/IEC/IEEE 15288:2015(E) [B16]) have been achieved.

### 8.12.2 Outcomes

As a result of the successful implementation of the Operation V&V process, objective evidence is developed to assess whether the operation strategy satisfies stakeholder requirements and needs.

### 8.12.3 Activities and tasks

The V&V effort shall perform, as specified in Table 2b for the selected integrity level, the following Operation V&V activity and tasks described in Table 1b, Activity 8.12:

a) Operation V&V: This activity consists of the following tasks:

1) Operating Procedures Evaluation
2) Hazard Analysis
3) Security Analysis
4) Risk Analysis

The Operation V&V tasks listed shall be used to verify and validate the Operation process outcomes described in ISO/IEC/IEEE 15288:2015(E) [B16]. The mappings of IEEE 1012 V&V tasks to ISO/IEC/IEEE 15288 Operation process outcomes are contained in Annex L.

## 8.13 Maintenance V&V process

### 8.13.1 Purpose

The purpose of the Maintenance V&V process is to provide assurance that the outcomes of the Maintenance process (ISO/IEC/IEEE 15288:2015(E) [B16]) have been achieved.

### 8.13.2 Outcomes

As a result of the successful implementation of the Maintenance V&V process, objective evidence is developed to assess whether:

a) The maintenance strategy is comprehensive and explicitly documented.
b) Corrective actions resolve the issue or negative trend.
c) The effect is assessed for corrective, adaptive, perfective, and preventive changes on stakeholder and system requirements, architecture, design, and implementation.
d) Evaluation is performed on problem reports, corrective actions, and trends to determine the possible corrective, adaptive, perfective, and preventive actions.

### 8.13.3 Activities and tasks

The V&V effort shall perform, as specified in Table 2b for the selected integrity level, the following Maintenance V&V tasks described in Table 1b, Activity 8.13:

a) Maintenance V&V: This activity consists of the following tasks:

1) System Maintenance Strategy Assessment
2) System Maintenance Execution Assessment

System modifications may be derived from requirements specified to correct errors (e.g., corrective), to adapt to a changed operating environment (e.g., adaptive), or to respond to additional user requests or enhancements (e.g., perfective). Modifications of the system shall be treated as development efforts and shall be verified and validated by performing V&V tasks corresponding to the modifications. Integrity level assignments shall be assessed as described in Clause 5. The integrity level assignments shall be revised as appropriate to reflect requirements derived from the Maintenance process.

The integrity level could be revised on the basis of corrective, perfective, or adaptive changes to the system if these changes modify the original integrity level of the system. If the integrity level is revised, then the effect of the revision on existing system requirements shall be evaluated to identify additional activities and tasks to be performed regressively on the system, software, and hardware. Corresponding V&V activities and tasks shall be identified to confirm that the system conforms to its required integrity level.

If system V&V were performed in accordance with this standard, then the maintenance process shall continue to conform to this standard. If the system were not verified and validated using this standard and appropriate documentation is not available or adequate, then the Maintenance V&V effort shall determine whether the missing or incomplete documentation should be generated. In making this determination of whether to generate missing documentation, the minimum V&V requirements of the assigned integrity level shall be taken into consideration.

The Maintenance V&V tasks listed shall be used to verify and validate the Maintenance process outcomes described in ISO/IEC/IEEE 15288:2015(E) [B16]. The mappings of IEEE 1012 V&V tasks to ISO/IEC/IEEE 15288 Maintenance process outcomes are contained in Annex L.

## 8.14 Disposal V&V process

### 8.14.1 Purpose

The purpose of the Disposal V&V process is to provide assurance that the outcomes of the Disposal process (ISO/IEC/IEEE 15288:2015(E) [B16]) have been achieved.

### 8.14.2 Outcomes

As a result of the successful implementation of the Disposal V&V process, objective evidence is developed to assess whether the Disposal plan:

a) Defines system boundaries and identifies system elements.

b) Is commensurate with the complexity and risk of the disposal and accounts for all system elements.

c) Addresses environmental considerations, applicable laws, regulations, and organizational policies and procedures.

### 8.14.3 Activities and tasks

The V&V effort shall perform, as specified in Table 2b for the selected integrity level, the following Disposal V&V activity and task described in Table 1b, Activity 8.14:

a) Disposal V&V: This activity consists of the following task:

   1) Disposal Plan Evaluation

The Disposal V&V task listed shall be used to verify and validate the Disposal process outcomes described in ISO/IEC/IEEE 15288:2015(E) [B16]. The mappings of IEEE 1012 V&V tasks to ISO/IEC/IEEE 15288 Disposal process outcomes are contained in Annex L.

## Table 1b—V&V tasks, inputs, and outputs

| 8.1 Activity: Business or Mission Analysis V&V (System, 15288—Business or Mission Analysis process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(1) Business or Mission Analysis Results Evaluation**<br>a) Evaluate the results of business or mission analysis for correctness, consistency, and completeness.<br>b) Verify and validate that the problem or opportunity space definition adheres to the organizational strategy.<br>c) Verify that the solution space characterization is consistent with the problem or opportunity space.<br>d) Verify that the preliminary life cycle concepts of the candidate solutions are consistent with the solution space.<br>e) Verify that the preferred candidate solution alternative(s) are selected.<br>f) Verify and validate that inputs for requirements of any enabling systems or system elements that serve the business or mission analysis activities are identified.<br>g) Verify availability of enabling systems or services needed for business or mission analysis. | Business or mission analysis results<br>Organization strategy<br>Organizational concept of operations<br>Organizational strategic goals and plans<br>New market or mission elements<br>Identified problem or opportunity space<br>Identified solution space<br>Identified candidate solution(s)<br>Organizational processes and procedures | Task report(s)—Business or mission analysis results evaluation<br>Anomaly report(s) |
| **(2) Traceability Analysis**<br>a) Establish the root of traceability, starting with the organization strategy.<br>b) Verify that the problem or opportunity space traces back to the organization strategy.<br>c) Verify that the solution space traces back to the problem or opportunity space.<br>d) Verify that the candidate solution(s) traces back to the solution space. | Business or mission analysis results<br>Organization strategy<br>Organizational concept of operations<br>Identified problem or opportunity space<br>Identified solution space<br>Preferred candidate solution(s) | Task report(s)—Root of traceability<br>Anomaly report(s) |
| **(3) Criticality Analysis**<br>a) Determine whether integrity levels are established for the identified solution space.<br>b) Verify that the assigned integrity levels are correct. If integrity levels are not assigned, then assign integrity levels to the solution space.<br>c) Determine whether integrity levels are established for the preferred candidate solutions.<br>d) Verify that the assigned integrity levels are correct. If integrity levels are not assigned, then assign integrity levels to the preferred candidate solution(s). Preferred candidate solutions. | Identified problem or opportunity space<br>Identified solution space<br>Preferred candidate solution(s) | Task report(s)—Criticality analysis<br>Anomaly report(s) |
| **(4) Hazard Analysis**<br>Analyze the potential hazards to and from the preferred candidate solutions. The analysis shall perform the following:<br>a) Identify the potential solution hazards.<br>b) Assess the consequences of each hazard. | Preferred candidate solution(s) | Task report(s)—Hazard analysis<br>Anomaly report(s) |

| 8.1 Activity: Business or Mission Analysis V&V (System, 15288—Business or Mission Analysis process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| c) Assess the probability of each hazard.<br>d) Identify mitigation strategies for each hazard. | | |
| **(5) Security Analysis**<br>a) Review the preferred candidate solution(s) to determine an acceptable level of security risk.<br>b) Analyze the preferred candidate solution(s) from a security perspective and assure that potential security risks with respect to confidentiality (disclosure of sensitive information/data), integrity (modification of information/data), availability (withholding of information or services), and accountability (attributing actions to an individual/process) have been identified. Include an assessment of the sensitivity of the information/data to be processed.<br>c) Analyze security risks introduced by the preferred candidate solution(s). | Preferred candidate solution(s)<br>Preliminary threat and risk assessment (TRA) | Task report(s)—Security analysis<br>Anomaly report(s) |
| **(6) Risk Analysis**<br>a) Identify the technical and management risks.<br>b) Provide recommendations to eliminate, reduce, or mitigate the risks. | Preferred candidate solution(s)<br>Hazard analysis report<br>Security analysis report<br>V&V task results | Task report(s)—Risk analysis<br>Anomaly report(s) |

| 8.2 Activity: Stakeholder Needs and Requirements Definition V&V (System, 15288—Stakeholder Needs and Requirements Definition process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(1) Stakeholder Needs and Requirements Evaluation**<br>Evaluate the stakeholder requirements for correctness, consistency, completeness, readability, and testability. The task criteria are as follows:<br>a) Correctness<br>1) Verify and validate that the requirements satisfy the stakeholder needs for the system.<br>2) Verify that the requirements comply with standards, references, regulations, policies, physical laws, and business rules.<br>3) Validate that the requirements define the intended interaction of the system with its operating environment and other interfacing systems.<br>4) Validate the suitability of the preferred candidate solution(s) to meet the stakeholder requirements.<br>b) Consistency<br>1) Verify that all terms, concepts, and requirements are documented consistently in accordance with accepted syntax and structure (e.g., style guides and requirements modeling structure).<br>2) Verify that there is consistency between assumptions, requirements, and between groups of requirements.<br>c) Completeness<br>1) Validate that performance criteria and functionality are described in the requirements, within the assumptions and | Preferred candidate solution(s)<br>Stakeholders requirements<br>Concept documentation<br>Organizational processes and procedures | Task report(s)—Stakeholder requirements evaluation<br>Anomaly report(s) |

| 8.2 Activity: Stakeholder Needs and Requirements Definition V&V (System, 15288—Stakeholder Needs and Requirements Definition process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| constraints of the operating environment and system boundaries.<br>2) Verify that all stakeholders, or stakeholder classes (used here as groupings of stakeholders), are identified.<br>3) Verify that the stakeholder requirements satisfy specified configuration management procedures. Verify stakeholder requirements are in a form suitable for requirements management throughout the life cycle.<br>d) Readability<br>1) Verify that the documentation is legible, understandable, and unambiguous to the intended audience.<br>2) Verify that the documentation defines all acronyms, mnemonics, abbreviations, terms, and symbols.<br>e) Testability<br>1) Verify that objective acceptance criteria can be developed to validate the requirements. | | |
| **(2) Traceability Analysis**<br>a) Verify that all requirements are traceable to one or more preferred candidate solutions.<br>b) Verify that all requirements are traceable to one or more stakeholders or stakeholder classes. | Preferred candidate solution(s)<br>Stakeholders requirements<br>Concept documentation | Task report(s)—Traceability report<br>Anomaly report(s) |
| **(3) Criticality Analysis**<br>a) Determine whether system integrity levels are established for stakeholder and system requirements, detailed functions, subsystems, or other partitions.<br>b) Verify that the assigned system integrity levels are correct. If system integrity levels are not assigned, then assign system integrity levels to the stakeholder requirements.<br>c) Document the system integrity level assigned to stakeholder requirements. For V&V planning purposes, the system shall be assigned the same integrity level as the highest level assigned to any individual stakeholder requirement. | Stakeholders requirements<br>Concept documentation | Task report(s)—Criticality analysis<br>Anomaly report(s) |
| **(4) Hazard Analysis**<br>a) Analyze the potential hazards to and from the conceptual system. The analysis shall perform the following:<br>b) Identify the potential system hazards.<br>c) Assess the consequences of each hazard.<br>d) Assess the probability of each hazard.<br>e) Identify mitigation strategies for each hazard. | Stakeholders requirements<br>Concept documentation | Task report(s)—Hazard analysis<br>Anomaly report(s) |
| **(5) Security Analysis**<br>a) Review the system owner's definition of an acceptable level of security risk.<br>b) Analyze the system concept from a security perspective and assure that potential security risks with respect to confidentiality (disclosure of sensitive information/data), integrity (modification of information/data), availability (withholding of information or services), and accountability (attributing actions to an individual/process) have been identified. Include an assessment of the sensitivity of the | Stakeholders requirements<br>Concept documentation<br>Preliminary threat and risk assessment (TRA) | Task report(s)—Security analysis<br>Anomaly report(s) |

| 8.2 Activity: Stakeholder Needs and Requirements Definition V&V (System, 15288—Stakeholder Needs and Requirements Definition process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| information/data to be processed.<br>c) Analyze security risks introduced by the system itself as well as those associated with the environment with which the system interfaces. | | |
| **(6) Risk Analysis**<br>a) Identify the technical and management risks.<br>b) Provide recommendations to eliminate, reduce, or mitigate the risks. | Stakeholders requirements<br>Concept documentation<br>Supplier development plans and schedules<br>Hazard analysis report<br>Security analysis report<br>V&V task results | Task report(s)—Risk analysis<br>Anomaly report(s) |

| 8.3 Activity: System Requirements Definition V&V (System, 15288—System Requirements Definition process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(1) Requirements Evaluation**<br>Evaluate the system requirements for correctness, consistency, completeness, readability, and testability. The task criteria are as follows:<br>a) Correctness<br>1) Verify and validate that the required characteristics, attributes, constraints (e.g., mechanical, electrical, mass, thermal, data, procedural flows), and functional and performance requirements for a product solution are correct (e.g., security, ergonomics, human-machine interface, safety, reliability, maintainability, response time).<br>2) Verify and validate that the system requirements satisfy the stakeholder requirements.<br>3) Verify that the system requirements comply with standards, references, regulations, policies, physical laws, and business rules.<br>4) Validate that the system requirements define the intended interaction of the system with its operating environment and other interfacing systems.<br>b) Consistency<br>1) Verify that all terms, concepts, and requirements are documented consistently in accordance with accepted syntax and structure (e.g., style guides and requirements modeling structure).<br>2) Verify that there is consistency among the requirements, groups of requirements (functional interaction), and assumptions.<br>c) Completeness<br>1) Validate that all stakeholder needs are satisfied by the set of system requirements. | Stakeholders requirements<br>System requirements<br>Concept documentation<br>Organizational processes and procedures | Task report(s)—Requirements evaluation<br>Anomaly report(s) |

| 8.3 Activity: System Requirements Definition V&V (System, 15288—System Requirements Definition process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| 2) Validate that performance criteria and functionality are described in the requirements, within the assumptions and constraints of the operating environment and system boundaries.<br>3) Verify that the System requirements satisfy specified configuration management procedures. Verify that system requirements are in a form suitable for requirements management throughout the life cycle.<br>d) Readability<br>1) Verify that the documentation is legible, understandable, and unambiguous to the intended audience.<br>2) Verify that the documentation defines all acronyms, mnemonics, abbreviations, terms, and symbols.<br>e) Testability<br>1) Verify that objective acceptance criteria can be developed to validate the requirements. | | |
| **(2) Interface Analysis**<br>Verify and validate that the requirements for system interfaces with other systems are correct, complete, and testable. The task criteria are as follows:<br>a) Correctness<br>Validate the external interface requirements, including information to be exchanged.<br>b) Completeness<br>Verify that all external interface requirements are defined.<br>c) Testability<br>Verify that objective acceptance criteria can be developed to validate the requirements. | System requirements<br>Stakeholders requirements<br>Organizational processes and procedures | Task report(s)—Interface analysis<br>Anomaly report(s) |
| **(3) Traceability Analysis**<br>Verify that the traceability analysis is complete. The task criteria are as follows:<br>a) All system requirements are traceable to one or more stakeholder requirements.<br>b) All stakeholder requirements are traceable to one or more system requirements. | System requirements<br>Stakeholders requirements | Task report(s)—Traceability analysis<br>Anomaly report(s) |
| **(4) Criticality Analysis**<br>Review and update the existing criticality analysis results from the prior criticality task report using the stakeholder requirements and system requirements. | Criticality task report<br>System requirements<br>Stakeholders requirements | Task report(s)—Criticality analysis<br>Anomaly report(s) |
| **(5) System Integration Test Plan V&V**<br>a) System elements of integrity level 4<br>1) Plan V&V system integration testing to validate that the system element correctly implements the system requirements and design as each system element is incrementally integrated with other elements.<br>2) Plan tracing of system requirements to test designs, cases, procedures, and results.<br>3) Plan documentation of test designs, cases, procedures, and results.<br>4) The V&V system integration test plan shall address the | System requirements<br>Stakeholders requirements<br>System integration test plan | V&V system integration test plan (integrity level 4)<br>Task report(s)—Review of system integration test plan (integrity levels 3 and 2)<br>Anomaly report(s) |

| 8.3 Activity: System Requirements Definition V&V (System, 15288—System Requirements Definition process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| following:<br>i) Conformance to increasingly larger set of functional requirements at each stage of integration.<br>ii) Assessment of timing, sizing, and accuracy.<br>iii) Performance at boundaries and under stress conditions.<br>iv) Measures of requirements test coverage and system reliability.<br>5) Verify that the V&V system integration test plan conforms to project-defined test document purpose, format, and content (e.g., IEEE Std 829™-2008 [B3]).<br>6) Validate that the V&V system integration test plan satisfies the following criteria:<br>i) Traceable to the system requirements.<br>ii) External consistency with the system requirements.<br>iii) Internal consistency.<br>iv) Test coverage of the system requirements.<br>v) Appropriateness of test standards and methods used.<br>vi) Conformance to expected results.<br>vii) Feasibility of system integration testing.<br>viii) Feasibility of operation and maintenance (e.g., capability to be operated and maintained in accordance with user needs).<br>b) System elements of integrity levels 3 and 2<br>1) Verify that the developer's system integration test plan conforms to the project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>2) Validate that the developer's system integration test plan satisfies the following criteria:<br>i) Traceable to the system requirements.<br>ii) External consistency with the system requirements.<br>iii) Internal consistency.<br>iv) Test coverage of the system requirements.<br>v) Appropriateness of test standards and methods.<br>vi) Conformance to expected results.<br>c) System elements of integrity level 1<br>There are no system integration V&V test plan requirements. | | |
| **(6) System Qualification Test Plan V&V**<br>a) System integrity level 4<br>1) Plan V&V system qualification testing to validate the system against system requirements. The resulting V&V system qualification test plan shall address the following:<br>i) Tracing of system requirements to test designs, cases, procedures, and results.<br>ii) Documentation of test designs, cases, procedures, and results.<br>iii) Satisfaction of all system requirements (e.g., functional, performance, security, operation, and maintenance) in the system environment.<br>iv) Adequacy of user documentation (e.g., training | System requirements<br>Stakeholders requirements<br>System qualification test plan (developer's) | V&V system qualification test plan (integrity level 4)<br>Task report(s)—Review of system qualification test plan (integrity levels 3 and 2)<br>Anomaly report(s) |

| 8.3 Activity: System Requirements Definition V&V (System, 15288—System Requirements Definition process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| materials, procedural changes, and user guides).<br>v) Performance at boundaries (e.g., data and interfaces) and under stress conditions.<br>vi) Conformance to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>vii) Test coverage of system requirements.<br>viii) Expected results.<br>b) System integrity levels 3 and 2<br>1) Verify that the developer's system qualification test plan satisfies the following criteria:<br>i) Conformance to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>ii) Test coverage of system requirements.<br>2) Verify that the developer's system qualification test plan addresses the following:<br>i) Appropriateness of test methods and standards used.<br>ii) Expected results.<br>iii) Feasibility of system qualification testing.<br>iv) Capability to be operated and maintained.<br>c) System integrity level 1<br>There are no system qualification V&V test plan requirements. | | |
| **(7) System Acceptance Test Plan V&V**<br>a) System integrity level 4<br>1) Plan V&V system acceptance testing to validate that the system correctly implements system requirements in the intended operational environment or as close to the intended operational environment as possible. The resulting V&V system acceptance test plan shall address the following:<br>i) Tracing of acceptance test requirements to test design, cases, procedures, and execution results.<br>ii) Documentation of test tasks and results.<br>iii) Conformance to acceptance requirements in the operational environment (limitations of testing).<br>iv) Adequacy of user documentation (e.g., training materials, procedural changes, user guides).<br>v) Conformance to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>vi) Test coverage of acceptance requirements.<br>vii) Expected results.<br>b) System integrity levels 3 and 2<br>1) Verify that the acquirer's system acceptance test plan conforms to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>2) Verify that the acquirer's system acceptance test plan addresses the following:<br>i) Test coverage of acceptance requirements. | System requirements<br>Stakeholders requirements<br>System acceptance test plan (acquirer's) | V&V system acceptance test plan (integrity level 4)<br>Task report(s)—Review of system acceptance test plan (integrity levels 3 and 2)<br>Anomaly report(s) |

| 8.3 Activity: System Requirements Definition V&V (System, 15288—System Requirements Definition process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| ii) Expected results.<br>iii) Feasibility of operation and maintenance (e.g., capability to be operated and maintained in accordance with user needs).<br>c) System integrity level 1<br>There are no system acceptance V&V test plan requirements. | | |
| **(8) Hazard Analysis**<br>Analyze the potential hazards to and from the stakeholder requirements. The analysis shall perform the following:<br>a) Identify the potential system hazards.<br>b) Assess the consequences of each hazard.<br>c) Assess the likelihood of each hazard.<br>d) Identify mitigation strategies for each hazard. | System requirements<br>Stakeholders requirements<br>Concept documentation<br>Hazard analysis report | Task report(s)—Hazard analysis<br>Anomaly report(s) |
| **(9) Security Analysis**<br>a) Review the system owner's definition of an acceptable level of security risk.<br>b) Analyze the stakeholder requirements from a security perspective and assure that potential security risks with respect to confidentiality (disclosure of sensitive information/data), integrity (modification of information/data), availability (withholding of information or services), and accountability (attributing actions to an individual/process) have been identified. Include an assessment of the sensitivity of the information/data to be processed.<br>c) Analyze security risks introduced by the system itself as well as those associated with the environment with which the system interfaces. | System requirements<br>Stakeholders requirements<br>Concept documentation<br>Preliminary threat and risk assessment (TRA)<br>Security analysis report | Task report(s)—Security analysis<br>Anomaly report(s) |
| **(10) Risk Analysis**<br>a) Identify the technical and management risks.<br>b) Provide recommendations to eliminate, reduce, or mitigate the risks. | System requirements<br>Stakeholders requirements<br>Concept documentation<br>Supplier development plans and schedules<br>Hazard analysis report<br>Security analysis report<br>Risk analysis report<br>V&V task results | Task report(s)—Risk analysis<br>Anomaly report(s) |

| 8.4 Activity: Architecture Definition V&V (System, 15288—Architecture Definition process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(1) Architecture Evaluation**<br>Evaluate the system architecture(s) for correctness, consistency, completeness, and testability. The task criteria are as follows:<br>a) Correctness<br>1) Verify the characteristics, attributes, constraints, and | System requirements<br>Business needs<br>Architecture models and views | Task report(s)—Architecture evaluation<br>Anomaly report(s) |

| 8.4 Activity: Architecture Definition V&V (System, 15288—Architecture Definition process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| functional and performance requirements of the selected architecture(s) correctly implement the system requirements.<br>2) Verify the selected architecture(s) complies with standards, regulations, policies, physical laws, and business rules.<br>3) Validate the product solution(s) defined by the system architecture(s) satisfies the stakeholder needs.<br>4) Validate that the selected architecture(s) and its element interactions do not result in unnecessary, unintended, or deleterious consequences.<br>5) Validate the selected architecture(s) defines the intended interaction of the system with its operating environment.<br>b) Consistency<br>1) Verify the selected architecture(s) conforms to the architectural guidance, principles, and tenets of the organization processes and procedures (e.g., service-oriented architecture, modular open-systems architecture).<br>2) Verify the architectural principles, characteristics, and rules established for the system are being applied across the selected architecture(s).<br>c) Completeness<br>1) Verify the system functions are allocated to the elements of the selected architecture(s).<br>2) Verify all system requirements are included in the selected architecture(s).<br>NOTE—Typically, the Stakeholder Needs and Requirements Definition, System Requirements Definition, Architecture Definition and Design Definition processes are recursively applied to successive levels of detail in the system architecture and design until elements are completely defined. | Architecture trade-off analyses<br>Organizational processes and procedures | |
| **(2) Interface Analysis**<br>Verify and validate the architectural interfaces between system elements and with other systems are correct and complete. The task criteria are:<br>a) Correctness<br>1) Verify the system architecture satisfies the system interface requirements between system elements.<br>2) Validate the system architecture satisfies the system interface requirements with external systems (external system boundaries).<br>b) Completeness<br>Verify the architecture describes all internal and external interfaces. | System requirements<br>Architecture models and views | Task report(s)—Interface analysis<br>Anomaly report(s) |
| **(3) Requirements Allocation Analysis**<br>Verify the correctness and completeness of the system requirements allocation to the hardware, software, and user interfaces against user needs.<br>a) Correctness<br>Verify that the system requirements allocated to software and hardware elements can be accomplished by the designated element. Review the allocations to verify that tradeoff considerations of significance (e.g., reliability, maintainability, safety, robustness, and cost effectiveness) were factored into | User needs<br>Concept documentation<br>System requirements<br>Architecture models and views | Task report(s)—Requirements allocation analysis<br>Anomaly report(s) |

| 8.4 Activity: Architecture Definition V&V (System, 15288—Architecture Definition process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| architecture decisions.<br>b) Completeness<br>Verify that each system requirement is allocated to at least one system element or user. | | |
| **(4) Traceability Analysis**<br>Verify that the traceability analysis is complete. The task criteria are as follows:<br>a) Verify that all architectural elements are traceable to one or more system requirements.<br>b) Verify that all system requirements are traceable to one or more architectural elements. | System requirements<br>Architecture models and views | Task report(s)—Traceability analysis<br>Anomaly report(s) |
| **(5) Criticality Analysis**<br>a) Review and update the existing criticality analysis results from the prior criticality task report using the system architectural definition to assign a system integrity level to each architectural element.<br>b) Implementation methods and interfacing technologies may cause previously assigned system integrity levels to be raised or lowered for a given stakeholder or system requirement. Verify that no inconsistent or undesired system integrity consequences are introduced by reviewing the revised system integrity levels. | Criticality task report<br>System requirements<br>Architecture models and views | Task report(s)—Criticality analysis<br>Anomaly report(s) |
| **(6) System Integration Test Design V&V**<br>a) System integrity level 4<br>1) Design tests for V&V system integration testing.<br>2) Continue tracing required by the V&V system integration test plan. Verify that the V&V system integration test designs conform to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>3) Validate that the V&V system integration test designs satisfy the criteria in V&V activity 8.3, Task 5.<br>b) System integrity levels 3 and 2<br>1) Verify that the developer's test designs for system integration testing conform to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>2) Validate that the developer's system integration test designs satisfy the criteria in V&V activity 8.3, Task 5.<br>c) System integrity level 1<br>There are no system integration V&V test design requirements. | System requirements<br>Architecture models and views<br>System integration test design | V&V system integration test design(s) (integrity level 4)<br>Task report(s)—Review of system integration test design (integrity levels 3 and 2)<br>Anomaly report(s) |
| **(7) System Qualification Test Design V&V**<br>a) System integrity level 4<br>1) Design tests for V&V system qualification testing.<br>2) Continue tracing required by the V&V system qualification test plan. Verify that the V&V system acceptance test designs conform to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>3) Validate that the V&V system qualification test designs satisfy the criteria in V&V activity 8.3, Task 6.<br>b) System integrity levels 3 and 2<br>1) Verify that the developer's test designs for system | System requirements<br>Architecture models and views<br>System qualification test design | V&V system qualification test design(s) (integrity level 4)<br>Task report(s)—Review of system qualification test design (integrity levels 3 and 2)<br>Anomaly report(s) |

| 8.4 Activity: Architecture Definition V&V (System, 15288—Architecture Definition process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| qualification testing conform to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>2) Verify that the developer's system qualification test designs satisfy the criteria in V&V activity 8.3, Task 6.<br>c) System integrity level 1<br>There are no system qualification V&V test design requirements. | | |
| **(8) System Acceptance Test Design V&V**<br>a) System integrity level 4<br>1) Design tests for V&V system acceptance testing.<br>2) Continue tracing required by the V&V system acceptance test plan. Verify that the V&V system acceptance test designs conform to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>3) Validate that the V&V system acceptance test designs satisfy the criteria in V&V activity 8.3, Task 7.<br>b) System integrity levels 3 and 2<br>1) Verify that the acquirer's test designs for system acceptance testing conform to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>2) Validate that the acquirer's system acceptance test designs satisfy the criteria in V&V activity 8.3, Task 7.<br>c) System integrity level 1<br>There are no system acceptance V&V test plan requirements. | System requirements<br>Architecture models and views<br>System acceptance test design | V&V system acceptance test design(s) (integrity level 4)<br>Task report(s)—Review of system acceptance test design (integrity levels 3 and 2)<br>Anomaly report(s) |
| **(9) Hazard Analysis**<br>Analyze the potential hazards to and from the conceptual system. The analysis shall perform the following:<br>a) Identify the potential system hazards.<br>b) Assess the consequences of each hazard.<br>c) Assess the probability of each hazard.<br>d) Assess the identified mitigation strategies to verify each hazard is prevented, mitigated, or controlled. (Any unmitigated hazards are documented and addressed as part of system operations.) | Architecture models and views<br>Hazard analysis report | Task report(s)—Hazard analysis<br>Anomaly report(s) |
| **(10) Security Analysis**<br>a) Review the system owner's definition of an acceptable level of security risk.<br>b) Analyze the system requirements from a security perspective and assure that potential security risks with respect to confidentiality (disclosure of sensitive information/data), integrity (modification of information/data), availability (withholding of information or services), and accountability (attributing actions to an individual/process) have been identified. Include an assessment of the sensitivity of the information/data to be processed.<br>c) Analyze security risks introduced by the system itself as well as those associated with the environment with which the system interfaces.<br>d) Verify the identified security threats and vulnerabilities are prevented, controlled, or mitigated (any unmitigated threats and | Architecture models and views<br>Preliminary threat and risk assessment (TRA)<br>Security analysis report | Task report(s)—Security analysis<br>Anomaly report(s) |

| 8.4 Activity: Architecture Definition V&V (System, 15288—Architecture Definition process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| vulnerabilities are documented and addressed as part of system operations). | | |
| **(11) Risk Analysis**<br>a) Identify the technical and management risks.<br>b) Provide recommendations to eliminate, reduce, or mitigate the risks. | Architecture models and views<br>Supplier development plans and schedules<br>Hazard analysis report<br>Security analysis report<br>Risk analysis report<br>V&V task results | Task report(s)—Risk analysis<br>Anomaly report(s) |

| 8.5 Activity: Design Definition V&V (System, 15288—Design Definition process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(1) Design Evaluation**<br>Evaluate the system design for correctness, consistency, completeness, and testability. The task criteria are as follows:<br>a) Correctness<br>1) Verify the characteristics, attributes, constraints, and functional and performance requirements of the system design correctly implements the architecture definition.<br>2) Verify the system design complies with standards, regulations, policies, physical laws, and business rules.<br>3) Validate the product solution(s) defined by the system design satisfies the stakeholder needs.<br>4) Validate that the system design and its element interactions do not result in unnecessary, unintended, or deleterious consequences.<br>5) Validate the system design defines the intended interaction of the system with its operating environment.<br>b) Consistency<br>1) Verify the system design conforms to the design guidance, principles, and tenets of the organization processes and procedures (e.g., service-oriented architecture, modular open-systems architecture).<br>2) Verify the design principles, characteristics, and rules established for the system are being applied across the system design.<br>c) Completeness<br>1) Verify the system requirements are allocated to the elements of the system design.<br>2) Verify all system requirements are included in the system design.<br>NOTE—Typically, the Stakeholder Needs and Requirements Definition, System Requirements Definition, Architecture Definition and Design Definition processes are recursively applied to successive levels of detail in the system architecture and design until elements are completely defined. | System requirements<br>Business needs<br>Architecture models and views<br>Architecture trade-off analyses<br>Design documents<br>Organizational processes and procedures | Task report(s)—Design evaluation<br>Anomaly report(s) |

| 8.5 Activity: Design Definition V&V (System, 15288—Design Definition process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(2) Interface Analysis**<br>Verify the design interfaces between system elements and with other systems are correct and complete. The task criteria are:<br>a) Correctness<br>1) Verify the system design satisfies the system interface requirements between system elements.<br>2) Validate the system design satisfies the system interface requirements with external systems (external system boundaries).<br>b) Completeness<br>1) Verify the system design describes all internal and external interfaces. | System requirements<br>Design documents | Task report(s)—Interface analysis<br>Anomaly report(s) |
| **(3) Traceability Analysis**<br>Verify that the traceability analysis is complete. The task criteria are as follows:<br>a) Verify that all design elements are traceable to one or more architectural elements.<br>b) Verify that all architectural elements are traceable to one or more design elements. | Architecture models and views<br>Design documents | Task report(s)—Traceability analysis<br>Anomaly report(s) |
| **(4) Criticality Analysis**<br>a) Review and update the existing criticality analysis results from the prior criticality task report using the system design to assign a system integrity level to each design element.<br>b) Implementation methods and interfacing technologies may cause previously assigned system integrity levels to be raised or lowered for a given stakeholder or system requirement. Verify that no inconsistent or undesired system integrity consequences are introduced by reviewing the revised system integrity levels. | Criticality task report<br>System requirements<br>Design documents | Task report(s)—Criticality analysis<br>Anomaly report(s) |
| **(5) System Integration Test Case V&V**<br>a) System integrity level 4<br>1) Develop test cases for V&V system integration testing.<br>2) Continue tracing required by the V&V system integration test plan.<br>3) Verify that the system integration V&V test cases conform to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>4) Validate that the V&V system integration test cases satisfy the criteria in V&V activity 8.3, Task 5.<br>b) System integrity levels 3 and 2<br>1) Verify that the developer's system integration test cases conform to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>2) Validate that the developer's system integration test cases satisfy the criteria in V&V activity 8.3, Task 5.<br>c) System integrity level 1<br>There are no system integration test case V&V requirements. | System requirements<br>Design documents<br>System integration test cases | V&V system integration test cases (integrity level 4)<br>Task report(s)—Review of system integration test cases (integrity levels 3 and 2)<br>Anomaly report(s) |

| 8.5 Activity: Design Definition V&V (System, 15288—Design Definition process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(6) System Qualification Test Case V&V**<br>a) System integrity level 4<br>1) Develop test cases for V&V system qualification testing.<br>2) Continue tracing required by the V&V system qualification test plan.<br>3) Verify that the V&V system qualification test cases conform to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>4) Validate that the V&V system qualification test cases satisfy the criteria in V&V activity 8.3, Task 6.<br>b) System integrity levels 3 and 2<br>1) Verify that the developer's system qualification test cases conform to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>2) Validate that the developer's system qualification test cases satisfy the criteria in V&V activity 8.3, Task 6.<br>c) System integrity level 1<br>There are no system qualification test case V&V requirements. | System requirements<br>Design documents<br>System qualification test cases | V&V system qualification test cases (integrity level 4)<br>Task report(s)—Review of system qualification test cases (integrity levels 3 and 2)<br>Anomaly report(s) |
| **(7) System Acceptance Test Case V&V**<br>a) System integrity level 4<br>1) Develop test cases for V&V system acceptance testing.<br>2) Continue tracing required by the V&V system acceptance test plan.<br>3) Verify that the V&V system acceptance test cases conform to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>4) Validate that the V&V system acceptance test cases satisfy the criteria in V&V activity 8.3, Task 7.<br>b) System integrity levels 3 and 2<br>1) Verify that the acquirer's system acceptance test cases conform to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>2) Verify that the acquirer's system acceptance test cases satisfy the criteria in V&V activity 8.3, Task 7.<br>c) System integrity level 1<br>There are no system acceptance test case V&V requirements. | System requirements<br>Design documents<br>System acceptance test cases | V&V system acceptance test cases (integrity level 4)<br>Task report(s)—Review of system acceptance test cases (integrity levels 3 and 2)<br>Anomaly report(s) |
| **(8) Hazard Analysis**<br>a) Analyze the potential hazards to and from the conceptual system. The analysis shall perform the following:<br>b) Identify the potential system hazards.<br>c) Assess the consequences of each hazard.<br>d) Assess the probability of each hazard.<br>e) Assess the identified mitigation strategies to verify each hazard is prevented, mitigated, or controlled (any unmitigated hazards are documented and addressed as part of system operations). | Design documents<br>Hazard analysis report | Task report(s)—Hazard analysis<br>Anomaly report(s) |
| **(9) Security Analysis**<br>a) Review the system owner's definition of an acceptable level of security risk.<br>b) Analyze the system concept from a security perspective and assure that potential security risks with respect to | Design documents<br>Preliminary threat and risk assessment (TRA)<br>Subsystems security | Task report(s)—Security analysis<br>Anomaly report(s) |

| 8.5 Activity: Design Definition V&V (System, 15288—Design Definition process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| confidentiality (disclosure of sensitive information/data), integrity (modification of information/data), availability (withholding of information or services), and accountability (attributing actions to an individual/process) have been identified. Include an assessment of the sensitivity of the information/data to be processed.<br>c) Analyze security risks introduced by the system itself as well as those associated with the environment with which the system interfaces.<br>d) Verify the identified security threats and vulnerabilities are prevented, controlled, or mitigated (any unmitigated threats and vulnerabilities are documented and addressed as part of system operations). | analysis<br>Security analysis report | |
| **(10) Risk Analysis**<br>a) Identify the technical and management risks.<br>b) Provide recommendations to eliminate, reduce, or mitigate the risks. | Design documents<br>Supplier development plans and schedules<br>Hazard analysis report<br>Security analysis report<br>Risk analysis report<br>V&V task results | Task report(s)—Risk analysis<br>Anomaly report(s) |

| 8.6 Activity: System Analysis V&V (System, 15288—System Analysis process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(1) System Analysis Strategy Evaluation**<br>Evaluate the system analysis strategy for completeness and for consistency with the criticality of the system or system element. The task criteria are as follows:<br>a) Completeness<br>1) Verify that the scope of the system analysis addresses all aspects related to the decision.<br>2) Verify that all assumptions have been identified and are correct.<br>3) Verify that any inputs for enabling systems or services have been identified and are available.<br>4) Verify that any inputs for enabling system have been identified and are available in the system analysis strategy plan.<br>b) Consistency with Criticality<br>Verify that the rigor and approach specified in the system analysis strategy is consistent with that needed for the system or system elements that could be affected by the decision. | System analysis strategy | Task report(s)—System analysis strategy evaluation |
| **(2) System Analysis Results Evaluation**<br>Evaluate the results of the system analysis to determine that the analysis was conducted as specified in the strategy and the results support its conclusions and recommendations. | System analysis strategy<br>System analysis results | Task report(s)—System analysis results evaluation |

| 8.7 Activity: Implementation V&V (System, 15288—Implementation process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(1) Implementation Strategy Assessment**<br>a) Verify that the implementation strategy accounts for all implementation procedures (e.g., technical manuals, organizational policies, or standards), fabrication processes, tools and equipment, implementation tolerances, and verification uncertainties needed to construct the system element.<br>b) Verify that the implementation strategy defines the limitations and constraints imposed on the system element design solution.<br>c) Verify that execution of the implementation strategy will produce a system element that conforms to the system element description in the system design. | Implementation strategy<br>Implementation procedures<br>Fabrication processes, tools and equipment<br>System element description from the system design | Task report(s)—Implementation strategy assessment<br>Anomaly report(s) |
| **(2) System Element Implementation Analysis**<br>a) V&V of system element requirements<br>1) System elements of integrity levels 4 and 3<br>i) Verify (e.g., through analysis, reviews, and audits) that integrity level 4 and 3 element requirements trace to system requirements.<br>ii) Verify (e.g., through analysis, reviews, and audits) that the element requirements satisfy the integrity level 4 and 3 system requirements.<br>2) System elements of integrity level 2<br>Verify (e.g., through reviews and audits) that the element requirements satisfy the level 2 system requirements.<br>3) System elements of integrity level 1<br>There are no system element requirements V&V requirements.<br>b) V&V of system element design<br>1) System elements of integrity level 4<br>i) Verify that the design of integrity level 4 element is consistent with the system design.<br>ii) Verify that the design of the integrity level 4 element satisfies the requirements of the system element.<br>2) System elements of integrity levels 3 and 2<br>Verify that the design of each element is consistent with the system design.<br>3) System elements of integrity level 1<br>There are no system element design V&V requirements.<br>c) V&V of system element implementation<br>1) System elements of integrity level 4<br>Begin pre-integration testing using early partial deliveries of system elements (software and hardware) to derive early visibility into potential system integration testing issues and to initiate corrective changes to system element's development to correct or mitigate the potential system integration issue(s).<br>2) System elements of integrity levels 4 and 3<br>Evaluate the system element artifacts (requirements, design, anomaly reports/trends, element performance metrics, schedule compliance, resource usage actuals, and projected resource needs) produced from the software/hardware development life cycle process to | Concept documentation<br>System requirements<br>Software requirements specification(s)<br>Software interface requirements specification(s)<br>Hardware requirements specification(s)<br>System design<br>Software design documents(s)<br>Hardware drawings<br>System element(s)<br>Software traceability analysis<br>Hardware traceability analysis | Task report(s)—System element implementation analysis<br>Anomaly report(s) |

| 8.7 Activity: Implementation V&V (System, 15288—Implementation process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| perform the following:<br>i) Derive an evolving assessment of each system element's performance (i.e., preview of how well the system element is meeting its requirements) and to recommend corrective actions (i.e., feedback to element development process or change to system architecture) to mitigate any projected performance shortfalls.<br>ii) Assess each system element's project schedule performance (i.e., estimated system element schedule completion dates for system element milestone reviews and delivery dates) and to recommend system schedule changes if the system element project completion dates are slipping.<br>iii) Estimate remaining schedule resource requirements (i.e., labor or equipment budget) if performance or schedule shortfalls are projected.<br>3) System elements of integrity levels 2 and 1<br>There are no system element implementation V&V requirements.<br>d) V&V of system element integration testing<br>1) System elements of integrity level 4<br>Verify through independently produced objective evidence (e.g., independent test) that integrity level 4 requirements in that element are satisfied by the system element hardware/software integration testing.<br>2) System elements of integrity levels 3 and 2<br>Verify through the data produced by the development organization (e.g., reviews, audits) that the integrity levels 3 and 2 requirements in that element are satisfied by the system element hardware/software integration testing.<br>3) System elements of integrity levels 1<br>There are no system element integration testing V&V requirements.<br>e) V&V of system element qualification testing<br>1) System elements of integrity level 4<br>i) Develop V&V test cases for system element qualification testing.<br>ii) Continue tracing required by the system element V&V test plan.<br>iii) Verify that the system element V&V test cases conform to project-defined test document purpose, format, and content.<br>iv) Validate that the system element V&V test cases satisfy the criteria in system element V&V qualification test plan generation activity.<br>2) System elements of integrity levels 3 and 2<br>Review the results of the developer's qualification testing.<br>3) System elements of integrity level 1<br>There are no system element qualification testing V&V requirements.<br>f) V&V of system element acceptance testing | | |

| 8.7 Activity: Implementation V&V (System, 15288—Implementation process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| 1) System elements of integrity level 4<br>i) Plan acceptance V&V testing to validate that the system element correctly implements system requirements in an operational environment.<br>ii) Design tests for acceptance V&V testing.<br>iii) Develop test cases for acceptance V&V testing.<br>iv) Perform acceptance V&V testing.<br>v) Analyze test results to validate that the system element satisfies the V&V test acceptance criteria.<br>2) System elements of integrity levels 3 and 2<br>Review the acquirer's acceptance test results to validate that the system element satisfies the test acceptance criteria.<br>3) System elements of integrity level 1<br>There are no system element acceptance testing V&V requirements. | | |
| **(3) System Element Interaction Analysis**<br>The System Element Interaction Analysis shall analyze the results of each element V&V to determine whether directly or indirectly coupled system elements require their V&V tasks to be reiterated (repeated, redone) or new V&V tasks performed. As each element V&V results are determined, V&V may have to be recursively applied to all directly or indirectly coupled system elements. The System Analysis process may be used to establish the criteria of how to recursively apply V&V to system elements. | System element implementation analysis results<br>System architecture<br>System design | Task report(s)—System element interaction analysis<br>Anomaly report(s)<br>V&V Plan update (if tasks are added or changed) |
| **(4) Criticality Analysis**<br>a) Review and update the existing criticality levels of the system elements during the implementation process based on the implementation of the software and hardware components.<br>b) Verify that no inconsistent or undesired system element integrity consequences have been introduced due to implementation methods and interfacing technologies that may cause previously assigned system element integrity levels to be raised or lowered. | Criticality task report<br>System element requirements, designs, and implementations | Task report(s)—Criticality analysis<br>Anomaly report(s) |
| **(5) System Integration Test Procedure V&V**<br>a) System integrity level 4<br>1) Develop test procedures for V&V system integration testing.<br>2) Continue tracing required by the V&V system integration test plan.<br>3) Verify that the V&V system integration test procedures conform to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>4) Validate that the V&V system integration test procedures satisfy the criteria in V&V activity 8.3, Task 5.<br>b) System integrity levels 3 and 2<br>1) Verify that the developer's system integration test procedures conform to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>2) Validate that the developer's system integration test procedures satisfy the criteria in V&V activity 8.3, Task 5. | System requirements<br>Design documents<br>System integration test cases | V&V system integration test procedures (integrity level 4)<br>Task report(s)—Review of system integration test procedures (integrity levels 3 and 2)<br>Anomaly report(s) |

| 8.7 Activity: Implementation V&V (System, 15288—Implementation process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| c) System integrity level 1<br>There are no system integration test procedure V&V requirements. | | |
| **(6) System Qualification Test Procedure V&V**<br>a) System integrity level 4<br>1) Develop test procedures for V&V system qualification testing.<br>2) Continue tracing required by the V&V system qualification test plan.<br>3) Verify that the V&V system qualification test procedures conform to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>4) Validate that the V&V system qualification test procedures satisfy the criteria in V&V activity 8.3, Task 6.<br>b) System integrity levels 3 and 2<br>1) Verify that the developer's system qualification test procedures conform to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>2) Validate that the developer's system qualification test procedures satisfy the criteria in V&V activity 8.3, Task 6.<br>c) System integrity level 1<br>There are no system qualification test case V&V requirements. | System requirements<br>Design documents<br>System qualification test cases | V&V system qualification test procedures (integrity level 4)<br>Task report(s)—Review of system qualification test procedures (integrity levels 3 and 2)<br>Anomaly report(s) |
| **(7) System Acceptance Test Procedure V&V**<br>a) System integrity level 4<br>1) Develop test procedures for V&V system acceptance testing.<br>2) Continue the tracing required by the V&V system acceptance test plan.<br>3) Verify that the V&V system acceptance test procedures conform to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>4) Validate that the V&V system acceptance test procedures satisfy the criteria in V&V activity 8.3, Task 7.<br>b) System integrity levels 3 and 2<br>1) Verify that the acquirer's system acceptance test procedures conform to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>2) Verify that the acquirer's system acceptance test procedures satisfy the criteria in V&V activity 8.3, Task 7.<br>c) System integrity level 1<br>There are no system acceptance test case V&V requirements. | System requirements<br>Design documents<br>System acceptance test cases | V&V system acceptance test procedures (integrity level 4)<br>Task report(s)—Review of system acceptance test procedures (integrity levels 3 and 2)<br>Anomaly report(s) |
| **(8) Hazard Analysis**<br>a) Verify the system elements that implement critical requirements introduce no new hazards.<br>b) Update the hazard analysis.<br>c) Assess the identified mitigation strategies to verify each hazard is prevented, mitigated, or controlled (any unmitigated hazards are documented and addressed as part of system operations). | Subsystems<br>Hazard analysis report | Task report(s)—Hazard analysis<br>Anomaly report(s) |

| 8.7 Activity: Implementation V&V (System, 15288—Implementation process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(9) Security Analysis**<br>a) Verify that the system element is implemented in accordance with the system architecture in that it addresses the identified security risks and that the implementation does not introduce new security risks.<br>b) Verify the identified security threats and vulnerabilities are prevented, controlled, or mitigated (any unmitigated threats and vulnerabilities are documented and addressed as part of system operations). | System architecture<br>Subsystems<br>Security analysis report<br>V&V task results | Task report(s)—Security analysis<br>Anomaly report(s) |
| **(10) Risk Analysis**<br>Review and update risk analysis using prior task reports. Provide recommendations to eliminate, reduce, or mitigate the risks. | Subsystems<br>Hazard analysis report<br>Security analysis report<br>Risk analysis report | Task report(s)—Risk analysis<br>Anomaly report(s) |

| 8.8 Activity: Integration V&V (System, 15288—Integration process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(1) System Integration Strategy Assessment**<br>a) Verify the system integration strategy.<br>b) Verify the constraints on the system requirements and design due to the integration strategy.<br>c) Integration test specification and procedure generation. | System integration strategy<br>System architecture<br>System requirements | Task report(s)—System integration strategy assessment<br>Anomaly report(s) |
| **(2) System Integration Test Execution V&V**<br>a) System integrity level 4<br>1) Perform V&V system integration testing.<br>2) Use the V&V system integration test results to validate that the system satisfies the test acceptance criteria.<br>3) Document the results as required by the V&V system integration test plan.<br>4) Use the V&V system integration test results to validate that the system satisfies the test acceptance criteria.<br>5) Document discrepancies between the actual and expected test results.<br>b) System integrity levels 3 and 2<br>Use the developer's system integration test results to verify that the system satisfies the test acceptance criteria.<br>c) System integrity level 1<br>There are no system integration test execution V&V requirements. | Integration sequence and strategy (e.g., test scenario inputs, test procedure sequence)<br>Hardware element(s)<br>Software element(s)<br>Other external system element(s) | V&V system integration test execution results (integrity level 4)<br>Task report(s)—Review of system integration test execution (integrity levels 3 and 2)<br>Anomaly report(s) |
| **(3) System Element Interaction Analysis**<br>The System Element Interaction Analysis shall analyze the results of system integration V&V to determine whether directly or indirectly coupled system elements require their V&V tasks to be reiterated (repeated, redone) or new V&V tasks performed. As integration results are determined, V&V may have to be recursively applied to all directly or indirectly coupled system elements. The System Analysis process may be used to establish the criteria of how to recursively apply V&V to system elements. | System integration results<br>System architecture<br>System design | Task report(s)—System element interaction analysis<br>Anomaly report(s)<br>V&V Plan update (if tasks are added or changed) |

| 8.8 Activity: Integration V&V (System, 15288—Integration process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(4) System Qualification Test Execution V&V**<br>a) System integrity level 4<br>1) Perform V&V system qualification testing.<br>2) Use the V&V system qualification test results to validate that the system satisfies the test acceptance criteria.<br>3) Document discrepancies between the V&V system qualification test results and the test acceptance criteria.<br>4) Complete the traceability by documenting the location of the V&V system qualification test results.<br>5) Analyze test results to validate that the system delivers required services when installed in its operational location and staffed by operators. Additionally, the often less formally expressed but sometimes overriding attitudes, experience, and subjective tests that comprise customer satisfaction also need consideration.<br>6) Document the results as required by the V&V system qualification test plan.<br>b) System integrity levels 3 and 2<br>Use the developer's system qualification test results to verify that the acceptance criteria are satisfied.<br>c) System integrity level 1<br>There are no system qualification test execution V&V requirements. | Stakeholders requirements<br>System requirements<br>Concept documentation<br>System qualification test results | V&V system qualification test execution results (integrity level 4)<br>Task report(s)—Review of system qualification test execution (integrity levels 3 and 2)<br>Anomaly report(s) |

| 8.9 Verification (System, 15288—Verification process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| The activities and tasks for the system Verification process are conducted in system technical life cycle processes, and are contained in Table 1b, Activity 8.1 (Business or Mission Analysis V&V), Activity 8.2 (Stakeholder Needs and Requirements Definition V&V), Activity 8.3 (System Requirements Definition V&V), Activity 8.4 (Architecture Definition V&V), Activity 8.5 (Design Definition V&V), Activity 8.6 (System Analysis V&V), Activity 8.7 (Implementation V&V), Activity 8.8 (Integration V&V), Activity 8.10 (Transition V&V), Activity 8.12 (Operation V&V), Activity 8.13 (Maintenance V&V) and Activity 8.14 (Disposal V&V). The system verification activities and tasks in Table 1b and the common verification activities and tasks in Table 1a represent all verification activities and tasks needed to perform system verification. | The required inputs for the system Verification process are found in Table 1b required inputs. | The required outputs for the system Verification process are found in Table 1b required outputs. |

| 8.10 Activity: Transition V&V (System, 15288—Transition process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| NOTE—If system transition is taking place by parts then the transition process V&V tasks should be executed for each of the parts. | | |
| **(1) Transition Strategy Evaluation**<br>a) Verify that the transition strategy is comprehensive. Verify that the transition strategy includes the following:<br>1) All the system parts and the system as a whole (e.g., hardware [HW]/software [SW] functionality and databases) are considered in the transition execution. | Transition strategy<br>Installation package (e.g., user documentation, system requirements, SDD, | Task report(s)—Transition plan evaluation<br>Anomaly report(s) |

| 8.10 Activity: Transition V&V (System, 15288—Transition process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| 2) Transition schedule and sequence.<br>3) Identification of transition hardware and software tools, equipment, and instructions.<br>4) Archiving system artifacts, such as documentation and code.<br>5) Impact of interacting systems in terms of transition timing and transition impacts.<br>6) Continuity of capabilities when replacing or upgrading a legacy system.<br>7) Site preparation for installation and legacy system retirement, storage, and/or incorporation.<br>8) Provisions for documentation of the process results.<br>9) A fallback position, in case of transition failure (e.g., going back to the old system) and other risk mitigation considerations.<br>b) Verify that the transition strategy has a defined approach to establishing the system in the operational environment that is consistent with stakeholder requirements (e.g., by running the old and new systems in parallel or by well-defined system characteristics that can be compared). | IDD, SRS, IRS, concept documentation, installation procedures, site-specific parameters, installation tests, and configuration management data) | |
| **(2) Transition Demonstration Assessment**<br>a) Validate that acceptance tests defined in the acquirer agreement (as documented in the acceptance test plan) demonstrate satisfactory installation at the specified location(s). Where the exact location or environment of operation is not available, a representative example is selected.<br>b) Verify and validate that the installed system (software and hardware elements) and related site-specific parameters are identical to the final as-verified and as-validated system (software and hardware elements). | Transitioning system (operational system under test)<br>User documentation<br>Installation package (e.g., user documentation, system requirements, SDD, IDD, SRS, IRS, concept documentation, installation procedures, site-specific parameters, installation tests, and configuration management data)<br>Acquirer agreement<br>Acceptance test plan | Task report(s)—Transition demonstration assessment<br>Anomaly report(s) |
| **(3) System Acceptance Test Execution V&V**<br>a) System integrity level 4<br>1) Perform V&V system acceptance testing.<br>2) Use the system V&V acceptance test results to validate that the system satisfies the test acceptance criteria.<br>3) Document discrepancies between the V&V system acceptance test results and the test acceptance criteria.<br>4) Complete the traceability by documenting the location of the V&V system acceptance test results.<br>5) Analyze test results to validate that the system delivers required services when installed in its operational location and staffed by operators. Additionally, the often less formally expressed but sometimes overriding attitudes, | Stakeholders requirements<br>System requirements<br>Concept documentation<br>System acceptance test results | V&V system acceptance test execution results (integrity level 4)<br>Task report(s)—System acceptance test execution V&V (integrity levels 3 and 2)<br>Anomaly report(s) |

| 8.10 Activity: Transition V&V (System, 15288—Transition process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| experience, and subjective tests that comprise customer satisfaction also need consideration.<br>6) Document the results as required by the V&V system acceptance test plan.<br>b) System integrity levels 3 and 2<br>Use the acquirer's system acceptance test results to verify that the system satisfies the test acceptance criteria.<br>c) System integrity level 1<br>There are no system acceptance test execution V&V requirements. | | |

| 8.11 Validation (System, 15288—Validation process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| The activities and tasks for the system Validation process are conducted in system technical life cycle processes, and are contained in Table 1b, Activity 8.1 (Business or Mission Analysis V&V), Activity 8.2 (Stakeholder Needs and Requirements Definition V&V), Activity 8.3 (System Requirements Definition V&V), Activity 8.4 (Architecture Definition V&V), Activity 8.5 (Design Definition V&V), Activity 8.6 (System Analysis V&V), Activity 8.7 (Implementation V&V), Activity 8.8 (Integration V&V), Activity 8.10 (Transition V&V), Activity 8.12 (Operation V&V), Activity 8.13 (Maintenance V&V) and Activity 8.14 (Disposal V&V). The system Validation activities and tasks in Table 1b and the common Validation activities and tasks in Table 1a represent all Validation activities and tasks needed to perform system validation. | The required inputs for the system Validation process are found in Table 1b required inputs. | The required outputs for the system Validation process are found in Table 1b required outputs. |

| 8.12 Activity: Operation V&V (System, 15288—Operation process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(1) Operating Procedures Evaluation**<br>a) Verify that the operating procedures are consistent with the user documentation and conform to the system requirements.<br>b) Evaluate new or revised constraints or changes in the environment (e.g., operational requirements, platform characteristics, and operating environment) on the system requirements to verify the applicability of the System VVP (see Annex H). | Concept documentation<br>Operating procedures<br>User documentation<br>System VVP<br>Constraints<br>Environmental changes | Task report(s)—Operating procedures evaluation<br>Anomaly report(s)<br>Updated security analysis |
| **(2) Hazard Analysis**<br>a) Verify that the operating procedures (e.g., instructions to the operator or user, standard operating procedures, abnormal operating procedures, safety procedures, and emergency operating procedures) and operational environment do not introduce new hazards.<br>b) Assess the identified mitigation strategies to verify each hazard is prevented, mitigated, or controlled (any unmitigated hazards are documented and addressed as part of system operations).<br>c) Update the hazard analysis. | Operating procedures<br>Hazard analysis report | Task report(s)—Hazard analysis<br>Anomaly report(s) |
| **(3) Security Analysis**<br>a) Verify that no new security risks are introduced due to changes in the operational environment. | New constraints<br>Environmental changes | Task Reports—Security analysis |

| 8.12 Activity: Operation V&V (System, 15288—Operation process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| b) Verify the identified security threats and vulnerabilities are prevented, controlled, or mitigated (any unmitigated threats and vulnerabilities are documented and addressed as part of system operations).<br>c) Over time, changes in external interfaces, threats, or technology in general require that an updated security analysis be performed to determine an updated residual risk. | Operating procedures<br>Security analysis report | |
| **(4) Risk Analysis**<br>a) Review and update risk analysis using prior task reports.<br>b) Provide recommendations to eliminate, reduce, or mitigate the risks. | Installation package<br>Proposed changes<br>Hazard analysis report<br>Security analysis report<br>Risk analysis report<br>Supplier development plans and schedules<br>Operation problem reports<br>V&V task results | Task report(s)—Risk Analysis<br>Anomaly report(s) |

| 8.13 Activity: Maintenance V&V (System, 15288—Maintenance process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(1) System Maintenance Strategy Assessment**<br>a) Verify the system maintenance strategy.<br>b) Verify the constraints on the system requirements and design due to the maintenance strategy. | System maintenance strategy<br>System performance data<br>System requirements | Task report(s)—System maintenance strategy analysis<br>Corrective actions assessment<br>Anomaly report(s) |
| **(2) System Maintenance Execution Assessment**<br>a) Verify the maintenance operational strategy results by monitoring the system maintenance execution.<br>b) Evaluate the maintenance operational strategy results.<br>c) Stakeholder requirements evaluation.<br>d) Requirements.<br>e) Traceability analysis.<br>f) Criticality analysis.<br>g) Hazard analysis.<br>h) Security analysis.<br>i) Risk analysis.<br>j) Interface analysis.<br>k) Design evaluation.<br>l) System element implementation analysis.<br>m) Integration analysis.<br>n) System test analysis (integration, qualification, and acceptance).<br>o) System installation analysis.<br>p) Operation transition analysis. | System maintenance strategy (e.g., operational availability requirements, system failure, suspension of services) | Task report(s)—System maintenance execution assessment and quality metrics<br>Anomaly report(s) |
| NOTE—System changes are maintenance activities (see Clause 8.13). | | |

| 8.14 Activity: Disposal V&V (System, 15288—Disposal process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(1) Disposal Plan Evaluation**<br>a) Verify that system boundaries are defined and all relevant system elements (information, hardware, media, etc.) are identified.<br>b) Verify that disposal has been planned to a degree commensurate with the complexity and risk of the disposal and all that identified elements are accounted for in the plan.<br>c) Verify that environmental considerations, all applicable laws, regulations, and organizational policies and procedures, as well as other constraints are identified and communicated to relevant stakeholders.<br>d) Verify that system elements to be stored have available billets and established retention criteria. | Concept documentation<br>Configuration repository<br>Inventory records<br>Disposal plan<br>Applicable laws<br>Organizational policies and procedures<br>List of constraints<br>Management and technical decisions | Task report(s)—System description<br>Task report(s)—Constraints<br>Task report(s)—Disposal plan<br>Anomaly report(s) |

NOTE (for Table 1b)—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 2b—Minimum V&V tasks assigned to each integrity level for system V&V**

| V&V Activities | Activity: Business or Mission Analysis V&V (see 8.1) | | | | Activity: Stakeholder Needs and Requirements Definition V&V (see 8.2) | | | | Activity: System Requirements Definition (see 8.3) | | | | Activity: Architecture Definition V&V (see 8.4) | | | | Activity: Design Definition V&V (see 8.5) | | | | Activity: System Analysis V&V (see 8.6) | | | | Activity: Implementn V&V (see 8.7) | | | | Activity: Integration V&V (see 8.8) | | | | Activity: Transition V&V (see 8.10) | | | | Activity: Operation V&V (see 8.12) | | | | Activity: Maintenance V&V (see 8.13) | | | | Activity: Disposal V&V (see 8.14) | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Integrity Levels | Levels | | | | Levels | | | | Levels | | | | Levels | | | | Levels | | | | Levels | | | | 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 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 |
| Architecture Evaluation | | | | | | | | | | | | | X | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Business or Mission Analysis Results Evaluation | X | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Criticality Analysis | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X | | X | X | X | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | |
| Design Evaluation | | | | | | | | | | | | | | | | | X | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Disposal Plan Evaluation | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | X | X | X | X |
| Hazard Analysis | X | X | | | X | X | | | X | X | | | X | X | | | X | X | | | | | | | X | X | | | | | | | | | | | X | X | | | | | | | | |
| Implementation Strategy Assessment | | | | | | | | | | | | | | | | | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | |
| Interface Analysis | | | | | | | | | X | X | X | | X | X | X | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Operating Procedures Evaluation | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Requirements Allocation Analysis | | | | | | | | | | | | | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Requirements Evaluation | | | | | | | | | X | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Risk Analysis | X | X | | | X | X | | | X | X | | | X | X | | | X | X | | | | | | | X | X | | | | | | | | | | | X | X | | | | | | | | |
| Security Analysis | X | X | | | X | X | | | X | X | | | X | X | | | X | X | | | | | | | X | X | | | | | | | | | | | X | X | | | | | | | | |
| Stakeholder Needs and Requirements Evaluation | | | | | X | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| System Acceptance Test Case V&V | | | | | | | | | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| System Acceptance Test Design V&V | | | | | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| V&V Activities | Activity: Business or Mission Analysis V&V (see 8.1) | | | | Activity: Stakeholder Needs and Requirements Definition V&V (see 8.2) | | | | Activity: System Requirements Definition (see 8.3) | | | | Activity: Architecture Definition V&V (see 8.4) | | | | Activity: Design Definition V&V (see 8.5) | | | | Activity: System Analysis V&V (see 8.6) | | | | Activity: Implementn V&V (see 8.7) | | | | Activity: Integration V&V (see 8.8) | | | | Activity: Transition V&V (see 8.10) | | | | Activity: Operation V&V (see 8.12) | | | | Activity: Maintenance V&V (see 8.13) | | | | Activity: Disposal V&V (see 8.14) | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Integrity Levels | Levels | | | | Levels | | | | Levels | | | | Levels | | | | Levels | | | | Levels | | | | 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 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 |
| System Acceptance Test Execution V&V | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | X | X | X | | | | | | | | | | | | | |
| System Acceptance Test Plan V&V | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| System Acceptance Test Procedure V&V | | | | | | | | | | | | | | | | | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | |
| System Analysis Results Evaluation | | | | | | | | | | | | | | | | | | | | | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | |
| System Analysis Strategy Evaluation | | | | | | | | | | | | | | | | | | | | | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | |
| System Element Implementation Analysis | | | | | | | | | | | | | | | | | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | |
| System Element Interaction Analysis | | | | | | | | | | | | | | | | | | | | | | | | | X | X | X | | X | X | X | | | | | | | | | | | | | | | | |
| System Integration Strategy Assessment | | | | | | | | | | | | | | | | | | | | | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | |
| System Integration Test Case V&V | | | | | | | | | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| System Integration Test Design V&V | | | | | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| System Integration Test Execution V&V | | | | | | | | | | | | | | | | | | | | | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | |
| System Integration Test Plan V&V | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| System Integration Test Procedure V&V | | | | | | | | | | | | | | | | | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | |
| System Maintenance Execution Assessment | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | X | X | X | | | | |
| System Maintenance Strategy Assessment | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | X | X | X | | | | |
| System Qualification Test Case V&V | | | | | | | | | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| V&V Activities | Activity: Business or Mission Analysis V&V (see 8.1) | | | | Activity: Stakeholder Needs and Requirements Definition V&V (see 8.2) | | | | Activity: System Requirements Definition (see 8.3) | | | | Activity: Architecture Definition V&V (see 8.4) | | | | Activity: Design Definition V&V (see 8.5) | | | | Activity: System Analysis V&V (see 8.6) | | | | Activity: Implementn V&V (see 8.7) | | | | Activity: Integration V&V (see 8.8) | | | | Activity: Transition V&V (see 8.10) | | | | Activity: Operation V&V (see 8.12) | | | | Activity: Maintenance V&V (see 8.13) | | | | Activity: Disposal V&V (see 8.14) | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Integrity Levels | Levels | | | | Levels | | | | Levels | | | | Levels | | | | Levels | | | | Levels | | | | 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 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 |
| System Qualification Test Design V&V | | | | | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| System Qualification Test Execution V&V | | | | | | | | | | | | | | | | | | | | | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | |
| System Qualification Test Plan V&V | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| System Qualification Test Procedure V&V | | | | | | | | | | | | | | | | | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | |
| Traceability Analysis | X | X | X | | X | X | X | | X | X | X | | X | X | X | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Transition Demonstration Assessment | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | X | X | X | | | | | | | | | |
| Transition Strategy Evaluation | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | X | X | X | | | | | | | | | |

NOTE (for Table 2b)—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 analysis or test. Higher integrity level implementation requires greater rigor (e.g., formal methods and structured analysis methods), intensity (e.g., consideration of all system conditions and system environment states), and depth (e.g., abnormal cases, boundary conditions, and comprehensive fault and recovery scenarios) of analysis or test than the lower integrity level implementation.

The recommended applicability of optional tasks to the System V&V processes described in Clause 8 is shown in Table 3a. Annex G provides a description of each of the optional V&V tasks.

**Table 3b—Optional V&V tasks and suggested applications in system technical processes**

| | Business or Mission Analysis (8.1) | Stakeholder Needs and Requirements Definition (8.2) | System Requirements Definition (8.3) | Architecture Definition (8.4) | Design Definition (8.5) | System Analysis (8.6) | Implementation (8.7) | Integration (8.8) | Transition (8.10) | Operation (8.12) | Maintenance (8.13) | Disposal (8.14) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Algorithm analysis | | | X | X | | | X | | | | X | |
| Audit performance | | | X | X | | | X | X | X | | X | |
| Audit support | | | X | X | | | X | X | X | | X | |
| Control flow analysis | | | X | X | | | X | | | | X | |
| Cost analysis | | X | X | X | | | X | X | X | | X | |
| Database analysis | | | X | X | | | X | X | X | | X | |
| Data flow analysis | | | X | X | | | X | | | | X | |
| Disaster recovery plan assessment | | X | X | X | | | X | | | X | X | X |
| Distributed architecture assessment | | X | X | X | | | | | | | X | |
| Exploratory testing | X | X | X | X | X | X | X | X | X | X | X | |
| Feasibility study evaluation | | X | X | X | | | | | | | X | |
| Independent risk assessment | | | | | | | | | | | X | |
| Inspection | | | | | | | | | | | | |
| Inspection—Concept | | X | | | | | | | | | X | |
| Inspection—Requirements | | | X | | | | | | | | X | |
| Inspection—Design | | | | X | | | | | | | X | |
| Inspection—Source code | | | | | | | | | | | | |
| Inspection—Test plan | | | X | X | | | X | X | X | | X | |
| Inspection—Test design | | | | X | | | X | X | X | | X | |
| Inspection—Test case | | | | X | | | X | X | X | | X | |
| Operational evaluation | | | | | | | | | | X | | |
| Performance monitoring | | X | X | X | | | X | X | X | X | X | X |
| Post-installation validation | | | | | | | | | | X | X | |
| Project management oversight support | | X | X | X | | | X | X | X | X | X | X |
| Proposal evaluation support | | | | | | | | | | | | |
| Qualification testing | | | | | | | X | | X | | | |
| Regression analysis and testing | | | X | X | | | X | X | X | | X | |
| Reusability analysis | | X | X | X | | | X | | | | X | |
| Reuse analysis | | X | X | X | | | | | | | X | |
| Simulation analysis | | X | X | X | | | X | X | X | X | X | X |
| Sizing and timing analysis | | | X | X | | | X | X | X | | X | |
| System software assessment | | | | X | | | X | X | X | X | X | |
| Test certification | | | | | | | X | X | X | X | X | X |
| Test evaluation | | | X | X | | | X | X | X | X | X | X |
| Test witnessing | | | | | | | X | X | X | X | X | X |
| Training documentation evaluation | | | X | X | | | X | X | X | X | X | X |
| Usability analysis | | X | X | X | | | X | X | X | X | X | |
| User documentation evaluation | | X | X | X | | | X | X | X | X | X | |
| User training | | | | | | | X | X | X | X | X | |
| V&V tool plan generation | | | | | | | | | | | | |
| V&V tool qualification | | X | X | X | | | X | X | X | X | X | |

| | Business or Mission Analysis (8.1) | Stakeholder Needs and Requirements Definition (8.2) | System Requirements Definition (8.3) | Architecture Definition (8.4) | Design Definition (8.5) | System Analysis (8.6) | Implementation (8.7) | Integration (8.8) | Transition (8.10) | Operation (8.12) | Maintenance (8.13) | Disposal (8.14) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Walkthrough | | | | | | | | | | | | |
| Walkthrough—Design | | | | X | | | | | | | X | |
| Walkthrough—Requirements | | | X | | | | | | | | X | |
| Walkthrough—Source code | | | | | | | | | | | | |
| Walkthrough—Test | | | | | | | X | X | | | X | |
| Work Breakdown Structure (WBS) Evaluation | | | | | | | | | | | | |

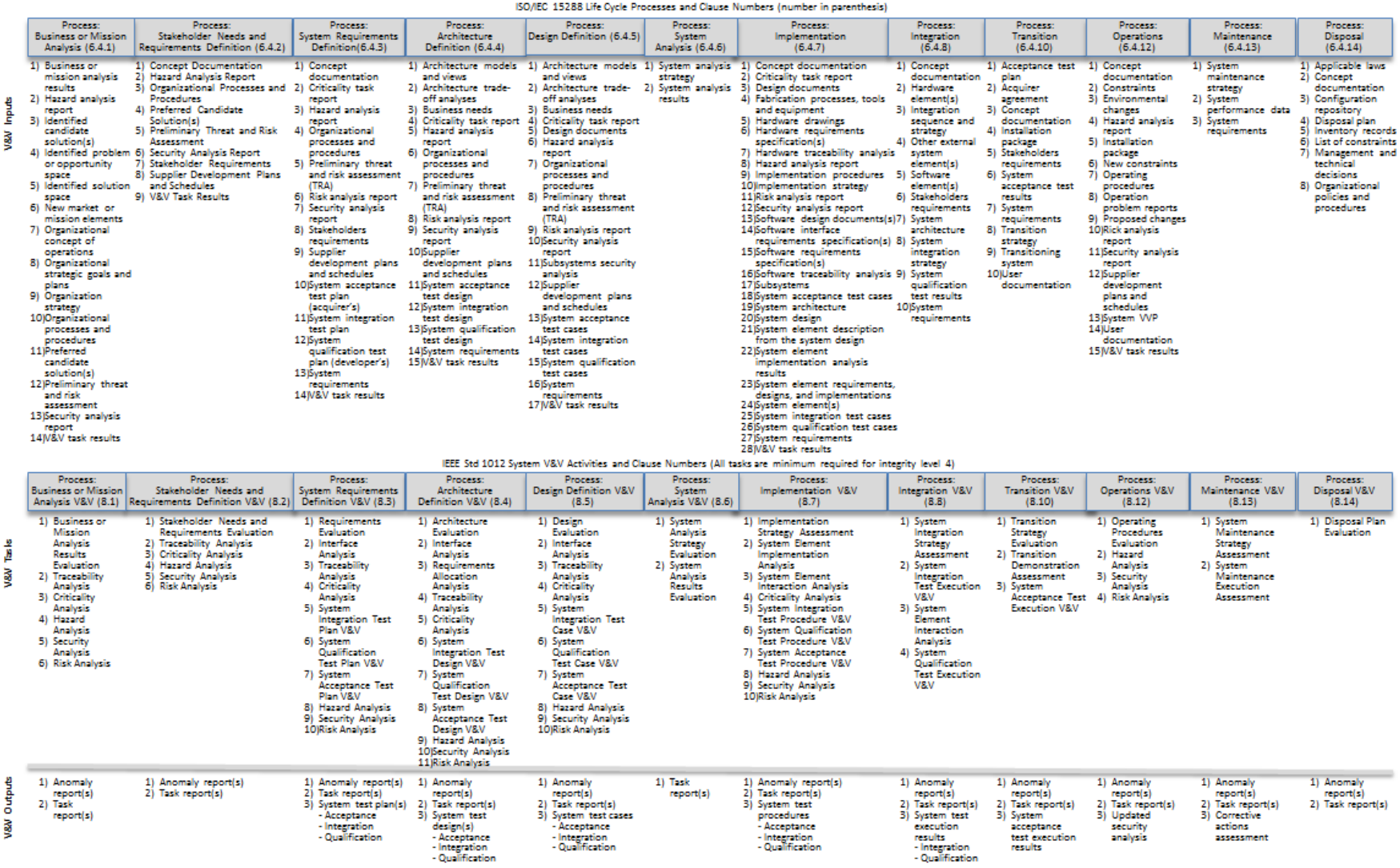
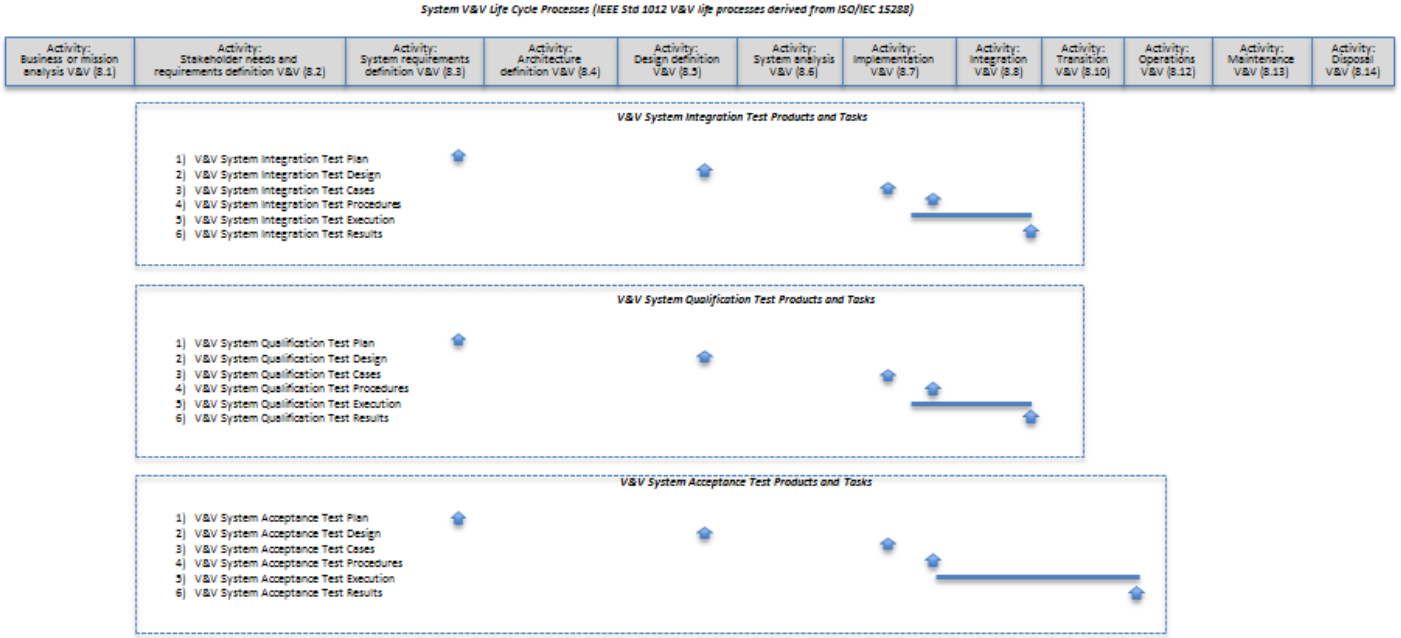



**Figure 1b—Summary of system V&V activities and tasks**




NOTE 1—All V&V system test products and tasks represent the activities and products required as a minimum for integrity level 4.

NOTE 2—This is an example of the phasing of system V&V test products and tasks across the system life cycle. The system V&V test products (upward arrows) are shown in the system life cycle stages when the products are generated (per IEEE Std 1012). System test execution tasks are shown to occur during one or more system life cycle stages as indicated by "activity bars" in the diagram. The life cycle stage (in which each test product is generated) and phasing of each test product and task can vary from this diagram in accordance with project-specific needs.

NOTE 3—The V&V activity clauses referenced in the system V&V life cycle stages are IEEE Std 1012 clauses.

**Figure 2b—Summary of system V&V test products and tasks**

# 9. Software V&V processes

## 9.1 Software Concept V&V process

### 9.1.1 Purpose

The purpose of the Software Concept V&V process is to provide assurance that the outcomes of the Software Requirements Analysis process (ISO/IEC 12207:2008 [B11]) related to software have been achieved.

### 9.1.2 Outcomes

As a result of the successful implementation of the Software Concept V&V process, objective evidence is developed to assess whether:

a) System requirements have been allocated to software (primary focus on software with consideration of interactions with hardware and user allocations).

b) The selected software solution satisfies the allocated software requirements.

c) No false assumptions are incorporated in the solution.

### 9.1.3 Activities and tasks

The V&V effort shall perform, as specified in Table 2c for the selected integrity level, the following Software Concept V&V activity and tasks described in Table 1c, Activity 9.1:

a) Software Concept V&V: This activity consists of the following tasks:

1) Concept Documentation Evaluation
2) Requirements Allocation Analysis
3) Traceability Analysis
4) Criticality Analysis
5) Hazard Analysis
6) Security Analysis
7) Risk Analysis

The Software Concept V&V tasks listed shall be used to verify and validate the Software Requirements Analysis process outcomes described in ISO/IEC 12207:2008 [B11]. The mappings of IEEE 1012 V&V tasks to ISO/IEC 12207 Software Requirements Analysis process outcomes are contained in Annex L.

## 9.2 Software Requirements Analysis V&V process

### 9.2.1 Purpose

The purpose of the Software Requirements Analysis V&V process is to provide assurance that outcomes of the Software Requirements Analysis process, the Software Qualification Testing process, and the Software Acceptance Support process (ISO/IEC 12207:2008 [B11]) have been achieved.

### 9.2.2 Outcomes

As a result of the successful implementation of the Software Requirements Analysis V&V process, objective evidence is developed to assess whether:

a) The software requirements are correct.

b) The software requirements are complete.

c) The software requirements are accurate.

d) The software requirements are testable.

e) The software requirements are consistent with the system software requirements.

### 9.2.3 Activities and tasks

The V&V effort shall perform, as specified in Table 2c for the selected integrity level, the following Software Requirements Analysis V&V tasks described in Table 1c, Activity 9.2:

a) Software Requirements Analysis V&V: This activity consists of the following tasks:

1) Requirements Evaluation

2) Interface Analysis

3) Traceability Analysis

4) Criticality Analysis

5) Software Qualification Test Plan V&V

6) Software Acceptance Test Plan V&V

7) Hazard Analysis

8) Security Analysis

9) Risk Analysis

The Software Requirements Analysis V&V process addresses software requirements analysis of the functional and performance requirements; interfaces external to the software; and requirements for qualification, safety and security, human factors engineering, data definitions, user documentation for the software, installation and acceptance, user operation and execution, and user maintenance. V&V test planning begins in the Software Requirements Analysis V&V process and spans several software V&V processes.

The Software Requirements Analysis V&V tasks listed shall be used to verify and validate the Software Requirements Analysis process outcomes, Software Qualification Testing process outcomes, and Software Acceptance Support process outcomes described in ISO/IEC 12207:2008 [B11]. The mappings of IEEE 1012 V&V tasks to ISO/IEC 12207:2008 [B11] Software Requirements Analysis process outcomes, Software Qualification Testing process outcomes, and Software Acceptance Support process outcomes are contained in Annex L.

## 9.3 Software Design V&V process

### 9.3.1 Purpose

The purpose of the Software Design V&V process is to provide assurance that outcomes of the Software Architectural Design process, the Software Detailed Design process, the Software Integration process, the Software Qualification Testing process, and the Software Acceptance Support process (ISO/IEC 12207:2008 [B11]) have been achieved.

### 9.3.2 Outcomes

As a result of the successful implementation of the Software Design V&V process, objective evidence is developed to assess whether:

a) The software design is correct, accurate, and a complete transformation of the software requirements.

b) No unintended features are introduced into the software design.

### 9.3.3 Activities and tasks

The V&V effort shall perform, as specified in Table 2c for the selected integrity level, the following Software Design V&V tasks described in Table 1c, Activity 9.3:

a) Software Design V&V: This activity consists of the following tasks:

1) Design Evaluation
2) Interface Analysis
3) Traceability Analysis
4) Criticality Analysis
5) Software Component Test Plan V&V
6) Software Integration Test Plan V&V
7) Software Component Test Design V&V
8) Software Integration Test Design V&V
9) Software Qualification Test Design V&V
10) Software Acceptance Test Design V&V
11) Hazard Analysis
12) Security Analysis
13) Risk Analysis

The Software Design V&V activity addresses software architectural design and software detailed design. V&V test planning continues during the Software Design V&V activity.

The Software Design V&V tasks listed shall be used to verify and validate the Software Architectural Design process outcomes, Software Detailed Design process outcomes, Software Integration process outcomes, Software Qualification Testing process outcomes, and Software Acceptance Support process outcomes described in ISO/IEC 12207:2008 [B11]. The mappings of IEEE 1012 V&V tasks to ISO/IEC 12207 Software Architectural Design process outcomes, Software Detailed Design process outcomes, Software Integration process outcomes, Software Qualification Testing process outcomes, and Software Acceptance Support process outcomes are contained in Annex L.

## 9.4 Software Construction V&V process

### 9.4.1 Purpose

The purpose of the Software Construction V&V process is to provide assurance that outcomes of the Software Construction process, the Software Integration process, the Software Qualification Testing process, and the Software Acceptance Support process (ISO/IEC 12207:2008 [B11]) have been achieved.

### 9.4.2 Outcomes

As a result of the successful implementation of the Software Construction V&V process, objective evidence is developed to assess whether the transformations from the software design into code, database structures, and related machine executable representation are:

a) Correct.

b) Accurate.

c) Complete.

### 9.4.3 Activities and tasks

The V&V effort shall perform, as specified in Table 2c for the selected integrity level, the following Software Construction V&V activity and tasks described in Table 1c, Activity 9.4:

a) Software Construction V&V: This activity consists of the following tasks:

1) Source Code and Source Code Documentation Evaluation
2) Interface Analysis
3) Traceability Analysis
4) Criticality Analysis
5) Software Component Test Case V&V
6) Software Integration Test Case V&V
7) Software Qualification Test Case V&V
8) Software Acceptance Test Case V&V
9) Software Component Test Procedure V&V
10) Software Integration Test Procedure V&V
11) Software Qualification Test Procedure V&V
12) Software Component Test Execution V&V
13) Hazard Analysis
14) Security Analysis
15) Risk Analysis

The Software Construction V&V activity addresses software coding and testing, including the incorporation of reused software products.

The Software Construction V&V tasks listed shall be used to verify and validate the Software Construction process outcomes, Software Integration process outcomes, Software Qualification Testing process outcomes, and Software Acceptance Support process outcomes described in ISO/IEC 12207:2008 [B11]. The mappings of IEEE 1012 V&V tasks to the ISO/IEC 12207 Software Construction process outcomes, Software Integration process outcomes, Software Qualification Testing process outcomes, and Software Acceptance Support process outcomes are contained in Annex L.

## 9.5 Software Integration V&V process

### 9.5.1 Purpose

The purpose of the Software Integration V&V process is to provide assurance that the outcomes of the Software Integration process (ISO/IEC 12207:2008 [B11]) have been achieved.

### 9.5.2 Outcomes

As a result of the successful implementation of the Software Integration V&V process, objective evidence is developed to assess whether the software requirements and system requirements allocated to software are validated as each software component (e.g., unit or module) is incrementally integrated.

### 9.5.3 Activities and tasks

The V&V effort shall perform, as specified in Table 2c for the selected integrity level, the following Software Integration V&V tasks described in Table 1c, Activity 9.5:

a) Software Integration V&V: This activity consists of the following tasks:

1) Software Integration Test Execution V&V
2) Traceability Analysis
3) Hazard Analysis
4) Security Analysis
5) Risk Analysis

The Software Integration V&V tasks listed shall be used to verify and validate the Software Integration process outcomes described in ISO/IEC 12207:2008 [B11]. The mappings of IEEE 1012 V&V tasks to ISO/IEC 12207 Software Integration process outcomes are contained in Annex L.

## 9.6 Software Qualification Testing V&V process

### 9.6.1 Purpose

The purpose of the Software Qualification Testing V&V process is to provide assurance that the outcomes of the Software Qualification Testing process (ISO/IEC 12207:2008 [B11]) have been achieved.

### 9.6.2 Outcomes

As a result of the successful implementation of the Software Qualification Testing V&V process, objective evidence is developed to assess whether the integrated software product satisfies its requirements.

### 9.6.3 Activities and tasks

The V&V effort shall perform, as specified in Table 2c for the selected integrity level, the following Software Qualification Testing V&V tasks described in Table 1c, Activity 9.6:

a) Software Qualification Testing V&V: This activity consists of the following tasks:

1) Software Qualification Test Execution V&V
2) Traceability Analysis
3) Hazard Analysis

4) Security Analysis

5) Risk Analysis

Software qualification (e.g., demonstration, analysis, inspection, or test) is performed on the complete software element.

The Software Qualification Testing V&V tasks listed shall be used to verify and validate the Software Qualification Testing process outcomes described in ISO/IEC 12207:2008 [B11]. The mappings of IEEE 1012 V&V tasks to ISO/IEC 12207 Software Qualification Testing process outcomes are contained in Annex L.

## 9.7 Software Acceptance Testing V&V process

### 9.7.1 Purpose

The purpose of the Software Acceptance Testing V&V process is to provide assurance that outcomes of the Software Acceptance Support process and the Software Operation process (ISO/IEC 12207:2008 [B11]) have been achieved.

### 9.7.2 Outcomes

As a result of the successful implementation of the Software Acceptance Testing V&V process, objective evidence is developed to assess whether:

a) The software satisfies its acceptance criteria.

b) The customer is able to determine whether or not to accept the integrated software product.

### 9.7.3 Activities and tasks

The V&V effort shall perform, as specified in Table 2c for the selected integrity level, the following Software Acceptance Testing V&V tasks described in Table 1c, Activity 9.7:

a) Software Acceptance Testing V&V: This activity consists of the following tasks:

1) Software Acceptance Test Procedure V&V

2) Software Acceptance Test Execution V&V

3) Traceability Analysis

4) Hazard Analysis

5) Security Analysis

6) Risk Analysis

The Software Acceptance Testing V&V tasks listed shall be used to verify and validate the Software Acceptance Support process outcomes and Software Operation process outcomes described in ISO/IEC 12207:2008 [B11]. The mappings of IEEE 1012 V&V tasks to ISO/IEC 12207:2008 [B11] Software Acceptance Support process outcomes and Software Operation process outcomes are contained in Annex L.

## 9.8 Software Verification process

### 9.8.1 Purpose

The purpose of the Software Verification process is to provide objective evidence for whether the outcomes achieve the following:

a) Conform to requirements (e.g., for correctness, completeness, consistency, and accuracy) for all activities during each life cycle process.

b) Satisfy the standards, practices, and conventions during life cycle processes.

c) Successfully complete each life cycle activity and satisfy all the criteria for initiating succeeding life cycle activities (i.e., the product is built correctly).

### 9.8.2 Outcomes

As a result of successful implementation of the Software Verification process:

a) A Verification and Validation Plan is developed and implemented.

b) The system of interest (software) and all components of the system of interest are assigned integrity levels that are reevaluated throughout the life cycle of the system.

c) The software and each of its components are evaluated for requirements satisfaction based on assigned integrity levels.

d) Objective evidence is developed to determine whether the software and each of its components conform to requirements and satisfy all the criteria for each successive life cycle activity.

### 9.8.3 Activities and tasks

Descriptions of the activities and tasks for the Software Verification process as applied to the Technical processes of the software life cycle processes from ISO/IEC 12207:2008 [B11] are described in Clause 9.1 (Software Concept V&V process), Clause 9.2 (Software Requirements Analysis V&V process), Clause 9.3 (Software Design V&V process), Clause 9.4 (Software Construction V&V process), Clause 9.5 (Software Integration V&V process), Clause 9.6 (Software Qualification Testing V&V process), Clause 9.7 (Software Acceptance Testing V&V process), Clause 9.9 (Software Installation and Checkout V&V process), Clause 9.11 (Software Operation V&V process), Clause 9.12 (Software Maintenance V&V process), and Clause 9.13 (Software Disposal V&V process).

## 9.9 Software Installation and Checkout V&V process

### 9.9.1 Purpose

The purpose of the Software Installation and Checkout V&V process is to provide assurance that outcomes of the Software Installation process and the Software Acceptance Support process (ISO/IEC 12207:2008 [B11]) have been achieved.

### 9.9.2 Outcomes

As a result of the successful implementation of the Software Installation and Checkout V&V process, objective evidence is developed to assess whether the software installation in the target environment is correct.

### 9.9.3 Activities and tasks

The V&V effort shall perform, as specified in Table 2c for the selected integrity level, the following Software Installation and Checkout V&V activity and tasks described in Table 1c, Activity 9.9:

a) Software Installation and Checkout V&V: This activity consists of the following tasks:

1) Installation Configuration Audit
2) Installation Checkout
3) Hazard Analysis
4) Security Analysis
5) Risk Analysis

In installation and checkout, the software product is installed and tested in the target environment. The Software Installation and Checkout V&V activity supports the software system installation activities.

The Software Installation and Checkout V&V tasks listed shall be used to verify and validate the Software Installation process outcomes and Software Acceptance Support process outcomes described in ISO/IEC 12207:2008 [B11]. The mappings of IEEE 1012 V&V tasks to ISO/IEC 12207 Software Installation process outcomes and Software Acceptance Support process outcomes are contained in Annex L.

## 9.10 Software Validation process

### 9.10.1 Purpose

The purpose of the Software Validation process is to provide objective evidence for whether the outcomes achieve the following:

a) Satisfy requirements allocated to the products at the end of each life cycle activity.

b) Solve the right problem (e.g., correctly model physical laws, implement business rules, and use the proper system assumptions).

c) Satisfy intended use and user needs in the operational environment (i.e., the correct product is built).

### 9.10.2 Outcomes

As a result of successful implementation of the Software Validation process:

a) A Verification and Validation Plan is developed and implemented.

b) The system of interest (software) and all components of the system of interest are assigned integrity levels that are maintained throughout the life cycle of the system.

c) The software and each of its components are evaluated for satisfaction of allocated system requirements and of intended use and user needs based on assigned integrity levels.

d) Objective evidence is developed to determine whether the software and each of its components satisfy all system requirements allocated to software and meet intended use and user needs.

### 9.10.3 Activities and tasks

Descriptions of the activities and tasks for the Software Validation process as applied to the Technical processes of the software life cycle processes from ISO/IEC 12207:2008 [B11] are described in Clause 9.1 (Software Concept V&V process), Clause 9.2 (Software Requirements Analysis V&V process), Clause 9.3 (Software Design V&V process), Clause 9.4 (Software Construction V&V process), Clause 9.5 (Software Integration V&V process), Clause 9.6 (Software Qualification Testing V&V process), Clause 9.7 (Software Acceptance Testing V&V process), Clause 9.9 (Software Installation and Checkout V&V process), Clause 9.11 (Software Operation V&V process), Clause 9.12 (Software Maintenance V&V process), and Clause 9.13 (Software Disposal V&V process).

## 9.11 Software Operation V&V process

### 9.11.1 Purpose

The purpose of the Software Operation V&V process is to provide assurance that outcomes of the Software Operation process (ISO/IEC 12207:2008 [B11]) have been achieved.

### 9.11.2 Outcomes

As a result of the successful implementation of the Software Operation V&V process, objective evidence is developed to assess whether:

a) New constraints in the system are evaluated.

b) Proposed system changes and their impacts on the software are assessed.

c) Operating procedures are evaluated for correctness and usability.

### 9.11.3 Activities and tasks

The V&V effort shall perform, as specified in Table 2c for the selected integrity level, the following Software Operation V&V tasks described in Table 1c, Activity 9.11:

a) Software Operation V&V: This activity consists of the following tasks:

1) Evaluation of New Constraints
2) Operating Procedures Evaluation
3) Hazard Analysis
4) Security Analysis
5) Risk Analysis

The Software Operation V&V activity evaluates the impact of changes in the operating environment, assesses the effect on the system of any proposed changes, evaluates operating procedures for adherence with the intended use, and analyzes risks affecting the user and the system.

The Software Operation V&V tasks listed shall be used to verify and validate the Software Operation process outcomes described in ISO/IEC 12207:2008 [B11]. The mappings of IEEE 1012 V&V tasks to ISO/IEC 12207 Software Operation process outcomes are contained in Annex L.

## 9.12 Software Maintenance V&V process

### 9.12.1 Purpose

The purpose of the Software Maintenance V&V process is to provide assurance that outcomes of the Software Maintenance process (ISO/IEC 12207:2008 [B11]) have been achieved.

### 9.12.2 Outcomes

As a result of the successful implementation of the Software Maintenance V&V process, objective evidence is developed to assess whether:

a) Proposed software changes and their impact on the system are assessed.

b) Anomalies that are discovered during operation are evaluated.

c) Migration requirements are assessed.

d) Retirement requirements are assessed.

e) V&V tasks are re-performed.

### 9.12.3 Activities and tasks

The V&V effort shall perform, as specified in Table 2c for the selected integrity level, the following Software Maintenance V&V tasks described in Table 1c, Activity 9.12:

a) Software Maintenance V&V: This activity consists of the following tasks:

1) VVP Revision
2) Anomaly Evaluation
3) Criticality Analysis
4) Migration Assessment
5) Retirement Assessment
6) Hazard Analysis
7) Security Analysis
8) Risk Analysis
9) Task Iteration

Proposed changes are assessed by the Proposed/Baseline Change Assessment task of the Management of V&V activity.

The Software Maintenance process is activated when the software or associated documentation is changed in response to a need for system maintenance. The Software Maintenance V&V activity addresses the following software system processes:

— Modifications (i.e., corrective, adaptive, or perfective changes).

— Migration (i.e., the movement of software to a new operational environment).

— Retirement (i.e., the withdrawal of active support by the operation and maintenance organization, partial or total replacement by a new system, or installation of an upgraded system).

System modifications may be derived from the requirements specified to correct software errors (e.g., corrective), to adapt to a changed operating environment (e.g., adaptive), or to respond to additional user requests or enhancements (e.g., perfective). Modifications of the software system shall be treated as development processes and shall be verified and validated by performing V&V tasks corresponding to the modifications. Integrity level assignments shall be assessed as described in Clause 5. The integrity level assignments shall be revised as appropriate to reflect the requirements derived from the maintenance process.

If software V&V was performed in accordance with this standard, then the maintenance process shall continue to conform to this standard. If the software was not verified and validated using this standard and appropriate documentation is not available or adequate, then the Software Maintenance V&V effort shall determine whether the missing or incomplete documentation should be generated. In making this determination of whether to generate missing documentation, the minimum V&V requirements of the assigned integrity level shall be taken into consideration.

The Software Maintenance V&V tasks listed shall be used to verify and validate the Software Maintenance process outcomes described in ISO/IEC 12207:2008 [B11]. The mappings of IEEE 1012 V&V tasks to the ISO/IEC 12207 Software Maintenance process outcomes are contained in Annex L.

## 9.13 Software Disposal V&V process

### 9.13.1 Purpose

The purpose of the Software Disposal V&V process is to provide assurance that outcomes of the Software Disposal process (ISO/IEC 12207:2008 [B11]) have been achieved.

### 9.13.2 Outcomes

As a result of the successful implementation of the Software Disposal V&V process, objective evidence is developed to assess whether:

a) The constraints in the software disposal strategy are included in software requirements.

b) Disposal leaves the system in an agreed-on state.

### 9.13.3 Activities and tasks

The V&V effort shall perform, as specified in Table 2c for the selected integrity level, the following Software Disposal V&V activity and task described in Table 1c, Activity 9.13:

a) Software Disposal V&V: This activity consists of the following task:

   1) Software Disposal Evaluation

This process ends active support by the operation and maintenance organization, or deactivates, disassembles, and removes the affected software products, consigning them to a final condition and leaving the environment in an acceptable condition. This process destroys or stores system software elements and related products in a sound manner, in accordance with legislation, agreements, organizational constraints, and stakeholder requirements. Where required, it maintains records that may be monitored.

The Software Disposal V&V task listed shall be used to verify and validate the Software Disposal process outcomes described in ISO/IEC 12207:2008 [B11]. The mappings of IEEE 1012 V&V tasks to ISO/IEC 12207 Software Disposal process outcomes are contained in Annex L.

## Table 1c—V&V tasks, inputs, and outputs

| 9.1 Activity: Software Concept V&V (Software, 12207—Software Requirements Analysis process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(1) Concept Documentation Evaluation**<br>a) Validate that the concept documentation satisfies user needs and is consistent with acquisition needs.<br>b) Validate constraints of interfacing systems and constraints or limitations of proposed approach.<br>c) Analyze system requirements and validate that the following satisfy user needs:<br>1) System functions.<br>2) End-to-end system performance.<br>3) Feasibility and testability of the functional requirements.<br>4) System architecture design.<br>5) Operation and maintenance requirements and environments.<br>6) Migration requirements from an existing system where applicable. | Concept documentation<br>System architectural design<br>Supplier development plans and schedules<br>User needs<br>Acquisition needs | Task report(s)—Concept documentation evaluation<br>Anomaly report(s) |
| **(2) Requirements Allocation Analysis**<br>Verify the correctness, accuracy, and completeness of the system requirements allocation to the software against user needs.<br>a) Correctness<br>Verify that performance requirements (e.g., timing, response time, and throughput) allocated to the hardware, software, and user interfaces satisfy user needs.<br>b) Accuracy<br>Verify that the internal and external interfaces specify the data formats, interface protocols, frequency of data exchange at each interface, and other performance requirements to demonstrate satisfaction of user requirements.<br>c) Completeness<br>1) Verify that application-specific requirements such as functional diversity, fault detection, fault isolation, and diagnostic and error recovery satisfy user needs.<br>2) Verify that the user's maintenance requirements for the system are completely specified.<br>3) Verify that the migration from existing system and replacement of the system satisfies user needs. | User needs<br>Concept documentation<br>System requirements<br>System architecture | Task report(s)—Requirements allocation analysis<br>Anomaly report(s) |
| **(3) Traceability Analysis**<br>a) Identify all system requirements.<br>b) Verify that these system requirements are traceable to acquisition needs.<br>c) Start the requirements traceability analysis with system requirements. | Concept documentation | Task report(s)—Traceability analysis<br>Anomaly report(s) |
| **(4) Criticality Analysis**<br>a) Determine whether integrity levels are established for requirements, detailed functions, software modules, hardware elements, subsystems, or other partitions.<br>b) Verify that the assigned integrity levels are correct. If integrity levels are not assigned, then assign integrity levels to the system requirements.<br>c) Document the integrity level assigned to individual components | Concept documentation (System requirements)<br>Developer integrity level assignments | Task report(s)—Criticality analysis<br>Anomaly report(s) |

| 9.1 Activity: Software Concept V&V (Software, 12207—Software Requirements Analysis process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| (e.g., requirements, detailed functions, software modules, hardware elements, subsystems, or other partitions). For V&V planning purposes, the system shall be assigned the same integrity level as the highest level assigned to any individual element.<br>d) Verify whether any component can influence the individual components assigned a higher software integrity level, and if such conditions exist, then assign that component the same higher integrity level. | | |
| **(5) Hazard Analysis**<br>Analyze the potential hazards to and from the conceptual system. The analysis shall perform the following:<br>a) Identify the potential system hazards.<br>b) Assess the consequences of each hazard.<br>c) Assess the probability of each hazard.<br>d) Identify mitigation strategies for each hazard. | Concept documentation | Task report(s)—Hazard analysis<br>Anomaly report(s) |
| **(6) Security Analysis**<br>a) Review the system owner's definition of an acceptable level of security risk.<br>b) Analyze the system concept from a security perspective and assure that potential security risks with respect to confidentiality (disclosure of sensitive information/data), integrity (modification of information/data), availability (withholding of information or services), and accountability (attributing actions to an individual/process) have been identified. Include an assessment of the sensitivity of the information/data to be processed.<br>c) Analyze the security risks introduced by the system itself as well as those associated with the environment with which the system interfaces. | Concept documentation<br>Preliminary TRA | Task report(s)—Security analysis<br>Anomaly report(s) |
| **(7) Risk Analysis**<br>a) Identify the technical and management risks.<br>b) Provide recommendations to eliminate, reduce, or mitigate the risks. | Concept documentation<br>Supplier development plans and schedules<br>Hazard analysis report<br>Security analysis report<br>V&V task results | Task report(s)—Risk analysis<br>Anomaly report(s) |

| 9.2 Activity: Software Requirements Analysis V&V (Software, 12207—Software Requirements Analysis process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(1) Requirements Evaluation**<br>Evaluate the requirements (e.g., functional, capability, interface, qualification, safety, security, human factors, data definitions, user documentation, installation and acceptance, user operation, and user maintenance) of the SRS and IRS for correctness, consistency, completeness, accuracy, readability, and testability. The task criteria are as follows:<br>Correctness<br>1) Verify and validate that the software requirements satisfy the system requirements allocated to software within the | Concept documentation<br>SRS<br>IRS | Task report(s)—Software requirements evaluation<br>Anomaly report(s) |

| 9.2 Activity: Software Requirements Analysis V&V (Software, 12207—Software Requirements Analysis process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| assumptions, constraints, and operating environment for the system.<br>2) Verify that the software requirements comply with standards, references, regulations, policies, physical laws, and business rules.<br>3) Validate the sequences of states and state changes using logic and data flows coupled with domain expertise, prototyping results, engineering principles, or other basis.<br>4) Validate that the flow of data and control satisfy functionality and performance requirements.<br>5) Validate data usage and format.<br>b) Consistency<br>1) Verify that all terms and concepts are documented consistently.<br>2) Verify that the function interactions and assumptions are consistent and satisfy system requirements and acquisition needs.<br>3) Verify that there is internal consistency between the software requirements and external consistency with the system requirements.<br>c) Completeness<br>1) Verify that the following elements are in the SRS or IRS, within the assumptions and constraints of the system:<br>i) Functionality (e.g., algorithms, state/mode definitions, input/output validation, exception handling, reporting, and logging).<br>ii) Process definition and scheduling.<br>iii) Hardware, software, and user-interface descriptions.<br>iv) Performance criteria (e.g., timing, sizing, speed, capacity, accuracy, precision, safety, and security).<br>v) Critical configuration data.<br>vi) System, device, and software control (e.g., initialization, transaction and state monitoring, and self-testing).<br>2) Verify that the SRS and IRS satisfy specified configuration management procedures.<br>d) Accuracy<br>1) Validate that the logic, computational, and interface precision (e.g., truncation and rounding) satisfy the requirements in the system environment.<br>2) Validate that the modeled physical phenomena conform to system accuracy requirements and physical laws.<br>e) Readability<br>1) Verify that the documentation is legible, understandable, and unambiguous to the intended audience.<br>2) Verify that the documentation defines all acronyms, mnemonics, abbreviations, terms, and symbols.<br>f) Testability<br>Verify that that there are objective acceptance criteria for validating the requirements of the SRS and IRS. | | |

| 9.2 Activity: Software Requirements Analysis V&V (Software, 12207—Software Requirements Analysis process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(2) Interface Analysis**<br>Verify and validate that the requirements for software interfaces with hardware, user, operator, and other systems are correct, consistent, complete, accurate, and testable. The task criteria are as follows:<br>a) Correctness<br>Validate the external and internal system and software interface requirements.<br>b) Consistency<br>Verify that the interface descriptions are consistent between the SRS and IRS.<br>c) Completeness<br>Verify that each interface is described and includes data format and performance criteria (e.g., timing, bandwidth, accuracy, safety, and security).<br>d) Accuracy<br>Verify that each interface provides information with the required accuracy.<br>e) Testability<br>Verify that there are objective acceptance criteria for validating the interface requirements. | Concept documentation<br>SRS<br>IRS | Task report(s)—Interface analysis<br>Anomaly report(s) |
| **(3) Traceability Analysis**<br>Trace the software requirements (SRS and IRS) to the system requirements (Concept Documentation) and the system requirements to the software requirements.<br>Analyze identified relationships for correctness, consistency, completeness, and accuracy. The task criteria are as follows:<br>a) Correctness<br>Validate that the relationships between each software requirement and its system requirement are correct.<br>b) Consistency<br>Verify that the relationships between the software and system requirements are specified to a consistent level of detail.<br>c) Completeness<br>1) Verify that every software requirement is traceable to a system requirement with sufficient detail to show conformance to the system requirement.<br>2) Verify that all system requirements related to software are traceable to software requirements.<br>d) Accuracy<br>Validate that the system performance and operating characteristics are accurately specified by the traced software requirements. | Concept documentation (System requirements)<br>SRS<br>IRS | Task report(s)—Traceability analysis<br>Anomaly report(s) |
| **(4) Criticality Analysis**<br>a) Review and update the existing criticality analysis results from the prior Criticality Task Report using the SRS and IRS.<br>b) Implementation methods and interfacing technologies may cause previously assigned integrity levels to be raised or lowered for a given software element (i.e., requirement, module, function, subsystem, and other software partition). Verify that no inconsistent or undesired integrity consequences are introduced by reviewing the revised integrity levels. | Criticality task report<br>SRS<br>IRS | Task report(s)—Criticality analysis<br>Anomaly report(s) |

| 9.2 Activity: Software Requirements Analysis V&V (Software, 12207—Software Requirements Analysis process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(5) Software Qualification Test Plan V&V**<br>a) Integrity levels 4 and 3<br>1) Plan V&V software qualification testing to validate software requirements.<br>2) Plan tracing of system requirements to software qualification test designs, cases, procedures, and results.<br>3) Plan documentation of V&V software qualification test designs, cases, procedures, and results.<br>4) The V&V software qualification test plan shall address the following:<br>i) Conformance to all system requirements (e.g., functional, performance, security, operation, and maintenance) as complete software end items in the system environment.<br>ii) Adequacy of user documentation (e.g., training materials and procedural changes).<br>iii) Performance at boundaries (e.g., data and interfaces) and under stress conditions.<br>5) Verify that the V&V software qualification test plan satisfies the following criteria:<br>i) Conformance to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>ii) Test coverage of system requirements.<br>6) Validate that the V&V software qualification test plan satisfies the following criteria:<br>i) Appropriateness of test methods and standards used.<br>ii) Conformance to expected results.<br>iii) Feasibility of system qualification testing.<br>iv) Feasibility and testability of operation and maintenance requirements.<br>b) Integrity level 2<br>1) Verify that the developer's software qualification test plan satisfies the following criteria:<br>i) Conformance to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>ii) Test coverage of system requirements.<br>2) Validate that the developer's software qualification test plan satisfies the following criteria:<br>i) Appropriateness of test methods and standards used.<br>ii) Conformance to expected results.<br>iii) Feasibility of system qualification testing.<br>iv) Capability to be operated and maintained.<br>c) Integrity level 1<br>There are no software qualification test plan V&V requirements. | Concept documentation (System requirements)<br>SRS<br>IRS<br>User documentation<br>Software qualification test plan | V&V software qualification test plan (integrity levels 4 and 3)<br>Task report(s)—Review of software qualification test plan (integrity level 2)<br>Anomaly report(s) |
| **(6) Software Acceptance Test Plan V&V**<br>a) Integrity levels 4 and 3<br>1) Plan V&V software acceptance testing to validate that the software correctly implements system and software requirements in an operational environment. | Concept documentation<br>SRS<br>IRS<br>User documentation | V&V software acceptance test plan (integrity levels 4 and 3)<br>Task report(s)—Review of software |

| 9.2 Activity: Software Requirements Analysis V&V (Software, 12207—Software Requirements Analysis process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| 2) Plan tracing of test requirements to test software acceptance design, cases, procedures, and execution results.<br>3) Plan documentation of test tasks and results.<br>4) The V&V software acceptance test plan shall address the following:<br>i) Conformance to acceptance requirements in the operational environment.<br>ii) Adequacy of user documentation.<br>5) Verify that the V&V software acceptance test plan satisfies the following criteria:<br>i) Conformance to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>ii) Test coverage of acceptance requirements.<br>6) Validate that the V&V software acceptance test plan satisfies the following criteria:<br>i) Conformance to expected results.<br>ii) Feasibility of operation and maintenance (e.g., capability to be operated and maintained in accordance with user needs).<br>b) Integrity level 2<br>1) Verify that the acquirer's software acceptance test plan conforms to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>2) Validate that the acquirer's software acceptance test plan satisfies the following criteria:<br>i) Test coverage of acceptance requirements.<br>ii) Conformance to expected results.<br>iii) Feasibility of operation and maintenance (e.g., capability to be operated and maintained in accordance with user needs).<br>c) Integrity level 1<br>There are no software acceptance V&V test requirements. | Software acceptance test plan | acceptance test plan (integrity level 2)<br>Anomaly report(s) |
| **(7) Hazard Analysis**<br>a) Determine software contributions to system hazards. The hazard analysis shall perform the following:<br>b) Identify the software requirements that contribute to each system hazard.<br>c) Validate that the software addresses, controls, or mitigates each hazard. | SRS<br>IRS<br>Hazard analysis report | Task report(s)—Hazard analysis<br>Anomaly report(s) |
| **(8) Security Analysis**<br>a) Determine that the security requirements identified in the SRS and IRS address the security risks introduced by the system concept.<br>b) Verify that the system security requirements will mitigate the identified security risks to an acceptable level. | SRS<br>IRS<br>Preliminary TRA<br>Security analysis report | Task report(s)—Security analysis<br>Anomaly report(s) |

| 9.2 Activity: Software Requirements Analysis V&V (Software, 12207—Software Requirements Analysis process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(9) Risk Analysis**<br>a) Review and update risk analysis using prior task reports.<br>b) Provide recommendations to eliminate, reduce, or mitigate the risks. | Concept documentation<br>SRS<br>IRS<br>Supplier development plans and schedules<br>Hazard analysis report<br>Security analysis report<br>Risk analysis report<br>V&V task results | Task report(s)—Risk analysis<br>Anomaly report(s) |

| 9.3 Activity: Software Design V&V (Software, 12207—Software Architecture Design process, Software Detailed Design process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(1) Design Evaluation**<br>Evaluate the design elements (SDD and IDD) for correctness, consistency, completeness, accuracy, readability, and testability. The task criteria are as follows:<br>a) Correctness<br>1) Verify and validate the allocation of software requirements to the software design elements.<br>2) Verify and validate that the software design satisfies the software requirements.<br>3) Verify that the software design complies with standards, references, regulations, policies, physical laws, and business rules.<br>4) Validate the design sequences of states and state changes using logic and data flows coupled with domain expertise, prototyping results, engineering principles, or other basis.<br>5) Validate that the detailed design and its element interactions do not result in unnecessary, unintended, or deleterious consequences.<br>6) Validate that the flow of data and control satisfy functionality and performance requirements.<br>7) Validate data usage and format.<br>8) Assess the appropriateness of design methods and standards used.<br>b) Consistency<br>1) Verify that all terms and design concepts are documented consistently.<br>2) Verify that there is internal consistency between the design elements and external consistency with architectural design.<br>c) Completeness<br>1) Verify that the following elements are in the SDD, within the assumptions and constraints of the system:<br>i) Functionality (e.g., algorithms, state/mode definitions, input/output validation, exception | SRS<br>IRS<br>SDD<br>IDD<br>Design standards (e.g., standards, practices, and conventions) | Task report(s)—Design evaluation<br>Anomaly report(s) |

| 9.3 Activity: Software Design V&V (Software, 12207—Software Architecture Design process, Software Detailed Design process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| handling, reporting, and logging).<br>ii) Process definition and scheduling.<br>iii) Hardware, software, and user interface descriptions.<br>iv) Performance criteria (e.g., timing, sizing, speed, capacity, accuracy, precision, safety, and security).<br>v) Critical configuration data.<br>vi) System, device, and software control (e.g., initialization, transaction and state monitoring, and self-testing).<br>2) Verify that the SDD and IDD satisfy specified configuration management procedures.<br>d) Accuracy<br>1) Validate that the logic, computational, and interface precision (e.g., truncation and rounding) satisfy the requirements in the system environment.<br>2) Validate that the modeled physical phenomena conform to system accuracy requirements and physical laws.<br>e) Readability<br>1) Verify that the documentation is legible, understandable, and unambiguous to the intended audience.<br>2) Verify that the documentation defines all acronyms, mnemonics, abbreviations, terms, symbols, and design language, if any.<br>f) Testability<br>1) Verify that there are objective acceptance criteria for validating each software design element and the system design.<br>2) Verify that each software design element is testable to objective acceptance criteria. | | |
| **(2) Interface Analysis**<br>Verify and validate that the software design interfaces with hardware, user, operator, software, and other systems for correctness, consistency, completeness, accuracy, and testability. The task criteria are as follows:<br>a) Correctness<br>Validate the external and internal software interface design in the context of system requirements.<br>b) Consistency<br>Verify that the interface design is consistent between the SDD and IDD.<br>c) Completeness<br>Verify that each interface is described and includes data format and performance criteria (e.g., timing, bandwidth, accuracy, safety, and security).<br>d) Accuracy<br>Verify that each interface provides information with the required accuracy.<br>e) Testability<br>Verify that there are objective acceptance criteria for validating the interface design. | Concept documentation<br>System requirements<br>SRS<br>IRS<br>SDD<br>IDD | Task report(s)—Interface analysis<br>Anomaly report(s) |

| 9.3 Activity: Software Design V&V (Software, 12207—Software Architecture Design process, Software Detailed Design process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(3) Traceability Analysis**<br>Trace design elements (SDD and IDD) to requirements (SRS and IRS) and the requirements to design elements. Analyze relationships for correctness, consistency, and completeness. The task criteria are as follows:<br>a) Correctness<br>Validate the relationship between each design element and the software requirement(s).<br>b) Consistency<br>Verify that the relationships between the design elements and the software requirements are specified to a consistent level of detail.<br>c) Completeness<br>1) Verify that all design elements are traceable from the software requirements.<br>2) Verify that all software requirements are traceable to the design elements. | SRS<br>SDD<br>IRS<br>IDD | Task report(s)—Traceability analysis<br>Anomaly report(s) |
| **(4) Criticality Analysis**<br>a) Review and update the existing criticality analysis results from the prior Criticality Task Report using the SDD and IDD.<br>b) Implementation methods and interfacing technologies may cause previously assigned integrity levels to be raised or lowered for a given software element (i.e., requirement, module, function, subsystem, other software partition). Verify that no inconsistent or undesired integrity consequences are introduced by reviewing the revised integrity levels. | Criticality Task Report<br>SDD<br>IDD | Task report(s)—Criticality analysis<br>Anomaly report(s) |
| **(5) Software Component Test Plan V&V**<br>a) Integrity levels 4 and 3<br>1) Plan V&V software component testing to validate that the software components (e.g., units and source code modules) correctly implement component requirements.<br>2) Plan tracing of design requirements to test design, cases, procedures, and results.<br>3) Plan documentation of test tasks and results.<br>4) The V&V software component test plan shall address the following:<br>i) Conformance to design requirements.<br>ii) Assessment of timing, sizing, and accuracy.<br>iii) Performance at boundaries and interfaces and under stress and error conditions.<br>iv) Measures of requirements test coverage and software reliability and maintainability.<br>5) Verify that the V&V software component test plan conforms to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>6) Validate that the V&V software component test plan satisfies the following criteria:<br>i) Traceable to the software requirements and design.<br>ii) External consistency with the software requirements and design.<br>iii) Internal consistency between unit requirements. | SRS<br>SDD<br>IRS<br>IDD<br>Software component test plan | V&V software component test plan (integrity levels 4 and 3)<br>Task report(s)—Review of software component test plan (integrity level 2)<br>Anomaly report(s) |

| 9.3 Activity: Software Design V&V (Software, 12207—Software Architecture Design process, Software Detailed Design process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| iv) Test coverage of requirements in each unit.<br>v) Feasibility of software integration and testing.<br>vi) Feasibility of operation and maintenance (e.g., capability to be operated and maintained in accordance with user needs).<br>b) Integrity level 2<br>1) Verify that the developer's software component test plan conforms to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>2) Validate that the developer's software component test plan satisfies the following criteria:<br>i) Traceable to the software requirements and design.<br>ii) External consistency with the software requirements and design.<br>iii) Internal consistency between unit requirements.<br>iv) Test coverage of units.<br>v) Feasibility of software integration and testing.<br>vi) Feasibility of operation and maintenance (e.g., capability to be operated and maintained in accordance with user needs).<br>c) Integrity level 1<br>There are no software component V&V test requirements. | | |
| **(6) Software Integration Test Plan V&V**<br>a) For integrity levels 4 and 3<br>1) Plan V&V software integration testing to validate that the software correctly implements the software requirements and design as each software component (e.g., units or modules) is incrementally integrated with each other.<br>2) Plan tracing of requirements to test design, cases, procedures, and results.<br>3) Plan documentation of test tasks and results.<br>4) The V&V software integration test plan shall address the following:<br>i) Conformance to increasingly larger set of functional requirements at each stage of integration.<br>ii) Assessment of timing, sizing, and accuracy.<br>iii) Performance at boundaries and under stress conditions.<br>iv) Measures of requirements test coverage and software reliability.<br>5) Verify that the V&V software integration test plan satisfies the following criteria:<br>Conformance to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>6) Validate that the V&V software integration test plan satisfies the following criteria:<br>i) Traceable to the system requirements.<br>ii) External consistency with the system requirements.<br>iii) Internal consistency.<br>iv) Test coverage of the software requirements.<br>v) Appropriateness of test standards and methods used. | SRS<br>IRS<br>SDD<br>IDD<br>Software integration test plan | V&V software integration test plan (integrity levels 4 and 3)<br>Task report(s)—Review of software integration test plan (integrity level 2)<br>Anomaly report(s) |

| 9.3 Activity: Software Design V&V (Software, 12207—Software Architecture Design process, Software Detailed Design process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| vi) Conformance to expected results.<br>vii) Feasibility of software qualification testing.<br>viii) Feasibility of operation and maintenance (e.g., capability to be operated and maintained in accordance with user needs).<br>b) Integrity level 2<br>1) Verify that the developer's software integration test plan conforms to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>2) Validate that the developer's software integration test plan satisfies the following criteria:<br>i) Traceable to the system requirements.<br>ii) External consistency with the system requirements.<br>iii) Internal consistency.<br>iv) Test coverage of the software requirements.<br>v) Appropriateness of test standards and methods.<br>vi) Conformance to expected results.<br>vii) Feasibility of software qualification testing.<br>viii) Feasibility of operation and maintenance (e.g., capability to be operated and maintained in accordance with user needs).<br>c) Integrity level 1<br>There are no software integration test plan V&V requirements. | | |
| **(7) Software Component Test Design V&V**<br>a) Integrity levels 4 and 3<br>1) Design tests for V&V software component testing.<br>2) Continue tracing required by the V&V software component test plan.<br>3) Verify that the V&V software component test designs conform to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>4) Validate that the V&V software component test designs satisfy the criteria in V&V activity 9.3 Task 5.<br>b) Integrity level 2<br>1) Verify that the developer's test designs for software component testing conform to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>2) Validate that the developer's software component test designs satisfy the criteria in V&V activity 9.3 Task 5.<br>c) Integrity level 1<br>There are no software component V&V test requirements. | SDD<br>IDD<br>User documentation<br>Software component test plans<br>Software component test designs | V&V software component test design(s) (integrity levels 4 and 3)<br>Task report(s)—Review of software component test design (integrity level 2)<br>Anomaly report(s) |
| **(8) Software Integration Test Design V&V**<br>a) Integrity levels 4 and 3<br>1) Design tests for V&V software integration testing.<br>2) Continue tracing required by the V&V software integration test plan. Verify that the V&V software integration test designs conform to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>3) Validate that the V&V software integration test designs | SDD<br>IDD<br>User documentation<br>Software integration test plans<br>Software integration test designs | V&V software integration test design(s) (integrity levels 4 and 3)<br>Task report(s)—Review of software integration test design(s) (integrity level 2) |

| 9.3 Activity: Software Design V&V (Software, 12207—Software Architecture Design process, Software Detailed Design process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| satisfy the criteria in V&V activity 9.3, Task 6.<br>b) Integrity levels 1 and 2<br>1) Verify that the developer's designs for software integration testing conform to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>2) Validate that the developer's software integration test designs satisfy the criteria in V&V activity 9.3, Task 6.<br>c) Integrity level 1<br>There are no software integration test design V&V requirements. | | Anomaly report(s) |
| **(9) Software Qualification Test Design V&V**<br>a) Integrity levels 4 and 3<br>1) Design tests for V&V software qualification testing.<br>2) Continue tracing required by the V&V software qualification test plan. Verify that the V&V software qualification test designs conform to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>3) Validate that the V&V software qualification test designs satisfy the criteria in V&V activity 9.2, Task 5.<br>b) Integrity level 2<br>1) Verify that the developer's designs for software qualification testing conform to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>2) Validate that the developer's software qualification test designs satisfy the criteria in V&V activity 9.2, Task 5.<br>c) Integrity level 1<br>There are no software integration test plan V&V requirements. | SDD<br>IDD<br>User documentation<br>Software qualification test plans<br>Software qualification test designs | V&V software qualification test design(s) (integrity levels 4 and 3)<br>Task report(s)—Review of software qualification test design(s) (integrity level 2)<br>Anomaly report(s) |
| **(10) Software Acceptance Test Design V&V**<br>a) Integrity levels 4 and 3<br>1) Design tests for V&V software acceptance testing.<br>2) Continue tracing required by the V&V software acceptance test plan. Verify that the V&V software acceptance test designs conform to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>3) Validate that the V&V software acceptance test designs satisfy the criteria in V&V activity 9.2, Task 6.<br>b) Integrity level 2<br>1) Verify that the acquirer's test designs for software acceptance testing conform to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>2) Validate that the acquirer's software acceptance test designs satisfy the criteria in V&V activity 9.2, Task 6.<br>c) Integrity level 1<br>There are no software acceptance V&V test requirements. | SDD<br>IDD<br>User documentation<br>Software acceptance test plans<br>Software acceptance test designs | V&V software acceptance test design(s) (integrity levels 4 and 3)<br>Task report(s)—Review of software acceptance test design(s) (integrity level 2)<br>Anomaly report(s) |

| 9.3 Activity: Software Design V&V (Software, 12207—Software Architecture Design process, Software Detailed Design process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(11) Hazard Analysis**<br>a) Verify the logic design and associated data elements that implement critical requirements introduce no new hazards.<br>b) Assess the identified mitigation strategies to verify each hazard is prevented, mitigated, or controlled (any unmitigated hazards are documented and addressed as part of the system and software operations).<br>c) Update the hazard analysis. | SDD<br>IDD<br>Hazard analysis Report | Task report(s)—Hazard analysis<br>Anomaly report(s) |
| **(12) Security Analysis**<br>a) Verify that the architecture and detailed design outputs adequately address the identified security requirements. This verification includes both the system itself and security risks introduced as a result of interfacing with external components.<br>b) Verify the identified security threats and vulnerabilities are prevented, controlled, or mitigated (any unmitigated threats and vulnerabilities are documented and addressed as part of the system and software operations). | SDD<br>IDD<br>Subsystems security analysis<br>Security analysis report<br>V&V task results | Task report(s)—Security analysis<br>Anomaly report(s) |
| **(13) Risk Analysis**<br>a) Review and update risk analysis using prior task reports.<br>b) Provide recommendations to eliminate, reduce, or mitigate the risks. | SDD<br>IDD<br>Supplier development plans and schedules<br>Hazard analysis report<br>Security analysis report<br>Risk analysis report<br>V&V task results | Task report(s)—Risk analysis<br>Anomaly report(s) |

| 9.4 Activity: Software Construction V&V (Software, 12207—Software Construction process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(1) Source Code and Source Code Documentation Evaluation**<br>Evaluate the source code components (source code and source code documentation) for correctness, consistency, completeness, accuracy, readability, and testability. The task criteria are as follows:<br>a) Correctness<br>1) Verify and validate that the source code component satisfies the software design.<br>2) Verify that the source code components comply with standards, references, regulations, policies, physical laws, and business rules.<br>3) Validate the source code component sequences of states and state changes using logic and data flows coupled with domain expertise, prototyping results, engineering principles, or other basis.<br>4) Validate that the software code and its interactions with other elements do not result in unnecessary, unintended, or deleterious consequences.<br>5) Validate that the flow of data and control satisfy functionality and performance requirements. | Source Code<br>SDD<br>IDD<br>Coding standards (e.g., standards, practices, project restrictions, and conventions)<br>User documentation | Task report(s)—Source code and source code documentation evaluation<br>Anomaly report(s) |

| 9.4 Activity: Software Construction V&V (Software, 12207—Software Construction process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| 6) Validate data usage and format.<br>7) Assess the appropriateness of coding methods and standards.<br>b) Consistency<br>1) Verify that all terms and code concepts are documented consistently.<br>2) Verify that there is internal consistency between the source code components.<br>3) Validate external consistency with the software design and requirements.<br>c) Completeness<br>1) Verify that the following elements are in the source code, within the assumptions and constraints of the system:<br>i) Functionality (e.g., algorithms, state/mode definitions, input/output validation, exception handling, reporting, and logging).<br>ii) Process definition and scheduling.<br>iii) Hardware, software, and user interface descriptions.<br>iv) Performance criteria (e.g., timing, sizing, speed, capacity, accuracy, precision, safety, and security).<br>v) Critical configuration data.<br>vi) System, device, and software control (e.g., initialization, transaction and state monitoring, defensive programming practices, and self-testing).<br>2) Verify that the source code documentation satisfies specified coding standards.<br>d) Accuracy<br>1) Validate the logic, computational, and interface precision (e.g., truncation and rounding) in the system environment.<br>2) Validate that the modeled physical phenomena conform to system accuracy requirements and physical laws.<br>e) Readability<br>1) Verify that the documentation is legible, understandable, and unambiguous to the intended audience.<br>2) Verify that the documentation defines all acronyms, mnemonics, abbreviations, terms, and symbols.<br>f) Testability<br>1) Verify that there are objective acceptance criteria for validating each source code component.<br>2) Verify that each source code component is testable against objective acceptance criteria. | | |
| **(2) Interface Analysis**<br>Verify and validate that the software source code interfaces with hardware, user, operator, software, and other systems for correctness, consistency, completeness, accuracy, and testability. The task criteria are as follows:<br>a) Correctness<br>Validate the external and internal software interface code in the context of system requirements.<br>b) Consistency<br>Verify that the interface code is consistent between source code components and to external interfaces (i.e., hardware, user, | Concept Documentation<br>System requirements<br>SDD<br>IDD<br>Source code<br>User documentation | Task report(s)—Interface analysis<br>Anomaly report(s) |

| 9.4 Activity: Software Construction V&V (Software, 12207—Software Construction process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| operator, and other software).<br>c) Completeness<br>Verify that each interface is described and includes data format and performance criteria (e.g., timing, bandwidth, accuracy, safety, and security).<br>d) Accuracy<br>Verify that each interface provides information with the required accuracy.<br>e) Testability<br>Verify that there are objective acceptance criteria for validating the interface code. | | |
| **(3) Traceability Analysis**<br>a) Trace the source code components to corresponding design specification(s), and design specification(s) to source code components.<br>b) Analyze identified relationships for correctness, consistency, and completeness. The task criteria are as follows:<br>1) Correctness<br>Validate the relationship between the source code components and design element(s).<br>2) Consistency<br>Verify that the relationships between the source code components and design elements are specified to a consistent level of detail.<br>3) Completeness<br>i) Verify that all source code components are traceable from the design elements.<br>ii) Verify that all design elements are traceable to the source code components. | SDD<br>IDD<br>Source code | Task report(s)—Traceability analysis<br>Anomaly report(s) |
| **(4) Criticality Analysis**<br>a) Review and update the existing criticality analysis results from the prior Criticality Task Report using the source code.<br>b) Implementation methods and interfacing technologies may cause previously assigned integrity levels to be raised or lowered for a given software element (i.e., requirement, module, function, subsystem, or other software partition). Verify that no inconsistent or undesired integrity consequences are introduced by reviewing the revised integrity levels. | Criticality task report<br>Source code | Task report(s)—Criticality analysis<br>Anomaly report(s) |
| **(5) Software Component Test Case V&V**<br>a) Integrity levels 4 and 3<br>1) Develop test cases for V&V software component testing (e.g., statistical sampling, boundary conditions, and code coverage).<br>2) Continue tracing required by the V&V software component test plan.<br>3) Verify that the software component test cases conform to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>4) Validate that the software component test cases satisfy the criteria in V&V activity 9.3, Task 5.<br>b) Integrity level 2<br>1) Verify that the developer's software component test cases | SRS<br>IRS<br>SDD<br>IDD<br>User documentation<br>Software component test design<br>Software component test cases | V&V software component test cases (integrity levels 4 and 3)<br>Task report(s)—Review of software component test cases (integrity level 2)<br>Anomaly report(s) |

| 9.4 Activity: Software Construction V&V (Software, 12207—Software Construction process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| conform to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>2) Validate that the developer's software component test cases satisfy the criteria in V&V activity 9.3, Task 5.<br>c) Integrity level 1<br>There are no software component V&V test requirements. | | |
| **(6) Software Integration Test Case V&V**<br>a) Integrity levels 4 and 3<br>1) Develop test cases for V&V software integration testing.<br>2) Continue tracing required by the V&V software integration test plan.<br>3) Verify that the V&V software integration test cases conform to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>4) Validate that the V&V software integration test cases satisfy the criteria in V&V activity 9.3, Task 6.<br>b) Integrity level 2<br>1) Verify that the developer's software integration test cases conform to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>2) Validate that the developer's software integration test cases satisfy the criteria in V&V activity 9.3, Task 6.<br>c) Integrity level 1<br>There are no software integration test case V&V requirements. | SRS<br>IRS<br>SDD<br>IDD<br>User documentation<br>Software integration test design<br>Software integration test cases | V&V software integration test cases (integrity levels 4 and 3)<br>Task report(s)—Review of software integration test cases (integrity level 2)<br>Anomaly report(s) |
| **(7) Software Qualification Test Case V&V**<br>a) Integrity levels 4 and 3<br>1) Develop test cases for V&V software qualification testing.<br>2) Continue tracing required by the V&V software qualification test plan.<br>3) Verify that the V&V software qualification test cases conform to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>4) Validate that the V&V software qualification test cases satisfy the criteria in V&V activity 9.2, Task 5.<br>b) Integrity level 2<br>1) Verify that the developer's software qualification test cases conform to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>2) Validate that the developer's software qualification test cases satisfy the criteria in V&V activity 9.2, Task 5.<br>c) Integrity level 1<br>There are no software qualification test case V&V requirements. | SRS<br>IRS<br>SDD<br>IDD<br>User documentation<br>Software qualification test design<br>Software qualification test cases | V&V software qualification test cases (integrity levels 4 and 3)<br>Task report(s)—Review of software qualification test cases (integrity level 2)<br>Anomaly report(s) |
| **(8) Software Acceptance Test Case V&V**<br>a) Integrity levels 4 and 3<br>1) Develop test cases for V&V software acceptance testing.<br>2) Continue tracing required by the V&V software acceptance test plan.<br>3) Verify that the V&V software acceptance test cases conform to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]). | SRS<br>IRS<br>SDD<br>IDD<br>User documentation<br>Software acceptance test design | V&V software acceptance test cases (integrity levels 4 and 3)<br>Task report(s)—Review of software acceptance test cases (integrity level 2) |

| 9.4 Activity: Software Construction V&V (Software, 12207—Software Construction process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| 4) Validate that the V&V software acceptance test cases satisfy the criteria in V&V activity 9.2, Task 6.<br>b) Integrity level 2<br>1) Verify that the acquirer's software acceptance test cases conform to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>2) Validate that the acquirer's software acceptance test cases satisfy the criteria in V&V activity 9.2, Task 6.<br>c) Integrity level 1<br>There are no software acceptance V&V test requirements. | Software acceptance test cases | Anomaly report(s) |
| **(9) Software Component Test Procedure V&V**<br>a) Integrity levels 4 and 3<br>1) Develop test procedures for V&V software component testing.<br>2) Continue tracing required by the V&V software component test plan.<br>3) Verify that the V&V software component test procedures conform to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>4) Validate that the V&V software component test procedures satisfy the criteria in V&V activity 9.3, Task 5.<br>b) Integrity level 2<br>1) Verify that the developer's software component test procedures conform to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>2) Validate that the developer's software component test procedures satisfy the criteria in V&V activity 9.3, Task 5.<br>c) Integrity level 1<br>There are no software component V&V test requirements. | SRS<br>IRS<br>SDD<br>IDD<br>User documentation<br>Software component test cases<br>Software component test procedures | V&V software component test procedures (integrity levels 4 and 3)<br>Task report(s)—Review of software component test procedures (integrity level 2)<br>Anomaly report(s) |
| **(10) Software Integration Test Procedure V&V**<br>a) Integrity levels 4 and 3<br>1) Develop test procedures for V&V software integration testing.<br>2) Continue tracing required by the V&V software integration test plan.<br>3) Verify that the V&V software integration test procedures conform to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>4) Validate that the V&V software integration test procedures satisfy the criteria in V&V activity 9.3, Task 6.<br>b) Integrity level 2<br>1) Verify that the developer's software integration test procedures conform to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>2) Validate that the developer's software integration test procedures satisfy the criteria in V&V activity 9.3, Task 6.<br>c) Integrity level 1<br>There are no software integration test procedure V&V requirements. | SRS<br>IRS<br>SDD<br>IDD<br>User documentation<br>Software integration test cases<br>Software integration test procedures | V&V software integration test procedures (integrity levels 4 and 3)<br>Task report(s)—Review of software integration test procedures (integrity level 2)<br>Anomaly report(s) |

| 9.4 Activity: Software Construction V&V (Software, 12207—Software Construction process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(11) Software Qualification Test Procedure V&V**<br>Integrity levels 4 and 3<br>1) Develop test procedures for V&V software qualification testing.<br>2) Continue tracing required by the V&V software qualification test plan.<br>3) Verify that the V&V software qualification test procedures conform to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>4) Validate that the V&V software qualification test procedures satisfy the criteria in V&V activity 9.2 Task 5.<br>b) Integrity level 2<br>1) Verify that the developer's software qualification test procedures conform to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>2) Validate that the developer's software qualification test procedures satisfy the criteria in V&V activity 9.2 Task 5.<br>c) Integrity level 1<br>There are no software qualification test procedure V&V requirements. | SRS<br>IRS<br>SDD<br>IDD<br>User documentation<br>Software qualification test cases<br>Software qualification test procedures | V&V software qualification test procedures (integrity levels 4 and 3)<br>Task report(s)—Review of software qualification test procedures (integrity level 2)<br>Anomaly report(s) |
| **(12) Software Component Test Execution V&V**<br>a) Integrity levels 4 and 3<br>1) Perform V&V software component testing.<br>2) Analyze test results to validate that software correctly implements the design.<br>3) Validate that the test results trace to test criteria established by the test traceability in the test planning documents.<br>4) Document the results as required by the V&V software component test plan.<br>5) Use the V&V software component test results to validate that the software satisfies the test acceptance criteria.<br>6) Document discrepancies between the actual and expected test results.<br>b) Integrity level 2<br>Use the developer's software component test results to validate that the software satisfies the test acceptance criteria.<br>c) Integrity level 1<br>There are no software component V&V test requirements. | Source code<br>Executable code<br>SDD<br>IDD<br>Software component test plans<br>Software component test procedures<br>Software component test results | Task report(s)—V&V software component test results (integrity levels 4 and 3)<br>Task report(s)—Review of software component test execution results (integrity level 2)<br>Anomaly report(s) |
| **(13) Hazard Analysis**<br>a) Verify that the implementation and associated data elements correctly implement the critical requirements and introduce no new hazards.<br>b) Assess the identified mitigation strategies to verify each hazard is prevented, mitigated, or controlled (any unmitigated hazards are documented and addressed as part of the system and software operations).<br>c) Update the hazard analysis. | Source code<br>SDD<br>IDD<br>Hazard analysis Report | Task report(s)—Hazard analysis<br>Anomaly report(s) |
| **(14) Security Analysis**<br>a) Verify that the implementation is completed in accordance with the system design in that it addresses the identified security risks and that the implementation does not introduce new | Source code<br>SDD<br>IDD | Task report(s)—Security analysis<br>Anomaly report(s) |

| 9.4 Activity: Software Construction V&V (Software, 12207—Software Construction process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| security risks through coding flaws, or compiler error.<br>b) Verify the identified security threats and vulnerabilities are prevented, controlled, or mitigated (any unmitigated threats and vulnerabilities are documented and addressed as part of the system and software operations). | Security analysis report | |
| **(15) Risk Analysis**<br>Review and update risk analysis using prior task reports. Provide recommendations to eliminate, reduce, or mitigate the risks. | Source code<br>Supplier development plans and schedules<br>Hazard analysis report<br>Security analysis report<br>Risk analysis report<br>V&V task results | Task report(s)—Risk analysis<br>Anomaly report(s) |

| 9.5 Activity: Software Integration V&V (Software, 12207—Software Integration process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(1) Software Integration Test Execution V&V**<br>a) Integrity levels 4 and 3<br>1) Perform V&V software integration testing.<br>2) Analyze test results to verify that the software components are integrated correctly.<br>3) Validate that the test results trace to test criteria established by the test traceability in the test planning documents.<br>4) Document the results as required by the V&V software integration test plan.<br>5) Use the V&V software integration test results to validate that the software satisfies the test acceptance criteria.<br>6) Document discrepancies between the actual and expected test results.<br>b) Integrity level 2<br>Use the developer's software integration test results to verify that the software satisfies the test acceptance criteria.<br>c) Integrity level 1<br>There are no software integration test execution V&V requirements. | Source code<br>Executable code<br>Software integration test plan<br>Software integration test procedures<br>Software integration test results | Task report(s)—V&V software integration test results (integrity levels 4 and 3)<br>Task report(s)—Review of software integration test execution results (integrity level 2)<br>Anomaly report(s) |
| **(2) Traceability Analysis**<br>Analyze relationships in the V&V Test Plans, Designs, Cases, and Procedures for correctness and completeness. The task criteria are as follows:<br>a) Correctness<br>Verify that there is a valid relationship between the V&V Test Plans, Designs, Cases, and Procedures.<br>b) Completeness<br>Verify that all V&V Test Procedures are traceable to the V&V Test Plans. | V&V test plans<br>V&V test designs<br>V&V test procedures | Task report(s)—Traceability analysis<br>Anomaly report(s) |
| **(3) Hazard Analysis**<br>a) Verify that the test instrumentation does not introduce new hazards. | Source code<br>Executable code<br>Test results | Task report(s)—Hazard analysis<br>Anomaly report(s) |

| 9.5 Activity: Software Integration V&V (Software, 12207—Software Integration process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| b) Assess the identified mitigation strategies to verify each hazard is prevented, mitigated, or controlled (any unmitigated hazards are documented and addressed as part of the system and software operations).<br>c) Update the hazard analysis. | Hazard analysis report | |
| **(4) Security Analysis**<br>a) Verify that the implemented system does not increase the security risk.<br>b) Verify the identified security threats and vulnerabilities are prevented, controlled, or mitigated (any unmitigated threats and vulnerabilities are documented and addressed as part of the system and software operations). | Source code<br>Executable code<br>Security analysis report | Task report(s)—Security analysis<br>Anomaly report(s) |
| **(5) Risk Analysis**<br>a) Review and update risk analysis using prior task reports.<br>b) Provide recommendations to eliminate, reduce, or mitigate the risks. | Supplier development plans and schedules<br>Hazard analysis report<br>Security analysis report<br>Risk analysis report<br>V&V task results | Task report(s)—Risk analysis<br>Anomaly report(s) |

| 9.6 Activity: Software Qualification Testing V&V (Software, 12207—Software Qualification Testing process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(1) Software Qualification Test Execution V&V**<br>a) Integrity levels 4 and 3<br>1) Perform V&V software qualification testing.<br>2) Analyze test results to validate that the software satisfies the system requirements.<br>3) Validate that the test results trace to test criteria established by the test traceability in the test planning documents.<br>4) Document the results as required by the V&V software qualification test plan.<br>5) Use the V&V software qualification test results to validate that the software satisfies the test acceptance criteria.<br>6) Document discrepancies between the actual and expected test results.<br>b) Integrity level 2<br>Use the developer's software qualification test results to verify that the software satisfies the test acceptance criteria.<br>c) Integrity level 1<br>There are no software qualification test execution V&V requirements. | Source code<br>Executable code<br>Software qualification test plan<br>Software qualification test procedures<br>Software qualification test results | Task report(s)—V&V software qualification test results (integrity levels 4 and 3)<br>Task report(s)—Review of software qualification test execution results (integrity level 2)<br>Anomaly report(s) |
| **(2) Traceability Analysis**<br>Analyze the relationships in the V&V software qualification test plans, designs, cases, and procedures for correctness and completeness. The task criteria are as follows:<br>a) Correctness<br>Verify that there is a valid relationship between the V&V software qualification test plans, designs, cases, and procedures. | V&V software qualification test plans<br>V&V software qualification test designs<br>V&V software | Task report(s)—Traceability analysis<br>Anomaly report(s) |

| 9.6 Activity: Software Qualification Testing V&V (Software, 12207—Software Qualification Testing process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| b) Completeness<br>Verify that all V&V software qualification test procedures are traceable to the V&V test plans. | qualification test cases<br>V&V software qualification test procedures | |
| **(3) Hazard Analysis**<br>a) Verify that the test instrumentation does not introduce new hazards.<br>b) Assess the identified mitigation strategies to verify each hazard is prevented, mitigated, or controlled (any unmitigated hazards are documented and addressed as part of the system and software operations).<br>c) Update the hazard analysis. | Source code<br>Executable code<br>Test results<br>Hazard analysis report | Task report(s)—Hazard analysis<br>Anomaly report(s) |
| **(4) Security Analysis**<br>a) Verify that the implemented system does not increase the security risk.<br>b) Verify the identified security threats and vulnerabilities are prevented, controlled, or mitigated (any unmitigated threats and vulnerabilities are documented and addressed as part of the system and software operations). | Source code<br>Executable code<br>Security analysis report | Task report(s)—Security analysis<br>Anomaly report(s) |
| **(5) Risk Analysis**<br>a) Review and update risk analysis using prior task reports.<br>b) Provide recommendations to eliminate, reduce, or mitigate the risks. | Supplier development plans and schedules<br>Hazard analysis report<br>Security analysis report<br>Risk analysis report<br>V&V task results | Task report(s)—Risk analysis<br>Anomaly report(s) |

| 9.7 Activity: Software Acceptance Testing V&V (Software, 12207—Software Acceptance Support process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(1) Software Acceptance Test Procedure V&V**<br>a) Integrity levels 4 and 3<br>1) Develop test procedures for V&V software acceptance testing.<br>2) Continue the tracing required by the V&V software acceptance test plan.<br>3) Verify that the V&V software acceptance test procedures conform to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>4) Validate that the V&V software acceptance test procedures satisfy the criteria in V&V activity 9.2, Task 6.<br>b) Integrity level 2<br>1) Verify that the acquirer's software acceptance test procedures conform to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>2) Validate that the acquirer's software acceptance test procedures satisfy the criteria in V&V activity 9.2, Task 6.<br>c) Integrity level 1<br>There are no software acceptance V&V test requirements. | SDD<br>IDD<br>Source code<br>User documentation<br>Software acceptance test plan<br>Software acceptance test procedures | V&V software acceptance test procedures (integrity levels 4 and 3)<br>Task report(s)—Review of software acceptance test execution procedures (integrity level 2)<br>Anomaly report(s) |

| 9.7 Activity: Software Acceptance Testing V&V (Software, 12207—Software Acceptance Support process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(2) Software Acceptance Test Execution V&V**<br>a) Integrity levels 4 and 3<br>1) Perform V&V software acceptance testing.<br>2) Analyze test results to validate that the software satisfies the system requirements.<br>3) Validate that the test results trace to test criteria established by the test traceability in the V&V software acceptance test planning documents.<br>4) Document the results as required by the V&V software acceptance test plan.<br>5) Use the V&V software acceptance test results to validate that the software satisfies the V&V test acceptance criteria.<br>6) Document discrepancies between the actual and expected test results.<br>b) Integrity level 2<br>Use the acquirer's software acceptance test results to verify that the software satisfies the test acceptance criteria.<br>c) Integrity level 1<br>There are no software acceptance V&V test requirements. | Source code<br>Executable code<br>User documentation<br>Software acceptance test plan<br>Software acceptance test procedures<br>Software acceptance test results<br>V&V task results | Task report(s)—V&V software acceptance test results (integrity levels 4 and 3)<br>Task report(s)—Review of software acceptance test execution results (integrity level 2)<br>Anomaly report(s) |
| **(3) Traceability Analysis**<br>Analyze the relationships in the V&V software acceptance test plans, designs, cases, and procedures for correctness and completeness. The task criteria are as follows:<br>a) Correctness<br>Verify that there is a valid relationship among the V&V software acceptance test plans, designs, cases, and procedures.<br>b) Completeness<br>Verify that all V&V software acceptance test procedures are traceable to the V&V software acceptance test plans. | V&V software acceptance test plans<br>V&V software acceptance test designs<br>V&V software acceptance test procedures | Task report(s)—Traceability analysis<br>Anomaly report(s) |
| **(4) Hazard Analysis**<br>a) Verify that the test instrumentation does not introduce new hazards.<br>b) Assess the identified mitigation strategies to verify each hazard is prevented, mitigated, or controlled (any unmitigated hazards are documented and addressed as part of the system and software operations).<br>c) Update the hazard analysis. | Source code<br>Executable code<br>Test results<br>Hazard analysis report | Task report(s)—Hazard analysis<br>Anomaly report(s) |
| **(5) Security Analysis**<br>a) Verify that the implemented system does not increase the security risk.<br>b) Verify the identified security threats and vulnerabilities are prevented, controlled, or mitigated (any unmitigated threats and vulnerabilities are documented and addressed as part of the system and software operations). | Source code<br>Executable code<br>Security analysis report | Task report(s)—Security analysis<br>Anomaly report(s) |
| **(6) Risk Analysis**<br>a) Review and update risk analysis using prior task reports.<br>b) Provide recommendations to eliminate, reduce, or mitigate the risks. | Supplier development plans and schedules<br>Hazard analysis report<br>Security analysis report<br>Risk analysis report<br>V&V task results | Task report(s)—Risk analysis<br>Anomaly report(s) |

| 9.8 Activity: Software Verification (Software, 12207—Software Verification process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| The activities and tasks for the Software Verification process are conducted in software technical life cycle processes, and are contained in Table 1c, Activity 9.1 (Software Concept V&V), Activity 9.2 (Software Requirements Analysis V&V), Activity 9.3 (Software Design V&V), Activity 9.4 (Software Construction V&V), Activity 9.5 (Software Integration V&V), Activity 9.6 (Software Qualification Testing V&V), Activity 9.7 (Software Acceptance Testing V&V), Activity 9.9 (Software Installation and Checkout V&V), Activity 9.11 (Software Operation V&V), Activity 9.12 (Software Maintenance V&V), and Activity 9.13 (Software Disposal V&V). The software verification activities and tasks in Table 1c and the common verification activities and tasks in Table 1a represent all activities and tasks needed to perform software verification. | The required inputs for the Software Verification process are found in Table 1c required inputs. | The required outputs for the Software Verification process are found in Table 1c required outputs. |

| 9.9 Activity: Software Installation and Checkout V&V (Software, 12207—Software Installation process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(1) Installation Configuration Audit**<br>a) Verify that all software products required to correctly install and operate the software are present in the installation package.<br>b) Validate that all site-dependent parameters or conditions to verify supplied values are correct. | Installation package (e.g., source code, executable code, user documentation, SDD, IDD, SRS, IRS, concept documentation, installation procedures, site-specific parameters, installation tests, and configuration management data) | Task report(s)—Installation configuration audit<br>Anomaly report(s) |
| **(2) Installation Checkout**<br>a) Conduct analyses or tests to verify that the installed software corresponds to the software subjected to V&V.<br>b) Verify that the software code and databases initialize, execute, and terminate as specified.<br>c) In the transition from one version of software to the next, validate that the software can be replaced with the new version without adversely affecting or degrading the functionality of the remaining system components.<br>d) Verify the requirements for continuous operation and service during transition, including requirements for user notification. | User documentation<br>Installation package | Task report(s)—Installation checkout<br>Anomaly report(s) |
| **(3) Hazard Analysis**<br>a) Verify that the installation procedures and installation environment does not introduce new hazards.<br>b) Assess the identified mitigation strategies to verify each hazard is prevented, mitigated, or controlled (any unmitigated hazards are documented and addressed as part of the system and software operations).<br>c) Update the hazard analysis. | Installation package<br>Hazard analysis report | Task report(s)—Hazard analysis<br>Anomaly report(s) |

| 9.9 Activity: Software Installation and Checkout V&V (Software, 12207—Software Installation process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(4) Security Analysis**<br>a) Verify that the installed software does not introduce new or increased vulnerabilities or security risks to the overall system.<br>b) Verify the identified security threats and vulnerabilities are prevented, controlled, or mitigated (any unmitigated threats and vulnerabilities are documented and addressed as part of the system and software operations). | Installation package<br>User documentation<br>Security analysis report | Task report(s)—Security analysis<br>Anomaly report(s) |
| **(5) Risk Analysis**<br>a) Review and update risk analysis using prior task reports.<br>b) Provide recommendations to eliminate, reduce, or mitigate the risks. | Installation package<br>Supplier development plans and schedules<br>Hazard analysis report<br>Security analysis report<br>Risk analysis report<br>V&V task results | Task report(s)—Risk analysis<br>Anomaly report(s) |

| 9.10 Activity: Software Validation (Software, 12207—Software Validation process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| The activities and tasks for the Software Validation process are conducted in software technical life cycle processes, and are contained in Table 1c, Activity 9.1 (Software Concept V&V), Activity 9.2 (Software Requirements Analysis V&V), Activity 9.3 (Software Design V&V), Activity 9.4 (Software Construction V&V), Activity 9.5 (Software Integration V&V), Activity 9.6 (Software Qualification Testing V&V), Activity 9.7 (Software Acceptance Testing V&V), Activity 9.9 (Software Installation and Checkout V&V), Activity 9.11 (Software Operation V&V), Activity 9.12 (Software Maintenance V&V), and Activity 9.13 (Software Disposal V&V). The software Validation activities and tasks in Table 1c and the common Validation activities and tasks in Table 1a represent all activities and tasks needed to perform software validation. | The required inputs for the Software Validation process are found in Table 1c required inputs. | The required outputs for the Software Validation process are found in Table 1c required outputs. |

| 9.11 Activity: Software Operation V&V (Software, 12207—Software Operation process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(1) Evaluation of New Constraints**<br>Evaluate new constraints (e.g., operational requirements, platform characteristics, and operating environment) on the system or software requirements to verify the applicability of the VVP. | VVP<br>New constraints | Task report(s)—Evaluation of new constraints |
| **(2) Operating Procedures Evaluation**<br>Verify that the operating procedures are consistent with the user documentation and conform to the system requirements. | Operating procedures<br>User documentation<br>Concept documentation | Task report(s)—Operating procedures evaluation<br>Anomaly report(s) |
| **(3) Hazard Analysis**<br>a) Verify that the operating procedures and operational environment do not introduce new hazards.<br>b) Assess the identified mitigation strategies to verify each hazard | Operating procedures<br>Hazard analysis report | Task report(s)—Hazard analysis<br>Anomaly report(s) |

| 9.11 Activity: Software Operation V&V (Software, 12207—Software Operation process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| is prevented, mitigated, or controlled (any unmitigated hazards are documented and addressed as part of the system and software operations).<br>c) Update the hazard analysis. | | |
| **(4) Security Analysis**<br>a) Verify that no new security risks are introduced due to changes in the operational environment.<br>b) Over time, changes in external interfaces, threats, or technology in general require that an updated security analysis be performed to determine an updated residual risk.<br>c) Verify the identified security threats and vulnerabilities are prevented, controlled, or mitigated (any unmitigated threats and vulnerabilities are documented and addressed as part of the system and software operations). | New constraints<br>Environmental changes<br>Operating procedures<br>Security analysis report | Task report(s)—Security analysis |
| **(5) Risk Analysis**<br>a) Review and update risk analysis using prior task reports.<br>b) Provide recommendations to eliminate, reduce, or mitigate the risks. | Installation package<br>Proposed changes<br>Hazard analysis report<br>Security analysis report<br>Risk analysis report<br>Supplier development plans and schedules<br>Operation problem reports<br>V&V task results | Task report(s)—Risk analysis<br>Anomaly report(s) |

| 9.12 Activity: Software Maintenance V&V (Software, 12207—Software process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(1) VVP Revision**<br>a) Revise the VVP to conform to the approved changes.<br>b) When the development documentation required by this standard is not available, generate a new VVP and consider the methods in Annex D for deriving the required development documentation. | VVP<br>Approved changes<br>Installation package<br>Supplier development plans and schedules | Updated VVP |
| **(2) Anomaly Evaluation**<br>Evaluate the effect of software operation anomalies. | Anomaly report(s) | Task report(s)—Anomaly evaluation |
| **(3) Criticality Analysis**<br>a) Determine the integrity levels for the proposed modifications.<br>b) Validate the integrity levels provided by the maintainer. For V&V planning purposes, the highest integrity level assigned to the software shall be the integrity level of the system. | Proposed changes<br>Installation package<br>Maintainer integrity levels | Task report(s)—Criticality analysis<br>Anomaly report(s) |
| **(4) Migration Assessment**<br>Assess whether the software requirements and implementation address the following:<br>a) Specific migration requirements<br>b) Migration tools<br>c) Conversion of software products and data | Installation package<br>Approved changes | Task report(s)—Migration assessment<br>Anomaly report(s) |

| 9.12 Activity: Software Maintenance V&V (Software, 12207—Software process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| d) Software archiving<br>e) Support for the prior environment<br>f) User notification | | |
| **(5) Retirement Assessment**<br>Assess whether the installation package addresses the following:<br>a) Software support<br>b) Impact on existing systems and data bases<br>c) Software archiving<br>d) Transition to a new software product<br>e) User notification | Installation package<br>Approved changes | Task report(s)—Retirement assessment<br>Anomaly report(s) |
| **(6) Hazard Analysis**<br>a) Verify that software modifications correctly implement the critical requirements and introduce no new hazards.<br>b) Assess the identified mitigation strategies to verify each hazard is prevented, mitigated, or controlled (any unmitigated hazards are documented and addressed as part of the system and software operations).<br>c) Update the hazard analysis. | Proposed changes<br>Installation package<br>Hazard analysis report | Task report(s)—Hazard analysis<br>Anomaly report(s) |
| **(7) Security Analysis**<br>a) Verify that the proposed changes/updates to the software do not introduce new or increased security risks to the overall system.<br>b) Verify the identified security threats and vulnerabilities are prevented, controlled, or mitigated (any unmitigated threats and vulnerabilities are documented and addressed as part of the system and software operations). | Proposed changes<br>Installation package<br>Security analysis report | Task reports—Security analysis |
| **(8) Risk Analysis**<br>a) Review and update risk analysis using prior task reports.<br>b) Provide recommendations to eliminate, reduce, or mitigate the risks. | Installation package<br>Proposed changes<br>Hazard analysis report<br>Security analysis report<br>Risk analysis report<br>Supplier development plans and schedules<br>Operation problem reports<br>V&V task results | Task report(s)—Risk analysis<br>Anomaly report(s) |
| **(9) Task Iteration**<br>Perform V&V tasks, as needed, to assure the following are performed:<br>a) Planned changes are implemented correctly.<br>b) Documentation is complete and current.<br>c) Changes do not cause unacceptable or unintended system behaviors. | Approved changes<br>Installation package | Task report(s)<br>Anomaly report(s) |
| NOTE—Software changes are maintenance activities (see Clause 9.12). | | |

| 9.13 Activity: Software Disposal V&V (Software, 12207—Software process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(1) Software Disposal Evaluation**<br>Verify that any constraints specified or implied by the software disposal strategy are included in the software requirements, including software element destruction/storage and recording disposal actions and analysis of disposal impacts on the system. Validate that disposal leaves the system in an agreed-on state. | Software disposal strategy | Task report(s)—Software Disposal Evaluation<br>Anomaly report(s) |

NOTE (for Table 1c)—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 2c—Minimum V&V tasks assigned to each integrity level for software V&V**

| V&V Activities | Activity: Software Concept V&V (see 9.1) | | | | Activity: Software Requirements V&V (see 9.2) | | | | Activity: Software Design V&V (see 9.3) | | | | Activity: Software Construction V&V (see 9.4) | | | | Activity: Software Integration V&V (see 9.5) | | | | Activity: Software Qualification V&V (see 9.6) | | | | Activity: Software Acceptance V&V (see 9.7) | | | | Activity: Software Installation and Checkout V&V (see 9.9) | | | | Activity: Software Operation V&V (see 9.11) | | | | Activity: Software Maintenance V&V (see 9.12) | | | | Activity: Software Disposal V&V (see 9.13) | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Integrity Levels | Levels | | | | Levels | | | | Levels | | | | Levels | | | | Levels | | | | 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 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 |
| Anomaly Evaluation | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | X | X | X | | | | | |
| Concept Documentation Evaluation | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Criticality Analysis | X | X | X | X | X | X | X | X | X | X | X | | X | X | X | | | | | | | | | | | | | | | | | | | | | | X | X | X | X | | | | |
| Design Evaluation | | | | | | | | | X | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Evaluation of New Constraints | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | X | X | X | | | | | | | | | |
| Hazard Analysis | X | X | | | X | X | | | X | X | | | X | X | | | X | X | | | X | X | | | X | X | | | X | X | | | X | X | | | X | X | | | | | | |
| Installation Checkout | | | | | | | | | | | | | | | | | | | | | | | | | | | | | X | X | | | | | | | | | | | | | | |
| Installation Configuration Audit | | | | | | | | | | | | | | | | | | | | | | | | | | | | | X | X | | | | | | | | | | | | | | |
| Interface Analysis | | | | | X | X | X | | X | X | X | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Migration Assessment | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | X | X | | | | | | |
| Operation Procedures Evaluation | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | X | X | | | | | | | | | | |
| Requirements Allocation Analysis | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Requirements Evaluation | | | | | X | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Retirement Assessment | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | X | X | | | | | | |
| Risk Analysis | X | X | | | X | X | | | X | X | | | X | X | | | X | X | | | X | X | | | X | X | | | X | X | | | X | X | | | X | X | | | | | | |

| V&V Activities | Activity: Software Concept V&V (see 9.1) | | | | Activity: Software Requirements V&V (see 9.2) | | | | Activity: Software Design V&V (see 9.3) | | | | Activity: Software Construction V&V (see 9.4) | | | | Activity: Software Integration V&V (see 9.5) | | | | Activity: Software Qualification V&V (see 9.6) | | | | Activity: Software Acceptance V&V (see 9.7) | | | | Activity: Software Installation and Checkout V&V (see 9.9) | | | | Activity: Software Operation V&V (see 9.11) | | | | Activity: Software Maintenance V&V (see 9.12) | | | | Activity: Software Disposal V&V (see 9.13) | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Integrity Levels | Levels | | | | Levels | | | | Levels | | | | Levels | | | | Levels | | | | 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 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 |
| Security Analysis | X | X | | | X | X | | | X | X | | | X | X | | | X | X | | | X | X | | | X | X | | | X | X | | | X | X | | | X | X | | | | | | |
| Software Acceptance Test Case V&V | | | | | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Software Acceptance Test Design V&V | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Software Acceptance Test Execution V&V | | | | | | | | | | | | | | | | | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | |
| Software Acceptance Test Plan V&V | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Software Acceptance Test Procedure V&V | | | | | | | | | | | | | | | | | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | |
| Software Component Test Case V&V | | | | | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Software Component Test Design V&V | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Software Component Test Execution V&V | | | | | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Software Component Test Plan V&V | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Software Component Test Procedure V&V | | | | | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Software Disposal Evaluation | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | X | X | | |
| Software Integration Test Case V&V | | | | | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Software Integration Test Design V&V | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Software Integration Test Execution V&V | | | | | | | | | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | |
| Software Integration Test Plan V&V | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Software Integration Test Procedure V&V | | | | | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| V&V Activities | Activity: Software Concept V&V (see 9.1) | | | | Activity: Software Requirements V&V (see 9.2) | | | | Activity: Software Design V&V (see 9.3) | | | | Activity: Software Construction V&V (see 9.4) | | | | Activity: Software Integration V&V (see 9.5) | | | | Activity: Software Qualification V&V (see 9.6) | | | | Activity: Software Acceptance V&V (see 9.7) | | | | Activity: Software Installation and Checkout V&V (see 9.9) | | | | Activity: Software Operation V&V (see 9.11) | | | | Activity: Software Maintenance V&V (see 9.12) | | | | Activity: Software Disposal V&V (see 9.13) | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Integrity Levels | Levels | | | | Levels | | | | Levels | | | | Levels | | | | Levels | | | | 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 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 |
| Software Qualification Test Case V&V | | | | | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Software Qualification Test Design V&V | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Software Qualification Test Execution V&V | | | | | | | | | | | | | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | |
| Software Qualification Test Plan V&V | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Software Qualification Test Procedure V&V | | | | | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Source Code and Source Code Doc. Evaluation | | | | | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Task Iteration | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | X | X | X | X | | | | |
| Traceability Analysis | X | X | X | | X | X | X | | X | X | X | | X | X | X | | X | X | X | | X | X | X | | X | X | X | | | | | | | | | | | | | | | |
| VVP Revision | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | X | X | X | X | | | | |

NOTE (for Table 2c)—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. Higher integrity level implementation requires greater rigor (e.g., formal methods and structured analysis methods), intensity (e.g., consideration of all system conditions and system environment states), and depth (e.g., abnormal cases, boundary conditions, and comprehensive fault and recovery scenarios) of the analysis or test than the lower integrity level implementation.

The recommended applicability of optional tasks to the Software V&V processes described in Clause 9 is shown in Table 3a. Annex G provides a description of each of the optional V&V tasks.

**Table 3c—Optional V&V tasks and suggested applications in software technical and implementation processes**

| | Software Concept (9.1) | Software Requirements Analysis (9.2) | Software Design (9.3) | Software Construction (9.4) | Software Integration (9.5) | Software Qualification Testing (9.6) | Software Acceptance Testing (9.7) | Software Installation and Checkout (9.9) | Software Operation (9.11) | Software Maintenance (9.12) | Software Disposal (9.13) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Algorithm analysis | X | X | X | X | | | | | | X | |
| Audit performance | X | X | X | X | X | X | X | X | | X | |
| Audit support | X | X | X | X | X | X | X | X | | X | |
| Control flow analysis | X | X | X | X | | | | | | X | |
| Cost analysis | X | X | X | X | X | X | X | X | | X | |
| Database analysis | X | X | X | X | | | X | | | X | |
| Data flow analysis | X | X | X | X | | | | | | X | |
| Disaster recovery plan assessment | X | X | X | X | | | | | X | X | X |
| Distributed architecture assessment | X | X | | | | | | | | X | |
| Exploratory testing | X | X | X | X | X | X | X | X | X | X | |
| Feasibility study evaluation | X | X | X | | | | | | | X | |
| Independent risk assessment | | | | | | | | | | X | |
| Inspection | | | | | | | | | | | |
| Inspection—Concept | | | | | | | | | | X | |
| Inspection—Requirements | X | | | | | | | | | X | |
| Inspection—Design | | X | X | | | | | | | X | |
| Inspection—Source code | | | | X | | | | | | | |
| Inspection—Test plan | X | X | X | X | X | X | X | | | X | |
| Inspection—Test design | | X | X | X | X | X | X | | | X | |
| Inspection—Test case | | X | X | X | X | X | X | | | X | |
| Operational evaluation | | | | | | | | | X | | |
| Performance monitoring | X | X | X | X | X | X | X | X | X | X | X |
| Post-installation validation | | | | | | | | | X | X | |
| Project management oversight support | X | X | X | X | X | X | X | X | X | X | X |
| Proposal evaluation support | | | | | | | | | | | |
| Qualification testing | | | | X | | X | X | | | | |
| Regression analysis and testing | X | X | | X | X | X | X | | | X | |
| Reusability analysis | X | X | X | X | | | | | | X | |
| Reuse analysis | X | X | X | | | | | | | X | |
| Simulation analysis | X | X | X | X | X | X | X | X | X | X | X |
| Sizing and timing analysis | X | X | X | X | X | X | X | X | | X | |
| System software assessment | | X | X | X | X | X | X | X | X | X | |
| Test certification | | | | X | X | X | X | | X | X | X |
| Test evaluation | X | X | X | X | X | X | X | | X | X | X |
| Test witnessing | | | | X | X | X | X | | X | X | X |
| Training documentation evaluation | X | X | X | X | X | X | X | | X | X | X |
| Usability analysis | X | X | X | X | X | X | X | | X | X | |
| User documentation evaluation | X | X | X | X | X | X | X | | X | X | |
| User training | | | | X | X | X | X | | X | X | |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| V&V tool plan generation | | | | | | | | | | | |
| V&V tool qualification | X | X | X | X | X | X | X | X | X | X | |
| Walkthrough | | | | | | | | | | | |
| Walkthrough—Design | | X | | | | | | | | X | |
| Walkthrough—Requirements | X | | | | | | | | | X | |
| Walkthrough—Source code | | | | X | | | | | | | |
| Walkthrough—Test | | | | X | X | X | | | | X | |
| Work Breakdown Structure (WBS) Evaluation | | | | | | | | | | | |

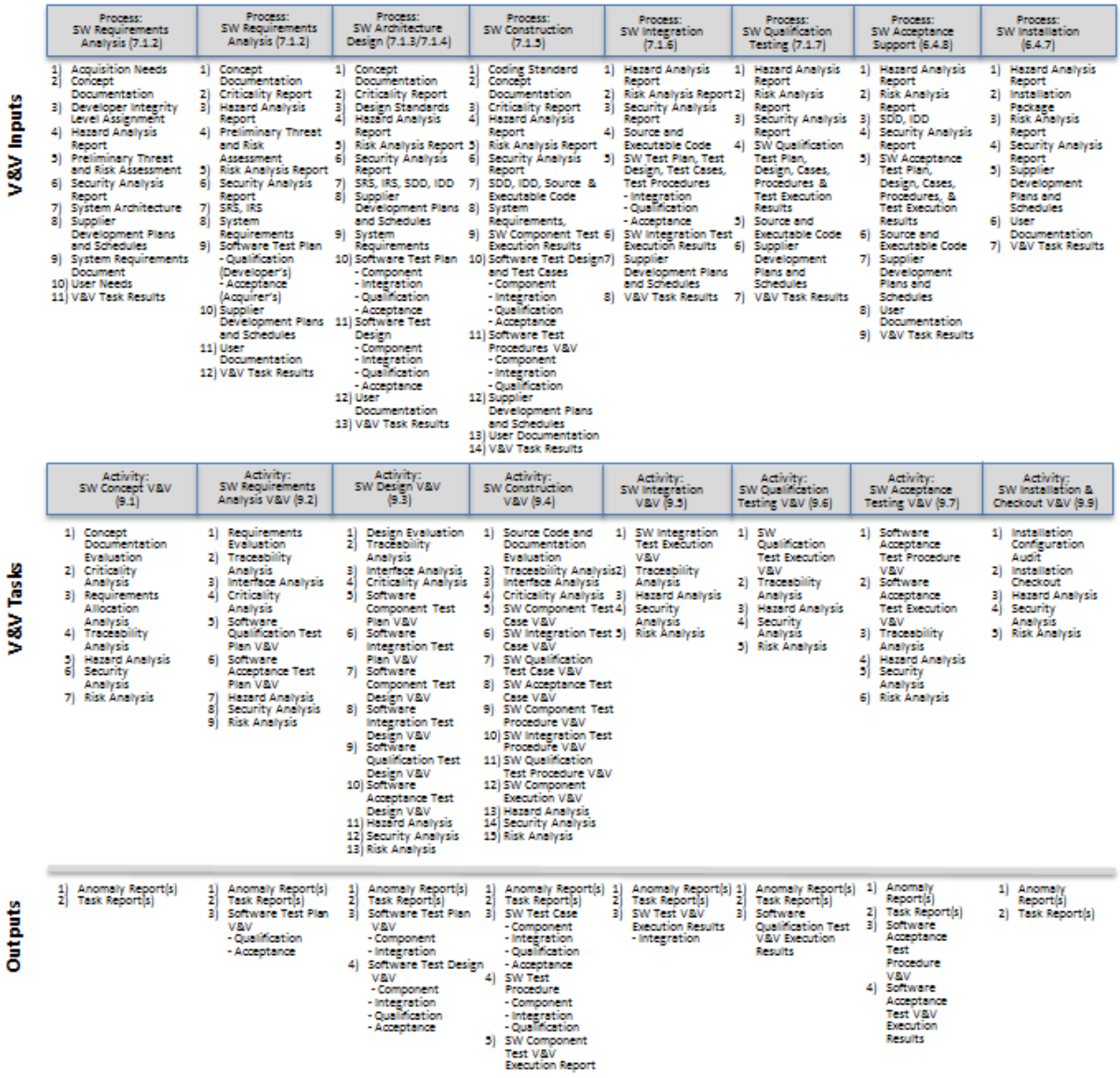
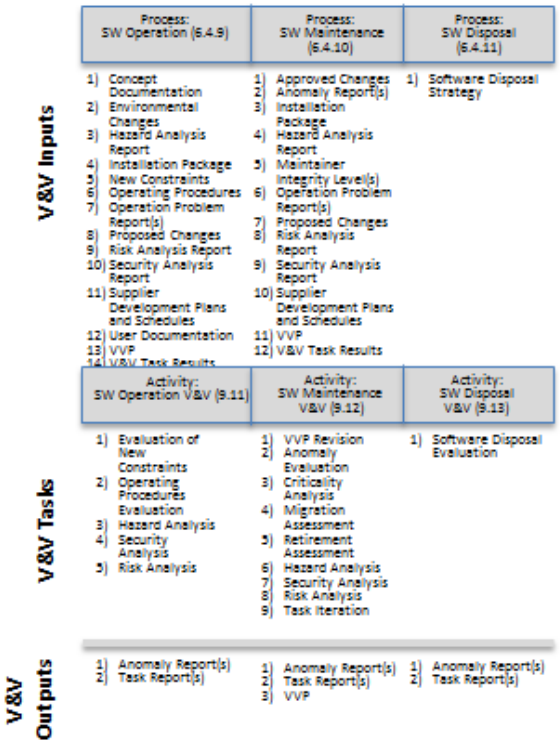



**Figure 1c—Summary of software V&V activities and tasks**




NOTE 1—Clause references in the process definitions (top graphic bar) are ISO/IEC 12207:2008 [B11] clause numbers.

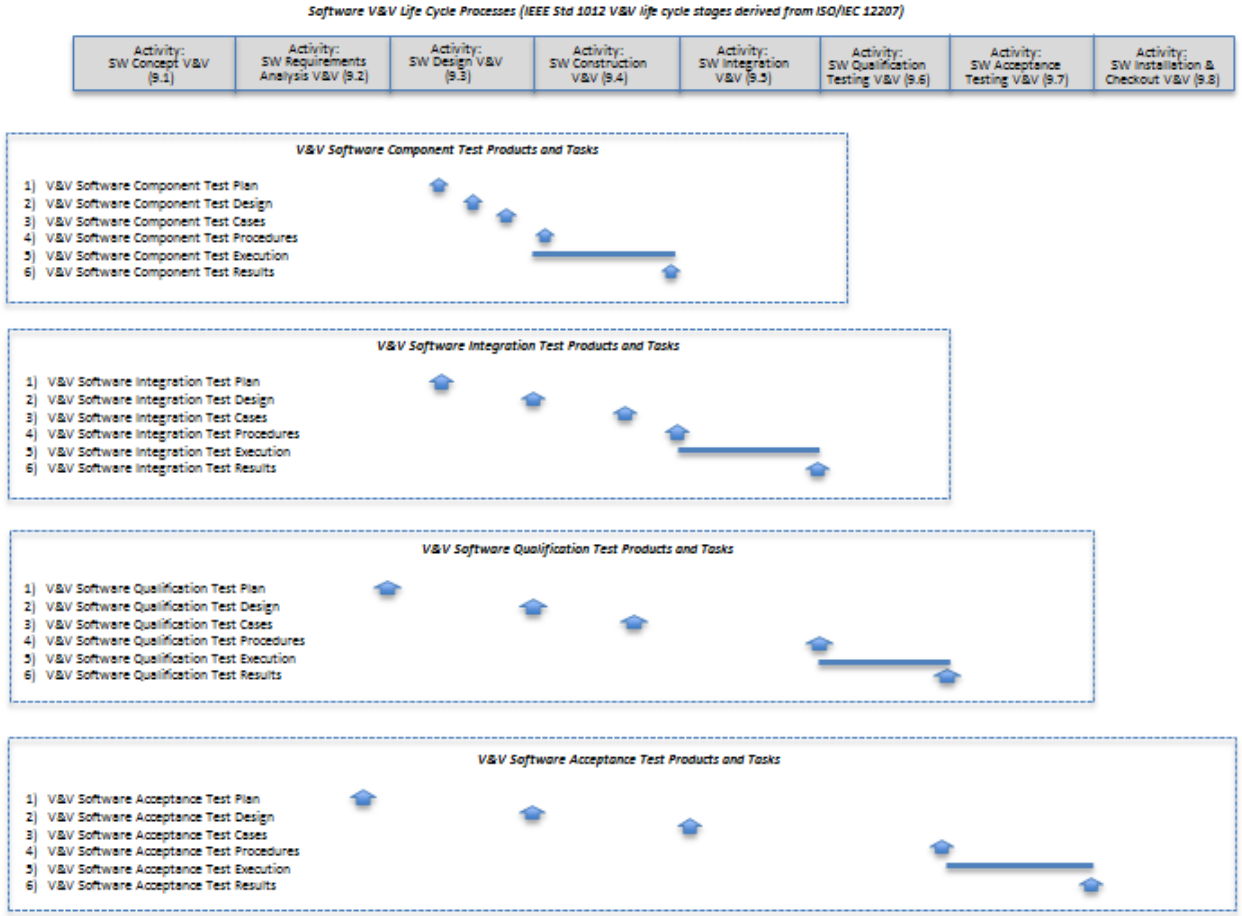
NOTE 2—Clause references in the activity V&V definitions (middle graphic bar) are IEEE Std 1012 clause numbers.

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

NOTE 4—Software Acceptance Testing process supports the Systems Integration Testing process.

NOTE 5—Software Installation and Checkout process supports the System Transition process.

**Figure 1c—Summary of software V&V activities and tasks (continued)**




NOTE 1—All V&V software test products and tasks represent the activities and products required as a minimum for integrity level 4.

NOTE 2—This is an example of the phasing of software V&V test products and tasks across the software life cycle. The software V&V test products (upward arrows) are shown in the software life cycle stages when the products are generated. Software test execution tasks are shown to occur during one or more software life cycle stages as indicated by "activity bars" in the diagram. The life cycle stage (in which each test product is generated) and phasing of each test product and task can vary from this diagram in accordance with project specific needs.

NOTE 3—The V&V activity clauses referenced in the software V&V life cycle stages are IEEE Std 1012 clauses.

**Figure 2c—Summary of software V&V test products and tasks**

# 10. Hardware V&V processes

## 10.1 Hardware Concept V&V process

### 10.1.1 Purpose

The purpose of the Hardware Concept V&V process is to provide assurance that the outcomes of the System Architectural Design process (ISO/IEC 12207:2008 [B11]) related to hardware have been achieved.

### 10.1.2 Outcomes

As a result of the successful implementation of the Hardware Concept V&V process, objective evidence is developed to assess whether:

a) System requirements allocated to hardware components are addressed.

b) Selected hardware concepts satisfy the system needs (i.e., performance and schedule).

### 10.1.3 Activities and tasks

The V&V effort shall perform, as specified in Table 2d for the selected integrity level, the following Hardware Concept V&V activity and tasks described in Table 1d, Activity 10.1:

a) Hardware Concept V&V: This activity consists of the following tasks:

1) Concept Documentation Evaluation
2) Requirements Allocation Analysis
3) Traceability Analysis
4) Criticality Analysis
5) Hazard Analysis
6) Security Analysis
7) Risk Analysis

The primary focus is on hardware with consideration of the interactions with software and user allocations to verify the allocation of system requirements, validate the selected solution, and assure that no false assumptions have been incorporated in the solution.

During the concept process, different hardware concepts are investigated and trade studies are conducted on each concept before a final concept is selected. These trade studies may involve assessing the performance features of each concept, estimating the cost of parts, determining the manufacturing efficiency, identifying the technology risks, and estimating the schedule to develop the hardware. Hardware models and prototypes may be constructed to conduct these trade studies in conjunction with simulations and analytic analyses. The hardware concept stage may provide preliminary hardware models and prototypes to the systems concept stage to support trade studies for system concept definition. In such cases, the hardware concept stage may start before final hardware requirements are allocated.

## 10.2 Hardware Requirements Analysis V&V process

### 10.2.1 Purpose

The purpose of the Hardware Requirements Analysis V&V process is to provide assurance that outcomes of the Hardware Requirements Analysis process, the Hardware Qualification Testing process, and the Hardware Acceptance Support process have been achieved.

### 10.2.2 Outcomes

As a result of the successful implementation of the Hardware Requirements Analysis V&V process, objective evidence is developed to assess whether:

a) The hardware requirements correctly, completely, and accurately satisfy the system requirements allocated to the hardware element.

b) The hardware requirements, in total, satisfy the system needs.

### 10.2.3 Activities and tasks

The V&V effort shall perform, as specified in Table 2d for the selected integrity level, the following Hardware Requirements Analysis V&V tasks described in Table 1d, Activity 10.2:

a) Hardware Requirements Analysis V&V: This activity consists of the following tasks:

1) Requirements Evaluation
2) Interface Analysis
3) Traceability Analysis
4) Criticality Analysis
5) Hardware Qualification Test Plan V&V
6) Hardware Acceptance Test Plan V&V
7) Hazard Analysis
8) Security Analysis
9) Risk Analysis

The Hardware Requirements Analysis process begins after the system requirements have been defined and allocated to each software and hardware element of the system. Given the system requirements and hardware concept architecture, this stage of the hardware life cycle further refines the allocated system requirements into specific requirements for the hardware element. Any constraints or limitations imposed by the hardware requirements on the system performance are identified and verified with the system acquirer that these limitations or constraints are acceptable. V&V test planning begins during the Hardware Requirements Analysis V&V activity and spans several V&V activities.

## 10.3 Hardware Design V&V process

### 10.3.1 Purpose

The purpose of the Hardware Design V&V process is to provide assurance that outcomes of the Hardware Architectural Design process, the Hardware Integration process, the Hardware Qualification Testing process, and the Hardware Acceptance Support process have been achieved.

### 10.3.2 Outcomes

As a result of the successful implementation of the Hardware Design V&V process, objective evidence is developed to assess whether:

a) Hardware design components satisfy the hardware requirements specification of the hardware element.

b) The design solution satisfies the system performance, safety, and reliability requirements.

c) No unintended or undesired consequences are introduced into the system.

### 10.3.3 Activities and tasks

The V&V effort shall perform, as specified in Table 2d for the selected integrity level, the following Hardware Design V&V activity and tasks described in Table 1d, Activity 10.3:

a) Hardware Design V&V: This activity consists of the following tasks:

1) Design Evaluation
2) Interface Analysis
3) Traceability Analysis
4) Criticality Analysis
5) Hardware Component Test Plan Assessment
6) Hardware Integration Test Plan Assessment
7) Hardware Component Test Design Assessment
8) Hardware Integration Test Design Assessment
9) Hardware Qualification Test Design V&V
10) Hardware Acceptance Test Design V&V
11) Hazard Analysis
12) Security Analysis
13) Risk Analysis

After the hardware requirements have been approved, the hardware design process is initiated. Detailed design solutions are developed that will satisfy the specific hardware requirements. Depending on the hardware, the design can take the form of selection of the materials or composites, drawings showing dimensions, circuit diagrams, and other electromechanical descriptions. Often, the hardware element involves subtiered design components from a variety of suppliers. These subtier designs are documented and evaluated as part of the entire hardware element.

## 10.4 Hardware Fabrication V&V process

### 10.4.1 Purpose

The purpose of the Hardware Fabrication V&V process is to provide assurance that outcomes of the Hardware Fabrication process, the Hardware Integration process, the Hardware Qualification Testing process, and the Hardware Acceptance Support process have been achieved.

### 10.4.2 Outcomes

As a result of the successful implementation of the Hardware Fabrication V&V process, objective evidence is developed to assess whether:

a) The final fabrication elements comply with the hardware design.

b) Each fabricated hardware component satisfies the overall system performance, safety, and reliability requirements.

### 10.4.3 Activities and tasks

The V&V effort shall perform, as specified in Table 2d for the selected integrity level, the following Hardware Fabrication V&V tasks described in Table 1d, Activity 10.4:

a) Hardware Fabrication V&V: This activity consists of the following tasks:

1) Fabricated Component Documentation Evaluation
2) Interface Analysis
3) Traceability Analysis
4) Criticality Analysis
5) Hardware Component Test Case Assessment
6) Hardware Integration Test Case Assessment
7) Hardware Qualification Test Case V&V
8) Hardware Acceptance Test Case V&V
9) Hardware Component Test Procedure Assessment
10) Hardware Integration Test Procedure Assessment
11) Hardware Qualification Test Procedure V&V
12) Hardware Component Test Execution Assessment
13) Hazard Analysis
14) Security Analysis
15) Risk Analysis

The methods used in this activity include visual analysis/inspection, quality sampling testing, physical measurements, form/fit checks, and complete component analysis/test. After the hardware design has been approved, the hardware fabrication (implementation) process is initiated. During fabrication, the hardware is built from the raw materials, electronic components are selected and integrated onto circuit boards, mechanical elements are shaped and interconnected, manufactured parts are created from molds and milling processes and other hardware fabrication methods. The Hardware Fabrication V&V determines whether or not deviations have been introduced into the solution as the hardware progressed from the hardware design to actual fabrication. For example, an electronic component selected from a catalog may be similar to the specified part but not identical. The Hardware Fabrication V&V investigates whether the small difference in the final fabrication creates any limitations or constraints that affect the overall system performance. The hardware components received from subtiered suppliers are validated by either the manufacturer or the supplier before being included in the overall hardware element fabrication.

## 10.5 Hardware Integration V&V process

### 10.5.1 Purpose

The purpose of the Hardware Integration V&V process is to provide assurance that outcomes of the Hardware Integration process have been achieved.

### 10.5.2 Outcomes

As a result of the successful implementation of the Hardware Integration V&V process, objective evidence is developed to assess whether:

a) Hardware parts conform to the hardware element requirements during the integration process.

b) The hardware element satisfies the system requirements.

### 10.5.3 Activities and tasks

The V&V effort shall perform, as specified in Table 2d for the selected integrity level, the following Hardware Integration V&V tasks described in Table 1d, Activity 10.5:

a) Hardware Integration V&V: This activity consists of the following tasks:

1) Hardware Integration Test Execution Assessment
2) Traceability Analysis
3) Hazard Analysis
4) Security Analysis
5) Risk Analysis

The Hardware Integration V&V process occurs in parallel with hardware fabrication. As fabrication progresses, hardware parts are integrated into components, components are integrated into the hardware element, and a series of tests are conducted to verify and validate conformance with requirements.

NOTE—In some programs, the Hardware Integration Test process determines the efficiency of the fabrication and integration manufacturing steps, especially when multiple hardware copies (hardware assembly line) are produced.

## 10.6 Hardware Qualification Testing V&V process

### 10.6.1 Purpose

The purpose of the Hardware Qualification Testing V&V process is to provide assurance that outcomes of the Hardware Qualification Testing process have been achieved.

### 10.6.2 Outcomes

As a result of the successful implementation of the Hardware Qualification Testing V&V process, objective evidence is developed to assess whether:

a) The hardware element as tested satisfies the hardware requirements.

b) The hardware element satisfies system requirements.

c) The hardware element does not cause unintended or undesired consequences.

### 10.6.3 Activities and tasks

The V&V effort shall perform, as specified in Table 2d for the selected integrity level, the following Hardware Qualification Testing V&V tasks described in Table 1d, Activity 10.6:

a) Hardware Qualification Testing V&V: This activity consists of the following tasks:

1) Hardware Qualification Test Execution V&V
2) Traceability Analysis
3) Hazard Analysis
4) Security Analysis
5) Risk Analysis

Hardware qualification (e.g., demonstration, analysis, inspection, or test) is performed on the complete hardware element. However, preliminary qualification tests and prototype (dry run) qualification tests can be performed on parts of the hardware element as they become available from integration testing. Hardware qualification testing occurs on the completed hardware element using other available system elements or simulators and test drivers to provide stimuli and responses from system elements that are not available.

NOTE—The hardware element used for hardware qualification testing may not be suitable for operational use.

## 10.7 Hardware Acceptance Testing V&V process

### 10.7.1 Purpose

The purpose of the Hardware Acceptance Testing V&V process is to provide assurance that outcomes of the Hardware Acceptance Support process have been achieved.

### 10.7.2 Outcomes

As a result of the successful implementation of the Hardware Acceptance Testing V&V process, objective evidence is developed to assess whether:

a) The hardware element meets the acceptance criteria and requirements.
b) The system requirements allocated to this particular hardware element are satisfied.

### 10.7.3 Activities and tasks

The V&V effort shall perform, as specified in Table 2d for the selected integrity level, the following Hardware Acceptance Testing V&V tasks described in Table 1d, Activity 10.7:

a) Hardware Acceptance Testing V&V: This activity consists of the following tasks:

1) Hardware Acceptance Test Procedure V&V
2) Hardware Acceptance Test Execution V&V
3) Traceability Analysis
4) Hazard Analysis
5) Security Analysis
6) Risk Analysis

Hardware acceptance testing occurs with the hardware element working with all other hardware and software elements. These tests provide the data for hardware acceptance, allowing the acquiring organization to formally accept the hardware product.

## 10.8 Hardware Verification process

### 10.8.1 Purpose

The purpose of the Hardware Verification process is to provide objective evidence for whether the outcomes achieve the following:

a) Conform to requirements (e.g., for correctness, completeness, consistency, and accuracy) for all activities during each life cycle process.

b) Satisfy the standards, practices, and conventions during life cycle processes.

c) Successfully complete each life cycle activity and satisfy all the criteria for initiating succeeding life cycle activities (i.e., the product is built correctly).

### 10.8.2 Outcomes

As a result of successful implementation of the Hardware Verification process:

a) A Verification and Validation Plan is developed and implemented.

b) The system of interest (hardware) and all components of the system of interest are assigned integrity levels that are reevaluated throughout the life cycle of the system.

c) The hardware and each of its components are evaluated for requirements satisfaction based on assigned integrity levels.

d) Objective evidence is developed to determine whether the hardware and each of its components conform to requirements and satisfy all the criteria for each successive life cycle activity.

### 10.8.3 Activities and tasks

Descriptions of the activities and tasks for the Hardware Verification process as applied to the Technical processes of the hardware life cycle processes are described in Clause 10.1 (Hardware Concept V&V process), Clause 10.2 (Hardware Requirements Analysis V&V process), Clause 10.3 (Hardware Design V&V process), Clause 10.4 (Hardware Fabrication V&V process), Clause 10.5 (Hardware Integration V&V process), Clause 10.6 (Hardware Qualification Testing V&V process), Clause 10.7 (Hardware Acceptance Testing V&V process), Clause 10.9 (Hardware Transition V&V process), Clause 10.11 (Hardware Operation V&V process), Clause 10.12 (Hardware Maintenance V&V process), and Clause 10.13 (Hardware Disposal V&V process).

## 10.9 Hardware Transition V&V process

### 10.9.1 Purpose

The purpose of the Hardware Transition V&V process is to provide assurance that outcomes of the Hardware Transition process have been achieved.

### 10.9.2 Outcomes

As a result of the successful implementation of the Hardware Transition V&V process, objective evidence is developed to assess whether:

a) The hardware installation in the operational environment is correct.

b) The hardware is capable of delivering its required services.

### 10.9.3 Activities and tasks

The V&V effort shall perform, as specified in Table 2d for the selected integrity level, the following Hardware Transition V&V tasks described in Table 1d, Activity 10.9:

a) Hardware Transition V&V: This activity consists of the following tasks:

1) Installation Configuration Audit
2) Installation Checkout
3) Hazard Analysis
4) Security Analysis
5) Risk Analysis

## 10.10 Hardware Validation process

### 10.10.1 Purpose

The purpose of the Hardware Validation process is to provide objective evidence for whether the outcomes achieve the following:

a) Satisfy requirements allocated to the products at the end of each life cycle activity.

b) Solve the right problem (e.g., correctly model physical laws, implement business rules, and use the proper system assumptions).

c) Satisfy intended use and user needs in the operational environment (i.e., the correct product is built).

### 10.10.2 Outcomes

As a result of successful implementation of the Hardware Validation process:

a) A Verification and Validation Plan is developed and implemented.

b) The system of interest (hardware) and all components of the system of interest are assigned integrity levels that are maintained throughout the life cycle of the system.

c) The hardware and each of its components are evaluated for satisfaction of allocated system requirements and of intended use and user needs based on assigned integrity levels.

d) Objective evidence is developed to determine whether the hardware and each of its components satisfy all system requirements allocated to hardware and meet intended use and user needs.

### 10.10.3 Activities and tasks

Descriptions of the activities and tasks for the Hardware Validation process as applied to the Technical processes of the hardware life cycle processes are described in Clause 10.1 (Hardware Concept V&V process), Clause 10.2 (Hardware Requirements Analysis V&V process), Clause 10.3 (Hardware Design V&V process), Clause 10.4 (Hardware Fabrication V&V process), Clause 10.5 (Hardware Integration V&V process), Clause 10.6 (Hardware Qualification Testing V&V process), Clause 10.7 (Hardware Acceptance Testing V&V process), Clause 10.9 (Hardware Transition V&V process), Clause 10.11 (Hardware Operation V&V process), Clause 10.12 (Hardware Maintenance V&V process), and Clause 10.13 (Hardware Disposal V&V process).

## 10.11 Hardware Operation V&V process

### 10.11.1 Purpose

The purpose of the Hardware Operation V&V process is to provide assurance that outcomes of the Hardware Operation process have been achieved.

### 10.11.2 Outcomes

As a result of the successful implementation of the Hardware Operation V&V process, objective evidence is developed to assess whether:

a) New constraints in the system are evaluated.

b) Proposed system changes and their impacts on the software are assessed.

c) Operating procedures are evaluated for correctness and usability.

### 10.11.3 Activities and tasks

The V&V effort shall perform, as specified in Table 2d for the selected integrity level, the following Hardware Operation V&V tasks described in Table 1d, Activity 10.11:

a) Hardware Operation V&V: This activity consists of the following tasks:

1) Evaluation of New Constraints

2) Operating Procedures Evaluation

3) Hazard Analysis

4) Security Analysis

5) Risk Analysis

The Hardware Operation V&V activity evaluates the impact of changes in the operating environment, assesses the effect on the system of any proposed changes, evaluates operating procedures for adherence with the intended use, and analyzes the risks affecting the user and the system.

## 10.12 Hardware Maintenance V&V process

### 10.12.1 Purpose

The purpose of the Hardware Maintenance V&V process is to provide assurance that outcomes of the Hardware Maintenance process have been achieved.

### 10.12.2 Outcomes

As a result of the successful implementation of the Hardware Maintenance V&V process, objective evidence is developed to assess whether:

a) Proposed hardware changes and their impact on the system are assessed.

b) Anomalies that are discovered during operation are evaluated.

c) Migration requirements are assessed.

d) Retirement requirements are assessed.

e) V&V tasks are re-performed.

### 10.12.3 Activities and tasks

The V&V effort shall perform, as specified in Table 2d for the selected integrity level, the following Hardware Maintenance V&V tasks described in Table 1d, Activity 10.12:

a) Hardware Maintenance V&V: This activity consists of the following tasks:

1) VVP Revision
2) Anomaly Evaluation
3) Criticality Analysis
4) Migration Assessment
5) Retirement Assessment
6) Hazard Analysis
7) Security Analysis
8) Risk Analysis
9) Task Iteration

Proposed changes are assessed by the Proposed/Baseline Change Assessment task of the Management of V&V activity.

The Hardware Maintenance process is activated when the hardware or associated documentation are changed in response to a need for system maintenance. The Hardware Maintenance V&V activity addresses the following:

— Hardware modifications (i.e., corrective, adaptive, or perfective changes).
— Hardware migration (i.e., the movement of hardware to a new operational environment).
— Hardware retirement (i.e., the withdrawal of active support by the operation and maintenance organization, partial or total replacement by a new system, or installation of an upgraded system).

System modifications may be derived from the requirements specified to correct hardware errors (e.g., corrective), to adapt to a changed operating environment (e.g., adaptive), or to respond to additional user requests or enhancements (e.g., perfective). Modifications of the hardware shall be treated as development processes and shall be verified and validated by performing V&V tasks corresponding to the modifications. Integrity level assignments shall be assessed as described in Clause 5. The integrity level assignments shall be revised as appropriate to reflect the requirements derived from the maintenance process.

If the hardware V&V was performed in accordance with this standard, then the maintenance process shall continue to conform to this standard. If the hardware was not verified and validated using this standard and appropriate documentation is not available or adequate, then the Hardware Maintenance V&V effort shall determine whether the missing or incomplete documentation should be generated. In making this determination of whether to generate missing documentation, the minimum V&V requirements of the assigned integrity level shall be taken into consideration.

## 10.13 Hardware Disposal V&V process

### 10.13.1 Purpose

The purpose of the Hardware Disposal V&V process is to provide assurance that outcomes of the Hardware Disposal process have been achieved.

### 10.13.2 Outcomes

As a result of the successful implementation of the Hardware Disposal V&V process, objective evidence is developed to assess whether:

a) The constraints in the hardware disposal strategy are included in hardware requirements.

b) Disposal leaves the system in an agreed-on state.

### 10.13.3 Activities and tasks

The V&V effort shall perform, as specified in Table 2d for the selected integrity level, the following Hardware Disposal V&V task described in Table 1d, Activity 10.13:

a) Hardware Disposal V&V: This activity consists of the following task:

1) Hardware Disposal Evaluation

This process ends active support by the operation and maintenance organization, or deactivates, disassembles, and removes the affected hardware products, consigning them to a final condition and leaving the environment in an acceptable condition. This process destroys or stores system hardware elements and related products in a sound manner, in accordance with legislation, agreements, organizational constraints, and stakeholder requirements. Where required, it maintains records that may be monitored.

## Table 1d—V&V tasks, inputs, and outputs

| 10.1 Activity: Hardware Concept V&V (Hardware, Hardware Requirements Analysis process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(1) Concept Documentation Evaluation**<br>a) Validate that the concept documentation satisfies user needs and is consistent with acquisition needs.<br>b) Validate constraints of interfacing systems and constraints or limitations of proposed approach.<br>c) Analyze system requirements related to hardware and validate that the following satisfy user needs:<br>1) System functions.<br>2) End-to-end system performance (e.g., timing response of relay dropout, throughput of network switches, developed torque, power consumption, weight, structural integrity, and reliability independence).<br>3) Feasibility and testability of the functional requirements.<br>4) System architecture design.<br>5) Operation and maintenance requirements (e.g., parts design life) and environments.<br>6) Migration requirements from an existing system where applicable.<br>7) Hardware technologies (existing, emerging, new, and new applications). | Concept documentation<br>System requirements<br>System architecture<br>Supplier development plans and schedules<br>User needs<br>Acquisition needs | Task report(s)—Concept documentation evaluation<br>Anomaly report(s) |
| **(2) Requirements Allocation Analysis**<br>Verify the correctness, accuracy, and completeness of the system requirements allocation to hardware, software, and user interfaces against user needs.<br>a) Correctness<br>Verify that performance requirements (e.g., timing, response time, and throughput) allocated to hardware, software, and user interfaces satisfy user needs.<br>b) Accuracy<br>Verify that the internal and external interfaces specify the hardware interface capabilities, interface form-factor, and other performance requirements to demonstrate satisfaction of user requirements.<br>c) Completeness<br>1) Verify that application-specific requirements such as functional diversity, fault detection, fault isolation, and diagnostic and error recovery satisfy user needs.<br>2) Verify that the user's maintenance requirements for the system are completely specified.<br>3) Verify that the migration from existing system and replacement of the system satisfy user needs. | User needs<br>Concept documentation<br>System requirements<br>System architecture | Task report(s)—Requirements allocation analysis<br>Anomaly report(s) |
| **(3) Traceability Analysis**<br>a) Identify all system requirements related to hardware. (This is the start of hardware requirements traceability.)<br>b) Verify that these system requirements related to hardware are traceable to acquisition needs. | Concept documentation<br>System requirements<br>Acquisition needs | Task report(s)—Traceability analysis<br>Anomaly report(s) |
| **(4) Criticality Analysis**<br>a) Verify that the assigned integrity levels are correct. If integrity levels are not assigned, then assign integrity levels to the system requirements related to hardware, detailed functions, hardware components, subsystem, or other partitions. | Concept documentation (System requirements) | Task report(s)—Criticality analysis<br>Anomaly report(s) |

| 10.1 Activity: Hardware Concept V&V (Hardware, Hardware Requirements Analysis process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| b) Document the integrity level assigned to individual components (e.g., requirements, detailed functions, hardware components, subsystems, or other partitions). For V&V planning purposes, the hardware component shall be assigned the same integrity level as the highest level assigned to any individual element.<br>c) Verify whether any component can influence individual components assigned a higher integrity level, and if such conditions exist, then assign that component the same higher integrity level. | Developer integrity level assignments | |
| **(5) Hazard Analysis**<br>Analyze the potential hazards to and from the conceptual system. The analysis shall perform the following:<br>a) Identify the potential system hazards (e.g., environmental conditions such as pressure, radiation, temperature, and humidity, electrostatic sensitivity, EMI/RFI, seismic, electro-mechanical properties, aging).<br>b) Assess the consequences of each hazard.<br>c) Assess the probability of each hazard.<br>d) Identify mitigation strategies for each hazard. | Concept documentation | Task report(s)—Hazard analysis<br>Anomaly report(s) |
| **(6) Security Analysis**<br>a) Review the system owner's definition of an acceptable level of security risk.<br>b) Analyze the system concept from a security perspective and assure that potential security risks with respect to confidentiality (disclosure of sensitive information/data), integrity (modification of information/data), availability (withholding of information or services), and accountability (attributing actions to an individual/process) have been identified. Include an assessment of the sensitivity of the information/data to be processed. Security attributes include access control, electrical/optical isolation, location tracking, and network medium control.<br>c) Analyze security risks introduced by the system itself as well as those associated with the environment with which the system interfaces. | Concept documentation<br>System architecture<br>Preliminary TRA | Task report(s)—Security analysis<br>Anomaly report(s) |
| **(7) Risk Analysis**<br>a) Identify hardware technical and management risks.<br>b) Provide recommendations to eliminate, reduce, or mitigate the risks. | Concept documentation<br>Supplier development plans and schedules<br>Hazard analysis report<br>Security analysis report<br>V&V task results | Task report(s)—Risk analysis<br>Anomaly report(s) |

| 10.2 Activity: Hardware Requirements Analysis V&V (Hardware, Hardware Requirements Analysis process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(1) Requirements Evaluation**<br>Evaluate the requirements (e.g., functional, capability, interface, qualification, safety, security, human factors, data definitions, user documentation, installation and acceptance, user operation, and user maintenance) of the hardware requirements specification (HRS) and | Concept documentation<br>HRS<br>IRS | Task report(s)—Hardware requirements evaluation |

| 10.2 Activity: Hardware Requirements Analysis V&V (Hardware, Hardware Requirements Analysis process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| IRS for correctness, consistency, completeness, accuracy, readability, and testability. | | Anomaly report(s) |
| **(2) Interface Analysis**<br>Verify and validate that the requirements for hardware interfaces with software, user, operator, other hardware, and other systems are correct, consistent, complete, accurate, and testable. | Concept documentation<br>HRS<br>IRS | Task report(s)—Interface analysis<br>Anomaly report(s) |
| **(3) Traceability Analysis**<br>a) Trace the hardware requirements (HRS and IRS) to system requirements (Concept Documentation) and system requirements to the hardware requirements.<br>b) Analyze identified relationships for correctness, consistency, completeness, and accuracy. | Concept documentation<br>System requirements<br>HRS<br>IRS | Task report(s)—Traceability analysis<br>Anomaly report(s) |
| **(4) Criticality Analysis**<br>Review and update the existing criticality analysis results from the prior Criticality Task Report using the HRS and IRS. | Criticality task report<br>HRS<br>IRS | Task report(s)—Criticality analysis<br>Anomaly report(s) |
| **(5) Hardware Qualification Test Plan V&V**<br>a) Integrity levels 4 and 3<br>1) Plan V&V hardware qualification testing to validate hardware requirements (e.g., static, transient, or dynamic loads; interface compatibility; electromagnetic compatibility; electromagnetic interference; thermal, mechanical, electrical, acoustic, environmental [humidity, water, saltwater, etc.], acceleration, vibration, shock, and pressure).<br>2) Plan tracing of system requirements to test designs, cases, procedures, and results.<br>3) Plan documentation of test designs, cases, procedures, and results.<br>4) The V&V hardware qualification test plan shall address the following:<br>i) Conformance to all system requirements (e.g., functional, performance, security, operation, and maintenance) as complete hardware end items in the system environment.<br>ii) Adequacy of user documentation (e.g., training materials and procedural changes).<br>iii) Performance at boundaries (e.g., data and interfaces) and under stress conditions.<br>5) Verify that the V&V hardware qualification test plan satisfies the following criteria:<br>i) Conformance to project-defined test document purpose, format, and content.<br>ii) Test coverage of system requirements.<br>6) Validate that the V&V hardware qualification test plan satisfies the following criteria:<br>i) Appropriateness of test methods and standards used.<br>ii) Conformance to expected results.<br>iii) Feasibility of system qualification testing.<br>iv) Feasibility and testability of operation and maintenance requirements. | Concept documentation<br>System requirements<br>HRS<br>IRS<br>User documentation<br>Developer's hardware qualification test plan | V&V hardware qualification test plan (integrity levels 4 and 3)<br>Task report(s)—Review of hardware qualification test plan (integrity level 2)<br>Anomaly report(s) |

| 10.2 Activity: Hardware Requirements Analysis V&V (Hardware, Hardware Requirements Analysis process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| b) Integrity level 2<br>1) Verify that the developer's hardware qualification test plan satisfies the following criteria:<br>i) Conformance to project-defined test document purpose, format, and content.<br>ii) Test coverage of system requirements.<br>2) Validate that the developer's hardware qualification test plan satisfies the following criteria:<br>i) Appropriateness of test methods and standards used.<br>ii) Conformance to expected results.<br>iii) Feasibility of system qualification testing.<br>iv) Capability to be operated and maintained.<br>c) Integrity level 1<br>There are no hardware qualification V&V test requirements. | | |
| **(6) Hardware Acceptance Test Plan V&V**<br>a) Integrity levels 4 and 3<br>1) Plan V&V hardware acceptance testing to validate that the hardware correctly implements system and hardware requirements (e.g., static, transient, or dynamic loads; interface compatibility; electromagnetic compatibility; electromagnetic interference; thermal; mechanical; electrical; acoustic; environmental (humidity, water, saltwater, etc.); acceleration; vibration; and shock, pressure) in an operational environment.<br>2) Plan tracing of acceptance test requirements to test design, cases, procedures, and execution results.<br>3) Plan documentation of test tasks and results.<br>4) The V&V hardware acceptance test plan shall address the following:<br>i) Conformance to acceptance requirements in the operational environment.<br>ii) Adequacy of user documentation.<br>5) Verify that the V&V hardware acceptance test plan satisfies the following criteria:<br>i) Conformance to project-defined test document purpose, format, and content.<br>ii) Test coverage of acceptance requirements.<br>6) Validate that the V&V hardware acceptance test plan satisfies the following criteria:<br>i) Conformance to expected results.<br>ii) Feasibility of operation and maintenance (e.g., capability to be operated and maintained in accordance with user needs).<br>b) Integrity level 2<br>1) Verify that the acquirer's hardware acceptance test plan conforms to project-defined test document purpose, format, and content.<br>2) Validate that the acquirer's hardware acceptance test plan satisfies the following criteria:<br>i) Test coverage of acceptance requirements.<br>ii) Conformance to expected results. | Concept documentation<br>HRS<br>IRS<br>User documentation<br>Hardware acceptance test plan | V&V hardware acceptance test plan (integrity levels 4 and 3)<br>Task report(s)—Review of hardware acceptance test plan (integrity level 2)<br>Anomaly report(s) |

| 10.2 Activity: Hardware Requirements Analysis V&V (Hardware, Hardware Requirements Analysis process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| iii) Feasibility of operation and maintenance (e.g., capability to be operated and maintained in accordance with user needs).<br>c) Integrity level 1<br>There are no hardware acceptance V&V test requirements. | | |
| **(7) Hazard Analysis**<br>Determine hardware contributions to system hazards. The hazard analysis shall perform the following:<br>a) Identify the hardware requirements that contribute to each system hazard.<br>b) Validate that the hardware addresses, controls, or mitigates each hazard. | HRS<br>IRS<br>Hazard analysis report | Task report(s)—Hazard analysis<br>Anomaly report(s) |
| **(8) Security Analysis**<br>a) Determine that the security requirements identified in the HRS and IRS address the security risks introduced by the system concept.<br>b) Verify that the system security requirements will mitigate the identified security risks to an acceptable level. | HRS<br>IRS<br>Preliminary TRA<br>Security analysis report | Task report(s)—Security analysis<br>Anomaly report(s) |
| **(9) Risk Analysis**<br>a) Review and update risk analysis using prior task reports.<br>b) Provide recommendations to eliminate, reduce, or mitigate the risks. | Concept documentation<br>HRS<br>IRS<br>Supplier development plans and schedules<br>Hazard analysis report<br>Security analysis report<br>Risk analysis report<br>V&V task results | Task report(s)—Risk analysis<br>Anomaly report(s) |

| 10.3 Activity: Hardware Design V&V (Hardware, Hardware Architecture Design process, Hardware Detailed Design process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(1) Design Evaluation**<br>Evaluate the design elements (hardware design description [HDD] and IDD) for correctness, consistency, completeness, accuracy, readability, testability, and design margins. Verify and validate the allocation of hardware requirements to the hardware design elements. | HRS<br>IRS<br>HDD<br>IDD<br>Hardware drawings<br>Design standards (e.g., standards, practices, and conventions) | Task report(s)—Hardware design evaluation<br>Anomaly report(s) |
| **(2) Interface Analysis**<br>Verify and validate the hardware design interfaces with software, user, operator, and conditioning and enabling hardware/systems (e.g., RC filter network, gear reduction, communication protocol), for correctness, consistency, completeness, accuracy, and testability. | Concept documentation (System requirements)<br>HRS<br>IRS | Task report(s)—Interface analysis<br>Anomaly report(s) |

| 10.3 Activity: Hardware Design V&V (Hardware, Hardware Architecture Design process, Hardware Detailed Design process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| | HDD<br>IDD<br>Hardware drawings | |
| **(3) Traceability Analysis**<br>Trace the design elements (HDD and IDD) to the requirements (HRS and IRS), and the requirements to the design elements. Analyze the relationships for correctness, consistency, and completeness. | HRS<br>HDD<br>IRS<br>IDD | Task report(s)—Traceability analysis<br>Anomaly report(s) |
| **(4) Criticality Analysis**<br>Review and update the existing criticality analysis results from the prior Criticality Task Report using the HDD and IDD. | Criticality task report<br>HDD<br>IDD | Task report(s)—Criticality analysis<br>Anomaly report(s) |
| **(5) Hardware Component Test Plan Assessment**<br>a) Integrity levels 4, 3, and 2<br>1) Verify that the developer's hardware component test plan conforms to project-defined test document purpose, format, and content.<br>2) Validate that the developer's hardware component test plan satisfies the following criteria:<br>i) Traceable to the hardware requirements and design.<br>ii) External consistency with the hardware requirements and design.<br>iii) Internal consistency between unit requirements.<br>iv) Test coverage of units.<br>v) Feasibility of hardware integration and testing.<br>vi) Feasibility of operation and maintenance (e.g., capability to be operated and maintained in accordance with user needs).<br>b) Integrity level 1<br>There are no hardware component V&V test requirements. | HRS<br>HDD<br>IRS<br>IDD<br>Hardware drawings<br>Hardware component test plan | Task report(s)—Review of hardware component test plan assessment (integrity levels 4, 3, and 2)<br>Anomaly report(s) |
| **(6) Hardware Integration Test Plan Assessment**<br>a) Integrity levels 4, 3, and 2<br>1) Verify that the developer's hardware integration test plan conforms to project-defined test document purpose, format, and content.<br>2) Validate that the developer's hardware integration test plan satisfies the following criteria:<br>i) Traceable to the system requirements.<br>ii) External consistency with the system requirements.<br>iii) Internal consistency.<br>iv) Test coverage of the hardware requirements.<br>v) Appropriateness of test standards and methods.<br>vi) Conformance to expected results.<br>vii) Feasibility of hardware qualification testing.<br>viii) Feasibility of operation and maintenance (e.g., capability to be operated and maintained in accordance with user needs).<br>b) Integrity level 1<br>There are no hardware integration V&V test requirements. | HRS<br>IRS<br>HDD<br>IDD<br>Hardware drawings<br>Hardware integration test plan | Task report(s)—Review of hardware integration test plan assessment (integrity levels 4, 3, and 2)<br>Anomaly report(s) |

| 10.3 Activity: Hardware Design V&V (Hardware, Hardware Architecture Design process, Hardware Detailed Design process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(7) Hardware Component Test Design Assessment**<br>a) Integrity levels 4, 3, and 2<br>1) Verify that the developer's test designs for hardware component testing conform to project-defined test document purpose, format, and content.<br>2) Validate that the developer's hardware component test designs satisfy the criteria in V&V activity 10.3, Task 5.<br>b) Integrity level 1<br>There are no hardware component V&V test requirements. | HDD<br>IDD<br>Hardware drawings<br>User documentation<br>Hardware test plans<br>Hardware test designs | Task report(s)—Review of hardware component test design assessment (integrity levels 4, 3, and 2)<br>Anomaly report(s) |
| **(8) Hardware Integration Test Design Assessment**<br>a) Integrity levels 4, 3, and 2<br>1) Verify that the developer's test designs for hardware integration testing conform to project-defined test document purpose, format, and content.<br>2) Validate that the developer's hardware integration test designs satisfy the criteria in V&V activity 10.3, Task 6.<br>b) Integrity level 1<br>There are no hardware integration V&V test requirements. | HDD<br>IDD<br>Hardware drawings<br>User documentation<br>Hardware test designs | Task report(s)—Review of hardware integration test design assessment (integrity levels 4, 3, and 2)<br>Anomaly report(s) |
| **(9) Hardware Qualification Test Design V&V**<br>a) Integrity levels 4 and 3<br>1) Design tests for qualification testing.<br>2) Continue tracing required by the V&V qualification test plan. Verify that the V&V qualification test designs conform to project-defined test document purpose, format, and content.<br>3) Validate that the V&V qualification test designs satisfy the criteria in V&V activity 10.2, Task 5.<br>b) Integrity level 2<br>1) Verify that the developer's test designs for hardware qualification testing conform to project-defined test document purpose, format, and content.<br>2) Validate that the developer's hardware qualification test designs satisfy the criteria in V&V activity 10.2, Task 5.<br>c) Integrity level 1<br>There are no hardware V&V qualification test requirements. | HDD<br>IDD<br>Hardware drawings<br>User documentation<br>Hardware test designs | V&V hardware qualification test design(s) (integrity levels 4 and 3)<br>Task report(s)—Review of hardware qualification test designs (integrity level 2)<br>Anomaly report(s) |
| **(10) Hardware Acceptance Test Design V&V**<br>a) Integrity levels 4 and 3<br>1) Design tests for V&V hardware acceptance testing.<br>2) Continue tracing required by the V&V hardware acceptance test plan. Verify that the V&V hardware acceptance test designs conform to project-defined test document purpose, format, and content<br>3) Validate that the V&V hardware acceptance test designs satisfy the criteria in V&V activity 10.2, Task 6.<br>b) Integrity level 2<br>1) Verify that the acquirer's hardware test designs for acceptance testing conform to project-defined test document purpose, format, and content.<br>2) Validate that the acquirer's hardware acceptance test designs satisfy the criteria in V&V activity 10.2, Task 6.<br>c) Integrity level 1<br>There are no hardware acceptance V&V test requirements. | HDD<br>IDD<br>Hardware drawings<br>User documentation<br>Hardware test designs | V&V hardware acceptance test design(s) (integrity levels 4 and 3)<br>Task report(s)—Review of hardware acceptance test design(s) (integrity level 2)<br>Anomaly report(s) |

| 10.3 Activity: Hardware Design V&V (Hardware, Hardware Architecture Design process, Hardware Detailed Design process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(11) Hazard Analysis**<br>a) Verify the design elements that implement critical requirements introduce no new hazards.<br>b) Assess the identified mitigation strategies to verify each hazard is prevented, mitigated, or controlled (any unmitigated hazards are documented and addressed as part of system and hardware operations).<br>c) Update the hazard analysis. | HDD<br>IDD<br>Hardware drawings<br>Hazard analysis report | Task report(s)—Hazard analysis<br>Anomaly report(s) |
| **(12) Security Analysis**<br>a) Verify that the design element complies with the security features of the architectural design and that the design element does not introduce new security risks.<br>b) Verify the identified security threats and vulnerabilities are prevented, controlled, or mitigated (any unmitigated threats and vulnerabilities are documented and addressed as part of system and hardware operations). | System architecture<br>Subsystems security analysis<br>Hardware drawings<br>Security analysis report<br>V&V task results | Task report(s)—Security analysis<br>Anomaly report(s) |
| **(13) Risk Analysis**<br>a) Review and update risk analysis using prior task reports.<br>b) Provide recommendations to eliminate, reduce, or mitigate the risks. | HDD<br>IDD<br>Hardware drawings<br>Supplier development plans and schedules<br>Hazard analysis report<br>Security analysis report<br>Risk analysis report<br>V&V task results | Task report(s)—Risk analysis<br>Anomaly report(s) |

| 10.4 Activity: Hardware Fabrication V&V (Hardware, Hardware Fabrication process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(1) Fabricated Component Documentation Evaluation**<br>Evaluate the fabricated component documentation for correctness, consistency, completeness, accuracy, and readability. | Component documentation<br>HDD<br>IDD<br>Hardware drawings (e.g., shop drawings, bill of materials)<br>User Documentation | Task report(s)—Component documentation evaluation<br>Anomaly report(s) |
| **(2) Interface Analysis**<br>Verify and validate the fabricated component interfaces with software, user, operator, other hardware, and other systems for correctness, consistency, completeness, accuracy, and testability. | Concept Documentation<br>System requirements<br>HDD<br>IDD<br>Hardware drawings (e.g., shop drawings, bill of materials)<br>User documentation | Task report(s)—Interface analysis<br>Anomaly report(s) |

| 10.4 Activity: Hardware Fabrication V&V (Hardware, Hardware Fabrication process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(3) Traceability Analysis**<br>a) Trace the fabricated component(s) to the design, and the design to the fabricated component(s).<br>b) Analyze identified relationships for correctness, consistency, and completeness. | HDD<br>IDD<br>Hardware drawings (e.g., shop drawings, bill of materials)<br>Component documentation | Task report(s)—Traceability analysis<br>Anomaly report(s) |
| **(4) Criticality Analysis**<br>Review and update the existing criticality analysis results from the prior Criticality Task Report using the fabricated component and its associated documentation. | Criticality Task Report<br>Component documentation | Task report(s)—Criticality analysis<br>Anomaly report(s) |
| **(5) Hardware Component Test Case Assessment**<br>a) Integrity levels 4, 3, and 2<br>1) Verify that the developer's hardware component test cases conform to project-defined test document purpose, format, and content.<br>2) Validate that the developer's hardware component test cases satisfy the criteria in V&V activity 10.3, Task 5.<br>b) Integrity level 1<br>There are no hardware component V&V test requirements. | HRS<br>IRS<br>HDD<br>IDD<br>Hardware drawings (e.g., shop drawings, bill of materials)<br>User documentation<br>Hardware component test cases | Task report(s)—Review of hardware component test cases (integrity levels 4, 3, and 2)<br>Anomaly report(s) |
| **(6) Hardware Integration Test Case Assessment**<br>a) Integrity levels 4, 3, and 2<br>1) Verify that the developer's hardware integration test cases conform to project-defined test document purpose, format, and content.<br>2) Validate that the developer's hardware integration test cases satisfy the criteria in V&V activity 10.3, Task 6.<br>b) Integrity level 1<br>There are no hardware integration V&V test requirements. | HRS<br>IRS<br>HDD<br>IDD<br>Hardware drawings (e.g., shop drawings, bill of materials)<br>User documentation<br>Hardware integration test cases | Task report(s)—Review of hardware integration test cases (integrity levels 4, 3, and 2)<br>Anomaly report(s) |
| **(7) Hardware Qualification Test Case V&V**<br>a) Integrity levels 4 and 3<br>1) Develop test cases for V&V hardware qualification testing.<br>2) Continue tracing required by the V&V hardware qualification test plan.<br>3) Verify that the V&V hardware qualification test cases conform to project-defined test document purpose, format, and content.<br>4) Validate that the V&V hardware qualification test cases satisfy the criteria in V&V activity 10.2, Task 5.<br>b) Integrity level 2<br>1) Verify that the developer's hardware qualification test cases conform to project-defined test document purpose, format, and content.<br>2) Validate that the developer's hardware qualification test cases satisfy the criteria in V&V activity 10.2, Task 5.<br>c) Integrity level 1<br>There are no hardware V&V qualification test requirements. | HRS<br>IRS<br>HDD<br>IDD<br>Hardware drawings (e.g., shop drawings, bill of materials)<br>User documentation<br>Hardware qualification test cases | V&V hardware qualification test cases (integrity levels 4 and 3)<br>Task report(s)—Review of hardware qualification test cases (integrity level 2)<br>Anomaly report(s) |

| 10.4 Activity: Hardware Fabrication V&V (Hardware, Hardware Fabrication process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(8) Hardware Acceptance Test Case V&V**<br>a) Integrity levels 4 and 3<br>1) Develop test cases for V&V hardware acceptance testing.<br>2) Continue tracing required by the V&V hardware acceptance test plan.<br>3) Verify that the V&V hardware Acceptance test cases conform to project-defined test document purpose, format, and content.<br>4) Validate that the V&V hardware acceptance test cases satisfy the criteria in V&V activity 10.2, Task 6.<br>b) Integrity level 2<br>1) Verify that the acquirer's hardware acceptance test cases conform to project-defined test document purpose, format, and content.<br>2) Validate that the acquirer's hardware acceptance test cases satisfy the criteria in V&V activity 10.2, Task 6.<br>c) Integrity level 1<br>There are no hardware acceptance V&V test requirements. | HRS<br>IRS<br>HDD<br>IDD<br>Hardware drawings (e.g., shop drawings, bill of materials)<br>User documentation<br>Hardware acceptance test cases | V&V hardware acceptance test cases (integrity levels 4 and 3)<br>Task report(s)—Review of hardware acceptance test cases (integrity level 2)<br>Anomaly report(s) |
| **(9) Hardware Component Test Procedure Assessment**<br>a) Integrity levels 4, 3, and 2<br>1) Verify that the developer's hardware component test procedures conform to project-defined test document purpose, format, and content.<br>2) Validate that the developer's hardware component test procedures satisfy the criteria in V&V activity 10.3, Task 5.<br>b) Integrity level 1<br>There are no hardware component V&V test requirements. | HRS<br>IRS<br>HDD<br>IDD<br>Hardware drawings (e.g., shop drawings, bill of materials)<br>User documentation<br>Hardware component test cases<br>Hardware component test procedures | Task report(s)—Review of hardware component test procedures (integrity levels 4 3 and 2)<br>Anomaly report(s) |
| **(10) Hardware Integration Test Procedure Assessment**<br>a) Integrity levels 4, 3, and 2<br>1) Verify that the developer's hardware integration test procedures conform to project-defined test document purpose, format, and content.<br>2) Validate that the developer's hardware integration test procedures satisfy the criteria in V&V activity 10.3, Task 6.<br>b) Integrity level 1<br>There are no hardware integration V&V test requirements. | HRS<br>IRS<br>HDD<br>IDD<br>Hardware drawings (e.g., shop drawings, bill of materials)<br>User documentation<br>Hardware integration test cases<br>Hardware integration test procedures | Task report(s)—Review of hardware integration test procedures (integrity levels 4, 3, and 2)<br>Anomaly report(s) |
| **(11) Hardware Qualification Test Procedure V&V**<br>a) Integrity levels 4 and 3<br>1) Develop test procedures for V&V hardware qualification testing.<br>2) Continue tracing required by the V&V hardware qualification test plan. | HRS<br>IRS<br>HDD<br>IDD<br>Hardware drawings (e.g., shop drawings, | V&V hardware qualification test procedures (integrity levels 4 and 3)<br>Task report(s)—Review of hardware qualification test |

| 10.4 Activity: Hardware Fabrication V&V (Hardware, Hardware Fabrication process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| 3) Verify that the V&V hardware qualification test procedures conform to project-defined test document purpose, format, and content.<br>4) Validate that the V&V hardware qualification test procedures satisfy the criteria in V&V activity 10.2, Task 5.<br>b) Integrity level 2<br>1) Verify that the developer's hardware qualification test procedures conform to project-defined test document purpose, format, and content.<br>2) Validate that the developer's hardware qualification test procedures satisfy the criteria in V&V activity 10.2, Task 5.<br>c) Integrity level 1<br>There are no hardware V&V qualification test requirements. | bill of materials)<br>User documentation<br>Hardware qualification test cases<br>Hardware qualification test procedures | procedures (integrity level 2)<br>Anomaly report(s) |
| **(12) Hardware Component Test Execution Assessment**<br>a) Integrity levels 4, 3, and 2<br>Use the developer's hardware component test results to validate that the hardware component satisfies the test acceptance criteria.<br>b) Integrity level 1<br>There are no hardware component V&V test requirements. | Component documentation<br>HDD<br>IDD<br>Hardware drawings (e.g., shop drawings, bill of materials)<br>Component test plans<br>Hardware component test procedures<br>Hardware component test results | Task report(s)—Review of hardware component test execution results (integrity levels 4, 3, and 2)<br>Anomaly report(s) |
| **(13) Hazard Analysis**<br>a) Verify that the fabricated component correctly implements the critical requirements and introduces no new hazards.<br>b) Assess the identified mitigation strategies to verify each hazard is prevented, mitigated, or controlled (any unmitigated hazards are documented and addressed as part of system and hardware operations).<br>c) Update the hazard analysis. | Component documentation<br>HDD<br>IDD<br>Hardware drawings (e.g., shop drawings, bill of materials)<br>Hazard analysis report | Task report(s)—Hazard analysis<br>Anomaly report(s) |
| **(14) Security Analysis**<br>a) Verify that the fabricated component is completed in accordance with the security features of the system design and that the fabricated component does not introduce new security risks.<br>b) Verify the identified security threats and vulnerabilities are prevented, controlled, or mitigated (any unmitigated threats and vulnerabilities are documented and addressed as part of system and hardware operations). | Component documentation<br>HDD<br>IDD<br>Hardware drawings (e.g., shop drawings, bill of materials)<br>Security analysis report | Task report(s)—Security analysis<br>Anomaly report(s) |
| **(15) Risk Analysis**<br>Review and update risk analysis using prior task reports. Provide recommendations to eliminate, reduce, or mitigate the risks. | Component documentation<br>Hardware drawings (e.g., shop drawings, | Task report(s)—Risk analysis<br>Anomaly report(s) |

| 10.4 Activity: Hardware Fabrication V&V (Hardware, Hardware Fabrication process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| | bill of materials)<br>Supplier development plans and schedules<br>Hazard analysis report<br>Security analysis report<br>Risk analysis report<br>V&V task results | |

| 10.5 Activity: Hardware Integration V&V (Hardware, Hardware Integration process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(1) Hardware Integration Test Execution Assessment**<br>a) Integrity levels 4, 3, and 2<br>Use the developer's hardware integration test results to verify that the hardware satisfies the test acceptance criteria.<br>b) Integrity level 1<br>There are no hardware acceptance V&V test requirements. | Hardware component specifications<br>Hardware integration test plan<br>Hardware integration test procedures<br>Hardware integration test results | Task report(s)—Review of hardware integration test execution results (integrity levels 4, 3, and 2)<br>Anomaly report(s) |
| **(2) Traceability Analysis**<br>Analyze relationships in the V&V Test Plans, Designs, Cases, and Procedures for correctness and completeness. The task criteria are as follows:<br>a) Correctness<br>Verify that there is a valid relationship between the V&V test plans, designs, cases, and procedures.<br>b) Completeness<br>Verify that all V&V test procedures are traceable to the V&V test plans. | V&V test plans<br>V&V test designs<br>V&V test procedures | Task report(s)—Traceability analysis<br>Anomaly report(s) |
| **(3) Hazard Analysis**<br>a) Verify that the test instrumentation does not introduce new hazards.<br>b) Assess the identified mitigation strategies to verify each hazard is prevented, mitigated, or controlled (any unmitigated hazards are documented and addressed as part of system and hardware operations).<br>c) Update the hazard analysis. | Hardware component specifications<br>Test results<br>Hazard analysis report | Task report(s)—Hazard analysis<br>Anomaly report(s) |
| **(4) Security Analysis**<br>a) Verify that the implemented system does not increase the security risk.<br>b) Verify the identified security threats and vulnerabilities are prevented, controlled, or mitigated (any unmitigated threats and vulnerabilities are documented and addressed as part of system and hardware operations). | Hardware component specifications<br>Security analysis report | Task report(s)—Security analysis<br>Anomaly report(s) |

| 10.5 Activity: Hardware Integration V&V (Hardware, Hardware Integration process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(5) Risk Analysis**<br>a) Review and update risk analysis using prior task reports.<br>b) Provide recommendations to eliminate, reduce, or mitigate the risks. | Supplier development plans and schedules<br>Hazard analysis report<br>Security analysis report<br>Risk analysis report<br>V&V task results | Task report(s)—Risk analysis<br>Anomaly report(s) |

| 10.6 Activity: Hardware Qualification Testing V&V (Hardware, Hardware Qualification Testing process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(1) Hardware Qualification Test Execution V&V**<br>a) Integrity levels 4 and 3<br>1) Perform V&V hardware qualification testing.<br>2) Analyze test results to validate that the hardware satisfies the system requirements.<br>3) Validate that the test results trace to test criteria established by the test traceability in the test planning documents.<br>4) Document the results as required by the V&V hardware qualification test plan.<br>5) Use the V&V hardware qualification test results to validate that the hardware satisfies the test acceptance criteria.<br>6) Document discrepancies between the actual and expected test results.<br>b) Integrity levels 1 and 2<br>Use the developer's hardware qualification test results to verify that the hardware satisfies the test acceptance criteria. | Hardware component specifications<br>Hardware qualification test plan<br>Hardware qualification test procedures<br>Hardware qualification test results | V&V hardware qualification test execution results (integrity levels 4 and 3)<br>Task report(s)—Review of hardware qualification test execution results (integrity level 2)<br>Anomaly report(s) |
| **(2) Traceability Analysis**<br>Analyze relationships in the V&V Test Plans, Designs, Cases, and Procedures for correctness and completeness. The task criteria are as follows:<br>a) Correctness<br>Verify that there is a valid relationship between the V&V test plans, designs, cases, and procedures.<br>b) Completeness<br>Verify that all V&V test procedures are traceable to the V&V test plans. | V&V test plans<br>V&V test designs<br>V&V test procedures | Task report(s)—Traceability analysis<br>Anomaly report(s) |
| **(3) Hazard Analysis**<br>a) Verify that the test instrumentation does not introduce new hazards.<br>b) Assess the identified mitigation strategies to verify each hazard is prevented, mitigated, or controlled (any unmitigated hazards are documented and addressed as part of system and hardware operations).<br>c) Update the hazard analysis. | Hardware component specifications<br>Test results<br>Hazard analysis report | Task report(s)—Hazard analysis<br>Anomaly report(s) |
| **(4) Security Analysis**<br>a) Verify that the implemented system does not increase the security risk. | Hardware component specifications | Task report(s)—Security analysis<br>Anomaly report(s) |

| 10.6 Activity: Hardware Qualification Testing V&V (Hardware, Hardware Qualification Testing process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| b) Verify the identified security threats and vulnerabilities are prevented, controlled, or mitigated (any unmitigated threats and vulnerabilities are documented and addressed as part of system and hardware operations). | Security analysis report | |
| **(5) Risk Analysis**<br>a) Review and update risk analysis using prior task reports.<br>b) Provide recommendations to eliminate, reduce, or mitigate the risks. | Supplier development plans and schedules<br>Hazard analysis report<br>Security analysis report<br>Risk analysis report<br>V&V task results | Task report(s)—Risk analysis<br>Anomaly report(s) |

| 10.7 Activity: Hardware Acceptance Testing V&V (Hardware, Hardware Acceptance Support process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(1) Hardware Acceptance Test Procedure V&V**<br>a) Integrity levels 4 and 3<br>1) Develop test procedures for V&V hardware acceptance testing.<br>2) Continue the tracing required by the V&V hardware acceptance test plan.<br>3) Verify that the V&V hardware acceptance test procedures conform to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>4) Validate that the V&V hardware acceptance test procedures satisfy the criteria in V&V activity 10.2, Task 6.<br>b) Integrity level 2<br>1) Verify that the acquirer's hardware acceptance test procedures conform to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]).<br>2) Validate that the acquirer's hardware acceptance test procedures satisfy the criteria in V&V activity 10.2, Task 6.<br>c) Integrity level 1<br>There are no hardware acceptance V&V test requirements. | HDD<br>IDD<br>Hardware drawings<br>Hardware component specifications<br>User documentation<br>Hardware acceptance test plan<br>Hardware acceptance test procedures | V&V hardware acceptance test procedures (integrity levels 4 and 3)<br>Task report(s)—Review of hardware acceptance test procedures (integrity level 2)<br>Anomaly report(s) |
| **(2) Hardware Acceptance Test Execution V&V**<br>a) Integrity levels 4 and 3<br>1) Perform V&V hardware acceptance testing.<br>2) Analyze test results to validate that the hardware satisfies the system requirements.<br>3) Validate that the test results trace to test criteria established by the test traceability in the test planning documents.<br>4) Document the results as required by the V&V hardware acceptance test plan.<br>5) Use the V&V hardware acceptance test results to validate that the hardware satisfies the test acceptance criteria.<br>6) Document discrepancies between the actual and expected test results. | Hardware component specifications<br>User documentation<br>Hardware acceptance test plan<br>Hardware acceptance test procedures<br>Hardware acceptance test results | V&V hardware acceptance test execution results (integrity levels 4 and 3)<br>Task report(s)—Review of hardware acceptance test execution results (integrity level 2)<br>Anomaly report(s) |

| 10.7 Activity: Hardware Acceptance Testing V&V (Hardware, Hardware Acceptance Support process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| b) Integrity level 2<br>Use the acquirer's hardware acceptance test results to verify that the hardware satisfies the test acceptance criteria.<br>c) Integrity level 1<br>There are no hardware acceptance V&V test requirements. | | |
| **(3) Traceability Analysis**<br>Analyze relationships in the V&V Test Plans, Designs, Cases, and Procedures for correctness and completeness. The task criteria are:<br>a) Correctness<br>Verify that there is a valid relationship between the V&V test plans, designs, cases, and procedures.<br>b) Completeness<br>Verify that all V&V test procedures are traceable to the V&V test plans. | V&V test plans<br>V&V test designs<br>V&V test procedures | Task report(s)—Traceability analysis<br>Anomaly report(s) |
| **(4) Hazard Analysis**<br>a) Verify that the test instrumentation does not introduce new hazards.<br>b) Assess the identified mitigation strategies to verify each hazard is prevented, mitigated, or controlled (any unmitigated hazards are documented and addressed as part of system and hardware operations).<br>c) Update the hazard analysis. | Hardware component specifications<br>Test results<br>Hazard analysis report | Task report(s)—Hazard analysis<br>Anomaly report(s) |
| **(5) Security Analysis**<br>a) Verify that the implemented system does not increase the security risk.<br>b) Verify the identified security threats and vulnerabilities are prevented, controlled, or mitigated (any unmitigated threats and vulnerabilities are documented and addressed as part of system and hardware operations). | Hardware component specifications<br>Security analysis report | Task report(s)—Security analysis<br>Anomaly report(s) |
| **(6) Risk Analysis**<br>a) Review and update risk analysis using prior task reports.<br>b) Provide recommendations to eliminate, reduce, or mitigate the risks. | Supplier development plans and schedules<br>Hazard analysis report<br>Security analysis report<br>Risk analysis report<br>V&V task results | Task report(s)—Risk analysis<br>Anomaly report(s) |

| 10.8 Activity: Hardware Verification (Hardware, Hardware Verification process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| The activities and tasks for the Hardware Verification process are conducted in hardware technical life cycle processes, and are contained in Table 1d, Activity 10.1 (Hardware Concept V&V), Activity 10.2 (Hardware Requirements Analysis V&V), Activity 10.3 (Hardware Design V&V), Activity 10.4 (Hardware Fabrication V&V), Activity 10.5 (Hardware Integration V&V), Activity 10.6 (Hardware Qualification Testing V&V), Activity 10.7 (Hardware Acceptance Testing V&V), Activity 10.9 (Hardware Transition V&V), Activity 10.11 (Hardware Operation V&V), Activity 10.12 (Hardware Maintenance V&V), and Activity 10.13 (Hardware Disposal V&V). The hardware verification activities and tasks in Table 1d and the common verification activities and tasks in Table 1a represent all activities and tasks needed to perform hardware verification. | The required inputs for the Hardware Verification process are found in Table 1d required inputs. | The required outputs for the Hardware Verification process are found in Table 1d required outputs. |

| 10.9 Activity: Hardware Transition V&V (Hardware, Hardware Transition process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(1) Installation Configuration Audit**<br>a) Verify that all hardware products required to correctly install and operate the hardware are present in the installation package.<br>b) Validate that all site-dependent parameters or conditions to verify supplied values are correct. | Installation package (e.g., user documentation, HDD, IDD, HRS, IRS, hardware drawings, concept documentation, installation procedures, site-specific parameters, installation tests, and configuration management data) | Task report(s)—Installation configuration audit<br>Anomaly report(s) |
| **(2) Installation Checkout**<br>a) Conduct analyses or tests to verify that the installed hardware corresponds to the hardware subjected to V&V.<br>b) Verify that the hardware initializes, executes, and terminates as specified.<br>c) In the transition from one version of hardware to the next, validate that the hardware can be replaced with the new version without adversely affecting or degrading the functionality of the remaining system components.<br>d) Verify the requirements for continuous operation and service during transition, including requirements for user notification. | User documentation<br>Installation package | Task report(s)—Installation checkout<br>Anomaly report(s) |
| **(3) Hazard Analysis**<br>a) Verify that the installation procedures and installation environment does not introduce new hazards.<br>b) Assess the identified mitigation strategies to verify each hazard is prevented, mitigated, or controlled (any unmitigated hazards are documented and addressed as part of system and hardware operations).<br>c) Update the hazard analysis. | Installation package<br>Hazard analysis report | Task report(s)—Hazard analysis<br>Anomaly report(s) |
| **(4) Security Analysis**<br>a) Verify that the installed hardware does not introduce new or increased vulnerabilities or security risks to the overall system.<br>b) Verify the identified security threats and vulnerabilities are prevented, controlled, or mitigated (any unmitigated threats and | Installation package<br>User documentation<br>Security analysis report | Task report(s)—Security analysis<br>Anomaly report(s) |

| 10.9 Activity: Hardware Transition V&V (Hardware, Hardware Transition process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| vulnerabilities are documented and addressed as part of system and hardware operations). | | |
| **(5) Risk Analysis**<br>a) Review and update risk analysis using prior task reports.<br>b) Provide recommendations to eliminate, reduce, or mitigate the risks. | Installation package<br>Supplier development plans and schedules<br>Security analysis report<br>Risk analysis report<br>V&V task results | Task report(s)—Risk analysis<br>Anomaly report(s) |

| 10.10 Activity: Hardware Validation (Hardware, Hardware Validation process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| The activities and tasks for the Hardware Validation process are conducted in hardware technical life cycle processes, and are contained in Table 1d, Activity 10.1 (Hardware Concept V&V), Activity 10.2 (Hardware Requirements Analysis V&V), Activity 10.3 (Hardware Design V&V), Activity 10.4 (Hardware Fabrication V&V), Activity 10.5 (Hardware Integration V&V), Activity 10.6 (Hardware Qualification Testing V&V), Activity 10.7 (Hardware Acceptance Testing V&V), Activity 10.9 (Hardware Transition V&V), Activity 10.11 (Hardware Operation V&V), Activity 10.12 (Hardware Maintenance V&V), and Activity 10.13 (Hardware Disposal V&V). The hardware validation activities and tasks in Table 1d and the common validation activities and tasks in Table 1a represent all activities and tasks needed to perform hardware validation. | The required inputs for the Hardware Validation process inputs are found in Table 1d required inputs. | The required outputs for the Hardware Validation process outputs are found in Table 1d required outputs. |

| 10.11 Activity: Hardware Operation V&V (Hardware, Hardware Operation process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(1) Evaluation of New Constraints**<br>Evaluate new constraints (e.g., operational requirements, platform characteristics, and operating environment) on the system or hardware requirements to verify the applicability of the VVP. | VVP<br>New constraints | Task report(s)—Evaluation of new constraints |
| **(2) Operating Procedures Evaluation**<br>Verify that the operating procedures are consistent with the user documentation and conform to the system requirements. | Operating procedures<br>User documentation<br>Concept documentation | Task report(s)—Operating procedures evaluation<br>Anomaly report(s) |
| **(3) Hazard Analysis**<br>a) Verify that the operating procedures and operational environment does not introduce new hazards.<br>b) Assess the identified mitigation strategies to verify each hazard is prevented, mitigated, or controlled (any unmitigated hazards are documented and addressed as part of system and hardware operations).<br>c) Update the hazard analysis. | Operating procedures<br>Hazard analysis report | Task report(s)—Hazard analysis<br>Anomaly report(s) |
| **(4) Security Analysis**<br>a) Verify that no new security risks are introduced due to changes in the operational environment. | New constraints<br>Environmental changes | Task Reports—Security analysis |

| 10.11 Activity: Hardware Operation V&V (Hardware, Hardware Operation process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| b) Over time, changes in external interfaces, threats, or technology in general require that an updated security analysis be performed to determine an updated residual risk.<br>c) Verify the identified security threats and vulnerabilities are prevented, controlled, or mitigated (any unmitigated threats and vulnerabilities are documented and addressed as part of system and hardware operations). | Operating procedures<br>Security analysis report | |
| **(5) Risk Analysis**<br>a) Review and update risk analysis using prior task reports.<br>b) Provide recommendations to eliminate, reduce, or mitigate the risks. | Installation package<br>Proposed changes<br>Hazard analysis report<br>Security analysis report<br>Risk analysis report<br>Supplier development plans and schedules<br>Operation problem reports<br>V&V task results | Task report(s)—Risk analysis<br>Anomaly report(s) |

| 10.12 Activity: Hardware Maintenance V&V (Hardware, Hardware Maintenance process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(1) VVP Revision**<br>a) Revise the VVP to conform to approved changes.<br>b) When the development documentation required by this standard is not available, generate a new VVP and consider the methods in Annex D for deriving the required development documentation. | VVP<br>Approved changes<br>Installation package<br>Supplier development plans and schedules | Updated VVP |
| **(2) Anomaly Evaluation**<br>Evaluate the effect of hardware operation anomalies. | Anomaly report(s) | Task report(s)—Anomaly evaluation |
| **(3) Criticality Analysis**<br>a) Determine the integrity levels for proposed modifications.<br>b) Validate the integrity levels provided by the maintainer. For V&V planning purposes, the highest integrity level assigned to the hardware shall be the integrity level of the system. | Proposed changes<br>Installation package<br>Maintainer integrity levels | Task report(s)—Criticality analysis<br>Anomaly report(s) |
| **(4) Migration Assessment**<br>Assess whether the hardware requirements and fabrication address the following:<br>a) Specific migration requirements.<br>b) Migration tools.<br>c) Conversion of hardware products and data.<br>d) Hardware archiving.<br>e) Support for the prior environment.<br>f) User notification. | Installation package<br>Approved changes | Task report(s)—Migration assessment<br>Anomaly report(s) |
| **(5) Retirement Assessment**<br>Assess whether the installation package addresses the following:<br>a) Hardware support.<br>b) Impact on existing systems and data bases. | Installation package<br>Approved changes | Task report(s)—Retirement assessment<br>Anomaly report(s) |

| 10.12 Activity: Hardware Maintenance V&V (Hardware, Hardware Maintenance process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| c) Hardware archiving.<br>d) Transition to a new hardware product.<br>e) User notification. | | |
| **(6) Hazard Analysis**<br>a) Verify that hardware modifications correctly implement the critical requirements and introduce no new hazards.<br>b) Assess the identified mitigation strategies to verify each hazard is prevented, mitigated, or controlled (any unmitigated hazards are documented and addressed as part of system and hardware operations).<br>c) Update the hazard analysis. | Proposed changes<br>Installation package<br>Hazard analysis report | Task report(s)—Hazard analysis<br>Anomaly report(s) |
| **(7) Security Analysis**<br>a) Verify that proposed changes/updates to the hardware do not introduce new or increased security risks to the overall system.<br>b) Verify the identified security threats and vulnerabilities are prevented, controlled, or mitigated (any unmitigated threats and vulnerabilities are documented and addressed as part of system and hardware operations). | Proposed changes<br>Installation package<br>Security analysis report | Task reports—Security analysis |
| **(8) Risk Analysis**<br>a) Review and update risk analysis using prior task reports.<br>b) Provide recommendations to eliminate, reduce, or mitigate the risks. | Installation package<br>Proposed changes<br>Hazard analysis report<br>Security analysis report<br>Risk analysis report<br>Supplier development plans and schedules<br>Operation problem reports<br>V&V task results | Task report(s)—Risk analysis<br>Anomaly report(s) |
| **(9) Task Iteration**<br>Perform V&V tasks, as needed, to assure that the following is performed:<br>a) Planned changes are implemented correctly.<br>b) Documentation is complete and current.<br>c) Changes do not cause unacceptable or unintended system behaviors. | Approved changes<br>Installation package | Task report(s)<br>Anomaly report(s) |
| NOTE—Hardware changes are maintenance activities (see Clause 10.12). | | |

| 10.13 Activity: Hardware Disposal V&V (Hardware, Hardware Disposal process) | | |
|---|---|---|
| **V&V tasks** | **Required inputs** | **Required outputs** |
| **(1) Hardware Disposal Evaluation**<br>Verify that any constraints specified or implied by the hardware disposal strategy are included in the hardware requirements, including hardware element destruction/storage and recording disposal actions, and analysis of disposal impacts on the system. Validate that disposal leaves the system in an agreed-on state. | Hardware disposal strategy | Task report(s)—Hardware Disposal Evaluation<br>Anomaly report(s) |

NOTE (for Table 1d)—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 2d—Minimum V&V tasks assigned to each integrity level for hardware V&V**

| V&V Activities | Activity: Hardware Concept V&V (see 10.1) | | | | Activity: Hardware Requirements V&V (see 10.2) | | | | Activity: Hardware Design V&V (see 10.3) | | | | Activity: Hardware Fabrication V&V (see 10.4) | | | | Activity: Hardware Integration V&V (see 10.5) | | | | Activity: Hardware Qualification V&V (see 10.6) | | | | Activity: Hardware Acceptance V&V (see 10.7) | | | | Activity: Hardware Transition V&V (see 10.9) | | | | Activity: Hardware Operation V&V (see 10.11) | | | | Activity: Hardware Maintenance V&V (see 10.12) | | | | Activity: Hardware Disposal V&V (see 10.13) | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Integrity Levels | Levels | | | | Levels | | | | Levels | | | | Levels | | | | Levels | | | | 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 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 |
| Anomaly Evaluation | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | X | X | X | | | | | |
| Concept Documentation Evaluation | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Criticality Analysis | X | X | X | X | X | X | X | X | X | X | X | | X | X | X | | | | | | | | | | | | | | | | | | | | | | X | X | X | X | | | | |
| Design Evaluation | | | | | | | | | X | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Evaluation of New Constraints | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | X | X | X | | | | | | | | | |
| Fabricated Component Documentation Evaluation | | | | | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Hardware Acceptance Test Case V&V | | | | | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Hardware Acceptance Test Design V&V | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Hardware Acceptance Test Execution V&V | | | | | | | | | | | | | | | | | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | |
| Hardware Acceptance Test Plan V&V | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Hardware Acceptance Test Procedure V&V | | | | | | | | | | | | | | | | | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | |
| Hardware Component Test Case Assessment | | | | | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Hardware Component Test Design Assessment | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Hardware Component Test Execution Assessment | | | | | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Hardware Component Test Plan Assessment | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Hardware Component Test Procedures Assessment | | | | | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| V&V Activities | Activity: Hardware Concept V&V (see 10.1) | | | | Activity: Hardware Requirements V&V (see 10.2) | | | | Activity: Hardware Design V&V (see 10.3) | | | | Activity: Hardware Fabrication V&V (see 10.4) | | | | Activity: Hardware Integration V&V (see 10.5) | | | | Activity: Hardware Qualification V&V (see 10.6) | | | | Activity: Hardware Acceptance V&V (see 10.7) | | | | Activity: Hardware Transition V&V (see 10.9) | | | | Activity: Hardware Operation V&V (see 10.11) | | | | Activity: Hardware Maintenance V&V (see 10.12) | | | | Activity: Hardware Disposal V&V (see 10.13) | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Integrity Levels | Levels | | | | Levels | | | | Levels | | | | Levels | | | | Levels | | | | 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 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 |
| Hardware Disposal Evaluation | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | X | X | | |
| Hardware Integration Test Case Assessment | | | | | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Hardware Integration Test Design Assessment | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Hardware Integration Test Execution Assessment | | | | | | | | | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | |
| Hardware Integration Test Plan Assessment | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Hardware Integration Test Procedure Assessment | | | | | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Hardware Qualification Test Case V&V | | | | | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Hardware Qualification Test Design V&V | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Hardware Qualification Test Execution V&V | | | | | | | | | | | | | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | |
| Hardware Qualification Test Plan V&V | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Hardware Qualification Test Procedure V&V | | | | | | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Hazard Analysis | X | X | | | X | X | | | X | X | | | X | X | | | X | X | | | X | X | | | X | X | | | X | X | | | X | X | | | X | X | | | | | | |
| Installation Checkout | | | | | | | | | | | | | | | | | | | | | | | | | | | | | X | X | | | | | | | | | | | | | | |
| Installation Configuration Audit | | | | | | | | | | | | | | | | | | | | | | | | | | | | | X | X | | | | | | | | | | | | | | |
| Interface Analysis | | | | | X | X | X | | X | X | X | | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Migration Assessment | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | X | X | X | | | | | |
| Operation Procedures Evaluation | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | X | X | | | | | | | | | | |
| Requirements Allocation Analysis | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| V&V Activities | Activity: Hardware Concept V&V (see 10.1) | | | | Activity: Hardware Requirements V&V (see 10.2) | | | | Activity: Hardware Design V&V (see 10.3) | | | | Activity: Hardware Fabrication V&V (see 10.4) | | | | Activity: Hardware Integration V&V (see 10.5) | | | | Activity: Hardware Qualification V&V (see 10.6) | | | | Activity: Hardware Acceptance V&V (see 10.7) | | | | Activity: Hardware Transition V&V (see 10.9) | | | | Activity: Hardware Operation V&V (see 10.11) | | | | Activity: Hardware Maintenance V&V (see 10.12) | | | | Activity: Hardware Disposal V&V (see 10.13) | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Integrity Levels | Levels | | | | Levels | | | | Levels | | | | Levels | | | | Levels | | | | 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 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 | 4 | 3 | 2 | 1 |
| Requirements Evaluation | | | | | X | X | X | X | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Retirement Assessment | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | X | X | | | | | | |
| Risk Analysis | X | X | | | X | X | | | X | X | | | X | X | | | X | X | | | X | X | | | X | X | | | X | X | | | X | X | | | X | X | | | | | | |
| Security Analysis | X | X | | | X | X | | | X | X | | | X | X | | | X | X | | | X | X | | | X | X | | | X | X | | | X | X | | | X | X | | | | | | |
| Task Iteration | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | X | X | X | X | | | | |
| Traceability Analysis | X | X | X | | X | X | X | | X | X | X | | X | X | X | | X | X | X | | X | X | X | | X | X | X | | | | | | | | | | | | | | | | | |
| VVP Revision | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | X | X | X | X | | | | |

NOTE (for Table 2d)—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 analysis or test. A higher integrity level implementation requires greater rigor (e.g., formal methods, structured analysis methods), intensity (e.g., consideration of all system conditions and system environment states) and depth (e.g., abnormal cases, boundary conditions, comprehensive fault, and recovery scenarios) of analysis or test than the lower integrity level implementation.

### Table 3d—Optional V&V tasks and suggested applications in Hardware Technical and Implementation processes

The recommended applicability of optional tasks to the Hardware V&V processes described in Clause 10 is shown in Table 3a. Annex G provides a description of each of the optional V&V tasks.

| | Hardware Concept (10.1) | Hardware Requirements Analysis (10.2) | Hardware Design (10.3) | Hardware Fabrication (10.4) | Hardware Integration (10.5) | Hardware Qualification Testing (10.6) | Hardware Acceptance Testing (10.7) | Hardware Transition (10.9) | Hardware Operation (10.11) | Hardware Maintenance (10.12) | Hardware Disposal (10.13) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Algorithm analysis | X | X | X | X | | | | | | X | |
| Audit performance | X | X | X | X | X | X | X | X | | X | |
| Audit support | X | X | X | X | X | X | X | X | | X | |
| Control flow analysis | X | X | X | X | | | | | | X | |
| Cost analysis | X | X | X | X | X | X | X | X | | X | |
| Database analysis | X | X | X | X | | | X | | | X | |
| Data flow analysis | X | X | X | X | | | | | | X | |
| Disaster recovery plan assessment | X | X | X | X | | | | | X | X | X |
| Distributed architecture assessment | X | X | | | | | | | | X | |
| Exploratory testing | X | X | X | X | X | X | X | X | X | X | |
| Feasibility study evaluation | X | X | X | | | | | | | X | |
| Independent risk assessment | | | | | | | | | | X | |
| Inspection | | | | | | | | | | | |
| Inspection—Concept | | | | | | | | | | X | |
| Inspection—Requirements | X | | | | | | | | | X | |
| Inspection—Design | | X | X | | | | | | | X | |
| Inspection—Source code | | | | X | | | | | | | |
| Inspection—Test plan | X | X | X | X | X | X | X | | | X | |
| Inspection—Test design | | X | X | X | X | X | X | | | X | |
| Inspection—Test case | | X | X | X | X | X | X | | | X | |
| Operational evaluation | | | | | | | | | X | | |
| Performance monitoring | X | X | X | X | X | X | X | X | X | X | X |
| Post-installation validation | | | | | | | | | X | X | |
| Project management oversight support | X | X | X | X | X | X | X | X | X | X | X |
| Proposal evaluation support | | | | | | | | | | | |
| Qualification testing | | | | X | | X | X | | | | |
| Regression analysis and testing | X | X | | X | X | X | X | | | X | |
| Reusability analysis | X | X | X | X | | | | | | X | |
| Reuse analysis | X | X | X | | | | | | | X | |
| Simulation analysis | X | X | X | X | X | X | X | X | X | X | X |
| Sizing and timing analysis | X | X | X | X | X | X | X | X | | X | |
| System software assessment | | X | X | X | X | X | X | X | X | X | |
| Test certification | | | | X | X | X | X | | X | X | X |
| Test evaluation | X | X | X | X | X | X | X | | X | X | X |
| Test witnessing | | | | X | X | X | X | | X | X | X |
| Training documentation evaluation | X | X | X | X | X | X | X | | X | X | X |
| Usability analysis | X | X | X | X | X | X | X | | X | X | |
| User documentation evaluation | X | X | X | X | X | X | X | | X | X | |
| User training | | | | X | X | X | X | | X | X | |

| | Hardware Concept (10.1) | Hardware Requirements Analysis (10.2) | Hardware Design (10.3) | Hardware Fabrication (10.4) | Hardware Integration (10.5) | Hardware Qualification Testing (10.6) | Hardware Acceptance Testing (10.7) | Hardware Transition (10.9) | Hardware Operation (10.11) | Hardware Maintenance (10.12) | Hardware Disposal (10.13) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| V&V tool plan generation | | | | | | | | | | | |
| V&V tool qualification | X | X | X | X | X | X | X | X | X | X | |
| Walkthrough | | | | | | | | | | | |
| Walkthrough—Design | | X | | | | | | | | X | |
| Walkthrough—Requirements | X | | | | | | | | | X | |
| Walkthrough—Source code | | | | X | | | | | | | |
| Walkthrough—Test | | | | X | X | X | | | | X | |
| Work Breakdown Structure (WBS) Evaluation | | | | | | | | | | | |

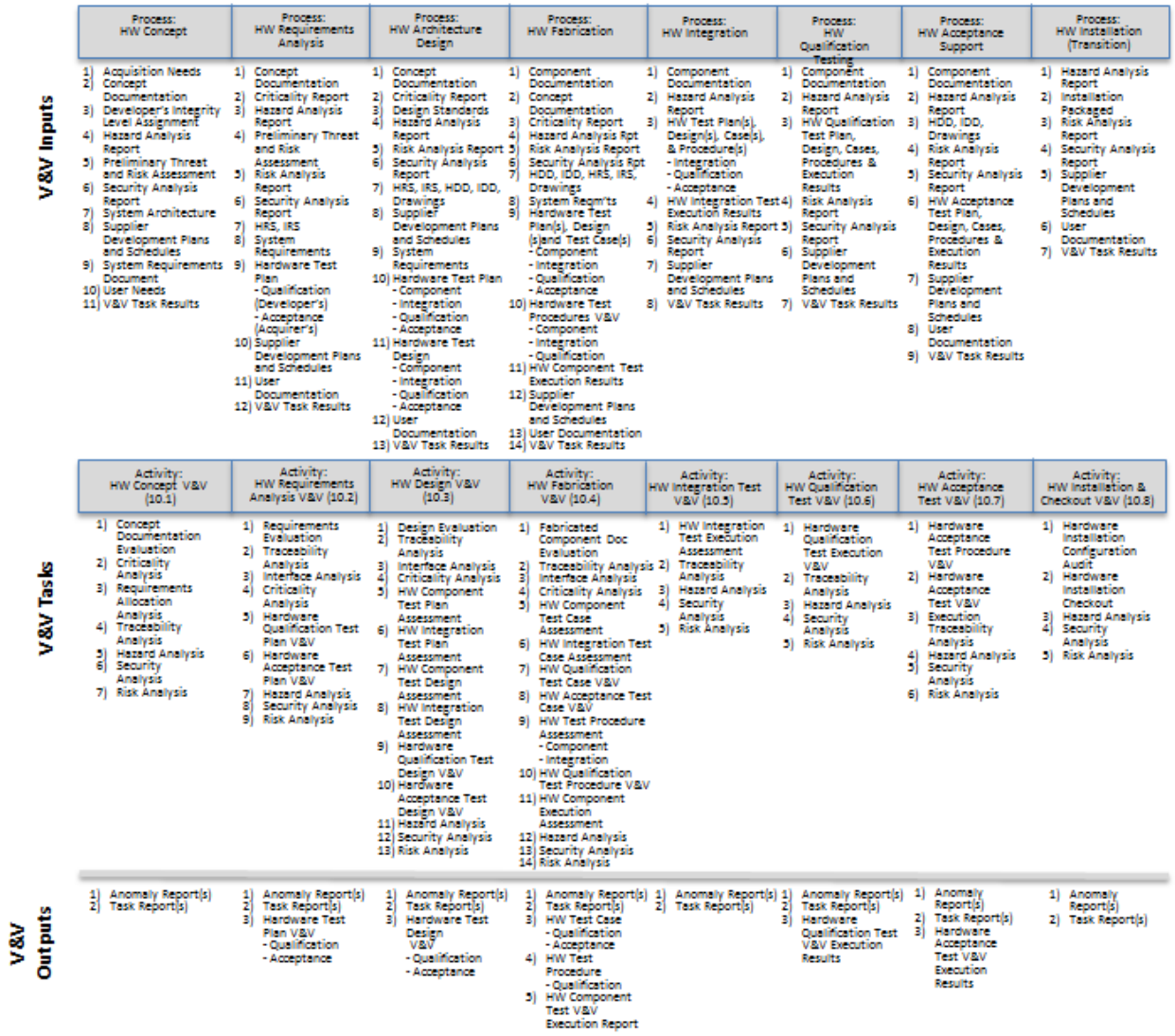
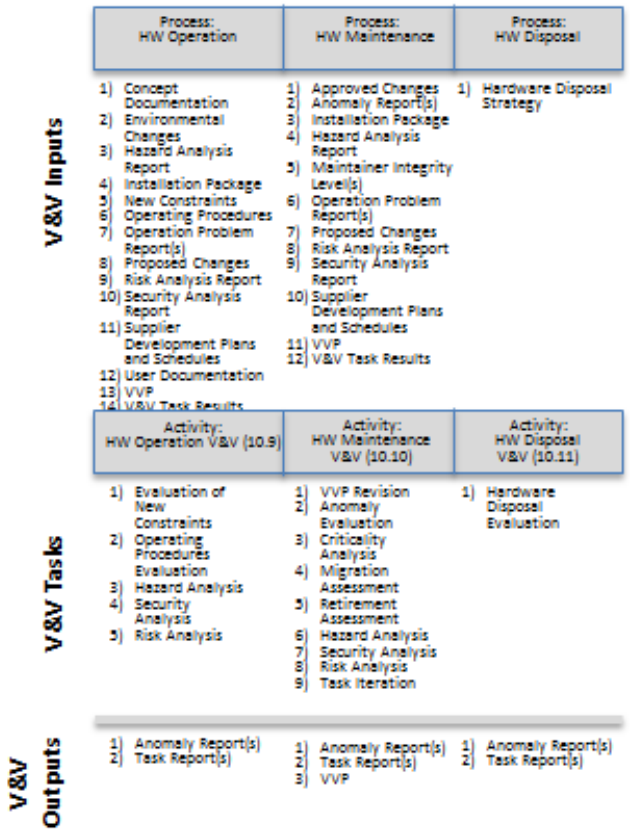



**Figure 1d—Example of hardware V&V processes, activities, and tasks**




NOTE 1—No clause references are listed in the process definitions (top graphic bar) as there are no ISO/IEC or IEEE hardware life cycle definition standards used.

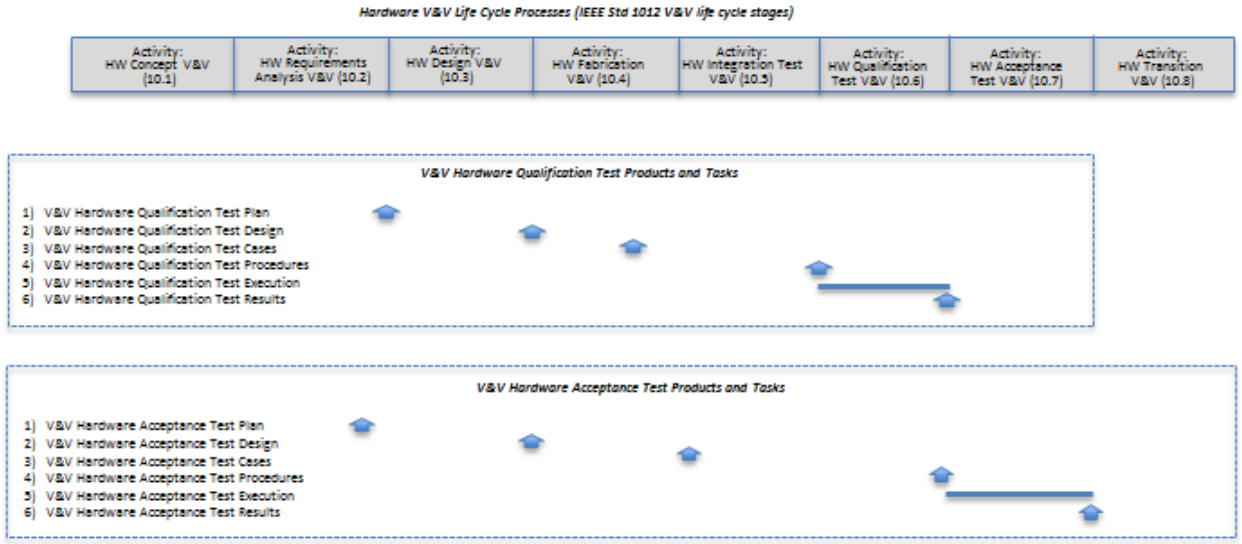
NOTE 2—Clause references in the activity V&V definitions (middle graphic bar) are IEEE Std 1012 clause numbers.

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

NOTE 4—Hardware Acceptance Testing process supports the Systems Integration Testing process.

NOTE 5—Hardware Installation and Checkout process supports the System Transition process.

**Figure 1d—Example of hardware V&V processes, activities, and tasks (continued)**




NOTE 1—All V&V hardware test products and tasks represent the activities and products required as a minimum for integrity level 4.

NOTE 2—This is an example of the phasing of hardware V&V test products and tasks across the hardware life cycle. The hardware V&V test products (upward arrows) are shown in the hardware life cycle stages when the products are generated. Hardware test execution tasks are shown to occur during one or more hardware life cycle stages as indicated by "activity bars" in the diagram. The life cycle stage (in which each test product is generated) and phasing of each test product and task can vary from this diagram in accordance with project specific needs.

NOTE 3—The V&V activity clauses referenced in the hardware V&V life cycle stages are IEEE Std 1012 clauses.

**Figure 2d—Summary of hardware V&V test products and tasks**

# 11. V&V reporting, administrative, and documentation requirements

## 11.1 V&V reporting requirements

V&V reporting occurs throughout the system, software, or hardware life cycle. The V&V effort shall produce the required outputs listed in Table 1a through Table 1d for each V&V task performed. The format and grouping of the V&V reports may be user defined. The V&V activity and task reports shall constitute the V&V report.

The V&V report shall consist of the following:

a) V&V task reports. The V&V effort shall document V&V task results and status. A task report may be combined with its associated activity report or with other task reports. Task reports are generated for the following tasks:

   1) Acceptance Support
   2) Anomaly Evaluation
   3) Concept Documentation Evaluation
   4) Configuration Management Assessment
   5) Contract Verification
   6) Criticality Analysis
   7) Design Evaluation
   8) Disposal Plan Evaluation
   9) Evaluation of New Constraints
   10) Fabricated Component Documentation Evaluation
   11) Hardware Acceptance Test Case V&V
   12) Hardware Acceptance Test Design V&V
   13) Hardware Acceptance Test Execution V&V
   14) Hardware Acceptance Test Plan V&V
   15) Hardware Acceptance Test Procedure V&V
   16) Hardware Component Test Case Assessment
   17) Hardware Component Test Design Assessment
   18) Hardware Component Test Execution Assessment
   19) Hardware Component Test Plan Assessment
   20) Hardware Component Test Procedure Assessment
   21) Hardware Disposal Evaluation
   22) Hardware Integration Test Case Assessment
   23) Hardware Integration Test Design Assessment
   24) Hardware Integration Test Execution Assessment
   25) Hardware Integration Test Plan Assessment
   26) Hardware Integration Test Procedure Assessment

27) Hardware Qualification Test Case V&V
28) Hardware Qualification Test Design V&V
29) Hardware Qualification Test Execution V&V
30) Hardware Qualification Test Plan V&V
31) Hardware Qualification Test Procedure V&V
32) Requirements Allocation Analysis
33) Hazard Analysis
34) Identify Process Improvement Opportunities in the Conduct of V&V
35) Implementation Strategy Assessment
36) Installation Checkout
37) Installation Configuration Audit
38) Interface Analysis
39) Interface with other Processes
40) Migration Assessment
41) Operating Procedures Evaluation
42) Project Planning Strategy Assessment
43) Proposed/Baseline Change Assessment
44) Requirements Evaluation
45) Requirements Review
46) Retirement Assessment
47) Risk Analysis
48) Scoping the V&V Effort
49) Security Analysis
50) Software Acceptance Test Case V&V
51) Software Acceptance Test Design V&V
52) Software Acceptance Test Execution V&V
53) Software Acceptance Test Plan V&V
54) Software Acceptance Test Procedure V&V
55) Software Component Test Case V&V
56) Software Component Test Design V&V
57) Software Component Test Execution V&V
58) Software Component Test Plan V&V
59) Software Component Test Procedure V&V
60) Software Disposal Evaluation
61) Software Integration Test Case V&V
62) Software Integration Test Design V&V

63) Software Integration Test Execution V&V
64) Software Integration Test Plan V&V
65) Software Integration Test Procedure V&V
66) Software Qualification Test Case V&V
67) Software Qualification Test Design V&V
68) Software Qualification Test Execution V&V
69) Software Qualification Test Plan V&V
70) Software Qualification Test Procedure V&V
71) Source Code and Source Code Documentation Evaluation
72) Stakeholder Requirements Evaluation
73) System Acceptance Test Case V&V
74) System Acceptance Test Design V&V
75) System Acceptance Test Execution V&V
76) System Acceptance Test Plan V&V
77) System Acceptance Test Procedure V&V
78) System Element Implementation Analysis
79) System Integration Strategy Assessment
80) System Integration Test Case V&V
81) System Integration Test Design V&V
82) System Integration Test Execution V&V
83) System Integration Test Plan V&V
84) System Integration Test Procedure V&V
85) System Maintenance Execution Assessment
86) System Maintenance Strategy Assessment
87) System Qualification Test Case V&V
88) System Qualification Test Design V&V
89) System Qualification Test Execution V&V
90) System Qualification Test Plan V&V
91) System Qualification Test Procedure V&V
92) Traceability Analysis
93) Transition Demonstration Assessment
94) Transition Strategy Evaluation

b) V&V activity summary reports. An activity summary report shall summarize the results of V&V tasks performed for the following V&V life cycle activities:

**System V&V**

1) Acquisition Support
2) Supply Planning
3) Project Planning

4) Configuration Management
5) Stakeholder Requirements Definition
6) Requirements Analysis
7) Architectural Design
8) Implementation
9) Integration
10) Transition
11) Operation
12) Maintenance
13) Disposal

**Software V&V**

14) Software Concept
15) Software Requirements
16) Software Design
17) Software Construction
18) Software Integration Test
19) Software Qualification Test
20) Software Acceptance Test
21) Software Installation and Checkout
22) Software Operation
23) Software Maintenance
24) Software Disposal

**Hardware V&V**

25) Hardware Concept
26) Hardware Requirements
27) Hardware Design
28) Hardware Fabrication
29) Hardware Integration Test
30) Hardware Qualification Test
31) Hardware Acceptance Test
32) Hardware Transition
33) Hardware Operation
34) Hardware Maintenance
35) Hardware Disposal

For the operation and maintenance life cycle activities, V&V activity summary reports may be either updates to previous V&V activity summary reports or separate documents.

a) V&V anomaly reports. The V&V effort shall document in an anomaly report each anomaly it detects.

b) V&V final report. The V&V final report shall be issued at the conclusion of the V&V effort.

c) Optional V&V reports. The V&V reports may also include optional reports (i.e., special studies reports and other reports). The V&V effort shall document in a special studies report any special V&V studies conducted during the life cycle. The V&V effort shall document in a report the results of tasks conducted but not defined in the VVP. These other task reports may include, for example, quality assurance results, end-user testing results, safety assessment report, or configuration and data management status results. The title of the report may vary according to the subject matter.

Task report(s) and Anomaly report(s) should be provided as feedback to the development process regarding the technical quality of each product and process.

## 11.2 V&V administrative requirements

The V&V administrative requirements shall consist of the following:

a) Anomaly resolution and reporting policy

b) Task iteration policy

c) Deviation policy

d) Control procedures

e) Standards, practices, and conventions

These administrative requirements shall be documented in the VVP.

## 11.3 V&V documentation requirements

### 11.3.1 V&V test documentation

V&V test documentation requirements shall include the test plans, designs, cases, procedures, and results for component, integration, qualification, and acceptance testing developed by the V&V effort. The V&V test documentation shall conform to project-defined test document purpose, format, and content (e.g., IEEE Std 829-2008 [B3]). If the V&V effort uses test documentation or test types different from those in this standard (i.e., component, integration, qualification, and acceptance), the V&V effort shall show a mapping of the proposed test documentation and execution to the test items defined in this standard. Test planning tasks defined in Table 1a through Table 1d shall be documented in the test plan, test design(s), test case(s), and test procedure(s).

### 11.3.2 VVP documentation

The V&V effort shall generate a VVP that addresses the topics described in Clause 12 of this standard. If there is no information pertinent to a topic, then the VVP shall contain the phrase “This topic is not applicable to this plan” and shall state an appropriate reason for the exclusion. Additional topics may be added to the plan. If some VVP material appears in other documents, the VVP may repeat the material or make reference to the material. The VVP shall be maintained throughout the life cycle of the system, software, or hardware.

# 12. V&V plan

## 12.1 Overview

The VVP shall contain the content described in this subclause. The user of this standard may adopt any format and section numbering system for the VVP. The VVP section numbers listed in this clause are provided to assist readability. An example VVP outline is shown in the following boxed text.

**VVP outline (example)**

1. Purpose
2. Referenced documents
3. Definitions
4. V&V overview
    - 4.1 Organization
    - 4.2 Master schedule
    - 4.3 Integrity level schema
    - 4.4 Resources summary
    - 4.5 Responsibilities
    - 4.6 Tools, techniques, and methods
5. V&V processes
    - 5.1 Common V&V processes, activities, and tasks
        - 5.1.1 Acquisition support V&V
        - 5.1.2 Supply planning V&V
        - 5.1.3 Project planning V&V
        - 5.1.4 Configuration management V&V
    - 5.2 System V&V processes, activities, and tasks
        - 5.2.1 Business or mission analysis V&V
        - 5.2.2 Stakeholder needs and requirements definition V&V
        - 5.2.3 System requirements definition V&V
        - 5.2.4 Architecture definition V&V
        - 5.2.5 Design definition V&V
        - 5.2.6 System analysis V&V
        - 5.2.7 Implementation V&V
        - 5.2.8 Integration V&V
        - 5.2.9 Transition V&V
        - 5.2.10 Operation V&V
        - 5.2.11 Maintenance V&V
        - 5.2.12 Disposal V&V
    - 5.3 Software V&V processes, activities, and tasks
        - 5.3.1 Software concept V&V
        - 5.3.2 Software requirements V&V
        - 5.3.3 Software design V&V
        - 5.3.4 Software construction V&V
        - 5.3.5 Software integration Test V&V
        - 5.3.6 Software qualification Test V&V
        - 5.3.7 Software acceptance Test V&V
        - 5.3.8 Software installation and checkout (transition) V&V
        - 5.3.9 Software operation V&V
        - 5.3.10 Software maintenance V&V
        - 5.3.11 Software disposal V&V
    - 5.4 Hardware V&V processes, activities, and tasks
        - 5.4.1 Hardware concept V&V
        - 5.4.2 Hardware requirements V&V
        - 5.4.3 Hardware design V&V
        - 5.4.4 Hardware fabrication V&V
        - 5.4.5 Hardware integration Test V&V
        - 5.4.6 Hardware qualification Test V&V
        - 5.4.7 Hardware acceptance Test V&V
        - 5.4.8 Hardware transition V&V
        - 5.4.9 Hardware operation V&V
        - 5.4.10 Hardware maintenance V&V
        - 5.4.11 Hardware disposal V&V

6. V&V reporting requirements
    6.1 Task reports
    6.2 Anomaly reports
    6.3 V&V final report
    6.4 Special studies reports (optional)
    6.5 Other reports (optional)
7. V&V administrative requirements
    7.1 Anomaly resolution and reporting
    7.2 Task iteration policy
    7.3 Deviation policy
    7.4 Control procedures
    7.5 Standards, practices, and conventions
8. V&V test documentation requirements

## 12.2 VVP Section 1: Purpose

The VVP shall describe the purpose, goals, and scope of the V&V effort, including waivers from this standard. The date of issue and status, identification of issuing organization, and identification of approval authority shall be provided.

## 12.3 VVP Section 2: Referenced documents

The VVP shall identify the compliance documents, documents referenced by the VVP, and any supporting documents supplementing or implementing the VVP.

## 12.4 VVP Section 3: Definitions

The VVP shall define or reference all terms used in the VVP, including the criteria for classifying an anomaly as a critical anomaly. All abbreviations and notations used in the VVP also shall be described.

## 12.5 VVP Section 4: V&V overview

### 12.5.1 VVP Section 4.1: Organization

The VVP shall describe the organization of the V&V effort, including the degree of independence required (see Annex C). The VVP shall describe the relationship of the V&V processes to other processes, such as development, project management, quality assurance, and configuration management. The VVP shall describe the lines of communication within the V&V effort, the authority for resolving issues raised by V&V tasks, and the authority for approving V&V products. Annex F illustrates a sample organizational interrelationship chart.

### 12.5.2 VVP Section 4.2: Master schedule

The VVP shall describe the project life cycle and milestones and shall summarize the schedule of V&V tasks and task results as feedback to the development, organizational project-enabling, and supporting processes (e.g., quality assurance and configuration management). V&V tasks should be scheduled to be re-performed according to the task iteration policy. The detailed V&V schedule (e.g., task start and end dates, dependencies, assigned resources) may be maintained outside the VVP in order to accommodate the inevitable changes that occur in a project schedule.

If the life cycle used in the VVP differs from the life cycle model in this standard, this section shall describe how all requirements of the standard are satisfied (e.g., by cross referencing to this standard).

### 12.5.3 VVP Section 4.3: Integrity level schema

The VVP shall describe the agreed-on integrity level schema established for the system, software, or hardware, and the mapping of the selected schema to the model used in this standard. Where different integrity levels are assigned within the system of interest, the VVP shall document (by inclusion or by reference to the criticality analysis) the assignment of integrity levels to individual components (e.g., requirements, detailed functions, subsystems, software modules, hardware component, or other components).

### 12.5.4 VVP Section 4.4: Resources summary

The VVP shall summarize the V&V resources, including staffing, facilities, tools, finances, and special procedural requirements (e.g., security, access rights, and documentation control).

### 12.5.5 VVP Section 4.5: Responsibilities

The VVP shall identify an overview of the organizational element(s) and responsibilities for V&V tasks.

### 12.5.6 VVP Section 4.6: Tools, techniques, and methods[1]

The VVP shall describe documents, hardware and software V&V tools, techniques, methods, and operating and test environment to be used in the V&V processes. Acquisition, training, support, and qualification information for each tool, technology, and method shall be included.

The VVP should document the measures to be used by V&V (see Annex E) and should describe how these measures support the V&V objectives.

## 12.6 VVP Section 5: V&V processes

### 12.6.1 General

The VVP also shall identify the specific processes and products covered by the V&V effort and the activities and tasks performed as derived from the Table 2a through Table 2d minimum V&V requirements and the optional tasks selected for the project.

[1] The information in this footnote is based on excerpts from ISO/IEC/IEEE 29148-2011 [B22].

Verification and validation methods define how (including success criteria and closure approach), where, and when each requirement's conformance will be proven. A verification or validation method is associated with each requirement to define activities that yield objective information to prove satisfaction of the requirement. A verification or validation method definition addresses the following content considerations:

- How: Identify which method(s) will be applied (e.g., inspection, analysis, demonstration, and test).
- Who: Identify the organization/person with the lead responsibility for performing the method, such as a contractor, subcontractor, vendor, product team, or supplier.
- When: Designate a time in the program plan when the method is to be done. This should be event based and not a calendar date or accomplishment.
- Where: Specify any unique venue and environment needed for the method.
- Examples of verification and validation methods to use to obtain the objective evidence that the requirements have been fulfilled are inspection, analysis or simulation, demonstration, and test. The definitions are as follows:
- Inspection: An examination of the item against applicable documentation to confirm compliance with requirements.
- Analysis (including modeling and simulation): Use of analytical data or simulations under defined conditions to show theoretical compliance.
- Demonstration: A qualitative exhibition of functional performance, usually accomplished with no or minimal instrumentation or test equipment.
- Test: An action by which the operability, supportability, or performance capability of an item is quantitatively verified when subjected to controlled conditions that are real or simulated.

### 12.6.2 VVP Section 5.1: Common V&V processes, activities, and tasks

The VVP shall identify and describe the Common V&V processes, activities, and tasks as identified in Table 1a to be implemented and performed for this V&V project. The minimum common V&V tasks for the selected system integrity level are defined in Table 2a.

### 12.6.3 VVP Section 5.2: System V&V processes, activities, and tasks

The VVP shall identify and describe the System V&V processes, activities, and tasks as identified in Table 1b to be implemented and performed for this V&V project. The minimum system V&V tasks for the selected system integrity level are defined in Table 2b.

### 12.6.4 VVP Section 5.3: Software V&V processes, activities, and tasks

The VVP shall identify and describe the Software V&V processes, activities, and tasks as identified in Table 1c to be implemented and performed for this V&V project. The minimum software V&V tasks for the selected system integrity level are defined in Table 2c.

### 12.6.5 VVP Section 5.4: Hardware V&V processes, activities, and tasks

The VVP shall identify and describe the Hardware V&V processes, activities, and tasks as identified in Table 1d to be implemented and performed for this V&V project. The minimum hardware V&V tasks for the selected system integrity level are defined in Table 2d.

## 12.7 VVP Section 6: V&V reporting requirements

The VVP shall specify the purpose, content, format, recipients, and timing of all V&V reports. The V&V reporting requirements are specified in Clause 11.

## 12.8 VVP Section 7: V&V administrative requirements

### 12.8.1 General

The VVP shall describe the anomaly resolution and reporting, task iteration policy, deviation policy, control procedures, and standards, practices, and conventions.

### 12.8.2 VVP Section 7.1: Anomaly resolution and reporting

The VVP shall describe the method of reporting and resolving anomalies, including the criteria for reporting an anomaly, the anomaly report distribution list, the authority and time lines for resolving anomalies, and the anomaly criticality levels. Classification for software anomalies may be found in IEEE Std 1044-2009 [B7].

### 12.8.3 VVP Section 7.2: Task iteration policy

The VVP shall describe the criteria used to determine the extent to which a V&V task should be repeated when its input is changed or task procedure is changed. These criteria may include assessments of change, integrity level, and effects on budget, schedule, and quality.

### 12.8.4 VVP Section 7.3: Deviation policy

The VVP shall describe the procedures and criteria used to deviate from the plan. The information required for deviations shall include task identification, rationale, and effect on quality. The VVP shall identify the authorities responsible for approving deviations.

### 12.8.5 VVP Section 7.4: Control procedures

The VVP shall identify control procedures applied to the V&V effort. These procedures shall describe how products and V&V results should be configured, protected, and stored.

These procedures may describe quality assurance, configuration management, data management, or other activities if they are not addressed by other efforts. The VVP shall describe how the V&V effort shall conform to existing security provisions and how the validity of V&V results shall be protected from unauthorized alterations.

### 12.8.6 VVP Section 7.5: Standards, practices, and conventions

The VVP shall identify the standards, practices, and conventions that govern the performance of V&V tasks, including internal organizational standards, practices, and policies.

## 12.9 VVP Section 8: V&V test documentation requirements

The VVP shall describe the purpose, format, and content for the following V&V test documents:

a) Test plan

b) Test design

c) Test cases

d) Test procedures

e) Test results

The V&V effort may define the format for these documents. IEEE Std 829-2008 [B3] contains sample formats for these test documents.

# Annex A

(informative)

# Mapping of IEEE 1012 verification and validation (V&V) activities and tasks

## A.1 Mapping of ISO/IEC/IEEE 15288 activities to IEEE 1012 V&V activities and tasks

Table A.1 shows a mapping of ISO/IEC/IEEE 15288:2015(E) [B16] activities to the V&V activities and tasks of this standard.

The first column of Table A.1 lists the ISO/IEC/IEEE 15288:2015(E) [B16] clause numbers and titles of activities. The second column of Table A.1 lists the IEEE Std 1012 clauses and tables that map to the activities listed in the first column.

**Table A.1—Mapping ISO/IEC/IEEE 15288 V&V requirements to IEEE 1012 V&V activities and tasks**

| ISO/IEC/IEEE 15288 Activities | IEEE 1012 V&V Activities and Tasks (see corresponding clause/table) |
|---|---|
| 6.1.1.3 d Monitor the agreement [with the supplier] | **7.2.3 a) Activity: Acquisition Support V&V**<br>Task 2 Planning the Interface between the V&V Effort and Supplier<br>Task 3 System Requirements Review<br><br>**7.3.3 a) Activity: Supply Planning V&V**<br>Task 1 Planning the Interface between the V&V Effort and Supplier<br>Task 2 Contract Verification |
| 6.1.1.3 e Accept the product or service [from the supplier] | **7.2.3 a) Activity: Acquisition Support V&V**<br>Task 4 Acceptance Support |
| 6.4.1.3 c Characterize the solution space | **8.1.3 a) Activity: Business or Mission Analysis V&V**<br>Task 1 Business or Mission Analysis Results Evaluation<br>Task 2 Traceability Analysis<br>Task 3 Criticality Analysis<br>Task 4 Hazard Analysis<br>Task 5 Security Analysis<br>Task 6 Risk Analysis |
| 6.4.1.3 d Evaluate alternative solution classes | **8.1.3 a) Activity: Business or Mission Analysis V&V**<br>Task 1 Business or Mission Analysis Results Evaluation |
| 6.4.2.3 b Define stakeholder needs | **5. Integrity Levels**<br><br>**8.2.3 a) Activity: Stakeholder Needs and Requirements Definition V&V**<br>Task 1 Stakeholder Needs and Requirements Evaluation<br>Task 2 Traceability Analysis<br>Task 3 Criticality Analysis<br>Task 4 Hazard Analysis<br>Task 5 Security Analysis<br>Task 6 Risk Analysis |
| 6.4.2.3 e Analyze stakeholder requirements | **8.2.3 a) Activity: Stakeholder Needs and Requirements Definition V&V**<br>Task 1 Stakeholder Needs and Requirements Evaluation |

| ISO/IEC/IEEE 15288 Activities | IEEE 1012 V&V Activities and Tasks (see corresponding clause/table) |
|---|---|
| 6.4.3.3 b Define system requirements | **5. Integrity Levels**<br><br>**8.3.3 a) Activity: System Requirements Definition V&V**<br>Task 1 Requirements Evaluation<br>Task 2 Interface Analysis<br>Task 3 Traceability Analysis<br>Task 4 Criticality Analysis<br>Task 5 System Integration Test Plan V&V<br>Task 6 System Qualification Test Plan V&V<br>Task 7 System Acceptance Test Plan V&V<br>Task 8 Hazard Analysis<br>Task 9 Security Analysis<br>Task 10 Risk Analysis |
| 6.4.3.3 c Analyze system requirements | **8.3.3 a) Activity: System Requirements Definition V&V**<br>Task 1 Requirements Evaluation |
| 6.4.4.3 b Develop architecture viewpoints | **5. Integrity Levels**<br><br>**8.4.3 a) Activity: Architecture Definition V&V**<br>Task 1 Architecture Evaluation<br>Task 2 Interface Analysis<br>Task 3 Requirements Allocation Analysis<br>Task 4 Traceability Analysis<br>Task 5 Criticality Analysis<br>Task 6 System Integration Test Design V&V<br>Task 7 System Qualification Test Design V&V<br>Task 8 System Acceptance Test Design V&V<br>Task 9 Hazard Analysis<br>Task 10 Security Analysis<br>Task 11 Risk Analysis |
| 6.4.4.3 c Develop models and views of candidate architectures | **8.4.3 a) Activity: Architecture Definition V&V**<br>Task 1 Architecture Evaluation |
| 6.4.4.3 d Relate the architecture to design | **8.4.3 a) Activity: Architecture Definition V&V**<br>Task 1 Architecture Evaluation |
| 6.4.4.3 f Assess architecture candidates | **8.4.3 a) Activity: Architecture Definition V&V**<br>Task 1 Architecture Evaluation |
| 6.4.5.3 b Establish design characteristics and design enablers related to each system element | **5. Integrity Levels**<br><br>**8.5.3 a) Activity: Design Definition V&V**<br>Task 1 Design Evaluation<br>Task 2 Interface Analysis<br>Task 3 Traceability Analysis<br>Task 4 Criticality Analysis<br>Task 5 System Integration Test Case V&V<br>Task 6 System Qualification Test Case V&V<br>Task 7 System Acceptance Test Case V&V<br>Task 8 Hazard Analysis<br>Task 9 Security Analysis<br>Task 10 Risk Analysis |
| 6.4.5.3 d Manage the design | **5. Integrity Levels**<br><br>**8.5.3 a) Activity: Design Definition V&V**<br>Task 1 Design Evaluation<br>Task 2 Interface Analysis<br>Task 3 Traceability Analysis<br>Task 4 Criticality Analysis<br>Task 8 Hazard Analysis<br>Task 9 Security Analysis<br>Task 10 Risk Analysis |

| ISO/IEC/IEEE 15288 Activities | IEEE 1012 V&V Activities and Tasks (see corresponding clause/table) |
|---|---|
| 6.4.6.3 a Prepare for system analysis | **8.6.3 a) Activity: System Analysis V&V**<br>Task 1 System Analysis Strategy Evaluation |
| 6.4.6.3 b Perform system analysis | **8.6.3 a) Activity: System Analysis V&V**<br>Task 2 System Analysis Results Evaluation |
| 6.4.7.3 b Perform implementation | **5. Integrity Levels**<br><br>**8.7.3 a) Activity: Implementation V&V**<br>Task 1 Implementation Strategy Assessment<br>Task 2 System Element Implementation Analysis<br>Task 3 System Element Interaction Analysis<br>Task 4 Criticality Analysis<br>Task 5 System Integration Test Procedure V&V<br>Task 6 System Qualification Test Procedure V&V<br>Task 7 System Acceptance Test Procedure V&V<br>Task 8 Hazard Analysis<br>Task 9 Security Analysis<br>Task 10 Risk Analysis |
| 6.4.8.3 b Perform integration—Successively integrate system element configurations until the complete system is synthesized | **8.3.3 a) Activity: System Requirements Definition V&V**<br>Task 5 System Integration Test Plan V&V<br><br>**8.4.3 a) Activity: Architecture Definition V&V**<br>Task 5 System Integration Test Design V&V<br><br>**8.5.3 a) Activity: Design Definition V&V**<br>Task 5 System Integration Test Case V&V<br><br>**8.7.3 a) Activity: Implementation V&V**<br>Task 4 System Integration Test Procedure V&V<br><br>**8.8.3 a) Activity: Integration V&V**<br>Task 1 System Integration Strategy Assessment<br>Task 2 System Integration Test Execution V&V<br>Task 3 System Element Interaction Analysis<br>Task 4 System Qualification Test Execution V&V |
| 6.4.9.3 a Prepare for verification | **7.1 Activity: V&V Management**<br>Task 1 VVP Generation |
| 6.4.9.3 b Perform verification | Clause 1 through Clause 8, Clause 11, Clause 12, Table 1a, Table 1b, Table 2a, Table 2b, Table 3a, and Table 3b, Figure 1a, Figure 1b, Figure 2a, and Figure 2b, all annexes |
| 6.4.9.3 c Manage results of verification | Clause 8, Clause 11, Clause 12, Table 1a, Table 1b |
| 6.4.10.3 b Perform the transition | **8.3.3 a) Activity: System Requirements Definition V&V**<br>Task 7 System Acceptance Test Plan V&V<br><br>**8.4.3 a) Activity: Architectural Definition V&V**<br>Task 7 System Acceptance Test Design V&V<br><br>**8.5.3 a) Activity: Design Definition V&V**<br>Task 7 System Acceptance Test Case V&V<br><br>**8.7.3 a) Activity: Implementation V&V**<br>Task 6 System Acceptance Test Procedure V&V<br><br>**8.8.3 a) Activity: Integration V&V**<br>Task 6 System Acceptance Test Execution V&V<br><br>**8.10.3 a) Activity: Transition V&V**<br>Task 1 Transition Strategy Evaluation |

| ISO/IEC/IEEE 15288 Activities | IEEE 1012 V&V Activities and Tasks (see corresponding clause/table) |
|---|---|
| | Task 2 Transition Demonstration Assessment<br>Task 3 System Acceptance Test Execution V&V |
| 6.4.11.3 a Plan validation | **7.1 Activity: V&V Management**<br>Task 1 VVP Generation |
| 6.4.11.3 b Perform validation | Clause 1 through Clause 8, Clause 11, Clause 12, Table 1a, Table 1b, Table 2a, Table 2b, Table 3a, and Table 3b, Figure 1a, Figure 1b, Figure 2a, and Figure 2b, all annexes |
| 6.4.11.3 c Manage results of validation | Clause 8, Clause 11, Clause 12, Table 1a, Table 1b |
| 6.4.12.3 b Perform operation | **8.12.3 a) Activity: Operation V&V**<br>Task 1 Operating Procedures Evaluation<br>Task 2 Hazard Analysis<br>Task 3 Security Analysis<br>Task 4 Risk Analysis |
| 6.4.13.3 b Perform maintenance | **8.13.3 a) Activity: Maintenance V&V**<br>Task 1 System Maintenance Strategy Assessment<br>Task 2 System Maintenance Execution Assessment |
| 6.4.14.3 a Prepare for disposal | **8.14.3 a) Activity: Disposal V&V**<br>Task 1 Disposal Plan Evaluation |

## A.2 Mapping of IEEE 1012 V&V activities to ISO/IEC/IEEE 15288 system life cycle processes and activities

This standard defines five Common V&V activities and nine System V&V activities, as shown in the first column of Table A.2, that are part of the V&V processes. These 14 V&V activities evaluate the products produced or revised by the ISO/IEC/IEEE 15288:2015(E) [B16] system life cycle processes and activities shown in columns two and three of Table A.2.

**Table A.2—Mapping IEEE 1012 V&V activities to ISO/IEC/IEEE 15288**

| IEEE 1012 V&V Activities (see corresponding clause) | ISO/IEC/IEEE 15288 system life cycle | |
|---|---|---|
| | Process | Activity |
| 7.1.3 a) Activity: V&V Management | 6.4.9 Verification Process<br>6.4.11 Validation Process | 6.4.9.3 Prepare for verification<br>6.4.11.3 Prepare for validation |
| 7.2.3 a) Activity: Acquisition Support V&V | 6.1.1 Acquisition Process | 6.1.1.3.a Prepare for the acquisition<br>6.1.1.3.c Initiate an agreement<br>6.1.1.3.d Monitor the agreement<br>6.1.1.3.e Accept the product or service |
| 7.3.3 a) Activity: Supply Planning V&V | 6.1.2 Supply Process | 6.1.2.3.c Initiate an agreement<br>6.1.2.3.d Execute the agreement<br>6.1.2.3.e Deliver and support the product or service |
| 7.4.3 a) Activity: Project Planning V&V | 6.3.1 Project Planning Process | 6.3.1.3. a Define the project<br>6.3.1.3.b Plan project and technical management |
| 7.5.3 a) Activity: Configuration Management V&V | 6.3.5 Configuration Management Process | 6.3.5.3.a Plan configuration management<br>6.3.5.3.b Perform configuration identification<br>6.3.5.3.b Perform configuration change management |
| 8.1.3 a) Activity: Business or Mission Analysis Results Evaluation | 6.4.1 Business or Mission Analysis Process | 6.4.1.3.c Characterize the solution space<br>6.4.1.3.d Evaluate alternatives |
| 8.2.3 a) Activity: Stakeholder Needs and Requirements Definition V&V | 6.4.2 Stakeholder Needs and Requirements Definition Process | 6.4.1.3.b Define stakeholder needs<br>6.4.1.3. c Develop the operational concept and other life cycle concepts |

| IEEE 1012 V&V Activities (see corresponding clause) | ISO/IEC/IEEE 15288 system life cycle | |
|---|---|---|
| | **Process** | **Activity** |
| | | 6.4.1.3. d Transform stakeholder needs into stakeholder requirements<br>6.4.1.3. e Analyze stakeholder requirements |
| 8.3.3 a) Activity: System Requirements Definition V&V | 6.4.3 System Requirements Definition Process | 6.4.3.3.b Define system requirements<br>6.4.3.3.c Analyze system requirements |
| 8.4.3 a) Activity: Architecture Definition V&V | 6.4.4 Architecture Definition Process | 6.4.4.3.b Develop architecture viewpoints<br>6.4.4.3.c Develop models and views of candidate architectures<br>6.4.4.3.d Related the architecture to design<br>6.4.4.3.f Assess architecture candidates |
| 8.5.3 a) Design Definition V&V | 6.4.5 Design Definition Process | 6.4.5.3.b Establish design characteristics and design enablers related to each system element<br>6.4.5.3 d Manage the design |
| 8.6.3 a) System Analysis V&V | 6.4.6 System Analysis Process | 6.4.6.3.a Prepare for system analysis<br>6.4.6.3.b Perform system analysis |
| 8.7.3 a) Activity: Implementation V&V | 6.4.7 Implementation Process | 6.4.7.3.a Prepare for implementation<br>6.4.7.3.b Perform implementation |
| 8.8.3 a) Activity: Integration V&V | 6.4.8 Integration Process | 6.4.8.3.a Prepare for integration<br>6.4.8.3.b Perform integration—Successively integrate system element configurations until the complete system is synthesized |
| 7.1.3 a) Activity: V&V Management<br>8.1.3 a) Activity: Business or Mission Analysis Results Evaluation<br>8.2.3 a) Activity: Stakeholder Needs and Requirements Definition V&V<br>8.3.3 a) Activity: System Requirements Definition V&V<br>8.4.3 a) Activity: Architecture Definition V&V<br>8.5.3 a) Design Definition V&V<br>8.6.3 a) System Analysis V&V<br>8.7.3 a) Activity: Implementation V&V<br>8.8.3 a) Activity: Integration V&V | 6.4.9 Verification Process | 6.4.9.3.a Prepare for verification<br>6.4.9.3.b Perform verification<br>6.4.9.3.c Manage results of verification |
| 8.10.3 a) Activity: Transition V&V | 6.4.10 Transition Process | 6.4.10.3.a Prepare for the transition<br>6.4.10.3.b Perform the transition |
| 7.1.3 a) Activity: V&V Management<br>8.1.3 a) Activity: Business or Mission Analysis Results Evaluation<br>8.2.3 a) Activity: Stakeholder Needs and Requirements Definition V&V<br>8.3.3 a) Activity: System Requirements Definition V&V<br>8.4.3 a) Activity: Architecture Definition V&V<br>8.5.3 a) Design Definition V&V<br>8.6.3 a) System Analysis V&V<br>8.7.3 a) Activity: Implementation V&V<br>8.8.3 a) Activity: Integration V&V | 6.4.11 Validation Process | 6.4.11.3.a Prepare for validation<br>6.4.11.3.b Perform validation<br>6.4.11.3.c Manage results of validation |
| 8.12.3 a) Activity: Operation V&V | 6.4.12 Operation Process | 6.4.12.3.a Prepare for operation |

| IEEE 1012 V&V Activities (see corresponding clause) | ISO/IEC/IEEE 15288 system life cycle | |
|---|---|---|
| | Process | Activity |
| | | 6.4.12.3.b Perform operation |
| 8.13.3 a) Activity: Maintenance V&V | 6.4.13 Maintenance Process | 6.4.13.3.a Prepare for maintenance<br>6.4.13.3.b Perform maintenance |
| 8.14.3 a) Activity: Disposal V&V | 6.4.14 Disposal Process | 6.4.14.3.a Prepare for disposal<br>6.4.14.3.b Perform disposal |

## A.3 Mapping of ISO/IEC 12207 V&V activities to IEEE 1012 V&V activities and tasks

Table A.3 shows a mapping of all ISO/IEC 12207:2008 [B11] V&V activities to the V&V activities and tasks of this standard.

The first column of Table A.3 lists the clause numbers and titles of activities from ISO/IEC 12207:2008 [B11]. The second column of Table A.3 lists the clauses and tables from IEEE Std 1012 that map to the activities listed in the first column.

### Table A.3—Mapping ISO/IEC 12207 V&V requirements to IEEE 1012 V&V activities and tasks

| ISO/IEC 12207 V&V Requirements | IEEE 1012 V&V Activities and Tasks (see corresponding clause/table) |
|---|---|
| 6.1.1.3.5 Agreement monitoring | **7.2 Activity: Acquisition Support V&V**<br>Task 1 Scoping the V&V Effort<br>Task 2 Planning the Interface between the V&V Effort and Supplier<br>Task 3 System Requirements Review<br>Task 4 Acceptance Support |
| 6.1.2.3.4.5(h) and 6.1.2.3.4.10 Interfacing with V&V[a] | **7.2 Activity: Acquisition Support V&V**<br>Task 2 Planning the Interface between the V&V Effort and Supplier<br><br>**7.3 Activity: Supply Planning V&V**<br>Task 2 Planning the Interface between the V&V Effort and Supplier<br><br>**Annex C Definition of independent V&V (IV&V)** |
| 6.1.2.3.4.14 Verification and Validation[a] | Clause 1 through Clause 7, Clause 9, Clause 11, Clause 12, Table 1a, Table 1c, Table 2a, Table 2c, Table 3a, and Table 3c, Figure 1a, Figure 1c, Figure 2a, and Figure 2c, all annexes |
| 7.2.4.3.1 [Software Verification] Process implementation | **5. Integrity Levels**<br><br>**7.1 Activity: V&V Management**<br>Task 1 VVP Generation<br><br>**9.1 Activity: Software Concept V&V**<br>Task 2 Criticality Analysis<br><br>**9.2 Activity: Software Requirements V&V**<br>Task 4 Criticality Analysis<br><br>**9.3 Activity: Software Design V&V**<br>Task 4 Criticality Analysis<br><br>**9.4 Activity: Software Construction V&V**<br>Task 4 Criticality Analysis<br>**9.10 Activity: Software Maintenance V&V**<br>Task 3 Criticality Analysis<br><br>**Annex C** |

| ISO/IEC 12207 V&V Requirements | IEEE 1012 V&V Activities and Tasks (see corresponding clause/table) |
|---|---|
| 7.2.4.3.2.1 Requirements verification | **9.2 Activity: Software Requirements V&V** |
| 7.2.4.3.2.2 Design verification | **9.3 Activity: Software Design V&V** |
| 7.2.4.3.2.3 Code verification | **9.4 Activity: Software Construction V&V** |
| 7.2.4.3.2.4 Integration verification | **9.3 Activity: Software Design V&V**<br>Task 6 Software Integration Test Plan V&V<br>Task 8 Software Integration Test Design V&V<br><br>**9.4 Activity: Software Construction V&V**<br>Task 6 Software Integration Test Case V&V<br><br>**9.5 Activity: Software Integration Test V&V** |
| 7.2.4.3.2.5 Documentation verification | **7.5 Activity: Configuration Management V&V** |
| 7.2.5.3.1 [Software Validation] Process implementation | **5. Integrity Levels**<br><br>**7.1 Activity: V&V Management**<br>Task 1 VVP Generation<br><br>**9.1 Activity: Software Concept V&V**<br>Task 2 Criticality Analysis<br><br>**9.2 Activity: Software Requirements V&V**<br>Task 4 Criticality Analysis<br><br>**9.3 Activity: Software Design V&V**<br>Task 4 Criticality Analysis<br><br>**9.4 Activity: Software Construction V&V**<br>Task 4 Criticality Analysis<br><br>**9.10 Activity: Software Maintenance V&V**<br>Task 3 Criticality Analysis<br><br>**Annex C** |
| 7.2.5.3.2 Validation | **9.2 Activity: Software Requirements V&V**<br>Task 5 Software Qualification Test Plan V&V<br><br>**9.3 Activity: Software Design V&V**<br>Task 5 Software Component Test Plan V&V<br>Task 7 Software Component Test Design V&V<br>Task 9 Software Qualification Test Design V&V<br><br>**9.4 Activity: Software Construction V&V**<br>Task 5 Software Component Test Case V&V<br>Task 7 Software Qualification Test Case V&V<br>Task 9 Software Component Test Procedure V&V<br>Task 11 Software Qualification Test Procedure V&V<br>Task 12 Software Component Test Execution V&V<br><br>**9.6 Activity: Software Qualification Test V&V** |
| 7.2.6.3.2 Project Management Reviews | **7.1 Activity: V&V Management**<br>Task 5 Management and Technical Review Support |

[a] No ISO/IEC 12207:2008 [B11] clause title was listed. For purposes of this mapping, this standard assigned a clause title to reflect the clause contents.

## A.4 Mapping of IEEE 1012 V&V activities to ISO/IEC 12207 software life cycle processes and activities

This standard defines 5 Common V&V activities and 11 Software V&V activities, as shown in the first column of Table A.4, which are part of the V&V processes. These 16 V&V activities correspond to the ISO/IEC 12207 software life cycle processes and activities shown in columns two and three of Table A.4. For the 12207 Software Verification and Software Validation processes, the corresponding V&V activities are the activities of the process. For the other 12207 processes, correspondence indicates a V&V activity that evaluates the products produced or revised by the 12207 process.

**Table A.4—Mapping IEEE 1012 V&V activities to ISO/IEC 12207:2008 [B11]**

| IEEE 1012 V&V Activities (see corresponding clause) | ISO/IEC 12207 Software Life Cycle | |
|---|---|---|
| | Process | Activity |
| 7.2.3 a) Activity: Acquisition Support V&V | 6.1.1 Acquisition Process | 6.1.1.3 1 Acquisition preparation<br>6.1.1.3.4 Contract agreement<br>6.1.1.3.5 Agreement monitoring<br>6.1.1.3.6 Acquirer acceptance |
| 7.3.3 a) Activity: Supply Planning V&V | 6.1.2 Supply Process | 6.1.2.3.3 Contract agreement<br>6.1.2.3.4 Contract execution<br>6.1.2.3.5 Product/service delivery and support |
| 7.4.3 a) Activity: Project Planning V&V | 6.3.1 Project Planning Process | 6.3.1.3.2 Project planning |
| 7.5.3 a) Activity: Configuration Management V&V | 6.3.5 Configuration Management Process | 6.3.5.3.1 Configuration management planning<br>6.3.5.3.2 Configuration management execution |
| 9.2.3 a) Activity: Software Requirements V&V | 7.1.2 Software Requirements Analysis Process | 7.1.2.3.1 Software requirements analysis |
| 9.3.3 a) Activity: Software Design V&V | 7.1.3 Software Architectural Design Process<br>7.1.4 Software Detailed Design Process | 7.1.3.3.1 Software architectural design<br>7.1.4.3.1 Software detailed design |
| 9.4.3 a) Activity: Software Construction V&V | 7.1.5 Software Construction Process | 7.1.5.3.1 Software construction |
| 9.5.3 a) Activity: Software Integration Test V&V | 7.1.6 Software Integration Process | 7.1.6.3.1 Software integration |
| 9.6.3 a) Activity: Software Qualification Test V&V | 7.1.7 Software Qualification Testing Process | 7.1.7.3.1 Software qualification testing |
| 9.7.3 a) Activity: Software Acceptance Test V&V | 6.4.8 Software Acceptance Support Process | 6.4.8.3.1 Software acceptance support |
| 7.1.3 a) Activity: V&V Management<br>9.1.3 a) Activity: Software Concept V&V<br>9.2.3 a) Activity: Software Requirements V&V<br>9.3.3 a) Activity: Software Design V&V<br>9.4.3 a) Activity: Software Construction V&V<br>9.5.3 a) Activity: Software Integration Test V&V<br>9.6.3 a) Activity: Software Qualification Test V&V<br>9.7.3 a) Activity: Software Acceptance Test V&V | 7.2.4 Software Verification Process | 7.2.4.3.1 Process implementation<br>7.2.4.3.2 Verification |

| IEEE 1012 V&V Activities (see corresponding clause) | ISO/IEC 12207 Software Life Cycle | |
|---|---|---|
| | **Process** | **Activity** |
| 9.9.3 a) Activity: Software Installation and Checkout V&V | 6.4.7 Software Installation Process | 6.4.7.3.1 Software installation |
| 7.1.3 a) Activity: V&V Management<br>9.1.3 a) Activity: Software Concept V&V<br>9.2.3 a) Activity: Software Requirements V&V<br>9.3.3 a) Activity: Software Design V&V<br>9.4.3 a) Activity: Software Construction V&V<br>9.5.3 a) Activity: Software Integration Test V&V<br>9.6.3 a) Activity: Software Qualification Test V&V<br>9.7.3 a) Activity: Software Acceptance Test V&V | 7.2.5 Software Validation Process | 7.2.5.3.1 Process implementation<br>7.2.5.3.2 Verification |
| 9.11.3 a) Activity: Software Operation V&V | 6.4.9 Software Operation Process | 6.4.9.3.1 Preparation for operation<br>6.4.9.3.2 Operation activation and check-out<br>6.4.9.3.3 Operational use |
| 9.12.3 a) Activity: Software Maintenance V&V | 6.4.10 Software Maintenance Process | 6.4.10.3.1 Process implementation<br>6.4.10.3.2 Problem and modification analysis<br>6.4.10.3.3 Modification implementation<br>6.4.10.3.4 Maintenance review/acceptance<br>6.4.10.3.5 Migration |
| 9.13.3 a) Activity: Software Disposal V&V | 6.4.11 Software Disposal Process | 6.4.11.3.1 Software disposal planning |

# Annex B

(informative)

# A risk-based integrity level schema

Table B.1 defines four integrity levels used for reference purposes by this standard. Table B.2 describes the consequences of errors for each of the four integrity levels. There are overlaps between the integrity levels to allow for individual interpretations of acceptable risk depending on the application.

**Table B.1—Assignment of integrity levels**

| Integrity level | Description |
|---|---|
| 4 | Behavior of the system, in combination with its environment, causes the following:<br>— Catastrophic consequences for which the likelihood of the behavior occurring is at most occasional<br>or<br>— Critical consequences for which the likelihood of the behavior occurring is at most probable |
| 3 | Behavior of the system, in combination with its environment, causes the following:<br>— Catastrophic consequences for which the likelihood of the behavior occurring is at most infrequent<br>or<br>— Critical consequences for which the likelihood of the behavior occurring is at most occasional<br>or<br>— Marginal consequences for which the likelihood of the behavior occurring is at most probable |
| 2 | Behavior of the system, in combination with its environment, causes the following:<br>— Critical consequences for which the likelihood of the behavior occurring is at most infrequent<br>or<br>— Marginal consequences for which the likelihood of the behavior occurring is at most probably<br>or<br>— Negligible consequences for which the likelihood of the behavior occurring is at most reasonable |
| 1 | Behavior of the system, in combination with its environment, causes the following:<br>— Critical consequences for which the likelihood of the behavior occurring is at most infrequent<br>or<br>— Marginal consequences for which the likelihood of the behavior occurring is at most occasional<br>or<br>— Negligible consequences for which the likelihood of the behavior occurring is at most probable |

**Table B.2—Definition of consequences**

| Consequence | Definition |
|---|---|
| Catastrophic | Loss of human life, complete mission failure, loss of system security and safety, or extensive financial or social loss. |
| Critical | Major and permanent injury, partial loss of mission, major system damage, or major financial or social loss. |
| Marginal | Severe injury or illness, degradation of secondary mission, or some financial or social loss. |
| Negligible | Minor injury or illness, minor impact on system performance, or operator inconvenience. |

Table B.3 illustrates the risk-based schema shown in Table B.1 and Table B.2. Each cell in the table assigns an integrity level based on the combination of an error consequence and the likelihood of occurrence of an operating state that contributes to the error. Some table cells reflect more than one integrity level, indicating that the final assignment of the integrity level can be selected to address the system application and risk mitigation recommendations. For some industry applications, the definition of likelihood of occurrence categories may be expressed as probability figures derived by analysis or from system requirements.

**Table B.3—Graphic illustration of the assignment of integrity levels**

| **Error** | **Likelihood of occurrence of an operating state that contributes to the error (decreasing order of likelihood)** | | | |
|---|---|---|---|---|
| **Consequence** | **Reasonable** | **Probable** | **Occasional** | **Infrequent** |
| Catastrophic | 4 | 4 | 4 or 3 | 3 |
| Critical | 4 | 4 or 3 | 3 | 2 or 1 |
| Marginal | 3 | 3 or 2 | 2 or 1 | 1 |
| Negligible | 2 | 2 or 1 | 1 | 1 |

# Annex C

# (informative)

# Definition of independent verification and validation (IV&V)

## C.1 Independence parameters

### C.1.1 Introduction

Independent V&V (IV&V) is defined by three parameters: technical independence, managerial independence, and financial independence.

### C.1.2 Technical independence

Technical independence requires the V&V effort to use personnel who are not involved in the development of the system or its elements. The IV&V effort should formulate its own understanding of the problem and how the proposed system is solving the problem. Technical independence ("fresh viewpoint") is an important method to detect subtle errors overlooked by those too close to the solution.

For system tools, technical independence means that the IV&V effort uses or develops its own set of test and analysis tools separate from the developer's tools. Sharing of tools is allowable for computer support environments (e.g., compilers, assemblers, and utilities) or for system simulations where an independent version would be too costly. For shared tools, IV&V conducts qualification tests on tools to assure that the common tools do not contain errors that may mask errors in the system being analyzed and tested. Off-the-shelf tools that have extensive history of use do not require qualification testing. The most important aspect for the use of these tools is to verify the input data used.

### C.1.3 Managerial independence

This requires that the responsibility for the IV&V effort be vested in an organization separate from the development and program management organizations. Managerial independence also means that the IV&V effort independently selects the segments of the software, hardware, and system to analyze and test, chooses the IV&V techniques, defines the schedule of IV&V activities, and selects the specific technical issues and problems to act on. The IV&V effort provides its findings in a timely fashion simultaneously to both the development and program management organizations. The IV&V effort is allowed to submit to program management the IV&V results, anomalies, and findings without any restrictions (e.g., without requiring prior approval from the development group) or adverse pressures, direct or indirect, from the development group.

### C.1.4 Financial independence

This requires that control of the IV&V budget be vested in an organization independent of the development organization. This independence prevents situations where the IV&V effort cannot complete its analysis or test or deliver timely results because funds have been diverted or adverse financial pressures or influences have been exerted.

## C.2 Forms of independence

### C.2.1 Introduction

The extent to which each of the three independence parameters (technical, managerial, and financial) is vested in a V&V effort determines the degree of independence achieved.

Many forms of independence can be adopted for a V&V effort. The five most prevalent are as follows: 1) classical, 2) modified, 3) integrated, 4) internal, and 5) embedded. Table C.1 illustrates the degree of independence achieved by these five forms.

**Table C.1—Forms of IV&V**

| IV&V form | Technical | Management | Financial |
|---|---|---|---|
| Classical | I | I | I |
| Modified | I | i | I |
| Integrated | i | I | I |
| Internal | i | i | i |
| Embedded | e | e | e |

NOTE—I = rigorous independence; i = conditional independence; e = minimal independence.

### C.2.2 Classical IV&V

Classical IV&V embodies all three independence parameters. The IV&V responsibility is vested in an organization that is separate from the development organization. The IV&V effort establishes a close working relationship with the development organization to assure that IV&V findings and recommendations are integrated rapidly back into the development process. Typically, classical IV&V is performed by one organization (e.g., supplier) and the development is performed by a separate organization (i.e., another vendor). Classical IV&V is generally required for integrity level 4 (i.e., loss of life, loss of mission, significant social loss, or financial loss) through regulations and standards imposed on the system development.

### C.2.3 Modified IV&V

Modified IV&V is used in many large programs where the system prime integrator is selected to manage the entire system development including the IV&V. The prime integrator selects organizations to assist in the development of the system and to perform the IV&V. In the modified IV&V form, the acquirer reduces its own acquisition time by passing this responsibility to the prime integrator. Because the prime integrator performs all or some of the development, the managerial independence is compromised by having the IV&V effort report to the prime integrator. Technical independence is preserved because the IV&V effort formulates an unbiased opinion of the system solution and uses an independent staff to perform the IV&V. Financial independence is preserved because a separate budget is set aside for the IV&V effort. Modified IV&V effort would be appropriate for systems with integrity level 3 (i.e., an important mission and purpose).

### C.2.4 Integrated IV&V

This form is focused on providing rapid feedback of V&V results into the development process and is performed by an organization that is financially and managerially independent of the development organization to minimize compromises with respect to independence. The rapid feedback of V&V results into the development process is facilitated by the integrated IV&V effort: working side by side with the development organization, reviewing interim work products, and providing V&V feedback during inspections, walkthroughs, and reviews conducted by the development staff (potential impact on technical independence). Impacts to technical independence are counterbalanced by benefits associated with a focus on interdependence between the integrated IV&V effort and the development organization. Interdependence means that the successes of the organizations are closely coupled, ensuring that they work together in a cooperative fashion.

### C.2.5 Internal IV&V

Internal IV&V exists when the developer conducts the IV&V with personnel from within its own organization, although preferably not the same personnel involved directly in the development effort. Technical, managerial, and financial independence are compromised. Technical independence is compromised because the IV&V analysis and test is vulnerable to overlooking errors by using the same assumptions or development environment that masked the error from the developers. Managerial independence is compromised because the internal IV&V effort uses the same common tools and corporate analysis procedures as the development group. Peer pressure from the development group may adversely influence how aggressively the system is analyzed and tested by the IV&V effort. Financial independence is compromised because the development group controls the IV&V budget. IV&V funds, resources, and schedules may be reduced as development pressures and needs redirect the IV&V funds into solving development problems. The benefit of an internal IV&V effort is access to staff who know the system and its software. This form of IV&V is used when the degree of independence is not explicitly stated and the benefits of preexisting staff knowledge outweigh the benefits of objectivity.

### C.2.6 Embedded V&V

This form is similar to internal IV&V in that it uses personnel from the development organization who should not be involved directly in the development effort. Embedded V&V is focused on ensuring conformance to the development procedures and processes. The embedded V&V effort works side by side with the development organization and attends the same inspections, walkthroughs, and reviews as the development staff (i.e., compromise of technical independence). Embedded V&V is not tasked specifically to assess independently the original solution or conduct independent tests (i.e., compromise of managerial independence). Financial independence is compromised because the V&V staff resource assignments are controlled by the development group. Embedded V&V allows rapid feedback of V&V results into the development process, but compromises the technical, managerial, and financial independence of the V&V effort.

# Annex D

(informative)

# V&V of reuse software

## D.1 Purpose

The purpose of this annex is to provide options and suggestions to aid verification and validation of reuse software. Reuse software can take many forms and could include software from software libraries, custom software developed for other applications, COTS software, software requirements, software designs, or other artifacts from existing software. This annex addresses both 1) reuse software developed and used as part of a reuse process, and 2) reuse software developed and used outside of a reuse process. Figure D.1 illustrates V&V activities and tasks for reuse software whether it was developed under a reuse process or outside of a reuse process.

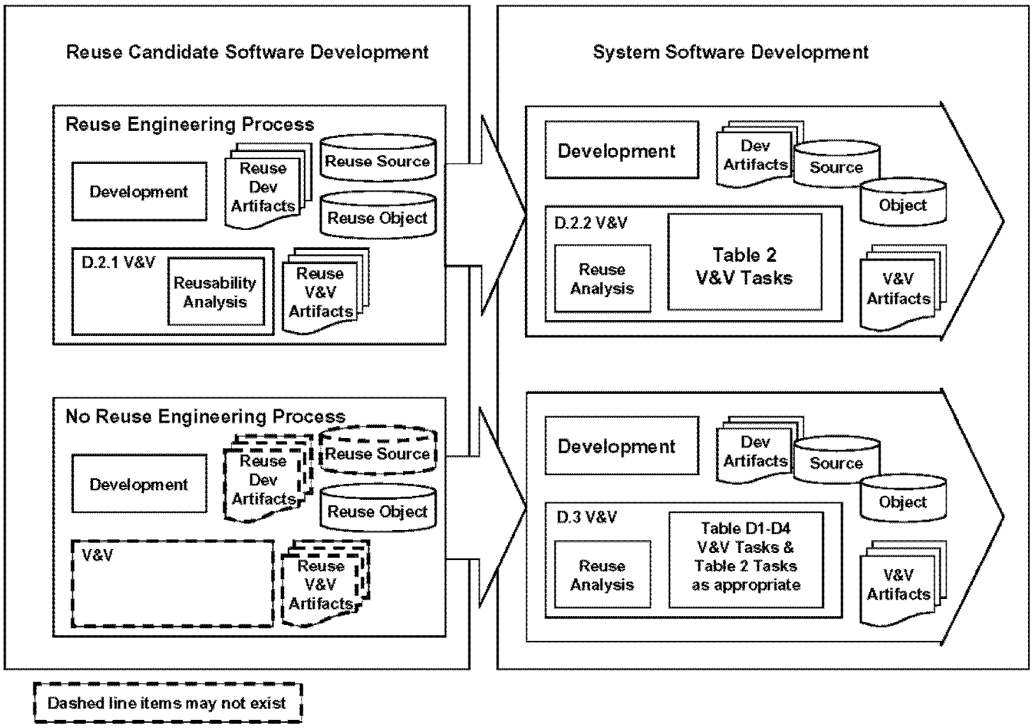



**Figure D.1—V&V of reuse software**

## D.2 V&V of software developed in a reuse process

### D.2.1 Introduction

A structured software reuse process develops assets (e.g., design, code, and documentation) intended for use in multiple contexts. The software reuse processes of IEEE Std 1517-2010 [B10] provide a framework for extending the software life cycle processes of ISO/IEC 12207:2008 [B11] to include a systematic domain engineering process for software reuse. The domain scope and the domain analysis of an asset provide the requirements, the intended use, the interface parameters, and other information necessary for V&V of the asset, or an understanding of previously performed V&V of the asset.

### D.2.2 V&V of assets in development

The V&V effort should analyze the artifacts (e.g., plans, models, and architecture) of the domain engineering as part of the required V&V tasks. Significant analysis of the domain engineering products should occur during system requirements review, software requirements evaluation, interface analysis, software design evaluation, source code and source code documentation evaluation, and all test planning. The V&V effort includes the assignment of an integrity level to the asset, in the context of the domain for its intended use, to determine the minimum V&V tasks to be performed (see Table 2). When planning the V&V effort, the optional task reusability analysis (see Annex G) should be included.

### D.2.3 V&V of reused assets

A domain engineering process assures that the information used in developing software systems is identified, captured, and organized so that it can be reused to create new systems within a domain. The V&V effort includes the assignment of an integrity level to the asset, in the context of its actual use, to determine the minimum V&V tasks to be performed (see Table 2). When planning the V&V effort, the optional task reuse analysis (see Annex G) should be included.

## D.3 V&V of software developed and reused outside of a reuse process

Some software systems are developed, operated, and maintained using software items that were not designed for use in multiple contexts or were not developed as part of a structured software reuse process (e.g., domain engineering products are not available). In these cases, the V&V effort should perform the optional task reuse analysis (see Annex G) to produce inputs for determining the suitability of the reuse candidate software. The V&V effort assigns an integrity level to the reuse candidate software to determine the minimum V&V tasks to be performed.

Reused software requires special consideration during the V&V effort when any one of the following is applicable:

- The inputs for a required V&V task are not available for the reused software.
- The reused software was developed as part of a system that is different in function or application from the system where it will be reused.
- The reused software was developed to meet different user needs from the current system.
- The original user needs are unknown.

In some cases, inputs for the V&V tasks may not be available, reducing visibility into the software products and processes. Options and techniques are available to compensate for the lack of inputs. Each technique has varying strengths and weaknesses—consideration should be given to performing multiple techniques to counter the weaknesses of one technique with strengths of another technique when high confidence is demanded. These options are addressed in decreasing order of desirability.

First, substitute tasks. Substitution for Table 1a through Table 1d V&V tasks is permitted if equivalent substitute V&V tasks can be shown to satisfy the same criteria as in Table 1. Two substitution task techniques are suggested in Table D.1.

**Table D.1—Substitution tasks to establish V&V task inputs**

<table>
<tr><td colspan="2">Substitution Tasks<br><br>Description: Substitute alternative analysis and test methods in lieu of the IEEE 1012 requirement V&V tasks to generate objective conclusions about the correctness, completeness, accuracy, and usability of the reused software.</td></tr>
<tr><td rowspan="2">Technique 1: Black box testing<br><br>Black box testing and validation: Execute the reused software against a spectrum of test case inputs and validate the correctness of the output.<br><br>User's manual analysis: Derive system and software requirements from the user's manual and validate that the black box testing results satisfy the requirements.<br><br>Limit checks in interfacing software: Add limit checks within all interface software on all data and logical information received from the reused software to assure that no erroneous information is accepted.</td><td>Pros<br>— Test results reflect actual target software<br>— Limits catastrophic errors from propagating into interfacing systems<br>— Ability to check the major system and user requirements derived from user's manual<br>— Independent analysis</td></tr>
<tr><td>Cons<br>— Inability to detect all test errors if presence of error not observable in black box outputs (e.g., latent errors)<br>— Limit checks difficult to cover all execution scenarios<br>— Limited by the thoroughness of the user's manual</td></tr>
<tr><td rowspan="2">Technique 2: Review developer's quality assurance (QA)<br><br>Developer's QA results: Review developer's QA results and confirm the evidence of data similar to those that would be generated from V&V tasks.<br><br>Developer's test results: Review the developer's test results and confirm the evidence of data similar to those that would be generated from V&V tasks.<br><br>Review of developer's notebook: Review the developer's notebook to derive additional insights and problems with the software during early stages of development.<br><br>User's manual analysis: Derive system and software requirements from the user's manual and validate that the developer's QA and test results satisfy the requirements.</td><td>Pros<br>— Ability to derive insight into the details of the software design and internal performance characteristics<br>— Identification of possible program error characteristics warranting further analysis and testing by other methods<br>— Observations of program performance using test results reflecting actual software execution characteristics</td></tr>
<tr><td>Cons<br>— Limited by the scope and extent of the QA analysis and the specific focus of the testing performed<br>— Limited by the thoroughness of the user's manual<br>— Not a totally independent analysis</td></tr>
</table>

Second, use alternative sources of information to perform the V&V tasks in Table 1a through Table 1d and Table 2a through Table 2d of this standard. Three alternative source techniques are suggested in Table D.2.

**Table D.2—Alternative sources to establish V&V task inputs**

| **Alternative sources**<br><br>**Description:** Use alternative sources of program data to derive conclusions about the correctness, completeness, accuracy, and usability of the reused software. | |
|---|---|
| **Technique 3: Operational history**<br><br>*Historical data analysis*: Examine and analyze the operational history of the reused software with particular attention to how the software performed in a system with similar characteristics to the new system being proposed.<br><br>*User interviews*: Conduct interviews with operational users. Focus data gathering on how the system performed in scenarios and conditions similar to those expected in the new system being proposed. | Pros<br>— Real data of the reused software in an operational environment.<br>— User observations about the performance of the software and its related system.<br>— Software burn-in established and track record of discrepancies recorded.<br>— Independent analysis.<br><br>Cons<br>— Different characteristics, technologies, and user interfaces with new proposed system could cause error not observed in historical system.<br>— Not all interactions recordable or observable in historical systems, so data completeness and accuracy are limited.<br>— User observations can be subjective, biased, and error prone, so correctness, completeness, and accuracy may be limited. |
| **Technique 4: Audit results**<br><br>*Developer's interview*: Conduct interviews with development team to extract pertinent information about the design and performance characteristics of the reused software.<br><br>*Design walkthrough review analysis*: Analyze the design and code walkthrough data to determine how the reused software would interact in the new proposed system.<br><br>*Standard compliance analysis*: Review the results of any standards compliance audits to determine that the proper software standards were followed in the construction of the reused software. | Pros<br>— Depending on the thoroughness of the development team's records, good insight into the design and code approaches can be obtained from the interviews.<br>— Historical artifacts of design and code walkthroughs may be of sufficient quality to act as a substitute of the actual source code and design details.<br><br>Cons<br>— Limited by the thoroughness of the development team's documentation and recollection during interviews.<br>— Not a totally independent analysis. |
| **Technique 5: Artifacts**<br><br>*Product documentation analysis*: Review any product documentation to derive artifacts similar to requirements, design, and code (if possible—for example, if a pseudo design language is used).<br><br>*Prior V&V results analysis*: Analyze any prior V&V results and develop inferences and extrapolation of the data to the new proposed system. | Pros<br>— Uses actual artifacts representing some form of the reused software.<br>— Prior V&V results for an initial basis for formulating additional analysis and testing to conduct to fill in the analysis and testing voids caused by lack of program documentation.<br>— Independent analysis.<br><br>Cons<br>— Overstating a conclusion without having a solid basis for knowing the system conditions could lead to faulty conclusions about the suitability in the new proposed system and its different system conditions.<br>— Limited by the thoroughness of the product documentation. |

Third, use reverse engineering to generate inputs to perform the V&V tasks in Table 1a through Table 1d and Table 2a through Table 2d of this standard. One reverse engineering technique is suggested in Table D.3.

### Table D.3—Reverse engineering to establish V&V task inputs

<table>
<tr><td colspan="2">Reverse engineering<br><br>Description: Reverse engineer requirements, design, and code data to generate objective conclusions about the correctness, completeness, accuracy, and usability of the reused software.</td></tr>
<tr><td rowspan="2">Technique 6: Black box testing<br><br>Reverse engineer source code: Reverse compile “pseudo source” code from the program object file. Analyze the reverse compiled pseudo code using normal V&V procedures including all the V&V test strategies and methods.<br><br>Reverse engineer requirements: Derive the system and software requirements from the user’s manual. Analyze the requirements using the IEEE 1012 V&V tasks and test the reused software against these reverse engineered requirements.</td><td>Pros<br>— Uses the actual code—no hidden or implied data.<br>— Perform all of the IEEE 1012 V&V tasks.<br>— Test data reflects actual performance of the reused software under the system conditions of the new proposed system.<br>— Independent analysis.</td></tr>
<tr><td>Cons<br>— Time consuming to reverse engineer data.<br>— Pseudocode hard to read.</td></tr>
</table>

Fourth, use independent prototyping and comparison of performance results with those of the reuse asset to perform the V&V tasks in Table 1a through Table 1d and Table 2a through Table 2d of this standard. Two independent prototyping and comparison techniques are suggested in Table D.4.

### Table D.4—Independent prototyping and comparison to establish V&V task inputs

<table>
<tr><td colspan="2">Independent prototyping and comparison<br><br>Description: Develop a model (prototype) of the proposed software or use portions of the prior system.<br><br>Execute test scenarios on the prototype or prior system and compare the test results against the reused software. Analyze the results to generate objective conclusions about the correctness, completeness, accuracy, and usability of the reused software.</td></tr>
<tr><td rowspan="2">Technique 7: Prototyping<br><br>Comparison of prototype code: Develop a replication model (prototype) of the function or requirements in a user-friendly language. Execute test cases representing the range of system scenarios on both the model and reuse software. Compare the results and analyze the differences to determine whether the reused software is performing as intended.</td><td>Pros<br>— Useful for small functions and sets of requirements.<br>— Easy to diagnose problems in the reused software.<br>— Ability to run a wide range of system scenarios and compare against a benchmark program.<br>— Independent analysis.</td></tr>
<tr><td>Cons<br>— Cost and time of building the model.<br>— Errors in the model can mask similar errors in the reused software (likelihood of two similar errors generated by two independent sources should be small or unlikely).</td></tr>
<tr><td rowspan="2">Technique 8: Prior system results<br><br>Comparison with prior system/function: Execute test cases representing the range of system scenarios on the prior system/function and the reused software. Compare the results and analyze the differences to determine whether the reused software is performing as intended.</td><td>Pros<br>— Inexpensive to execute test cases on prior system and compare.<br>— Proven track record of performance of the prior system/function establishes a performance baseline.<br>— Differences in execution results leads to other analysis and testing to be conducted.<br>— Independent analysis.</td></tr>
<tr><td>Cons<br>— Limited in scope to smaller functions.<br>— Ability to instrument prior system/function to extract diagnosis data about interim program steps may be difficult and make it harder to diagnose exact location of a problem.<br>— Any problems hidden in the prior system/function may go undetected or untested in the new proposed system/function (inheritance of errors).</td></tr>
</table>

Last, use a combination of the following circumstantial evidence to provide visibility and insight into the reused software to perform the V&V tasks in Table 1a through Table 1d and Table 2a through Table 2d of this standard:

a) Operational history

b) Test history

c) Audit results

d) User interviews

e) Engineering judgment

f) Product documentation

g) Prior hazard analysis results

h) Prior V&V results

i) Software developer's notebook

j) Design process documentation

k) Original developers' interviews

l) Static code analysis results

m) Standards compliance assessments

If V&V of reused software cannot be accomplished at the appropriate level, then the items may be used, as long as the risk associated with this use is recognized and accounted for in the risk mitigation strategy. The V&V effort should assure that the risks are thoroughly understood, properly documented, and properly tracked under the risk analysis tasks.

# Annex E

(informative)

# Verification and validation (V&V) measures

## E.1 Introduction

The management of V&V activity uses measures to provide feedback for the continuous improvement of the V&V processes and to evaluate the system development processes and products. Trends can be identified and addressed by computing evaluation measures over a period of time. Threshold values of measures should be established and trends should be evaluated to serve as indicators as to whether a process, product, or V&V task has been satisfactorily accomplished. No standard set of measures is applicable for all projects, so the use of measures may vary according to the application domain and software development environment.

No consensus exists on measures for evaluating the quality and coverage of the V&V tasks. IEEE Std 1061™-1998 [B8] provides a standard definition of the available software quality measures. Another measure-related standard is IEEE Std 982.1-2005 [B4].

This standard considers three categories of measures associated with the V&V effort: 1) measures for evaluating anomaly density, 2) measures for assessing V&V effectiveness, and 3) measures for evaluating V&V efficiency.

## E.2 Measures for evaluating anomaly density

Anomaly density measures can provide insightful information on the product quality, the quality of the system development processes, and the quality of the V&V effort to discover anomalies in the system/software/hardware and to facilitate correction of the anomalies. Anomaly density measures are influenced by numerous variables (e.g., software complexity, hardware complexity, type of domain, and time-phase application of the V&V processes); consequently, the measures are analyzed to gain insight into the interdependencies between the development efforts and the V&V efforts.

If the V&V anomaly density measure value is low, then this suggests that the program development quality is high, that the V&V processes need to be improved, or a combination of both. If the measure value is high, then this suggests that the program development quality is low, that the V&V processes are effective, or a combination of both. Regardless of the measure value, the next step is to evaluate related program development measures to clarify and discern the measure trends to determine the need for process improvements.

Anomaly measures and trends can be used to improve the quality of the current project and can be used to improve the planning and execution of V&V processes for future projects with similar characteristics. The measures defined by Equation (E.1) through Equation (E.4) are applicable for four system life cycle phases:

$$\text{Requirements anomaly density} = \frac{\text{\# Requirements anomalies found by V\&V effort}}{\text{\# Requirements reviewed by V\&V effort}} \quad \text{(E.1)}$$

$$\text{Design anomaly density} = \frac{\text{\# Design statement anomalies found by V\&V effort}}{\text{\# Design statements reviewed by V\&V effort}} \quad \text{(E.2)}$$

$$\text{Implementation anomaly density} = \frac{\text{\# Implementation anomalies found by V\&V effort}}{\text{\# Implementation volume reviewed by V\&V effort}} \quad \text{(E.3)}$$

$$\text{Test anomaly density} = \frac{\text{\# Test anomalies found by V\&V effort}}{\text{\# Tests reviewed by V\&V effort}} \quad \text{(E.4)}$$

## E.3 Measures for evaluating V&V effectiveness

Measures associated with V&V effort effectiveness provide quantitative indications that characterize the added benefits of V&V to discover anomalies in system products and processes. These measures delineate the percentage of the total anomalies found by the V&V effort. The measures are influenced by numerous variables (e.g., complexity), and the measures are analyzed to gain insight into the interdependencies between the development efforts and the V&V efforts.

The V&V effectiveness measure values are highly influenced by the degree of parallelism between the software development effort and the V&V effort. Assuming that the efforts are parallel, a low V&V effectiveness measure value suggests that the development effort is effective, or that the V&V effort may require improvement, or a combination of both. If the V&V effectiveness measure value is high, then this suggests that the development processes may require improvement, or that the V&V processes are effective, or that only incremental changes to the V&V processes may be required. Regardless of the measure value, the next step is to evaluate related system development measures to further clarify and discern the measure trends to determine the need for process improvements. The measures defined by Equation (E.5) through Equation (E.8) are applicable for four system life cycle phases.

$$\text{Requirements V\&V effectiveness} = \frac{\text{\# Requirements anomalies found by V\&V effort}}{\text{\# Requirements anomalies found by all sources}} \quad \text{(E.5)}$$

$$\text{Design V\&V effectiveness} = \frac{\text{\# Design statement anomalies found by V\&V effort}}{\text{\# Design statements anomalies found by all sources}} \quad \text{(E.6)}$$

$$\text{Implementation V\&V effectiveness} = \frac{\text{\# Implementation anomalies found by V\&V effort}}{\text{\# Implementation anomalies found by all sources}} \quad \text{(E.7)}$$

$$\text{Test V\&V effectiveness} = \frac{\text{\# Test anomalies found by V\&V effort}}{\text{\# Test anomalies found by all sources}} \quad \text{(E.8)}$$

## E.4 Measures for evaluating V&V efficiency

The measures associated with V&V effort efficiency provide data that characterize the capability of the V&V effort to discover anomalies in software products and processes in the development activity in which they are injected. Maximum benefits are realized when anomalies are discovered as early as possible in the development life cycle, thereby minimizing rework and development costs. Analysis of these measures, the anomalies, and the causal factors that prevented discovery of the anomaly in the phase in which it was injected can reveal needed improvements in methods, processes, tools, and skills to improve the overall V&V effort.

A low V&V efficiency measure value suggests that the V&V effort is not discovering anomalies in the earliest possible activity, or that the development products are immature, or a combination of both. If the V&V efficiency measure value is high, then this suggests that the V&V effort is discovering anomalies in

the earliest possible activity, or that the development products are mature, or a combination of both. Regardless of the measure value, the next step is to evaluate related system program development measures to further clarify and discern the measure trends to determine the need for process improvements. The measures defined by Equation (E.9) through Equation (E.12) are applicable for four system life cycle phases.

$$\text{Requirements V\&V effectiveness} = \frac{\text{\# Requirements anomalies found by V\&V in requirements activities}}{\text{\# Requirements anomalies found by V\&V in all activities}} \times 100\% \quad \text{(E.9)}$$

$$\text{Design V\&V effectiveness} = \frac{\text{\# Design statement anomalies found by V\&V in design activities}}{\text{\# Design statements anomalies found by V\&V in all activities}} \times 100\% \quad \text{(E.10)}$$

$$\text{Implementation V\&V effectiveness} = \frac{\text{\# Implementation anomalies found by V\&V in implementation activities}}{\text{\# Implementation anomalies found by V\&V in all activities}} \times 100\% \quad \text{(E.11)}$$

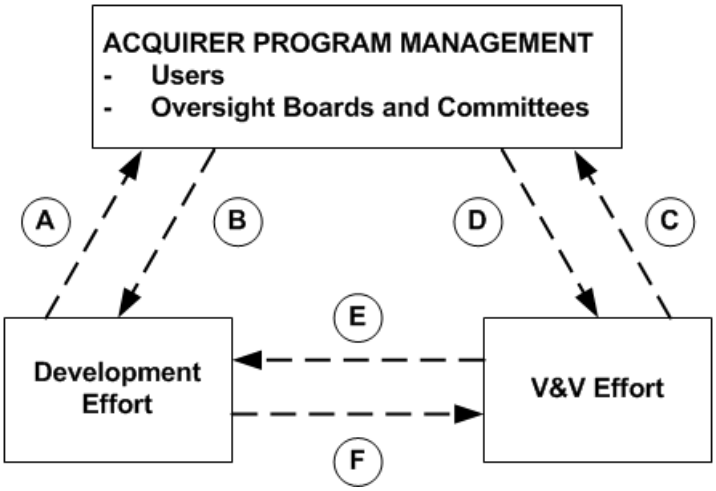
$$\text{Test V\&V effectiveness} = \frac{\text{\# Test anomalies found by V\&V in test activities}}{\text{\# Test anomalies found by V\&V in all activities}} \times 100\% \quad \text{(E.12)}$$

# Annex F

(informative)

## Example of verification and validation (V&V) relationships to other project responsibilities

Figure F.1 provides an example of relationships among the V&V team, the acquirer, and the supplier, and it identifies the information and data flows throughout the V&V effort. Many other relationships will work well as long as the project responsibilities, data flows, and reporting flows are defined and documented.




NOTE—The lines in Figure F.1 represent the flow of control and data as follows:

a) Submittal of program documentation (e.g., concept, requirements, design, and user manuals), source code, program status, program budgets, and developmental plans and schedules.
b) Approval, denial, and recommendations on development issues and deliverables listed in a).
c) Submittal of verification and validation plan (VVP), V&V task results, anomaly reports, activity reports, and other special reports.
d) Approval, denial, and recommendations on V&V issues and deliverables listed in c).
e) Submittal of V&V task results, anomaly reports, activity reports, and special reports as directed by the acquirer program management.
f) Submittal of program documentation (e.g., concept, requirements, design, user manuals, special reports, source code, and program schedules).

**Figure F.1—Relationship of V&V to other project responsibilities**

# Annex G

(informative)

# Optional verification and validation (V&V) tasks

*Algorithm analysis.* Verify the correct implementation of algorithms, equations, mathematical formulations, or expressions. Re-derive any significant algorithms and equations from basic principles and theories. Compare against established references or proven historical data. Validate the algorithms, equations, mathematical formulations, or expressions with respect to the system and software requirements. Assure that the algorithms and equations are appropriate for the problem solution. Validate the correctness of any constraints or limitations, such as rounding, truncation, expression simplifications, best-fit estimations, and nonlinear solutions imposed by the algorithms and equations.

*Audit performance.* Provide an independent assessment of whether a software process and its products conform to applicable regulations, standards, plans, procedures, specifications, and guidelines. Audits may be applied to any software process or product at any development stage. Audits may be initiated by the supplier, the acquirer, the developer, or other involved party such as a regulatory agency. The initiator of the audit selects the audit team and determines the degree of independence required. The initiator of the audit and the audit team leader establish the purpose, scope, plan, and reporting requirements for the audit.

The auditors collect sufficient evidence to decide whether the software processes and products meet the evaluation criteria. They identify major deviations; assess risk to quality, schedule, and cost; and report their findings. Examples of processes that could be audited include configuration management practices, use of software tools, degree of integration of the various software engineering disciplines particularly in developing an architecture, security issues, training, and project management.

*Audit support.* Provide technical expertise to the auditors on request. They may represent the acquirer at audit proceedings and may assist in the V&V of remedial activities identified by the audit.

*Control flow analysis.* Assess the correctness of the software by diagramming the logical control. Examine the flow of the logic to identify missing, incomplete, or inaccurate requirements. Validate whether the flow of control among the functions represents a correct solution to the problem.

*Cost analysis.* Evaluate the cost status of the development processes. Compare budgeted costs against actual costs. Correlate cost expenditures with technical status and schedule progress. Identify program risks if actual costs indicate behind schedule and over cost estimates.

*Database analysis.* Evaluation of database design as part of a design review process could include the following:

- Physical limitations analysis. Identify the physical limitations of the database, such as maximum number of records, maximum record length, largest numeric value, smallest numeric value, and maximum array length in a data structure and compare them to designed values.
- Index versus storage analysis. Analyze the use of multiple indexes compared to the volume of stored data to determine whether the proposed approach meets the requirements for data retrieval performance and size constraints.
- Data structures analysis. Some database management systems have specific data structures within a record, such as arrays, tables, and date formats. Review the use of these structures for potential impact on requirements for data storage and retrieval.

— Backup and disaster recovery analysis. Review the methods employed for backup against the requirements for data recovery and system disaster recovery, and identify deficiencies.

*Data flow analysis.* Evaluation of data flow diagrams as part of a design review process could include the following:

— Symbology consistency check. The various methods used to depict data flow diagrams employ very specific symbology to represent the actions performed. Verify that each symbol is used consistently.

— Flow balancing. Compare the output data from each process to the data inputs and the data derived within the process to assure the data are available when required. This process does not specifically examine timing or sequence considerations.

— Confirmation of derived data. Examine the data derived within a process for correctness and format. Data designed to be entered into a process by operator action should be confirmed to assure availability.

— Keys to index comparison. Compare the data keys used to retrieve data from data stores within a process to the database index design to confirm that no invalid keys have been used and the uniqueness properties are consistent.

*Disaster recovery plan assessment.* Verify that the disaster recovery plan is adequate to restore critical operation of the system in the case of an extended system outage. The disaster recovery plan should include the following:

— Identification of the disaster recovery team and a contact list.

— Recovery operation procedures.

— Procedure for establishing an alternative site including voice and data communications, mail, and support equipment.

— Plans for replacement of computer equipment.

— Establishment of a system backup schedule.

— Procedures for storage and retrieval of software, data, documentation, and vital records off-site.

— Logistics of moving staff, data, documentation, etc.

*Distributed architecture assessment.* Assess the distribution of data and processes in the proposed architecture for feasibility, timing conflicts, availability of telecommunications, cost, backup and restore features, downtime, system degradation, and provisions for installation of software updates.

*Exploratory testing.* Perform exploratory testing (i.e., simultaneous learning, test design and execution rather than scripted testing) on the system, software, or hardware.

*Feasibility study evaluation.* Verify that the feasibility study is correct, accurate, and complete. Validate that all logical and physical assumptions (e.g., physical models, business rules, and logical processes), constraints, and user requirements are satisfied.

*Independent risk assessment.* Conduct an independent risk assessment on any aspect of the software project and report on the findings. Such risk assessments will be primarily from a system perspective. Examples of risk assessment include: appropriateness of the selected development methodology or tools for the project; and quality risks associated with proposed development schedule alternatives.

*Inspection*. Inspect the software products to detect defects in the product at each selected development stage to assure the quality of the emerging software. The inspection process may consist of multiple steps for the segregation of the inspection functions of the following:

- Inspection planning
- Product overview
- Inspection preparation
- Examination meeting
- Defect rework
- Resolution follow-up

An inspection is performed by a small team of peer developers and includes, but is not led by, the author. The inspection team usually consists of three to six persons, and in some cases includes personnel from the test group, quality assurance, or V&V. The participants assume specific roles to find, classify, report, and analyze defects in the product. Each type of inspection is specifically defined by its intended purpose, required entry criteria, defect classification, checklists, exit criteria, designated participants, and its preparation and examination procedures. Inspections do not debate engineering judgments, suggest corrections, or educate project members; inspections detect anomalies and problems and verify their resolution by the author.

*Inspection (concept)*. Validate that the system architecture and requirements satisfy customer needs. Verify that the system requirements are complete and correct, and that omissions, defects, and ambiguities in the requirements are detected.

*Inspection (design)*. Verify that the design can be implemented, is traceable to the requirements, all interface and procedural logic is complete and correct, and omissions, defects, and ambiguities in the design are detected.

*Inspection (requirements)*. Validate that the requirements meet customer needs and can be implemented. Verify that they are complete, traceable, testable, and consistent so that omissions, defects, and ambiguities in the requirements are detected.

*Inspection (source code)*. Verify that the source code implementation is traceable to the design, all interfaces and procedural logic are complete and correct, and omissions, defects, and ambiguities in the source code are detected.

*Inspection—Test case (component, integration, system, acceptance)*. Verify that the (component, integration, system, acceptance) test plan has been followed accurately, that the set of component test cases is complete, and that all component test cases are correct.

*Inspection—Test design (component, integration, system, acceptance)*. Verify that the (component, integration, system, acceptance) test design is consistent with the test plan, and that the test design is correct, complete, and readable.

*Inspection—Test plan (component, integration, system, acceptance)*. Verify that the scope, strategy, resources, and schedule of the (component, integration, system, acceptance) testing process have been completely and accurately specified, that all items to be tested and all required tasks to be performed have been defined, and to assure that all personnel and resources necessary to perform the testing have been identified.

*Operational evaluation.* Assess the deployment readiness and operational readiness of the software. Operational evaluation may include examining the results of operational tests, audit reviews, and anomaly reports. This evaluation verifies that the software is as follows:

— At a suitable point of correctness for mass production of that software.

— Valid and correct for site-specific configurations.

*Performance monitoring.* Collect information on the performance of software under operational conditions. Determine whether system and software performance requirements are satisfied. Performance monitoring is a continual process and may include evaluation of the following items:

— Database transaction rates to determine the need to reorganize or re-index the database.

— Central processing unit (CPU) performance monitoring for load balancing.

— Direct access storage utilization.

— Network traffic to assure adequate bandwidth.

— Critical outputs of a system (e.g., scheduled frequency, expected range of values, scheduled system reports, and reports of events).

*Post-installation validation.* Execute a reference benchmark or periodic test for critical software when reliability is crucial or there is a possibility of software corruption. By automatically or manually comparing results with the established benchmark results, the system can be validated prior to each execution of the software. When pre-use benchmark testing is impractical, such as for real time, process control, and emergency-use software, a periodic test, conducted at a predetermined interval, can be used to assure continued reliability.

*Project management oversight support.* Assess project development status for technical and management issues, risks, and problems. Coordinate oversight assessment with the acquirer and development organization. Evaluate project plans, schedules, development processes, and status. Collect, analyze, and report on key project measures.

*Proposal evaluation support.* Participate in the development organization source selection process. Develop proposal evaluation factors and assessment criteria. Independently evaluate development organization proposals to assess conformance to the statement of work and performance requirements.

*Qualification testing.* Verify that all software requirements are tested according to qualification testing requirements demonstrating the feasibility of the software for operation and maintenance. Conduct, as necessary, any tests to verify and validate the correctness, accuracy, and completeness of the qualification testing results. Document the qualification test results together with the expected qualification test results. Planning for qualification testing may begin during the Requirements V&V activity.

*Regression analysis and testing.* Determine the extent of V&V analyses and tests to be repeated when changes are made to any previously examined software products. Assess the nature of the change to determine the potential ripple or side effects and the impacts on other aspects of the system. Rerun test cases based on changes, error corrections, and impact assessment to detect errors spawned by software modifications.

*Reusability analysis.* Verify that the artifacts (products) of the domain engineering process conform to project-defined purpose, format, and content (e.g., IEEE Std 1517-2010 [B10]). Verify that the domain models and domain architecture are correct, consistent, complete, and accurate, and that they conform to the domain engineering plan. Analyze the asset (software item intended for reuse) to verify that the asset is consistent with the domain model and domain architecture.

*Reuse analysis.* Analyze the developer's documentation to verify that the original domain of the candidate reuse software will satisfy the domain of the new system (e.g., integrity level, user needs, operating environment, safety, security, and interfaces). If the developer has performed no domain analysis, perform domain analysis (IEEE Std 1517-2010 [B10]) to compare the original domain and the new domain of the candidate reuse software. Verify that the developer's reuse plan dispositions and documents all domain differences.

*Simulation analysis.* Use a simulation to exercise the software or portions of the software to measure the performance of the software against predefined conditions and events. The simulation can take the form of a manual walkthrough of the software against specific program values and inputs. The simulation can also be another software program that provides the inputs and simulation of the environment to the software under examination. Simulation analysis is used to examine critical performance and response time requirements or the software's response to abnormal events and conditions.

*Sizing and timing analysis.* Collect and analyze data about the software functions and resource utilization to determine whether system and software requirements for speed and capacity are satisfied. The types of software functions and resource utilization issues include, but are not limited to, the following:

— CPU load

— Random access memory and secondary storage (e.g., disk, tape) utilization

— Network speed and capacity

— Input and output speed

Sizing and timing analysis is started at software design and iterated through acceptance testing.

*System software assessment.* Assess system software (e.g., operating system, computer-aided software engineering tools, database management system, repository, telecommunications software, and graphical user interface) for feasibility, impact on performance and functional requirements, maturity, supportability, adherence to standards, developer's knowledge of and experience with the system software and hardware, and software interface requirements.

*Test certification.* Certify the test results by verifying that the tests were conducted using baseline requirements, a configuration control process, and repeatable tests, and by witnessing the tests. Certification may be accomplished at a software configuration item level or at a system level.

*Test evaluation.* Evaluate the developer's tests for requirements coverage and test completeness. Assess coverage by assessing the extent of the software exercised. Assess test completeness by determining whether the set of inputs used during testing are a fair representative sample from the set of all possible inputs to the software. Assess whether test inputs include boundary condition inputs, rarely encountered inputs, and invalid inputs. For some software, it may be necessary to have a set of sequential or simultaneous inputs on one or several processors to test the software adequately.

*Test witnessing.* Monitor the fidelity of test execution to the specified test procedures and witness the recording of test results. When a test failure occurs, the testing process can be continued by: (1) implementing a "work around" to the failure, (2) inserting a temporary code patch, or (3) halting the testing process and implementing a software repair. In all cases, assess the test continuation process for test process breakage (e.g., some software is not tested or a patch is left in place permanently), adverse impact on other tests, and loss of configuration control. Regression analysis and testing should be done for all the software affected by the test failure.

*Training documentation evaluation.* Evaluate the training materials and procedures for completeness, correctness, readability, and effectiveness.

*Usability analysis.* Verify that stakeholder needs and interests are considered during development, operation, and maintenance process activities. The analysis will assure that: human-centered design activities are performed; human factors and ergonomics considerations are incorporated into the design, potential adverse effects on human health and safety are addressed in the design; and user needs are satisfied in a manner that supports user effectiveness and efficiency.

*User documentation evaluation.* Evaluate the user documentation for its completeness, correctness, and consistency with respect to requirements for user interface and for any functionality that can be invoked by the user. The review of the user documentation for its readability and effectiveness should include representative end users who are unfamiliar with the software. Employ the user documentation in planning an acceptance test that is representative of the operational environment.

*User training.* Assure that the user training includes rules that are specific to the administrative, operational, and application aspects, as well as the industry standards for that system. This training should be based on the technical user documentation and procedures provided by the manufacturer of the system. The organization responsible for the use of the system should be responsible for providing appropriate user training.

*V&V tool plan generation.* Prepare a plan that describes the tools needed to support the V&V effort. The plan includes a description of each tool's performance, required inputs and associated tools, outputs generated, need date, and cost of tool purchase or development. The tool plan should also describe test facilities and integration, and system test laboratories supporting the V&V effort. The scope and rigor of the V&V effort as defined by the selected integrity level should be considered in defining the performance required of each tool.

*V&V tool qualification.* Verify the features and usability of a V&V tool to assure that the tool is functioning properly and it does not mask errors that it was designed to find. Validate correct operation, limitations, and workarounds for known problems and deficiencies.

*Walkthrough.* Participate in the evaluation processes in which development personnel lead others through a structured examination of a product. Assure that the participants are qualified to examine the products and are not subject to undue influence. See specific descriptions of the requirement walkthrough, design walkthrough, source code walkthrough, and test walkthrough.

*Walkthrough (design).* Participate in a walkthrough of the design and updates of the design to assure completeness, correctness, technical integrity, and quality.

*Walkthrough (requirements).* Participate in a walkthrough of the requirements specification to assure that the software requirements are correct, unambiguous, complete, verifiable, consistent, modifiable, traceable, testable, and usable throughout the life cycle.

*Walkthrough (source code).* Participate in a walkthrough of the source code to assure that the code is complete, correct, maintainable, and free from logic errors; also assure the code conforms to coding standards and conventions, and will operate efficiently.

*Walkthrough (test).* Participate in a walkthrough of the test documentation to assure that the planned testing is correct and complete, and that the test results will be correctly analyzed.

*Work Breakdown Structure (WBS) Evaluation.* Verify that the WBS represents all of the project scope and captures all deliverables, including internal, external, and interim deliverables. Verify that the WBS decomposes the project scope into a set of deliverables that comprehensively defines the work to be performed. If a WBS dictionary exists, then verify that the WBS dictionary contains a brief definition of the project scope, each WBS component is included, each WBS component has a list of associated activities, and each major milestone is included.

# Annex H

(informative)

# Environmental factors consideration

## H.1 Introduction

The performance of system, software, and hardware V&V should be planned and executed to account for environmental factors that will influence the life cycle stages of the system—from concept development through disposal. These environmental factors may drive and constrain activities and tasks in each of the V&V life cycle processes; therefore, all environmental factors should be assessed to determine relevance and influence on the V&V activities and tasks to be performed.

## H.2 In the agreement processes

Environmental factor requirements and constraints should be defined during the Acquisition process and specified for the Supply process. These processes define the activities necessary to establish an agreement between two organizations. When preparing for the acquisition, the strategy development should consider the system, software, and hardware attributes, requirements, and/or constraints to verify that appropriate environmental factor requirements are included in the request for proposal/quotation and the resulting contract. The V&V for this stage should perform the following:

- Assess the need definition to verify that all environmental factors affecting system design, development, production, operation, and disposal throughout the life cycle are clearly and comprehensively stated.
- Review the solution approach selection process (such as analysis of alternatives) to verify that environmental factors are adequately incorporated into the decision process and criteria.
- Review the acquisition documentation for adequacy and sufficiency of definition/specification for the system operating environment(s), system non-operating environment(s), development environment(s), and maintenance environment(s) to assure that the resultant program or contract delivers a system that satisfies the defined need. The request for proposal/quotation should be reviewed to verify that all pertinent environmental requirements are incorporated.
- Review the acceptance documentation to assess planned and specified testing environment(s) to assure that the testing will provide full spectrum, operationally representative tests to determine whether the system is properly designed and produced for operation per the need definition.
- Assess the supplier qualifications to verify that selected supplier has the industrial capability to design, develop, produce, and support the program in accordance with acquisition documentation requirements. This assessment should include development, testing, production, and repair environments, processes, and tools.
- Assess the supplier’s proposal to verify that system design and development, testing and manufacturing approaches, and processes adequately and sufficiently address all environmental requirements of the acquisition documentation’s request for proposal/quotation.
- Assess the contract documentation to verify that environmental requirements reflect defined need and the supplier’s proposed solution with clear and binding terms.

## H.3 In the organizational project-enabling processes

Environmental considerations should be assessed to verify that the processes for infrastructure management, human resource management, and quality management adequately address the ability of the acquirer and supplier to provision, execute, monitor, assess, maintain, and improve processes and products that satisfy the system, software, and hardware needs over the full range of environmental requirements and constraints. The V&V for this stage should perform the following:

— Assess the supplier's infrastructure to be employed in the development and production of the system, software, and hardware to verify that the environmental requirements and constraints will be maintained throughout the acquisition contract. This assessment should include development, testing, production and repair environments, processes, and tools.

— Assess the human resources assigned to the contract to verify that they have the necessary education, experience, training, and certifications for the activities and tasks to which they are assigned. Assess the supplier's strategy and plans to verify that qualified human resources will be assigned to the project throughout the contract life.

— Assess the quality management strategy for the project to verify that environmental requirements and constraints for the infrastructure and the product (system, software, and hardware) will be monitored and maintained compliant throughout the contract life.

## H.4 In the project processes

The project processes should address environmental requirements and constraints in the project plan development, execution, and monitoring. The V&V for this stage should perform the following:

— Review the project technical management plan to verify that environmental factors will be included in technical reviews throughout the project.

— Assess the quality management plan to verify that environmental requirements and constraints for the infrastructure and the product (system, software, and hardware) will be monitored and maintained compliant throughout the contract life.

— Review the project performance measures to verify that environmental factors will be collected throughout the contract life.

— Verify that project assessments will include environmental factors on a continuing basis.

— Verify that the configuration management process will include adequate controls for environmental requirements and constraints affecting infrastructure, facilities, manufacturing processes, and tools.

## H.5 In the technical processes

The V&V should assess environmental factors throughout the technical processes as well as perform the following:

— Assess that all environmental requirements and constraints included in the acquirer's request for proposal and in the resulting contract with the supplier are completely specified in the project requirements documents and are appropriately allocated to the system elements, software, and hardware.

— Assess the architectural documents to verify that the environmental requirements and constraints from the project requirements documents have been incorporated into the architectural design.

— Monitor the implementation process, the integration process, and the development qualification testing to verify that the system elements, software, and hardware conform to and perform throughout the complete range of specified environmental conditions. Review the test environments,

tools, test plans/procedures, and results to assure the design is adequately tested to verify that the system will meet performance in all operating and non-operating environment requirements of the contract. Review anomaly clearing procedures and re-test procedures for adequacy and sufficiency. Specific test environments to be monitored and assessed include the following:

1) Functional
2) Integration
3) System
4) Qualification
5) Manufacturing (parts, subassembly, process sampling, etc.)
6) Certification and accreditation testing (interoperability, architecture and standards, security, etc.)
7) Operational

— Review the transition plans to verify that the environmental requirements and constraints are adequately addressed.

— Assess the effectiveness and suitability of design, procedures, training, and support by reviewing operational use data, operational failure data, and user feedback to determine whether environmental factors are adversely impacting system performance, safety, or security, or whether requested changes could improve system performance, safety, of security.

— Perform evaluations of new constraints to determine whether changing environments are impacting, or have the potential to impact, system performance, safety, or security in an adverse way.

— Assess operating procedures to determine whether changes in operational procedures or operational use profiles are impacting, or have the potential to impact, system performance, safety, or security adversely.

— Review metrics from the maintenance processes, tools, staffing, and controls to verify predictable and consistent results are achieved, adverse trends are identified, and corrective action/process improvements are incorporated when warranted. Review parts/component/COTS substitution and technical refresh processes to verify that environmental considerations are incorporated in the decision process and criteria. Review repair/upgrade kits and procedures intended for operational site location incorporation to verify environmental factors are adequately and sufficiently addressed.

— Assess plans for disposal of the system elements to verify that adequate provisions are delineated for retirement of the elements and subsequent storage, destruction, or disposal to preclude or contain hazardous and environmentally destructive materials and to prevent hazardous conditions.

# Annex I

(informative)

# Verification and validation (V&V) of system, software, and hardware integration

## I.1 Introduction

Disciplines required to develop software elements in digital systems are distinctly different from those required to develop the hardware components of digital systems in many important aspects. Developing software for a digital system requires knowledge of software engineering principles, the software language(s) to be used, the limitations of the language(s), and the processes by which the software requirements can be translated into a set of functions that meet a user's requirements. Optimally, some members of the software development team also should have system domain expertise to understand the system requirements allocated to software. Developing the hardware on which system software is to operate requires knowledge of electrical engineering, computer engineering, hardware performance characteristics, printed circuit board layout, equipment qualification, and similar considerations. Managing these separate disciplines and integrating the disciplines into a unified development process requires its own set of project management disciplines.

Given the diverse disciplines involved in the development of digital systems, misconceptions about the relationships among the system, software, and hardware should not be unexpected. Resolving these differences in specializations prevents incompatibilities arising between the three categories comprising a digital system (i.e., system, software, and hardware). Consequently, in addition to verifying and validating system, software, and hardware requirements, V&V efforts should verify and validate system, software, and hardware integration.

This annex provides examples of system, software, and hardware integration issues that should be addressed in the phases of the system development life cycle. The integration considerations discussed in this annex are not the full set of integration considerations a system developer should explore. Instead, the integration considerations are intended to encourage system developers to view the system development effort holistically instead of thinking of the software and hardware development efforts as tasks to be performed in isolation.

This annex provides summaries of digital system faults that were introduced during system development as a result of failing to identify potential adverse integration effects between the systems, software, and hardware. Table I.1 provides examples of integration considerations that should be addressed in the following life cycle phases:

- Acquisition
- Requirements (stakeholder and analysis)
- Architectural design
- Implementation
- Integration

## I.2 Examples of system failures caused by integration issues

### I.2.1 Introduction

Despite the individual skills of the specialists developing a system, there have been events in which integration of the software and hardware into the system did not result in desired system performance reliability goals. The following events' histories highlight the necessity for tightly coupling the system development effort with the software and hardware development efforts.

### I.2.2 Year 2000 system integration issue

Hardware memory limitation constraints in conjunction with the historical period in which early date/time-usage systems were developed (e.g., 1970) encouraged system developers to represent calendar year dates with two digits instead of four (e.g., 70 instead of 1970) when calculating elapsed time between two events. A contributing premise (when even considered) was that the system being developed would likely be updated or replaced before the year 2000 (i.e., 00) could affect elapsed time/date calculations over the transition period between December 31, 1999 and January 1, 2000.

In validating the software during development, developers used ranges of dates that did not include dates beyond December 31, 1999. The dates used to validate the software were at the time reasonable, since the software requirements were developed with the hardware limitations in mind.

System performance considerations of the effect of dates transitioning from "99" to "00" arose circa 1998 to 1999 as industries realized the degree to which digital systems had been integrated into critical digital assets. The nuclear industry, as well as other industries, began an intensive effort to identify date-related dependencies in critical systems. This industry-wide effort required significant expenditures of resources and funds to remediate critical systems, implement software revisions, and install new equipment.

The issue in this case is not attributed to software or hardware deficiencies; the software and hardware, when integrated, performed as required during the initially planned performance period. The issue in this case was in not identifying the full set of parameters that constrained the system operating space. The system temporal limits were defined for a date/time period that did not include dates in the following century.

The lesson from this example is that the full extent of a system boundary needs to be verified when developing software and hardware requirements. In the case of the year 2000 example, the system boundary should have included both physical and temporal constraints. For those cases in which hardware limitations forced software requirements limits, it is not enough that software integrated with hardware performs in accordance with software and hardware requirements; a verification process has to include the system boundaries that completely constrain the system performance parameters.

### I.2.3 System architecture integration issues

In the late 1990s, a consortium developed system requirements for a digital safety system function to be installed at several industrial sites. The system developer was selected for this development effort on the basis of its extensive experience developing high-integrity digital systems for the defense industry.

The consortium developed requirements for a master–slave system architecture to enhance system self-testing capabilities and thereby improve digital safety system availability. This type of architecture, which is common in high-integrity systems in many industries, used a duplicate (i.e., slave) system to check the operability of the master system functions. The assumption was that identical outputs from the master and slave system functions implied the system was operating as required. If the two output signals were different, then the system was not operating as required, and a system reset would be needed to alert the operators that either the master channel was inoperable or the slave channel was inoperable (or perhaps both were inoperable).

To verify that the master–slave calculations in this system were identical when the system was operating, the master system processor synchronized the slave processor to verify that the input signal values were the same in both microprocessor channels. This synchronization required the slave processor to prioritize safety function checking calculations over internal self-testing functions such that self-testing functions were placed on hold until the checking calculations were completed. The self-testing functions then resumed as the highest priority function in the slave processor.

Both the master processor channel and the slave processor channel performed channel self-testing to verify the two channels were operable. These self-testing functions operated cyclically such that the system was continuously tested when it was not performing safety function processing. Both channels used watchdog timers to verify their respective processor did not have an error that would prevent the channel from performing every self-testing function. If the self-testing was not completed within a set period, then the watchdog timer would reset the offending channel and thereby alert the operators that a channel was inoperable.

After the system was installed in several facilities, sporadic watchdog timer-initiated resets occurred in the slave processor channel. In response to these channel resets, the channel was required to be declared inoperable until the system could be placed back in service. The system developer was tasked with determining the cause of the sporadic watchdog timer resets.

After extensive root cause analyses, the system developer determined the fault to be in the priority baton-passing function built into the microprocessor. This microprocessor fault only arose when a high-priority task acquired the priority baton from a lower priority task before the lower priority task was completed. Upon completion of the high-priority task in the slave processor (i.e., the safety function processing in the slave processor that was initiated by the master processor), the slave microprocessor sometimes would not release the priority baton back to the interrupted self-testing function. This caused the self-testing function to fail to meet the watchdog timer restriction, and thereby caused the slave channel watchdog timer to reset the channel microprocessor. Approximately 10 months were required for the system developer to identify and correct this fault.

While the system developer had extensive experience developing systems using the microprocessor, that experience did not translate into the master-slave architecture. Interestingly, if the developer had reviewed publically available failure history reports from the microprocessor vendor’s Website at the start of the project, the priority baton-passing error would have been discovered during the hardware acquisition life cycle phase instead of in the operations life cycle phase.

This event illustrates the necessity for verifying that the hardware acquisition requirements and the software requirements (both internal to the hardware and imposed by software on the hardware) are compatible with the system architecture.

### I.2.4 System, software, and hardware interaction issues

The following example interaction issues provide a starting point for identifying issues that should be addressed during the system development process:

- Software size relative to hardware capability
- Hardware compatibility with software type (e.g., C, Hardware Design Language, etc.)
- System timing constraints on software design and hardware capabilities
- System architecture and software architecture relative to hardware capabilities
- Capability to validate software in an environment representative of the hardware architecture
- Hardware restrictions relative to system environment (e.g., equipment qualification issues, etc.)
- Software integrity requirements relative to hardware architecture

— System maintainability relative to hardware acquisition constraints

— Software architecture relative to system maintainability (e.g., use of object-oriented structure or an arcane structure that becomes outdated over time, thereby limiting the number of personnel qualified to perform corrective, adaptive, or perfective changes on the system)

— Hardware availability over the projected lifetime of the system

This list of potential interaction issues is not exhaustive. The purpose of the list is to instill in system developers the realization that digital system performance issues can arise from interactions among software, hardware, and the system.

Table I.1 graphically summarizes the potential interactions among the system, software, and hardware for the example issues described for each system development life cycle phase in which the software and hardware are developed relatively individually. The cells in Table I.1 marked with an "X" correspond to the system, software, and hardware potential contributors to interactions corresponding to the life cycle phases in which the potential interactions should be addressed during the development effort.

The purpose of Table I.1 is to provide a sample framework system developers can use to summarize potential interaction issues identified or anticipated during life cycle development activities. By identifying these interactions in a graphical format, the developer can refine the scope of verification and validation activities to address system, software, and hardware interaction issues specifically. Other interaction concerns may need to be added to the list of examples depending on specific system architecture requirements.

**Table I.1—Examples of integration V&V issues**

| Interaction issue | System development life cycle phases | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Acquisition | | | Requirements | | | Arch. design | | | Implementation | | | Integration | | |
| | Interactions to be addressed | | | | | | | | | | | | | | |
| | Sys | SW | HW | Sys | SW | HW | Sys | SW | HW | Sys | SW | HW | Sys | SW | HW |
| Software size relative to hardware capability | X | X | X | X | X | X | | X | X | | X | X | | X | X |
| Hardware compatibility with software language and structure | | X | X | | X | X | | X | X | | X | X | | X | X |
| System timing relative to software design and hardware capabilities | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| System and software architecture relative to hardware capabilities | X | X | X | X | X | X | X | X | X | X | X | X | X | X | X |
| Capability to validate software in environment representative of the hardware architecture | | X | X | X | X | X | | X | X | | X | X | | X | X |
| Hardware restrictions relative to system environment | X | | X | X | | X | X | | X | X | | X | X | | X |
| Software integrity relative to hardware architecture | | X | X | X | X | X | | X | X | | X | X | | X | X |
| System maintainability relative to hardware acquisition | X | | X | X | | X | X | | X | X | | X | X | | X |
| System maintainability relative to software architecture | X | X | | X | X | | X | X | | X | X | | X | X | |
| Hardware availability relative to projected system lifetime | X | | X | X | | X | | | | | | | | | |

# Annex J

(informative)

# Hazard, security, and risk analysis

## J.1 Introduction

Hazard, security, and risk analysis are systems engineering disciplines that enable systematic understanding of technical, operational, and environmental factors that can cause harm. Table J.1 provides an overview of each type of analysis and discusses the relationships among the three disciplines.

**Table J.1—Examples of integration verification and validation (V&V) issues**

| Discipline | Overview | Relationships |
|---|---|---|
| Hazard analysis | Identifies hazardous conditions that could lead to adverse consequences. The analysis identifies hazard contributors or combinations of contributors. The hazard analysis allows the development project to control or mitigate identified hazards. | — Hazard analysis enables system responses to realized events.<br>— Security analysis focuses on protecting the system in life cycle.<br>— Preventing a threat can occur as part of either hazard or security analysis.<br>— Both hazard analysis and security analysis are based on system risk assessment, so they support the risk analysis process. An output of both includes understanding of residual risks in the respective areas after the technical, operational, or management steps are taken during system development, operation, and maintenance processes.<br>— Risk analysis addresses all areas of the system life cycle. |
| Security analysis | Develops processes and mechanisms to protect the assets (system of interest). Analysis activities include identification of assets and threats, assessing vulnerabilities, and developing countermeasures to minimize the security risk. Security analysis also includes an assessment of processes to determine that the development, V&V, and operational environments are safe.<br>The protection of the system includes sub-disciplines including physical security, computer security, and information assurance. A quickly emerging field within security analysis is cyber security, which is the process of applying security measures for confidentiality, integrity, and availability of assets. The rapidity of the cyber threats is necessitating system 1) development and V&V techniques, 2) processes (system life cycle) management to respond accordingly. | |
| Risk analysis | Identifies and defines actions for risks that have a measureable possibility of negative consequences to either the successful development or operation of the system. The risk process is also viewed as a management tool to understand potential consequences to the development or operation of the system. | |

Details including V&V objectives for each of the three areas are detailed in subsequent sections.

## J.2 Hazard analysis

V&V often uses the results of hazard analyses to target V&V activities in a manner that provides greater assurance that the controls for hazards work as needed and that the system does not contribute to a hazardous condition by behaving in an undesirable way. Generally, one or more additional conditions need to exist or additional events need to occur in conjunction with the existence of the hazard in order for an accident or mishap with consequences adverse to safety to result. These additional events enable the hazard to proceed to the adverse consequence. Hazards analysis involves the application of systematic and replicable methods to identify and understand hazards, as well as to characterize the risk of mishaps that involve hazards.

The hazard analysis is a systems engineering activity that will account for the system design, operational conditions, system physical constraints, and regulations to identify hazardous conditions that could lead to adverse consequences. Once the end hazardous conditions are identified, the hazard analysis typically uses a fault tree analysis approach to identify the contributors or combination of contributors (within the bounds of required system fault tolerance) to reaching the hazardous condition. The fault tree is a symbolic logic diagram showing the cause–effect relationship between a top undesired event (failure) and one or more contributing causes. It is a type of logic tree that is developed by deductive logic from a top undesired event to all sub-events that must occur to cause it. The contributing causes may be the result of hardware or software faults, human actions (e.g., procedures), or hostile environmental conditions. The hazard analysis is repeated in each life cycle phase and accounts for further elaboration of designs, changes to intended system use and operations, and the emergence of new hazardous conditions. The hazard analysis may be performed by any organization within the project such as systems engineering, reliability, safety, or V&V. In any case, V&V reviews the hazard analysis for completeness and usability, and it assures that stated hazards and contributors are clearly identified to sufficient detail to affect engineering and mitigation activities properly and to develop V&V plans and evaluation criteria.

Not all hazards represent the same risk. Systems engineers, operations experts, and reliability engineers may all contribute to evaluating the magnitude of risk that a hazard may present. The risk-based integrity level schema presented in Annex B is suitable as well for the assessment of risk associated with a hazard.

As a result of the hazard analysis, the project will define requirements for the control or mitigation of hazards (as well as re-design the system to reduce risk exposure). These requirements may be in the form of system capabilities, redundancy and fault tolerance requirements, use of engineering standards, or operational procedures. The traceability of these requirements and associated design elements to the specific hazard and the hazard's risk magnitude will serve to determine the V&V integrity level for the requirement or system element and the level of V&V rigor needed.

Specific V&V activities that may be appropriate for "critical" requirements necessary to control, mitigate, or prevent hazards may include the following activities:

a) Traceability of critical requirements through the life cycle to verify implementation

b) Evaluation of potential hazard contributors to validate that critical requirements are complete and are appropriate for the system operational need

c) Evaluation of architectures and designs to determine whether hazard mitigation functions meet required capabilities and whether additional mitigation strategies are needed

d) Application of verification methods (analyses, inspections, demonstrations, or tests) that are intended to determine whether the contributing conditions to a hazardous state are possible. These verification methods may include the following:

1) Statistical analyses to determine whether the probability of reaching a contributing condition is within acceptable levels. This may include random testing, Monte Carlo analysis, stress testing, duration testing, or mathematical models.

2) Inspections to verify that hazard causes are not present and that hazard controls are implemented as specified. This may also include inspections to confirm that regulatory or engineering standards have been followed.

3) Demonstrations in an operational setting to show that operational and human factor–based hazard controls are reasonable and effective.

4) Tests to verify that specific hazard controls (physical, procedural, and automated controls) are capable of identifying the faults or hazard contributors and isolating them from propagating into a hazardous condition.

The objective for the V&V of hazards is to perform a sufficient set of V&V tasks for all contributors such that the likelihood of reaching a hazardous condition is known to a desired level of confidence. The V&V integrity levels and their use in tailoring V&V activities as described in this standard provide for more rigor as the integrity level increases. Additionally, the use of assurance cases provides for the evidence to satisfy claims that certain desired properties or behaviors exist, or undesired properties or behaviors do not exist, as necessary to prevent a specific hazardous condition.

## J.3 Security analysis

### J.3.1 Summary

One of the objectives of security analysis performed by the V&V effort is to verify that the system-required threat controls and safeguards are correctly implemented and to validate that they provide the desired levels of protection of system vulnerabilities. The other objective is to verify that there is a process for describing the system, software, and hardware process security. Figure J.1 (reference ISO/IEC 15408-1:2009 [B17]) shows the basic concept for the security context of the system. Except for general threat-risk assessment, information security analysis becomes more important to assure confidence in countermeasures to minimize the security risk for the final product. A system should consider different security issues in each phase of the life cycle because the system owner may change as the product evolves. The V&V security analysis should consider:

— The context of the system (e.g., the development process and environment, the final operational environment, organization structures and management policy, operational and maintenance personnel roles, interfaces with other external systems or support systems);

— The system of interest and its elements, threats, vulnerabilities, and countermeasures;

— Tradeoffs between techniques, operations, and management to address security requirements.

— Identification of threats. These threats may be natural (e.g., inclement weather, earthquakes), human (e.g., unintended or malicious), or environmental (e.g., chemical leak, power loss).

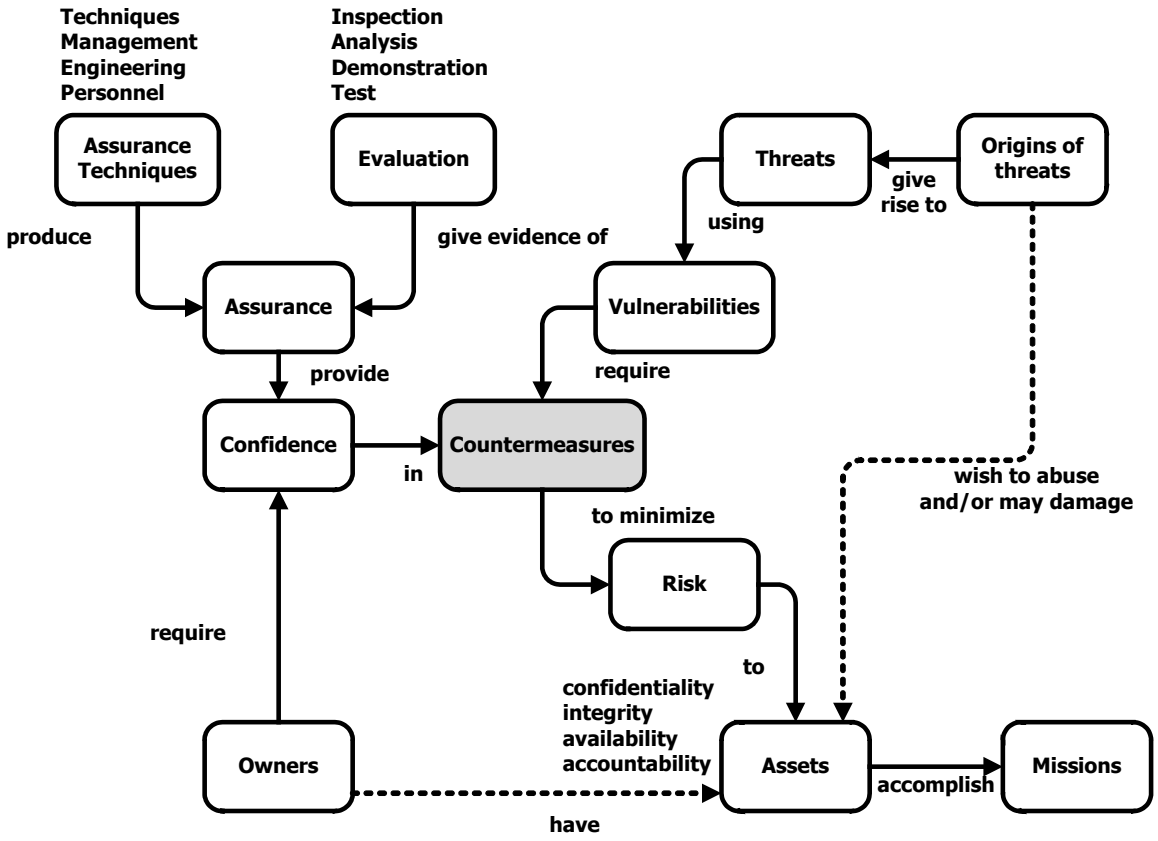



**Figure J.1—The security context of the system**

### J.3.2 Threat-based security analysis

#### J.3.2.1 Overview

The V&V security analysis task may rely on threat-based analyses. A threat has the potential to harm assets such as information, processes, and systems and, therefore, organizations. A vulnerability is a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of security policy. The desired levels of protection and security policies are unique to the stakeholder organization.

The V&V security analysis is performed in parallel with project system security risk assessments that generally include the following activities:

— Identification of threats.

— An identification of system vulnerabilities. Vulnerabilities may include items such as system physical exposure, inability to recognize an intrusion, security perimeters that can be compromised, or accessibility of sensitive computing systems or data.

— Evaluation of controls needed to prevent threats from exercising a potential vulnerability.

— Evaluation of the likelihood of a threat exercising a potential vulnerability according to current or planned controls.

— Evaluation of the impact of a security breach or security policy violation. Impacts may include items such as human safety, financial loss, social loss, environmental mission loss, or business continuity.

The system security risk assessment creates security threat controls to mitigate security risk to levels acceptable to the stakeholders. The security control requirements may be in the form of system functional capabilities, physical perimeter safeguards, redundancy, backup and recovery, or operational procedures. Much like the hazard analysis, the traceability of these requirements and associated design elements to the specific security impact severity will serve to determine the V&V integrity level for the requirement or system element and the level of V&V rigor needed.

Specific V&V activities that may be appropriate for "critical" security requirements necessary to control threats and exposure to vulnerabilities may include the following activities:

a) Traceability of critical requirements through the life cycle to verify implementation.

b) Evaluation of potential threat sources and vulnerabilities to validate that critical security requirements are complete and are appropriate for the system operational need.

c) Evaluation of architectures and designs to determine whether security functions meet required capabilities, whether additional threat controls are needed, and whether design changes are needed to remove vulnerabilities.

d) Application of verification methods (analyses, inspections, demonstrations, or tests) that are intended to determine whether plausible threats can exploit vulnerabilities. These verification methods may include the following:

    1) Statistical analyses to determine whether the probability of breaching a security control is within acceptable levels. This may include simulations or mathematical models (e.g., for encryption methods).

    2) Inspections to verify that security controls are implemented as specified. This may also include inspections that regulatory or policy standards have been followed.

    3) Demonstrations in an operational setting to show that security controls are reasonable and effective.

    4) Tests to verify that specific security controls (physical, procedural, and automated controls) cannot be breached. For IT systems, this may also include vulnerability scanning and penetration testing.

e) Review of the residual security risks (residual security risk can contain unidentified risk or be known as "retained risk") to validate whether the risks are acceptable and meet the organization's risk acceptance criteria.

### J.3.2.2 Typical threats

Based on the V&V object, a system defense-in-depth protection strategy and its threat approach may be more systematic. The system elements may require different technical or management measures to support the system security design, so the risks that threats successfully use vulnerabilities through some approaches may be more specialized.

For any system or its element, Table J.2 provides examples of types of typical threats, examples of specific threats within each type, and the origin of the types of threats. The list and following explanation, referenced from Annex C, "Examples of typical threats" in ISO/IEC 27005:2011 [B21] could be helpful during V&V security analysis activities.

**Table J.2—Types of typical threats**

| Type | Threats | Origin |
|---|---|---|
| Physical damage | Fire | Accidental<br>Deliberate<br>Environmental |
| | Water damage | |
| | Pollution | |
| | Major accident | |
| | Destruction of equipment or media | |
| Natural events | Climatic phenomenon | Environmental |
| | Seismic phenomenon | Environmental |
| | Volcanic phenomenon | Environmental |
| | Meteorological phenomenon | Environmental |
| | Flood | Environmental |
| Loss of essential services | Failure of air-conditioning or water supply system | Accidental<br>Deliberate |
| | Loss of power supply | Accidental<br>Deliberate<br>Environmental |
| | Failure of telecommunication equipment | Accidental<br>Deliberate |
| Disturbance due to radiation | Electromagnetic radiation | Accidental<br>Deliberate<br>Environmental |
| | Thermal radiation | |
| | Reactive radiation | |
| | Electromagnetic pulses | |
| Compromise of information | Interception of compromising interference signals | Deliberate |
| | Remote spying | Deliberate |
| | Eavesdropping | Deliberate |
| | Theft of media or documents | Deliberate |
| | Theft of equipment | Deliberate |
| | Retrieval of recycled or discarded media | Deliberate |
| | Disclosure | Accidental<br>Deliberate |
| | Data from untrustworthy sources | Accidental<br>Deliberate |
| | Tampering with hardware | Deliberate |
| | Tampering with software | Accidental<br>Deliberate |
| | Position detection | Deliberate |
| Technical failures | Equipment failure | Accidental |
| | Equipment malfunction | Accidental |
| | Saturation of the information system | Accidental<br>Deliberate |
| | Software malfunction | Accidental |
| | Breach of information system maintainability | Accidental<br>Deliberate |
| Unauthorized actions | Unauthorized use of equipment | Deliberate |
| | Fraudulent copying of software | Deliberate |
| | Use of counterfeit or copied software | Accidental<br>Deliberate |
| | Corruption of data | Deliberate |
| | Illegal processing of data | Deliberate |
| Compromise of function | Error in use | Accidental |
| | Abuse of rights | Accidental<br>Deliberate |
| | Forging of rights | Deliberate |
| | Denial of actions | Deliberate |
| | Breach of personnel availability | Accidental<br>Deliberate<br>Environmental |

Threats may be deliberate, accidental, or environmental (natural), and may result in damage or loss of essential services. The origin of threats may be categorized as follows:

Deliberate threats (also called active threats) arise from deliberate actions aimed at assets. Updates, corrections, and other changes to operating systems, application programs, configurations, connectivity, and equipment can provide an unexpected security threat to the systems or the respective production processes from deliberate threats. These may come in various forms:

- Communication attack
- Database injection
- Signals replay
- Spoofing and impersonation
- Social engineering
- Phishing
- Malicious code (virus, worm, Trojan horse, etc.)
- Denial of service
- Escalation of privileges
- Physical destruction attack

Accidental threats (also called passive threats) arise from human actions than can accidentally damage assets. For example, a person unfamiliar with proper procedures and policies, or through an honest oversight, causes an accidental risk. Also, a user may not be aware of potential risks in a system and may trigger a threat by accident as the user operates a complex system. Environmental threats arise from conditions or external events that are not based on human actions.

The origins of threats come in many different forms. Examples from IEC/TS 62443-1-1: 2009—Security for Industrial Automation and Control Systems: Terminology, Concepts and Models include:

a) Insider—An insider is a “trusted” person, employee, contractor, or supplier who has information that is not generally known to the public. An insider can present a threat even if there is no intent to do harm. For example, the threat may arise as a result of an insider bypassing security controls “to get the job done.”

b) Outsider—An outsider is a person or group not “trusted” with inside access, who may or may not be known to the targeted organization. Outsiders may or may not have been insiders at one time.

c) Natural—Natural events include storms, earthquakes, floods, and tornadoes, and are generally considered a physical threat.

Particular attention (based on different businesses) should be paid to human threat sources. These are specifically itemized in Table J.3.

**Table J.3—Example origins of threats**

| Origin of threat | Motivation | Possible consequences |
|---|---|---|
| Hacker, cracker | Challenge<br>Ego<br>Rebellion<br>Status<br>Money | Hacking<br>Social engineering<br>System intrusion break-ins<br>Unauthorized system access |
| Computer criminal | Destruction of information<br>Illegal information disclosure<br>Monetary gain<br>Unauthorized data alteration | Computer crime (e.g., cyber stalking)<br>Fraudulent act (e.g., replay, impersonation, interception)<br>Information bribery<br>Spoofing<br>System intrusion |
| Terrorist | Blackmail<br>Destruction of information<br>Exploitation<br>Revenge<br>Political gain<br>Media coverage | Bomb/terrorism<br>Information warfare<br>System attack (e.g., distributed denial of service)<br>System penetration<br>System tampering |
| Industrial espionage (intelligence, companies, foreign governments, other government interests) | Competitive advantage<br>Economic espionage | Defense advantage<br>Political advantage<br>Economic exploitation<br>Information theft<br>Intrusion on personal privacy<br>Social engineering<br>System penetration<br>Unauthorized system access (access to classified, proprietary, and/or technology-related information) |
| Insiders | Curiosity<br>Ego<br>Intelligence<br>Monetary gain<br>Revenge<br>Unintentional errors and omissions | Assault on an employee<br>Blackmail<br>Browsing of proprietary information<br>Computer abuse<br>Fraud and theft<br>Information bribery<br>Input of falsified, corrupted data<br>Interception<br>Malicious code (e.g., virus, logic bomb, Trojan horse)<br>Sale of personal information<br>System bugs<br>System intrusion<br>System sabotage<br>Unauthorized system access |

### J.3.2.3 Typical vulnerabilities

Vulnerabilities may be present objectively in any system. The following table (referenced from Annex D, "Vulnerabilities and methods for vulnerability assessment" in ISO/IEC 27005:2011 [B21]) gives examples of typical vulnerabilities in various security areas, including examples of threats that might exploit these vulnerabilities. The table could provide help during the assessment of threats and vulnerabilities to determine relevant incident scenarios. It is emphasized that in some cases other threats may exploit these vulnerabilities as well. Table J.4 provides examples of typical vulnerabilities.

**Table J.4—Example origins of threats**

| System of Interest | Examples of vulnerabilities | Examples of threats |
|---|---|---|
| Hardware | Insufficient maintenance/faulty installation of storage media | Breach of information system maintainability |
| | Lack of periodic replacement schemas | Destruction of equipment or media |
| | Susceptibility to humidity, dust, soiling | Dust, corrosion, freezing |
| | Sensitivity to electromagnetic radiation | Electromagnetic radiation |
| | Lack of efficient configuration change control | Error in use |
| | Susceptibility to voltage variations | Loss of power supply |
| | Susceptibility to temperature variations | Meteorological phenomenon |
| | Unprotected storage | Theft of media or documents |
| | Lack of care at disposal | Theft of media or documents |
| | Uncontrolled copying | Theft of media or documents |
| Software | No or insufficient software testing | Abuse of rights |
| | Well-known flaws in the software | Abuse of rights |
| | No “logout” when leaving the workstation | Abuse of rights |
| | Disposal or reuse of storage media without proper erasure | Abuse of rights |
| | Lack of audit trail | Abuse of rights |
| | Wrong allocation of access rights | Abuse of rights |
| | Widely-distributed software | Corruption of data |
| | Applying application programs to the wrong data in terms of time | Corruption of data |
| | Complicated user interface | Error in use |
| | Lack of documentation | Error in use |
| | Incorrect parameter set up | Error in use |
| | Incorrect dates | Error in use |
| Network | Lack of identification and authentication mechanisms like user authentication | Forging of rights |
| | Unprotected password tables | Forging of rights |
| | Poor password management | Forging of rights |
| | Unnecessary services enabled | Illegal processing of data |
| | Immature or new software | Software malfunction |
| | Unclear or incomplete specifications for developers | Software malfunction |
| | Lack of effective change control | Software malfunction |
| | Uncontrolled downloading and use of software | Tampering with software |
| | Lack of back-up copies | Tampering with software |
| | Lack of physical protection of the building, doors, and windows | Theft of media or documents |
| | Failure to produce management reports | Unauthorized use of equipment |
| | Lack of proof of sending or receiving a message | Denial of actions |
| | Unprotected communication lines | Eavesdropping |
| | Unprotected sensitive traffic | Eavesdropping |
| | Poor joint cabling | Failure of telecommunication equipment |
| | Single point of failure | Failure of telecommunication equipment |
| | Lack of identification and authentication of sender and receiver | Forging of rights |
| | Insecure network architecture | Remote spying |
| | Transfer of passwords in clear communication | Remote spying |
| | Inadequate network management (resilience of routing) | Saturation of the information system |
| | Unprotected public network connections | Unauthorized use of equipment |
| Personnel | Absence of personnel | Breach of personnel availability |
| | Inadequate recruitment procedures | Destruction of equipment or media |
| | Insufficient security training | Error in use |
| | Incorrect use of software and hardware | Error in use |
| | Lack of security awareness | Error in use |

| System of Interest | Examples of vulnerabilities | Examples of threats |
|---|---|---|
| | Lack of monitoring mechanisms | Illegal processing of data |
| | Unsupervised work by outside or cleaning staff | Theft of media or documents |
| | Lack of policies for the correct use of telecommunications media and messaging | Unauthorized use of equipment |
| Site | Inadequate or careless use of physical access control to buildings and rooms | Destruction of equipment or media |
| | Location in an area susceptible to flood | Flood |
| | Unstable power grid | Loss of power supply |
| | Lack of physical protection of the building, doors, and windows | Theft of equipment |
| Organization | Lack of formal procedure for user registration and de-registration | Abuse of rights |
| | Lack of formal process for access right review (supervision) | Abuse of rights |
| | Insufficient provisions (concerning security) in contracts with customers and/or third parties | Abuse of rights |
| | Lack of procedure of monitoring of information processing facilities | Abuse of rights |
| | Lack of regular audits (supervision) | Abuse of rights |
| | Lack of procedures of risk identification and assessment | Abuse of rights |
| | Lack of fault reports recorded in administrator and operator logs | Abuse of rights |
| | Inadequate service maintenance response | Breach of maintainability |
| | Insufficient Service Level Agreement | Breach of maintainability |
| | Lack of change control procedure | Breach of maintainability |
| | Lack of formal procedure for security documentation control | Corruption of data |
| | Lack of formal procedure for security record supervision | Corruption of data |
| | Lack of formal process for authorization of public available information | Data from untrustworthy sources |
| | Lack of proper allocation of information security responsibilities | Denial of actions |
| | Lack of continuity plans | Equipment failure |
| | Lack of e-mail usage policy | Error in use |
| | Lack of procedures for introducing software into operational systems | Error in use |
| | Lack of records in administrator and operator logs | Error in use |
| | Lack of procedures for classified information handling | Error in use |
| | Lack of information security responsibilities in job descriptions | Error in use |
| | Insufficient provisions (concerning information security) in contracts with customers and/or third parties | Illegal processing of data employees |
| | Lack of defined disciplinary process in case of information security incident | Theft of equipment |
| | Lack of formal policy on mobile computer usage | Theft of equipment |
| | Lack of control of off-premise assets | Theft of equipment |
| | Insufficient “clear desk and clear screen policy” | Theft of media or documents |
| | Lack of information processing facilities authorization | Theft of media or documents |
| | Lack of established monitoring mechanisms for security breaches | Theft of media or documents |
| | Lack of regular management reviews | Unauthorized use of equipment |
| | Lack of procedures for reporting security weaknesses | Unauthorized use of equipment |
| | Lack of procedures of provisions compliance with intellectual rights | Use of counterfeit or copied software |

### J.3.3 Process assurance consideration in system life cycle

As shown in Figure J.1, the system owner should consider the assurance for system security. Generally, the final users or operational organization shall undertake the responsibility. But, when a certain system is under development or integration, the supplier or its vendor is the temporary owner who designs the system or system elements for operations. Unless the supplier or its vendor has considered the security problems,

the development or integration process also has certain risks that could be introduced into system. Furthermore, the V&V team evaluates the security implementations, so any result or issue of demonstration should be controlled under the configuration management process.

Assurance requires that stakeholders of the system of interest should have:

- A robust development, agreement (acquisition or supply), and V&V process (see note) to achieve a product. For some critical systems, the supplier should verify no security issue (unwanted or unnecessary code and function) has been introduced.
- A secure development and operational environment against undocumented, unneeded, and unwanted modifications.
- A secure V&V environment to protect V&V result.
- Secure tools for development and V&V.
- Long-standing resource (human and budget) for security management, training, design, implementation, evaluation, operation, maintenance, and emergency preparedness.

NOTE—Subclause 12.8.5 requires that the verification and validation plan (VVP) shall describe how the V&V effort conforms to existing security provisions and how the validity of V&V results shall be protected from unauthorized alterations. The security V&V process should not only verify and validate the secure development and operational environment feature criteria and functions, but also assure protection from inadvertent manipulation of the test environment and test results.

## J.4 Risk analysis

### J.4.1 Risk analysis objectives

The objective of risk analyses performed by the V&V effort is to identify technical and engineering risks that have a measureable possibility of negative consequences to either the operation of the system or the successful development of the system. The risk analysis activity includes the following:

- Identifying the initiating events, hazards, threats, or situations that create risks.
- Estimating the probability of occurrence, the consequences for each risk, and the expected timing of the risk.
- Evaluating each risk or defined combination of risks against its applicable threshold, generate alternatives to treat risks above their risk thresholds, and make recommendations for treatment based on a priority order.

Risk analysis shall be performed continuously throughout the life cycle.

### J.4.2 Risk analysis context

The V&V effort risk analysis activity falls within a broader risk management approach. For example, the risk analysis process steps of identify, estimate, and evaluate described in J.3.3 follow the risk analysis process activity within the broader risk process described in ISO/IEC 16085-2006 [B19], which also addresses the risk management activities of managing the project risk portfolio, risk treatment, or risk monitoring.

Risks identified by the V&V effort often require management and mitigation by other project organizations. Accordingly, the V&V Plan should have clear provisions for communicating and escalating V&V identified risks to the organization with the responsibility to perform risk treatment.

Some risks of concern to the V&V effort are tightly coupled with hazard analyses and integrity levels. The severity of the consequence of a system operational risk will likely not exceed the worst case severity of a system hazard or integrity level. Risks are often directly coupled to hazards. The likelihood that a hazard is reachable may be too high and cause re-engineering of the system to add hazard controls (or security controls for security hazards). There may be risk that a particular hazard control is unreliable or not verifiable. Both cases are of interest to the V&V effort. The hazard analysis is driven by the system design and operating environment. Probabilistic risk assessments evaluate the likelihood of reaching the hazardous condition and risk management determines whether the probabilities exceed acceptable thresholds and require treatment. The V&V effort may identify risks when the probability of reaching a hazardous condition is perceived by the V&V effort to be beyond levels of acceptability for the system and there is no plan to treat the risk. The V&V effort may also identify a risk when there is inadequate evidence that hazard controls provide the desired behavior/function or when there is uncertainty with regard to the conditions that may lead to a hazard. The same hazard-based risk analysis concepts apply to security-based risk analyses where undesired conditions may result from uncontrolled vulnerabilities or inadequate protection from threats.

### J.4.3 V&V risk analysis

#### J.4.3.1 Risk identification

Various approaches to identifying risks should be used. These approaches may include the use of risk questionnaires, taxonomies, brainstorming, scenario analysis, lessons learned, and prototyping or other knowledge acquisition approaches. Repeatable identification processes may be used to aid in the capture of lessons learned. Where possible, events, hazards, threats, or situations that can create risks should be identified to aid future risk treatment. Risks not identified are implicitly accepted. Risk categories should be used consistently for effective communication to stakeholders. Risks that are related may be combined for ease of analysis, monitoring, and treatment. System or software anomalies, reports on measures, and other indicators should be continuously reviewed as sources for risks.

NOTE—IEEE Std 1044-2009 [B7] provides useful information regarding anomaly classification. IEEE Std 982.1-2005 [B4] provides useful information regarding software measures related to reliability. ISO/IEC 15939-2007 [B18] provides a measurement process that can be used to help identify and characterize risks.

The V&V risk analysis is complementary to the risk analyses performed by the project management and developer organizations. The focus for V&V effort risk analysis is driven by the visibility the V&V effort has into life cycle products and is often concerned with the following types of risks:

a) Risk that the system, as specified, will not meet stakeholder needs and requirements.

b) Risk that the system may exhibit undesired behavior.

c) Risk that engineering and integration plans will not enable accomplishment of V&V objectives through system integration/buildup.

d) Risk that the acceptability of system or system elements cannot be determined.

e) Risk that artifact quality or defect trends will impair accomplishment of project milestones or system operational objectives.

f) Risk that the likelihood of reaching a defined hazardous condition is too high.

g) Risk that security threats protections are not adequate.

h) Risk that security vulnerabilities are not adequately ameliorated.

i) Risk that the system is not maintainable.

Less frequently, but in some cases, the V&V effort may focus on programmatic risk such as cost and schedule performance.

### J.4.3.2 Risk estimation

The likelihood of occurrence and consequences of each risk identified shall be estimated. Estimates may be either quantitative or qualitative. The stakeholders should define which risks will be evaluated using a qualitative scale and which will be evaluated using a quantitative scale. The scale(s) used for estimating risk likelihood and consequences shall be used consistently. The descriptive and measurement uncertainty inherent in the scale used should be described in the risk management plan. The level of confidence in a risk's estimate should be captured in its risk state.

### J.4.3.3 Risk evaluation

Each risk shall be evaluated against its risk thresholds. Risks should be evaluated independently, in combination, and along with their interactions with system and enterprise risks. Risks should be evaluated against the project risk threshold to assure that a combination of risks, while below their individual thresholds, does not unacceptably place the project as a whole at risk. Different techniques may be used to evaluate the risks, such as decision trees, scenario planning, game theory, probabilistic analysis, and linear programming.

Risks shall be placed in a priority ordering where the ordering criteria are determined by the stakeholders. Priority may be based on when the risk is anticipated to become a problem, the risk exposure, risk-related measures, or some other consistent criteria. Various treatment alternatives to addressing risk should be considered to reduce or eliminate risks. For each risk that is above its risk threshold, recommended treatment strategies such as eliminating the risk, reducing its probability of occurrence or severity of consequence, or accepting the risk shall be defined and documented in a risk action request such as that found in Annex B. Contingency plans should be developed for all risks above their thresholds. Measures indicating the effectiveness of the treatment alternatives shall also be defined. The risks, their recommended treatments, and measures of risk treatment effectiveness shall be communicated to the stakeholders for approval, rejection, or modification.

# Annex K

(informative)

# Example of assigning and changing the system integrity level of "supporting system functions"

The integrity level of system functions that are designated as critical functions does not change during the system life cycle unless authorized by the authorized system acquirer or regulatory organization. Noncritical system functions may become critical if the system is configured such that the originally noncritical 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. We will refer to these system functions as "critical supporting system functions." Any of the "critical supporting system functions" can lower their assigned system integrity level during development stages by the selection of technology or design/implementation techniques.

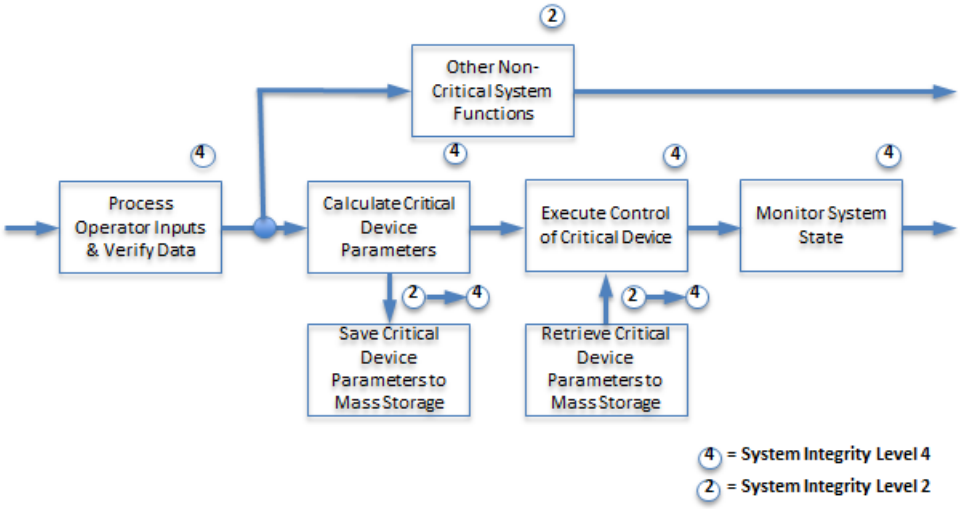
The V&V criticality analysis task performed at each development stage verifies the criticality of each system function and verifies that the correct system integrity level has been assigned. It is in this V&V task that a determination can occur where a "critical supporting system function" from a previous stage can be lowered or raised due to a technology selection or design/implementation technique being used by the subsequent development stage. The following two figures illustrate both the raising and the later lowering of system integrity levels for a supporting system function.

The example is a functional control flow diagram of the function of controlling a critical device. During the design stage of development, the control flow shows the receipt of device control inputs from an operator and critical device control parameters being calculated from the operator inputs. Those critical parameters are stored in a mass storage device and then retrieved by the critical device controller for execution of control of the critical device. Initial system integrity level assignment from the criticality analysis task designates the following system functions at the highest system criticality level 4 (in a four-level system integrity schema):

- Process operator inputs and verify data
- Calculate critical device parameters
- Execute control of critical device
- Monitor system

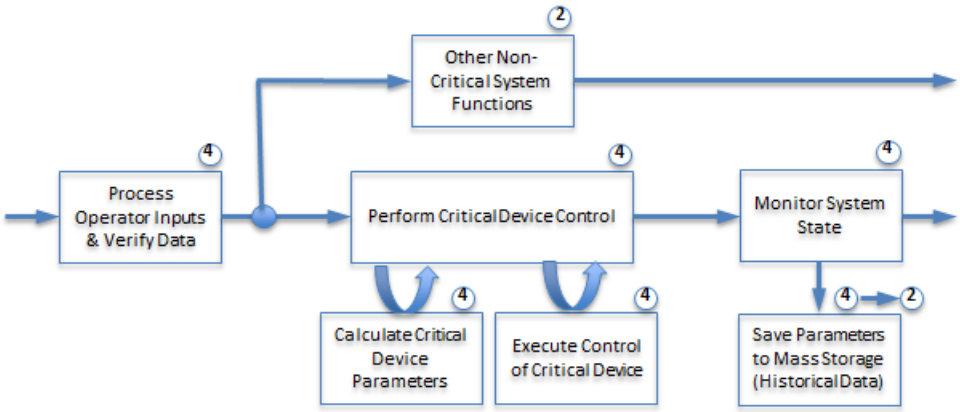
Supporting system functions in Figure K.1 are initially designated as low criticality and thus are assigned a system integrity level 2. However, the criticality analysis of the control flow logic diagram in the design stage clearly indicates that the supporting system functions of "Save" and "Retrieve" critical device parameters from the mass storage device have the possibility of modifying or altering the critical parameters. Thus, these supporting system functions are raised to the high system integrity level 4 so that the level 4 verification and validation tasks are conducted.

However, during the subsequent implementation stage (shown in Figure K.2), the developer has adopted an implementation technique whereby a "critical device controller" module is used to invoke the "calculate critical device parameters" and "execute control of critical devices" as subroutine calls. The critical parameters are passed parameters in the subroutine calls and thus eliminate the need to store and retrieve the critical data from a mass storage device. The storage of data on the mass storage device is later performed only for historical record keeping, and thus, the system integrity level is lowered from level 4 to level 2 being that it is no longer a critical execution function.




*Design Stage Functional Diagram Illustrating the Raising System Integrity Level for Critical Supporting System Functions* 2 → 4

**Figure K.1—Example of raising system criticality level**




*Implementation Stage Functional Diagram Illustrating the Lowering of System Integrity Level for Supporting System Functions* 4 → 2

**Figure K.2—Example of lowering system integrity level**

# Annex L

(informative)

# Mapping of ISO/IEC/IEEE 15288 and ISO/IEC 12207 process outcomes to verification and validation (V&V) tasks

**Table L.1—Mapping of ISO/IEC/IEEE 15288 technical process outcomes to V&V tasks**

| ISO/IEC/IEEE 15288 Business or Mission Analysis Process Outcomes | IEEE 1012 V&V Tasks Mapped to Outcomes |
|---|---|
| a) The problem or opportunity space is defined. | Activity 8.1.3 a) **Business or Mission Analysis V&V**<br>Task 1: Business or Mission Analysis Results Evaluation |
| b) The solution space is characterized. | Activity 8.1.3 a) **Business or Mission Analysis V&V**<br>Task 1: Business or Mission Analysis Results Evaluation<br>Task 4: Hazard Analysis<br>Task 5: Security Analysis<br>Task 6: Risk Analysis |
| c) Preliminary life cycle concepts are defined. | Activity 8.1.3 a) **Business or Mission Analysis V&V**<br>Task 2: Traceability Analysis |
| d) Candidate solution alternatives are identified and analyzed. | Activity 8.1.3 a) **Business or Mission Analysis V&V**<br>Task 1: Business or Mission Analysis Results Evaluation<br>Task 3: Criticality Analysis |
| e) The preferred candidate solution alternative(s) are selected. | Activity 8.1.3 a) **Business or Mission Analysis V&V**<br>Task 1: Business or Mission Analysis Results Evaluation<br>Task 2: Traceability Analysis |
| f) Any enabling systems or services needed for business or mission analysis are available. | Activity 8.1.3 a) **Business or Mission Analysis V&V**<br>Task 1: Business or Mission Analysis Results Evaluation |
| g) Traceability of business or mission problems and opportunities and the preferred alternative solution classes is established. | Activity 8.1.3 a) **Business or Mission Analysis V&V**<br>Task 2: Traceability Analysis |

| ISO/IEC/IEEE 15288 Stakeholder Needs and Requirements Definition Process Outcomes | IEEE 1012 V&V Tasks Mapped to Outcomes |
|---|---|
| a) Stakeholders of the system are identified. | Activity 8.2.3 a) **Stakeholder Needs and Requirements Definition V&V**<br>Task 1: Stakeholder Requirements Evaluation |
| b) Required characteristics and context of use of capabilities and life cycle concepts, including operational concepts, are defined. | Activity 8.2.3 a) **Stakeholder Needs and Requirements Definition V&V**<br>Task 1: Stakeholder Requirements Evaluation |
| c) Constraints on a system are identified. | Activity 8.2.3 a) **Stakeholder Needs and Requirements Definition V&V**<br>Task 1: Stakeholder Requirements Evaluation<br>Task 4: Hazard Analysis<br>Task 5: Security Analysis<br>Task 6: Risk Analysis |
| d) Stakeholder needs are defined. | Activity 8.2.3 a) **Stakeholder Needs and Requirements Definition V&V**<br>Task 1: Stakeholder Requirements Evaluation |

| | |
|---|---|
| e) Stakeholder needs are prioritized and transformed into clearly defined stakeholder requirements. | Activity 8.2.3 a) **Stakeholder Needs and Requirements Definition V&V**<br>Task 1: Stakeholder Requirements Evaluation<br>Task 2: Criticality Analysis |
| f) Critical performance measures are defined. | Activity 8.2.3 a) **Stakeholder Needs and Requirements Definition V&V**<br>Task 1: Stakeholder Requirements Evaluation<br>Task 2: Criticality Analysis |
| g) Stakeholder agreement that their needs and expectations are reflected adequately in the requirements is achieved. | Activity 8.2.3 a) **Stakeholder Needs and Requirements Definition V&V**<br>Task 1: Stakeholder Requirements Evaluation |
| h) Inputs for requirements of any enabling systems or system elements that serve the stakeholder needs and requirements activities are identified. | Activity 8.2.3 a) **Stakeholder Needs and Requirements Definition V&V**<br>Task 1: Stakeholder Requirements Evaluation |
| i) Any enabling systems or services needed for stakeholder needs and requirements are available. | Activity 8.2.3 a) **Stakeholder Needs and Requirements Definition V&V**<br>Task 1: Stakeholder Requirements Evaluation |
| j) Traceability of stakeholder requirements to stakeholders and their needs is established. | Activity 8.2.3 a) **Stakeholder Needs and Requirements Definition V&V**<br>Task 2: Traceability Analysis |

| **ISO/IEC/IEEE 15288 System Requirements Definition Process Outcomes** | **IEEE 1012 V&V Tasks Mapped to Outcomes** |
|---|---|
| a) The system description, including system interfaces, functions, and boundaries, for a system solution is defined. | Activity 8.3.3 a) **System Requirements Definition V&V**<br>Task 1: Requirements Evaluation<br>Task 2: Interface Analysis |
| b) System requirements (functional, performance, process, non-functional, and interface) and design constraints are defined. | Activity 8.3.3 a) **System Requirements Definition V&V**<br>Task 1: Requirements Evaluation<br>Task 2: Interface Analysis<br>Task 4: Criticality Analysis<br>Task 5: System Integration Test Plan V&V<br>Task 6: System Qualification Test Plan V&V<br>Task 7: System Acceptance Test Plan V&V<br>Task 8: Hazard Analysis<br>Task 9: Security Analysis<br>Task 10: Risk Analysis |
| c) Critical performance measures are defined. | Activity 8.3.3 a) **System Requirements Definition V&V**<br>Task 1: Requirements Evaluation<br>Task 2: Interface Analysis<br>Task 4: Criticality Analysis |
| d) The system requirements are analyzed. | Activity 8.1.3 a) **Stakeholder Needs and Requirements Definition V&V**<br>Task 1: Requirements Evaluation<br>Task 2: Interface Analysis |
| e) Inputs for requirements of any enabling systems or system elements that serve the system requirements definition activities are identified. | Activity 8.1.3 a) **Stakeholder Needs and Requirements Definition V&V**<br>Task 1: Requirements Evaluation<br>Task 2: Interface Analysis |

| | |
|---|---|
| f) Any enabling systems or services needed for system requirements definition are available. | Activity 8.1.3 a) **Stakeholder Needs and Requirements Definition V&V**<br>Task 1: Requirements Evaluation |
| g) Traceability of system requirements to stakeholder requirements is developed. | Activity 8.1.3 a) **Stakeholder Needs and Requirements Definition V&V**<br>Task 3: Traceability Analysis |

| ISO/IEC/IEEE 15288 Architecture Definition Process Outcomes | IEEE 1012 V&V Tasks Mapped to Outcomes |
|---|---|
| a) Identified stakeholder concerns are addressed by the architecture. | Activity 8.4.3 a) **Architecture Definition V&V**<br>Task 1: Architecture Evaluation |
| b) Architecture viewpoints are developed. | Activity 8.4.3 a) **Architecture Definition V&V**<br>Task 1: Architecture Evaluation |
| c) Context, boundaries, and external interfaces of the system are defined. | Activity 8.4.3 a) **Architecture Definition V&V**<br>Task 1: Architecture Evaluation<br>Task 2: Interface Analysis<br>Task 5: System Integration Test Design V&V<br>Task 6: System Qualification Test Design V&V<br>Task 7: System Acceptance Test Design V&V<br>Task 8: Hazard Analysis<br>Task 9: Security Analysis<br>Task 10: Risk Analysis |
| d) Architecture views and models of the system are developed. | Activity 8.4.3 a) **Architecture Definition V&V**<br>Task 1: Architecture Evaluation |
| e) Concepts, properties, characteristics, behaviors, functions, and/or constraints that are significant to architecture decisions of the system are allocated to architectural entities. | Activity 8.4.3 a) **Architecture Definition V&V**<br>Task 1: Architecture Evaluation<br>Task 2: Interface Analysis |
| f) System elements and their interfaces are identified. | Activity 8.4.3 a) **Architecture Definition V&V**<br>Task 1: Architecture Evaluation<br>Task 2: Interface Analysis |
| g) Architecture candidates are assessed. | Activity 8.4.3 a) **Architecture Definition V&V**<br>Task 1: Architecture Evaluation<br>Task 2: Interface Analysis<br>Task 8: Hazard Analysis<br>Task 9: Security Analysis<br>Task 10: Risk Analysis |
| h) An architectural basis for processes throughout the life cycle is achieved. | Activity 8.4.3 a) **Architecture Definition V&V**<br>Task 1: Architecture Evaluation<br>Task 4: Criticality Analysis |
| i) Alignment of the architecture with requirements and design characteristics is achieved. | Activity 8.4.3 a) **Architecture Definition V&V**<br>Task 1: Architecture Evaluation<br>Task 3: Traceability Analysis |
| j) Any enabling systems or services needed for architecture definition are available. | Activity 8.4.3 a) **Architecture Definition V&V**<br>Task 1: Architecture Evaluation |
| k) Traceability of architecture elements to stakeholder and system requirements is developed. | Activity 8.4.3 a) **Architecture Definition V&V**<br>Task 3: Traceability Analysis |

| ISO/IEC/IEEE 15288 Design Definition Process Outcomes | IEEE 1012 V&V Tasks Mapped to Outcomes |
|---|---|
| a) Design characteristics of each system element are defined. | Activity 8.5.3 a) **Design Definition V&V**<br>Task 1: Design Evaluation |
| b) System requirements are allocated to system elements. | Activity 8.5.3 a) **Design Definition V&V**<br>Task 1: Design Evaluation<br>Task 2: Interface Analysis<br>Task 3: Traceability Analysis |
| c) Design enablers necessary for design definition are selected or defined. | Activity 8.5.3 a) **Design Definition V&V**<br>Task 1: Design Evaluation<br>Task 5: System Integration Test Design V&V<br>Task 6: System Qualification Test Design V&V<br>Task 7: System Acceptance Test Design V&V<br>Task 8: Hazard Analysis<br>Task 9: Security Analysis<br>Task 10: Risk Analysis |
| d) Interfaces between system elements composing the system are defined or consolidated. | Activity 8.5.3 a) **Design Definition V&V**<br>Task 1: Design Evaluation<br>Task 2: Interface Analysis |
| e) Design artifacts are developed. | Activity 8.5.3 a) **Design Definition V&V**<br>Task 1: Design Evaluation<br>Task 2: Interface Analysis |
| f) Any enabling systems or services needed for design definition are available. | Activity 8.5.3 a) **Design Definition V&V**<br>Task 1: Design Evaluation |
| g) Traceability of the design characteristics to the architectural elements of the system architecture is established. | Activity 8.5.3 a) **Design Definition V&V**<br>Task 3: Traceability Analysis |

| ISO/IEC/IEEE 15288 System Analysis Process Outcomes | IEEE 1012 V&V Tasks Mapped to Outcomes |
|---|---|
| a) System analyses needed are identified. | Activity 8.6.3 a) **System Analysis V&V:**<br>Task 1: System Analysis Strategy Evaluation |
| b) System analysis assumptions and results are validated. | Activity 8.6.3 a) **System Analysis V&V:**<br>Task 1: System Analysis Strategy Evaluation |
| c) System analysis results are provided for decisions. | Activity 8.6.3 a) **System Analysis V&V:**<br>Task 2: System Analysis Results Evaluation |
| d) Inputs for requirements of any enabling systems or system elements that serve the system analysis activities are identified. | Activity 8.6.3 a) **System Analysis V&V:**<br>Task 1: System Analysis Strategy Evaluation |
| e) Any enabling systems or services needed for system analysis are available. | Activity 8.6.3 a) **System Analysis V&V:**<br>Task 1: System Analysis Strategy Evaluation |

| ISO/IEC/IEEE 15288 Implementation Process Outcomes | IEEE 1012 V&V Tasks Mapped to Outcomes |
|---|---|
| a) Implementation constraints that influence the requirements, architecture, or design are identified. | Activity 8.7.3 a) **Implementation V&V**<br>Task 1: Implementation Strategy Assessment<br>Task 7: Hazard Analysis<br>Task 8: Security Analysis<br>Task 9: Risk Analysis |

| | |
|---|---|
| b) A system element is realized. | Activity 8.7.3 a) **Implementation V&V**<br>Task 2: System Element Implementation Analysis<br>Task 3: Criticality Analysis<br>Task 4: System Integration Test Case V&V<br>Task 5: System Qualification Test Case V&V<br>Task 6: System Acceptance Test Case V&V |
| c) A system element is packaged or stored. | Activity 8.7.3 a) **Implementation V&V**<br>Task 2: System Element Implementation Analysis |
| d) Inputs for requirements of any enabling systems or system elements that serve the implementation activities are identified. | Activity 8.7.3 a) **Implementation V&V**<br>Task 1: Implementation Strategy Assessment |
| e) Any enabling systems or services needed for implementation are available. | Activity 8.7.3 a) **Implementation V&V**<br>Task 2: System Element Implementation Analysis |
| f) Traceability is established. | Activity 8.7.3 a) **Implementation V&V**<br>Task 2: System Element Implementation Analysis |

| ISO/IEC/IEEE 15288 Integration Process Outcomes | IEEE 1012 V&V Tasks Mapped to Outcomes |
|---|---|
| a) Integration constraints that influence system requirements, architecture, or design, including interfaces, are identified. | Activity 8.8.3 a) **Integration V&V**<br>Task 1: System Integration Strategy Assessment<br>Task 2: System Integration Test Procedure V&V<br>Task 4: System Qualification Test Procedure V&V<br>Task 6: System Acceptance Test Procedure V&V |
| b) Approach and check points for the correct operation of the assembled interfaces and system functions are defined. | Activity 8.8.3 a) **Integration V&V**<br>Task 2: System Integration Test Procedure V&V<br>Task 4: System Qualification Test Procedure V&V<br>Task 6: System Acceptance Test Procedure V&V |
| c) Inputs for requirements of any enabling systems or system elements that serve the integration activities are identified. | Activity 8.8.3 a) **Integration V&V**<br>Task 2: System Integration Test Procedure V&V<br>Task 4: System Qualification Test Procedure V&V<br>Task 6: System Acceptance Test Procedure V&V |
| d) Any enabling systems or services needed for integration are available. | Activity 8.8.3 a) **Integration V&V**<br>Task 3: System Integration Test Execution V&V<br>Task 5: System Qualification Test Execution V&V |
| e) A system composed of implemented system elements is integrated. | Activity 8.8.3 a) **Integration V&V**<br>Task 3: System Integration Test Execution V&V<br>Task 5: System Qualification Test Execution V&V |
| f) The interfaces between the implemented system elements that compose the system are confirmed. | Activity 8.8.3 a) **Integration V&V**<br>Task 3: System Integration Test Execution V&V<br>Task 5: System Qualification Test Execution V&V |
| g) The interfaces between the system and the external environment are confirmed. | Activity 8.8.3 a) **Integration V&V**<br>Task 3: System Integration Test Execution V&V<br>Task 5: System Qualification Test Execution V&V |
| h) Anomalies due to integration activities are recorded. | Activity 8.8.3 a) **Integration V&V**<br>Task 3: System Integration Test Execution V&V<br>Task 5: System Qualification Test Execution V&V |

| ISO/IEC/IEEE 15288 Verification Process Outcomes | IEEE 1012 V&V Tasks Mapped to Outcomes |
|---|---|
| a) Constraints of verification that influence the requirements, architecture, or design are identified. | **Activity 7.1.3 a) V&V Management**<br>Task 1: VVP Generation<br>Task 2: Interface with Other Processes |
| b) Inputs for requirements of any enabling systems or system elements that serve the verification activities are identified. | **Activity 7.1.3 a) V&V Management**<br>Task 1: VVP Generation<br>Task 2: Interface with Other Processes |
| c) Any enabling systems or services needed for verification are available. | **Activity 7.1.3 a) V&V Management**<br>Task 4: Management Review of the V&V Effort |
| d) The system or system elements are verified. | The system verification activities and tasks in Table 1b and the common verification activities and tasks in Table 1a are the activities and tasks needed to perform system verification. |
| e) Data providing information for corrective actions is reported. | Task report outputs in Table 1b and Table 1a |
| f) Objective evidence that the realized system fulfils the requirements, architecture, and design is provided. | Task report outputs in Table 1b and Table 1a |
| g) Traceability of the verified system elements is established. | All traceability analysis tasks in System V&V |

| ISO/IEC/IEEE 15288 Transition Process Outcomes | IEEE 1012 V&V Tasks Mapped to Outcomes |
|---|---|
| a) Transition constraints that influence system requirements, architecture, or design are identified. | **Activity 8.10.3 a) Transition V&V**<br>Task 1: Transition Strategy Assessment |
| b) Any enabling systems or services needed for transition are available. | **Activity 8.10.3 a) Transition V&V**<br>Task 1: Transition Strategy Assessment |
| c) The site is prepared. | **Activity 8.10.3 a) Transition V&V**<br>Task 2: Transition Demonstration Assessment |
| d) The system installed in its operational location is capable of delivering its specified functions. | **Activity 8.10.3 a) Transition V&V**<br>Task 2: Transition Demonstration Assessment<br>Task 3: System Acceptance Test Execution V&V |
| e) Operators, users, and other stakeholders necessary to the system utilization and support are trained. | **Activity 8.10.3 a) Transition V&V**<br>Task 2: Transition Demonstration Assessment |
| f) The installed system is activated and ready for operation. | **Activity 8.10.3 a) Transition V&V**<br>Task 2: Transition Demonstration Assessment<br>Task 3: System Acceptance Test Execution V&V |
| g) Traceability of the transitioned elements is established. | **Activity 8.10.3 a) Transition V&V**<br>Task 3: System Acceptance Test Execution V&V |

| ISO/IEC/IEEE 15288 Validation Process Outcomes | IEEE 1012 V&V Tasks Mapped to Outcomes |
|---|---|
| a) Validation criteria for stakeholder requirements are defined. | **Activity 8.2.3 a) Stakeholder Needs and Requirements Definition V&V**<br>Task 1: Stakeholder Requirements Evaluation<br>**Activity 8.3.3 a) System Requirements Definition V&V**<br>Task 6: System Qualification Test Plan V&V<br>Task 7: System Acceptance Test Plan V&V |

| | |
|---|---|
| b) The availability of services required by stakeholders is confirmed. | The system validation activities and tasks in Table 1b and the common validation activities and tasks in Table 1a are the activities and tasks needed to perform system validation. |
| c) Constraints of validation that influence the requirements, architecture, or design are identified. | **Activity 7.1.3 a) V&V Management**<br>Task 1: VVP Generation<br>Task 2: Interface with Other Processes |
| d) The system or system element is validated. | The system validation activities and tasks in Table 1b and the common validation activities and tasks in Table 1a are the activities and tasks needed to perform system validation. |
| e) Any enabling systems or services needed for validation are available. | **Activity 7.1.3 a) V&V Management**<br>Task 4: Management Review of the V&V Effort |
| f) Validation results and anomalies are recorded. | Task report outputs in Table 1b and Table 1a |
| g) Objective evidence that the realized system satisfies stakeholder needs is provided. | Task report outputs in Table 1b and Table 1a |
| h) Traceability of the verified system elements is established. | All traceability analysis tasks in System V&V |

| ISO/IEC/IEEE 15288 Operation Process Outcomes | IEEE 1012 V&V Tasks Mapped to Outcomes |
|---|---|
| a) Operation constraints that influence system requirements, architecture, or design are identified. | **Activity 8.12.3 a) Operation V&V**<br>Task 1: Operating Procedures Evaluation<br>Task 2: Hazard Analysis<br>Task 3: Security Analysis<br>Task 4: Risk Analysis |
| b) Any enabling systems, services, and material needed for operation are available. | **Activity 8.12.3 a) Operation V&V**<br>Task 1: Operating Procedures Evaluation |
| c) Trained, qualified operators are available. | N/A |
| d) System services that meet stakeholder requirements are delivered. | **Activity 8.12.3 a) Operation V&V**<br>Task 1: Operating Procedures Evaluation<br>Task 2: Hazard Analysis<br>Task 3: Security Analysis<br>Task 4: Risk Analysis |
| e) System performance during operation is monitored. | N/A |
| f) Customer satisfaction is provided. | **Activity 8.12.3 a) Operation V&V**<br>Recursive application of prior stage V&V analysis, evaluation, assessments, or test of any stakeholder requirements to verify and validate that stakeholder satisfaction is maintained. |

| ISO/IEC/IEEE 15288 Maintenance Process Outcomes | IEEE 1012 V&V Tasks Mapped to Outcomes |
|---|---|
| a) Maintenance constraints that influence system requirements, architecture, or design are identified. | **Activity 8.13.3 a) Maintenance V&V**<br>Task 1: System Maintenance Strategy Assessment |
| b) Any enabling systems or services needed for maintenance are available. | **Activity 8.13.3 a) Maintenance V&V**<br>Task 2: System Maintenance Execution Assessment |
| c) Replacement, repaired, or revised system elements are made available. | **Activity 8.13.3 a) Maintenance V&V**<br>Task 2: System Maintenance Execution Assessment |

| | |
|---|---|
| d) The need for changes to the system requirements, architecture, or design to address corrective, perfective, or adaptive maintenance is reported. | Activity 8.13.3 a) **Maintenance V&V**<br>Task 2: System Maintenance Execution Assessment |
| e) Failure and lifetime data, including associated costs, is recorded. | Activity 8.13.3 a) **Maintenance V&V**<br>Task 2: System Maintenance Execution Assessment |

| ISO/IEC/IEEE 15288 Disposal Process Outcomes | IEEE 1012 V&V Tasks Mapped to Outcomes |
|---|---|
| a) Disposal constraints are provided as inputs to requirements, architecture, design, and implementation. | Activity 8.14.3 a) **Disposal V&V**<br>Task 1: Disposal Plan Evaluation |
| b) Any enabling systems or services needed for disposal are available. | Activity 8.14.3 a) **Disposal V&V**<br>Task 1: Disposal Plan Evaluation |
| c) The system elements or waste products are destroyed, stored, reclaimed, or recycled in accordance with safety and security requirements. | N/A |
| d) The environment is returned to its original or an agreed state. | N/A |
| e) Records of disposal actions and analysis are available. | N/A |

**Table L.2—Mapping of ISO/IEC 12207 Process Outcomes to V&V Tasks**

| ISO/IEC 12207 Software Requirements Analysis Process Outcomes | IEEE 1012 V&V Tasks Mapped to Outcomes |
|---|---|
| a) The requirements allocated to the software elements of the system and their interfaces are defined. | Activity 9.1.3 a) **Software Concept V&V**<br>Task 1: Concept Documentation Evaluation<br>Task 2: Requirements Allocation Analysis<br>Task 5: Hazard Analysis<br>Task 6: Security Analysis<br>Task 7: Risk Analysis<br><br>Activity 9.2.3 a) **Software Requirements Analysis V&V**<br>Task 1: Requirements Evaluation<br>Task 2: Interface Analysis<br>Task 7: Hazard Analysis<br>Task 8: Security Analysis<br>Task 9: Risk Analysis |
| b) Software requirements are analyzed for correctness and testability. | Activity 9.1.3 a) **Software Concept V&V**<br>Task 1: Concept Documentation Evaluation<br>Task 2: Requirements Allocation Analysis<br>Task 5: Hazard Analysis<br>Task 6: Security Analysis<br>Task 7: Risk Analysis<br><br>Activity 9.2.3 a) **Software Requirements Analysis V&V**<br>Task 1: Requirements Evaluation |

| | |
|---|---|
| | Task 2: Interface Analysis<br>Task 5: Software Qualification Test Plan V&V<br>Task 6: Software Acceptance Test Plan V&V<br>Task 7: Hazard Analysis<br>Task 8: Security Analysis<br>Task 9: Risk Analysis |
| c) The impact of software requirements on the operating environment is understood. | **Activity 9.1.3 a) Software Concept V&V**<br>Task 1: Concept Documentation Evaluation<br>Task 2: Requirements Allocation Analysis<br>Task 5: Hazard Analysis<br>Task 6: Security Analysis<br>Task 7: Risk Analysis<br><br>**Activity 9.2.3 a) Software Requirements Analysis V&V**<br>Task 1: Requirements Evaluation<br>Task 2: Interface Analysis<br>Task 5: Software Qualification Test Plan V&V<br>Task 6: Software Acceptance Test Plan V&V<br>Task 7: Hazard Analysis<br>Task 8: Security Analysis<br>Task 9: Risk Analysis |
| d) Consistency and traceability are established between the software requirements and system requirements. | **Activity 9.1.3 a) Software Concept V&V**<br>Task 3: Traceability Analysis<br><br>**Activity 9.2.3 a) Software Requirements Analysis V&V**<br>Task 3: Traceability Analysis |
| e) Prioritization for implementing the software requirements is defined. | **Activity 9.1.3 a) Software Concept V&V**<br>Task 4: Criticality Analysis<br><br>**Activity 9.2.3 a) Software Requirements Analysis V&V**<br>Task 4: Criticality Analysis |
| f) The software requirements are approved and updated as needed. | **Activity 9.1.3 a) Software Concept V&V**<br>Task 1: Concept Documentation Evaluation<br>Task 2: Requirements Allocation Analysis<br>Task 3: Traceability Analysis<br>Task 4: Criticality Analysis<br>Task 5: Hazard Analysis<br>Task 6: Security Analysis<br>Task 7: Risk Analysis<br><br>**Activity 9.2.3 a) Software Requirements Analysis V&V**<br>Task 1: Requirements Evaluation<br>Task 2: Interface Analysis<br>Task 3: Traceability Analysis<br>Task 4: Criticality Analysis |

| | |
|---|---|
| | Task 5: Software Qualification Test Plan V&V<br>Task 6: Software Acceptance Test Plan V&V<br>Task 7: Hazard Analysis<br>Task 8: Security Analysis<br>Task 9: Risk Analysis |
| g) Changes to the software requirements are evaluated for cost, schedule, and technical impact. | **Activity 9.1.3 a) Software Concept V&V**<br>Task 1: Concept Documentation Evaluation<br>Task 2: Requirements Allocation Analysis<br>Task 3: Traceability Analysis<br>Task 4: Criticality Analysis<br>Task 5: Hazard Analysis<br>Task 6: Security Analysis<br>Task 7: Risk Analysis<br><br>**Activity 9.2.3 a) Software Requirements Analysis V&V**<br>Task 1: Requirements Evaluation<br>Task 2: Interface Analysis<br>Task 3: Traceability Analysis<br>Task 4: Criticality Analysis<br>Task 5: Software Qualification Test Plan V&V<br>Task 6: Software Acceptance Test Plan V&V<br>Task 7: Hazard Analysis<br>Task 8: Security Analysis<br>Task 9: Risk Analysis |
| h) The software requirements are baselined and communicated to all affected parties. | N/A |

| ISO/IEC 12207 Software Architectural Design Process Outcomes | IEEE 1012 V&V Tasks Mapped to Outcomes |
|---|---|
| a) A software architectural design is developed and baselined that describes the software items that will implement the software requirements. | **Activity 9.3.3 a) Software Design V&V**<br>Task 1: Design Evaluation<br>Task 4: Criticality Analysis<br>Task 11: Hazard Analysis<br>Task 12: Security Analysis<br>Task 13: Risk Analysis |
| b) Internal and external interfaces of each software item are defined. | **Activity 9.3.3 a) Software Design V&V**<br>Task 1: Design Evaluation<br>Task 2: Interface Analysis<br>Task 3: Traceability Analysis |
| c) Consistency and traceability are established between software requirements and software design. | **Activity 9.3.3 a) Software Design V&V**<br>Task 1: Design Evaluation<br>Task 3: Traceability Analysis<br>Task 9: Software Qualification Test Design V&V<br>Task 10: Software Acceptance Test Design V&V |

| ISO/IEC 12207 Software Detailed Design Process Outcomes | IEEE 1012 V&V Tasks Mapped to Outcomes |
|---|---|
| a) A detailed design of each software component describing the software units to be built is developed. | **Activity 9.3.3 a) Software Design V&V**<br>Task 1: Design Evaluation<br>Task 4: Criticality Analysis<br>Task 11: Hazard Analysis<br>Task 12: Security Analysis<br>Task 13: Risk Analysis |
| b) External interfaces of each software unit are defined. | **Activity 9.3.3 a) Software Design V&V**<br>Task 1: Design Evaluation<br>Task 2: Interface Analysis<br>Task 3: Traceability Analysis |
| c) Consistency and traceability are established between detailed design and the requirements and architectural design. | **Activity 9.3.3 a) Software Design V&V**<br>Task 1: Design Evaluation<br>Task 3: Traceability Analysis<br>Task 5: Software Component Test Plan V&V<br>Task 6: Software Integration Test Plan V&V<br>Task 7: Software Component Test Design V&V<br>Task 8: Software Integration Test Design V&V<br>Task 9: Software Qualification Test Design V&V<br>Task 10: Software Acceptance Test Design V&V |

| ISO/IEC 12207 Software Construction Process Outcomes | IEEE 1012 V&V Tasks Mapped to Outcomes |
|---|---|
| a) Verification criteria are defined for all software units against their requirements. | **Activity 9.4.3 a) Software Construction V&V**<br>Task 1: Source Code and Source Code Documentation Evaluation<br>Task 2: Interface Analysis<br>Task 4: Criticality Analysis<br>Task 5: Software Component Test Case V&V<br>Task 9: Software Component Test Procedures V&V<br>Task 12: Software Component Test Execution V&V<br>Task 13: Hazard Analysis<br>Task 14: Security Analysis<br>Task 15: Risk Analysis |
| b) Software units defined by design are produced. | **Activity 9.4.3 a) Software Construction V&V**<br>Task 1: Source Code and Source Code Documentation Evaluation<br>Task 2: Interface Analysis<br>Task 5: Software Component Test Case V&V<br>Task 9: Software Component Test Procedures V&V<br>Task 12: Software Component Test Execution V&V |
| c) Consistency and traceability are established between the software units and the requirements and design. | **Activity 9.4.3 a) Software Construction V&V**<br>Task 3: Traceability Analysis |
| d) Verification of the software units against the requirements and the design is accomplished. | **Activity 9.4.3 a) Software Construction V&V**<br>Task 1: Source Code and Source Code Documentation Evaluation<br>Task 2: Interface Analysis |

| | |
|---|---|
| | Task 3: Traceability Analysis<br>Task 5: Software Component Test Case V&V<br>Task 6: Software Integration Test Case V&V<br>Task 7: Software Qualification Test Case V&V<br>Task 8: Software Acceptance Test Case V&V<br>Task 9: Software Component Test Procedure V&V<br>Task 10: Software Integration Test Procedure V&V<br>Task 11: Software Qualification Test Procedure V&V<br>Task 12: Software Component Test Execution V&V |

| ISO/IEC 12207 Software Integration Process Outcomes | IEEE 1012 V&V Tasks Mapped to Outcomes |
|---|---|
| a) An integration strategy is developed for software units consistent with software design and the prioritized software requirements. | **Activity 9.3.3 a) Software Design V&V**<br>Task 6: Software Integration Test Case V&V<br>Task 10: Software Integration Test Procedure V&V<br><br>**Activity 9.4.3 a) Software Construction V&V**<br>Task 10: Software Integration Test Procedure V&V<br><br>**Activity 9.5.3 a) Software Integration V&V**<br>Task 2: Traceability Analysis |
| b) Verification criteria for software items are developed to determine compliance with the software requirements allocated to the item. | **Activity 9.3.3 a) Software Design V&V**<br>Task 6: Software Integration Test Plan V&V<br>Task 8: Software Integration Test Design V&V<br><br>**Activity 9.4.3 a) Software Construction V&V**<br>Task 6: Software Integration Test Case V&V<br>Task 10: Software Integration Test Procedure V&V<br><br>**Activity 9.5.3 a) Software Integration V&V**<br>Task 2: Traceability Analysis<br>Task 3: Hazard Analysis<br>Task 4: Security Analysis<br>Task 5: Risk Analysis |
| c) Software items are verified using the defined criteria. | **Activity 9.5.3 a) Software Integration V&V**<br>Task 1: Software Integration Test Execution V&V |
| d) Software items that are defined by the integration strategy are produced. | **Activity 9.5.3 a) Software Integration V&V**<br>Task 1: Software Integration Test Execution V&V |
| e) Results of integration testing are recorded. | **Activity 9.5.3 a) Software Integration V&V**<br>Task 1: Software Integration Test Execution V&V |
| f) Consistency and traceability are established between software design and software items. | **Activity 9.5.3 a) Software Integration V&V**<br>Task 2: Traceability Analysis |
| g) A regression strategy is developed and applied for re-verifying software items when a change in software units (including associated requirements, design, and code) occur. | **Activity 7.1.3 a) V&V Management**<br>Task 3: Proposed/Baseline Change Assessment |

| ISO/IEC 12207 Software Qualification Testing Process Outcomes | IEEE 1012 V&V Tasks Mapped to Outcomes |
|---|---|
| a) Criteria for the integrated software are developed that demonstrate compliance with the software requirements. | **Activity 9.2.3 a) Software Requirements Analysis V&V**<br>Task 5: Software Qualification Test Plan V&V<br><br>**Activity 9.3.3 a) Software Design V&V**<br>Task 9: Software Qualification Test Design V&V<br><br>**Activity 9.4.3 a) Software Construction V&V**<br>Task 7: Software Qualification Test Case V&V<br>Task 11: Software Qualification Test Procedures V&V<br><br>**Activity 9.6.3 a) Software Qualification Testing V&V**<br>Task 2: Traceability Analysis<br>Task 3: Hazard Analysis<br>Task 4: Security Analysis<br>Task 5: Risk Analysis |
| b) Integrated software is verified using the defined criteria. | **Activity 9.6.3 a) Software Qualification Testing V&V**<br>Task 1: Software Qualification Test Execution V&V |
| c) Test results are recorded. | **Activity 9.6.3 a) Software Qualification Testing V&V**<br>Task 1: Software Qualification Test Execution V&V |
| d) A regression strategy is developed and applied for re-testing the integrated software when a change in software items is made. | **Activity 7.1.3 a) V&V Management**<br>Task 3: Proposed/Baseline Change Assessment |

| ISO/IEC 12207 Software Installation Process Outcomes | IEEE 1012 V&V Tasks Mapped to Outcomes |
|---|---|
| a) A software installation strategy is developed. | **Activity 9.9.3 a) Software Installation and Checkout V&V**<br>Task 1: Installation Configuration Audit<br>Task 2: Installation Checkout |
| b) Criteria for software installation are developed that demonstrate compliance with the software installation requirements. | **Activity 9.9.3 a) Software Installation and Checkout V&V**<br>Task 1: Installation Configuration Audit<br>Task 2: Installation Checkout<br>Task 3: Hazard Analysis<br>Task 4: Security Analysis<br>Task 5: Risk Analysis |
| c) The software product is installed in the target environment. | **Activity 9.9.3 a) Software Installation and Checkout V&V**<br>Task 1: Installation Configuration Audit<br>Task 2: Installation Checkout |
| d) Readiness of the software product for use in its intended environment is assured. | **Activity 9.9.3 a) Software Installation and Checkout V&V**<br>Task 1: Installation Configuration Audit<br>Task 2: Installation Checkout<br>Task 3: Hazard Analysis<br>Task 4: Security Analysis<br>Task 5: Risk Analysis |

| ISO/IEC 12207 Software Acceptance Support Process Outcomes | IEEE 1012 V&V Tasks Mapped to Outcomes |
|---|---|
| a) The product is completed and delivered to the acquirer. | **Activity 9.7.3 a) Software Acceptance Testing V&V**<br>Task 2: Software Acceptance Test Execution V&V |
| b) Acquirer acceptance tests and reviews are supported. | **Activity 9.2.3 a) Software Requirements Analysis V&V**<br>Task 6: Software Acceptance Test Plan V&V<br><br>**Activity 9.3.3 a) Software Design V&V**<br>Task 10: Software Acceptance Test Design V&V<br><br>**Activity 9.4.3 a) Software Construction V&V**<br>Task 8: Software Acceptance Test Case V&V<br><br>**Activity 9.7.3 a) Software Acceptance Testing V&V**<br>Task 1: Software Acceptance Test Procedure V&V<br>Task 2: Software Acceptance Test Execution V&V<br>Task 3: Traceability Analysis<br>Task 4: Hazard Analysis<br>Task 5: Security Analysis<br>Task 6: Risk Analysis |
| c) The product is put into operation in the customer's environment. | **Activity 9.9.3 a) Software Installation and Checkout V&V**<br>Task 1: Installation Configuration Audit<br>Task 2: Installation Checkout |
| d) Problems detected during acceptance are identified and communicated to those responsible for resolution. | **Activity 9.7.3 a) Software Acceptance Testing V&V**<br>Task 2: Software Acceptance Test Execution V&V |

| ISO/IEC 12207 Software Operation Process Outcomes | IEEE 1012 V&V Tasks Mapped to Outcomes |
|---|---|
| a) An operation strategy is defined. | **Activity 9.11.3 a) Software Operation V&V**<br>Task 2: Operating Procedures Evaluation |
| b) Conditions for correct operation of the software in its intended environment are identified and evaluated. | **Activity 9.11.3 a) Software Operation V&V**<br>Task 1: Evaluation of New Constraints<br>Task 2: Operating Procedures Evaluation<br>Task 3: Hazard Analysis<br>Task 4: Security Analysis<br>Task 5: Risk Analysis |
| c) The software is tested and determined to operate in its intended environment. | **Activity 9.7.3 a) Software Acceptance Testing V&V**<br>Task 2: Software Acceptance Test Execution V&V |
| d) Software is operated in its intended environment. | **Activity 9.11.3 a) Software Operation V&V**<br>Task 1: Evaluation of New Constraints<br>Task 2: Operating Procedures Evaluation<br>Task 3: Hazard Analysis<br>Task 4: Security Analysis<br>Task 5: Risk Analysis |
| e) Assistance and consultation is provided to the customers of the software product in accordance with the agreement. | N/A |

| ISO/IEC 12207 Software Maintenance Process Outcomes | IEEE 1012 V&V Tasks Mapped to Outcomes |
|---|---|
| a) A maintenance strategy is developed to manage the modification and migration of products according to the release strategy. | Activity 9.12.3 a) **Software Maintenance V&V**<br>Task 1: VVP Revision<br>Task 3: Criticality Analysis<br>Task 4: Migration Assessment<br>Task 5: Retirement Assessment |
| b) The impact of changes to the existing system on organization, operations, or interfaces is identified. | Activity 9.12.3 a) **Software Maintenance V&V**<br>Task 2: Anomaly Evaluation<br>Task 3: Criticality Analysis<br>Task 4: Migration Assessment<br>Task 5: Retirement Assessment<br>Task 6: Hazard Analysis<br>Task 7: Security Analysis<br>Task 8: Risk Analysis<br>Task 9: Task Iteration |
| c) Affected system and software documentation is updated as needed. | Activity 9.12.3 a) **Software Maintenance V&V**<br>Task 9: Task Iteration |
| d) Modified products are developed with associated tests that demonstrate that requirements are not compromised. | Activity 9.12.3 a) **Software Maintenance V&V**<br>Task 9: Task Iteration |
| e) Product upgrades are migrated to the customer's environment. | Activity 9.12.3 a) **Software Maintenance V&V**<br>Task 9: Task Iteration |
| f) The system software modification is communicated to all affected parties. | N/A |

| ISO/IEC 12207 Software Disposal Process Outcomes | IEEE 1012 V&V Tasks Mapped to Outcomes |
|---|---|
| a) A software disposal strategy is defined. | Activity 9.13.3 a) **Software Disposal V&V**<br>Task 1: Software Disposal V&V |
| b) Disposal constraints are provided as inputs to requirements. | Activity 9.13.3 a) **Software Disposal V&V**<br>Task 1: Software Disposal V&V |
| c) The system's software elements are destroyed or stored. | N/A |
| d) The environment is left in an agreed-on state. | Activity 9.13.3 a) **Software Disposal V&V**<br>Task 1: Software Disposal V&V |
| e) Records allowing knowledge retention of disposal actions and any analysis of long-term impacts are available. | Activity 9.13.3 a) **Software Disposal V&V**<br>Task 1: Software Disposal V&V |

# Annex M

(informative)

## Verification and validation (V&V) of $n^{th}$ of a kind systems

There may come a time where the same system is needed in multiple instances and therefore needs to be copied and installed numerous times to satisfy stakeholder needs. Examples include installing a redundant system for training, development, or continuous operation purposes; a second or third unit of a power plant with the same specifications; or manufacturing the same system for different customers under different projects. This copy of a system is often referred to as an "$n^{th}$ of a kind system."

The initial system design representing an identifiable set of functional and performance requirements and its implementation is defined as the first application. An $n^{th}$ of a kind system is defined as a re-manufacturing or re-installation of this first application. Consideration of what constitutes a first application versus an $n^{th}$ application needs to take into consideration the functional and performance requirements for the project as well as the regulatory environment. Any significant differences should cause the project to be considered a first application. For a system of interest to be determined as an "$n^{th}$ of a kind system," it needs to be an identical copy of a system that has been previously verified and validated, with an identical operating and regulatory environment. In this case, there would be no further V&V tasks needed beyond those to provide the body of evidence that the system and environment are identical.

The first application performs the entire V&V activities including testing for the hardware, software, and integration per this standard. All applications require demonstration of required V&V activities performed. However, to the extent that the design does not change from application to application (i.e., $n^{th}$ of a kind system) these activities do not necessarily need to be repeated. Therefore, required V&V activities on an $n^{th}$ of a kind system may be greatly reduced since the V&V plan could take credit for the previous life cycle activities performed on the first application system. A regression analysis of the requirements and the system/hardware/software design and implementation should be performed to demonstrate that the $n^{th}$ of a kind system application is identical to the first application in all relevant aspects.

Even when all design requirements and specifications were identical and previously verified, and the first application was implemented and tested to validate functional and performance requirements, the target hardware components for the $n^{th}$ of a kind system are likely to be procured and integrated separately from the first application. Hardware is subject to errors being introduced in the manufacturing process; hence, hardware testing is performed on each system instance to prove correctness. This necessitates a certain level of manufacturing and factory testing on each of the subsequent copies to validate the system was integrated correctly and continues to meet the performance requirements with the new set of hardware used in that particular copy. Additional testing and/or analyses may need to be performed on each copy of the $n^{th}$ of a kind system. For identical systems, these tests are expected to be focusing on correct integration and installation rather than a repeat of functional tests previously performed on the first application. Analysis may be performed to conclude equivalency of hardware components, for instance, when a hardware component needs to be replaced with another from a different manufacturer due to obsolescence or procurement issues. Software, on the other hand, can be installed from configuration managed files and remain identical to the reference system. The compilation and final load assembly tools used need to be identical, as different or updated compiler and load file generators may create minor alterations to the final object code. Regression analysis is performed to confirm that the software and software tools are identical in all relevant aspects.

A regression analysis is defined as a series of activities performed under configuration management that demonstrates the two implementations are identical, or identifies the differences between the implementations that need to be justified or re-qualified through further V&V activities. To confirm the

system is equivalent to that of the first application, the V&V activities for the n$^{th}$ of a kind system should consider:

- Equivalency of hardware (e.g., batch and version controlled, performance specifications),
- Equivalency of hardware qualifications (e.g., seismic evaluations, electromagnetic compatibility, temperature, humidity evaluations),
- Equivalency of software (e.g., cyclic redundancy code checks, configuration, version control),
- Location and orientation of the follow-on systems' installation (i.e., operating environment), and
- Regulatory environment (e.g., demands from licensing authorities and the customer).

The n$^{th}$ of a kind system developer should also implement processes to support change notices and updates to correct identified deficiencies in any of the installations, and have a means to keep track of system configurations after their delivery.

The regression analysis may also show that the two systems are not identical per the strict definition of n$^{th}$ of a kind system. However, depending on the differences between the first application (reference system) and its next implementation with certain level of differences/customization (repeat system), the V&V activities previously performed on the reference system may still be applicable and can be mapped to the life cycle activities of the repeat system. If these changes become large in the sense that user needs or the environment are different, the system should be considered a new "first application." The key to credit V&V activities of a first application in another first application lies on the configuration management and body of evidence that shows direct and undisputable mapping of life cycle activities from one project to another. Annex D provides guidance on the V&V of reuse software, which could be seen to apply to the case of n$^{th}$ of a kind systems as well as a new first application system.

# Annex N

(informative)

# Bibliography

Bibliographical references are resources that provide additional or helpful material but do not need to be understood or used to implement this standard. Reference to these resources is made for informational use only.

[B1] CMU/SEI-2010-TR-033, CMMI-DEV V1.3, Capability Maturity Model Integration (CMMI) for Development Version 1.3.[1]

[B2] *IEEE Standards Dictionary Online.*[2]

[B3] IEEE Std 829™-2008, IEEE Standard for Software and System Test Documentation.[3, 4]

[B4] IEEE Std 982.1™-2005, IEEE Standard Dictionary of Measures of the Software Aspects of Dependability.

[B5] IEEE Std 1012™-2012, IEEE Standard for System and Software Verification and Validation.

[B6] IEEE Std 1028™-2008, IEEE Standard for Software Reviews and Audits.

[B7] IEEE Std 1044™-2009, IEEE Standard Classification for Software Anomalies.

[B8] IEEE Std 1061™-1998, IEEE Standard for a Software Quality Metrics Methodology.

[B9] IEEE Std 1074™-2006, IEEE Standard for Developing a Software Project Life Cycle Process. (This standard has been superseded by IEEE Std 24774™-2012 IEEE Guide—Adoption of ISO/IEC TR 24774:2010 Systems and Software Engineering—Life Cycle Management—Guidelines for Process Description.)

[B10] IEEE Std 1517™-2010, IEEE Standard for Information Technology—System and Software Life Cycle Processes—Reuse Processes.

[B11] ISO/IEC 12207:2008 (IEEE Std 12207™-2008), Systems and Software Engineering—Software Life Cycle Processes.[5]

[B12] ISO/IEC TR 15026-1:2014, Systems and Software Engineering—Systems and Software Assurance—Part 1: Concepts and Vocabulary.

[B13] ISO/IEC 15026-2:2011, Systems and Software Engineering—Systems and Software Assurance—Part 2: Assurance Case.

[B14] ISO/IEC 15026-3:2013, Systems and Software Engineering—Systems and Software Assurance—Part 3: System Integrity Levels.

[B15] ISO/IEC 15026-4:2013, Systems and Software Engineering—Systems and Software Assurance—Part 4: Assurance in the Life Cycle.

[B16] ISO/IEC/IEEE 15288:2015(E), Systems and Software Engineering—System Life Cycle Processes.

[1] Software Engineering Institute publications are available from Carnegie Melon University (http://www.sei.cmu.edu/library/).
[2] The *IEEE Standards Dictionary Online* subscription is available at:
http://www.ieee.org/portal/innovate/products/standard/standards_dictionary.html.
[3] The IEEE standards or products referred to in this clause are trademarks of The Institute of Electrical and Electronics Engineers, Inc.
[4] IEEE publications are available from The Institute of Electrical and Electronics Engineers (http://standards.ieee.org/).
[5] ISO/IEC publications are available from the ISO Central Secretariat (http://www.iso.org/). ISO publications are also available in the United States from the American National Standards Institute (http://www.ansi.org/).

[B17] ISO/IEC 15408-1:2009, 1: Information Technology—Security Techniques—Evaluation Criteria for IT Security—Part 1: Introduction and General Model.

[B18] ISO/IEC 15939:2008, Systems and Software Engineering—Measurement Process.

[B19] ISO/IEC 16085:2006, Systems and Software Engineering—Life Cycle Processes—Risk Management.

[B20] ISO/IEC/IEEE 24765:2010, Systems and Software Engineering—Vocabulary.

[B21] ISO/IEC 27005:2011, Information Technology—Security Techniques—Information Security Risk Management.

[B22] ISO/IEC/IEEE 29148:2011, Systems and Software Engineering—Life Cycle Processes—Requirements Engineering.

# Consensus

## WE BUILD IT.

**Connect with us on:**

**Facebook:** https://www.facebook.com/ieeesa

**Twitter:** @ieeesa

**LinkedIn:** http://www.linkedin.com/groups/IEEESA-Official-IEEE-Standards-Association-1791118

**IEEE-SA Standards Insight blog:** http://standardsinsight.com

**YouTube:** IEEE-SA Channel

IEEE
standards.ieee.org
Phone: +1 732 981 0060 Fax: +1 732 562 1571