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). c) Update the hazard analysis.		
(4) Security Analysis a) Verify that no new security risks are introduced due to changes in the operational environment. 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. 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 Environmental changes Operating procedures Security analysis report	Task report(s)—Security analysis
(5) Risk Analysis a) Review and update risk analysis using prior task reports. b) Provide recommendations to eliminate, reduce, or mitigate the risks.	Installation package Proposed changes Hazard analysis report Security analysis report Risk analysis report Supplier development plans and schedules Operation problem reports V&V task results	Task report(s)—Risk analysis Anomaly report(s)

9.12 Activity: Software Maintenance V&V (Software, 12207—Software process)

V&V tasks	Required inputs	Required outputs
(1) VVP Revision a) Revise the VVP to conform to the approved changes. 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 Approved changes Installation package Supplier development plans and schedules	Updated VVP
(2) Anomaly Evaluation Evaluate the effect of software operation anomalies.	Anomaly report(s)	Task report(s)—Anomaly evaluation
(3) Criticality Analysis a) Determine the integrity levels for the proposed modifications. 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 Installation package Maintainer integrity levels	Task report(s)—Criticality analysis Anomaly report(s)
(4) Migration Assessment Assess whether the software requirements and implementation address the following: a) Specific migration requirements b) Migration tools c) Conversion of software products and data	Installation package Approved changes	Task report(s)—Migration assessment Anomaly report(s)

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

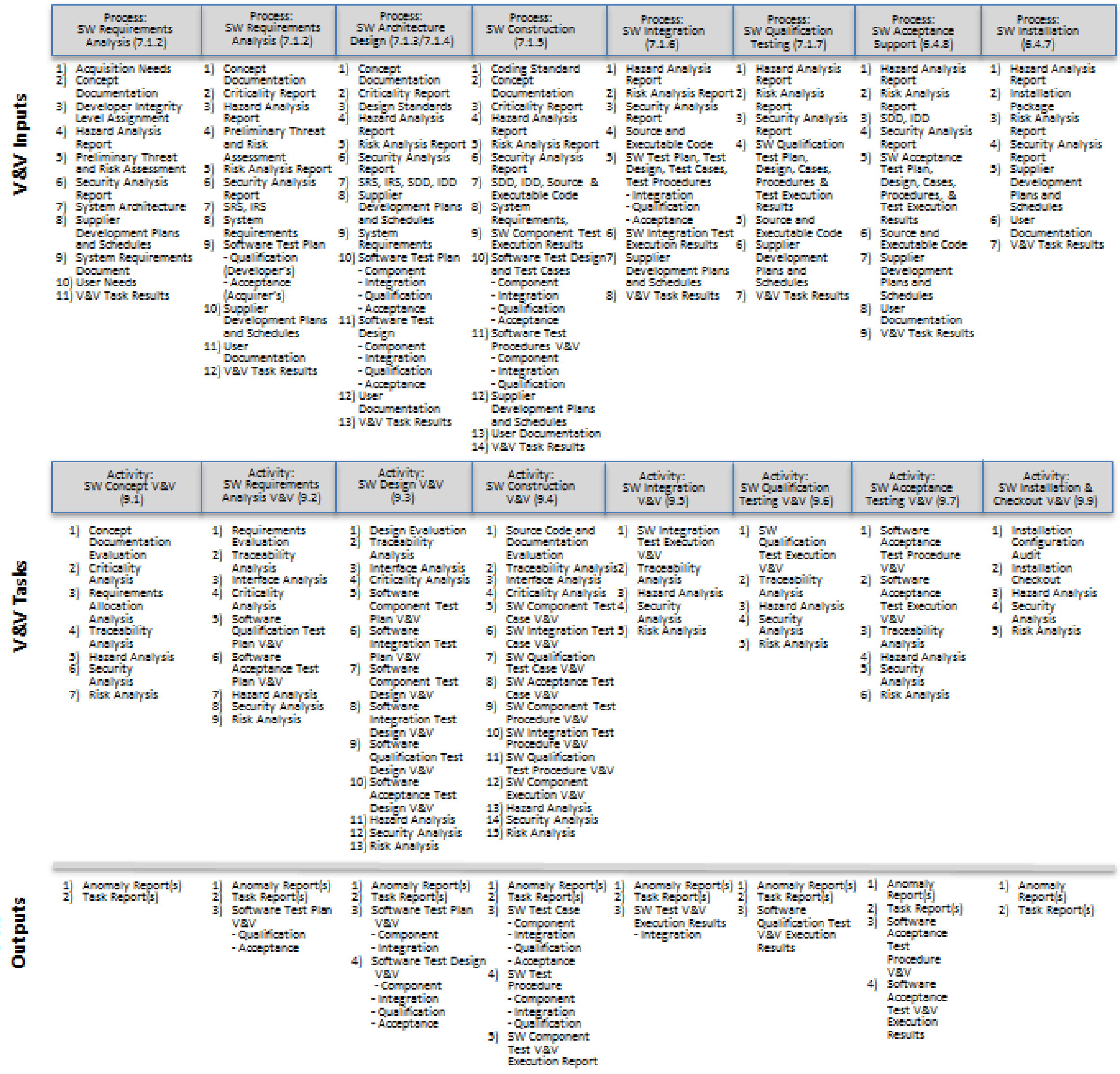
NOTE (for Table 2c)—Whenever a V&V task is selected as a mandatory requirement for multiple integrity levels, the V&V task implementation is dictated by the rigor, intensity, and depth of the analysis or test. Higher integrity level implementation requires greater rigor (e.g., formal methods and structured 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

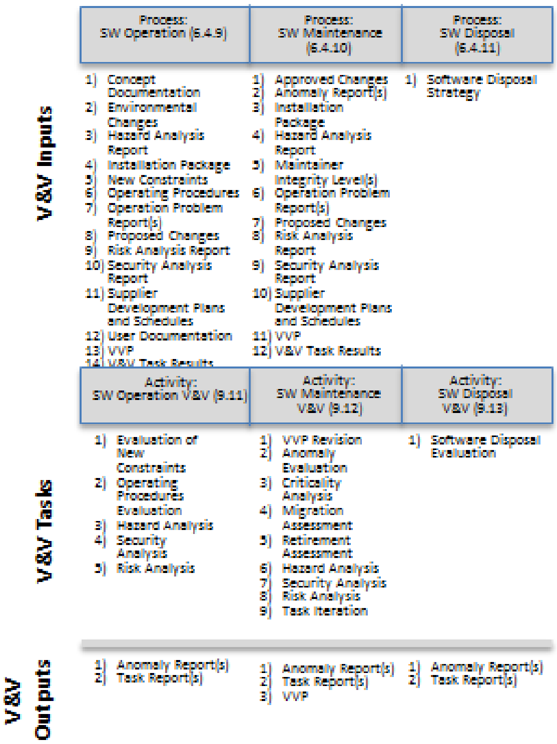
	Software Concept (9.1)	Software Requirements Analysis (9.2)	Software Design (9.3)	Software Construction (9.4)	Software Integration (9.5)	Software Qualification Testing (9.6)	Software Acceptance Testing (9.7)	Software Installation and Checkout (9.9)	Software Operation (9.11)	Software Maintenance (9.12)	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											



	Process: SW Requirements Analysis (7.1.2)	Process: SW Requirements Analysis (7.1.2)	Process: SW Architecture Design (7.1.3/7.1.4)	Process: SW Construction (7.1.5)	Process: SW Integration (7.1.6)	Process: SW Qualification Testing (7.1.7)	Process: SW Acceptance Support (6.4.8)	Process: SW Installation (6.4.7)
V&V Inputs	1) Acquisition Needs 2) Concept Documentation 3) Developer Integrity Level Assignment 4) Hazard Analysis Report 5) Preliminary Threat and Risk Assessment 6) Security Analysis Report 7) System Architecture 8) Supplier Development Plans and Schedules 9) System Requirements Document 10) User Needs 11) V&V Task Results	1) Concept Documentation 2) Criticality Report 3) Hazard Analysis Report 4) Preliminary Threat and Risk Assessment 5) Risk Analysis Report 6) Security Analysis Report 7) SRS, IRS 8) System Requirements 9) Software Test Plan - Qualification (Developer's) - Acceptance (Acquirer's) 10) Supplier Development Plans and Schedules 11) User Documentation 12) V&V Task Results	1) Concept Documentation 2) Criticality Report 3) Design Standards 4) Hazard Analysis Report 5) Risk Analysis Report 6) Security Analysis Report 7) SRS, IRS, SDD, IDD 8) Supplier Development Plans and Schedules 9) System Requirements 10) Software Test Plan - Component - Integration - Qualification - Acceptance 11) Software Test Design - Component - Integration - Qualification - Acceptance 12) User Documentation 13) V&V Task Results	1) Coding Standard 2) Concept Documentation 3) Criticality Report 4) Hazard Analysis Report 5) Risk Analysis Report 6) Security Analysis Report 7) SDD, IDD, Source & Executable Code 8) System Requirements, 9) SW Component Test Execution Results 10) Software Test Design and Test Cases - Component - Integration - Qualification - Acceptance 11) Software Test Procedures V&V - Component - Integration - Qualification 12) Supplier Development Plans and Schedules 13) User Documentation 14) V&V Task Results	1) Hazard Analysis Report 2) Risk Analysis Report 3) Security Analysis Report 4) Source and Executable Code 5) SW Test Plan, Test Design, Test Cases, Test Procedures - Integration - Qualification - Acceptance 6) SW Integration Test Execution Results 7) Supplier Development Plans and Schedules 8) V&V Task Results	1) Hazard Analysis Report 2) Risk Analysis Report 3) Security Analysis Report 4) SW Qualification Test Plan, Design, Cases, Procedures & Test Execution Results 5) Source and Executable Code 6) Supplier Development Plans and Schedules 7) V&V Task Results	1) Hazard Analysis Report 2) Risk Analysis Report 3) SDD, IDD 4) Security Analysis Report 5) SW Acceptance Test Plan, Design, Cases, Procedures, & Test Execution Results 6) Source and Executable Code 7) Supplier Development Plans and Schedules 8) User Documentation 9) V&V Task Results	1) Hazard Analysis Report 2) Installation Package 3) Risk Analysis Report 4) Security Analysis Report 5) Supplier Development Plans and Schedules 6) User Documentation 7) V&V Task Results
	Activity: SW Concept V&V (9.1)	Activity: SW Requirements Analysis V&V (9.2)	Activity: SW Design V&V (9.3)	Activity: SW Construction V&V (9.4)	Activity: SW Integration V&V (9.5)	Activity: SW Qualification Testing V&V (9.6)	Activity: SW Acceptance Testing V&V (9.7)	Activity: SW Installation & Checkout V&V (9.9)
V&V Tasks	1) Concept Documentation Evaluation 2) Criticality Analysis 3) Requirements Allocation Analysis 4) Traceability Analysis 5) Hazard Analysis 6) Security Analysis 7) Risk Analysis	1) Requirements Evaluation 2) Traceability Analysis 3) Interface 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	1) Design Evaluation 2) Traceability Analysis 3) Interface 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	1) Source Code and Documentation Evaluation 2) Traceability Analysis 3) Interface Analysis 4) Criticality Analysis 5) SW Component Test Case V&V 6) SW Integration Test Case V&V 7) SW Qualification Test Case V&V 8) SW Acceptance Test Case V&V 9) SW Component Test Procedure V&V 10) SW Integration Test Procedure V&V 11) SW Qualification Test Procedure V&V 12) SW Component Execution V&V 13) Hazard Analysis 14) Security Analysis 15) Risk Analysis	1) SW Integration Test Execution V&V 2) Traceability Analysis 3) Hazard Analysis 4) Security Analysis 5) Risk Analysis	1) SW Qualification Test Execution V&V 2) Traceability Analysis 3) Hazard Analysis 4) Security Analysis 5) Risk Analysis	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	1) Installation Configuration Audit 2) Installation Checkout 3) Hazard Analysis 4) Security Analysis 5) Risk Analysis
Outputs	1) Anomaly Report(s) 2) Task Report(s)	1) Anomaly Report(s) 2) Task Report(s) 3) Software Test Plan V&V - Qualification - Acceptance	1) Anomaly Report(s) 2) Task Report(s) 3) Software Test Plan V&V - Component - Integration 4) Software Test Design V&V - Component - Integration - Qualification - Acceptance	1) Anomaly Report(s) 2) Task Report(s) 3) SW Test Case - Component - Integration - Qualification - Acceptance 4) SW Test Procedure - Component - Integration - Qualification 5) SW Component Test V&V Execution Report	1) Anomaly Report(s) 2) Task Report(s) 3) SW Test V&V Execution Results - Integration	1) Anomaly Report(s) 2) Task Report(s) 3) Software Qualification Test V&V Execution Results	1) Anomaly Report(s) 2) Task Report(s) 3) Software Acceptance Test Procedure V&V 4) Software Acceptance Test V&V Execution Results	1) Anomaly Report(s) 2) Task Report(s)

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



	Process: SW Operation (6.4.9)	Process: SW Maintenance (6.4.10)	Process: SW Disposal (6.4.11)
V&V Inputs	1) Concept Documentation 2) Environmental Changes 3) Hazard Analysis Report 4) Installation Package 5) New Constraints 6) Operating Procedures 7) Operation Problem Report(s) 8) Proposed Changes 9) Risk Analysis Report 10) Security Analysis Report 11) Supplier Development Plans and Schedules 12) User Documentation 13) VVP 14) V&V Task Results	1) Approved Changes 2) Anomaly Report(s) 3) Installation Package 4) Hazard Analysis Report 5) Maintainer Integrity Level(s) 6) Operation Problem Report(s) 7) Proposed Changes 8) Risk Analysis Report 9) Security Analysis Report 10) Supplier Development Plans and Schedules 11) VVP 12) V&V Task Results	1) Software Disposal Strategy
	Activity: SW Operation V&V (9.11)	Activity: SW Maintenance V&V (9.12)	Activity: SW Disposal V&V (9.13)
V&V Tasks	1) Evaluation of New Constraints 2) Operating Procedures Evaluation 3) Hazard Analysis 4) Security Analysis 5) Risk Analysis	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	1) Software Disposal Evaluation
V&V Outputs	1) Anomaly Report(s) 2) Task Report(s)	1) Anomaly Report(s) 2) Task Report(s) 3) VVP	1) Anomaly Report(s) 2) Task Report(s)

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

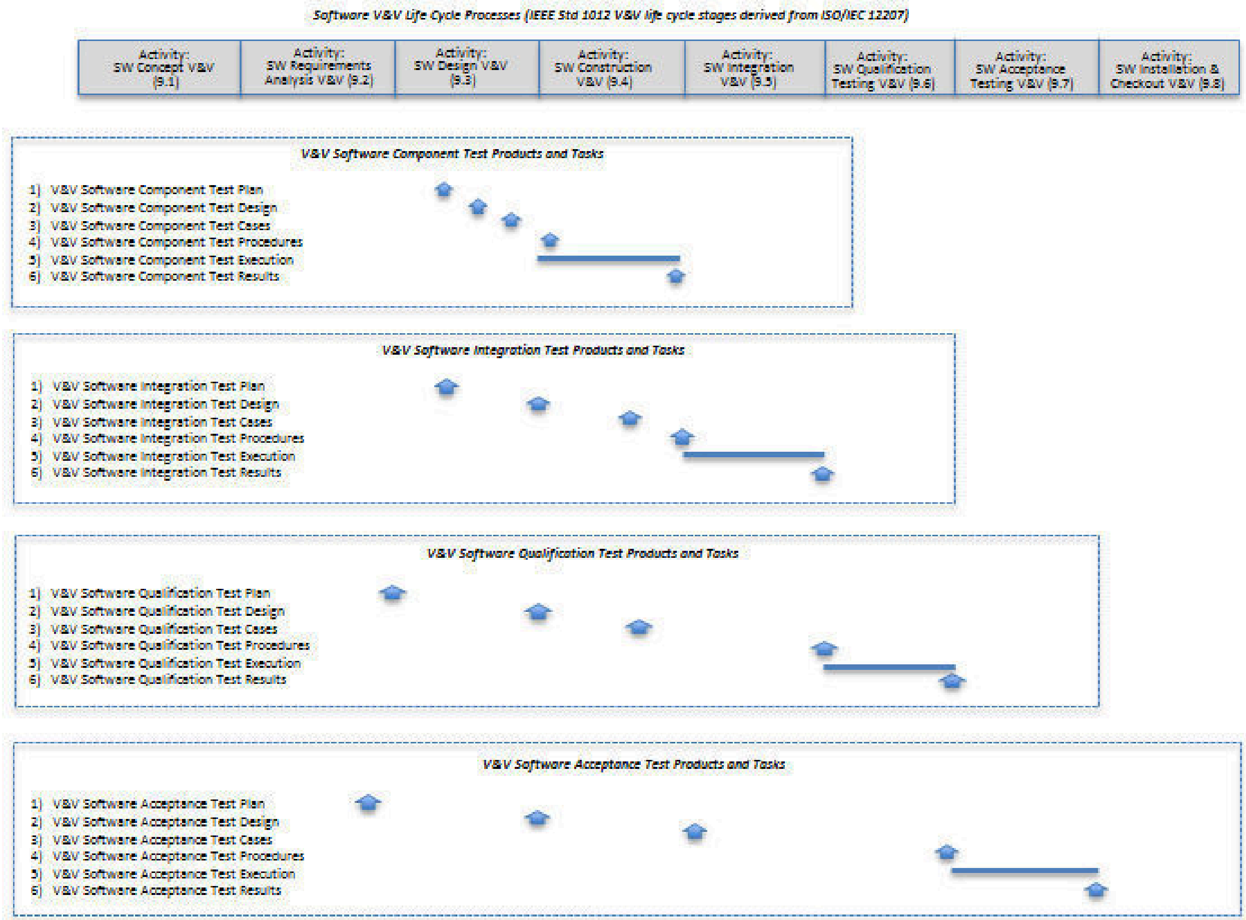
NOTE 2—Clause references in the activity V&V definitions (middle graphic bar) are IEEE Std 1012 clause numbers.

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)


Software V&V Life Cycle Processes (IEEE Std 1012 V&V life cycle stages derived from ISO/IEC 12207)
Activity: SW Concept V&V (9.1)
Activity: SW Requirements Analysis V&V (9.2)
Activity: SW Design V&V (9.3)
Activity: SW Construction V&V (9.4)
Activity: SW Integration V&V (9.5)
Activity: SW Qualification Testing V&V (9.6)
Activity: SW Acceptance Testing V&V (9.7)
Activity: SW Installation & Checkout V&V (9.8)
V&V Software Component Test Products and Tasks
1) V&V Software Component Test Plan
2) V&V Software Component Test Design
3) V&V Software Component Test Cases
4) V&V Software Component Test Procedures
5) V&V Software Component Test Execution
6) V&V Software Component Test Results
V&V Software Integration Test Products and Tasks
1) V&V Software Integration Test Plan
2) V&V Software Integration Test Design
3) V&V Software Integration Test Cases
4) V&V Software Integration Test Procedures
5) V&V Software Integration Test Execution
6) V&V Software Integration Test Results
V&V Software Qualification Test Products and Tasks
1) V&V Software Qualification Test Plan
2) V&V Software Qualification Test Design
3) V&V Software Qualification Test Cases
4) V&V Software Qualification Test Procedures
5) V&V Software Qualification Test Execution
6) V&V Software Qualification Test Results
V&V Software Acceptance Test Products and Tasks
1) V&V Software Acceptance Test Plan
2) V&V Software Acceptance Test Design
3) V&V Software Acceptance Test Cases
4) V&V Software Acceptance Test Procedures
5) V&V Software Acceptance Test Execution
6) V&V Software Acceptance Test Results

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.