Guide for

Software Systems Verification

ABS CyberSafety™ Volume 4

September 2016

GUIDE FOR

SOFTWARE SYSTEMS VERIFICATION
SEPTEMBER 2016

ABS CYBERSAFETY™ VOLUME 4

American Bureau of Shipping
Incorporated by Act of Legislature of
the State of New York 1862

ABS Plaza
1701 City Plaza Drive
Spring, TX 77389 USA

Foreword

The marine and offshore industries are increasingly relying on computer-based control systems. Therefore, the verification of the software used in control systems and their integration into the system is an important element within the overall safety assessment. This ABS *Guide for Software Systems Verification – ABS CyberSafetyTM Volume 4 (SSV Guide)* provides requirements and recommendations for software verification of integrated and non-integrated control systems aboard ships or offshore assets. This Guide is applicable during the initial construction and anytime during the life of the asset. This guide may also be used for new, modifications, retrofits, replacements, or upgrades of computer based control systems.

The SSV Guide was amended to harmonize with the ABS *Guide for Integrated Software Quality Management (ISQM) (ISQM Guide)* and the software development life cycle. The *SSV Guide* focuses on Hardware-Inthe-Loop (HIL) testing of control system software. HIL testing is an acceptable verification method for both the *ISQM Guide* and the *SSV Guide.*

This revision of the Guide incorporates the following changes:

- Addition of BOP control system
- Additional requirements
- Engineering drawing change
- Test cases for individual systems
- New definitions

This Guide is meant to be used with other Rules and Guides issued by ABS and other recognized industry standards.

This Guide becomes effective on the first day of the month of publication.

Users are advised to check periodically on the ABS website www.eagle.org to verify that this version of this Guide is the most current.

We welcome your feedback. Comments or suggestions can be sent electronically by email to rsd@eagle.org.

GUIDE FOR

SOFTWARE SYSTEMS VERIFICATION

CONTENTS

SECTION 1
General

1 Purpose and Scope *(1 September 2016)*

This Guide presents the procedures to be employed by ABS in the review and surveys of computer-based control system software. The objective of this Guide is to reduce software-related incidents that could negatively affect the security, safety and performance of such systems. Compliance with the procedures and criteria given in this Guide may result in the granting of the optional notation **SSV** to a vessel or offshore unit. This Guide emphasizes software verification of control systems and Hardware-In-the-Loop (HIL) testing. Criteria for the hardware, Failure Mode and Effect Analysis (FMEA), and security of computer-based control systems are given in other ABS Rules and Guides, such as the ABS *Rules for Building and Classing Marine Vessels (Marine Vessel Rules), the ABS Guidance Notes on Failure Mode and Effects Analysis (FMEA) for Classification*, and applicable national and international standards.

This Guide is applicable to standalone or integrated computer-based control systems. Such a computerbased control system can be installed on a ship, offshore unit, fixed or floating offshore installation, or other type of facility. The computer-based system can be associated with a control system of any level of complexity, including those used for propulsion and navigation.

The procedures and criteria given in this Guide involve a number of parties concerned with software development and maintenance. These include Systems Providers (SP), Driller or Crew Organization (DCO), Ship Builder Integrator (SBI) or the Shipyard, Verification and Validation Organizations (V&V), Owner, Sub-suppliers, and Subcontractors involved in integrated system software development, implementation, operation, and maintenance. Refer to 1/7 for definitions of these involved parties.

3 Basis of Notation

The **SSV** notation indicates compliance with the procedures and criteria given in this Guide for software verification. Maintenance of the **SSV** notation over the operational life of the system is subject to the periodic surveys carried out onboard.

When the **SSV** notation is given to a control system, the extent of the notation is detailed in the verification plan, based upon the boundaries of the system as tested. The connected control systems and functions of the connected equipment are not included in the notation unless detailed in the verification plan.

The term “approved” or “approval” is to be interpreted to mean that the plans, reports, or documents have been or are to be reviewed for compliance with one or more of the Rules, Guides, standards, or other criteria of ABS.

5 References

5.1 ABS *(1 September 2016)*

ABS *Rules for Building and Classing Marine Vessels*

ABS *Guide for Dynamic Postioning Systems*

ABS *Guide for Integrated Software Quality Management (ISQM)*

ABS *Guide for Survey Based on Reliability Centered Maintenance*

ABS *Guide for Surveys Using Risk-Based Inspection for the Offshore Industry*

ABS *Guidance Notes on Reliability-Centered Maintenance*

ABS *Guidance Notes on Risk Assessment Applications for the Marine and Offshore Industries*

ABS *Guidance Notes on Failure Mode and Effects Analysis (FMEA) for Classification*

ABS *Guidance Notes on Application of Cybersecurity Principles to Marine and Offshore Operations – ABS CyberSafetyTM Volume 1*

ABS *Guide for Cybersecurity Implementation for the Marine and Offshore Operations – ABS CyberSafetyTM Volume 2*

ABS *Guidance Notes on Data Integrity for Marine and Offshore Operations – ABS CyberSafetyTM Volume 3*

ABS *Guidance Notes on Software Provider Conformity Program – ABS CyberSafetyTM Volume 5*

5.3 IEEE

IEEE Std 14764-2006, Second edition 2006-09-01, *Software Engineering – Software Life Cycle Processes – Maintenance*

IEEE Std 12207-2008, Second edition, 2008-02-01, *Systems and software engineering – Software life cycle processes*

IEEE Std 730-2002, IEEE *Standard for Software Quality Assurance Plans*

IEEE Std 1012-2004, IEEE *Standard for Software Verification and Validation*

IEEE Std 1016-1998, IEEE *Recommended Practice for Software Design Descriptions*

IEEE Std 1219-1998, IEEE *Standard for Software Maintenance*

IEEE Std 1362-1998 (R2007), IEEE *Guide for Information Technology – System Definition – Concept of Operations (ConOps) Document*

IEEE SWEBOK 2004, *Software Engineering Body of Knowledge*

5.5 IEC

IEC 61508-0 (2005-01), *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 0: Functional safety and IEC 61508*

IEC 61508-1 (2010-04), *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

IEC 61508-2 (2010-04), *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-3 (2010-04), *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

IEC 61508-4 (2010-04), *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

IEC 61508-5 (2010-04), *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels*

IEC 61508-6 (2010-04), *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*

IEC 61508-7 (2010-04), *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7: Overview of techniques and measures*

IEC 61511-1 (2003-01), *Functional safety – Safety instrumented systems for the process industry sector, Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements*

IEC 61511-2 (2003-07), *Functional safety – Safety instrumented systems for the process industry sector, Functional safety – Safety instrumented systems for the process industry sector – Part 2: Guidelines for the application of IEC 61511-1*

IEC 61511-3 (2003-03), *Functional safety – Safety instrumented systems for the process industry sector, Functional safety – Safety instrumented systems for the process industry sector – Part 3: Guidance for the determination of the required safety integrity levels 5*

5.7 ISO

ISO 17894-2005 *General principles for the development and use of programmable electronic systems in marine applications*

ISO/IEC 9126-1:2001 *Software engineering – Product quality – Part 1: Quality model*

ISO 9001:2008, *Quality Management Systems – Requirements*

ISO/IEC 20000-1:2011 *Information Technology – Service Management - Part 1: Service management system requirements*

5.9 Other *(1 September 2016)*

ANSI/ISA-84.00.01-2004, Part 2 (IEC 61511-2 Mod) *Functional Safety: Safety Instrumented Systems for the Process Industry Sector – Part 2: Guidelines for the Application of ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod) – Informative*

Software Engineering Institute. *The Capability Maturity Model: Guidelines for Improving the Software Process,* Reading, MA, Addison-Wesley, 1995.

American Petroleum Institution (API) Specification 16D Third Edition Draft: *Control Systems for Drilling Well Control Equipment and Control Systems for Diverter Equipment.* October 2014.

7 Organizations *(1 September 2016)*

i) Owner (OW): The Owner is the Organization that initiates the project and owns the control system at the end of the project.

ii) Ship Builder Integrator (SBI): For new builds, the SBI is the shipyard. If no shipyard is involved, then the activities and requirements listed for the SBI are to be performed by the Owner.

iii) System Provider (SP): Suppliers that developed the software for the system under software verification test subject to SSV. If multiple systems are selected for the SSV notation, then there may be multiple SPs.

iv) Sub-supplier (CT): Supplier of connected equipment to the SP's control system and subject to integration portion of the verification testing.

v) Verification and Validation Organization (V&V): The organization that develops the verification plan and performs the software verification of the control system.

a) The V&V is to be an independent third party, or

b) Special consideration is to be requested from ABS if the V&V has some dependencies with the SP's software developers. ABS will review the technical, managerial, and financial dependencies and approve if there exists sufficient independence. The Owner or SBI are informed of the review(s) for their input.

c) The V&V validates the simulation per 3/3.11.

9 Quality Program and Training for V&V

9.1 Quality Program *(1 September 2016)*

The V&V is to have an ISO 9001 certificate detailing the quality processes of the company:

i) The V&V is to provide to ABS their internal quality policies and procedures.

ii) The V&V is to provide to ABS the training records of simulation software developers.

iii) ABS is to conduct a quality audit survey of the facility where simulation is taking place prior to the verification or once within the prior two years. During the survey, ABS is to interview simulation development engineers discussing the V&V's quality procedures.

Note: The interview is to occur every 2 years, not for every project.

iv) If the V&V does not have an ISO 9001 certificate, contact ABS for special consideration.

v) The V&V is to provide an organizational interrelationship chart that describes the lines of communication within the V&V organization.

9.3 Training

The V&V is to provide personnel who have been trained in the software testing as per the V&V's quality policies.

ABS is to review the policies, procedures, and quality processes of the V&V prior to the verification or once within the prior two years.

11 Independence of the Verification Organization

Maintaining independence of the verification and validation process is an essential element of the **SSV** notation. The Institute of Electrical and Electronics Engineers standard for Software Verification and Validation (IEEE Std 1012 – 2004, Annex C) has defined what is called classical independence.

11.1 Classically Independent Verification Organization *(1 September 2016)*

An organization that is classically independent is defined as being separate from the SP, SBI and Owner in the following categories (refer to Appendix 3 for a detailed explanation of classical independence):

i) *Technical.* Separate group of personnel not associated with code development for the SP of the system under test

ii) *Managerial.* Management of the V&V is separate from management of the SP's Organization

iii) *Financial.* V&V has no apparent financial association with the SP other than the contract to perform verification testing.

11.3 Other than Classically Independent Verification Organization *(1 September 2016)*

ABS will review the V&V for technical, managerial, and financial independence from the SP of the system(s) under test. Refer to Appendix 3 for a detailed explanation of other forms of independence.

Special consideration is required from ABS for dependencies other than classical independence.

Other forms of independence that the V&V can fall under:

i) Modified Independent V&V

ii) Integrated Independent V&V

iii) Internal Independent V&V

iv) Embedded Independent V&V

The SBI and Owner are to be informed of ABS assessment of the independence of the V&V.

13 Safety of Personnel and Equipment *(1 September 2016)*

13.1 Safety Considerations

Safety of personnel and equipment are to be considered by the V&V:

i) The V&V is to review the verification plan, equipment setup, and other activities at the testing location (at factory or onboard) for safety of personnel and protection of equipment and the environment during execution of the V&V Plan.

ii) The V&V is to review the re-activation of the system(s) (from testing state to normal (controlling equipment)) for safety of personnel, equipment, and the environment.

iii) Tests deemed to contain unacceptable risk are either to have risk mitigated or the test is not to be performed.

iv) It is recommended that the SP provide input on all test scenarios in the V&V Plan.

v) The Owner is to notify ABS before installation of software patches or upgrades on safety-critical systems.

13.3 Onboard Testing

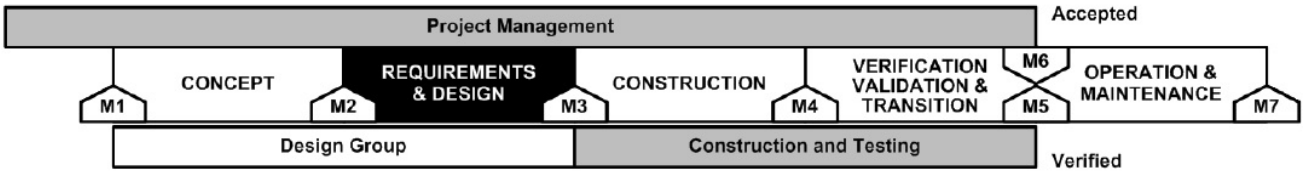
While the control system is installed onboard and testing is to be performed, the Owner, SBI, and V&V are to agree on the functions or functionality to be tested and the safe method to perform the testing. Some system tuning (parameters, set points, etc.) may occur during commissioning onboard under SBI's or the Owner's consent.

Tests or scenarios identified as having risk to safety, environmental, or equipment damage are not to be tested onboard.

SECTION 2

Introduction *(1 September 2016)*

FIGURE 1
ISQM's Software Development Life Cycle



1 Background

The software development life cycle is described in the ABS *Guide for Integrated Software Quality Management (ISQM) (ISQM Guide)*. Verification[1] of control system software is a requirement of the *ISQM Guide* and is a significant event in the Software Development Life Cycle (SDLC). Within the SDLC, the Verification, Validation & Transition Phase is where the software is verified and validated. Documentation required for verification of software in this Guide is also required in the *ISQM Guide*. It is necessary to have a detailed description of the functionality in order to develop the verification plan. Within ISQM, this description is called a Functional Description Document (FDD). It is required in ISQM to perform Risk Assessment to identify the risks associated with a software-intensive system and its related, or connected, systems. This Guide requires safety reviews, FMEA, FMECA, or other risk analyses to identify risks and to provide a method to generate additional testing scenarios.

Note: [1]Verification means the test-based determination that the software under test fully meets or satisfies all expected requirements, including both functional (system operation) and extra-functional (safety, security, etc.) requirements.

The *SSV Guide* requires a greater degree of independence between the code developers and the verification organization, see Appendix 3

This Guide is focused on the verification of the software that controls equipment and processes aboard marine and offshore assets.

This Guide is applicable to any control system where software is used to control, monitor, report, etc., on equipment or conditions utilizing computer-based control systems. The firmware's version number and serial numbers of the control system's hardware are to be recorded. The suitability of the control system hardware, the physical network, and other non-software items are addressed in other ABS Rules and Guides, *such as the Marine Vessel Rules*, and applicable national and international standards.

It is recommended that consideration be given to applying the **ISQM** and **SSV** notations together to cover the entire lifecycle of software development from concept to retirement of the control system. Several documents and activities listed in the **SSV** notation are also required in the **ISQM** notation.

3 Verification Methods

Verification is concerned with testing the system's functionality and functions to meet the specification as detailed in the control systems functional description or the FDD.

See the *ISQM Guide* for additional descriptions of verification methods.

3.1 Software-In-the-Loop (SIL) Testing

In Software-In-the-Loop verification, the control system's program is being executed on non-native hardware, and the simulation is being executed on the same or a separate computer. Software-In-the-Loop verification does not verify the networked connections, input or output hardware modules, system memory, or the processor; rather, it is intended to demonstrate only that the software runs without errors.

3.1.1 Software-In-the-Loop Testing Applicability

Software-In-the-Loop testing is limited in application. The following considerations are to be agreed upon by V&V and the Owner and acceptable to ABS:

i) Approval from the Owner to apply this method

a) The Owner is to agree that Software-In-the-Loop is acceptable for the control system or control systems under test, either contractually or by other written statement.

ii) Software-in-the-loop may not be used for process Safety Instrumented Systems (SIS) or other safety systems, which require more thorough testing than SIL provides.

iii) Special consideration from ABS is granted after a review of the V&V Plan's scope.

3.3 Hardware-In-the-Loop Testing (HIL)

In Hardware-In-the-Loop verification, the integrated system's program is being executed on its native hardware (native processor, native firmware), and the simulation is being executed on a separate machine.

There are no restrictions to utilize the Hardware-In-the-Loop method for testing.

Boundaries of the system under test in HIL verification must specify interfaces to other systems, machineto-machine communications pathways, and user interface or data exchange methods or protocols.

3.5 Closed Loop

Closed Loop verification involving less complex control systems is acceptable to ABS if the Owner chooses it as primary verification method (This method may be used for limited scope verification and with special consideration by ABS for the **SSV** notation.). In Closed Loop verification, detailed knowledge of the process and programming is necessary to verify correct actions of the software. The register data are interpreted to verify the integrated system's response is per the specifications (System Requirements Specification (SRS) and System Design Specification (SDS), FDD or description of functionality). This method may be used for limited scope verification and with special consideration by ABS for the **SSV** notation.

3.7 Cybersecurity Testing

If the system under test is networked and available for remote accessibility, then application and system cybersecurity testing may be required, especially for safety-related systems equipped with web communication. Testing for cybersecurity includes tests and scenarios for the functional system software; for applications or processes running on the system in support of system function; and for any sensors or reporting elements that provide critical data back to the system under test. If cybersecurity testing is required to demonstrate or prove security and/or quality of the system against specific threats[2], ABS will work with the V&V organization to include appropriate tests to complement the functional verification methods above.

Note: [2]Threats against networked systems include, but are not always, attacks; they may include inadvertent error introductions through user interfaces, employee errors in operation, malicious insider actions, and malicious outside actor activities.

5 Boundaries and Limitations of the SSV Notation

The **SSV** notation is limited to:

i) The functions and functionality as listed in the V&V Plan and tested as reported in the V&V Report

ii) Interface registers of the control system(s) under test as listed in the V&V Plan

iii) Operational boundaries and limitation of the tested control system as listed in the V&V Plan

iv) Design boundaries of the simulator and simulation used in the testing of the control system as listed in the V&V Plan and V&V Report

5.1 Focus on Software

This Guide's focus is to test the software of the equipment's control system. This Guide puts an emphasis on the selected equipment's software and its demonstrated behaviors under different states and network load conditions. This is expected to verify that the software operates in its expected environment and conforms to its functional description under all conditions, including any areas of concern raised by safety reviews or other safety analysis. This Guide is written as a process to acquire a software-focused notation, and it does not verify any piece of hardware or equipment as to the suitability of said equipment for the intended purpose.

SECTION 3

Verification and Documentation

1 General

Descriptive documentation of the functionality and functions of the control system to undergo the testing (target system) is to be reviewed by ABS, Owner, and SBI.

1.1 Traceability of Functions across Documents *(1 September 2016)*

i) Traceability of functions is important during the safety analysis and selection of functions or functionality to be tested, defect tracing in the simulation programming or control system code. The traceability may be any unique identifier to allow for tracing the function from the system functional description or FDD through safety review(s) or safety analysis, V&V Plan, and V&V Report.

ii) It is recommended that a traceability matrix be utilized[3].

Note: [3]The system Requirements Traceability Matrix (RTM) is applicable and expected to be included in the FDD. Software functions may require breakout to capture software-only functionality.

1.3 Integrity Level Assignments *(1 September 2016)*

i) The Owner is to assign Integrity Level (IL) to the functions listed in the Description of the Control System (SRS and SDS or FDD). The V&V, SBI or the SP may recommend IL levels to the functions and overall system.

ii) The *ISQM Guide* is to be followed for assignment of the Integrity Level (see 3/5.3 and 3/5.5 of the *ISQM Guide*).

iii) IL system data required for safe operation of the system under test must be shown in the Verification Plan (V&V Plan).

iv) The IL assignment numbers are to be included in the V&V Plan and Verification Report (V&V Report) for tested functions.

1.5 Network Data Information *(1 September 2016)*

i) Data and Commands going from and coming to the tested control system of the equipment under control.

ii) Communication protocol for the control system interfaces are to be listed in the test plan for each connected equipment for the functionality under test.

iii) Topology drawing showing networked and serial connected equipment.

iv) Network traffic packet captures to assess the command and control interface environment for potential security issues that may affect safety-critical operations[4].

Note: [4]This is applicable in cases of mixed-purpose networks (i.e., multiple equipment types or systems on the same network infrastructure) that may carry multiple message types or protocols.

1.7 Connected Instrumentation Listing

The SP or the SBI is to provide a connected instrument listing. This could be the I/O list.

1.9 Risk Management *(1 September 2016)*

i) A safety review, FMEA, FMECA, or other risk analysis is to be performed by the SP on the control system's functionality, depending on the system's Integrity Level (see 4/5.5.4 of the *ISQM Guide*). If the SP is not available, then the V&V is to provide this safety analysis.

ii) A safety review is required for systems that are rated as IL0 and IL1.

iii) Safety Reviews prior to executing the Verification Plan (V&V Plan) performed by the V&V:

- ***a)*** Safety reviews are to be conducted prior to all verification testing addressing the potential impact of each test scenario. Special attention is to be given when the control system's physical parts are connected to other control systems and any sub-supplier's control systems.
- ***b)*** Safety reviews are to verify the boundaries of the system under test prior to test scenario execution.
- ***c)*** Safety reviews are to be conducted for all test scenarios by the V&V as listed in the V&V Plan. The SP and ABS are to be involved in the safety reviews. This applies when there is to be retesting and regression testing.
- ***d)*** The V&V can provide a statement, after performing an internal safety review, that there is no physical equipment connected or used during the testing. In this case, there is no need to perform safety review involving all parties.

iv) The V&V is to provide:

- ***a)*** A report of the testing environment, and
- ***b)*** Test process safety review meeting(s) minutes to ABS (if any). Refer to 3/1.9iii).

v) Safety of personnel, the equipment, the asset, and the environment are to be considered in the safety review.

vi) The Owner, SBI, and ABS are to witness the testing of the control system.

vii) The Owner's or SP's Management of Change (MOC) records or documents are to be submitted to ABS for review for the target system's software, including any updates or revisions.

viii) The safety analysis for risk management may provide additional scenarios for the verification test.

ix) For Safety Instrumented System (SIS), it is recommended that IEC 61508, IEC 61511, or ISA 84 be utilized or followed

3 Documentation to be Submitted *(1 September 2016)*

The documentation listed below is to be reviewed by the V&V, Owner, SBI, and ABS.

3.1 System Functional Description

i) The SP is to provide a descriptive narrative of the control system functions and its functionality:

- ***a)*** The description may be the Functional Descriptive Document (FDD) as described in 9/7 of the *ISQM Guide.*
- ***b)*** The description may be provided along with the Software Requirements Specification (SRS) (see 4/5.1 of the *ISQM Guide*) and Software Design Specification (SDS) (see 4/5.3 of the *ISQM Guide*).

ii) For all functions of the control system the following states are to be described:

- ***a)*** Normal state, where everything is functioning normally

b) Degraded state, with some faults located in the system or connected systems affecting the system under test functionality:

- Hardware failures
- Degraded communication
- Reduction of network capacity or available services
- Loss of communication with connected equipment
- Individual input failure
- Propagation of erroneous values
- Common mode (common cause) failures

c) Failed state, where the target controls fail to execute the control system functions. The description is to include the programmed error handling routine for the degraded and failed states:

- Human error-caused conditions
- Potential attacks against system software components
- System failures and fail-safe conditions in software components and interfaces
- Software errors, crashes or failures that could result in safety-critical conditions

d) It is recommended that a template that facilitates FMEA or FMECA be considered for listings of the various states.

e) Normal startup of the equipment and equipment's programmed actions

f) Normal shutdown of the equipment and programmed actions

iii) Provide for the traceability of the functions and/or functionality. It is recommended that a matrix be utilized. See 3/1.1ii).

iv) If the SP is not available to provide the control system functional description, then the V&V is to provide the control system functional description.

v) Submit control system functional description at least four weeks prior to any verification for review.

vi) The control system functional description is to be provided for review by the Owner, V&V, SBI, and ABS

vii) The provider of the control system functional description (SP, or V&V) is to hold a meeting with the other involved parties to gather their input(s), as required. Meeting may be in person, teleconference, or e-meeting.

viii) The provider of the control system description is to provide meeting minutes of the meeting to ABS if ABS is not present at the review meeting(s).

3.3 Safety Analysis Report

i) Listing of items for safety consideration:

a) The developer of the control system functional description is to provide a safety item listing of the functions and functionality described in the control system Functional Description Document (FDD).

ii) The V&V is to provide a report on the safety analysis meeting and the results of the meeting:

a) The V&V is to submit the safety analysis report on testing environment and testing equipment, at least one week prior to any verification, for review.

b) It is recommended that the SP develop and provide the safety analysis for the functionality of the system under test and V&V provide the safety analysis for the test cases and test environment.

3.5 Verification Plan and Verification Scope

The verification scope is defined in the Verification Plan (V&V Plan). The V&V Plan will detail testing of functions and functionality, networking, and control system hardware involved in the testing. The V&V Plan defines the scope of the **SSV** notation. The following are minimum requirements for the verification scope.

i) The V&V is to provide the Verification Plan(s):

a) The V&V is to provide the scope of verification (what is to be tested).

b) The scope of verification is to include functions and/or functionality and may include control system hardware.

c) The V&V is to peer review the simulation for defects or deviations from intended functions or functionality to be tested.

d) The V&V is to provide a statement as to how the simulation programming was verified.

e) The V&V Plan is to contain the test scenarios that are safe to execute, and a list of those scenarios and objectives which are judged to be not safe to execute.

f) The V&V Plan is to contain the inputs to the system under verification. Refer to figures in Appendix 2.

ii) The V&V plan is to contain the following requirements for each testing scenario:

a) The V&V Plan is to include all the required functions of the control system as listed in the FDD, traceability matrix, or system description document.

b) Testing scenarios (individual tests) are to be traceable to the functions listed in the functional description.

c) The SP is to perform a software-focused FMECA along with any hardware FMEAs or other relevant Hazard Identification be reviewed to establish the testing scenarios for the listed functions in the function description of the Control System.

d) Rejected test scenarios by V&V are to be explained as to why the scenarios are not going to be executed as part of the V&V Plan separately from the V&V Plan to Owner, SBI and ABS.

iii) The Owner, SBI, and ABS may add additional testing scenarios to the Verification plans that are to be performed by the V&V.

iv) The Owner, SBI, and ABS are to provide a formalized reason for the additional testing scenarios.

v) ABS is to approve the Verification Plan prior to the actual testing. (See 6/9.3 of the *ISQM Guide*).

vi) The V&V is to include the safety reviews done (individual tests) for safety of personnel, equipment, the environment, and the asset.

vii) The initial V&V Plan is to be submitted two weeks before any verification activities or one week prior to the safety analysis meeting.

viii) For project-specific cases, ABS is allowed to add, modify or delete test cases when those provided are insufficient or does not test the function thoroughly.

3.7 Verification Report

i) The V&V is to provide the Verification Report (V&V Report) for each testing session.

ii) The SP or the V&V is to provide a listing of control system hardware used within the control system including local and remote hardware connected during the testing.

iii) The V&V Report is to contain:

a) Function name

b) Traceability identifier

c) Listing of defects found

d) Listing of any regression testing for any functions that failed the initial V&V tests

e) Ranking of the defects

f) An explanation of the defect ranking methodology

g) List and description of any functional coverage not tested

iv) After testing, the V&V is to conduct a meeting with the Owner, SBI, SP, and ABS to discuss findings.

v) The V&V is to provide defect ranking with inputs from the Owner, SBI, SP, and related CTs.

vi) The V&V and the SP are to correct defects or findings for retesting by the V&V.

3.9 Simulator Hardware

The V&V is to provide:

i) A listing of the simulator's hardware serial numbers

ii) A listing of the simulator's firmware version numbers

iii) The simulator's block diagram and interface schematic, hardware and software interfaces to the system under test

iv) A statement of whether the simulator contains new, novel or unproven technology

3.11 Simulation Software

The V&V is to provide:

i) The version number of the simulation software

ii) A statement that the simulation programming will test the functions listed in the V&V Plan. The V&V is to validate the simulation based on review of the V&V Plan and internal testing.

iii) A statement as to the safety of the testing, based on a review for safety of personnel and equipment for the testing of the control system

5 SSV is Applicable to (but not limited to) the Following Control Systems *(1 September 2016)*

5.1 Dynamic Positioning Control System

i) For dynamic positioning systems, the V&V is to verify the software performance, the calculated operating limits, functionality, and redundancy of the system.

ii) Maximum wind, current, and wave height as defined in the capability chart.

iii) To apply SSV to the Dynamic Positioning Control System, the following control systems are also to be tested:

a) Consequence Analyzer software package or control system

b) Power Management Control System

c) Thruster control system

See A2/1 for a simulation model of the Dynamic Positioning Control System.

5.3 Power Management Control System

The V&V is to verify:

i) Data transfer to and from the connected equipment, as specified in the V&V Plan

ii) All load sharing, load balance, and load shedding functions for normal and emergency operations

iii) The sequence and functions of Blackout Recovery modules

iv) The functions of emergency safety functions

v) The functions for defined electrical systems modes; isochronous, droop, etc.

vi) The functions for breaker control

vii) The functions for alarms and system monitoring

viii) Functions for Blackout Prevention

ix) Functions for Enhanced Generator Protection, if implemented

See A2/3 for a simulation model of the Power Management Control System.

5.5 Thruster Control System

The V&V is to verify:

i) The automatic control of all thruster functions as described in the system description (SRS and SDS or FDD).

ii) Thruster recovery after a blackout

iii) Functions for primary (and auxiliary if available) thruster power unit

iv) Local and remote transfer control and alarm functions

v) Thruster fast phase back

See A2/5 for a simulation model of the Thruster Control System.

5.7 Blowout Preventer (BOP)

The V&V is to verify:

i) The automatic control of all BOP functions as described in the FDD.

ii) The interface and communication between 3rd party and BOP control system

iii) Interlocks

iv) Subsea-to-surface communication

- *a)* Topside communication for BOP
- *b)* Surface to subsea communication
- *c)* Subsea module communication with connected controls such as acoustic controls, riser control box and power units.

v) Emergency control functions: Automatic mode/Deadman and backup power

vi) The interface and communication with backup control systems (if installed)

vii) Emergency Disconnect Sequence Systems (EDS)

- *a)* Emergency pump and valve control functions

b) Autoshear functions

c) LMRP functions

d) Pipe and blind shear ram functions

e) Casing shear ram functions

viii) Hydraulic Fluid Mixing Control System functions

a) Communication to DCU

b) Power supply

ix) Operational limits

See A2/7 for a simulation model for the BOP control system.

7 Re-testing *(1 September 2016)*

ABS is to be notified when testing or retesting is performed for failed test scenarios and functionality upgrades.

i) Re-testing of the control system is to be performed:

a) Upon upgrade of the control system software including functionality upgrades

b) When desired by the Owner

c) On failed test cases from V&V Report

d) When an IL3 software module is modified (refer to 4/3.1)

e) Prior to installation of software patches on safety-critical systems

ii) It is recommended that re-testing be performed:

a) With new or added functionality that is not defined as a upgrade

b) When system interfaces or network connections change

c) After a system insecurity or safety-related malfunction

iii) The documents listed in 3/3 are to be updated, as required, and reissued.

9 Simulation Program Maintenance *(1 September 2016)*

i) The V&V and the Owner are to agree upon simulation program archiving.

ii) It is recommended that the V&V maintain a backup of the simulation program or any modeling.

iii) The V&V is to update the simulation, as required for new functions added to the control system at the time of retesting.

iv) The SP is to update the functional description with software updates, changes or with additional functionality prior to retesting.

SECTION 4

Surveys After Construction and Maintenance of Class

1 General

The provisions of this Section are requirements for the maintenance of classification of the control system(s) associated with the Software Systems Verification (**SSV**) Notation. These requirements are in addition to the provisions noted in other ABS Rules and/or Guides, as applicable to the vessel or facility.

For purposes of this Section, the commissioning date will be the date on which a Surveyor issues an Interim Class Certificate to the vessel or facility with the **SSV** notation.

3 Surveys for the Software Systems Verification (SSV) Notation

3.1 Survey Intervals and Maintenance Manuals/Records *(1 September 2016)*

All Annual and Special Periodical Surveys associated with the **SSV** notation are to be carried out at the same time and interval as the periodical classification survey of the vessel or facility in order that they are recorded with the same crediting date.

An Annual Survey of the control system(s) associated with the **SSV** notation is to be carried out by a Surveyor within three months either way of each annual anniversary date of the initial certification survey.

A Special Periodical Survey of the control system(s) associated with the **SSV** notation is to be carried out within five years of the initial certification survey and at five-year intervals thereafter. SSV surveys may be offered for survey prior to the due date when so desired, in which case, the survey will be credited as of that date.

Maintenance records are to be kept and made available for review by the attending Surveyor. The maintenance records will be reviewed to establish the scope and content of the required Annual and Special Periodical Surveys that are to be carried out by a Surveyor[5]. During the service life of the software system components, maintenance records are to be updated on a regular basis. Re-test requirements, noted in Subsection 3/7, are to be included in maintenance records when re-tests are required.

Note: [5]Maintenance records and the FDD are to include software version control logs, change management logs, and the functional testing logs. These records, with other documentation specific to each asset, will support Surveyor assessment scope and content.

The Owner is to inform ABS whenever an IL3 Software Module is modified or installed in a control system with an **SSV** notation. ABS may audit the vessel upon notification of an IL3 Software Module function modification or installation.

3.3 Annual Surveys

At each Annual Survey, the Surveyor is to perform an integrated software and hardware configuration audit to include verification of the following:

i) Change control procedures, including periodic audits to confirm that procedures are also being followed

ii) Examination of Control Equipment Registry (see 8/3.3.1 of the *ISQM Guide*)

iii) Examination of Software Registry (see 8/3.3.2 of the *ISQM Guide*)

iv) Review of Integrated Control System's Hardware Registry (see 8/3.3.3 of the *ISQM Guide*)

3.3.1 Examination of Control Equipment Registry

i) Identify control equipment that has been changed since the last audit.

ii) Examine the current version of the control system registry.

iii) Record each changed equipment item.

iv) List all software hosted on the changed equipment.

v) Identify all documentation impacted by the change.

vi) Record each documentation change.

vii) Note any changes identified that were not listed on the registry.

3.3.2 Examination of Software Registry

i) Identify control software that has been changed since the last audit.

ii) Record each software item change.

iii) Inspect all software hosted on the changed equipment identified in 8/3.3.1 of the *ISQM Guide*.

iv) Record software changes on changed equipment in the Software Registry.

v) Identify all documentation impacted by the changes.

vi) Record all changed documentation in the software registry.

vii) Note any software changes identified that were not listed on the registry.

3.3.3 Review of Management of Change (MOC) Policy *(1 September 2016)*

i) Assess how closely the software MOC is followed by interviewing relevant Owner/DCO and SP as well as reviewing supporting documentation.

ii) Where possible, identify discrepancies and weaknesses, and recommend improvements to the process

3.5 Special Periodical Surveys

The Special Periodical Survey is to include all items listed under the Annual Survey to the satisfaction of the attending Surveyor.

5 Modifications, Damage and Repairs *(1 September 2016)*

When it is intended to carry out any modifications to the software system that affects the **SSV** notation of the vessel or facility, the details of such modifications are to be submitted for approval, and the work is to be carried out to the satisfaction of the Surveyor.

When a control system that affects the **SSV** notation of the vessel or facility has suffered any damage which may affect classification, ABS is to be notified, and the damage is to be assessed by a Surveyor.

Where a control system suffers a failure, and is subsequently repaired or replaced without Surveyor attendance during operations, details of the failure and corrective actions are to be retained onboard for examination by the Surveyor during the next scheduled survey/visit.

When major modifications are conducted, the system is to be tested as required by this Guide applicable for the specific system, and additional testing of the control system conducted in order to verify compliance with this Guide as deemed necessary the attending Surveyor.

APPENDIX 1

Terminology *(1 September 2016)*

1 Definitions

The following definitions are applied to the terms used in this Guide:

Component: One of the parts that make up a system. A component may be hardware or software and may be subdivided into other components. Note: The terms "module", "component", and "unit" are often used interchangeably or defined to be sub-elements of one another in different ways depending upon the context. The relationship of these terms is not yet standardized.

Control: The process of conveying a command or order to enable the desired action to be effected.

Control, Remote: A device or array of devices connected to a machine by mechanical, electrical, pneumatic, hydraulic, or other means and by which the machine may be operated remote from and not necessarily within sight of the operator.

Control System: An assembly of devices interconnected or otherwise coordinated to convey the command or order.

Defect: A software coding error.

Defects, Major: These are severe defects, which have not halted the system, but have seriously degraded the performance or caused unintended action or incorrect data to be transmitted.

Defects, Minor: Defects which can or have caused a low-level disruption of function(s). Such defects can result in data latency but not in essential or IL2 or IL3 functions. The integrated system and the function continue to operate, although with a failure. Such a disruption or non-availability of some functionality can be acceptable for a limited period of time for IL1 functions. Minor defects could cause corruption of some non-critical data values in a way that is tolerable for a short period.

Failure Modes, Effects, and Criticality Analysis (FMECA): The criticality analysis is used to chart the probability of failure modes against the severity of their consequences. The analysis highlights failure modes with relatively high probability and severity of consequences.

Failure Modes, Effects, and Criticality Analysis Testing: Testing to verify that the system performs as predicted upon introduction of failure.

Function: The purpose of the Equipment Under Control (i.e., the hydraulic power unit, winch, power management system).

Functional Description Document (FDD): In systems engineering and software development environment a FDD is a document that specifies the functions that a system or component must perform (often part of a

requirements specification). The documentation typically describes what is needed by the system user as well as requested properties of inputs and outputs.

Hardware: Physical equipment used to process, store, or transmit computer software or data.

Hardware in the Loop: A testing technique used for development and proof of complex process systems that provides real process components to increase realism in system operational and behavioral testing.

Human Machine Interface (HMI): A display and operator input device.

Instrumentation: A system designed to measure and to display the state of a monitored parameter and which may include one or more sensors, read-outs, displays, alarms, and means of signal transmission.

Integrity Level (IL#): A number assigned by Owner and/or Operator to a function based upon the severity of the consequence of a failure of the function, where 0 has little consequence to 3 where the consequence of a function failure is of significant concern with corresponding consequences.

Load Sharing: When more than one generator are running in parallel, load sharing distributes equal active (kW) and reactive (kVA) loading on all in order to provide more efficient operation.

Load Shedding: When the power demand is higher than the supply, certain loads are disconnected to prevent overload (and subsequently a total blackout) and so that essential services remain online. Please refer to the *Marine Vessel Rules* for the load shedding hierarchy.

Maintenance, Software: Modification of a software product after delivery to correct faults, to improve performance or other attributes, or to adapt the product to a modified environment.

Native Computer: The program is being executed on the hardware that it will execute upon when installed

Non-native Computer: The program is being executed on an emulation of the target hardware using an emulator.

Operational: (1) Pertaining to a system or component that is ready for use in its intended environment. (2) Pertaining to a system or component that is installed in its intended environment. (3) Pertaining to the environment in which a system or component is intended to be used.

Peer Review: A process where a document or author's work is scrutinized by others who are competent or are considered experts in the same field.

Quality Audit Survey: An initial meeting and interview of the V&V personnel for a gap analysis of existing quality policies and procedures and its compliance with the *ISQM Guide*. This is to help determine the efforts needed to perform the testing.

Remote Access: The ability to gain a degree of control-based entry to a networked system from a distance.

Retirement: Withdrawal of active support by the operation and maintenance organization, partial or total replacement by a new system, or installation of an upgraded system.

Safety Analysis: A risk assessment tool used to identify safety related risks in a given control system and all the functions within.

Safety Review: Review of documents submitted to support not only the system requirements but the considerations made to ensure fail-safe behavior of the system. Example: A safety review can include a review of simple safety report (IL0 or IL1 systems) or it can include reviews of FMECA report, FMEA report, fault tree analysis, etc.

Simulation Programming: A process of modeling or simulating a real phenomenon with a set of mathematical formulas and functions that meets a certain requirements.

Software: Computer programs, procedures, test scripts, and associated documentation and data pertaining to the operation of a computer system.

Software Design Specification: A document that describes the design of a system or component. Typical contents include system or component architecture, control logic, data structures, input/output formats, interface descriptions, and algorithms.

Software in the Loop: Software-only simulation to prove run-time effectiveness of system software.

Software Module: A smaller set of program code to carry out a logical subset of control actions controlled by the overriding program (i.e., A Software Module with program code to open a valve, monitor that the valve did open, and alarm if feedback is not provided within the prescribed time. Another example would be an analog loop where the main shaft is to rotate at 20 rpm and a closed loop control would adjust the drive's motor speed to maintain 20 rpm).

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

Software Risk: The potential loss due to failure during a specific time period.

Test, Regression: Selective retesting of a system or component to verify that modifications have not caused unintended effects and that the system or component still complies with its specified requirements.

Traceability: The ability of software to allow users to follow every function from the requirements to the implementation, with respect to the specific development and operational environment.

Tuning (Software): Minor changes made to the system that does not affect the function or the functionality of a given system. These changes may occur at the shipyard during commissioning and/or sea-trials.

V&V: Verification and Validation of the integrated software program.

Validation: Determination that an item (system) is suitable for the intended service.

Verifiability: The capability of software to be proved or confirmed by examination or investigation.

Verification: Determination that an item (system) meets the specified criteria.

Verification, Closed Loop: The inputs to the system are simulated and/or manipulated and the system output is recorded and compared to expected results. The results are fed back to the inputs to the system.

Worst Case Failure (WCF): The identified single fault in the system resulting in maximum effect on the system's capability as determined through the FMEA study.

3 Abbreviations

The following definitions are applied to the abbreviations used in this Guide:

BCP: Bridge Control Panel

BOP: Blowout Preventer

ConOps: Concept of Operations document

CT: Sub-supplier or Sub-Contractor

DCO: Driller or Crew Organization

DCP: Driller Control Panel

DCU: Diverter Control Unit

DP: Dynamic Positioning

DPCS: Dynamic Positioning Control System

DPS: Dynamic Positioning System

EDS: Emergency Disconnect Sequence

FDD: Functional Description Document

FMEA: Failure Mode and Effects Analysis

FMECA: Failure Modes, Effects, and Criticality Analysis

HiPAP: High Precision Acoustic Positioning

HMI: Human Machine Interface

HPR: Hydro-acoustic Position Reference

HPU: Hydraulic Pump Unit

HW: Hardware

IEEE: Institute of Electrical and Electronics Engineers

IL: Integrity Level

I/O: Input/Output

ISQM: Integrated Software Quality Management

LMRP: Lower Marine Riser Package

MOC: Management of Change

MRU: Motion Reference Unit

NMEA: National Marine Electronics Association

PLC: Programmable Logic Controller

PMS: Power Management System

SBI: Ship Builder Integrator (Shipyard)

SDLC: Software Development Life Cycle

SDS: Software Design Specification

SIS: Safety Integrated System

SP: System Provider Organization

SRS: Software Requirement Specification

UPS: Uninterrupted Power Source

VRS: Vertical Reference Sensor

V&V: Verification and Validation Organization

APPENDIX **2**

Specific Systems *(1 September 2016)*

1 Dynamic Positioning Control Systems (DPCS)

Dynamic Positioning Control System (DPCS) is a computer-controlled system to automatically maintain the vessel's position and heading by means of propellers and thrusters. The Dynamic Positioning systems built and tested in compliance with the requirements in this Guide and relevant Rules may be assigned with different classification notations depending on the degree of redundancy built into the system as defined per **DPS-1**, **DPS-2**, or **DPS-3** classification. For a general model of what is to be simulated for DP verification, please refer to Appendix 2, Figure 1 below.

Assignment of the **SSV** notation for **DPS** does not validate that the vessel is capable of maintaining station or heading nor does it imply that the vessel has a DPS notation.

i) Environmental maximums is to be specified by the SBI

ii) Operational envelope is to be specified by the SBI

In addition, the following elements are to be considered and incorporated into the Verification Plan if not incorporated into one of the above for a specific installation:

i) Thruster Control System

ii) Power Management System

iii) DP Alert Functionality (including alarms verification)

1.1 ABS Dynamic Positioning Control System (DPCS) Verification –Requirements

For all thruster combinations, vary environmental conditions to demonstrate that the vessel remains within the theoretical (calculated) operational envelope within the vessel's capability plot.

i) Verification of primary and backup (for DPS-2 and 3) DP system during start up and shutdown:

- *a)* System's response to main and backup power failure
- *b)* DPCS' response to UPS battery failure scenarios
- *c)* DP system startup and shutdown
- *d)* DP system response to failure of other connected control systems
- *e)* Manual Position Control response
- *f)* DP operational modes
- *g)* Switching of primary operating stations and backup stations for DP3 only
- *h)* DPCS' response to reduced power signals (loss of one or more generators)

ii) Verification of environmental parameters (such as wind, current, etc.), refer to the ABS *Guide for Dynamic Positioning Systems:*

- ***a)*** HMI interface for DP functions for Wind, Current, Gyro, VRS and BOP functions, where applicable
- ***b)*** Gyrocompass sensors and failure scenarios
- ***c)*** Wind sensors and failure scenarios
- ***d)*** MRU sensors and failure scenarios
- ***e)*** BOP communication and failure scenarios, where applicable
- ***f)*** Redundancy test

iii) Position-keeping with worst-case single non-concurrent failure:

- ***a)*** Reference systems failure
- ***b)*** Position Reference System inputs and failure and degraded scenarios
- ***c)*** Primary and secondary PLC failure
- ***d)*** Interface failures between connected control systems
- ***e)*** Blackout scenarios
- ***f)*** Drift-off scenarios due to loss of position keeping

iv) Verification of reference systems and sensors required for DP control system:

- ***a)*** HMI interface for DP functions for position reference system
- ***b)*** Sensor failure and degraded scenarios
- ***c)*** NMEA transmission failure and degraded scenario

v) Verification of DP system interface with position reference systems and sensors:

- ***a)*** Third party systems
- ***b)*** Position Reference System inputs and failure scenarios
- ***c)*** Position and heading limitations
- ***d)*** Loss of gyrocompass signals to position reference systems

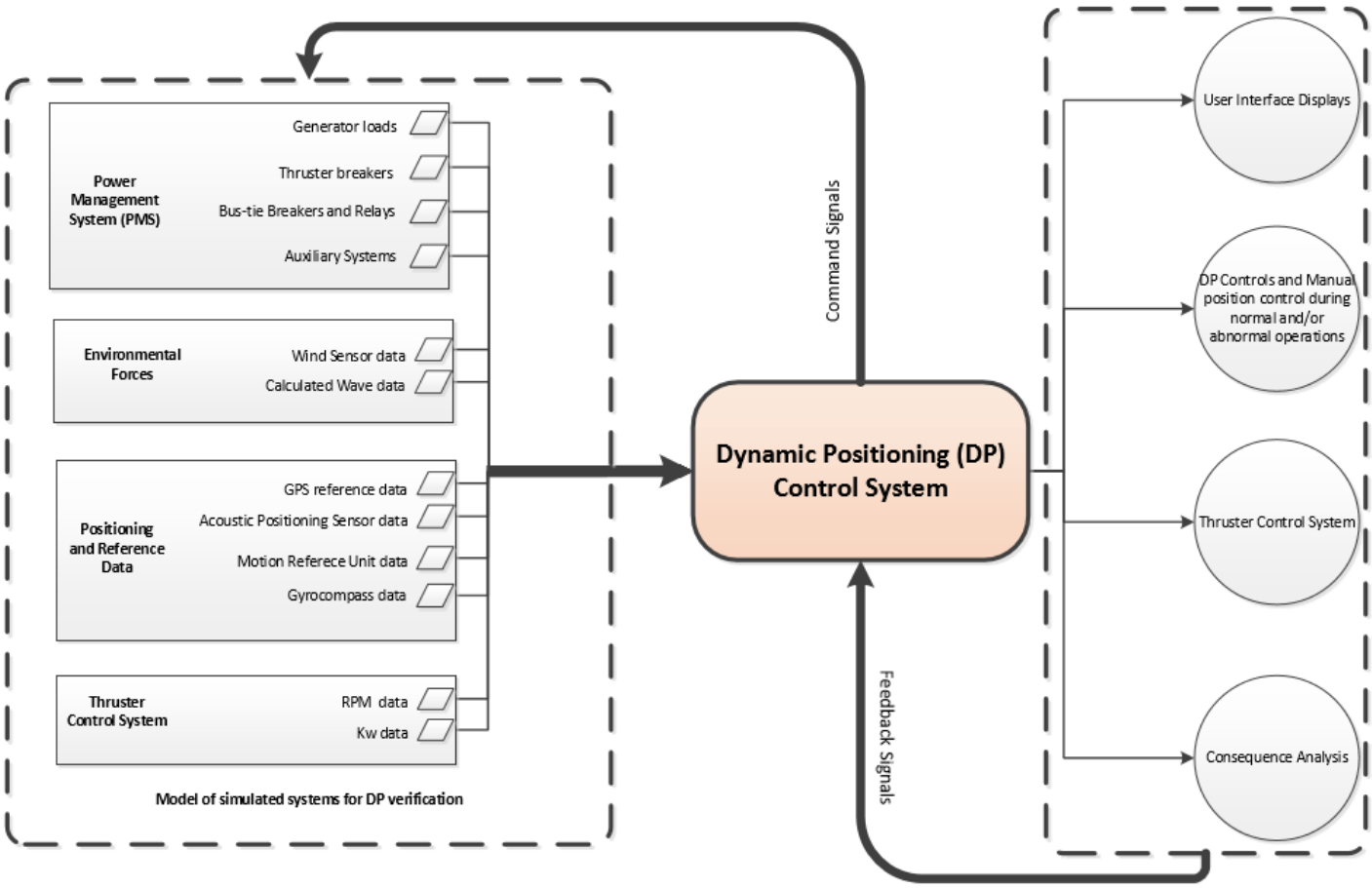
vi) Verification of DP system interface with other systems such as PMS, Thruster Control, Switchboards, and any third-party vendors connected to the DP system:

- ***a)*** Total network outage
- ***b)*** Position keeping with loss of communication with thrusters
- ***c)*** I/O error check
- ***d)*** Loss of redundancy
- ***e)*** Dynamic and Thruster biasing

vii) Verification of DP system alarms for all major functions:

- ***a)*** System response at boundary conditions
- ***b)*** Alarm and Warning prioritization
- ***c)*** Alarms and Warnings for reference data

FIGURE 1
Example of Simulation Model of Inputs for DP Verification



3 Power Management Control Systems (PMCS)

Accurate functioning and operation of the Power Management System is essential for a safe, reliable, and economical operation of the power generation and distribution system. A dependable source of power is critical for the successful operation of all major systems for operations. The PMS must be understandable, reliable, and operative. The PMS must keep operations personnel informed about the condition of the electrical power system, and should act promptly and effectively to prevent or correct situations which might result in an electrical blackout. Therefore, the PMS control system software should be thoroughly tested and verified before it is implemented. The input signals from connected systems (as listed below) can be simulated to test the PMS software. See Appendix 2, Figure 2 below for the simulation model to be verified.

- Engine Control Systems
- Governors
- Blackout Prevention (if equipped)
- Drilling Systems (if equipped)
- Blackout Recovery
- Blackout Recovery

3.1 ABS PMS Verification –Requirements

1) Failures of the Power Management Functions as identified from risk reduction analysis, FMEA, FMECA, and safety reviews

2) Verification of diesel engine generators functions:

- *a)* Engine start/stop during normal mode
- *b)* Engine start/stop failure scenario
- *c)* Safety or emergency shutdown system
- *d)* Generator automatic changeover system
- *e)* Generator alarms for all major functions
- *f)* Voltage, current and frequency deviation failure
- *g)* Normal, failed and degraded functions of operational modes

3) Verification of PMS load sharing functions:

- *a)* Load management system
- *b)* Consumer load sharing and limitations
- *c)* Automatic load dependent start/stop of the generators
- *d)* Load sharing during bus tie failure
- *e)* Fixed and Manual load sharing
- *f)* Load sharing failures during operational modes
- *g)* Overload failures and system reaction

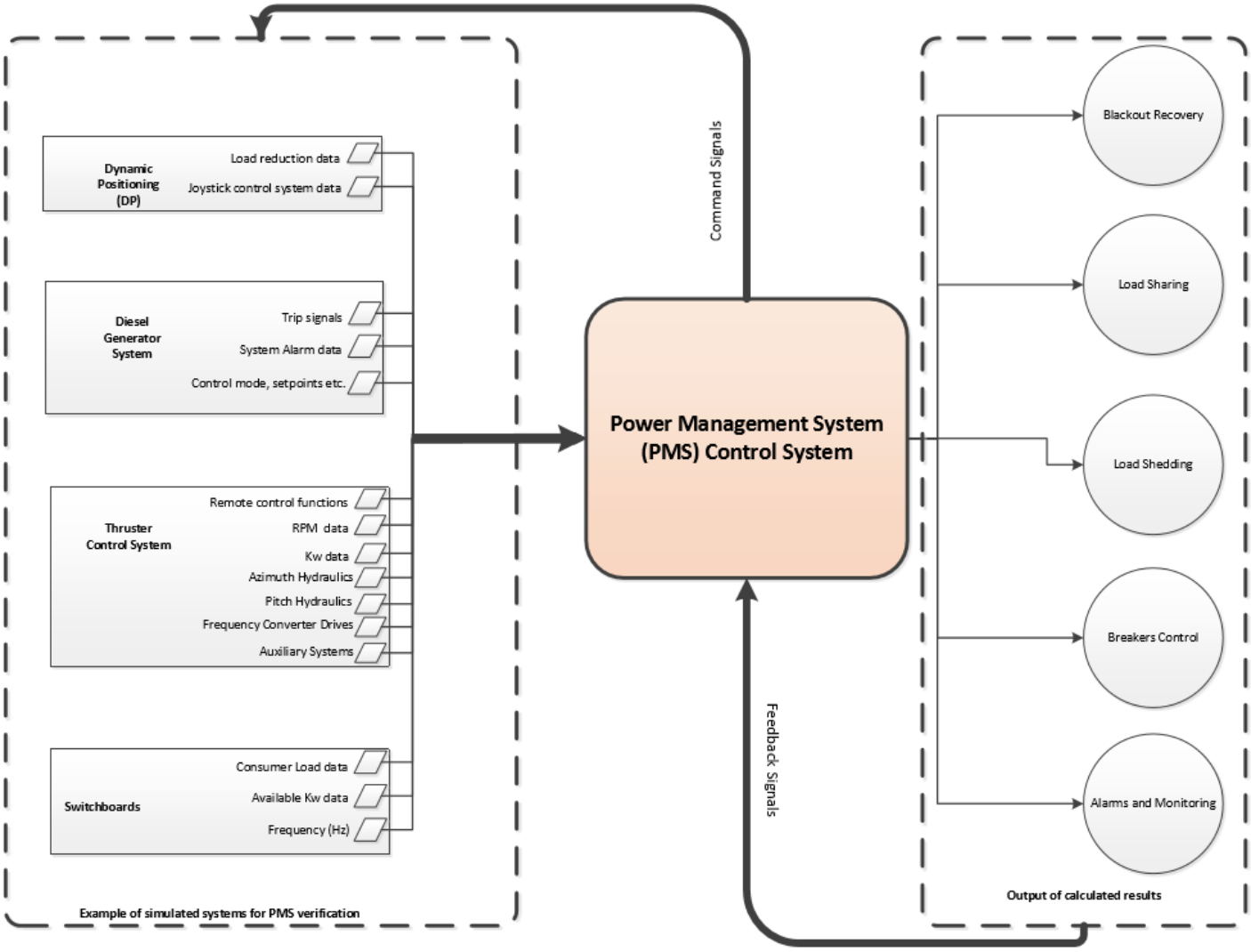
4) Verification of PMS blackout restart functions:

- *a)* Medium and Low Voltage Switchboards
- *b)* Circuit breakers to essential systems
- *c)* Restart of motors and pumps
- *d)* Power availability to all essential systems
- *e)* Open and closed bus tie configuration during blackout
- *f)* Blackout recovery (partial and full) in different operational modes

5) Verification of PMS emergency safety functions:

- *a)* Emergency shutdown function
- *b)* Safety functions
- *c)* Interface with all connected control systems to PMS

FIGURE 2
Example of Simulation Model of Inputs for PMS Verification



5 Thruster Control Systems (TCS)

i) The purpose of the Thruster Control System is to control the movement and operate the thrusters under any environment. Thruster Control System plays a key role in station-keeping and stability of the vessel. Thruster Control System is essential for normal operations.

ii) For a simulation model of what is to be tested, see Appendix 2, Figure 3 below for inputs to the Thruster Control System.

iii) Thruster Control System is to be verified for Worst Case Failure.

iv) Failed thruster scenarios are to be verified via re-testing until they pass.

5.1 ABS Thruster Control System Verification – Requirements

The purpose of the verification of the Thruster Control System is to provide reliable, safe, and efficient operations of all thrusters in a vessel.

i) Verification of remote control of all thrusters

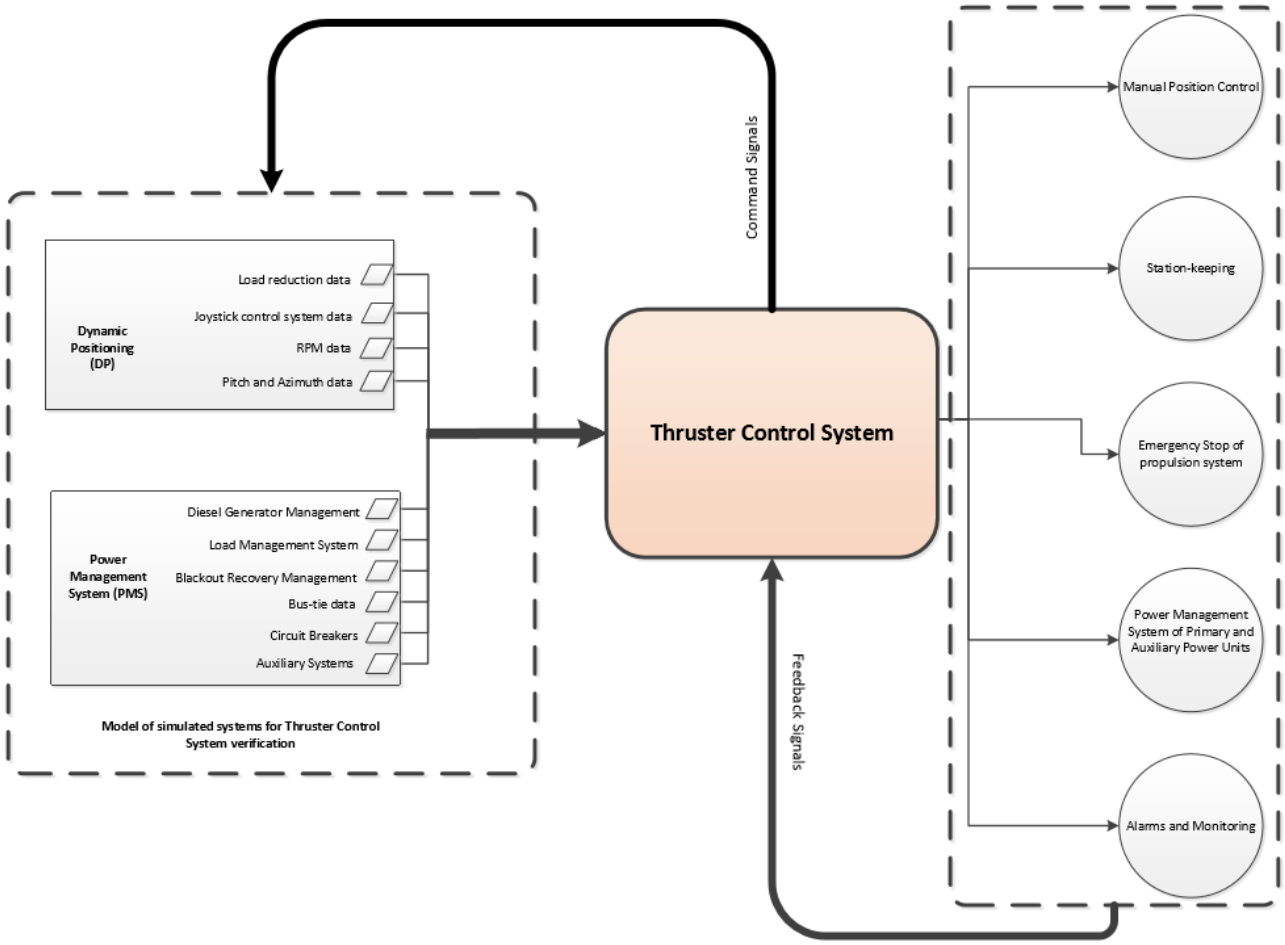
ii) Verification of automatic control of all thrusters during Autopilot of DP operations

iii) Verification of thruster ready signal for DP operations

iv) Thruster blackout recovery (i.e., sequential starting to prevent generator overload)

v) Thruster allocation for vessels with azimuth thrusters

FIGURE 3
Example of Simulation Model of Inputs for TCS Verification



7 Well Control System (WCS)

i) A well control system is critical to the safety of crew, the asset, the environment. Blow Out Preventer (BOP) being one of the essential and safety critical control systems, plays a vital role in controlling a well. The associated subsystems provided in this section are intended to provide fail-safety to the overall system. For a simulation model of what is to be tested, see Appendix 2, Figure 4 below for inputs to the BOP Control System

ii) BOP Control System is to be verified for failures.

iii) Degraded and failed BOP scenarios are to be verified.

iv) The BOP control system software process is to be (See API specification 16D)

- *a)* Traceable
- *b)* Consistent
- *c)* Documented

d) Repeatable

e) Auditable

7.1 ABS BOP Control System Verification – Requirements

The purpose of the verification of the BOP system is to provide reliable BOP control system through verifying the software functions as listed in the V&V Plan. As an example, this section provides testing requirements for BOP control system. In order to get an effective testing of the BOP control system, input signals from connected systems such as Choke & Kill manifold, LMRP, Acoustic systems and other third party systems are to be simulated.

1) Verification of Diverter Control Unit (DCU) functions as listed in the system description and interfaces between Operator panel (HMI) for remote control and alarms:

a) HMI interface for DCU functions b

b) Inputs from Flow meters

c) Pump control from DCU

d) Diverter valve operations from DCU

e) Diverter shutdown sequence

f) Upper and Lower Telescopic Joint Packers control from DCU

g) Alarms associated with DCU functions

h) Interlocks

2) Verification of automatic modes, primary and secondary pump functions of HPU, circulation pump operations, and alarms:

a) HMI interface from HPU functions

b) HPU pump operations for all included pumps

c) HPU valve operations for all included valves

d) Filters and Tank monitoring functions

e) Interfaces with connected control systems to HPU

3) Verification of the functions of mixing unit valve selections, and related alarms:

a) HMI interface for Flow meter functions

b) Mixing functions

c) Mixing Unit pump operations for all included pumps

d) Mixing Unit valve operations for all included valves

e) Interfaces with connected control systems to Mixing Unit

4) Verification of subsea boosting system and related alarms:

a) HMI inputs for boosting system functions

b) Boosting system pump operations for all included pumps

5) Verification of Driller Control Panel (DCP) functions, and related alarms:

a) HMI interface for DCP functions

b) Startup and shutdown of DCP system

c) Primary and backup Power Supply communications with control panel

d) DCP system interlock functions

e) Interfaces with connected control systems to DCP

f) Subsea valve data from DCP

6) Verification of interface and power distribution and communication functions to all (primary and secondary PLCs:

a) HMI interface for PLC control

b) Startup and shutdown of PLCs

c) Primary and backup Power Supply with control panel

d) Event logger

7) Verification of subsea control module data and interface with topside control panels:

a) Redundancy

b) Interfaces with connected control systems required for EDS

8) Verification of EDS including triggers and alarms:

a) HMI interface and monitoring for EDS functions

b) Interfaces with connected control systems required for EDS sequence

c) Line fault detection during EDS

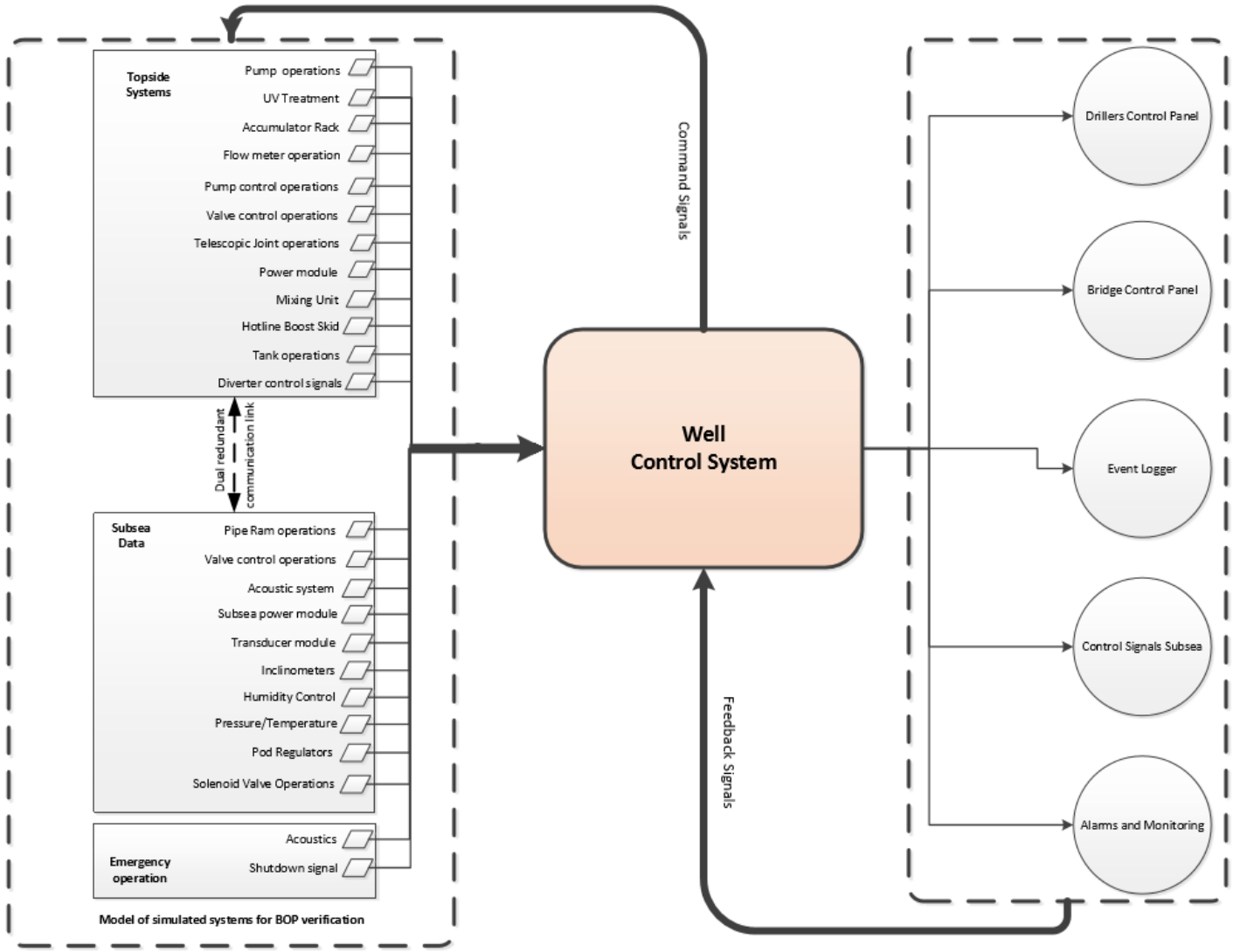
9) Choke and Kill Functionality

10) Lower Marine Riser Package signals

11) Acoustic control systems

12) Verification of interfaces with third party control systems connected to the BOP

FIGURE 4
Example of Simulation Model of Inputs for BOP Verification *(1 September 2016)*



APPENDIX 3

Definition of Independence

1 Types of Independence

1.1 Technical Independence

Technical independence requires the verification and validation (V&V) effort to utilize personnel who are not involved in the development of the software. The Independent V&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 software tools, technical independence means that the Independent V&V effort uses or develops its own set of test and analysis program separate from the developer's tools. Sharing of tools is allowable for computer support environments (e.g., compilers, assemblers, utilities) or for system simulations. For shared tools, the Independent V&V conducts qualification tests on tools to ensure that the common tools do not contain errors that may mask errors in the software being analyzed and tested. Off-the-shelf tools that have an 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.

1.3 Managerial Independence

This requires that the responsibility for the Independent V&V effort be vested in an organization separate from the development and program management organizations. Managerial independence also means that the Independent V&V independently selects the segments of the software and system to analyze and test, chooses the Independent V&V techniques, defines the schedule of Independent V&V activities, and selects the specific technical issues and problems to act upon. The Independent V&V effort provides its findings in a timely fashion simultaneously to both the development and program management organizations. The Independent V&V effort must be allowed to submit to program management the Independent V&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.

1.5 Financial Independence

This requires that control of the Independent V&V budget be vested in an organization independent of the development organization. This independence prevents situations where the Independent V&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.

1.7 Independence of the V&V Organization

ABS is to classify the independence of the V&V organization as established in IEEE Std 1012 – 2004, Annex C.

i) Classical

ii) Modified

iii) Integrated

iv) Internal

v) Embedded

3 Classically Independent Verification Organization

ABS reviews the V&V organization for technical, managerial, and financial independence from the SP of the system(s) under test. The Independent V&V organization is classically independent if it is technically, managerially, and financially independent from the software development enterprise that developed the software being tested. A classical Independent V&V organizational structure is to be applied to software V&V that can result in loss of life, loss of mission, loss of significant physical/financial assets, or loss of public confidence (e.g., IL2 and IL3 software components).

3.1 Technical Independence

Technical independence is reviewed based on the following criteria:

i) Independent V&V organization routinely works independently and without direction from the organization that developed the software subjected to V&V testing.

ii) Independent V&V organization formulates unbiased opinions of the software being subjected to V&V testing.

iii) Independent V&V organization develops test assumptions, test techniques, test inputs, test tools, and test environments internally and without direction from the organization that developed the software subjected to V&V testing.

iv) Independent V&V organization is allowed to select the software components to analyze and test without direction from the organization that developed the software subjected to V&V testing, subject to System Provider or development team guidance in safe operating practices during V&V testing.

v) Independent V&V organization is allowed to document test findings without influence from the organization that developed the software subjected to V&V testing.

3.3 Managerial Independence

Managerial independence is reviewed based on the following criteria:

i) Independent V&V organization is not affiliated with the company that develops the software subjected to V&V testing.

ii) Independent V&V organization is an organization identified within the software supplier company as being separate from the development organization, and reports to a management level above the operations director responsible for development of the subjected to V&V testing.

iii) Independent V&V organization is staffed by personnel who did not participate in the development of the software subjected to V&V testing.

iv) Independent V&V organization plans and executes software testing without direction from the organization that developed the software subjected to V&V testing.

v) Independent V&V organization defines the test schedule without direction from or alteration by the organization that developed the software subjected to V&V testing.

vi) Independent V&V organization is not subject to peer pressure or supervisory pressure from the organization that developed the software subjected to V&V testing when making test decisions or assessments, except for System Provider or development team guidance in safe operating practices during V&V testing.

3.5 Financial Independence

Financial independence is reviewed based on the following criteria:

i) Independent V&V organization operates from a budget not directly affiliated with the budget of the organization that developed the software subjected to V&V testing.

ii) Independent V&V budget is specifically identified in the project or departmental budget at a level above the organization that developed the software subjected to V&V testing.

iii) Independent V&V budget is not alterable by the organization that developed the software subjected to V&V testing.

5 Other than Classically Independent Verification Organization

Other forms of V&V organization may be used for IL0 and IL1 systems based on special considerations by ABS and acceptance by the Owner. The allowed Independent V&V forms are shown below as classical, modified, integrated, internal, and embedded. The internal and embedded Independent V&V forms are not preferred by ABS, but allowable with special consideration by ABS for software modules that are rated no higher than IL0 and IL1.

TABLE 1
IEEE Independent V&V Organization Independence Characteristics

V&V Independence Matrix		*Independent V&V Organizational Areas*				
Independence Category	*Conditions Contributing to V&V Independence*	*Classical*	*Modified*	*Integrated*	*Internal*	*Embedded*
Technical	Independent V&V staff are routinely assigned to testing activities	✓	✓	✓	✓	
	Independent V&V staff are capable of forming unbiased opinions of work product	✓	✓	✓		
	Independent V&V organization independently defines test assumptions, techniques, tools, inputs, environments	✓	✓			
	Independent V&V staff are responsible for selecting the components to test	✓	✓	✓	✓	✓
	Independent V&V staff are responsible for selecting the technical issues to work/resolve	✓	✓		✓	✓
Managerial	Independent V&V organization isnot affiliated with developing company	✓				
	Independent V&V is organizationally above and separated from the development function within the company		✓			
	Independent V&V organization is staffed by non-development personnel	✓	✓	✓		
	Independent V&V staff execute tesing without direction from development personnel/ management	✓	✓	✓		
	Independent V&V staff are allowed to define test schedule	✓		✓	✓	✓
	Independent V&V staff are not subject to developer peer/mamangement pressure	✓				
Financial	Independent V&V budget is separate from developmnet budget	✓	✓	✓		
	Independent V&V budget is controlled at a level above development budget	✓	✓	✓		
	Independent V&V budget is not alterable by development management	✓	✓	✓	✓	✓

5.1 Modified Independent V&V Form

This Independent V&V form is acceptable with special consideration by ABS. Modified Independent V&V is typically managed by a prime system integrator that acts as a customer advocate, manages the project budget containing a V&V set aside, objectively selects development organizations, objectively

selects Independent V&V organizations, does not participate in software development, and requests special considerations by ABS for V&V of system modules rated at IL3. A modified Independent V&V organizational structure may be applied to software V&V when a system integrator acts as a customer advocate, manages project budget containing a V&V set aside, objectively selects development organizations, objectively selects Independent V&V organizations, does not participate in software development, and requests special considerations by ABS for V&V of system modules rated IL3.

5.1.1 Technical Independence

Technical independence is reviewed based on the following criteria:

i) Independent V&V organization routinely works independently and without direction from the organization that developed the software subjected to V&V testing.

ii) Independent V&V organization formulates unbiased opinions of the software being subjected to V&V testing.

iii) Independent V&V organization develops test assumptions, test techniques, test inputs, test tools, and test environments internally and without direction from the organization that developed the software subjected to V&V testing.

iv) Independent V&V organization is allowed to select the software components to analyze and test without direction from the organization that developed the software subjected to V&V testing, subject to System Provider or development team guidance in safe operating practices during V&V testing.

v) Independent V&V organization is allowed to select the technical issue and problems (e.g., corrective actions) to act upon and/or resolve without influence from the organization that developed the software subjected to V&V testing.

5.1.2 Managerial Independence

Managerial independence is reviewed based on the following criteria:

i) Independent V&V organization is an organization identified within the software supplier company as being separate from the development organization, and reports to a management level above the operations director responsible for development of the subjected to V&V testing.

ii) Independent V&V organization is staffed by personnel who did not participate in the development of the software subjected to V&V testing.

iii) Independent V&V organization plans and executes software testing without direction from the organization that developed the software subjected to V&V testing.

5.1.3 Financial Independence

Financial independence is reviewed based on the following criteria:

i) Independent V&V organization operates from a budget not directly affiliated with the budget of the organization that developed the software subjected to V&V testing.

ii) Independent V&V budget is specifically identified in the project or departmental budget at a level above the organization that developed the software subjected to V&V testing.

iii) Independent V&V budget is not alterable by the organization that developed the software subjected to V&V testing.

5.3 Integrated Independent V&V Form

This Independent V&V form is acceptable with special consideration by ABS. Integrated Independent V&V is performed under formal revision control during build cycles while the software is constructed, with final V&V being performed at the time of software release to the customer. Key to the use of an

integrated Independent V&V organization is technical independence (or impartiality) during final test through management oversight and key aspects of financial and managerial independence. An integrated Independent V&V organizational structure may be applied to software V&V when certain aspects of technical, managerial, and financial independence listed below are in place during final test. Special consideration by ABS is needed if the Independent V&V organization reports to the development team, and the development team also developed code being subjected to Independent V&V. Special consideration by ABS is also needed for Independent V&V of system modules rated IL2 and IL3 when using this form of Independent V&V.

5.3.1 Technical Independence

Technical independence is reviewed based on the following criteria:

i) Independent V&V organization routinely works independently and without direction from the organization that developed the software subjected to V&V testing.

ii) Independent V&V organization formulates unbiased opinions of the software being subjected to V&V testing.

iii) Independent V&V organization is allowed to select the software components to analyze and test without direction from the organization that developed the software subjected to V&V testing, subject to System Provider or development team guidance in safe operating practices during V&V testing.

5.3.2 Managerial Independence

Managerial independence is reviewed based on the following criteria:

i) Independent V&V organization is staffed by personnel who did not participate in the development of the software subjected to V&V testing.

ii) Independent V&V organization plans and executes software testing without direction from the organization that developed the software subjected to V&V testing.

iii) Independent V&V organization defines the test schedule without direction from or alteration by the organization that developed the software subjected to V&V testing.

5.3.3 Financial Independence

Financial independence is reviewed based on the following criteria:

i) Independent V&V organization operates from a budget not directly affiliated with the budget of the organization that developed the software subjected to V&V testing.

ii) Independent V&V budget is specifically identified in the project or departmental budget at a level above the organization that developed the software subjected to V&V testing.

iii) Independent V&V budget is not alterable by the organization that developed the software subjected to V&V testing.

5.5 Internal Independent V&V Form

This Independent V&V form is allowable for V&V of software components rated as IL0 and IL1, with special consideration by ABS.

5.5.1 Technical Independence

Technical independence is reviewed based on the following criteria:

i) Independent V&V organization routinely works independently and without direction from the organization that developed the software subjected to V&V testing.

ii) Independent V&V organization is allowed to select the software components to analyze and test without direction from the organization that developed the software subjected to

V&V testing, subject to System Provider or development team guidance in safe operating practices during V&V testing.

iii) Independent V&V organization is allowed to select the technical issue and problems (e.g., corrective actions) to act upon and/or resolve without influence from the organization that developed the software subjected to V&V testing.

5.5.2 Managerial Independence

Managerial independence is reviewed based on the following criteria:

i) Independent V&V organization defines the test schedule without direction from or alteration by the organization that developed the software subjected to V&V testing.

5.5.3 Financial Independence

Financial independence is reviewed based on the following criteria:

i) Independent V&V budget is not alterable by the organization that developed the software subjected to V&V testing.

5.7 Embedded Independent V&V Form

This Independent V&V form is allowable for V&V of software components rated as IL0 and IL1, with special consideration by ABS.

5.7.1 Technical Independence

Technical independence is reviewed based on the following criteria:

i) Independent V&V organization is allowed to select the software components to analyze and test without direction from the organization that developed the software subjected to V&V testing, subject to System Provider or development team guidance in safe operating practices during V&V testing.

ii) Independent V&V organization is allowed to select the technical issue and problems (e.g., corrective actions) to act upon and/or resolve without influence from the organization that developed the software subjected to V&V testing.

5.7.2 Managerial Independence

Managerial independence is reviewed based on the following criteria:

i) Independent V&V organization defines the test schedule without direction from or alteration by the organization that developed the software subjected to V&V testing.

5.7.3 Financial Independence

Financial independence is reviewed based on the following criteria:

i) Independent V&V budget is not alterable by the organization that developed the software subjected to V&V testing.