



GUIDE FOR

SOFTWARE SYSTEMS VERIFICATION

ABS CyberSafety™ VOLUME 4

SEPTEMBER 2016

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

© 2016 American Bureau of Shipping. All rights reserved.
ABS Plaza
16855 Northchase Drive
Houston, TX 77060 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 CyberSafety™ 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-In-the-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

ABS CyberSafety™ VOLUME 4

CONTENTS

SECTION 1	General	1
1	Purpose and Scope	1
3	Basis of Notation	1
5	References	1
5.1	ABS	1
5.3	IEEE	2
5.5	IEC	2
5.7	ISO	3
5.9	Other	3
7	Organizations	3
9	Quality Program and Training for V&V	4
9.1	Quality Program	4
9.3	Training	4
11	Independence of the Verification Organization	4
11.1	Classically Independent Verification Organization	4
11.3	Other than Classically Independent Verification Organization	4
13	Safety of Personnel and Equipment	5
13.1	Safety Considerations	5
13.3	Onboard Testing	5
SECTION 2	Introduction	6
1	Background	6
3	Verification Methods	6
3.1	Software-In-the-Loop (SIL) Testing	7
3.3	Hardware-In-the-Loop Testing (HIL)	7
3.5	Closed Loop	7
3.7	Cybersecurity Testing	7
5	Boundaries and Limitations of the SSV Notation	7
5.1	Focus on Software	8
FIGURE 1	ISQM's Software Development Life Cycle	6

SECTION 3	Verification and Documentation.....	9
1	General	9
1.1	Traceability of Functions across Documents	9
1.3	Integrity Level Assignments	9
1.5	Network Data Information	9
1.7	Connected Instrumentation Listing	9
1.9	Risk Management.....	10
3	Documentation to be Submitted	10
3.1	System Functional Description	10
3.3	Safety Analysis Report	11
3.5	Verification Plan and Verification Scope	12
3.7	Verification Report	12
3.9	Simulator Hardware	13
3.11	Simulation Software	13
5	SSV is Applicable to (but not limited to) the Following Control Systems	13
5.1	Dynamic Positioning Control System.....	13
5.3	Power Management Control System	13
5.5	Thruster Control System.....	14
5.7	Blowout Preventer (BOP)	14
7	Re-testing.....	15
9	Simulation Program Maintenance.....	15
SECTION 4	Surveys After Construction and Maintenance of Class	16
1	General	16
3	Surveys for the Software Systems Verification (SSV) Notation.....	16
3.1	Survey Intervals and Maintenance Manuals/Records.....	16
3.3	Annual Surveys	16
3.5	Special Periodical Surveys	17
5	Modifications, Damage and Repairs.....	17
APPENDIX 1	Terminology	18
1	Definitions	18
3	Abbreviations	20
APPENDIX 2	Specific Systems	22
1	Dynamic Positioning Control Systems (DPCS)	22
1.1	ABS Dynamic Positioning Control System (DPCS) Verification – Requirements	22
3	Power Management Control Systems (PMCS)	24
3.1	ABS PMS Verification –Requirements.....	25
5	Thruster Control Systems (TCS).....	26
5.1	ABS Thruster Control System Verification – Requirements	26
7	Well Control System (WCS).....	27
7.1	ABS BOP Control System Verification – Requirements.....	28

FIGURE 1	Example of Simulation Model of Inputs for DP Verification	24
FIGURE 2	Example of Simulation Model of Inputs for PMS Verification	26
FIGURE 3	Example of Simulation Model of Inputs for TCS Verification	27
FIGURE 4	Example of Simulation Model of Inputs for BOP Verification	30

APPENDIX 3	Definition of Independence	31
1	Types of Independence	31
1.1	Technical Independence	31
1.3	Managerial Independence	31
1.5	Financial Independence	31
1.7	Independence of the V&V Organization	31
3	Classically Independent Verification Organization	32
3.1	Technical Independence	32
3.3	Managerial Independence	32
3.5	Financial Independence	32
5	Other than Classically Independent Verification Organization	33
5.1	Modified Independent V&V Form	33
5.3	Integrated Independent V&V Form	34
5.5	Internal Independent V&V Form	35
5.7	Embedded Independent V&V Form	36
TABLE 1	IEEE Independent V&V Organization Independence Characteristics	33

This Page Intentionally Left Blank



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 Steel Vessels (Steel 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 computer-based 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 Subsection 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 Steel Vessels

ABS Guide for Dynamic Positioning Systems

ABS Guide for Integrated Software Quality Management (ISQM)

ABS Guide for Risk Evaluations for the Classification of Marine Related Facilities

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 Application for the Marine and Offshore Oil and Gas 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 CyberSafety™ Volume 1

ABS Guide for Cybersecurity Implementation for the Marine and Offshore Operations – ABS CyberSafety™ Volume 2

ABS Guidance Notes on Data Integrity for Marine and Offshore Operations – ABS CyberSafety™ Volume 3

ABS Guidance Notes on Software Provider Conformity Program – ABS CyberSafety™ 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*

5.7 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.**

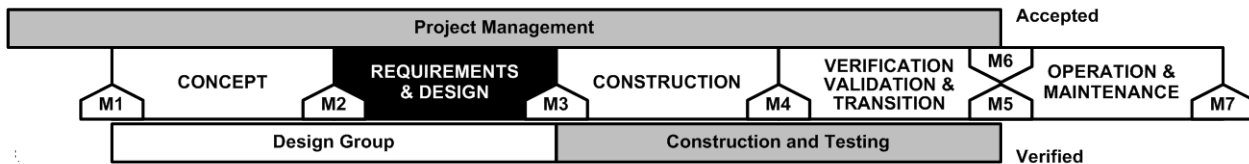
13.3 Onboard Testing

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)*. Verification¹ 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.

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 *Steel 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.

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.

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, machine-to-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 threats², ABS will work with the V&V organization to include appropriate tests to complement the functional verification methods above.

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

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.