Guidance Notes on

Software Provider Conformity Program

ABS CyberSafety™ Volume 5

ABS

September 2016

GUIDANCE NOTES ON

SOFTWARE PROVIDER CONFORMITY PROGRAM
SEPTEMBER 2016

ABS CYBERSAFETY™ VOLUME 5

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 importance of the development of a positive safety culture has been recognized for some time, particularly in large-scale systems where the consequences of losses may be severe. The marine and offshore industries are increasingly reliant on computer-based control systems; therefore, the specification and verification of the software used in the control systems and their integration into the system is an important element of safety assessments. This document has been developed with the objective of improving safety and environmental performance of ships and offshore assets by providing a process to improve control system software quality. The American Bureau of Shipping (ABS) provides this guidance in recognition of the beneficial effect that high software quality installed in various control systems has on the performance of assets.

The ABS *Guide for Integrated Software Quality Management (ISQM)* presents a risk-based software development and maintenance process for application on ships and offshore assets that is based upon internationally recognized standards. These Guidance Notes augment the *ISQM Guide* by documenting procedures and recommendations developed with input from ABS clients and software development professionals and best practices for quality software development. The guidance provided is based on industry-accepted software quality development activities and practices that are applicable to software System Providers (SPs) who are internally implementing and evaluating their application of ABS' ISQM processes. The Guidance Notes are also intended to help providers of control system software gain recognition of their quality software development policies, procedures, and practices. The guidance is applicable to all divisions, groups, and companies engaged in developing, supplying, deploying, and maintaining software, and provides information to assist SPs in preparing for ABS' ISQM conformity assessments.

The information in this document is sufficiently general to allow SPs appropriate latitude in software development practices, yet sufficiently detailed so as to provide useful guidance to SPs as they implement an ISQM conformant quality assurance program. The ISQM conformity program is patterned upon three (3) of five (5) Tiers of Approval described in Appendix 1-1-A4 of the ABS *Rules for Conditions of Classification (Part 1)* (Part 1 of the ABS *Rules for Building and Classing Marine Vessels (Marine Vessel Rules)*) and Appendix 1-1-A3 of the ABS *Rules for Conditions of Classification – Offshore Units and Structures (Part 1)* (Part 1 of the ABS *Rules for Building and Classing Mobile Offshore Units (MOU Rules)*). Although ABS does not offer type approval for software, Approval Tiers 1, 2 and 5 of the Marine Vessel Rules Type Approval are well suited for software quality management process certification, and are applied with certain alterations to the ABS ISQM Conformity Certification program. For comparison, Table 1 indicates the Tiers applicable to Marine Vessel Rules Approval and the Tiers applicable to the ISQM Conformity Certification.

TABLE 1
ISQM Conformity Program Based on Marine Vessel Rules Approval Tiers

Marine Vessel Rules Approval Tiers		*ISQM Certification Tiers*	
Tier 1	Manufacturer's Certification (MC)	Tier 1	***Manufacturer's Certification (MC)***
Tier 2	Product Design Assesment (PDA)	Tier 2	***Product Design Assesment (PDA)***
Tier 3	Type Approval (TA)	Tier 3	Not Applicable
Tier 4	Product Certification via Product Quality Assurance (PQA)	Tier 4	Not Applicable
Tier 5	Unit Certification via Survey During Fabrication (UC)	Tier 5	***Unit Certification via Survey During Final Test (USC)***

These Guidance Notes become 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 these Guidance Notes is the most current.

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

Terms of Use

The information presented herein is intended solely to assist the reader in the methodologies and/or techniques discussed. These Guidance Notes do not and cannot replace the analysis and/or advice of a qualified professional. It is the responsibility of the reader to perform their own assessment and obtain professional advice. Information contained herein is considered to be pertinent at the time of publication, but may be invalidated as a result of subsequent legislations, regulations, standards, methods, and/or more updated information and the reader assumes full responsibility for compliance. This publication may not be copied or redistributed in part or in whole without prior written consent from ABS.

GUIDANCE NOTES ON

SOFTWARE PROVIDER CONFORMITY PROGRAM

CONTENTS

SECTION **1**

Introduction

1 Software Quality

1.1 Introduction

The intended outcome of applying the American Bureau of Shipping (ABS) ISQM program to software development include improving the quality of software in the marine and offshore industries; expedited reviews and approvals; and providing a level of confidence that products available from the System Providers (SP) are developed so as to meet the minimum quality requirements set forth in the ABS *Guide for Integrated Software Quality Management (ISQM) (ISQM Guide).*

ISQM practices and processes are provided to help the SP establish a program that reinforces quality in the configuration and development of control system software. In addition to direct and specific application of ISQM to improve the quality of software, the SP may also find it useful to map internally developed quality assurance practices to those described in the *ISQM Guide*. By doing so, the SP can internally evaluate and measure its conformity to ISQM.

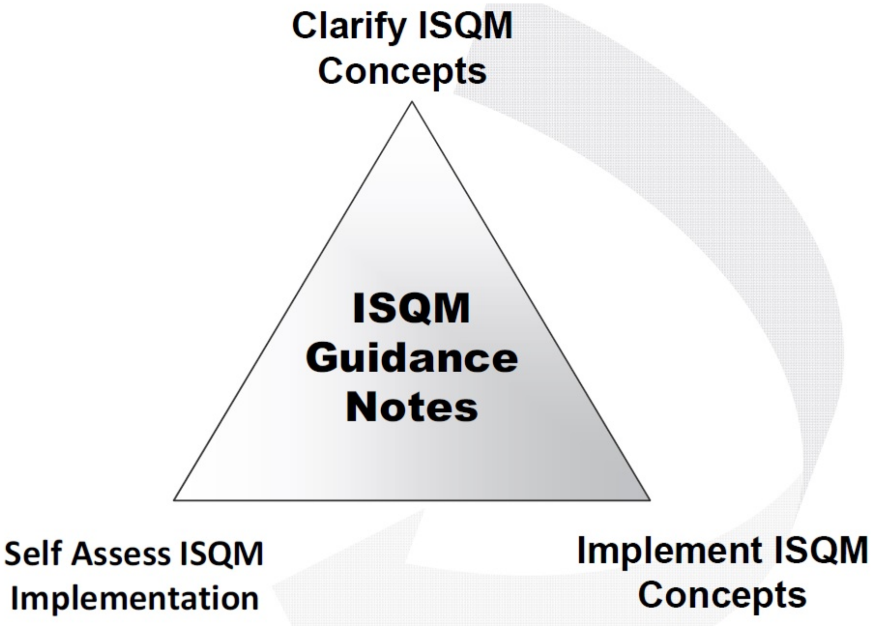
ABS has developed these Guidance Notes for managers, quality management personnel, and software developers engaged in software development or software quality assurance within SP organizations. These Guidance Notes are provided to:

i) Clarify the evaluation processes required for ABS conformity recognition

ii) Offer additional information to help the SP implement the ISQM principles

iii) Assist the SP in evaluating its conformity to the *ISQM Guide*

FIGURE 1
ISQM Guidance Notes



3 Three Tiers of Software Quality Assessment and Certification

3.1 Overview

The ISQM conformity program is patterned upon three (3) of five (5) Tiers of Approval described in Appendix 1-1-A4 of the ABS *Rules for Conditions of Classification (Part 1)* (Part 1 of the ABS *Rules for Building and Classing Marine Vessels (Marine Vessel Rules)*) and Appendix 1-1-A3 of the ABS *Rules for Conditions of Classification – Offshore Units and Structures (Part 1)* (Part 1 of the ABS *Rules for Building and Classing Mobile Offshore Units (MOU Rules)*). Although ABS does not offer type approval for software, Approval Tiers 1, 2 and 5 of the Marine Vessel Rules are well suited for software quality management process certification, and are applied with certain alterations to the ABS ISQM Conformity Certification program (Section 1, Table 1). For comparison, Section 1, Table 1 indicates the certification Tiers applicable to Marine Vessel Rules Type Approval (Section 4-9-3[1]), MOU Rules Type Approval (Section 4-3-4/5[2], Section 6-1-5[3]) and ISQM Conformity Certification.

Note:

[1] ABS *Marine Vessel Rules*, 2012; 4-9-3/1: “Computer based systems where used for control, monitoring and safety systems are to comply with the provisions of Section 4-9-3, and are subject to the classification requirements regardless of **ACC** or **ACCU** notation, see 4-9-3/Table 1 for examples. See 4-9-1/7.3.9 for plans and data to be submitted for review.”

[2] ABS *MOU Rules*, 2016; 4-3-4/5: “Computer-based systems are to meet the requirements of 4-9-3/3 of the Marine Vessel Rules, even when the drilling unit will not be assigned with **ACC** or **ACCU** notations.”

[3] ABS *MOU Rules*, 2016; Section 6-1-5: Survey and Certification

TABLE 1
Three Tiers of ISQM Conformity

Marine Vessel Rules Approval Tiers		*ISQM Certification Tiers*	
Tier 1	Manufacturer's Certification (MC)	Tier 1	*Manufacturer's Certification (MC)*
Tier 2	Product Design Assesment (PDA)	Tier 2	*Product Design Assesment (PDA)*
Tier 3	Type Approval (TA)	Tier 3	Not Applicable
Tier 4	Product Certification via Product Quality Assurance (PQA)	Tier 4	Not Applicable
Tier 5	Unit Certification via Survey During Fabrication (UC)	Tier 5	*Unit Certification via Survey During Final Test (USC)*

Demonstration of ISQM conformity by the supplier is recognized by ABS through the issuance of:

i) *A Manufacturer's Certification Letter of Acknowledgement* – Tier 1 conformity approval patterned upon the ABS Rules for Conditions of Classification (Part 1);

ii) A Product Design Assessment (PDA) certificate – Tier 2 conformity approval patterned upon the ABS *Rules for Conditions of Classification (Part 1);* and,

iii) A Unit Software Certification (USC) report – Tier 5 conformity approval patterned upon the ABS *Rules for Conditions of Classification (Part 1).*

ABS does not provide software approval for Tier 3 – Type Approval, or Tier 4 – Product Certification via Product Quality Assurance (PQA), as defined in the ABS *Rules for Conditions of Classification (Part 1)*. Type Approval of software products is not applicable because software is not "manufactured" in the conventional sense. Software is also subject to customization and frequent changes through field-installed updates and defect fixes, which makes Type Approval inappropriate for software. Additionally, Product Certification via PQA is conventionally applicable to Mass Produced Products, which is a process not commonly applied to software systems. Therefore, neither Tier 3 nor Tier 4 approval are applied to ISQM Conformity Certification.

3.1.1 Tier 1: Manufacturer's Certification (MC)

The System Provider (SP) initiates Tier 1 approval by notifying ABS of its desire to be assessed for conformity to ISQM USC or the ISQM PDA. At the same time, the SP provides a letter to ABS asserting or certifying that it implements an ISO 9001 quality management program or a recognized equivalent. ABS acknowledges receipt of the SP-provided Manufacturer's Certification, and collaborates with the SP to initiate the ABS USC or the ISQM PDA conformity certification assessment. No ABS certificate is issued, and ABS does not perform a quality management documentation review or on-site assessment in connection with the MC. The SP's documentary evidence that supports quality management certification is "M" classification documentation, and is to be kept by the SP and made available for review as requested by ABS. For additional information on documentation management refer to Section 4-9-3 of the *Marine Vessel Rules*, "M = Evidence kept by manufacturer and upon request checked by ABS."

TABLE 2
ISQM Manufacturer's Certification

Marine Vessel Rules Approval Tiers		*ISQM Certification Tiers*	
Tier 1	**Manufacturer's Certification (MC)**	**Tier 1**	***Manufacturer's Certification (MC)***
Tier 2	Product Design Assesment (PDA)	Tier 2	*Product Design Assesment (PDA)*

Marine Vessel Rules Approval Tiers		*ISQM Certification Tiers*	
Tier 3	Type Approval (TA)	Tier 3	Not Applicable
Tier 4	Product Certification via Product Quality Assurance (PQA)	Tier 4	Not Applicable
Tier 5	Unit Certification via Survey During Fabrication (UC)	Tier 5	*Unit Certification via Survey During Final Test (USC)*

3.1.2 Tier 2: ISQM Product Design Assessment

The ABS PDA for software is organized as two parts. Both parts are to be completed by the SP before an ABS ISQM PDA is issued. Part 1 is an offsite review of software quality engineering process documentation. Part 2 is an onsite assessment of the SP's implementation of its software quality process, and includes interviews with project management, quality and software development teams.

TABLE 3
ISQM Product Design Assesment

Marine Vessel Rules Approval Tiers		*ISQM Certification Tiers*	
Tier 1	Manufacturer's Certification (MC)	Tier 1	*Manufacturer's Certification (MC)*
Tier 2	**Product Design Assesment (PDA)**	**Tier 2**	***Product Design Assesment (PDA)***
Tier 3	Type Approval (TA)	Tier 3	Not Applicable
Tier 4	Product Certification via Product Quality Assurance (PQA)	Tier 4	Not Applicable
Tier 5	Unit Certification via Survey During Fabrication (UC)	Tier 5	*Unit Certification via Survey During Final Test (USC)*

3.1.3 Tier 2: Product Design Assessment – Part 1

The ISQM PDA-Part 1 assessment is a review of software quality management documentation pertinent to the software products to be named in the PDA or the USC. The ISQM-PDA-Part 1 assessment is an ABS review for indications that the SP possesses knowledge of the ISQM Guide, has implemented software quality management practices that conform to the ISQM Guide and recognized best practices, and has mapped its software quality processes to those described in these Guidance Notes in order to facilitate the assessment. The SP's software quality engineering documentation is "S" classification documentation, and is checked by ABS. For additional information on documentation management refer to Section 4-9-3 of the *Marine Vessel Rules*, S-category of documentation: "S = Evidence to be checked by ABS."

SP provided documentation is also reviewed for indications that formally documented software development life cycle development procedures, risk assessment and management procedures (i.e., safety reviews, FMEA or FMECA, revision control, etc.), and rigorous testing procedures (i.e., verification and validation) are in place.

The ISQM-PDA-Part 1 assessment is concluded after the ABS documentation review is complete, findings are reported to the SP. And the Findings are remedied by the SP. ABS' findings are communicated to the SP in a findings review meeting. To proceed to ISQM PDA-Part 2, the SP corrects any findings (shortfalls in process, procedure, or documentation) communicated by ABS.

The SP is allowed six (6) months from the date of ABS' findings communication meeting to respond to ABS with its remedies to findings. If ABS approves the remedies provided in the SP's response, the SP is issued an ISQM-PDA-Part 1 completion letter. From this point in the PDA assessment, the supplier may proceed with the PDA-Part 2 assessment in pursuit of an ISQM Product Design Assessment (PDA) Certification.

In the event the SP does not provide documentation to ABS that demonstrates remediation of ABS findings within the six-month period following the ISQM-PDA-Part 1 findings communication, the SP may not initiate a PDA-Part 2 assessment.

3.1.4 Tier 2: Product Design Assessment – Part 2

In continuation of the ISQM PDA assessment process, ABS provides the Product Design Assessment – Part 2 to document that ABS has reviewed the application-in-practice of the SP's quality processes, procedures, and tools in conformity to the *ISQM Guide* and these Guidance Notes. The PDA-Part 2 pertains only to the specific site, development team, and software products reviewed during the assessment.

ABS' PDA certification process includes an on-site assessment for conformance of the SP's implementation of quality processes in practice to the *ISQM Guide* and in these Guidance Notes. With special considerations by ABS, the assessment may also include an evaluation of the documents describing a previously completed project to which ISQM-mapped quality processes were applied. In this assessment, ABS witnesses a final integration/acceptance test and reviews a final report addressing any exceptions noted in the test. In the event that the Owner requests the SP to assign a unit/vessel number to the product as tested and witnessed, ABS may also provide a Unit Software Certification (USC) documenting that ABS witnessed the test of a specific product for a specific customer and application (typically a vessel or unit) as assigned.

Based on successful completion of the PDA-Part 2 assessment, the SP is issued an ISQM-PDA certificate that is published on the ABS website. This ISQM-PDA certification may be renewed every two years based on an ABS on-site assessment of the SP's software quality practices, with special considerations by ABS. Failure to complete a timely renewal of the PDA will result in expiration of the PDA and removal of the certificate from ABS' website.

3.1.5 Tier 5: Unit Software Certification (USC)

ABS issues the USC to an Owner and/or Operator of a vessel on which a specified software product is to be installed or deployed. The USC is provided after ABS receives an SP-provided MC letter, reviews pertinent software quality engineering documentation and witnesses a successful onsite final product test. The SP's software quality engineering USC documentation is "S" classification documentation, "S = Evidence to be checked by ABS." The final product test is witnessed by ABS, and is a "W" classification system test, "W = To be witnessed" by the ABS assessor. For additional information on documentation management refer to Section 4-9-3 of the *Marine Vessel Rules.*

TABLE 4
ISQM Unit Software Certification

Marine Vessel Rules Approval Tiers		*ISQM Certification Tiers*	
Tier 1	Manufacturer's Certification (MC)	Tier 1	*Manufacturer's Certification (MC)*
Tier 2	Product Design Assesment (PDA)	Tier 2	*Product Design Assesment (PDA)*
Tier 3	Type Approval (TA)	Tier 3	Not Applicable
Tier 4	Product Certification via Product Quality Assurance (PQA)	Tier 4	Not Applicable
Tier 5	**Unit Certification via Survey During Fabrication (UC)**	**Tier 5**	***Unit Certification via Survey During Final Test (USC)***

To initiate the USC, the Owner/Operator instructs the SP to notify ABS that the Owner/Operator is requesting a USC for a specified software product to be installed on a specified vessel. The SP provides an MC letter to ABS as well as pertinent product software quality engineering documents requested by ABS. The documents are reviewed offsite by ABS prior to the onsite witnessing of the final product test. The documents reviewed minimally include:

- The SP's software quality engineering policies and procedures
- Product's Functional Description Document (or ConOps, SRS and SDS) as described in the *ISQM Guide*
- Product safety review, FMEA and/or FMECA documentation
- Software management of change and configuration management policy and procedures
- Detailed test plan

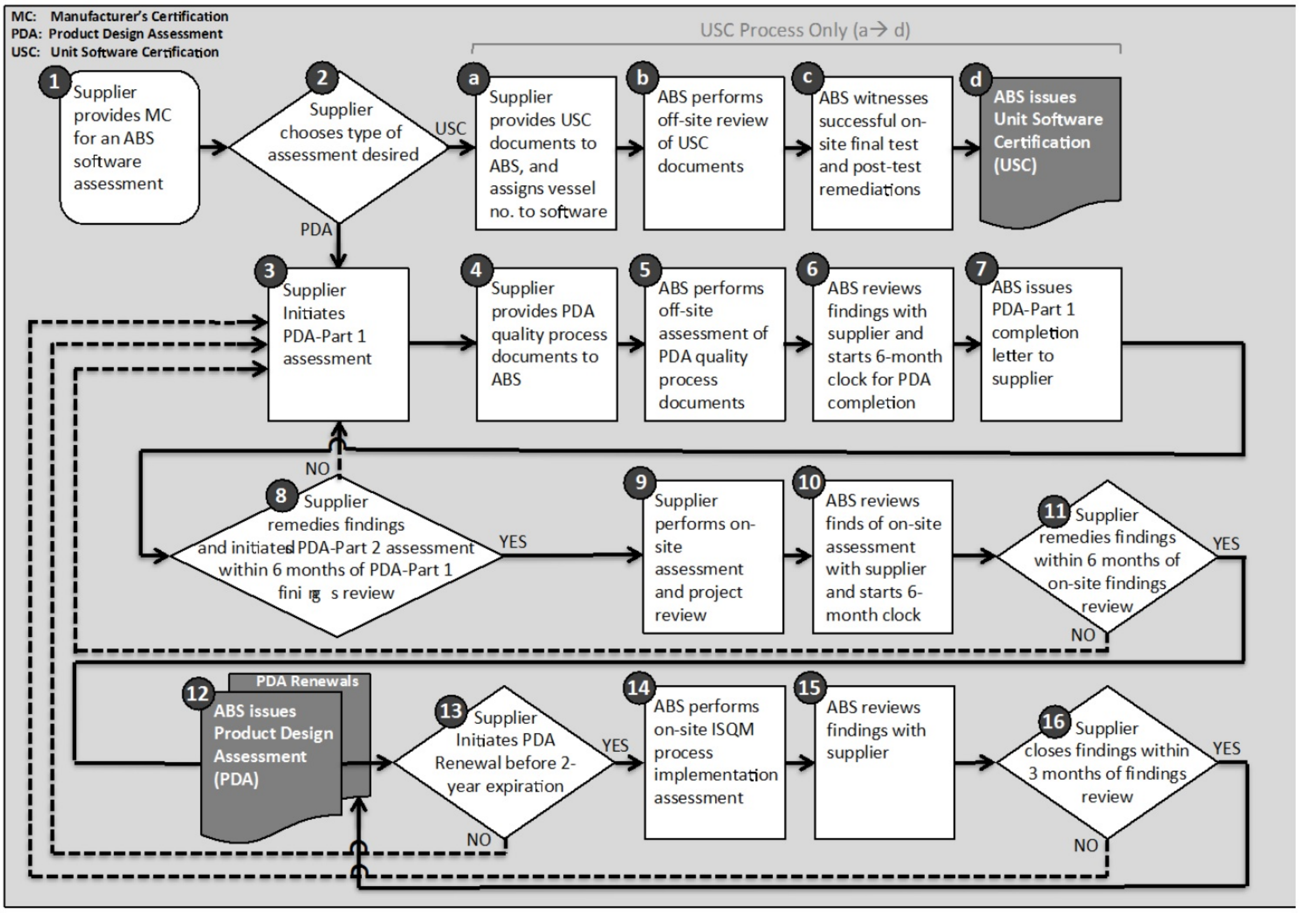
During the USC test activity, an ABS assessor witnesses the final product test (typically at the supplier site) of the software system being assessed for USC, witnesses meetings in which test issues are resolved with the Owner/Operator, witnesses any required retesting, reviews the SP's final test report, and responds to the SP and Owner/Operator with an ABS ISQM test report. If the software quality engineering documentation, test plan, test process, test outcomes, and final test report conform to ISQM practices, ABS provides a USC letter to the Owner/Operator that specifically names the equipment for which Owner requests certification.

The SP may elect to combine USC survey activities with PDA certification activities in order to efficiently and effectively demonstrate implementation of its software quality engineering processes

3.1.6 ISQM Conformity Certification Process Workflow

The ABS process for providing the three tiers of ISQM certification is provided in Section 1, Figure 2. In the conformity certification process graphic, the normal process flow is depicted as solid lines, and the remedial process flow is depicted as dashed lines.

FIGURE 2
ISQM Conformity Certification Process


MC: Manufacturer's Certification
PDA: Product Design Assessment
USC: Unit Software Certification
USC Process Only (a→ d)
1 Supplier provides MC for an ABS software assessment
2 Supplier chooses type of assessment desired
USC
PDA
a Supplier provides USC documents to ABS, and assigns vessel no. to software
b ABS performs off-site review of USC documents
c ABS witnesses successful on-site final test and post-test remediations
d ABS issues Unit Software Certification (USC)
3 Supplier Initiates PDA-Part 1 assessment
4 Supplier provides PDA quality process documents to ABS
5 ABS performs off-site assessment of PDA quality process documents
6 ABS reviews findings with supplier and starts 6-month clock for PDA completion
7 ABS issues PDA-Part 1 completion letter to supplier
NO
8 Supplier remedies findings and initiates PDA-Part 2 assessment within 6 months of PDA-Part 1 fini ng s review
YES
9 Supplier performs on-site assessment and project review
10 ABS reviews finds of on-site assessment with supplier and starts 6-month clock
11 Supplier remedies findings within 6 months of on-site findings review
YES
NO
PDA Renewals
12 ABS issues Product Design Assessment (PDA)
13 Supplier Initiates PDA Renewal before 2-year expiration
YES
NO
14 ABS performs on-site ISQM process implementation assessment
15 ABS reviews findings with supplier
16 Supplier closes findings within 3 months of findings review
YES
NO

3.3 Conformance to Quality Standards

Conformance to both explicit and implicit requirements as represented in specifications embodies the concept of quality for software. Explicit requirements as stated in specifications include the system's functional and performance criteria as guided by development (coding) standards – whether explicitly stated in the specification, or implicitly expected as inherent in quality software. Implicit requirements also include less quantifiable, but important operational and business software characteristics. Satisfaction of both explicit and implicit requirements, as verified in thorough system testing, combine to represent total software quality.

The three key points in this expression of software quality are:

i) Delivered software complies with the stated requirements;

ii) Delivered software is developed using appropriate development criteria (coding requirements) and specifications (user requirements); and,

iii) Delivered software meets implicit requirements.

- Implicit or extra-functional requirements are expected by the user to be satisfied in delivered software; however, those requirements may not be included in the coding specification. Examples of implicit (extra-functional) requirements include but are not limited to security, stability, usability, reliability, maintainability, testability, evolvability, etc. [4]

Note: [4] In software discussions, implicit requirements are sometimes referred to as the "…ilities" of requirements.

iv) If software conforms to its explicit requirements but fails to meet implicit requirements, software quality may be perceived as lacking.

The IEEE Standard for Software Quality Assurance Plans, 730-2002 provides guidance and details on Software Quality Assurance (SQA) organizations, activities, documents, reviews, etc.

i) Quality is defined as the sum total of characteristics and performance of a product or service that satisfies the stated or implied needs of customers. Viewpoints and relative importance concerning quality vary with respect to the different factors considered.

- The Owner's viewpoint may consider global quality, wherein the highest quality possible is provided within the selected equipment.
- The developer's viewpoint may consider adherence to and satisfaction of specifications throughout the software development life cycle, which in turn yields a high quality final product.
- The Operator's viewpoint may consider operational quality as characterized by consistent, predictable, safe performance of work by the integrated system throughout its specified operating life.

ii) Software quality is also characterized by how the software:

- Is designed (quality of design);
- Accurately resolves the design as software code (i.e., accuracy of coding execution); and
- Operates in the environment for which it is intended by faithfully fulfilling user needs and/or requirements.

3.5 Software Quality Activities and Metrics

3.5.1 Management

The most basic quality management requirements are to:

- Plan the project quality processes,
- Execute to the project according to the quality processes as planned, and
- Evaluate both the outcomes of the project and the execution of the project plan.

3.5.2 Planning

The IEEE Standard for Software Quality Assurance Plans, 730-2002 provides a table suggesting artifacts that are applicable in each of the SDLC phases. These include:

- Plans
- Specifications
- Descriptions
- Procedures
- Reports
- Records

3.5.3 Execution

Key to the execution of the plan is a well-developed functional test strategy. Referencing the IEEE 730 standard can guide a development organization and testers through a series of procedures and tests that are applicable to the system under development.

Peer reviews are effective for evaluating the software modules of individual development activities. These reviews are performed by development peers who check for compliance with a quality plan and development standards, for adherence to specification, and for comprehension of requirements. Also commonly referred to as "code walkthroughs", peer reviews as provided for in the IEEE Standard for Software Reviews 1028-1997, are defined as a process "…in which a designer or programmer leads members of the development team and other interested parties through a software product, and the participants ask questions and make comments about possible errors, violation of development standards, and other problems".

Project control review processes as suggested by the Project Management Institute's (PMI) Project Management Book of Knowledge (PMBOK®) are also useful for control of a software project. Reviews such as Preliminary Design Reviews and Critical Design Reviews are techniques used to evaluate both the cost and progress toward the schedule of a project. These reviews also provide opportunities to evaluate the execution of the quality plan.

3.5.4 Evaluation

Software quality evaluation includes techniques and operational activities that are used to control the accurate fulfillment of quality requirements. It involves an assessment of product quality relative to the initial quality requirements, and as-required adjustments to the product design and the project execution process. Variances from quality requirements discovered early in the development process have a smaller impact upon the project than variances discovered late in the project, and they typically have a much smaller impact than variances discovered after the product is placed in the field.

Product quality evaluation is performed through verification and validation activities, which are done in consideration of the various expectations and viewpoints of the owner, system developer, and operator. The differing viewpoints (owner, developer and operator) provide the aggregate basis for quality evaluation.

Verification is typically done by testing system components, by testing the integration of system components, by reviewing the veracity of potential test models, and by testing the performance of the final product. The system delivery group performs testing in conjunction with system verification and is responsible for the delivery of a software system that meets quality requirements.

Validation is typically done using prototyping and product review techniques and again during installation and integration at the vessel or unit. Documented requirements traceable to specifications and the specific tests performed commonly provide essential information when validating comprehensive satisfaction of user requirements in the delivered product.

3.5.5 Measurement

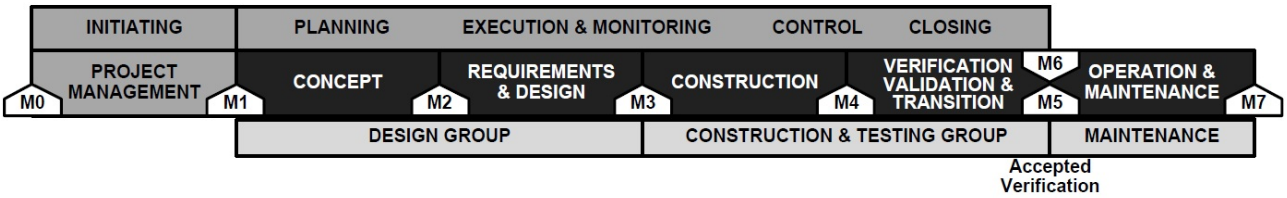
Quantitative measurement is central to achieving and improving software quality. Software quality is commonly attributed to software that achieves measurable attributes, such as Mean-Time-To-Failure (MTTF) and Fielded Errors. A failure is construed as an event in which the control system's programming causes the Equipment Under Control (EUC) to perform an action that is unpredicted, undesired, unsafe, etc. A fielded error is commonly construed as a software defect discovered after the software has been delivered to the customer. The SP typically collects and analyzes data to assist in evaluating software quality and reserves those metrics for proprietary quality analytics. While ABS encourages the use of quantitative software quality measurement techniques, the methods and results of quality measurement are left to the SP and are considered proprietary.

5 Software Development Life Cycle

The Software Development Life Cycle (SDLC) as shown in Section 1, Figure 7 is the seminal representation of ABS' ISQM process as presented in the *ISQM Guide*. It is the map of ABS' ISQM program, and provides the basic structure for guiding the discussion of software quality in this document.

Each phase of project management and software development processes are addressed by this graphic. It establishes the logical framework by which the critical elements of the SP's quality practices and policies are implemented and assessed. This software life cycle process has been refined and successfully used for years in many industries to develop well-engineered software products. For the convenience of the reader, this graphic is presented repeatedly to illuminate the discussion in each section of these Guidance Notes.

FIGURE 3
Software Development Life Cycle



7 Scope of the Guidance Notes

These Guidance Notes describe a number of recommended best practices for software quality management, as well as software quality management concepts based on research and industry convention. This convention indicates that rigorous project management and disciplined software engineering practices have a positive impact on the quality of software. The SP is encouraged to reference the *ISQM Guide*, the practices offered in this document, and the references cited in both documents when pursuing ABS ISQM certifications.

These Guidance Notes are organized in four major sections so as to be usable whether read "straight through" or referred to in sections.

- Section 1 provides a summary overview of the three tiers of ABS assessment and associated certifications for software: Manufacturer's Certification, PDA-Parts 1 and 2, and Unit Software Certification.
- Section 2 provides guidance to the SP for demonstrating conformity to the *ISQM Guide* in its Software Quality Assurance (SQA) process documentation during the PDA-Part 1 assessment, which in turn enables the SP to proceed to the PDA-Part 2 assessment.
- Section 3 provides guidance to the SP for demonstrating sufficient conformity to the *ISQM Guide* in its Software Quality Assurance practices during the PDA-Part 2 assessment, which results in issuance of ABS' Product Design Assessment (PDA) certification for the software explicitly named by product, the assessed software development team, and the assessed production location. Section 3 also provides information about PDA renewal.
- Section 4 provides guidance to the SP for obtaining ABS' Unit Software Certification for specific software systems that are to be installed on a specific unit or vessel.

Each Section of these Guidance Notes maps its content to Section 1, Figure 3, and presents useful examples and recommendations of both Project Management and Software Engineering practices and concepts in support of the *ISQM Guide* and ABS' software certifications. The reader should note that the PDA certification process is cumulative.

9 Definitions and Abbreviations

9.1 Definitions

Artifacts: Objects, documents, and data produced by efforts of personnel assigned to software projects.

Malware, Malicious Code, and Malicious Software: A software program (e.g., viruses, worms, Trojan horses, backdoors, keystroke loggers, phishing, hoaxes, etc.) that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system.[5]

Note: [5] NIST Special Publication 800-83r1, Guide to Malware Incident Prevention and Handling, 2013

Software: Internally developed programming satisfying the required functionality that meets specifications requested by the shipyard, owner, or operator.

Supplier: The designation used in process graphics and certification letters to represent a System Provider (SP) and Connected Equipment providers.

9.3 Abbreviations

ConOps: Concept of Operation Document

CM: Software Configuration Management

COTS: Commercial-off-the-shelf equipment or solutions

EUC: Equipment Under Control

FDD: Functional Description Document

HMI: Human Machine Interface

IL: Integrity Level assigned by the owner (see *ISQM Guide*, Section 3)

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

MC: Manufacturer's Certification

PDA: ABS Product Design Assessment (Certificate). For this specific PDA is issued when upon completion of PDA-Part 1 and PDA-Part 2 assessments

PDA-Part 1: ISQM Conformity Certification Process during which SQA process documentation is assessed for conformity to the *ISQM Guide* and these Guidance Notes

PDA-Part 2: ISQM Conformity Certification Process during which SQA process implementation is assessed for conformity to the *ISQM Guide* and these Guidance Notes

PM: Project Management

PMBOK®: Project Management Body of Knowledge

PQA: Product Quality Assurance

Secondary Entity: A supplier providing product and/or services to a System Provider (SP), a sub-contractor

SDLC: Software Development Life Cycle

SDS: Software Design Specification

SP: System Provider of control systems for major hardware, and the entity having legal or patent rights to produce a software product or system

SQA: Software Quality Assurance

SRS: Software Requirement Specification

TEP: Test and Evaluation Plan

USC: Unit Software Certification

V&V Plan: Verification and Validation Plan to include any commissioning/integration-testing plan(s)

WBS: Work Breakdown Structure

W-3: “What-When-Who”; a project management expression of “What is done When, and by Whom”.

SECTION 2

ISQM Product Design Assessment – Part 1

1 Introduction

The first step of the ABS PDA process for software is a review of ISQM software quality processes and procedures as documented for use by an SP's software development organization during the development and deployment of software products for a given application. The PDA-Part 1 process in Section 2, Table 1 is shown in detail in Section 2, Figure 1.

TABLE 1
ISQM Product Design Assesment Certification

Marine Vessel Rules Approval Tiers		*ISQM Certification Tiers*	
Tier 1	Manufacturer's Certification (MC)	Tier 1	*Manufacturer's Certification (MC)*
Tier 2	**Product Design Assesment (PDA)**	**Tier 2**	***Product Design Assesment (PDA)***
Tier 3	Type Approval (TA)	Tier 3	Not Applicable
Tier 4	Product Certification via Product Quality Assurance (PQA)	Tier 4	Not Applicable
Tier 5	Unit Certification via Survey During Fabrication (UC)	Tier 5	*Unit Certification via Survey During Final Test (USC)*

The PDA-Part 1 review concludes with documented findings concerning conformity of the SP's quality management processes to the information presented in the *ISQM Guide*. The findings contain ABS reviewer conclusions about the completeness and conformity of SP-documented software quality management processes, and procedures relative to the information presented in the *ISQM Guide*. The findings emphasize gaps or shortfalls found in SP's process documentation based on a comparison of that documentation to the processes or documentation included in the *ISQM Guide*.

1.1 Requesting a PDA-Part 1 Evaluation

1.1.1 Use of a Secondary Entity for Production of Software

A Product Design Assessment certification may only be issued to the original System Provider (SP). The SP is the entity possessing legal or patent rights to produce the software product or system. [6] ABS considers the SP to be responsible for the continued conformity of named products listed in the PDA.

Note: [6] 1-1-A3/5.1.1 of the ABS *Rules for Conditions for Classification*: "A Product Design Assessment (PDA) may only be issued to the Designer or the Original Equipment Manufacturer (OEM). This is the entity that has legal or patent rights to produce the material, component, product or system. ABS will consider the Designer or the OEM to be responsible for the continued compliance of the PDA as assessed."

If the SP engages a secondary entity for production, maintenance, or support of products named for PDA, then that secondary entity is to be included in the PDA-Part 1 assessment. This secondary assessment is performed at an increased level of effort and cost to be defined as part of the assessment initiation contracting process between the SP and ABS.

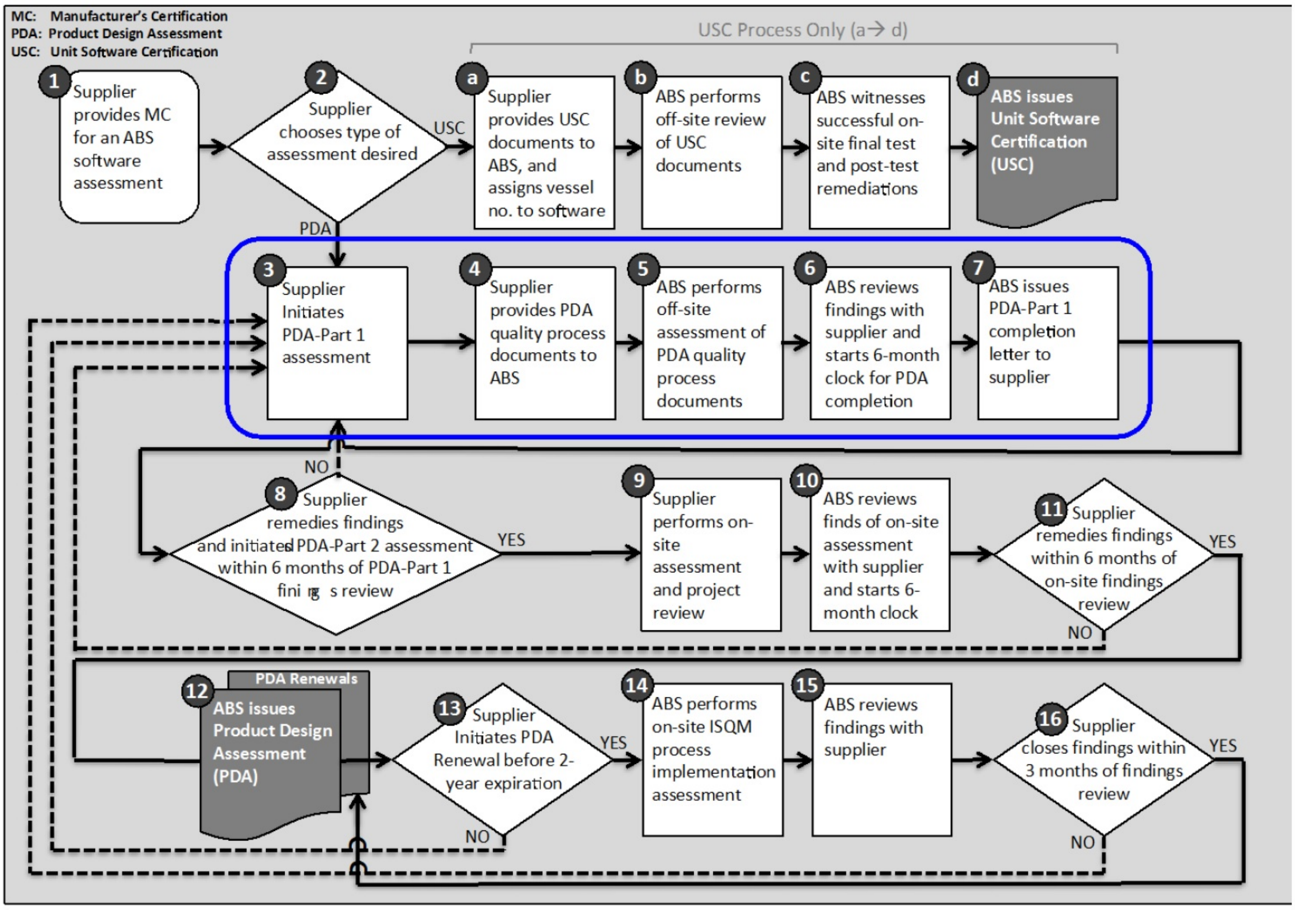
i) The SP is to provide written notification to ABS that a secondary SP entity (i.e., another internal group or third-party provider that is not collocated with the primary group being assessed) engages in the production or support of software products named for assessment and is participating in the PDA assessment. The notification is to include the name, address, and business relationship of the secondary entity.

ii) A secondary entity is to request an ABS conformity review, and provide documented SP approval of the secondary entity's participation in the review. The request is to also contain SP authorization for the secondary entity to provide SP documentation (hardcopy or electronic) that may be requested by ABS for PDA-Part 1 review.

1.3 Completing a PDA-Part 1 Evaluation

In order to successfully complete the PDA-Part 1 process, the SP is to remedy non-conforming documentation assessment findings communicated to the SP by ABS in a findings review meeting. The SP is provided six-months to remedy findings. The remediation period begins on the date of the ABS findings review meeting. During that time, the SP is to (a) remedy any process or documentation findings (gaps) discovered during the assessment, and (b) initiate the PDA-Part 2 assessment. Upon ABS' review and acceptance of the SP's remediation and closure of the findings, the successful completion of the PDA-Part 1 process is acknowledged by ABS in a letter from ABS to the SP. Upon receipt of the PDA-Part 1 successful completion letter, the SP may proceed with the PDA Part 2 assessment toward completion of the PDA assessment process. If the SP does not present documentation of findings remediation and closure to ABS and initiate the PDA-Part 2 assessment within six months of the PDA-Part 1 Findings Review, the SP is to reschedule a PDA-Part 1 assessment and repeat the PDA process in its entirety.

FIGURE 1
ISQM – Conformity Process: ISQM-PDA-Part 1

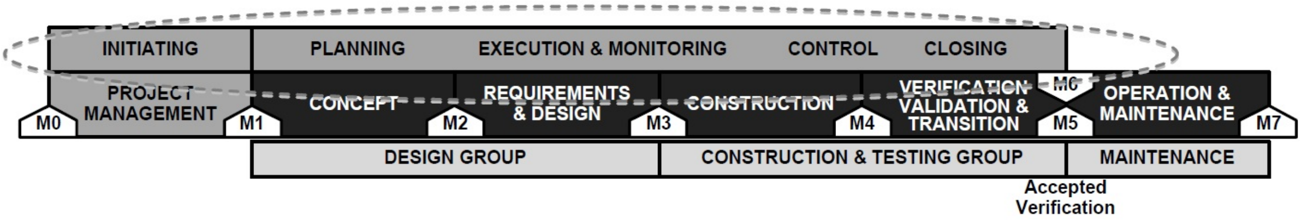

MC: Manufacturer's Certification
PDA: Product Design Assessment
USC: Unit Software Certification
USC Process Only (a→ d)
1 Supplier provides MC for an ABS software assessment
2 Supplier chooses type of assessment desired
USC
PDA
a Supplier provides USC documents to ABS, and assigns vessel no. to software
b ABS performs off-site review of USC documents
c ABS witnesses successful on-site final test and post-test remediations
d ABS issues Unit Software Certification (USC)
3 Supplier Initiates PDA-Part 1 assessment
4 Supplier provides PDA quality process documents to ABS
5 ABS performs off-site assessment of PDA quality process documents
6 ABS reviews findings with supplier and starts 6-month clock for PDA completion
7 ABS issues PDA-Part 1 completion letter to supplier
NO
8 Supplier remedies findings and initiated PDA-Part 2 assessment within 6 months of PDA-Part 1 fini ng s review
YES
9 Supplier performs on-site assessment and project review
10 ABS reviews finds of on-site assessment with supplier and starts 6-month clock
11 Supplier remedies findings within 6 months of on-site findings review
YES
NO
PDA Renewals
12 ABS issues Product Design Assessment (PDA)
13 Supplier Initiates PDA Renewal before 2-year expiration
YES
NO
14 ABS performs on-site ISQM process implementation assessment
15 ABS reviews findings with supplier
16 Supplier closes findings within 3 months of findings review
YES
NO

Section 3 of these Guidance Notes provides information that supports development of quality processes and procedure documentation in conformity with the *ISQM Guide* and issuance of the PDA-Part 1.

3 Project Management

This section provides guidance to the SP for reviewing critical Project Management (PM) processes for the ISQM-PDA-Part 1. Project management is considered important to the delivery of quality software and is highlighted in Section 2, Figure 2 as a set of processes that overarches the software development life cycle. The PDA-Part 1 review includes evaluation of process documentation that supports recognized project management practices that in turn support the development of quality software.

FIGURE 2
Integrated Best Practices Approach: Project Management



Project management practices as shown in Section 2, Figure 2 are executed concurrently with, and in support of the software development phases. Certain project management practices are positioned in close proximity to phases of the software development cycle in the above graphic. In practice however, the mapped phases of the PM cycle can also apply to each of the phases of the software development cycle. For example, each phase of the software development cycle has an initiation, planning, execution/ monitoring, and closing (or handoff) phase – as does the entire software development cycle. Sound PM processes are useful in managing each phase of software development, and for the entire project, regardless of the development model used (e.g., waterfall, spiral, V-Model, etc.), and can clarify ISQM conformity when mapped to the software quality management processes presented in the *ISQM Guide*.

For each of the PM phases described below, these Guidance Notes provide quality practices that are reviewed as part of the PDA-Part 1 documentation evaluation.

3.1 Initiating Activities

In order for processes as presented by ABS' ISQM to be successfully implemented by the SP, the SP must first be aware of the contents of the *ISQM Guide*, and either develop a quality program based on the *ISQM Guide*, or map internally developed quality processes to ISQM processes. This level of awareness helps SP's management and individual contributors consider important quality questions and gain a deeper understanding of the processes that tend to characterize quality software development organizations. Process documentation described in the *ISQM Guide*, as well as processes described below, are considered during the PDA-Part 1 review of initiating documentation.

3.1.1 Quality Policy and Procedure Documentation

i) The SP has mapped ABS' ISQM quality policies and procedures to internally developed software quality management processes, quality policies, and procedures.

ii) Indication of conformity includes a detailed description of SP-developed software quality management processes, including a one-to-one mapping of internal processes and procedures to those in the *ISQM Guide*.

3.1.2 Awareness of Quality Policies Requirement

i) The software development organization, including the project management and development teams, are aware of the company's policies and procedures.

ii) Indications of conformity to the ISQM processes include a quality processes training program and a roster of project staff (by position and/or name) trained in quality practices and processes.

3.3 Planning Activities

The Planning Phase of a project demands that project activities are defined, that those activities are scoped and scaled so as to achieve project schedule objectives; that activity dependencies are sufficiently understood so as to give the schedule credibility; and, that each activity is the responsibility of a named person. In project management terminology, the assignment of "Activity" (What is done), "Responsibility" (Who does it), and "Delivery Date" (When it is done) is often referred to as "W-3's". Even basic project plans contain W-3's in support of project clarity. The planning phase of a project also comprehends the risks to the success of the project product, project cost, and project schedule. Process documentation described in the *ISQM Guide*, as well as processes described below, are considered during the PDA-Part 1 review of planning documentation.

3.3.1 Project Roles

i) Project roles, responsibilities, and authority are designated.

ii) Indication of conformity includes designation of responsibility with process documentation assigning and explaining roles, responsibilities, and reporting structures.

3.3.2 Project Activities

i) Project activities are identified and a project plan or Work Breakdown Structure (WBS) containing activity durations and dependencies is created and managed by means of a manual process or a computerized project management tool.

ii) Indication of conformity includes a project work activity plan documented in a manual or computer-aided project planning system containing project activities, activity durations, activity dependencies, and completion milestones.

3.3.3 Risk Management

i) A risk identification and management plan is in place for identifying and managing risks to both the specified software product performance and the required project execution performance.

ii) Indication of conformity includes a document that describes:

- Risks to meeting product specifications;
- Risks to meeting project performance goals, such as delivery;
- The probability that each risk will impact the project; and,
- The risk management (mitigation or work-around) plan that is in place in the event the risk identified actually occurs.

3.3.4 Requirements Development

i) Requirements acquisition, assessment, and documentation activities are scheduled in the system design phase of the software development cycle.

ii) Indication of conformity includes a project schedule containing a requirements development activity; system design activity that supports the completion of the Design Group; a requirements traceability matrix showing how system requirements are tested for quality verification; and, related documentation outlined in the *ISQM Guide*. Collaboration meetings are scheduled for requirements acquisition with customers. Meeting minutes are captured, updated, and reviewed until action items are closed. [Best practice: The duration of the R&D Phase can be the longest software development life cycle phase in high performing organizations.[7]]

Note: [7] A. Neufelder, SoftRel, The Cold Hard Truth About Reliable Software, 2012

3.5 Execution and Monitoring

Project execution and monitoring are dependent on the establishment and successful implementation of project initiation activities. Those processes and artifacts described in the preceding sections enable the SP to understand the requirements, define and plan project scope and schedules, assign tasks, evaluate progress, and take action to correct activities that do not follow the plan. Further, successful execution is often defined by a commitment to carefully monitor the "W-3's" described above. Monitoring also maintains the integrity of the project planning process throughout the project life cycle. Process documentation described in the *ISQM Guide*, as well as processes described below, are considered during the PDA-Part 1 review of execution and monitoring documentation.

3.5.1 Schedule

i) Project progress review meetings involving project stakeholders are routinely held by the SP.

ii) Indications of conformity include ISQM collaboration activities in the project plan, frequent progress review meetings, and meeting minutes that document stakeholder participation, contributions of project collaborators, as well as action item lists that are maintained, updated, and archived.

3.5.2 Metrics

i) Metrics and reports as prescribed in the *ISQM Guide* (see *ISQM Guide*, Appendix 8) are collected, maintained, and shared with appropriate members of the project team.

ii) Indications of conformity include metrics templates, metrics monitoring reports, and presentations (e.g., quad-charts, stoplight charts, trend analyses, etc., containing ISQM reference metrics), as well as meeting minutes in which performance shortfalls are managed through corrective action reports, assignment of responsibilities, and due dates.

iii) ABS does not review metrics data, but reviews documents for indications that metrics are being collected and analyzed.

3.7 Control Activities

Project control is differentiated from execution and monitoring. Execution and monitoring is the process by which information is gathered and organized so that project control (schedule and document management) is possible. In software projects, the term "control" commonly refers to the careful creation and archiving of software development artifacts (requirements, designs, and code) that describe the physical output resulting from the construction of software. Software project control is performed not only by control of the project management elements (W-3's), but also through the implementation of formal documentation procedures, configuration management procedures, version control procedures, and processes or systems that manage the software as a physical product. Process documentation described in the *ISQM Guide*, as well as processes described below are considered during the PDA-Part 1 review of control activities documentation.

3.7.1 Revision Control

i) A formal revision management procedure or system is used for requirements documentation management and design documentation management.

ii) Indications of conformity include the documentation of a requirements and design version/ revision control system and/or reports from that system, including traceability of requirements changes to design evolution.

3.7.2 Version Control

i) A formal software version management procedure or system is used for managing revisions of code components and versions of the major software component (system), provides system evolution clarity and traceability, and includes version description documentation that accompanies each software release.

ii) Indications of conformity include the documentation of the software development version and revision control system and/or documented reports from the system, including descriptions of version releases.

3.7.3 Malware Control

i) A formal malware prevention and response management procedure is in place and applied within the software development software testing, and maintenance services organizations.

ii) Indication of conformity includes a documented procedure for preventing, detecting, and containing malware in product software during development, testing, installation, and maintenance (e.g., installing patches and upgrades in the field).

3.7.4 Change Management

i) A formal change (configuration) management (CM) plan, procedure, and system/tool is in place for implementing changes to software components during development and after code release, and implementing changes to firmware and hardware supporting the software; an independent organization manages configuration and change management.

ii) Indications of conformity include documented use of a CM system, and a formal CM control documentation. It is recommended that an independent CM organization within the SP organization.

3.7.5 Project Control Metrics

i) Project control metrics as prescribed by the *ISQM Guide* are collected and maintained for revisions of requirements and designs. Designs and software components are collected, maintained in a repository, and reviewed for management of requirements acquisition sessions, design revisions, and configuration change activity.

ii) Indication of conformity includes documented and reported metrics with respect to requirements changes, design changes, and configuration changes, with historical traceability.

iii) ABS does not review metrics data, but reviews documents for indications that metrics are being collected and analyzed.

3.7.6 Asset Control

i) A formal software access control policy, with procedures and a system, governs access to the code repositories and code-building tools while the project is ongoing, so that the PM understands exactly who can, or cannot, access components, modules or segments of code.

ii) Indications or conformity include documentation of access controls policies; access control lists (ACLs) for code repositories and/or tools; and written policies governing locations from which code access may occur, systems allowed to access code, and allowable copies or clones of code trees which may be maintained by developers.

3.9 Closing Activities

Formal closing of a project establishes boundaries for project completion and transfer of project responsibility. Software organizations also establish libraries of project documentation in order to capture code, code documentation, and performance metrics for SP's internal process improvement programs, as well as to capture intellectual property and code modules for potential code reuse. Process documentation described in the *ISQM Guide*, as well as processes described below are considered during the PDA-Part 1 review of closing activities documentation.

3.9.1 Closing Documentation

i) Maintenance manuals, configuration management information, and other software documentation are aggregated and delivered to the customer.

ii) Indication of conformity includes a letter of transmittal indicating that maintenance documents, configuration documents, and other customer support documents are organized and delivered as specified.

3.9.2 Project Performance

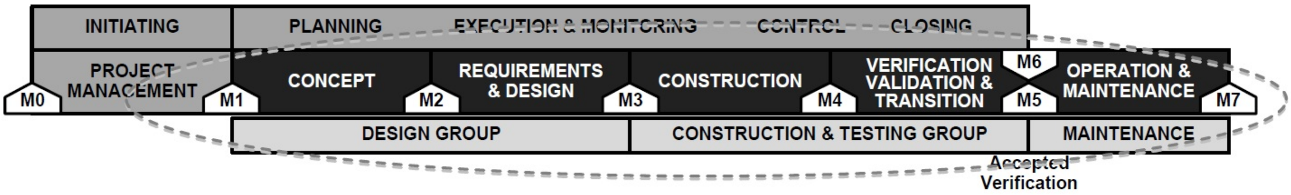
i) Project performance information is aggregated and stored for use in lessons-learned activities.

ii) Indication of conformity includes archived documents containing project performance data and minutes documenting lessons-learned reviews.

5 Software Development

Software development in the context of the ABS' ISQM includes all aspects of the Software Development Life Cycle (SDLC) from the Concept Phase through the Operation and Maintenance Phase.

FIGURE 3
Integrated Best Practices Approach: Software Development

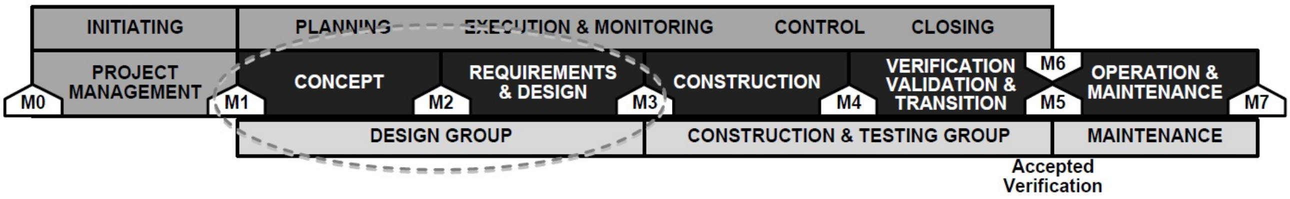


Process documentation described in the *ISQM Guide*, as well as document development processes described below are considered by ABS assessors during the PDA-Part 1 review of software development documentation.

5.1 Design Group

The documentation and practices described in this section assist the SP in conforming to recommended ISQM practices during execution of the Design Group activities associated with the software development process, and include Concept, Requirements, and Design Development. See Section 2, Figure 4. For circumstances in which the Concept of Operations (ConOps) document was previously developed for deployed software, a Functional Description Document (FDD) may replace the ConOps and requirements documentation, including the Software Requirements Document (SRS) and Software Design Specification (SDS). See 2/5.3 of the *ISQM Guide*, and Section 2, Figure 4.

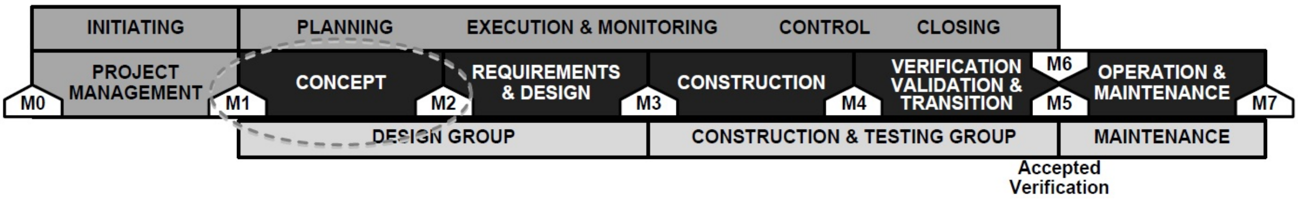
FIGURE 4
Integrated Best Practices Approach: Software Design Group



5.1.1 Concept Phase

The Concept Phase (*ISQM Guide*, Section 3), Section 2 Figure 4 provides the technical direction and limits the scope of the project by defining the system in sufficient detail to facilitate safety review(s), Integrity Level (IL) assessments, integrated system component selection, and anticipated verification approach; see Section 2, Figure 7. The SP reviews and improves the primary deliverable of this phase, the Concept of Operations (ConOps) document, which includes the high-level architectural design of the system, an analysis of the computer-based control system hardware requirements, and the high-level system software requirements. The owner of the asset may develop the ConOps, or alternatively, the SP may develop the ConOps under the direction of the owner.

FIGURE 5
Integrated Best Practices Approach: Software Concept Development



The ConOps document is a foundational document for the integrated Software Requirement Specification (SRS) and the integrated Software Design Specification (SDS) during the Requirements and Design Phase. Concept errors in the ConOps document may have significant impact if discovered late in the process.

i) *The Concept of Operations (ConOps) or Functional Description Document (FDD)*

- A Concept of Operations (ConOps) or FDD document is issued for review and approval.
- Indication of conformity includes a ConOps or FDD document containing the content defined in the *ISQM Guide*, as well as documentation indicating that key stakeholders collaborated in its development.

ii) *Integrity Level*

- Integrity Levels (IL) for system functions are assigned by the owner and documented by the SP. The SP assigns an IL number as a recommendation (see ISQM Guide, Section 3). The Integrity Level (IL) is assessed by evaluating the consequences of a failure of the function.
- Indication of conformity includes documentation (typically a table) in the ConOps or FDD showing an IL assignment to major system software functions in the system architectures.

iii) *System Architecture*

- The system hardware and software architectures are developed, and depict a preliminary description of the system's hardware and software functions, including interoperability interfaces.
- Indication of conformity includes documentation that describes and diagrams the system architecture, and describes and uniquely numbers system functions, module interfaces, and interoperability interfaces.

iv) *Reliability, Accessibility, Maintainability, and Safety*

- The initial non-functional or extra-functional system requirements (such as reliability- accessibility-maintainability-safety (RAMS), and the ability to evolve and service control systems, etc.) are outlined and documented and may be provided in the ConOps or FDD document.
- Indication of conformity includes a documented discussion of the non-functional system requirements expected and presented by the stakeholders – especially by the owners and operators of the system – that may be provided in the ConOps or FDD document.

v) *Traceability*

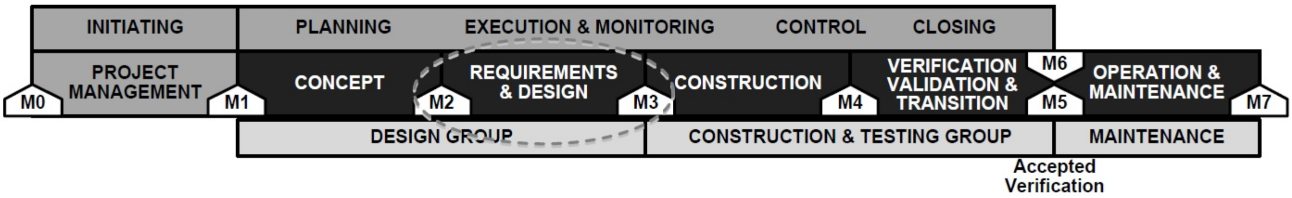
- Traceability of software system functions is established. Functions are designated with a numerical identifier to enable function traceability from requirements development through the ConOps, SRS, and SDS (or FDD), safety reviews, FMECA to the verification plan.
- Indications of traceability include a listing of functions with uniquely identifying alpha-numeric or numeric designators in the ConOps or FDD.

5.1.2 Requirements & Design Phase

During the Requirements and Design (RD) Phase (*ISQM Guide*, Section 4), the requirements and detailed specifications of the integrated software functions are developed, modeled, and documented based on the ConOps document. See Section 2, Figure 6. The RD Phase has two primary goals:

- Define the system's explicit (functional) requirements and implicit (non-functional) requirements sufficiently to communicate the needs of the owner and other relevant stakeholders to software engineers and developers.
- Transform the functional and non-functional requirements into software specifications that the SP's developers and programmers can use to construct (code) software that meets the user's needs.

FIGURE 6
Integrated Best Practices Approach: Software Requirements and Design



In the Requirements and Design phase of the SDLC, a typical workflow begins with the owner formally requesting information from the operator concerning operational practices and preferences. As a best practice, the SP and owner enlist the support of software engineers and requirements development specialists to create user scenarios and other requirements information based on input from domain experts. The SP then documents the requirements in the ConOps document. The user descriptions are transformed into requirements that provide the documented basis for functional specifications (descriptions of software functions), from which the software systems are developed (coded). Software development functions are testable, described in the specifications, traceable to documented requirements, and traceable to scenarios or use cases. This design information is also included in the ConOps document.

The deliverables from this phase are the Software Requirements Specifications (SRS) document, containing the traceable technical details of each software function including failure mode behaviors, and the Software Design Specification (SDS) document containing the traceable design details of each function, interface details, and system architecture components. These two documents represent the technical basis of the software developed in the Construction Phase.

The RD phase also details the non-functional requirements captured initially in the Concept Phase, and include but are not limited to:

- System performance capabilities
- Safety considerations
- Database performance capabilities
- Security requirements
- Adherence to standards
- HMI-related considerations

Further, the plan for acquiring and integrating commercial-off-the-shelf (COTS) solutions into the developed software, with the COTS verification and validation requirements and related integration test plans, are included in the requirements and design documentation.

The RD Phase documents detail owner and/or operator requirements. The owner and/or operator review these documents for completeness and accuracy. These detailed requirements, expressed as functional specifications, are coded during the Construction Phase.

i) *Review of Software Requirement Specification*

- Review and/or approval of Software Requirements Specification (SRS) or FDD is documented. SRS functionality is traceable to the ConOps.
- Indication of conformity includes the formal SRS or FDD document containing user requirements.

ii) *Review of Software Design Specification*

- Review and/or approval Software Design Specification or FDD is documented. SDS functionality is traceable to the ConOps.
- Indication of conformity includes the formal SDS or FDD document containing user requirements.

iii) *Review of System Architecture Design and Traceability*

- Review and confirm system architecture (reference IEEE 12207) requirements coverage and alignment with the SDS or FDD.
- Indication of conformity includes a report describing architectural alignment to the SDS and SRS, with stakeholder signoff.

iv) *Failure Modes, Effects and Criticality Analysis (FMECA)*

- Failure risks to system software and hardware components are identified, analyzed and documented as Failure Modes Effects and Criticality Analyses (FMECA) for IL2 and IL3 functions. Safety reviews for IL1 through IL3 are also performed, may be included as part of the FMECA, and are documented in the ConOps or FDD document.
- Indication of conformity includes documented failure risk assessments and FMECA analyses with corrective/mitigation action plans in the ConOps or FDD document.

v) *Safety Standards*

- Requirements, design, and functional specifications record that safety standards are identified, designed into the software, and included in the functional specifications.
- Indication of conformity includes documented requirements and design entries in the SRS and SDS (or FDD) documents pointing to application of safety standards.

vi) *RD Phase Metrics*

- Metrics as prescribed by ISQM are developed, tracked and reported in project reviews.
- Indication of conformity includes representations of metrics in presentations and other tracking documentation.
- ABS does not review metrics data, but reviews documents for indications that metrics are being collected and analyzed.

5.1.3 Design Group Using a Functional Description Document

For SPs that provide existing (production) software systems, or enhancements to existing software systems, an alternative approach to the development of the ConOps, SRS, and SDS documents is practical and acceptable (*ISQM Guide*, Section 9). For such cases, a Functional Description Document (FDD) contains descriptions of software functions that are traceable to owner requirements. The FDD can acceptably replace the ConOps, SRS, and SDS documentation for previously developed software systems in which at least 80% of the software functions are the same as previously provided control systems. The FDD provides software function descriptions that are traceable to owner and operator requirements. The FDD provides the contents otherwise included in the ConOps, SRS and SDS, and provides indications that change management systems are in place and utilized for tracking revisions in design, development, and documentation of production software. See the *ISQM Guide*.

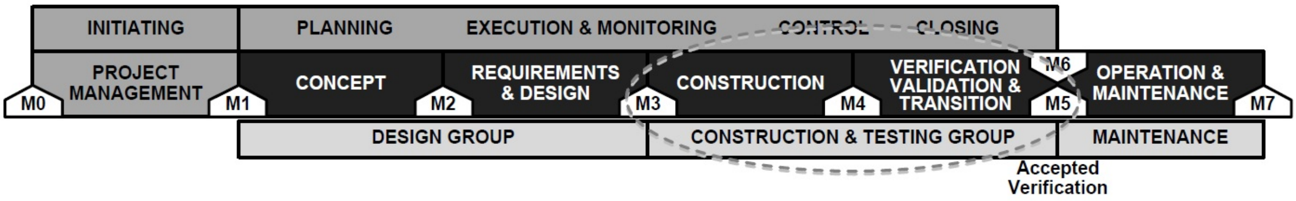
5.3 Construction Phase

The Construction Phase of the software development life cycle converts system requirements and the resulting designs and specifications into software code (*ISQM Guide*, Section 5). The development of code typically includes the following Construction Phase activities:

- Peer code reviews
- Repetitive build cycles
- Reevaluation during build cycles
- Updating of requirements
- Iterative component testing
- System testing
- Integration testing

If commercial-off-the-shelf software is used, then the purchased module's/sub-system's interfaces are integrated and tested during construction.

FIGURE 7
Integrated Best Practices Approach: Software Construction



Assurances that software failure modes are well understood and managed are important in deployed systems. While documentation of tests is beneficial for all functions, it is especially important for functions designated as IL2 and IL3. At the end of construction, the SP tests the completed system software, documents the outcomes of those tests, and provides the SP system test report to the V&V organization. The owner and/or operator review the documents resulting from this phase.

5.3.1 Internal Testing of the Software

i) Formal, documented internal testing approaches are implemented to provide accurate and rapid feedback to developers, including but not limited to peer review/testing and construction of a validated test simulator for rapid and accurate feedback of code performance. Other approaches for internal testing and verification are also acceptable.

ii) Indication of conformity includes documentation of testing performed during development and system build cycles. (Note: Best practices indicate that peer testing and testing using simulators have a highly positive impact on reducing defect density in fielded code.)[8]

Note: [8] A. Neufelder, SoftRel, The Cold Hard Truth About Reliable Software, 2012

5.3.2 Internal Testing Results

i) Test results are documented and fed back to developers for corrective action during the software development cycles. Specific dependencies between and among system components, especially when involving third-party (COTS) components being integrated with the system, must be shown and addressed.

ii) Indications of conformity include test feedback documentation and developer review meeting minutes containing corrective action reports and results.

5.3.3 Software Component Testing

i) It is recommended that Component testing be utilized.

ii) Indications of conformity include test feedback documentation and developer review meeting minutes containing corrective action reports and results.

5.3.4 Expected and Actual Results

i) Expected results of internal tests are documented and compared to actual test results.

ii) Indications of conformity include documented test result expectations and outcomes, an expected results test procedure referenced in the test plan, defect reports based on component and system tests, and corrective action reports addressing variances between expected and actual test results.

5.3.5 New Functionality and Modification

i) New features, and modifications to existing features are retested during regression tests.

ii) Indication of conformity includes a documented test plan outlining procedures for retesting new features, component and system test reports reflecting associated defects (if any), and corrective action reports.

5.3.6 Internal Software Quality Audits

i) An internal software quality audit process that is independent of the development process is documented.

ii) Indications of conformity include audit reports created by an internal software quality team during software development, including audits of defect tracking, reporting processes, corrective action results tracking, and the change management process during code development.

5.3.7 Functional Description Document Updates During Construction

i) The SRS and SDS or the FDD document are/is updated, with special attention given to changes/updates to requirements, specifications, and component redesigns. (Owner updates the ConOps)

ii) Indications of conformity include documented revision notes, revision dates, and approval signatures in the FDD document.

5.3.8 Verification Plan Updates

i) The V&V Plan is updated as appropriate, reviewed, and approved.

ii) Indication of conformity includes a documented V&V Plan signed and dated by the required parties.

5.3.9 Design Group Metrics

i) Metrics as prescribed by the ISQM Guide are developed, tracked, and reported in project reviews.

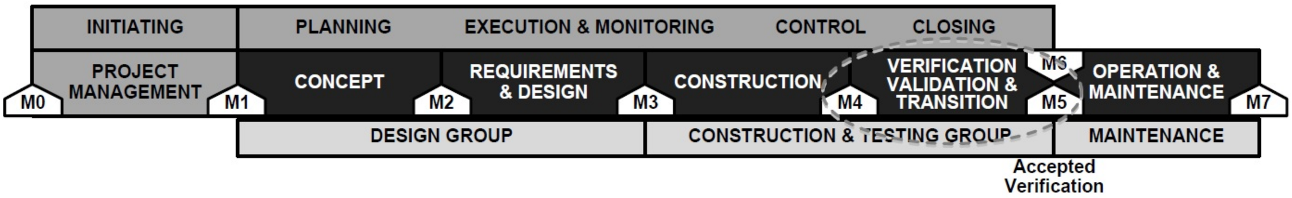
ii) Indication of conformity includes representations of metrics in presentations and other tracking documentation.

iii) ABS does not review metrics data, but reviews documents for indications that metrics are being collected and analyzed.

5.5 Verification, Validation, and Transition (V V&T) Phase

ABS' ISQM program integrates software testing or verification throughout the software development life cycle (*ISQM Guide*, Section 6). Development of code is a creative and often proprietary activity that is left to the discretion of the SP; therefore, the conformity information provided in the construction phase section of these Guidance Notes emphasizes construction that is well controlled, traceable, and characterized by integrated testing activities.

FIGURE 8
Integrated Best Practices Approach: Software V V&T



Testing in its various forms is a primary concern during system conceptualization, requirements development, design specification, and software construction. During the Concept Phase, the owner specifies which of the three verification methods are used to verify performance of the software as specified during the V V&T Phase of the software development life cycle. During the Requirements and Design Phase, requirements for testability and verification are developed so that the system is designed to optimize test and verification methods. During the Construction Phase, the software is developed (coded) to meet the design specifications, including specifications for testing and verification. Further, testing is a continuous process during construction. This approach indicates test processes are applied throughout the SDLC from concept, through requirements development, system design, and coding. This approach also assures that gaps in requirements, errors in design, and development flaws are discovered and corrected as early as possible.

The document that guides the V V&T Phase is the V&V Plan and the commissioning/integration-testing plan, if any. The V&V Plan documents the test methods, test tools, expected test outcomes, test targets, and processes for managing and tracking shortfalls and variances from expected outcomes. The documents that establish the capabilities and performance benchmarks for the V&V efforts include:

- The ConOps, along with the SRS and SDS documents, describe the functional system concept, which documents the development of and adherence to an approved verification approach, a map of software functions traceable to approved requirements, and design specifications documentation to be used for validation during sea trial(s) and commissioning activities.
- Functional Description Description (alternative to ConOps, SRS, and SDS), which documents the development of and adherence to an approved verification approach, a map of software functions traceable to approved requirements (also called the Requirements Traceability Matrix), and design specifications documentation.
- Test and Evaluation Plan (TEP), which details and compiles all testing methods, modes and needs, including test equipment and test harnesses, into a single-source testing document. The TEP must also include specific needs associated with performing testing and V&V for any third-party or COTS components, including security, reliability, availability, maintainability, and sustainability tests, protocols or parameters.

V&V organization develops the V&V plan based on the primary test methods chosen in the Concept Phase, develops and configures the simulator, and might support internal testing during the Construction Phase.

Errors and anomalies discovered during verification, including software defects, concept errors, and functional and non-functional deficiencies, are documented and reported. Concept errors are considered major issues in that they deal in the fundamentals of what the software is supposed to do, as opposed to functional and non-functional design and programming defects that deal in how the software is supposed to operate. Concept errors affect not only the verification process, but also the validation process and acceptance. Discovered errors are carefully documented during validation, and returned to the SP for corrective action.

After corrections are completed and tested by the SP, the software is returned to the verification team for regression testing and other testing as appropriate. The V&V process is iterative and regressive in order to discover any new defects introduced by the correction of previously detected and corrected defects. Validation of the software system is complete when the owner agrees that the control system software performs according to the current ConOps or FDD.

5.5.1 Verification and Validation Plan

i) The V&V Plan is documented and included in the SP's project plan.

ii) Indications of conformity include a documented V&V Plan, and completed V&V Report (including commissioning/integration results documentation) summarizing planned verification activities, verification activity outcomes, and action item resolutions.

5.5.2 Traceability of Functions

i) A unique function name and identifier in the V&V Plan is traceable to each function identified in the SDS and SRS, or FDD.

ii) Indication of conformity includes documented entries in the V&V Plan that reference function identifiers to code modules identified in the SDS and SRS, or FDD.

5.5.3 Verification of Hardware and Software Integration

i) The V&V Plan describes procedures that test the interactions of system software, hardware, and firmware.

ii) Indication of conformity includes documented entries in the V&V Plan that documents explicit procedures for testing the interaction of system software, hardware, and firmware.

5.5.4 Verification of As-delivered Functionality to As-designed Functionality

i) The V&V Plan compares the software system functionality described in the ConOps, SRS and SDS (or FDD) to the software system functionality that is validated during commissioning and sea trials.

ii) Indication of conformity includes a documented V&V Plan containing a comparative review of documented ConOps, SRS, and SDS documents to test outcomes documented during commissioning and sea trials.

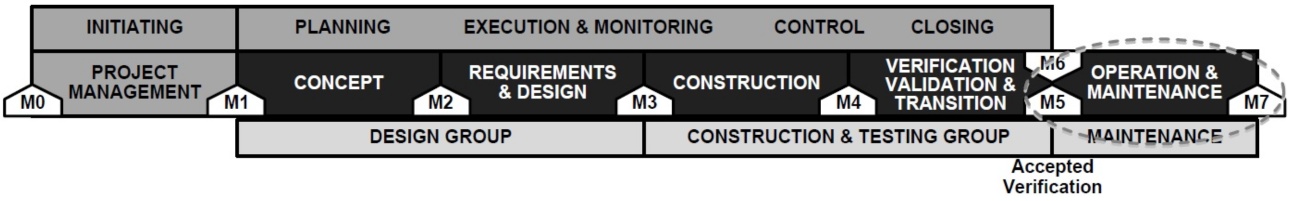
5.5.5 Verification of As-delivered Software to be Malware-free

i) The V&V Plan describes procedures that test for the presence of malware in the 3rd party software and supplier-developed software to be delivered for installation.

ii) Indication of conformity includes a documented V&V Plan that tests for malware prior to delivery to the user, as well as a documented procedure for protecting the software from the introduction of malware during on-site installation, including patches, defect fixes, and updates.

5.7 Operation and Maintenance

FIGURE 9
Integrated Best Practices Approach: Software Operation and Maintenance



The Maintenance and Operation Phase pertains to software operational and maintenance activities, scheduled and unscheduled upgrades, problem resolution activity, and retirement of the software system (*ISQM Guide*, Section 7). The key event of this phase is the delivery of the SP's operating and maintenance manuals, which are delivered to the owner and crew upon acceptance of the software system. The activities of this phase are the responsibility of the owner or crew and the SP(s), per specific contract agreements.

5.7.1 SP's Software Maintenance Plan

i) Final verification outcomes are documented in a V&V report(s).

ii) Indication of conformity includes a documented V&V report.

5.7.2 Malware Protection Procedure

i) Procedures used by the supplier to protect the installed software systems from malware during installation of patches, defect fixes, and updates are included in the Operations and Maintenance Plan as provided to the owner.

ii) Indication of conformity includes a documented process for malware protection that is followed during the transfer and installation of patches, defect fixes, updates, and other forms of software maintenance performed by the software provider.

SECTION 3

ISQM Product Design Assessment – Part 2

1 Introduction

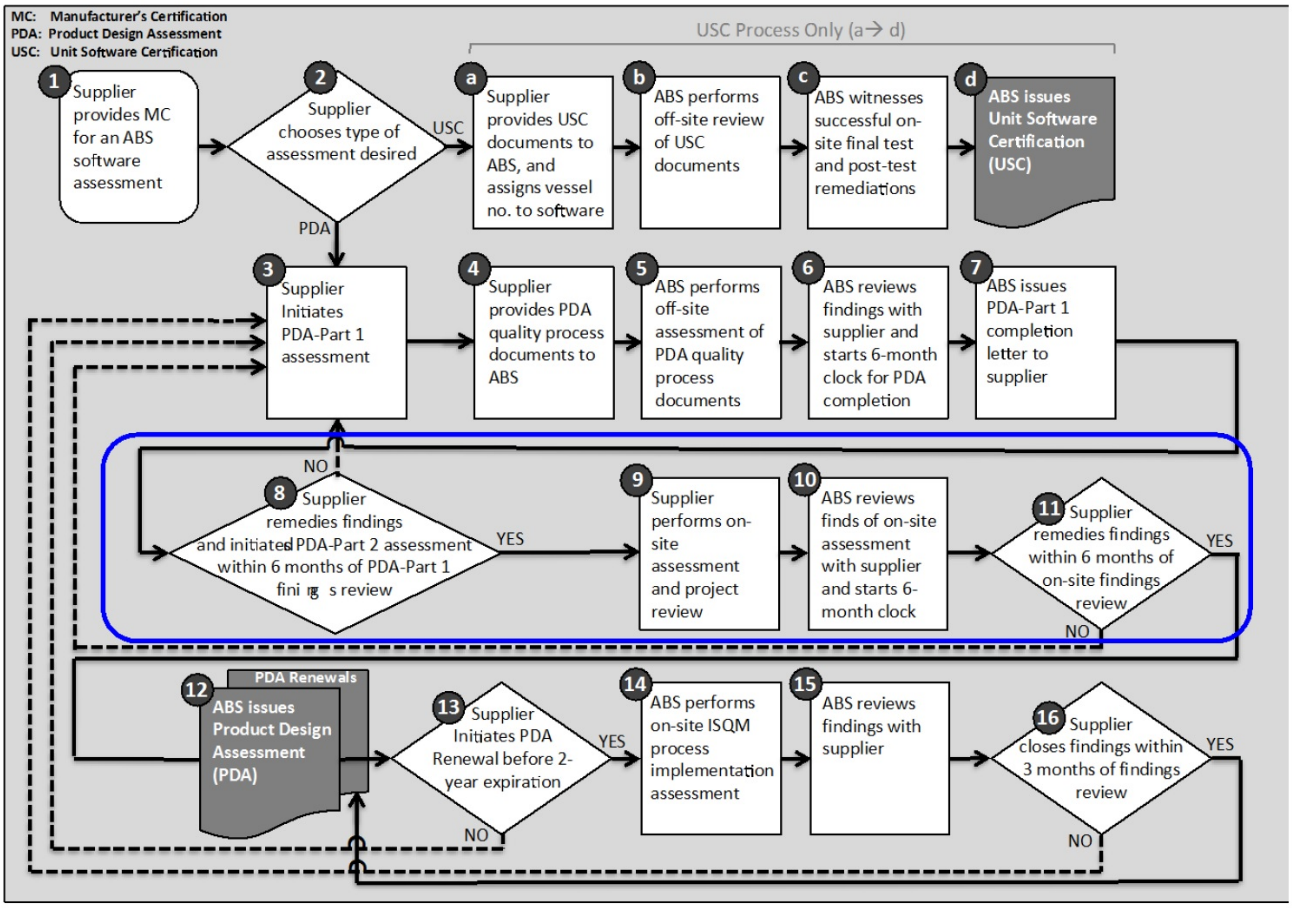
The ISQM Product Design Assessment – Part 2 (ISQM-PDA-Part 2) evaluation is performed to assess an SP's implementation conformity to the *ISQM Guide* during the SP's software development life cycle (SDLC). The PDA-Part 2 evaluation is performed only after the SP has completed ABS' ISQM-PDA-Part 1. Successful completion of the PDA-Part 2 assessment results in the issuance of an ABS PDA for software development of specific software products, developed by a specific software team, and at a specific SP location.

TABLE 1
ISQM Product Design Assesment Certification

Marine Vessel Rules Approval Tiers		*ISQM Certification Tiers*	
Tier 1	Manufacturer's Certification (MC)	Tier 1	*Manufacturer's Certification (MC)*
Tier 2	**Product Design Assesment (PDA)**	**Tier 2**	***Product Design Assesment (PDA)***
Tier 3	Type Approval (TA)	Tier 3	Not Applicable
Tier 4	Product Certification via Product Quality Assurance (PQA)	Tier 4	Not Applicable
Tier 5	Unit Certification via Survey During Fabrication (UC)	Tier 5	*Unit Certification via Survey During Final Test (USC)*

The ISQM-PDA is issued based on an assessment of SP-site quality process implementation and interviews with software product management, software quality personnel, and software development personnel. The interviews and site assessment allow ABS to ascertain the degree to which SP software production personnel implement the documented quality processes for which the ISQM-PDA-Part 1 completion letter was previously issued. The process for completing the PDA-Part 2 is highlighted in Section 3, Figure 1.

FIGURE 1
PDA-Part 2 Certification Process


MC: Manufacturer's Certification
PDA: Product Design Assessment
USC: Unit Software Certification
USC Process Only (a→ d)
1 Supplier provides MC for an ABS software assessment
2 Supplier chooses type of assessment desired
USC
PDA
a Supplier provides USC documents to ABS, and assigns vessel no. to software
b ABS performs off-site review of USC documents
c ABS witnesses successful on-site final test and post-test remediations
d ABS issues Unit Software Certification (USC)
3 Supplier Initiates PDA-Part 1 assessment
4 Supplier provides PDA quality process documents to ABS
5 ABS performs off-site assessment of PDA quality process documents
6 ABS reviews findings with supplier and starts 6-month clock for PDA completion
7 ABS issues PDA-Part 1 completion letter to supplier
NO
8 Supplier remedies findings and initiated PDA-Part 2 assessment within 6 months of PDA-Part 1 fini ng s review
YES
9 Supplier performs on-site assessment and project review
10 ABS reviews finds of on-site assessment with supplier and starts 6-month clock
11 Supplier remedies findings within 6 months of on-site findings review
YES
NO
PDA Renewals
12 ABS issues Product Design Assessment (PDA)
13 Supplier Initiates PDA Renewal before 2-year expiration
YES
NO
14 ABS performs on-site ISQM process implementation assessment
15 ABS reviews findings with supplier
16 Supplier closes findings within 3 months of findings review
YES
NO

1.1 Requesting a PDA-Part 2 Evaluation

1.1.1

In order to request a PDA-Part 2 evaluation, the SP is to:

i) Have been issued the PDA-Part 1 completion letter within six months of the PDA-Part 1 findings communication meeting date; and,

ii) Have initiated a PDA-Part 2 evaluation within six months of the PDA-Part 1 findings communication meeting date.

1.1.2

The ISQM-PDA-Part 2 is completed based on a review of SP-site quality process implementation and interviews with software product management, software quality personnel, and software development personnel. The interviews are intended to ascertain the degree to which SP software development personnel follow quality processes for which the ISQM-PDA-Part 1 completion letter was previously issued. The findings of the on-site assessment are communicated to the SP by ABS, with expectations that the SP will remediate shortfalls discussed in the findings and communicate those remedies to ABS within six months of the date of the PDA-Part 2 findings communication meeting.

1.1.3

ABS encourages the SP to provide supporting information to ABS before and during the site survey, with special considerations by ABS. Examples of supporting information include, but are not limited to, ISQM-related documentation describing previously completed software projects. It is recommended that ABS witness final or acceptance tests(s) of current software project(s). By making previously completed project data and current test information available to ABS, the SP can demonstrate patterns of quality management competency based on internally developed and implemented processes that are both effective and logically aligned with the *ISQM Guide*.

1.1.4

In the event that product testing witnessed by ABS conforms to ISQM practices, and the product tested is scheduled for delivery to a specified hull or rig, the product tested is issued an ABS Unit Software Certification (USC). The ABS USC is provided to the SP only for the product instance uniquely identified, tested, and installed on a specific hull or rig, and states that the test process conforms to the quality practices described in the *ISQM Guide*. See Appendix 4 of these Guidance Notes.

Although the USC is not a Type Certification, it does provide documentation that the instance of the product test as witnessed by ABS conforms to ISQM test practices.

A Unit Software Certification letter issued to a specific hull, rig number, or application specified in the USC, and is not valid for any other application, hull, or rig and to the witnessed software and firmware version numbers. The product identified in any USC is to be retested and witnessed by ABS when it is assigned to a rig number, hull number, or application not associated with or identified in a USC previously issued by ABS.

1.1.5

A Product Design Assessment certification may only be issued to the original System Provider (SP). The SP is the entity that has legal or patent rights to produce the software product or system.[9] ABS considers the SP to be responsible for the continued conformity of named products to the PDA as assessed and issued to the original SP. If the SP engages a secondary entity for production, maintenance, or support of products named for PDA, then that secondary entity is to be included in the PDA-Part-2 assessment.

Note: [9] 1-1-A3/5.1.1 of the ABS *Rules for Conditions for Classification*: "A Product Design Assessment (PDA) may only be issued to the Designer or the Original Equipment Manufacturer (OEM). This is the entity that has legal or patent rights to produce the material, component, product or system. ABS will consider the Designer or the OEM to be responsible for the continued compliance of the PDA as assessed."

i) A secondary entity engaged by the SP to produce, maintain, or support named software is to participate in the PDA program (Parts 1 and 2) with the SP in order for ABS to consider the SP's request for the PDA-Part 2 assessment.

ii) The SP is to provide written notification to ABS that a secondary entity (including entity name and location) engages in the production or support of software products named for assessment, and is participating in the PDA program.

iii) A secondary entity is to request an ABS conformity review, and include indication of the SP's approval of the secondary entity's participation in the review. The request is to also contain the SP's authorization for the secondary entity to provide SP documentation (hardcopy or electronic) to ABS that may be requested for PDA-Part 2 review. During the PDA-Part 2 assessment, the secondary entity is to provide access as requested by ABS to information, software staff, and documentation that support the SP's software product development or maintenance under assessment for PDA certification.

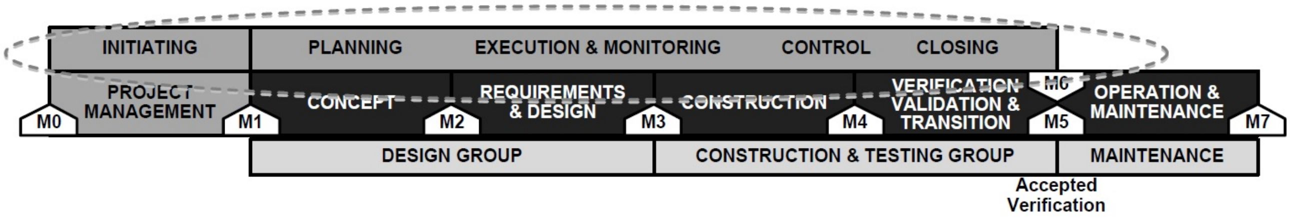
1.3 Completion of the PDA-Part 2 Evaluation

If the SP successfully remedies shortfalls communicated by ABS during the findings review meeting, and ABS reviews and approves the closure of shortfalls within six months of that findings review, ABS issues the PDA certification to the SP. If the SP fails to remedy shortfalls communicated by ABS within six months of the PDA-Part 2 findings communication meeting, the SP may re-initiate the PDA process by repeating the PDA-Part 1 and PDA-Part 2 assessment processes, with special considerations by ABS.

The PDA is effective for two years from the date of the certification. The PDA is published on the ABS website. The PDA is renewable. See Subsection 3/7 for details concerning the PDA renewal process.

3 Project Management

FIGURE 2
Integrated Best Practices Approach: Project Management



This section provides information to assist the SP in following a sufficient number of essential Project Management practices to receive a Product Design Assessment – Part 2 (PDA-Part 2). When reviewed by ABS, the SP will be assessed for conformity to accepted best practices in project management processes, procedures, and documentation, as well as for indications that the SP has both an in-depth knowledge of ISQM practices, and has implemented a minimum level of quality policies and procedures described in the *ISQM Guide*. Implementation of software quality processes described in the *ISQM Guide*, as well as processes described below, is considered during the on-site PDA-Part 2 assessment.

3.1 Initiating Activities

In addition to an awareness of ISQM requirements, SP project management practices are assessed for project initiating activities that promote productive stakeholder collaboration. Early collaboration is especially useful for customer buy-in and team level-setting in preparation for efficient and effective requirements gathering activities.

3.1.1 Stakeholder Involvement and Communications

i) Stakeholders are initially involved in the project planning, and customer buy-in is gained for stakeholder engagement over the full project life cycle.

ii) Indications of conformity include stakeholder meetings scheduled in the initial project plan, minutes from stakeholder meetings, agreements resulting from those meetings, and a documented communications plan.

3.1.2 Stated Objectives

i) Project objectives are outlined for planning purposes; initial project goals, resource commitments, and responsibilities are established; initial quality targets are set; and, initial project schedules are established, communicated to stakeholders, and agreed upon.

ii) Indications of conformity include a summary outline of project targets and commitments based on minutes from the stakeholder meeting(s).

3.3 Planning Activities

During the PDA-Part 2 assessment, SP software project planning activities are anticipated to be robust and detailed. In addition to definition of project activities and adherence to the fundamentals of project management, planning practices are reviewed for the following:

- Robust and disciplined project planning methods

- Project communications plans
- Full involvement and project oversight by software quality assurance and test teams for the duration of the project
- Documented project milestones (especially in connection to testing and test completions)
- Documented test activities, milestones, and completion schedules
- Detailed performance-to-schedule tracking and metrics
- Project-level defect density tracking and reporting throughout the software development life cycle

3.3.1 Use of Project Planning and Management Tools

i) Project planning and management tools are selected and the detailed activities are captured in formalized project management tools.

ii) Indication of conformity includes a demonstration of the planning tools used, showing active or completed project plan(s), as well as staff trained in and assigned to project plan management.

3.3.2 Project Revision and Communications

i) A process and method for revising, approving, and communicating project plans is documented and known to software development personnel.

ii) Indication of conformity includes a document describing the project revision and approval process; further, software development personnel are aware of the process.

3.3.3 Software Quality Milestones in the Project Plan

i) Software quality assurance team activities are included in the project plan and are evident for the entire software development life cycle.

ii) Indication of conformity includes software quality and test milestones present in the project plan throughout the software development life cycle.

3.3.4 Internal Test Plan within the Project Plan

i) Development of an internal test plan is included in the project plan.

ii) Indication of conformity includes internal test plan development activities early in the software development life cycle that are documented in the project plan.

3.3.5 Component Test Milestones in the Project Plan

i) Internal component or component test milestones are included in the project plan.

ii) Indication of conformity includes internal component test milestones throughout the software development life cycle that are documented in the project plan.

3.3.6 System Test Milestones in the Project Plan

i) Internal system and integration testing milestones are documented in the project plan.

ii) Indication of conformity includes internal system and integration test milestones that are documented in the project plan.

3.3.7 Regression Test in the Project Plan

i) Internal regression testing activities are documented in the project schedule.

ii) Indication of conformity includes internal regression testing documented in the project plan, subject to revisions anticipated or unanticipated.

3.3.8 Test Outcome Reporting in the Project Plan

i) Internal test completion status-reporting and metrics milestones are documented in the system test plan and the general project plan.

ii) Indication of conformity includes an internal system test plan, with completion metrics documented and updated in the test plan and general project plan.

3.5 Execution and Monitoring

Project execution is directly dependent on successful implementation of project initiation activities, and includes processes for the collection and analysis of data that facilitate accurate detection of project underperformance and effective "course correction". This typically also includes a formalized approach to project change management that effectively facilitates project course corrections and helps to control project "scope creep". Further, two best practice metrics that may be used to monitor overall project "health" in terms of delivery and software quality are frequency and scale of changes in project delivery schedule, where infrequent and small (e.g., under 10% for total project) changes in project delivery schedule are experienced; and, low software defect density is experienced. Effective management of these two metrics has proven to be closely linked to high quality software.[10] It is also anticipated that a number of other aspects of the project are measured, tracked, and reported depending on the preferences of management and the nature of the project.

Note: [10] A. Neufelder, SoftRel, The Cold Hard Truth About Reliable Software, Revision 6f, 2015

3.5.1 Customer Request Management

i) A formal method for filtering, prioritizing, and scheduling customer requests is established in the project communications plan.

ii) Indication of conformity includes the use of a documented customer request management process and accommodation of this process in the project communication plan.

3.5.2 Delivery Scheduling Metrics

i) Metrics noting delivery schedule changes with respect to initial schedule are formally established, tracked, and reported.

ii) Indication of conformity includes a report capturing contemporaneous project completion estimates and changes to completion estimates, with approval processes, accommodated in the project communication plan. A final delivery change of 10% or less is noted as a best practice benchmark for high software quality.[11]

Note: [11] A. Neufelder, SoftRel, The Cold Hard Truth About Reliable Software, Revision 6f, 2015

iii) ABS does not review metrics data, but reviews documents for indications that metrics are being collected and analyzed.

3.5.3 Density Defect Metrics

i) Defect density targets for each phase of the software construction process are established, tracked, and reported as an element of the project management plan.

ii) Indication of conformity includes documented targets for defect density and tracking of defect density for each development phase.

iii) ABS does not review metrics data, but reviews documents for indications that metrics are being collected and analyzed.

3.7 Control

Frequent scheduled qualitative and quantitative project performance feedback provided to project management and software development teams based on empirical project execution data is central to engineering processes.

3.7.1 Configuration Management Autonomy

i) The configuration management (CM) function is organizationally placed to reinforce configuration management process integrity.

ii) Indications of conformity include organizational placement of the CM function reporting to a management level responsible for assuring integrity of software configuration and revision control for all projects.

3.7.2 Configuration Management Discipline

i) Software, firmware, and computer hardware system configurations are identified and tracked with respect to system and subsystem versions for each installed system.

ii) Indication of conformity includes routine application of a process that traces system configurations by installation, including version change tracking by system and subsystems; and a configuration management log provided with each system or application under configuration management.

iii) Software, firmware and computer hardware system components and modules that are expected to require update are detailed with the authorized and expected methods and modes for update, with precursor conditions and permissives specified.

3.7.3 Version Control Discipline

i) Software revisions are uniquely identified in a managed revision control system for each software module, and traceable with respect to functional changes made in each version.

ii) Indication of conformity includes routine application of a process that provides version identifiers (typically version numbers) and revisions made, including a description of the revision, date of the revision, and the release status of the revision.

3.7.4 Change Control Discipline

i) A formal change (configuration) management (CM) plan, procedure, and system/tool is used for tracking changes to software components throughout the SDLC, and for implementing changes to firmware and hardware supporting the software; an independent organization manages configuration and change management.

ii) Indications of conformity include routine use of a CM system, formal CM control documentation, and a CM function placed so as to assure on organizational independence.

3.7.5 Malware Control Discipline

i) A formal malware prevention and response management procedure is in place and followed by personnel within the software development software, testing, and maintenance services organizations.

ii) Indication of conformity includes a routine adherence to malware prevention procedures that target malware protection of software products, and includes testing of software products for malware, installation of software products in the field, and field maintenance (e.g., installation defect fixes, patches, and upgrades) of software products.

3.7.6 Project Control Scaling

i) Project control processes are scaled and documented in consideration of project characteristics such as resource requirements, duration, and system integrity level (IL) ratings.

ii) Indication of conformity includes documentation that supports control process-scaling decisions when formal project control processes for a given project are eliminated or minimized.

3.7.7 Routine Project Status Meetings

i) Project status is routinely reviewed with appropriate management.

ii) Indication of conformity includes meeting schedules and minutes of routine project review meetings with management.

3.7.8 Metrics Collection for Software Development Performance Improvement Programs

i) Software development process improvement information and metrics are collected, maintained and used for formal continuous performance improvement programs.

ii) Indications of conformity include documentation of continuous process improvement metrics, and the documentation of collection and analysis of those metrics.

iii) ABS does not review metrics data, but reviews documents for indications that metrics are being collected and analyzed.

3.9 Closing

In addition to the formal project closing processes described in Section 3 in these Guidance Notes, an SP seeking PDA for software considers the long life of software products deployed in the maritime industry, and takes reasonable and prudent steps to assure the successful continuation deployed products. In addition to the establishment of a library of project documentation, updated code, and code documentation, the owner and operator have need access to source code and supporting documentation that assures continued operation in the event of business interruption by the SP that developed the deployed software.

3.9.1 Formal Documentation of Closed Projects

i) Documentation of closed project designs, performance data, operating data, maintenance data, lessons learned, and improved process implementation is captured, maintained, and referenced.

ii) Indications of conformity include formal archiving and referencing of closed project documentation and referencing of that documentation in active project, as applicable.

3.9.2 Software Availability Protection

i) Software and supporting documentation are archived and can be made available to existing customers in the event of SP business interruption or closure.

ii) Indication of conformity includes documented assurance that source code and descriptive documentation can be made available to existing customers in the event of business interruption or closure.

3.9.3 Lessons Learned and Process Improvement

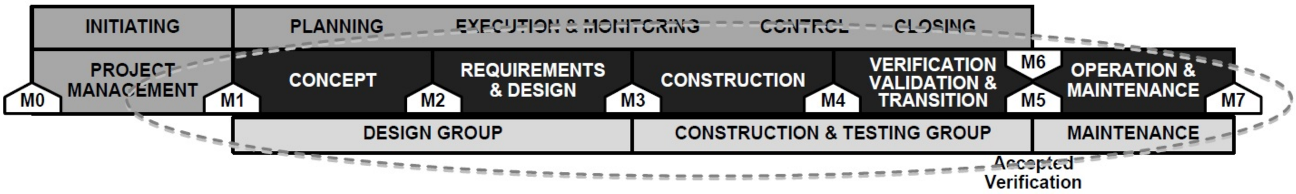
i) Performance-based lessons-learned internal assessment programs are useful for improving both project management and software development quality.

ii) Indication of conformity includes formal lessons-learned activities scheduled in documented project plans at the end of project phases and for completed projects.

5 Software Development

Software development in the context of ABS' ISQM processes includes all aspects of the software development life cycle from the Concept Phase through the Operation and Maintenance Phase, see Section 3, Figure 3.

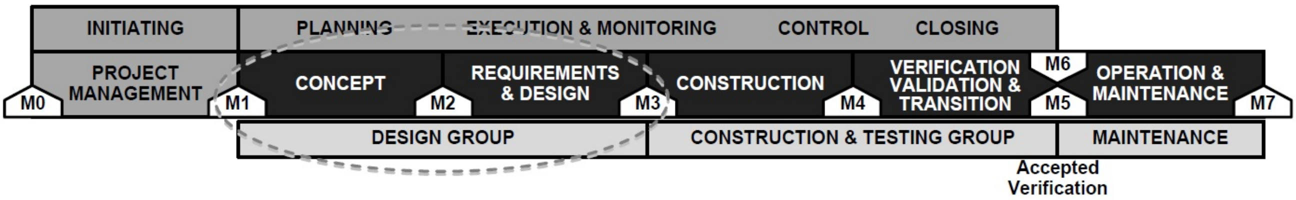
FIGURE 3
Integrated Best Practices Approach: Software Development



5.1 Design Group

The practices in this section assist the SP in conforming to Design Group processes presented in the *ISQM Guide* and assessed during the PDA-Part 2 on-site evaluation. It is anticipated that the Design Group approach will result in the development of a Functional Description Document (FDD) (replacing the ConOps, SRS and SDS documents) that describes production software development, reconfiguration, and customization for specific applications and customers, see Section 3, Figure 4.

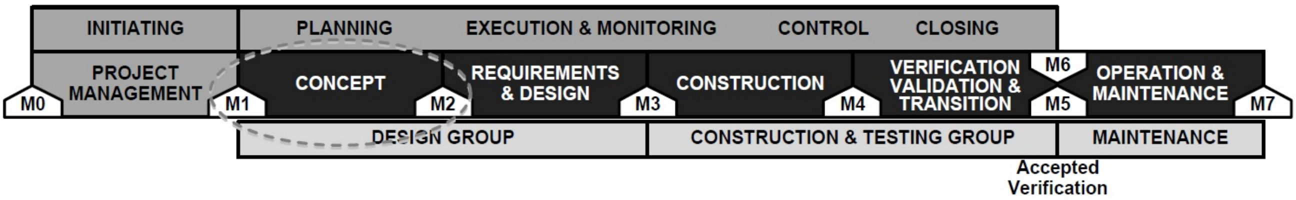
FIGURE 4
Integrated Best Practices Approach: Software Design Group



5.1.1 Concept

The Concept Phase provides the direction and scope of the project by defining the system in sufficient detail to facilitate safety review(s), IL assessments, integrated system component selection, and the anticipated verification approach, see Section 3, Figure 5.

FIGURE 5
Integrated Best Practices Approach: Software Concept Development



As stated in previous sections, the ConOps document (or alternately, the FDD) is the primary deliverable of this phase. In addition to the development of the FDD project document, the following processes are provided to assist the SP in conforming to processes presented in the *ISQM Guide*, and the processes assessed during the PDA-Part 2 evaluation.

i) *Description of Conceptual System Functions*

- Conceptual system functions with traceability to preliminary requirements are described and documented.
- Indication of conformity includes a demonstrable process for tracing the relationships between functions and documented requirements.

ii) *Integrated System Description*

- The integrated system is sufficiently designed and described in ConOps or FDD to enable safety reviews, IL assessments, FMECA processes, and integrated system component selection.
- Indication of conformity includes a conceptual system design description and diagram that is used to communicate the functions of the system, functional system capabilities, safety reviews, IL assignments, FMECA results, and preliminary COTS acquisition plans/evaluations, as applicable.

iii) *Computer Hardware Requirements*

- Control system hardware requirements are developed and documented.
- Indications of conformity include a computer hardware architectural design or description, as well as descriptions of operating system and middleware selections that are used to purchase and configure integrated control systems.

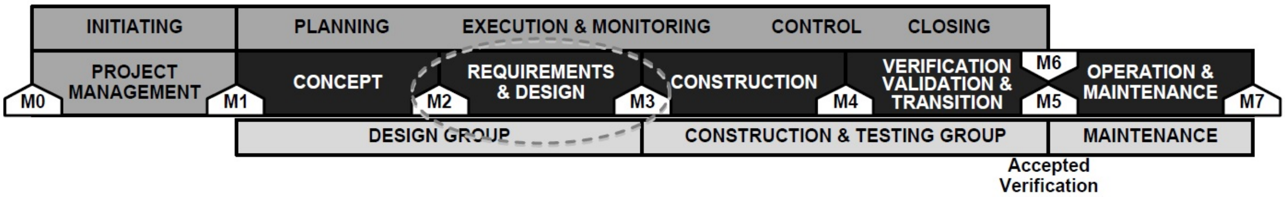
iv) *Safety Recommendations Supporting FMECA*

- Safety recommendations for each system function are documented sufficiently to enable FMECA targets and analyses.
- Indication of conformity includes contemporaneous minutes from safety reviews of system modules that provide safety targets and failure modes supporting FMECA assessments, with owner and operator review sign-offs.

5.1.2 Requirements and Design

During the Requirements and Design (RD) Phase, the requirements and detailed specifications of the integrated software functions are developed, modeled, and documented based on the ConOps (or FDD) document, see Section 3, Figure 6.

FIGURE 6
Integrated Best Practices Approach: Software Requirements and Design



The RD Phase defines system requirements that in turn inform the development of the functional and non-functional requirements provided by the owner (and other relevant stakeholders), and translates the functional and non-functional requirements into software specifications that developers and programmers can efficiently and effectively rely upon to construct (code) the software. Functions described in the specifications are traceable to specific documented requirements contained in the ConOps (or FDD) and are testable.

The RD Phase documents detail owner and operator requirements, as well as the resulting solutions, which are expressed as a defined system architecture with supporting specifications. The owner and/or operator review the RD Phase documents to assure completeness and alignment with the ConOps (or FDD) document. These specifications are coded during the Construction Phase.

i) *Formal Requirements Collection and Tracking*

- Formal requirements capture, collection, evaluation, and review/inclusion methods are used. If a computerized system or tool is used, it is described.
- Indications of conformity include description and/or demonstration of requirements collection methods, requirements acquisition session documentation, requirements analyses, and a listing of final requirements with traceable identifiers.

ii) *Use of Formal Requirements Management Process*

- A best practice and recommendation is the use of a formal requirements capture and management tool.
- Indications of conformity include demonstration of a requirements management tool (if used) and resulting reports.

iii) *Requirements and Design Communication*

- Requirements documents and designs (SRS and SDS, or FDD) are updated, approved, and communicated as specified in the project communications plan after development begins.
- Indications of conformity include a functional requirements change management process that tracks SRS and SDS (or FDD) updates and approvals, and communicates both to appropriate stakeholders.

iv) *Report of Variance from Standards*

- A standards variance report is developed and provided to stakeholders.
- Indication of conformity includes a reporting process, with reports that state which standards were considered but not applied (if any) to the project and product, including the rationale for deviating from standards.

v) *Statement of Performance Requirements*

- Component and system performance requirements are stated.
- Indication of conformity includes descriptions in the SRS and SDS (or FDD) documents of system performance characteristics.

vi) *Formal Requirements Review*

- Formal requirements reviews are held and updates are routinely performed as needed.
- Indications of conformity include routinely scheduled requirements reviews, documented minutes from the reviews, and documented requirements revision control tracking.

vii) *Requirements and Design Traceability*

- Requirements and designs are traceable to use cases or user scenarios, contributors, etc.
- Indication of conformity includes a process, system, or tool that is used to maintain mappings of designs, I/O, and functional specifications to requirements.

viii) *Software Service and Maintenance Requirements*

- Software service and maintenance requirements are in place.
- Indication of conformity includes service and maintenance specifications defined in the SDS (or FDD) and a process indicating that specifications are followed by software design and engineering staff.

ix) *Exceptions to Requirements*

- Design exceptions to requirements are captured and reported.
- Indication of conformity includes a process for identifying exceptions to requirements, and documentation of requirements in the SRS (or FDD) that are not comprehended in the SDS (or FDD), with an explanation of the exception design choice.

x) *Firmware Requirements*

- Firmware requirements (if applicable) are comprehended in the requirements collection and analysis.
- Indications of conformity include requirements in the SRS (or FDD) and design specifications in the SDS (or FDD) that address firmware interface choices and accommodations, where applicable.

xi) *Documentation of Boundary Conditions Requirements*

- Requirements for boundary conditions are formally stated and documented.
- Indications of conformity include processes and provisions for boundary condition management within the code and documented in the SRS and SDS documents.

xii) *Reporting of Defects Traceable to the Requirements Phase*

- Defects originating in the requirements phase are tracked and reported to the requirements development team.

- Indication of conformity includes defect origination tracking processes and reports that are provided to the requirements development team.

xiii) *Use of Computer-Aided Software Engineering (CASE) Tools*

- A best practice and recommendation is the use of CASE tools.
- Indications of conformity include demonstration of the use of a CASE tool (if used) and resulting reports.

xiv) *Event-generated Changes to Data Fields*

- Operational events that cause changes to data fields are noted, designed to enable that condition, and noted in user documentation.
- Indication of conformity includes a documented analysis of event-generated impacts on data fields (if applicable) in the SRS and SDS (or FDD), with explanatory information in user documentation.

xv) *Code Change-Protection*

- Code that is not intended to be modified is protected against modification by the system design.
- Indication of conformity includes processes for identification and accommodation of change-protected code, including any system memory management requirements, in the SRS and SDS (or FDD).

xvi) Design of Human-Machine Interfaces

- System interfaces are designed, described, documented, and uniquely identified.
- Indication of conformity includes specific references to human system engineering interface requirements and designs in the SRS and SDS (or FDD), with descriptions and unique identifiers.

xvii) *Design of Data Fields*

- User accessible data fields that are intended to be visible and/or altered by the user (e.g., HMI interfaces) are listed and designed for user inspection.

xviii) *Design of Machine-Machine Interfaces*

- System interfaces are designed, described, documented, and uniquely identified.
- Indication of conformity includes specific references to system interface requirements and designs in the SRS and SDS (or FDD), with descriptions and unique identifiers.
- Indications of conformity include specific identification and design of data fields made visible to users, and documentation of user input to the HMI designs in the SRS and SDS (or FDD).

xix) *Anticipated Availability*

- Software availability predictions are performed for critical and safety-related software modules based on IL assignments (FMECA, Root Cause Analysis, corrective action and mitigation procedures).
- Indications of conformity include FMECA assessments and failure response and mitigation procedure processes and documentation as appropriate for software modules based on IL assignments.

xx) *Corrective Action Decisions*

- Corrective action decisions in requirements and designs are based formal processes such as user inputs, design reviews, FMECA evaluations, or Root Cause Analysis results.

- Indication of conformity includes formal processes and documentation that supports requirements and design corrective actions.

xxi) *Exception Handling*

- Software exception handling is noted in the ConOps, SRS and SDS (or FDD) documents.
- Indication of conformity includes inclusion of exception handling capabilities in the software designs, the ConOps, SRS (or FDD), and functional specifications in the SDS (or FDD).

xxii) *Unexpected State Resolution*

- Requirements for resolving unexpected states, events, and user actions are stated.
- Indication of conformity includes provisions in software design processes, the SRS and SDS (or FDD) for resolving unexpected software system states.

xxiii) *Limited or Prohibited Data Values*

- Data values that are limited or prohibited, including user-accessible and non-user-accessible values, are described as requirements.
- Indication of conformity includes processes for identifying prohibited values and descriptions of the limited or prohibited entries or values documented in requirements and specifications.

xxiv) *Risk Management Plan for Incorrect Value Input*

- A risk management plan and process or system is specified and designed for prohibited, inadequate, or incorrect inputs (both user and interfaced system inputs).
- Indication of conformity includes processes for monitoring for, and managing degradation or failure of subsystems based on documented risk management requirements in the SRS (or FDD), and provisions in the SDS (or FDD) for managing human-generated and computer-generated input of prohibited, inadequate, and incorrect values.

xxv) *Definition of Hardware/Firmware Limitations*

- Computational resource limitations (i.e., memory limitations) are defined.
- Indications of conformity include processes for defining resource limitations requirements in the SRS (or FDD), and provisions for memory constraint, overflow, leak, and detection conditions in the SDS (or FDD).

xxvi) *Intentionally Self-modifying Code*

- A best practice and recommendation is that code be free from intentional self-modification.
- Indications of conformity include documented coding standards that prohibit self-modifying code, indications that self-modifying code is addressed in design reviews, and test plans indicating that self-modifying code is classified as a defect.

xxvii) *Use of Formal Reliability-estimating Tools*

- Best practices indicate that reliability-estimating tools are used.
- Indications of conformity include demonstration of the use of the tool and resulting reports.

xxviii) *Measurement of Defects Traceable to the Design Phase*

- Metrics concerning defects originating in the design phase are documented, maintained, and reported to the design teams.

- Indication of conformity includes defect origination tracking metrics in the metrics documents and presentations.

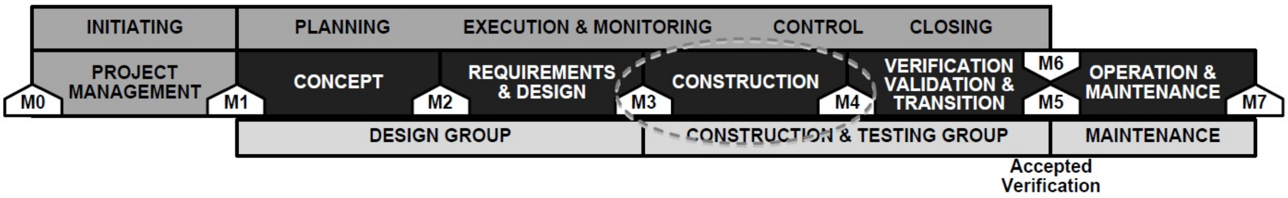
xxix) *Rapid Development of System Feasibility Prototypes*

- Best practices indicate that a system prototype (or module prototypes as appropriate) is rapidly developed and constructed to internally verify feasibility and assess accommodation of requirements and scheduling estimates.
- Indications of conformity include demonstration of the system feasibility prototype and/or documentation of results of prototyping.

5.3 Construction

As stated previously in these Guidance Notes, the Construction Phase of the software development life cycle converts system requirements and the resulting designs and specifications into software code. The construction phase activities facilitate the development of quality software, and include peer code reviews, repetitive build cycles, reevaluation and updating of requirements and designs, iterative component testing, system testing, regression testing, and integration testing, see Section 3, Figure 7. If Commercial-Off-The-Shelf (COTS) software is used, then the purchased modules/subsystems and their interfaces are also tested for both seamless integration into the developed system and for dependencies that COTS may bring to the final product set.

FIGURE 7
Integrated Best Practices Approach: Software Construction



During the PDA-Part 2 assessment, the evaluation of Construction Phase implementation is heavily focused on quality management and testing activities performed during software construction. The balance of the review focuses on processes, especially quality policy reviews, and construction practices based on those processes. This focus is intentional in order to provide maximum latitude to the SP in the execution of the creative and possibly proprietary activities performed during software development.

Further, a number of practices reviewed during the PDA-Part 2 assessment and discussed in these Guidance Notes are based on documented software construction and internal testing best practices for the delivery of high quality systems with low defect densities.[12] Further, these Guidance Notes reference sources that discuss practical application of internal test practices that are flexible, practical, and aligned with ISQM practices.

Note: [12] A. Neufelder, SoftRel, The Cold Hard Truth About Reliable Software, 2012

5.3.1 Scheduled Software Development

i) Software development activities are scheduled and milestones are met in a timely manner.

ii) Indications of conformity include software construction activities evident in the project schedule, documented schedule variance-to-plan reports, and corrective action activities.

5.3.2 Internal Coding Standards

i) Coding standards exist, are enforced, and are uniformly applied by the development team during coding.

ii) Indications of conformity include documented coding standards referenced in coding procedures, SRS and SDS (or FDD), and awareness of coding standards requirements by developers.

5.3.3 Exception Handling Standards

i) Exception handling standards are included in coding standards.

ii) Indication of conformity includes references in the SRS and SDS (or FDD) that note exception-handling conditions and allowed or recommended approaches for resolving exceptions.

5.3.4 Control of Code Complexity

i) A best practice and recommendation is that code complexity is explicitly controlled (i.e., coding standards limitations on the number of functions allowed per file) [*Note:* This is a quality management best practice that has a positive impact on software quality. [13]]

Note: [13] A. Neufelder, SoftRel, The Cold Hard Truth About Reliable Software, 2012

ii) Indications of conformity include documented coding processes, procedures or standards that limit code complexity, and code complexity measurement procedures and reports.

5.3.5 Measurement of Software Size and Related Testing

i) Lines-of-code-tested is measured and tracked.

ii) Indication of conformity includes line-of-code-tested metrics required by the test plan and reported in code review meetings and lines-tested reports.

5.3.6 Feedback of Coding Errors to Developers

i) Errors introduced in coding phase are formally tracked and reported (fed back) to developers for instruction and resolution.

ii) Indications of conformity include test results and corrective action reports that are formally reviewed by the development team; minutes from developer review meetings record analysis of coding errors resulting from the Construction Phase.

5.3.7 Use of Error Catalogs in Software Development and Internal Testing

i) A catalog of common defects (referenced or internally developed) is used and updated during construction and internal component testing.[14]

Note: [14] C. Kaner, J. Bach, B. Petticord, Lessons Learned in Software Testing, 2002

ii) Indications of conformity include general use of a catalog of common errors and regular updates of the catalog based on errors commonly found during internal peer reviews (if applicable) and testing.

5.3.8 Use of Formal Problem Reports

i) Problem reports are communicated to the configuration management team and the status of corrective actions (CA) are formally documented and dispositioned.

ii) Indication of conformity includes a configuration management plan and process for mapping defects and corrective actions to revision histories with a final disposition reflected in the revision and configuration management documentation.

5.3.9 Prioritization Management During Construction

i) An established prioritization method is used to manage customer and internal requests during code construction and priority changes are captured and documented.

ii) Indications of conformity include processes and documentation for development of priorities for making and implementing software changes, including potential impacts on the delivery schedule.

5.3.10 IEEE Internal Test Procedures

i) Accepted internal system test procedures (e.g., IEEE) are used.

ii) Indication of conformity includes references to accepted test procedures in the test plan and awareness of accepted internal test procedures by developers.

5.3.11 Mapping of Requirements to Tests

i) A 1:1 mapping of requirements to internal component test is performed and documented.

ii) Indication of conformity includes documentation or reports specifically linking or mapping test plans and test results to requirements, with reports listing untested requirements – using a requirements mapping tool if possible.

5.3.12 Internal Component Test During Construction

i) Internal component testing is included in the software construction schedule.

ii) Indication of conformity includes activities in the project plan that indicate implementation of scheduled component tests during development.

5.3.13 Data Recovery Testing

i) Data recovery after anomalous condition notification is system tested in internal test procedures.

ii) Indication of conformity includes anomalous condition notification and data recovery requirements in the SRS (or FDD), supporting design in the SDS (or FDD), and successful testing of an anomalous condition notification and data recovery capability in component and system test.

5.3.14 Coding and Testing Based on Defect Metrics

i) Coding and internal testing decisions are based on defect metrics.

ii) Indication of conformity includes documented defect metrics, discovered defect reports, and a documented developer feedback and corrective action reports.

5.3.15 Internal Test of Exception Handling

i) A best practice and recommendation is that exception handling and boundary conditions are stated and tested during internal testing. [15]

Note: [15] A. Neufelder, SoftRel, The Cold Hard Truth About Reliable Software, Revision 6f, 2015

ii) Indication of conformity includes exception handling and boundary condition testing procedures in the test plan, with found defects reported in component and system test reports, and in corrective action reports.

5.3.16 Internal Retest of New Features

i) New features are internally retested during coding and analysis.

ii) Indication of conformity includes a documented new feature retest (regression test) procedure in the test plan, with found defects reported in component and system test reports, as well as corrective action reports.

5.3.17 Internal Test of Hardware/Firmware Interfaces

i) Firmware and hardware interfaces are tested in internal test procedures.

ii) Indication of conformity includes a firmware and hardware test procedure referenced in the test plan, with found defects reported in component and system test reports, as well as corrective action reports.

5.3.18 Internal Test of Prohibited Values

i) A best practice and recommendation is that a test for prohibited values is performed during internal component testing.[16]

Note: [16] A. Neufelder, SoftRel, The Cold Hard Truth About Reliable Software, Revision 6f, 2015

ii) Indication of conformity includes a prohibited value test procedure referenced in the test plan, with found defects reported in component and system test reports, as well as corrective action reports.

5.3.19 Internal Test of Undesired Outputs

i) A best practice and recommendation is that undesired outputs are system tested during internal testing.[17]

Note: [17] A. Neufelder, SoftRel, The Cold Hard Truth About Reliable Software, Revision 6f, 2015

ii) Indication of conformity includes an undesired output test procedure that is referenced in the test plan and implemented during testing processes, with found defects reported in component and system test reports, as well as corrective action reports.

5.3.20 Internal Test of System Communications Faults During Construction

i) Communications faults are internally component tested during software construction.

ii) Indication of conformity includes a documented test procedure referenced in the test plan and implemented during testing processes, with defects reported in module and system test reports and in corrective action reports.

5.3.21 Internal Test of Input and Output Faults

i) I/O faults are internally system tested.

ii) Indications of conformity include I/O fault test procedures referenced in the test plan and implemented during testing processes, with faults reported in module and system test reports and in corrective action reports.

5.3.22 Internal Component Test of Algorithm Precision/Accuracy

i) Algorithm precision/accuracy is internally tested for each component.

ii) Indication of conformity includes an algorithm test procedure referenced in the test plan and implemented during testing processes, with faults reported in module and system test reports and in corrective action reports

5.3.23 Internal Test of Transaction Flows

i) Sequences (transaction flows) are internally component tested.

ii) Indication of conformity includes a sequence test procedure in the test processes and plan, with defects reported in module and system test reports, and in corrective action reports.

5.3.24 Internal Testing for Safety

i) Impact on safety is assessed and internally tested during and after corrective action implementation (defect fixes) and other code changes.

ii) Indication of conformity includes a safety-impact test procedure in the test processes and plan, with defects reported in test reports, as well as in corrective action reports.

5.3.25 Internal Testing for Changes in Code Execution Paths

i) Changed code execution paths are internally retested after corrective action implementation (defect fixes) and other code changes.

ii) Indication of conformity includes a changed-path test procedure referenced in the test processes and plan, with found defects reported in component and system test reports, as well as in corrective action reports.

5.3.26 Internal Retesting for Changed Modules

i) Changed modules are internally retested after corrective action implementation (defect fixes) and other code changes.

ii) Indication of conformity includes a changed-module test procedure referenced in the test processes and plan, with found defects reported in component and system test reports, as well as in corrective action reports.

5.3.27 Internal Retesting for New/Added Features

i) New features are internally retested after addition of new features.

ii) Indication of conformity includes a new-feature test procedure referenced in the test processes and plan, with found defects reported in component and system test reports, as well as in corrective action reports.

5.3.28 Internal Testing for Conflicts

i) Software components are internally tested for conflicts, and conflicts are resolved or managed through a documented risk management process.

ii) Indications of conformity include code development, component testing, and risk management processes for discovering and managing code conflicts, with internal conflict test procedure referenced in the test plan, and found conflicts reported in component and system test reports, as well as in corrective action reports.

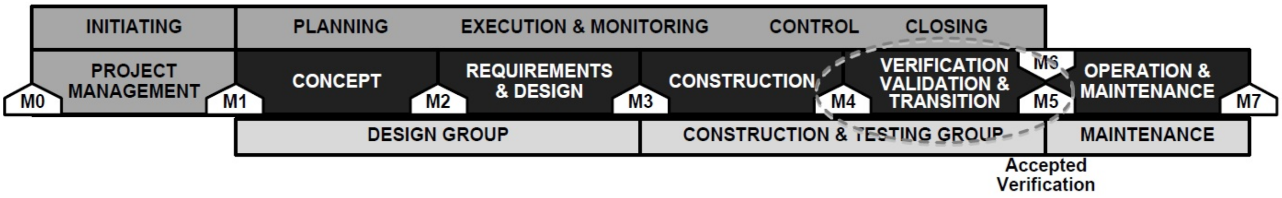
5.3.29 Internal Testing for Enhancements Made After Coding Phase

i) Program enhancements are avoided or retested as corrective actions after the coding phase has ended.

ii) Indication of conformity includes a code management plan and test plan specifying the code changes allowed after code completion are retested (i.e., regression tested) of post-completion module and system changes. Documented software construction workflow diagrams provide for post-completion testing, and test reports are available to indicate retesting after code changes.

5.5 Verification, Validation, and Transition

FIGURE 8
Integrated Best Practices Approach: Software V V&T



Attention is given to the Verification, Validation, and Transition Phase (V V&T) in previous sections of these Guidance Notes, and referral to those sections is recommended. The PDA-Part 2 assessment extends the ISQM assessment by reviewing additional verification activities, including test completion and results documentation. Processes and concepts reviewed in the PDA-Part 2 assessment are described below.

5.5.1 Peer Reviewed Simulation

i) A system simulation is performed with peer review, and corrective actions resolving discovered defects/issues are performed.

ii) Indication of conformity includes a documented, signed, and dated peer-reviewed system simulation, complete with simulation results, found defects/issues, and corrective actions.

5.5.2 Test of Configuration and Setup Requirements

i) Software configuration and setup requirements as documented are tested for accuracy and completeness, and results are documented.

ii) Indications of conformity include configuration and setup requirements that are documented in the verification plan, and include the documented test results of a simulated system installation and setup.

5.5.3 Verification of As-delivered Software to be Malware-free

i) Software products are tested for the presence of malware in the 3rd party software and supplier-developed software to be delivered for installation.

ii) Indication of conformity includes testing processes performed specifically for the identification of for malware prior to delivery to the user, as well as documented outcomes of the malware testing performed.

5.5.4 Integration Tests for Critical Defects

i) Integration testing is performed to test for Critical or Major Defects.

ii) Indications of conformity include a system test process and plan that specifically identifies anticipated Critical and Major Defects, and tests for those defects. Results are documented in a V&V report.

5.5.5 Integrity Level (IL) Rating Noted in Test Documentation

i) Best practice and recommendation is that the IL rating for each system function tested is noted in the test documentation or a referenced to the document that provides IL rating for each tested function.

ii) Indication of conformity includes an IL rated in the test documentation, test processes specifically targeting IL-rated functions; alternatively, a reference in the test procedure to another document that provides IL rating information for each tested function.

5.5.6 Integrity Level (IL) Test Reporting

i) An integration test assurance process and resulting report is provided indicating no defects that could cause a system halt in any IL rated system modules.

ii) Indication of conformity includes records of test processes, findings, and corrective actions implemented for defects discovered in testing of any IL rated system modules.

5.5.7 Internal and Independent ISQM Reviews

i) Internal and independent ISQM reviews are conducted prior to delivery of software to customer.

ii) Indication of conformity includes documentation of reviews, including discovered shortfalls and corrective action reports.

5.5.8 Independent Audit Records

i) Records of outcomes and findings of independent audits are documented and corrective action reports are maintained.

ii) Indication of conformity includes audit processes, records of audits, findings, and corrective actions planned/implemented.

5.5.9 Internal Software Quality Audits

i) An internal software quality assurance team audits the software development environment for conformity to internal procedures and processes.

ii) Indications of conformity include audit processes, records of audits, findings, and corrective actions planned/implemented.

5.5.10 Product Delivery Conformity to ISQM

i) Product delivery procedures and reviews of conformity to ISQM procedures are documented.

ii) Indication of conformity includes review processes, records of reviews, findings, and corrective actions planned/implemented.

5.5.11 Corrected Defects

i) Corrected defects are retested and reported in test results and/or a defect-tracking database.

ii) Indication of conformity includes a fully functional and utilized defect tracking system, including corrective actions, elapsed time-to-correction, and retest report results.

5.5.12 ISQM Prescribed Metrics

i) Metrics as prescribed by ISQM are developed, tracked, and reported in project reviews.

ii) Indication of conformity includes representations of metrics in presentations and other tracking documentation.

iii) ABS does not review metrics data, but reviews documents for indications that metrics are being collected and analyzed.

5.5.13 Verification of As-delivered Software to be Security Tested

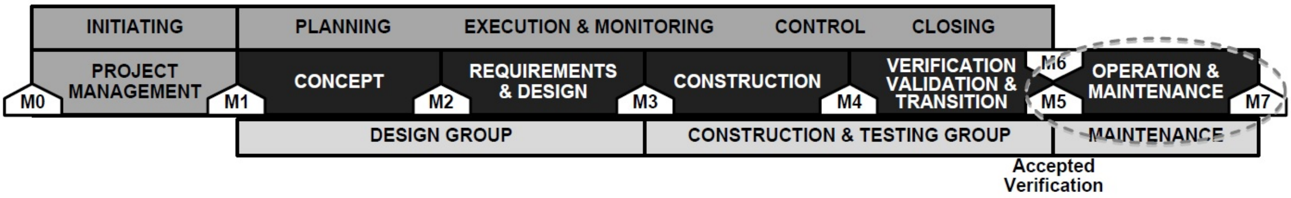
i) The V&V Plan describes procedures that test for common flaws or errors in coding and constructions that leave the product insecure, or susceptible to attacks[18]. Security flaws are noted and removed, and retest results demonstrate successful mitigation.

Note: [18] See '2011 CWE/SANS Top 25 Most Dangerous Software Errors, http://cwe.mitre.org/top25/#CWE-863 (last accessed 3/31/16)

ii) Indications of conformity include (a) security test plan, (b) security flaws log, with mitigation actions; (c) security test log.

5.7 Operation and Maintenance Phase

FIGURE 9
Integrated Best Practices Approach: Software Operation and Maintenance



The Maintenance and Operation Phase includes operational and maintenance activities, scheduled and unscheduled upgrades, problem resolution activities, and retirement of the software system. The key event of this phase is the delivery of the SP's Operation and Maintenance manuals, which are provided to the owner and operator upon acceptance of the software system. The SP's internal Operation and Maintenance Plan (O&M Plan) contains information concerning the operation of the system, and system support protocols. The activities of this phase are the responsibility of the owner/operator with the SP's involvement, if requested by the owner/operator, see Section 3, Figure 9.

5.7.1 Code Archiving

i) Code is physically archived for recovery of failed systems, and code is controlled for version, data and personnel access (i.e., restrictions) according to a documented configuration management procedure.

ii) Indication of conformity includes a code archiving process and archive that facilitates basic system recovery and a basic documented system restart/recovery procedure.

5.7.2 Release Control of Modified Code

i) Modifications (minor and major) of system functionality include a documented release control procedure and a documented on-site system modification procedure.

ii) Indication of conformity includes documentation that releases follow a documented release control feature that release notes are provided to the owner or operator as requested, and a history of supplier-controlled releases.

5.7.3 Verification of Software Updates to be Malware-free

i) Field installed modifications to software are tested to be malware-free, and are performed according to a malware prevention protocol.

ii) Indication of conformity includes software security processes and documentation that software modifications (e.g., patches, defect fixes and updates) are tested for malware prior to installation, and installed in adherence to a documented malware prevention process.

5.7.4 Problem Resolution Capability or Customer Help Desk

i) A best practice and recommendation is that the system user has access to supplier personnel capable of resolving software issues.

ii) Indication of conformity includes availability (to customers) of supplier personnel with the capability of resolving and documenting user issues, corrective actions recommended, results of those actions, and response times for addressing the issues.

7 Product Design Assessment Renewal-

7.1 Introduction

A Product Design Assessment for software expires two years after the date of issue by ABS. An ABS ISQM-PDA Renewal is provided based on the following conditions.

7.1.1 PDA Renewal Eligibility

An SP is eligible to request PDA renewal if the SP has successfully completed an ISQM-PDA assessment or ISQM-PDA Renewal assessment within the past 24 months, with special consideration by ABS. If the SP fails to renew the PDA prior to expiration, the SP is to reinitiate the PDA-Part 1 and PDA-Part 2 assessments, with special considerations by ABS.

7.1.2 PDA Renewal Applicability

The PDA Renewal applies only to the products, development organization(s), and site named on the original PDA. Additional products developed at this location are specially considered by ABS.

7.1.3 PDA Renewal Assessment

The PDA Renewal assessment is performed at the SP's site by ABS assessors and is based on the topics referenced in an original PDA assessment, with special considerations by ABS. The SP may request that the ISQM-PDA be renewed based on special considerations by ABS, such as participating in an ABS review of a successfully completed project for which ABS' ISQM Notation was issued to an asset.

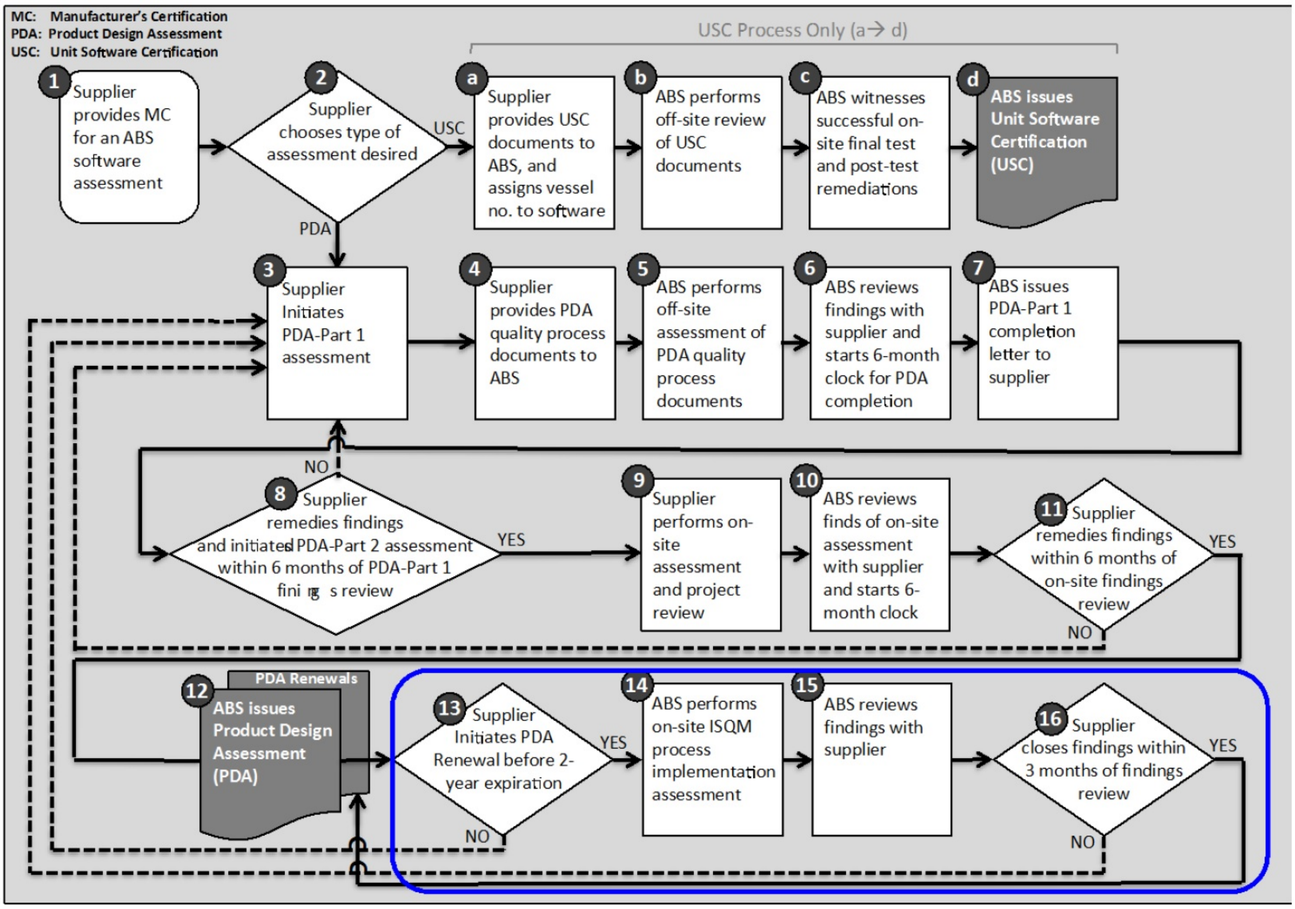
7.1.4 PDA Renewal and Secondary Entities

A Product Design Assessment Renewal certification may only be issued to the original System Provider (SP). The SP is the entity that has legal or patent rights to produce the software product or system. ABS considers the SP to be responsible for the continued conformity of named products to the PDA as assessed and issued to the original SP. If the SP engages a secondary entity for production, maintenance, or support of products named for PDA, then that secondary entity is to be included in the PDA Renewal Assessment, with special considerations by ABS. See 2/1.1.1 for additional details concerning use of a secondary entity and PDA Renewal.

7.1.5 PDA Renewal Term and Publication

The effective term of a PDA Renewal is two years. ABS recommends that the SP initiate the Renewal process in advance of PDA expiration. Renewals are made public on the ABS website. PDA certifications that expire are removed from the ABS website until the PDA is renewed.

FIGURE 10
PDA Renewal Process


MC: Manufacturer's Certification
PDA: Product Design Assessment
USC: Unit Software Certification
USC Process Only (a→ d)
1 Supplier provides MC for an ABS software assessment
2 Supplier chooses type of assessment desired
USC
PDA
a Supplier provides USC documents to ABS, and assigns vessel no. to software
b ABS performs off-site review of USC documents
c ABS witnesses successful on-site final test and post-test remediations
d ABS issues Unit Software Certification (USC)
3 Supplier Initiates PDA-Part 1 assessment
4 Supplier provides PDA quality process documents to ABS
5 ABS performs off-site assessment of PDA quality process documents
6 ABS reviews findings with supplier and starts 6-month clock for PDA completion
7 ABS issues PDA-Part 1 completion letter to supplier
NO
8 Supplier remedies findings and initiated PDA-Part 2 assessment within 6 months of PDA-Part 1 fini ng s review
YES
9 Supplier performs on-site assessment and project review
10 ABS reviews finds of on-site assessment with supplier and starts 6-month clock
11 Supplier remedies findings within 6 months of on-site findings review
YES
NO
PDA Renewals
12 ABS issues Product Design Assessment (PDA)
13 Supplier Initiates PDA Renewal before 2-year expiration
YES
NO
14 ABS performs on-site ISQM process implementation assessment
15 ABS reviews findings with supplier
16 Supplier closes findings within 3 months of findings review
YES
NO

SECTION 4
Unit Software Certification (USC)

1 Introduction

ABS offers a Unit Software Certification (USC) to software suppliers. This offering corresponds to the Tier 5 – Unit Certification described in the ABS *Rules for Conditions of Classification (Part 1)*. The USC is issued for software based on two criteria:

i) The SP has an active ISQM-PDA Certificate or the SP is to provide an MC letter and software quality engineering process documentation as indicated by ABS.

ii) An ABS assessor has witnessed the successful completion of a final test of a specific software system limited to installation on a specific vessel or asset.

TABLE 1
ISQM Unit Software Certification

Marine Vessel Rules Approval Tiers		*ISQM Certification Tiers*	
Tier 1	Manufacturer's Certification (MC)	Tier 1	*Manufacturer's Certification (MC)*
Tier 2	Product Design Assesment (PDA)	Tier 2	*Product Design Assesment (PDA)*
Tier 3	Type Approval (TA)	Tier 3	Not Applicable
Tier 4	Product Certification via Product Quality Assurance (PQA)	Tier 4	Not Applicable
Tier 5	**Unit Certification via Survey During Fabrication (UC)**	**Tier 5**	***Unit Certification via Survey During Final Test (USC)***

This Section provides information to help the software supplier obtain ABS Unit Software Certification for software products to be installed on a specific vessel or asset.

3 Supplier Preparation for Unit Software Certification

3.1 Unit Software Certification

i) The SP is to provide a Manufacturer’s Certification to ABS.

ii) The SP is to have an active ISQM-PDA Certificate, or is to have completed Part 1 of the ISQM-PDA certification process,

or

iii) The SP is to provide additional documentation for the equipment and control system as listed below to ABS prior to performing the final test of the product to be named in the USC. The documentation is to include:

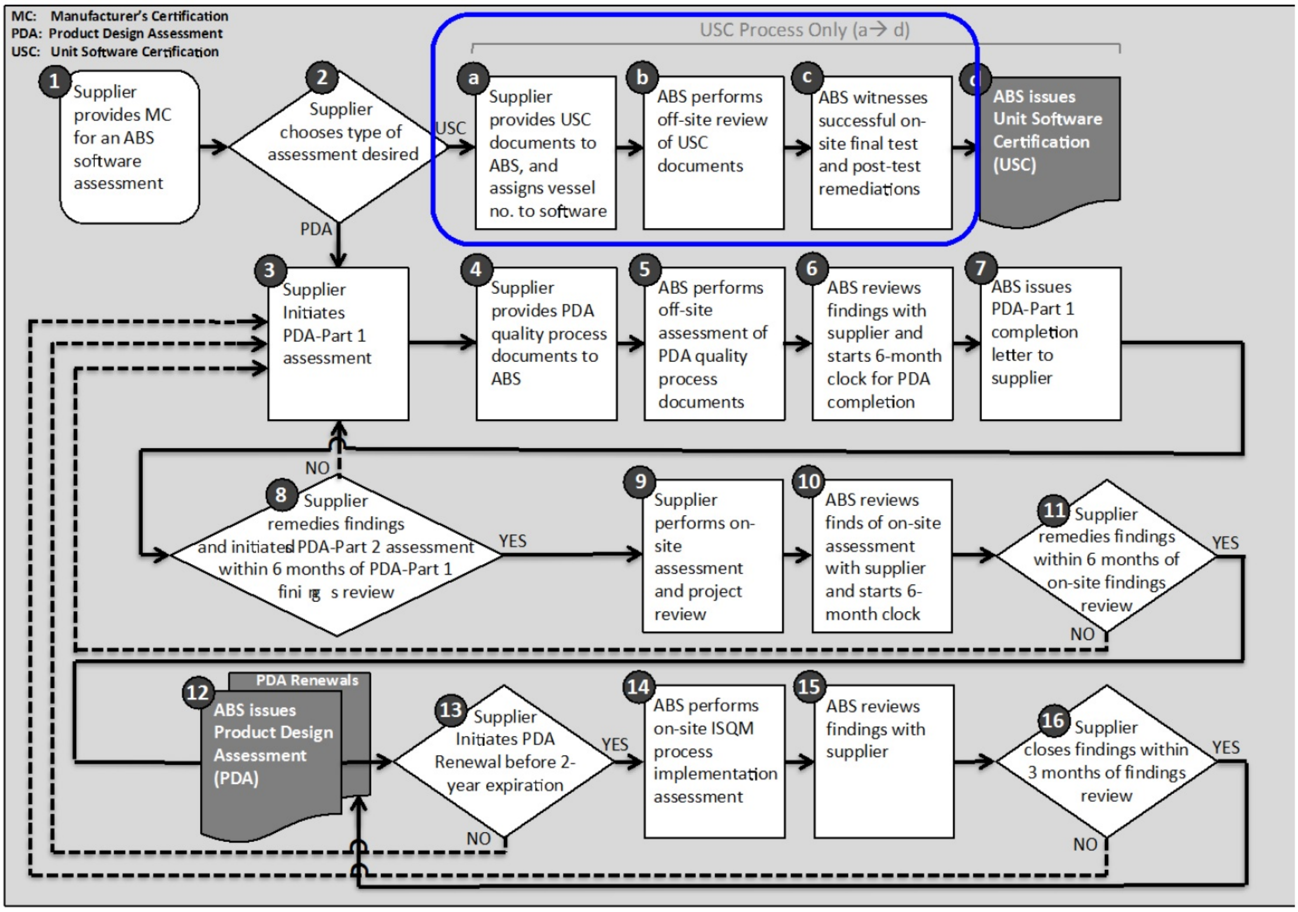
- The SP's software quality policies and procedures
- Product functional description document or equivalent as described in the ISQM Guide
- Product safety review and/or FMECA documentation
- Software management of change and configuration management policy and procedures
- Detailed test plan

iv) ABS witnesses the final or verification testing of the subject equipment and control system, or any subsequent retesting and provide a final report of findings.

v) Upon successful completion of the final test activity, the SP is to provide a Final Test Report to ABS for review.

The process for obtaining USC is shown in the ISQM conformity certification in the figure below.

FIGURE 1
ISQM Unit Software Certification


MC: Manufacturer's Certification
PDA: Product Design Assessment
USC: Unit Software Certification
USC Process Only (a→ d)
1 Supplier provides MC for an ABS software assessment
2 Supplier chooses type of assessment desired
USC
PDA
a Supplier provides USC documents to ABS, and assigns vessel no. to software
b ABS performs off-site review of USC documents
c ABS witnesses successful on-site final test and post-test remediations
d ABS issues Unit Software Certification (USC)
3 Supplier Initiates PDA-Part 1 assessment
4 Supplier provides PDA quality process documents to ABS
5 ABS performs off-site assessment of PDA quality process documents
6 ABS reviews findings with supplier and starts 6-month clock for PDA completion
7 ABS issues PDA-Part 1 completion letter to supplier
NO
8 Supplier remedies findings and initiated PDA-Part 2 assessment within 6 months of PDA-Part 1 fini g s review
YES
9 Supplier performs on-site assessment and project review
10 ABS reviews finds of on-site assessment with supplier and starts 6-month clock
11 Supplier remedies findings within 6 months of on-site findings review
YES
NO
PDA Renewals
12 ABS issues Product Design Assessment (PDA)
13 Supplier Initiates PDA Renewal before 2-year expiration
YES
NO
14 ABS performs on-site ISQM process implementation assessment
15 ABS reviews findings with supplier
16 Supplier closes findings within 3 months of findings review
YES
NO

3.3 PDA Certification and USC

3.3.1

If the SP has a current or is in the process of acquiring an ISQM-PDA and the product or software system is not listed in ISQM-PDA certificate or in the documentation associated with the acquiring process, then special consideration by ABS may by sought.

3.3.2

A supplier may request that a USC assessment to be included with a PDA evaluation.

5 ABS Issuance of a USC Report or Letter to the Software Supplier

5.1 ABS Review of Final Test Procedure

Prior to the initiation of the final test to be witnessed for USC, the SP is to submit a final test procedure document for the software system to be tested to ABS. Further, the SP is to provide to ABS a Functional Description Document (FDD) or equivalent documentation detailing the functionality and failure actions of the equipment to which the USC is applied. ABS assesses the test procedure document for conformity to the *ISQM Guide* processes and the SP's SQA processes that are to be provided to ABS by the SP. Nonconformity to the *ISQM Guide* or to the supplier's SQA system is to be communicated by ABS to the SP prior to the initiation of the final test.

5.3 ABS Witnessing of the Software System Final Test

i) An ABS assessor witnesses the final test of the software system being assessed for the USC. The ABS assessor observes the disciplined execution of final test activities as documented in the final test procedure. The ABS assessor notifies the SP of any discrepancies noted during the test activities. Retesting of corrected findings is to be witnessed by ABS.

ii) The version number of the software approved for the USC is to be recorded after testing.

iii) The processor's firmware version number is to be recorded.

iv) Type and serial numbers of all hardware under test is to be recorded.

5.5 System Provider Final Test Report

Final Test failures, customer concerns, "punch list" items, and resolutions/remedies are to be noted and reported by the SP in a Final Test Report.

i) The Final Test Report is to be provided to ABS for review.

ii) ABS reviews this report for:

a) Comprehensive coverage of test findings;

b) Resolution of test findings;

c) Indications that the software system performs as documented in the Final Test Procedure;

d) Firmware version tracking of the control system;

e) Software version number tracking for all software tested; and,

f) Designation of the asset/unit that is to receive the tested system.

5.7 ABS-issued Unit Software Certification

Based on the ABS evaluations during test witnessing, Final Test procedure, adherence to the Final Test procedure, test outcomes, and a review of the Supplier Final Test Report, ABS will issue a test report to the SP that either issues or denies USC for the product and software version number, and the associated vessel/unit named in the Final Test Procedure. ABS may also issue a USC Letter (see Appendix 4) to the SP.

APPENDIX 1
Recommended References

- American Bureau of Shipping, *Guide for Integrated Software Quality Management (ISQM), September 2012*
- American Bureau of Shipping, *Guidance Notes on Application of Cybersecurity Principles to Marine and Offshore Operations – ABS CyberSafety^{TM} Volume 1, September 2016*
- American Bureau of Shipping, *Guide for Cybersecurity Implementation for the Marine and Offshore Operations – ABS CyberSafety^{TM} Volume 2, September 2016*
- American Bureau of Shipping, *Guidance Notes on Data Integrity for Marine and Offshore Operations – ABS CyberSafety^{TM} Volume 3, September 2016*
- American Bureau of Shipping, *Guide for Software Systems Verification – ABS CyberSafety^{TM} Volume 4, September 2016*
- A. Neufelder, SoftRel, *The Cold Hard Truth About Reliable Software, Revision 6f, 2015*
- C. Kaner, J. Bach, B. Petticord, *Lessons Learned in Software Testing, 2002*
- N. Leveson, Safeware: *System Safety and Computers, April, 1995*
- 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* (International Standard ISO/IEC 12207)
- IEEE Std 1012-2004, *Standard for Software Verification and Validation*
- IEEE Std 730-2002, *Standard for Software Quality Assurance Plans*
- IEEE Std 1028-1997, *Standard for Software Reviews*
- IEEE Std 829-2008, *Standard for Software and System Test Documentation*
- R. Shaw – Editor, *Safety and Reliability of Software Systems*, Twelfth Annual CSR Workshop, September, 1995
- *Project Management Body of Knowledge* (PMBOK), Third Edition, 2013

APPENDIX 2

ISQM Software Quality Management – Certification Process

1 Tier 1 – Manufacturer's Certification (MC)

1.1 ISQM PDA Certification Process Requires a Manufacturer's Certification (MC)

i) The supplier notifies ABS of desire to be assessed for the ISQM USC or the ISQM PDA.

ii) The supplier provides an MC letter informing ABS that it implements an ISO 9001 quality management program or a recognized equivalent.

iii) ABS acknowledges receipt of the Manufacturer's Certification by the supplier, and collaborates with the supplier to initiate the ABS USC or the ISQM PDA.

iv) ABS performs no quality management documentation review

v) ABS performs no on-site assessment

1.3 No ABS Certificate is issued

3 Tier 2 – ISQM PDA Certification Process

3.1 Supplier Initiates ISQM PDA-Part 1 Certification Process

3.3 ABS Performs Off-Site PDA-Part 1 Review of Supplier Software Quality Engineering Documentation

3.3.1 ABS Notifies the Supplier of Specific Documentation Required for the PDA

i) ABS meets or communicates with the supplier to determine specific software product(s) or product families to be included in the PDA assessment.

ii) ABS communicates with the supplier to determine which specific product development sites and organizations materially contribute to product development and support (see NOTE below).

iii) ABS requests ISQM-related product description and quality management documentation pertinent to the review of the named product(s) and site(s), including subcontract or 3rd party provider sites utilized for product development and support for the named product(s).

Notes:

1 The term "support" means the act of making programming changes to the named software after delivery of the system to the customer.

2 Supplier informs ABS of 3rd-party software design, development, test, and field support activities performed at sites other than the supplier site named in the PDA. Supplier provides pertinent 3rd-party quality management documentation to ABS for assessment.

3.3.2 ABS Reviews Supplier Quality Management Documentation for ISQM Conformity

i) ABS performs an off-site review of supplier-provided quality management documentation for awareness of and conformance to the *ISQM Guide* and *SPCP Guidance Notes*, and maps the program to ABS ISQM practices.

ii) ABS determines the degree of conformity of ISQM practices presented in the supplier's quality program documentation.

3.3.3 ABS Identifies Supplier Quality Management Documentation Gaps

i) ABS identifies gaps in the supplier's quality program documentation based on criteria provided in the *ISQM Guide* and *SPCP Guidance Notes*.

ii) ABS prepares a findings report and submits the report to the supplier; further, ABS collaborates with the supplier in a “Findings Meeting” in order to clarify findings and gain agreement on Supplier remediation plans.

iii) Upon completion of the Findings Meeting, ABS "starts the 6-month clock" limiting the timeframe for remediation of findings and gaps and reporting those corrective actions to ABS for review.

iv) Upon completion of the Findings Meeting, full payment to ABS for the PDA assessment is due from supplier.

3.3.4 Supplier Closes ABS-identified Gaps and Submits a Remediation Report to ABS.

i) Supplier remedies findings and gaps provided by ABS in the Findings Meeting within 6 months of that Findings Meeting.

ii) Supplier provides a gap remediation report to ABS for evaluation.

iii) Supplier provides remedied documentation to ABS for review.

iv) ABS reviews supplier report and remedied documentation.

v) ABS determines if the supplier quality program as documented conforms to the *ISQM Guide* and *SPCP Guidance Notes*.

vi) ABS communicates conformity (or non-conformity) to the supplier in a documented response.

vii) The supplier expresses intent to proceed (or not) with an on-site evaluation of its implementation of quality management processes as documented.

3.5 ABS Performs a PDA-Part 1 On-Site Assessment of Conformity to Supplier Software Quality Engineering Documentation.

3.5.1 Supplier has Provided Documented Indications of Resolving ABS-identified Gaps in the Software Quality Management Process Documentation within 6 Months from the Date of the ABS Findings Meeting

i) ABS communicates with the supplier's point-of-contact personnel to communicate the interview process, interview timetables, and the job descriptions of supplier staff expected to participate in the interviews.

ii) ABS provides guidance materials to enable the supplier prepare for interviews and provide access to personnel who are expected to participate in the assessment.

3.5.2 ABS Coordinates Assessment Planning with the Supplier

i) ABS and the supplier agree on interview schedule dates and procedures.

ii) ABS interviews the site-specific and product-specific software production and support team(s).

iii) ABS logs findings from interviews.

Notes:

1 ABS may require that 3rd party software product and services suppliers are included in the on-site interviews.

2 ABS utilizes proprietary checklists of primary inquiry points. ABS develops derivative inquiry points during the interviews based on responses.

3.5.3 ABS Performs On-Site Interviews with Specialized Supplier Staff

i) ABS interviews the supplier management team.

a) ABS explains interview process to gain support for additional interviews.

b) ABS interviews software management team to understand operation of organization.

c) ABS interviews software management team to determine level of management participation in, and commitment to the quality program as documented.

ii) ABS interviews the supplier quality engineering team.

a) ABS interviews quality management team to verify its involvement in SDLC phases and its continued development of quality assurance practices to align with ISQM.

iii) ABS interviews the supplier development team.

a) ABS interviews the development team to verify the supplier commitment to, and execution of the quality assurance practices as documented in its quality program.

iv) ABS interviews the supplier test team.

a) ABS interviews test team to verify application of documented quality practices to test planning and execution activities.

v) ABS interviews the supplier software/system maintenance/update team.

a) ABS interviews the software support and maintenance team to verify extension of documented quality program execution to fielded software control systems.

b) ABS interviews software support and maintenance team to evaluate SMOC practices during field updates and fixes.

Note: For additional demonstration of conformity, the assessed supplier may also submit quality management documentation pertinent to the completion of a project based upon the principles and practices documented in the *ISQM Guide* and *SPCP Guidance Notes*.

3.5.4 ABS Communicates the Assessment Findings and Gaps to the Supplier

i) ABS identifies gaps in the supplier's quality program documentation based on criteria provided in the *ISQM Guide* and *SPCP Guidance Notes*.

ii) ABS prepares a findings report and submits the report to the supplier; further, ABS collaborates with the supplier in a “Findings Meeting” in order to clarify findings and gain agreement on Supplier remediation plans.

iii) Upon completion of the Findings Meeting, ABS starts the “6-month clock" limiting the timeframe for remediation of findings and gaps and reporting those corrective actions to ABS for review.

3.5.5 Supplier Closes the Identified and Reported Gaps and Submits a Remediation Report to ABS

i) Supplier remedies findings and gaps provided by ABS in the Findings Meeting within 6 months of that Findings Meeting.

ii) Supplier provides a gap remediation report to ABS for evaluation.

iii) ABS reviews supplier report and determines if the remediated execution of the supplier quality program to the quality program as documented.

iv) ABS communicates conformity (or non-conformity) to the supplier in a documented response.

v) If the supplier does not submit the remediation report within the allowed 6-month timeframe, the PDA process is initiated by the supplier from the beginning, and may be subject to additional ABS cost charges.

vi) ABS may request follow-up interviews with supplier personnel.

3.7 ABS Issues a PDA Certificate

3.7.1 ABS Issues a PDA Certificate for the Named and Assessed Supplier Products, Supplier Sites, and Supplier Teams

i) The ABS PDA is in force for two (2) years from the date of issue.

ii) The PDA is posted on the ABS website.

iii) PDA certifications that expire are removed from the ABS website until renewed.

Note: ABS provides PDA certification for only the supplier of the named products, and does not name or provide individual PDA certification to 3rd-party suppliers in the initiating supplier's PDA certification.

3.9 ABS Performs a PDA Certificate 2-Year Periodic Renewal Assessment

3.9.1 In Order for the Initial PDA Certificate to Remain Active and Present on the ABS Website, the Certificate Must be Renewed within Two (2) Years of the Date of Issue

i) The PDA renewal certification may only be issued to the original System Provider (SP).

ii) The PDA certificate may be renewed based on indications of continued application of ISQM practices provided to ABS in one of four (4) methods.

iii) If the supplier fails to meet PDA renewal requirements, the initial certification process is repeated in its entirety.

3.9.2 ABS Offers a PDA Certificate Renewal Based on an ISQM Reassessment

i) ABS performs a reassessment of the supplier's quality management program as applied to products and development sites named in the PDA. The reassessment includes review of pertinent quality management program documentation and site interviews, with special considerations by ABS.

ii) ABS personnel perform the PDA reassessment. Upon completion of the assessment, ABS provides a findings report to the supplier. ABS charges a fee to the supplier for reassessment.

iii) If the assessment indicates continued conformity to the *ISQM Guide* and *SPCP Guidance Notes*, the PDA certificate is renewed.

3.9.3 ABS Offers a PDA Certificate Renewal Based on Demonstrated Application of ISQM Practices to Completed Projects

i) ABS reviews documentation for at least 5 projects pertaining to products named in the PDA that have been completed during the two-year certification period.

ii) ABS personnel perform the PDA reassessment. Upon completion of the project assessments, ABS provides a findings report to the supplier. ABS charges a fee to the supplier for reassessment.

iii) If the assessments indicate continued conformity to the *ISQM Guide* and *SPCP Guidance Notes*, the PDA certificate is renewed.

3.9.4 ABS Offers a PDA Certificate Renewal Based on Vessel Type Certification

i) ABS renews the supplier PDA certificate if the supplier completes a project that has been implemented under its PDA-certified quality program governance and is installed/implemented aboard a vessel that receives an ABS Vessel Notation.

ii) The PDA certificate is renewed for period of two (2) years from the date of vessel commissioning.

iii) ABS does not charge a fee to the supplier for renewals based on Vessel Type Certification.

3.9.5 ABS Offers a PDA Certificate Renewal Based on Vessel Type Renewal

i) ABS renews the supplier PDA certificate if the supplier completes a project that has been implemented under its PDA-certified quality program governance and is installed/implemented aboard a vessel that receives an ABS Vessel Notation Renewal.

ii) The PDA certificate is renewed for period of two (2) years from the date of ABS Vessel Notation Renewal.

iii) ABS does not charge a fee to the supplier for renewals based on Vessel Type Certification Renewal.

3.11 ABS Performs a Non-periodic PDA Certificate Assessment as Required to Verify Continued Conformity

3.11.1 ABS May Initiate a non-periodic PDA Certificate Assessment Based Upon One or More Failures in the Software Applications or Systems Named in the PDA.

i) ABS may initiate a non-periodic PDA certificate assessment based upon failure of a software update provided by the SP from any supplier location.

ii) ABS does not charge a fee for ABS-initiated non-periodic PDA certificate assessments.

iii) ABS may initiate a non-periodic PDA certificate assessment based upon one or more major change in the named software applications or systems named in the PDA.

iv) ABS does not renew the PDA based on a non-periodic PDA assessment.

Note: For description "major" software changes, see ABS SMOC Section/Appendix of the *ISQM Guide*.

5 Tier 5 – Unit Software Certification (USC) Assessment

5.1 Vessel Owner/Operator Initiates an ABS Unit Software Certification with ABS

5.1.1 Customer/Owner/Operator or Supplier Notifies ABS of the Product Submitted for USC and the Designated Vessel on which the Product Will be Installed.

i) Supplier notifies ABS of the Final Test schedule for product to be USC assessed.

ii) If ABS PDA-Part 1 or ABS PDA has not been completed for the product identified for the USC assessment, the supplier provides pertinent quality management program documentation to ABS.

a) The supplier provides documentation governing the quality assurance policies, procedures, and practices for the product identified for USC assessment.

b) The supplier provides a product functional description document (FDD) or equivalent for the product identified for USC assessment to ABS.

c) The supplier provides a safety review or software failure modes, effects, and criticality analysis (SFMECA) document for the product identified for USC assessment to ABS, including the designated integrity level (IL) of the product or system identified for USC assessment.

d) Supplier provides a current/updated test plan for the product identified for a USC assessment to ABS.

iii) If the SP has an ISQM-PDA Certificate, then the review of software quality engineering documentation is waved; however, the product test plan is to be provided to ABS.

5.1.2 ABS Reviews Product Documentation and Develops a Findings Report for the Product Identified for Assessment

i) ABS presents a findings report that informs the owner/operator and supplier of any gaps found in the current/updated test plan and safety review or FMECA for the product identified for a USC assessment.

ii) ABS collaborates with the owner/operator to determine whether or not the owner/operator elects to proceed with the USC assessment with or without supplier correction of reported gaps.

5.3 ABS Witnesses the On-Site Test of the Named Product(s)

5.3.1 An ABS Assessor Attends the Final Acceptance in Order to Witness the Conformity of the Test as Executed to the Supplier Test Plan and Software Quality Engineering Practices as Provided in the ABS ISQM Guide and SPCP Guidance Notes.

i) ABS assessor attends on-site final acceptance test of the product(s) submitted for USC certification.

ii) ABS assessor records the software version number, firmware version numbers, operating system numbers and serial numbers of all parts of the control system associated with the USC.

iii) ABS assessor witnesses and evaluates test procedures for adherence to the test plan.

iv) ABS assessor maintains contemporaneous notes of the test activities and documents exceptions to the documented and reviewed test plan and ISQM practices.

v) ABS assessor may recommend delaying or restarting the test based on non-conformance to the test plan.

vi) ABS assessor may discontinue the USC assessment for non-conformance to the test plan.

vii) Upon completion of the test plan, ABS reviews the test punch-list with the supplier owner/operator.

viii) ABS assessor witnesses retesting of punch-list items for conformity to supplier and customer-approved test requirements.

ix) ABS assessor notes exceptions to the retest plan and ISQM practices.

x) ABS reports noted exceptions to the supplier and owner/operator.

xi) Supplier provides a gap analysis, punch-list, and final remediation report to ABS for evaluation.

xii) ABS reviews the supplier remediation report provided by the supplier and determines whether or not to issue the USC.

5.5 ABS Issues the USC Letter

5.5.1 ABS Issues a Non-renewable USC Certificate for the Assessed Supplier Product(s) Specified for Implementation Aboard the Named Asset/Vessel

i) ABS notifies the owner/operator of the USC certification.

ii) ABS invoices owner/operator for completed USC certification project.

APPENDIX 3

Sample ISQM-PDA-Part 1 Letter of Completion

Letter of Completion: ISQM Product Design Assessment – Part 1

Date of Issue: ***Day_Month_Year***

This Letter provides that:

Supplier Name

Specific Supplier Department, City, State, Country

requested that the American Bureau of Shipping (ABS) assess the software programming and configuration quality policies and procedures documentation developed and utilized within the above named [SUPPLIER NAME] department and at the above named [SUPPLIER NAME] location. As a result of that assessment, ABS represents that [SUPPLIER NAME-LOCATION] software quality management documentation demonstrated conformity to the policies and procedures described by the ABS *Integrated Software Quality Management (ISQM) Guide*. ABS further represents that this ISQM-PDA-Part 1 Letter is valid for software control systems programmed and configured according to policies and procedures as assessed by ABS within the [SUPPLIER NAME]-[SUPPLIER DIVISION] in [CITY], [STATE], [COUNTRY].

Neither this evaluation, nor the resulting ISQM-PDA-Part 1 Letter waives unit certification or classification procedures required by ABS Rules and applicable Guides for products to be installed in ABS classed vessels or facilities. This ISQM-PDA-Part 1 Letter does not claim, imply, or indicate that the software programmed and configured by the above-named company, or the equipment or products controlled by that software have been either assessed for ABS Type Approval or Type Approved by ABS. The scope of applicability and product limitations of this assessment are detailed in the attachment to this ISQM-PDA-Part 1 Letter, titled Appendix A.

Intended Service:

This ISQM-PDA-Part 1 Letter applies only to [SUPPLIER NAME] software systems configured or programmed following the [SUPPLIER NAME]-[SUPPLIER DIVISION] software development process assessed by ABS and applied to the specific products listed in Appendix A of this Letter.

Services Restrictions:

Unit Software Certification is not required for the software quality management process documentation that has been assessed; however, unit certification may be required for the separate and individual products listed in Appendix A. If the manufacturer or purchaser of the products listed in Appendix A requests an ABS certification for compliance with a specification or standard, then that specification or standard, including inspection standards and tolerances, must be designated and provided to ABS for the purposes of performing that certification.

Ratings:

This ABS ISQM-PDA-Part 1 Letter is provided to [SUPPLIER NAME]-[SUPPLIER DIVISION] based on that department’s conformity with the quality standards set by ABS’ *ISQM Guide* for software programming and configuration processes. Further, this ISQM-PDA-Part 1 Letter confirms that ABS has assessed software quality policies and procedures documentation provided by [SUPPLIER NAME]-[SUPPLIER DIVISION], and that the assessed documentation conforms to procedures sufficient for software quality process implementation as described in ABS’ *ISQM Guide*.

Notes/Drawings/Documentation:

The ABS ISQM reviewers have assessed the drawings and documents necessary for meeting the conformity requirements set forth by this ISQM-PDA-Part 1 Letter.

Comments:

This ABS ISQM-PDA-Part 1 Letter is provided to [SUPPLIER NAME]-[SUPPLIER DIVISION], [SUPPLIER DIVISION CITY, STATE, COUNTRY] to affirm that the named department has documented software quality procedures, policies and processes that meet the software development quality guidelines established by ABS’ *ISQM Guide*.

Terms of Validity:

This ISQM-PDA-Part 1 Letter is valid only for software products enumerated in Appendix A and configured or programmed by the [SUPPLIER NAME]-[SUPPLIER DIVISION] located in [CITY], [STATE], [COUNTRY]. This ISQM PSA-Part 1 is valid for six months from its Date of Issue, and is not renewable.

Standards:

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

Signature of ABS ISQM Engineer

ABS ISQM Engineer

ISQM DLR-CC Appendix A – Product(s) Developed by [SUPPLIER NAME]-[SUPPLIER DIVISION]

[SUPPLIER PRODUCT(S) LISTED]

APPENDIX 4
Sample PDA Certificate

SUPPLIER NAME AND DIVISION/DEPARTMENT

ATTN: [SUPPLIER CONTACT NAME]

[SUPPLIER DIVISION/DEPARTMENT ADDRESS]

Telephone: [SUPPLIER TELEPHONE NUMBER]

Email: [SUPPLIER CONTACT EMAIL ADDRESS]

Web: [SUPPLIER WEB ADDRESS]

Product: ISQM Product Design Assessment (PDA)

Model: Procedures Used in Developing Control System Software

Intended Service:

Developed Software Control Systems are intended for installation in the following Products (Tools), as configured or programmed following the [SUPPLIER NAME]-[SUPPLIER DIVISION] Software Development Process:

[LISTING OF PRODUCTS SURVEYED]

Description:

This assessment is a representation by ABS of the degree of conformity to, and implementation of, the policies and procedures related to applicable sections of the ABS *Integrated Software Quality Management (ISQM) Guide*. This assessment does not waive unit certification or classification procedures required by ABS Rules and applicable Guides for products to be installed in ABS classed vessels, MODUs, or facilities. This certificate, by itself, does not reflect that the product controlled by the developed, configured, and programmed software is Type Approved. The scope and limitations of this assessment are detailed on the pages attached to this Integrated Software Quality Management Product Design Assessment Certificate (ISQM-PDA).

This ABS Product Design Assessment Certificate for quality software development is awarded to [SUPPLIER NAME]-[SUPPLIER DIVISION] based on conformity with the quality standards set by ABS' *ISQM Guide* for software development processes. This certificate confirms that [SUPPLIER NAME]-[SUPPLIER DIVISION] has demonstrated application of quality standards, procedures, and policies in software development sufficient for the implementation of ISQM.

Service Restrictions:

Unit software certification is not required for the software quality management processes that have been assessed; however, unit certification may be required for the separate and individual products listed above. If the manufacturer or purchaser of the products listed above requests an ABS certification for compliance with a specification or standard, then that specification of standard, including inspection standards and tolerances, must be designated and provided to ABS for the purposes of performing that certification.

Comments

This ISQM-PDA has been earned by [SUPPLIER NAME]-[SUPPLIER DIVISION] based on the American Bureau of Shipping evaluation of the software quality policies and procedures followed by [SUPPLIER NAME]-[SUPPLIER DIVISION] during the development, programming, and configuration of software and installed as control systems in the above listed products or equipment. This certificate verifies that the [SUPPLIER NAME]-[SUPPLIER DIVISION] utilizes recognized software development policies, procedures, templates, and documents development, programming, and configuration of quality software for the products produced at this location.

Notes/Drawings/Documentation:

This ISQM-PDA is valid for the software quality policies and procedures used by [SUPPLIER NAME]-[SUPPLIER DIVISION] located in [CITY], [STATE], [COUNTRY], for developing the control system software for the products listed above.

Term of Validity:

This Product Design Assessment (PDA) Certificate [CERTIFICATE NUMBER], dated [CERTIFICATE EFFECTIVE DATE] remains valid until [CERTIFICATE EXPIRATION DATE] or until the Rules or specifications used in the assessment are revised (whichever occurs first).

This PDA is intended for a product to be installed on an ABS classed vessel, MODU or facility which is in existence or under contract for construction on the date of the ABS Rules or specifications used to assess the Product.

Use of the Product on an ABS classed vessel, MODU or facility which is contracted after the validity date of the ABS Rules and specifications used to assess the Product, will require re-evaluation of the PDA.

Use of the Product for non-ABS-classed vessels, MODUs or facilities is to be to an agreement between the manufacturer and intended client.

STANDARDS

ABS Rules:

The Rules applicable to this assessment are: ABS *Guide for Integrated Software Quality Management (ISQM)*

National:

NA

International:

NA

Government Authority:

NA

EUMED:

NA

Others:

NA

APPENDIX 5
Sample Unit Software Certification

Unit Software Certification Letter of

ISQM Conformity

Date of Issue: ***Day_Month_Year***

This letter provides that:

Supplier Name

Specific Supplier Department, City, State, Country

requested that the American Bureau of Shipping (ABS) witness the test of the [PRODUCT NAME, PRODUCT ID, PRODUCT REVISION NUMBER, PRODUCT REVISION DATE], tested on the date(s) [PRODUCT TEST DATE OR DATES] by the above named [SUPPLIER NAME] department, and at the above named [SUPPLIER NAME] location. As a result of that test witnessing, ABS represents that above named test procedure demonstrated conformity to the policies and procedures described by the ABS *Integrated Software Quality Management (ISQM) Guide*. ABS further represents that this Unit Software Certification (USC) Letter of ISQM Conformity is valid for only for the software product named above, described in Appendix A, and intended for use on [HULL OR RIG DESIGNATION ON WHICH THE NAMED SOFTWARE WILL BE DEPLOYED OR INSTALLED].

Neither this witnessing of product test, nor the resulting Unit Software Certification Letter, waives unit certification or classification procedures required by ABS Rules and applicable Guides for products to be installed in ABS classed vessels or facilities. This Unit Software Certification Letter does not claim, imply, or indicate that the software named in Appendix A as configured for the above designated hull or rig by the above-named company, or the equipment or products controlled by that software have been either assessed for ABS Type Approval or Type Approved by ABS. The scope of applicability and product limitations of the test witnessed are detailed in the attachment to this Unit Software Certification Letter, titled Appendix A.

Intended Service:

This Unit Software Certification Letter applies only to [SUPPLIER NAME] software product described in Appendix A, configured or programmed by [SUPPLIER NAME]-[SUPPLIER DIVISION] for [HULL OR RIG DESIGNATION ON WHICH THE NAMED SOFTWARE WILL BE DEPLOYED OR INSTALLED] as detailed below, as tested and witnessed by the undersigned ABS assessors. A USC Letter issued to a specific hull, rig number, or application specified in the USC Letter, and is not valid for any other application, hull, rig different software version number or firmware version number. The product identified in any USC Letter may to be retested and witnessed by ABS when it is assigned to a rig number, hull number, software or firmware is updated or application not associated with or identified in a USC Letter previously issued by ABS.

Services Restrictions:

Unit Software Certification is not required for the software quality management test process that has been witnessed; however, unit certification may be required for the separate and individual products listed in Appendix A. If the manufacturer or purchaser of the products listed in Appendix A requests an ABS certification for compliance with a specification or standard, then that specification or standard, including inspection standards and tolerances, must be designated and provided to ABS for the purposes of performing that certification. This USC does not imply fit for purpose and the software testing is limited to the functionality tested as listed in Appendix B.

Ratings:

This ABS ISQM Unit Software Certification Letter is provided to [SUPPLIER NAME]-[SUPPLIER DIVISION]-[PRODUCT NAME AS TESTED] based on the conformity of the test as witnessed with the quality standards set by ABS' *ISQM Guide* for software test processes. Further, this Unit Software Certification Letter confirms that ABS has assessed test procedures and processes documentation provided by [SUPPLIER NAME]-[SUPPLIER DIVISION] for the product named and described in Appendix A, and that the witnessed test conforms to test procedures sufficient for software quality test process implementation as described in ABS' *ISQM Guide*.

Notes/Drawings/Documentation:

The ABS ISQM reviewers have assessed the test procedure documents necessary for meeting the conformity requirements set forth by this Unit Software Certification Letter.

Comments:

This ABS ISQM Unit Software Certification Letter is provided to [SUPPLIER NAME]-[SUPPLIER DIVISION], [SUPPLIER DIVISION CITY, STATE, COUNTRY] to affirm that the named department has performed and documented testing of the product named and described in Appendix A for [HULL OR RIG DESIGNATION ON WHICH THE NAMED SOFTWARE WILL BE DEPLOYED OR INSTALLED] in conformance with policies and processes that meet the software testing quality guidelines established by ABS' *ISQM Guide*.

Terms of Validity:

This ISQM Unit Software Certification Letter is valid only for software products enumerated in Appendix A and configured or programmed by the [SUPPLIER NAME]-[SUPPLIER DIVISION] located in [CITY], [STATE], [COUNTRY] for the product named and described in Appendix A. This Unit Software Certification Letter is not renewable.

Standards:

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

Signature of ABS ISQM Engineer

ABS ISQM Engineer

Signature of ABS ISQM Department Manager

ABS ISQM Department Manager

ISQM DLR-CC Appendix A – Product(s) Developed by [SUPPLIER NAME]-[SUPPLIER DIVISION]

[SUPPLIER PRODUCT(S) LISTED]

Equipment Number 1: [ENTER NAME OF EQUIPMENT]

Serial Number of Equipment: [ENTER SERIAL NUMBER]

Software Version Number: [ENTER SOFTWARE VERSION NUMBER]

Processor's Firmware Version Number: [ENTER FIRMWARE VERSION NUMBER]

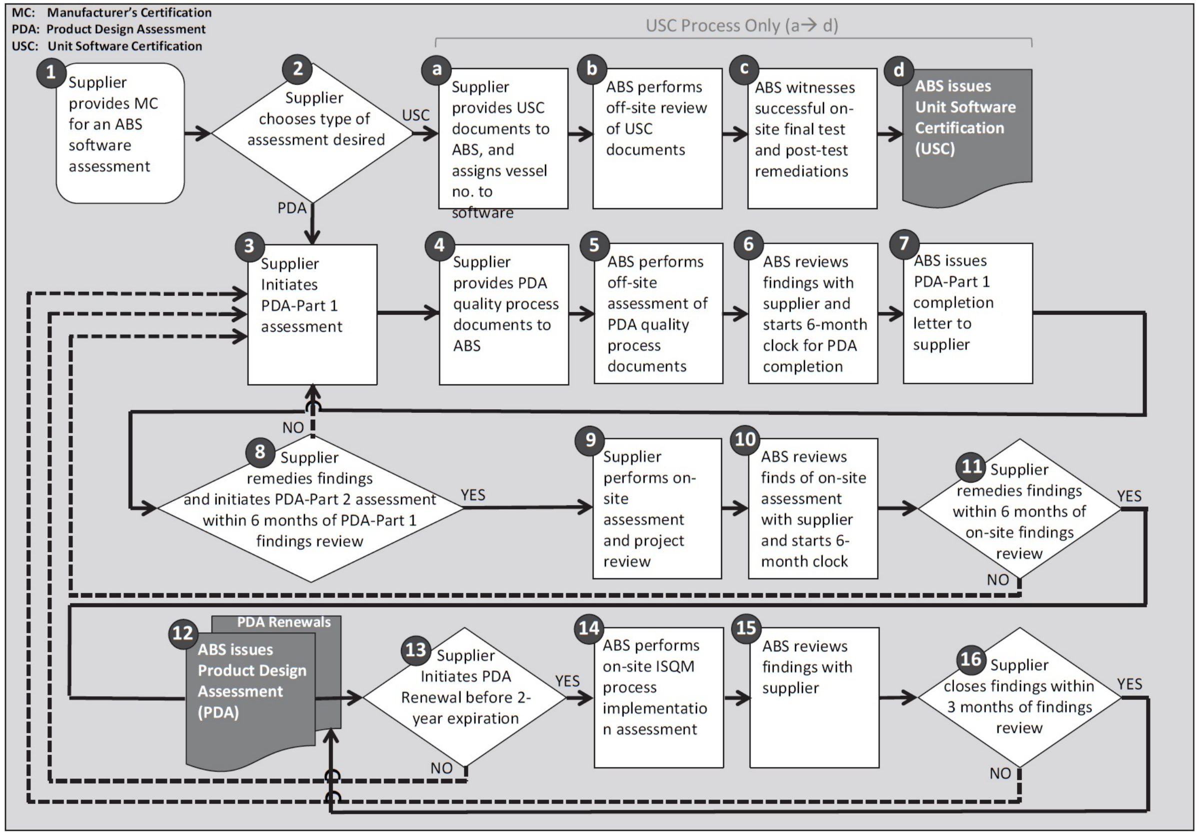
[REPEAT THE ABOVE FOR ALL EQUIPMENT ASSOCIATED WITH THIS USC, IF ANY]

Appendix B – V&V Reports

[ATTACH V&V REPORT, COMMISSIONING/INTEGRATION TEST REPORT]

APPENDIX 6

ISQM Conformity Certification Process


MC: Manufacturer's Certification
PDA: Product Design Assessment
USC: Unit Software Certification
USC Process Only (a→ d)
1 Supplier provides MC for an ABS software assessment
2 Supplier chooses type of assessment desired
USC
PDA
a Supplier provides USC documents to ABS, and assigns vessel no. to software
b ABS performs off-site review of USC documents
c ABS witnesses successful on-site final test and post-test remediations
d ABS issues Unit Software Certification (USC)
3 Supplier Initiates PDA-Part 1 assessment
4 Supplier provides PDA quality process documents to ABS
5 ABS performs off-site assessment of PDA quality process documents
6 ABS reviews findings with supplier and starts 6-month clock for PDA completion
7 ABS issues PDA-Part 1 completion letter to supplier
NO
8 Supplier remedies findings and initiates PDA-Part 2 assessment within 6 months of PDA-Part 1 findings review
YES
9 Supplier performs on-site assessment and project review
10 ABS reviews finds of on-site assessment with supplier and starts 6-month clock
11 Supplier remedies findings within 6 months of on-site findings review
YES
NO
PDA Renewals
12 ABS issues Product Design Assessment (PDA)
13 Supplier Initiates PDA Renewal before 2-year expiration
YES
NO
14 ABS performs on-site ISQM process implementatio n assessment
15 ABS reviews findings with supplier
16 Supplier closes findings within 3 months of findings review
YES
NO