

GUIDE FOR

INTEGRATED SOFTWARE QUALITY MANAGEMENT (ISQM)

SEPTEMBER 2012

Guide to Color Coding Used in Online Version of the Guide

The following summarizes the colors corresponding to Rule Changes, Corrigenda items and editorial changes in the Guide files which are available for download.

Rule Changes:

Changes effective 1 September 2012

Corrigenda:

CORRIGENDA/EDITORIALS – 1 February 2014

CORRIGENDA/EDITORIALS – 1 July 2014

CORRIGENDA/EDITORIALS – 22 February 2016

Editorials:

Editorial Changes



GUIDE FOR

INTEGRATED SOFTWARE QUALITY MANAGEMENT (ISQM)

SEPTEMBER 2012 (Updated February 2016 – see next page)

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

**Copyright © 2012
American Bureau of Shipping
ABS Plaza
16855 Northchase Drive
Houston, TX 77060 USA**

Updates

February 2016 consolidation includes:

- July 2014 version plus Corrigenda/Editorials

July 2014 consolidation includes:

- February 2014 version plus Corrigenda/Editorials

February 2014 consolidation includes:

- September 2012 version plus Corrigenda/Editorials

Copyright American Bureau of Shipping

Foreword

The marine and offshore industries are increasingly relying on computer-based control systems; therefore the verification of the software used in control systems and their integration into the system is an important element within the overall safety assessment. Accordingly, ABS is introducing this *Guide for Integrated Software Quality Management (ISQM)*. Compliance with the procedures and criteria given in this Guide may result in the granting of the optional notation **ISQM** to a vessel or offshore unit.

ISQM is a risk-based software development and maintenance process built on internationally recognized standards. The ISQM process verifies the software installation on the facility and then monitors for consistency when there are software updates or a change in hardware. ISQM provides a process to manage software over the vessel's or offshore facility's life. The benefit to **the Owner and Driller or Crew Organization** is an increased level of confidence in software reliability with the goal of **increasing safety**, decreasing commissioning time, decreasing downtime, and reducing the risk of software related incidents.

As control systems for marine and offshore vessels or units become increasingly more complex and highly integrated, successful implementation relies heavily on the software developed by multiple vendors and the interfaces required for the integration of the software. The *ABS ISQM Guide* places emphasis on the verification of the integration of multiple software packages.

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

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

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

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

GUIDE FOR INTEGRATED SOFTWARE QUALITY MANAGEMENT (ISQM)

CONTENTS

SECTION 1	General	1
1	Scope and Application	1
3	Basis of Notation	1
3.1	Extent of Notation	2
5	Documentation	2
5.1	Required Plans and Documentation to Be Submitted	2
7	References	2
9	Abbreviations, Acronyms and Definitions	3
SECTION 2	Introduction	4
1	Background	4
1.1	Software Development Life Cycle (SDLC)	4
1.3	Support Processes	5
3	Stakeholder Roles and Responsibilities	5
3.1	Roles of Organizations	6
5	Use of Terms	8
5.1	Explanation of Software Module	8
5.3	Verification	9
7	ISQM Process	11
7.1	Project Management (PM) and Software Development Life Cycle (SDLC)	12
7.3	Concept Phase (C)	12
7.5	Requirements and Design Phase (RD)	13
7.7	Design Group and Production Software	13
7.9	Construction Phase (CON)	15
7.11	Verification, Validation and Transition (V V&T) Phase	15
7.13	Operation and Maintenance (O & M) Phase	16
FIGURE 1	Integrated Best Practices Approach	4
FIGURE 2	Organization Interaction: Owner, SBI, DCO, SI and Independent Auditor	5
FIGURE 3	Organization Interaction: System Integrator, Suppliers or Subcontractors and Independent Auditor	7
FIGURE 4	Example Relationship of Components, Functions and Software Module	8

FIGURE 5	Closed Loop Verification Example	9
FIGURE 6	Software-In-the-Loop Verification	10
FIGURE 7	Hardware-In-the-loop Verification	11
FIGURE 8	Integrated Software Quality Management Stage Gate Approach.....	11
FIGURE 9	SDLC Design Group or Concept and RD Phase Decision Tree	14
FIGURE 10	Software Flow and Reporting Flow during the V V&T Phase	15

SECTION 3 Software Development Life Cycle: Concept Phase..... 17

1	Scope	17
1.1	Concept Phase Activities.....	18
1.3	Concept Phase Organizations Activities.....	19
3	Example Concept Phase Process Flow for ISQM	19
3.1	Scope and Magnitude	20
3.3	Identify Functionality of Functions	20
3.5	Integrity Level Assignment	20
3.7	Write Concept of Operations Documents (ConOps).....	20
5	Risk Management.....	20
5.1	Safety Reviews and New Technology	20
5.3	Integrity Level (IL) Assessment	21
5.5	IL Assignment Functions Documentation Requirements	22
5.7	Software Quality Management	25
5.9	Obsolescence Plans.....	26
7	Concept of Operations Document (ConOps).....	26
7.1	General Topics	26
7.3	Definition of the Project Scope	27
7.5	Integrated System Major Components and Boundary	27
7.7	Constraints	27
9	Deliverables	28
11	Milestones.....	28
11.1	Concept Phase Complete, Milestone M2	28
11.3	Authorization from the Owner to Proceed to the RD Phase	28
TABLE 1	Integrity Level Table.....	22
TABLE 2	Recommended Safety and Environmental Overall Control System IL Assignments	24
FIGURE 1	General Flow of Work During the Concept Phase.....	19

SECTION 4 Software Development Life Cycle: Requirements and Design (RD) Phase..... 29

1	Scope and Objectives	29
1.1	General.....	29
1.3	RD Phase Activities.....	30

3	Example RD Phase Design Process Flow for ISQM	31
3.1	Criteria and Standards Selection	32
3.3	Models	32
3.5	Identify Coding Units and Test Plans	32
3.7	RD Documents	32
5	Requirements and Design Phase Documents	32
5.1	Software Requirements Specification (SRS)	32
5.3	Software Design Specification (SDS)	33
5.5	Risk Management	33
5.7	Document Approval	34
5.9	Function Requirements for ConOps with IL assignment	34
7	V & V Activities during the RD Phase	34
9	RD Phase Deliverables	34
11	RD Phase Complete, Milestone M3	34

FIGURE 1 General Flow of Work During the Requirements and Design Phase 32

SECTION 5 Software Development Life Cycle: Construction Phase 36

1	Scope and Objectives	36
1.1	Construction Phase Activities	36
3	Example Construction Phase Process Flow for ISQM	38
3.1	Requirements Translated and Coded	38
3.3	Components Tested	38
3.5	Integration Plans	38
3.7	Creating Construction Document	38
5	Construction Phase Document	39
5.1	General Topics	39
5.3	Risk Management	39
5.5	Document Approval	39
7	V&V Activities during the Construction Phase	39
7.1	V&V Reviews	40
9	Construction Phase Deliverables	40
11	Construction Phase Complete, Milestone M4	40

FIGURE 1 General Flow of Work During the Construction Phase 38

SECTION 6 Software Development Life Cycle: Verification, Validation and Transition (V V&T) Phase..... 41

1	Scope	41
1.1	Review of V&V Report	42
1.3	Scan for Viruses and other Malicious Software Prior to Verification Activities	42
1.5	V&V Review of the Simulation	43
3	Objective	43

5	V V&T Methods.....	43
5.1	Closed Loop Verification.....	43
5.3	Software-In-The-Loop Verification.....	44
5.5	Hardware-In-The-Loop Verification	44
7	Defect Ranking	44
7.1	Integrity Level and Defect Category	45
9	V&V Plan.....	46
9.1	V&V Plan Description	46
9.3	V&V Plan Approval.....	51
11	Verification and Validation Report (V&V Report)	51
11.1	V&V Report Reviews.....	52
13	System Integrator's Operation and Maintenance (O&M) Plan and Operating Manual	52
15	V V&T Phase, Verification Accepted, Milestone M5.....	52
17	Deliverables	52
19	V V&T Phase, Validation and Acceptance, Milestone M6.....	52
21	Transition	52
21.1	Operations and Maintenance Plan (O&M Plan).....	53
TABLE 1	Defect Categories	45
TABLE 2	IL Ranking and Defect Category, Requirements and Recommendations	46
FIGURE 1	Software and Reporting Flow during the V V&T Phase.....	42
FIGURE 2	IL0 Verification Process Diagram.....	47
FIGURE 3	IL1 Verification Process Diagram.....	48
FIGURE 4	IL2 Verification Process Diagram.....	49
FIGURE 5	IL3 Verification Process Diagram.....	50
FIGURE 6	V&V Organizations Independence from SI Organization by IL Assignment	51

SECTION 7	Software Development Life Cycle: Operation and Maintenance (O & M) Phase.....	54
1	Scope	54
1.1	Scan for Viruses and other Malicious Software	54
3	Review of the O&M Artifacts	54
3.1	Operation & Maintenance Plan (O&M Plan)	55
3.3	Owner's Management of Change (MOC) Policy.....	56
3.5	Software Registry	56
3.7	Control Equipment Registry.....	57
3.9	Software Change Control Process	57
3.11	Software Configuration Management Plan.....	57
5	Integrated Control System Maintenance	58
5.1	Scheduled Upgrades – New Functionality.....	58
5.3	Unscheduled Upgrades	59
7	System Retirement	60
9	O & M Phase, Milestone M7	60

TABLE 1	O&M Phase Artifacts.....	54
FIGURE 1	ISQM SDLC Phase	58
SECTION 8	Surveys After Construction and Maintenance of Class	61
1	General	61
3	Surveys for the Integrated Software Quality Management Notation.....	61
3.1	Survey Intervals and Maintenance Manuals/Records.....	61
3.3	Annual Surveys	61
3.5	Special Periodical Surveys	62
5	Modifications, Damage and Repairs.....	62
SECTION 9	Software Development Life Cycle: Design Group	63
1	Scope and Objectives	63
1.1	General.....	63
1.3	Requirements for Use of Functional Description Documents	64
1.5	Design Group Activities	64
3	Example Design Phase Process Flow for ISQM	64
3.1	Scope and Magnitude.....	65
3.3	Identify Existing Functions and New Functions	65
3.5	Owner Assigns the Integrity Level	65
3.7	Develop Models.....	66
3.9	Safety Reviews and Failure Mode, Effect and Criticality Analysis	66
3.11	Identify Coding Units and Test Plans.....	66
3.13	Proceed to Construction Phase	66
5	Risk Management.....	66
5.1	Integrity Level	66
5.3	Safety Reviews and FMECA	66
5.5	New or Unproven Technology	66
7	Functional Description Document (FDD)	67
7.1	Requirements of the ISQM System Integrator's FDD	67
7.3	Requirements of the ISQM SI's Control System Supplier's Section of the FDD	68
9	V & V activities during the Design Group.....	69
11	Deliverables	69
13	Milestones.....	69
13.1	Design Group Complete, Milestone M3.....	69
13.3	Authorization from the Owner to Proceed to the Construction Phase	69
FIGURE 1	General Flow of Work During the Design Group	65

APPENDIX 1 Activities and Requirements of Organizations 70

1	Concept Phase Activities	71
1.1	Concept Phase Owner's (OW) Activities	71
1.3	Concept Phase Driller or Crew's (DCO) Activities	72
1.5	Concept Phase System Integrator's (SI) Activities	73
1.7	Concept Phase Subcontractors' (CT) Activities	74
1.9	Concept Phase Verification & Validation (V&V) Activities	74
1.11	Concept Phase Independent Auditor's (IA) Activities	75
3	Requirements and Design (RD) Phase Activities	75
3.1	RD Phase Owner's (OW) Activities	75
3.3	RD Phase Driller or Crew's (DCO) Activities	75
3.5	RD Phase System Integrator's (SI) Activities	76
3.7	RD Phase Subcontractors' (CT) Activities	77
3.9	RD Phase Verification & Validation (V&V) Activities	77
3.11	RD Phase Independent Auditor's (IA) Activities	77
5	Construction (CON) Phase Activities	77
5.1	Construction Phase Owner's (OW) Activities	77
5.3	Construction Phase Driller or Crew's (DCO) Activities	78
5.5	Construction Phase System Integrator's (SI) Activities	78
5.7	Construction Phase Subcontractors' (CT) Activities	79
5.9	Construction Phase Verification & Validation (V&V) Activities	79
5.11	Construction Phase Independent Auditor's (IA) Activities	80
7	Verification, Validation and Transition (V V&T) Phase Activities	80
7.1	Verification & Validation Phase Owner's (OW) Activities	80
7.3	Verification & Validation Phase Driller or Crew's (DCO) Activities	81
7.5	Verification & Validation Phase System Integrator's (SI) Activities	81
7.7	Verification & Validation Phase Subcontractors' (CT) Activities	82
7.9	Verification & Validation Phase Verification & Validation (V&V) Activities	82
7.11	Verification & Validation Phase Independent Auditor's (IA) Activities	83
9	Operation and Maintenance (O & M) Phase Activities	84
9.1	Operation and Maintenance Phase Owner's (OW) Activities	84
9.3	Operation and Maintenance Phase Driller or Crew's (DCO) Activities	84
9.5	Operation and Maintenance Phase System Integrator's (SI) Activities	85
9.7	Operation and Maintenance Phase Subcontractors' (CT) Activities	85
9.9	Operation and Maintenance Phase Verification & Validation (V&V) Activities	85
9.11	Operation and Maintenance Phase Independent Auditor's (IA) Activities	85

APPENDIX 2 Definitions and Abbreviations 86

1	Definitions	86
3	Abbreviations	90

APPENDIX 3	Concept Phase	93
1	Example Concept of Operations Document	93
3	Example Obsolescence Management Plan Outline	96
5	ConOps Traceability	97
5.1	Example of Traceability Matrix.....	98
APPENDIX 4	Requirements and Design Phase.....	99
1	Software Requirements Specification	99
1.1	Example of Software Requirements Specification Table of Contents	100
3	Software Design Specification	101
3.1	Example of Software Design Specification Table of Contents	101
5	Models.....	102
5.1	Models	102
	FIGURE 1.....	103
	FIGURE 2.....	104
	FIGURE 3.....	105
	FIGURE 4.....	106
	FIGURE 5.....	107
	FIGURE 6.....	108
	FIGURE 7.....	108
APPENDIX 5	Construction Phase.....	109
1	Software Coding and Testing	109
1.1	Software Integration.....	110
1.3	Software SI Integration Testing	110
3	Management	111
3.1	Organization	111
3.3	Software Configuration Management Responsibilities.....	111
3.5	Software Configuration Management Plan Implementation.....	111
3.7	Applicable Policies, Directives, and Procedures	111
5	SCM Activities	112
5.1	Configuration Identification	112
5.3	Change Control.....	113
5.5	Configuration Status Accounting	114
5.7	Audits and Reviews	114
7	Tools, Techniques, and Methodologies	114
9	Supplier Control	114
11	Records Collection and Retention	115
APPENDIX 6	Verification, Validation and Transition Phase.....	116
1	Example V&V Plan Outline	116
3	Grouping of Software Modules	117

APPENDIX 7 Operation and Maintenance Phase..... 118

1	Recommended ISQM Maintenance Personnel's Activities	118
3	Example O&M Plan Table of Contents	119
3.1	Example of Maintenance Plan.....	119
3.3	Example of Operation and Maintenance Plan Outline	120
3.5	Control System Hardware, Firmware and Software Retirement Plan.....	122
5	Software Change Control Process	123
7	Example Software Control Form Process Flow	124
9	Example MOC Process.....	125
11	Obsolete Control System Components Considerations	127

FIGURE 1 Recommended Management of Change Process.....125

APPENDIX 8 Project Management 128

1	Scope	128
3	Background	128
5	PM Process Groups.....	129
5.1	PM Initiating Group.....	130
5.3	PM Planning Group	130
5.5	PM Executing Group	132
5.7	PM Monitoring and Control Group	132
5.9	PM Closing Group	133
7	Software Project Management Plan (SPMP).....	134
9	Introduction	134
9.1	Project Overview	134
9.3	Project Deliverables	134
9.5	Evolution of the SPMP	135
9.7	Reference Materials	135
9.9	Definitions and Acronyms.....	135
11	Project Organization	135
11.1	Process Model.....	135
11.3	Organizational Structure.....	135
11.5	Organizational Interfaces.....	135
11.7	Project Responsibilities	136
13	Managerial Process	136
13.1	Management Objectives and Priorities	136
13.3	Assumptions, Dependencies, and Constraints	137
13.5	Risk Management	137
13.7	Monitoring and Controlling Mechanisms	137
13.9	Staffing Approach.....	137
15	Technical Process.....	138
15.1	Methods, Tools, and Techniques	138
15.3	Software Documentation	138
15.5	User Documentation.....	138
15.7	Project Support Functions	138

17	Work Packages, Schedule, and Budget	139
17.1	Work Packages.....	139
17.3	Dependencies.....	139
17.5	Resource Requirements	139
17.7	Budget and Resource Allocation	139
17.9	Schedule.....	139
19	Additional Components.....	139
19.1	Index.....	139
19.3	Appendices.....	139
21	Software Quality Assurance Discussion	140
21.1	Software Process and Product Metrics.....	140
23	Metrics.....	141
TABLE 1	39 Project Processes	128
FIGURE 1	Project Management Process Groups Relationship to SDLC.....	129
APPENDIX 9 Design Group.....		142
1	Activities and Submittals for Design Group	142

SECTION 1 General

1 Scope and Application (1 September 2012)

This Guide presents the procedures and criteria to be employed by ABS in the review and survey of computer based control systems involving software development. The objective of the Guide is to reduce software related incidents that could negatively affect the performance of such systems. Compliance with the procedures and criteria given in this Guide may result in the granting of the optional notation **ISQM** to a vessel or offshore unit.

This Guide emphasizes the software aspect of control systems. Criteria for the hardware, Failure Mode and Effect Analysis (FMEA), and security of computer based control systems are given in other Rules, Guides and other standards issued by ABS. These other criteria are to be satisfied in addition to those given in this Guide.

The procedures and criteria given in this Guide rely on a structured process, based on best practices, for the engineering management of the software development process in the design, construction and maintenance of computer based systems. Compliance with the process and criteria of this Guide is intended to increase safety, accessibility, reliability, and ease of maintenance of computer based control systems.

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

The procedures and criteria given in this Guide will involve a variety of parties concerned with software development and maintenance. These include Systems Integrators (SI), Driller or Crew Organization (DCO), Ship Builder Integrator (SBI) or the Shipyard, Verification and Validation Organizations (V&V), Independent Auditor (IA), Owner, Suppliers, and Subcontractors involved in integrated system software development, implementation, operation and maintenance. It is the Ship Builder Integrator (Shipyard) and/or Owner's (refer to Section 2/3.1.1) responsibility to verify that the other involved parties are aware of the need to comply with this Guide.

3 Basis of Notation (1 September 2012)

The **ISQM** notation indicates compliance with the procedures and criteria given in this Guide for software development from the *concept* phase or *Design Group* to the end of the *Verification, Validation and Transition* Phase (Refer to Sections 2 to 6, and Section 9 for *Design Group*, herein); subsequently, leading to the beginning of operation of the affected system. Maintenance of the **ISQM** notation over the operational life of the system is subject to the periodic surveys carried out on board the vessel or unit in accordance with Section 8 of this Guide.

Integrated or non-integrated control systems affected by and classed with the **ISQM** (for integrated control system) and **SQM** (for non-integrated control system) notation will be listed in the ABS *Record* to describe the exact coverage of the notation. For example, the describer could be one or more of the following:

- Dynamic Positioning **Control** System
- Drilling **Control** System
- Vessel Management **Control** System
- Hydraulic Power Unit's **Control** System
- Power Management **Control** System
- etc.

3.1 Extent of Notation

When the **ISQM** notation is given to a control system, the connected control systems of the controlled **equipment and** functions are not included in the notation. However, the interface between the ISQM control system and other connected control systems are included in the Guide.

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

5 Documentation

5.1 Required Plans and Documentation to Be Submitted (1 September 2012)

In order to receive the **ISQM** notation, plans and documentation, as applicable, are to be submitted by the **responsible organization**.

For plans and data to be submitted for approval, refer to Appendix 1 of this Guide.

7 References

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

IEEE Std 12207-2008 Second edition, 2008-02-01, *Systems and Software Engineering – Software Life Cycle Processes*

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

IEEE Std 828™-2005, *IEEE Standard for Software Configuration Management Plans*

IEEE Std 829™-2008, *IEEE Standard for Software and System Test Documentation*

IEEE Std 830-1998, *IEEE Recommended Practice for Software Requirements Specifications*

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

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

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

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

IEEE Std 1490™-2003, *IEEE Guide Adoption of PMI Standard A Guide to the Project Management Body of Knowledge*

IEEE SWEBOK 2004, *Software Engineering Body of Knowledge*

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

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

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

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

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

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

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

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

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

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

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

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

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

ISO 9001:2008 *Quality Management Systems – Requirements*

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

Department of Defense and US Army: *Practicable Software & System Measurement A Foundation for Objective Project Management*

9 Abbreviations, Acronyms and Definitions

For abbreviations, acronyms, and definitions used throughout this Guide, refer to Appendix 2.

SECTION 2 Introduction

1 Background

This Guide prescribes the best practices for the engineering management of the software development process for the design, construction and maintenance of integrated computer-based control systems. This section presents an overview of the phases and management practices with a goal of successful development and deployment of the software. There are five Software Development Life Cycle (SDLC) phases, one overall project management and eight milestones or stage gates. The SDLC depicted in this Guide is the minimum acceptable process. Milestone requirements are to be met before leaving a phase. The milestones verify that open issues are being addressed in a systematic manner and the documentation from the functions are detailed sufficiently to convey meaning and intent. There are three topics of significance in the successful development and deployment of software, with some overlap. These topics are:

- i) The Software Development Life Cycle (SDLC)
- ii) Project Management Practices (refer to Appendix 8)
- iii) Support Processes

This Guide is focused on the SDLC.

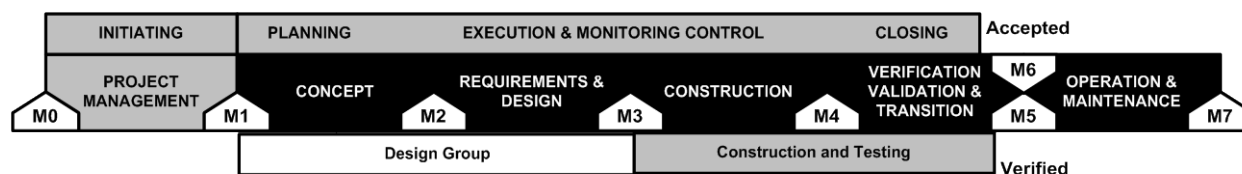
1.1 Software Development Life Cycle (SDLC) (1 September 2012)

The SDLC is the engineering plan for software development from concept to retirement of the computer-based control system.

This Guide follows industry standard practices, IEEE Std 12207-2008 Second edition, 2008-02-01, *Systems and Software Engineering — Software Life Cycle Processes* which is the basis of the SDLC denoted in black in Section 2, Figure 1. The Design Group allows for the use of “Production Software” (Section 9) where the System Integrator provides Functional Description Documents to replace the documents from the Concept and Requirements & Design Phases. The project management phases of IEEE Std 1490™-2003, *IEEE Guide Adoption of PMI Standard, A Guide to the Project Management Body of Knowledge* are denoted in grey. The SDLC below depicts five phases. Milestones (or stage gates) are often associated with distinct points within or at the boundaries of phases of an SDLC and are tied to the delivery of specific stage products.

A more detailed discussion of each phase of the SDLC is found in the individual phase sections in Sections 3 through 7 and Section 9. Project Management is discussed in Appendix 8.

FIGURE 1
Integrated Best Practices Approach (1 September 2012)



1.3 Support Processes

Support processes provide tools for the design, construction and maintenance of integrated control systems. These processes are implemented within the early stages of the SDLC and specific deliverables are defined. Support processes are especially critical to the Operations and Maintenance Phase of the lifecycle where a large portion of the re-configuration, new functionality and update effort is expended. The following support processes are necessary:

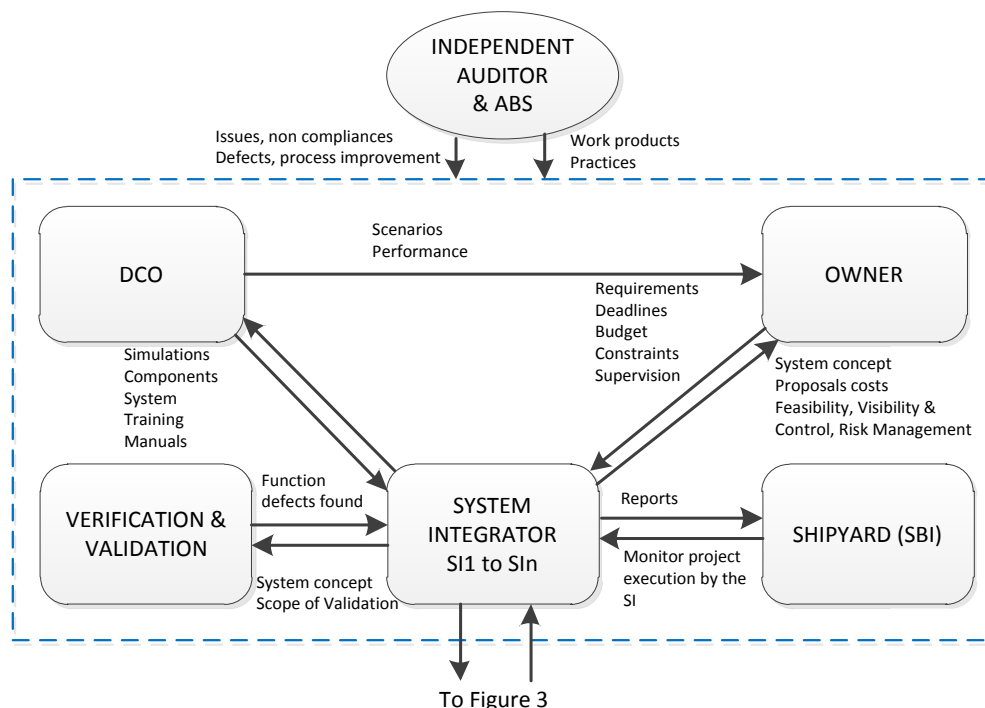
- i) Training
- ii) Management of Change
- iii) Configuration Management of hardware and software
- iv) Acceptance testing of all system changes
- v) Independent audit of change management
- vi) Metrics

3 Stakeholder Roles and Responsibilities

There are numerous roles required for the development and deployment of software systems. Terminology of a SDLC may vary from organization to organization, however the intent is the same. The SDLC process contains requirements, activities and deliverables. The SDLC requirements and activities are to be executed by various organizations. The requirements and activities for the organizations are listed in Appendix 1.

The organization interaction, flow of information and the timeliness of the information are factors in maintaining the project's schedule. Section 2, Figure 2 shows typical information flow between key stakeholder organizations.

FIGURE 2
Organization Interaction: Owner, SBI, DCO, SI and
Independent Auditor (1 September 2012)



3.1 Roles of Organizations (1 September 2012)

The stakeholder organizations are defined below. In some cases, the organization's responsibilities may be combined (i.e., The Owner could also be the **DCO and/or IA**; The Owner could be the **SBI (Builder or shipyard)** during initial construction; System Integrator (SI) could also be the Verification and Validation (V&V) organization). This Guide assumes the responsibilities and activities are performed by the organization assigned those activities. The activity assignments clarify the roles and deliverable per organization per phase.

3.1.1 Owner Organization (OW)

The Owner is the organization who provides funding and initiates the project. **The SBI is accountable (per contract) for the delivery of the contracted ISQM control system(s), as selected by the Owner, on the asset.**

3.1.2 System Integrator Organization (SI)

The System Integrator is responsible for the development of the integrated system. **Depending upon the selection of ISQM systems, there may be several System Integrator Organizations. The System Integrators are the experts of their respective control system and have integration awareness of connected equipment's control system requirements. The SI is responsible for the design of the integrated system, creation of the SRS & SDS (Section 4) or the FDD (Section 9), supplier management, integration and with the Owner's permission, verification of the control system software. The Owner may request input from the SI, as needed, for the development of the ConOps. The Owner may select the SI to perform the verification of the integrated system or the Owner may select an independent third party. The SI or SBI organizations are not to transfer responsibilities when delegating SI activities to a third party. If the project size does not warrant a SI, then these responsibilities are to be taken by Owner, DCO or a Supplier organization as selected by the Owner.**

- i) SI organization is to have a current ISO 9001 or be CMMI level 2 maturity level qualified or higher.
- ii) **Other software quality management systems may be specially considered by ABS. Please contact ABS.**

It is recommended that the System Integrator and the Shipyard make Suppliers aware of the verification requirements and activities.

3.1.3 Driller or Crew Organization (DCO)

The **Driller or Crew (DCO)** is the user of the integrated system and could also be the Duty Holder, drilling contractor or lessee. The **DCO** is responsible for the Operation and Maintenance Phase of the system. Maintenance responsibility facilitates continued reliable operation of the integrated system as improvements, upgrades and replacements or new components are added to the system over its lifetime.

3.1.4 Verification & Validation Organization (V&V)

The V&V organization is to verify the software as defined in the Software Requirement Specification (SRS) and integrated Software Design Specification (SDS) using Closed Loop (specially considered), Software-In-the-Loop, Hardware-In-the-Loop or a combination of the three methods. The V&V organization may be part of the System Integrator's organization or may be independent, as directed by the Owner, with limitation. Refer to Section 6, Figure 6.

3.1.5 Independent Auditor Organization (IA)

The **IA** organization monitors involved parties, including Suppliers for compliance with this Guide, produces reports for the Owner **and/or SBI, DCO & System Integrator**. The **IA** Organization is to be independent from the **SI's** software development team(s). The **IA** team is to coordinate with ABS, the Owner and the **SBI** on **IA** activities. The **IA** team may assist the Owner with validation of the system. During the Verification, Validation and Transition Phase (V V&T), the Concept Phase documents are reviewed by the Owner, **DCO** and **IA** Organizations to facilitate subsequent validation to the Owner's requirements. The Owner validates (accepts) the integrated control system.

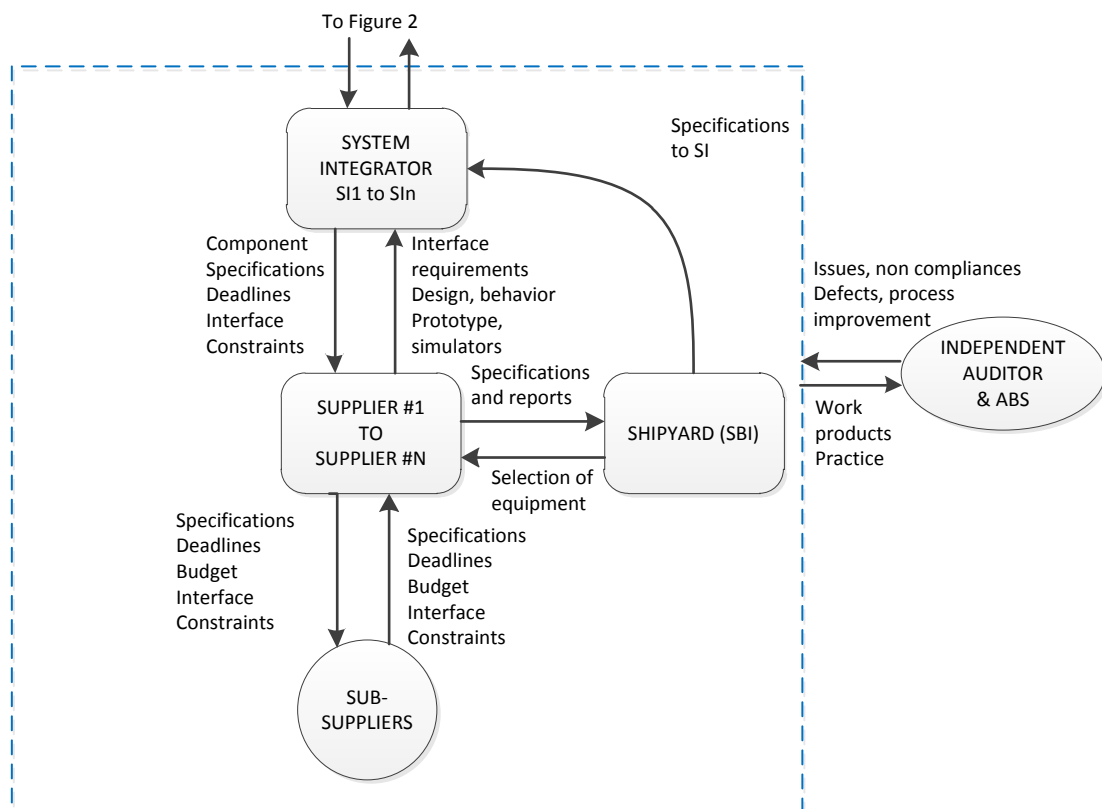
3.1.6 Ship Builder Integrator or Shipyard Organization (SBI)

The Ship Builder Integrator is the shipyard builder. The SBI is to contract with a System Integrator Organization or may use a division within the Shipyard Organization if the division meets the requirements listed for the SI Organization, refer to 2/3.1.2. The SBI has integration verification activities once the ISQM control system(s) is installed. The integration activities include verifying the communication (integration verification) between equipment connected to the ISQM control system(s). The SBI is accountable (per contract) for the delivery of the contracted ISQM control system(s), as selected by the Owner, on the asset.

3.1.7 ABS

ABS reviews documents during the development of the ISQM control system(s). ABS is to witness verification testing of control systems assigned a rating of IL2 or IL3. Refer to Section 6, Figure 6. ABS is to witness the integration verification performed by the SBI for new builds or the Owner.

FIGURE 3
Organization Interaction: System Integrator, Suppliers or Subcontractors and Independent Auditor (1 September 2012)



3.1.8 Supplier or Subcontractor Organization (CT)

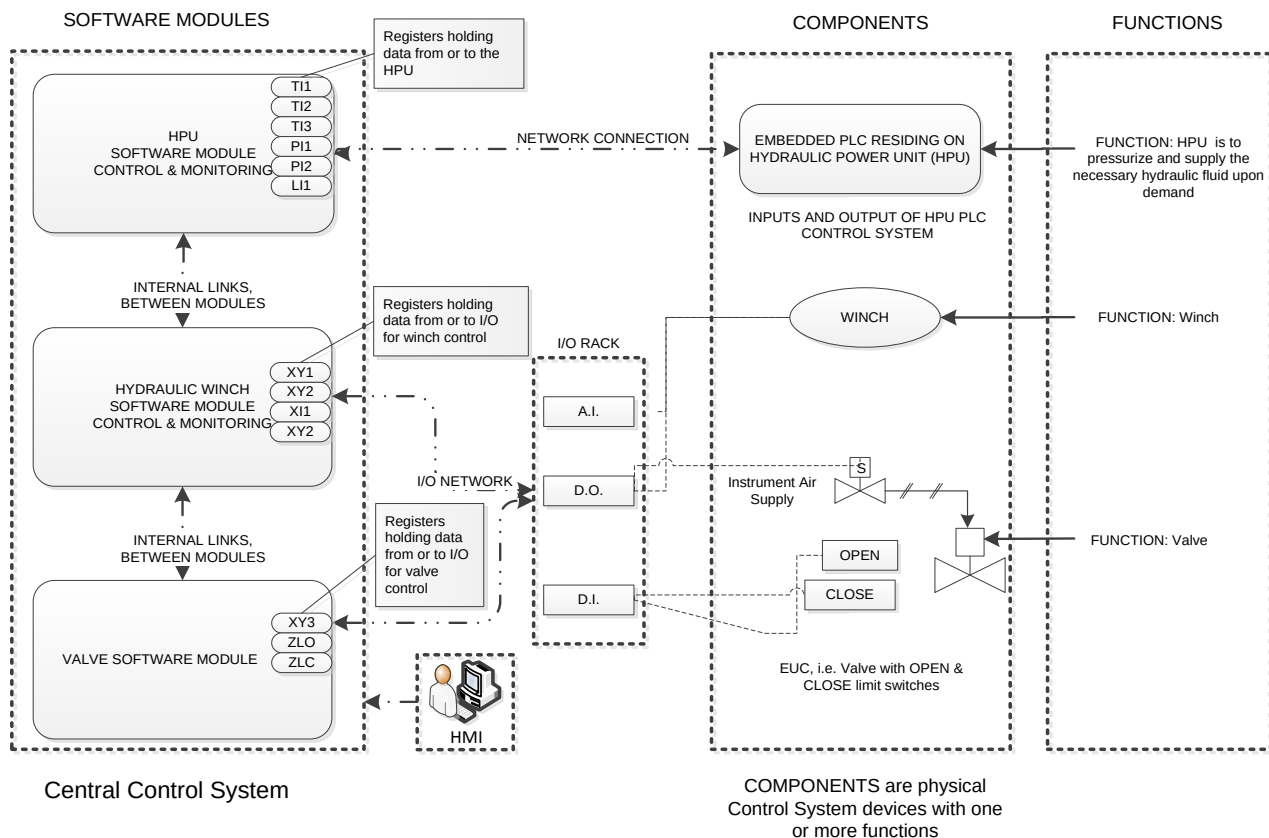
The Supplier is any contracted or subcontracted provider of integrated system components or software under the coordination of the System Integrator or Shipyard. The Supplier is to provide specifications and constraints of the control system's package(s) being supplied. The suppliers' verification is to be witnessed by ABS for IL2 and IL3 supplied equipment.

- CT organization is to have a current ISO 9001 or be CMMI level 2 maturity level qualified or higher.
- Other software quality management systems may be specially considered by ABS. Please contact ABS.

5 Use of Terms

Throughout this Guide terms are used with specific meaning. The relationships among function, Software Module and components are shown in Section 2, Figure 4.

FIGURE 4
Example Relationship of Components, Functions and Software Module



AI = Analog Input, DO = Discrete (Binary) Output, DI = Discrete (Binary) Input

5.1 Explanation of Software Module

5.1.1 Software Module

Grouping of software code which may contain other modules (code) to monitor, control and alarm. A valve's Software Module may contain:

- "Alarm" Software Module:** This software module monitors the time the valve takes to open or close and alarms if the valve did not confirm (through limit switches) that the valve is fully open or closed within the defined time. (If valve equipped with limit switches)
- "Interlock" Software Modules:** Sends a message to other affected functions to either remain in their current position or reverse as the alarm condition (state) of this valve changes.
- "Logic" Software Module:** If there are any interlocks on the opening or closing of the valve, these interlocks are programmed.
- "Diagnostic" Software Module:** The I/O may have diagnostics to monitor the "health" of inputs and outputs for failure.

5.1.2 Component or Package

A physical device, machine or instrument (i.e., HPU unit)

5.1.3 Function

What the Component is to do (e.g., Pressure transmitter has a function of transmitting the pressure signal. The HPU has a function of pressurizing the hydraulic fluid).

5.1.4 Human Machine Interface

Displays the status of the valve and may allow for control of the valve. An example is a graphical user interface.

5.3 Verification

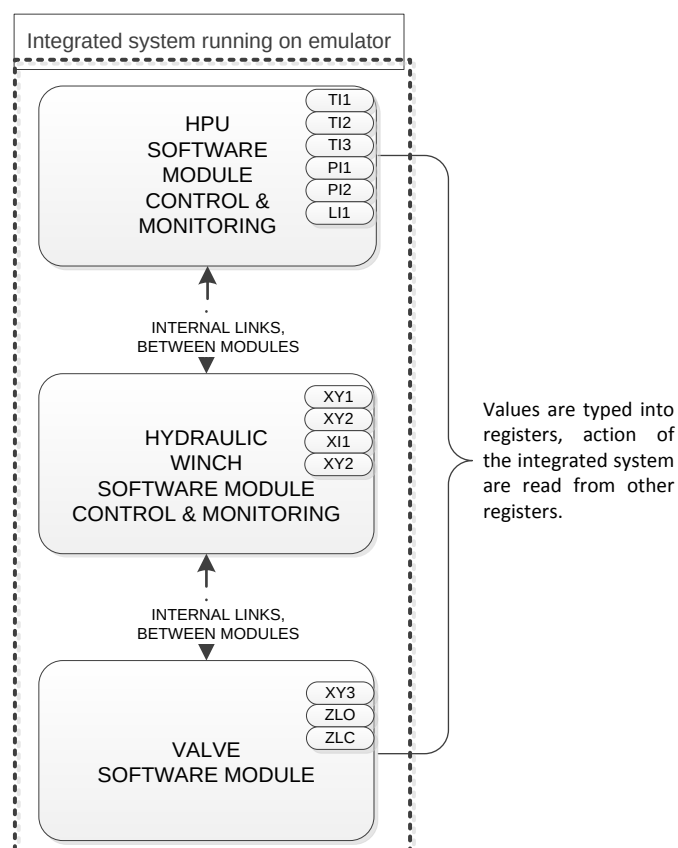
(1 September 2012). There are three verification methods to choose from that are acceptable to ABS.

- i) The simulation of the scenarios is to be of sufficient fidelity to verify the integrated system software to the specification. It is permissible to ABS to use a mix of methods to verify the software.
- ii) The primary verification method is to be selected by the Owner during the Concept Phase.
- iii) It is recommended that the SI state their preferred verification method for consideration by the Owner.

5.3.1 Closed Loop Verification (1 September 2012)

Closed Loop verification is acceptable with less complex control systems. In Closed Loop verification, detailed knowledge of the process and programming is necessary to verify correct actions of the software. The register data are interpreted to verify the integrated system's response is per the specifications (SRS and SDS or FDD). The use of Closed Loop Verification will be specially considered by ABS. Refer to Section 2, Figure 5.

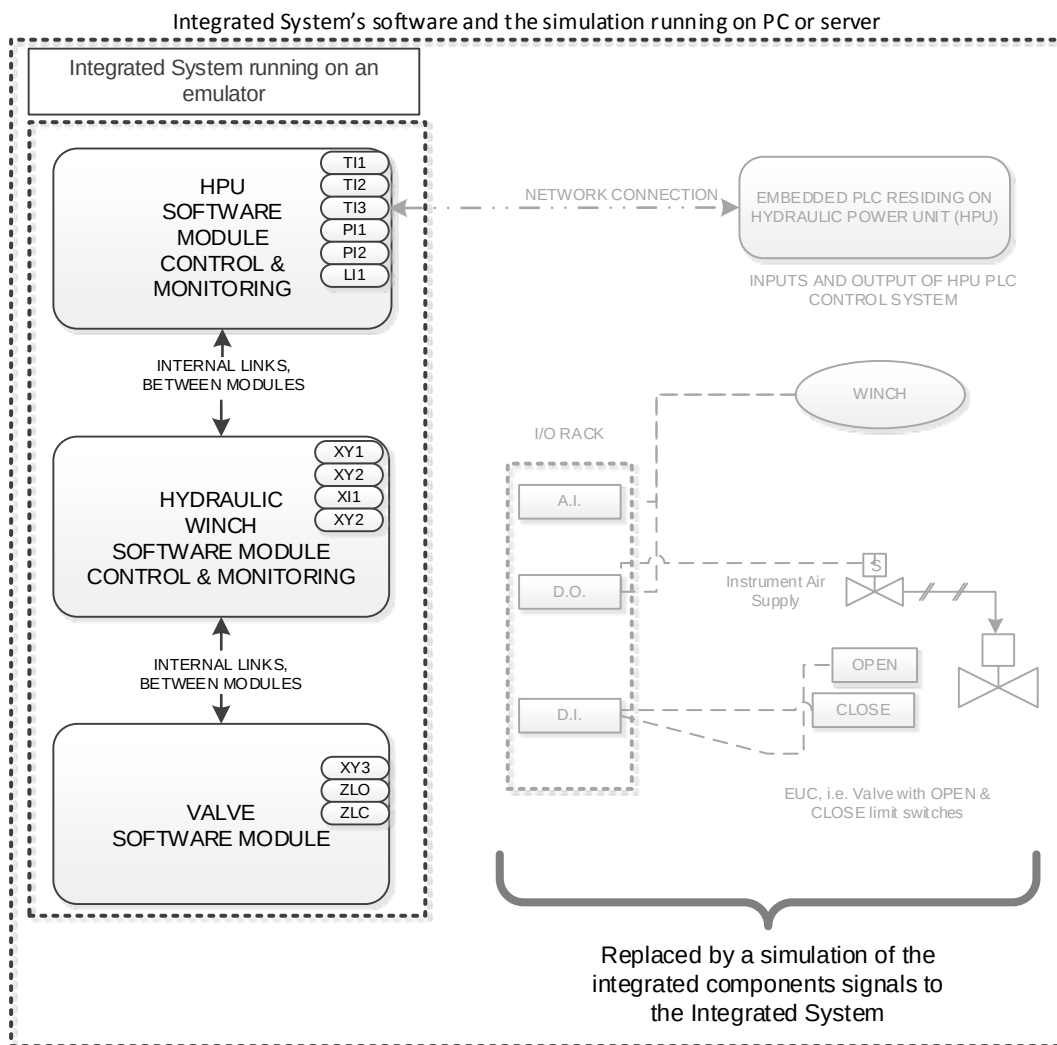
FIGURE 5
Closed Loop Verification Example



5.3.2 Software-In-the-Loop Verification

In Software-In-the-Loop verification, the integrated system program is running (executing) on a non-native computer. Within this computer, a simulation has been programmed to emulate components of the integrated system. The Software-In-the-Loop verification does not verify the networked connections, input or output hardware modules, or the processor. The program is run on an emulator on a PC, server or other computing device. Software-In-the-Loop verification does allow for a number of scenarios to be run to test the integrated system's code. The real world is represented by mathematical models in the simulation program. Refer to Section 2, Figure 6.

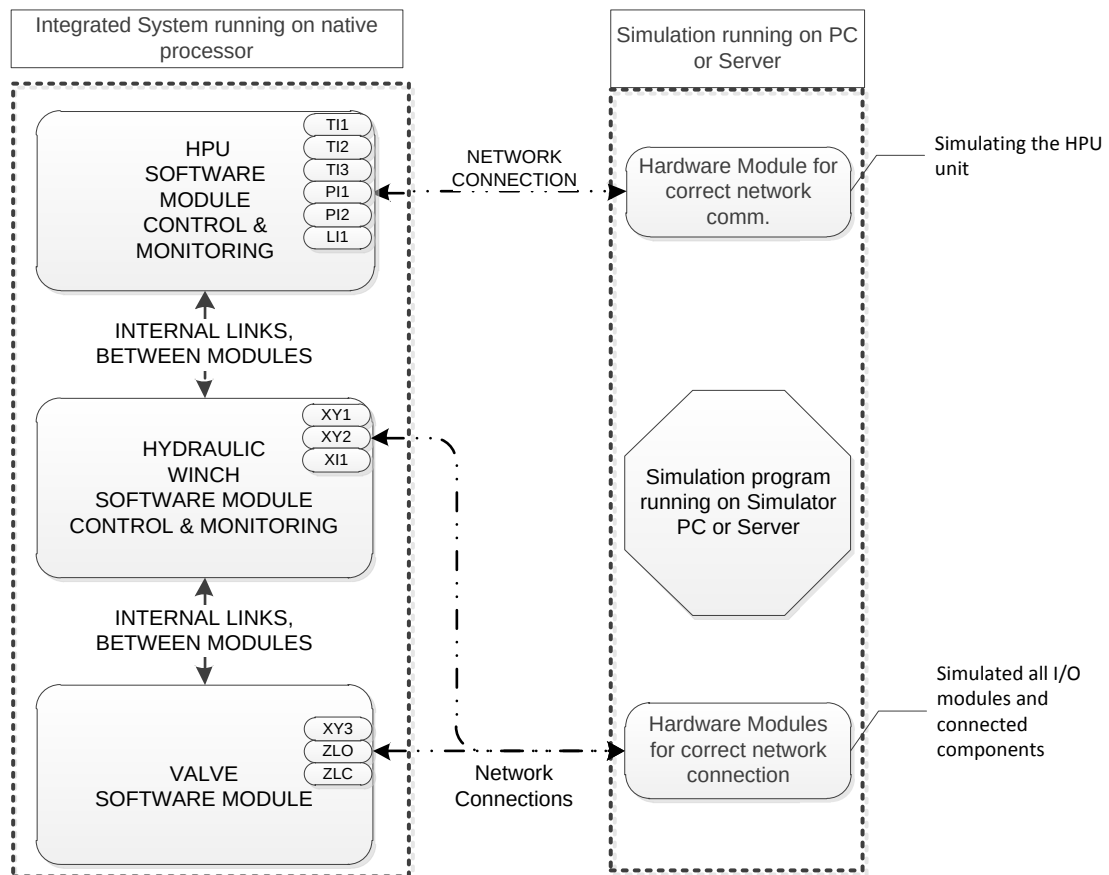
FIGURE 6
Software-In-the-Loop Verification



5.3.3 Hardware-In-the-Loop Verification

The integrated system's program is being executed on its native hardware (native processor, firmware) and the simulation is being executed on a separate machine. Interfaces between the two are developed for the testing. Hardware-In-the-Loop verification does allow for a number of scenarios to be run to test the integrated system's code. The real world is represented by mathematical models in the simulation program. Refer to Section 2, Figure 7.

FIGURE 7
Hardware-In-the-loop Verification

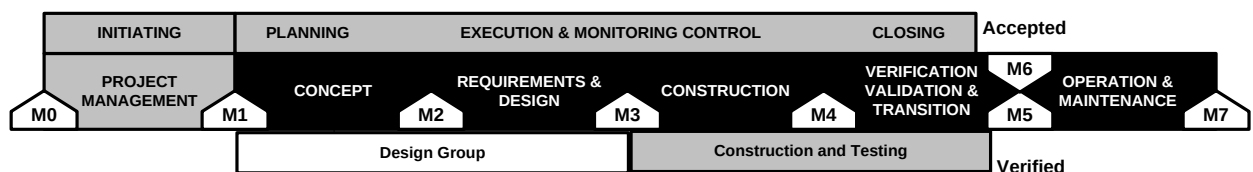


7 ISQM Process

(1 September 2012) Each of the four development phases and the *Design Group* plus the Operation and Maintenance phase are briefly described below. With reference to Section 2, Figure 8, individual paragraphs below will describe each of the topics listed in the figure. More detailed descriptions of milestones, deliverables, work flows, and activities are included in Sections 3 through 7 and Section 9 of this Guide. Project Management processes are described in Appendix 8.

Refer to Appendix 1 which contains a listing of activities and requirements for each organization by phase.

FIGURE 8
Integrated Software Quality Management Stage Gate Approach (1 September 2012)



7.1 Project Management (PM) and Software Development Life Cycle (SDLC)

7.1.1 Project Management (PM)

Project Management is discussed in Appendix 8. The Project Management (PM) processes are not bound by SDLC phases and milestones, as activities extend beyond SDLC phases. The Project Management Institute has developed a set of project management processes. The basic process groups are:

- i) Initiation
- ii) Planning
- iii) Execution
- iv) Monitoring and Controlling
- v) Closing

7.1.2 PM Initiating Group

In the Initiating group, the primary objective is the authorization of the project.

7.1.3 PM Planning Group (1 September 2012)

In the PM Planning group, the primary purpose is planning the work that needs to be done. **It is recommended to include:** development of initial schedules, resource plans, scope definition, activity duration estimates, etc. Planning is one of the processes that continue through the life cycle of the project from concept to deployment. There is operation & maintenance planning after the system is deployed.

7.1.4 PM Executing Group

In the PM Executing group, the primary purpose is to get the work done. This includes executing the plan, source selection, contractor management, and team development. The executing group also carries through the lifecycle as activities in each phase are accomplished. The executing group interacts with other PM groups.

7.1.5 PM Monitoring and Control Group

In the Monitoring and Control group, the primary purpose is to measure and assess the work being done. To support variance from the plan, change and schedule control is to be implemented and monitored. Scope management, resource analysis and other indicators that assist in gauging the health of a project are implemented.

7.1.6 PM Closing Group (1 September 2012)

In the Closing group, the primary purpose is to close the project. This includes administrative closure, final data gathering and delivery of maintenance manuals, drawing, etc., to the Owner and Driller or Crew (DCO).

7.3 Concept Phase (C) (1 September 2012)

The Concept Phase (Section 3) provides the direction and scope of the project. The goal of the Concept Phase is to define the integrated system in sufficient detail to allow for safety review(s), Integrity Level (IL) assessments, and **initial** integrated system component selection. The IL number is assigned based upon the risk and consequence of a failure of the function. Refer to Section 3, Table 1. Integrated system component identification is first done by determining which functions are allocated to software and which functions are non-computer based system controlled.

After the functions are defined, the Owner is to review consequences of failure of the function and assign an Integrity Level with input from other organizations. Refer to Section 3, Tables 1 and 2.

The Owner is to specify the primary verification method. There are three options for verification of the integrated system software as mentioned in 2/5.3. In the V V&T Phase, the software for the system is minimally determined to operate as specified in the SRS and SDS or FDD (verification).

It is recommended that the complexity of **the functions**, the functions' Integrity Level **numbers** and the quantity of Suppliers' packages that are to be integrated be considered when selecting the primary verification method. The simulation software development is performed in parallel with the integrated system software development and not at the conclusion of the software development.

The main deliverable for this phase is the Concept of Operations document (ConOps). Overall architecture of the system depicting the interoperability of the software is developed. **It is recommended that** an analysis of the computer-based control system hardware requirements is included so that the system and software requirements are separately identified within the ConOps. The ConOps is used to develop the integrated Software Requirement Specification (SRS) and the integrated Software Design Specification (SDS) in the Requirement and Design Phase. The SRS and SDS are used for verification while ConOps is a portion of the validation process of the computer-based control system. An example of a ConOps is included in Appendix 3. Functions listed in the ConOps are traceable and have been assigned an IL number. The IL number provides for visibility of the important functions and verification scenarios are influenced by the assigned IL number. **It may be acceptable for the Owner to request the SI to provide a Functional Design Document (FDD), See Section 2, Figure 9 and Section 9.**

Concept errors in the ConOps may have **project** schedule implications if the errors are discovered late in the **SDLC** process.

7.5 Requirements and Design Phase (RD) *(1 September 2012)*

During the Requirements and Design Phase **(Section 4)**, the requirements and detailed specifications of the integrated software functions are developed, modeled, and documented from the ConOps. The goal of the RD Phase is to translate the functions (in light of the system architecture) defined in the ConOps into documents that the System Integrator's developers and programmers can use to construct the software to provide the functions described in the ConOps. Functions are traceable back to the ConOps **using some function identifier**.

The deliverables from this phase are the integrated Software Requirements Specifications (SRS) and integrated Software Design Specification (SDS), the technical basis of the software developed in the Construction Phase.

The SRS contains the traceable technical details of each function from the ConOps. Verification requirements as specified in the ConOps are added and detailed for the functions.

The SDS contains the traceable design details of each function, communication node and system architecture components being integrated.

Performance, safety, database and security requirements, adherence to standards, ergonomic consideration, and capabilities are to be specified in detail in the RD Phase documents. Integration testing for all commercial off-the-shelf (COTS) packages is written as a V&V requirement. The COTS V&V Plan may be developed by the Supplier.

The RD Phase documents details all Owner and/or **DCO** requirements and the documents are reviewed by the Owner, **IA, SBI, and DCO** for ConOps compliance. It is recommended that the SRS and SDS clearly indicate to the expected functionality and action of the computer-based control system when there are failures.

7.7 Design Group and Production Software *(1 September 2012)*

The Design Group (Section 9) is the combination of two SDLC phases, Concept and the Requirements & Design Phases.

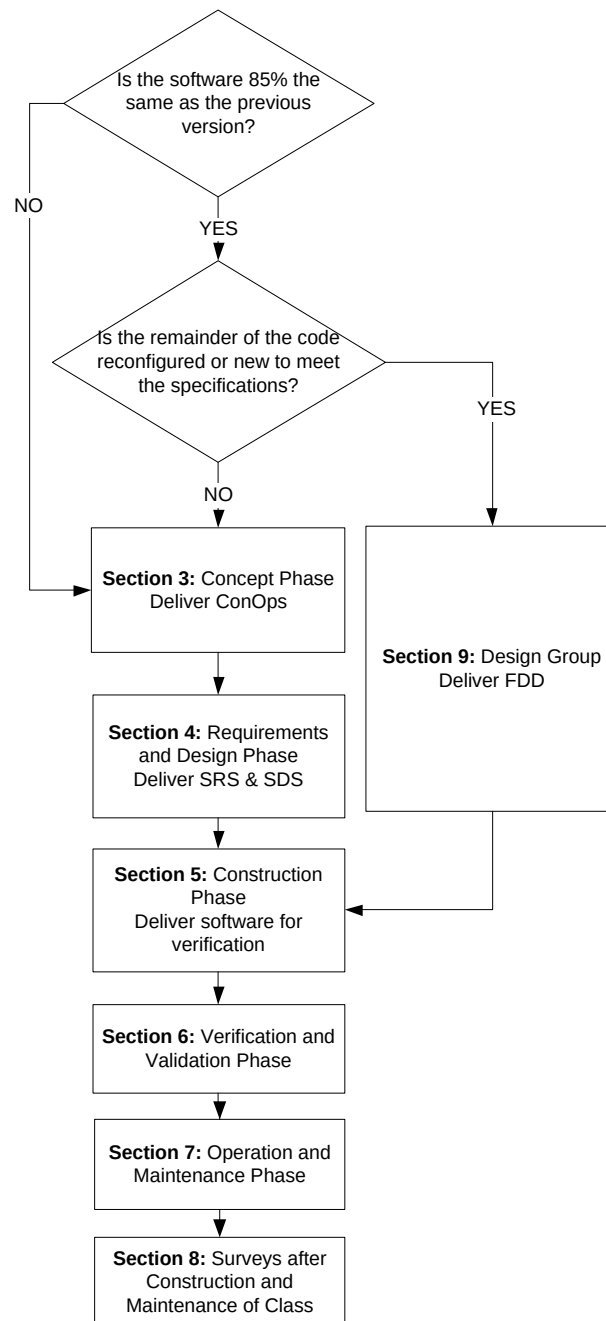
Control systems of equipment may be installed on existing offshore and marine assets, where a relatively small percentage of the code is unique or different from the installed systems, to meet the requirements of the specification. When a majority of the control system software modules or code utilizing established functions and code modules with the remainder being new or modified code to meet the specification.

Since the software is already in use within industry, the submittal documents are reduced. The ConOps and the SRS & SDS are combined into the Functional Description Documents (FDD) and some of the software requirement analysis is reduced. The FDD may be a combination of documents and drawings meeting the requirements from Section 9.

The FDD consists of information and details contained within the ConOps and SRS & SDS. Using the Design Group to develop the FDD does not lessen the verification activities or requirements that occur in the V V&T Phase.

Using the FDD, the Owner, assigns the Integrity Level to the functions. The Owner, SBI, DCO and IA adds normal, degraded or failed control system condition testing scenarios for the verification from their experience or prior knowledge. If the control system functions have been assigned an Integrity Level 2 or 3 (IL2 or IL3), then the System Integrator facilitates and performs a software-focused, top down, functional Failure Mode and Effect Criticality Analysis (FMECA). See Section 2, Figure 9 for the paths to follow with Design Group or the Concept and RD Phases.

FIGURE 9
SDLC Design Group or Concept and RD Phase Decision Tree (1 September 2012)



7.9 Construction Phase (CON) (1 September 2012)

The activities that occur during the Construction Phase (Section 5) are centered on translating the requirements and specifications from the SRS and SDS or FDD into functioning integrated system code. It is recommended that the SI tests the code for compliance with the SRS and SDS or FDD internally. It is also recommended that the SI testing not be limited to basic levels of compiling or individual Software Module testing, extend towards comprehensive internal module and module-to-module testing by the SI.

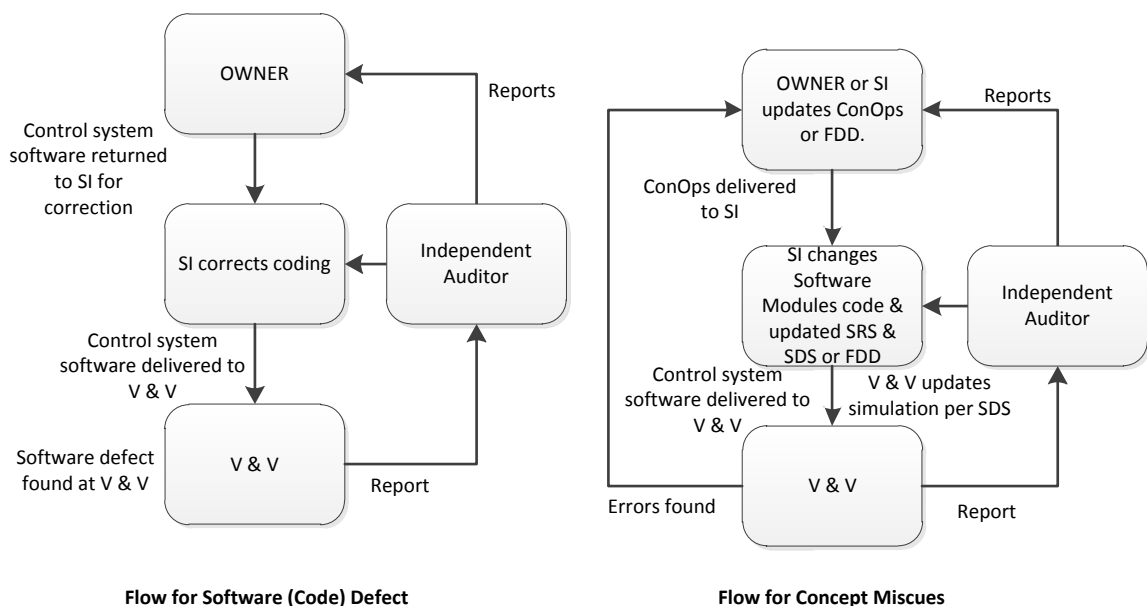
If any COTS software is part of the system, integration testing is to be performed by the SI to facilitate the verification testing. Testing activities in this phase focus on the software aspects of the system by the SI and suppliers. Verification and demonstration of the software performance and possibly the integration verification occurs in Verification, Validation and Transition Phase. Further integration testing occurs during commissioning of the integrated control systems.

7.11 Verification, Validation and Transition (V V&T) Phase (1 September 2012)

In the Concept Phase, the Owner has specified which of the three verification methods is to be used as the primary verification method. In the V V&T Phase (Section 6), the software for the system is determined to operate as specified in the SRS and SDS or FDD. The SRS and SDS or FDD is the governing document(s) for verification. The ConOps or the FDD is a document used for validation as well as for the commissioning and sea trial(s) activities. The V&V organization is to write a plan for verification (V&V Plan) based on the primary method chosen in the Concept Phase and configures the simulator. An example V&V Plan is provided in Appendix 6. The Independent Auditor and ABS are to witness the verification is in accordance with the V&V Plan for selected systems. Any software defects, concept errors or other deficiencies, compared to the SRS, SDS and ConOps or FDD, are to be documented and reported. The SI with input from the V&V, Owner or IA Organizations determines if the deficiency is a control system code defect, simulation code defect or a concept error. Concept errors affect validation and the ConOps and the FDD. The software is returned to the SI group for corrective action.

FIGURE 10

Software Flow and Reporting Flow during the V V&T Phase (1 September 2012)



Before the V&V organization can complete verification of the integrated system, the complete V&V Plan is to be performed. The V&V Plan is to verify the integrated software without;

- i) Detecting any Critical or Major Defects (Refer to Section 6, Table 1 for software defect ranking table)
- ii) Detecting any IL2 or IL3 defects or other defects that systemically affect IL2 or IL3 level functions.

Regression testing is used to test the “corrected” software for new defects that may have been introduced during the coding to correct a previously known or detected defect. Regression testing is to include complete testing of all inputs to and outputs from the changed software module that interfaces with any IL2 or IL3 components.

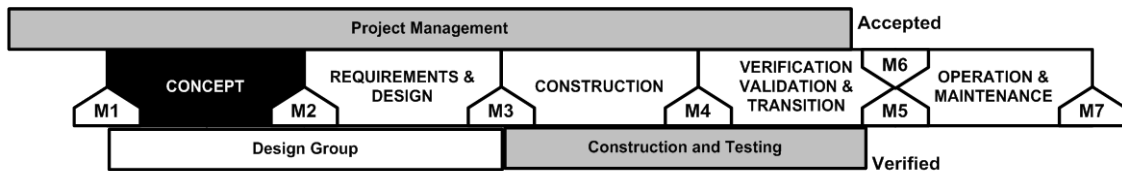
After verification of the completed software, all activities necessary to transition the integrated system to the Owner and DCO are accomplished. The software is installed on the target hardware and support services arranged, as selected by the Owner. The SI submits all documentation to the Owner and DCO.

7.13 Operation and Maintenance (O & M) Phase (1 September 2012)

This phase covers the operation and maintenance activities, including scheduled and unscheduled upgrades and problem resolution activities (Section 7). This phase also extends to retirement activities. The responsibilities for activities in this phase lie with the DCO with activities by Suppliers. The SI is to provide the Operation and Maintenance Plan towards the end of verification activities. Refer to Appendix 7 for an example Operation and Maintenance Plan template.

Most software requires maintenance such as adding functionality, correcting latent software defects, etc., over time.

SECTION 3 Software Development Life Cycle: Concept Phase



1 Scope

(1 September 2012) At the beginning of an ISQM software project, there are two paths for developing the software detailed description, see Section 2, Figure 9. The paths are:

- Design Group (Section 9) delivering Functional Description Documents (FDD).
- Concept Phase (Section 3) delivering a Concept of Operation Document (ConOps) followed by Requirements and Design Phase (Section 4) delivering the SRS and SDS documents.

If the control system functions (code) meet the following requirements, then proceeding using the Design Group and producing the FDD is acceptable to ABS:

- The control system software to be provided to control or monitor the equipment, control system or integrated system is to be comprised of approximately 85% or more utilizing established functions and code modules or code with the remainder being configuration modifications and/or new code to meet the requirements or specifications.

And

- The control system software is to be currently in use within the industry.
 - Multiple updates or modifications that have been made to the control system software over time does not preclude the use of this section and is acceptable to ABS.

Or

- Special consideration from ABS is granted.

If the control system software meets the above requirements, see Section 9.

Below are the requirements and recommendations for the Concept Phase with the major deliverable being the ConOps.

The goal of the Concept Phase is to define the integrated system with sufficient detail to facilitate safety review(s), Integrity Level assessments, and identify selected components of the integrated system. The objective of the Concept Phase is to complete a Concept of Operations document (ConOps) which contains the needed architecture, standards, descriptions and requirements that are used by the System Integrator (SI) to begin the Requirements and Design (RD) Phase. Refer to Appendix 1 for activities and requirements for this phase. The Owner may request input from the SI or SBI, as needed, for the development of the ConOps.

The goal of the Concept Phase is to define the integrated system within the ConOps in sufficient detail to:

- i) Identify functions and provide traceability of the functions for use in the SDLC.
- ii) Incorporate recommendations from safety reviews, if applicable, to the functions description and ConOps.
- iii) Assign Integrity Levels to the functions.
- iv) Identify integrated system components.
- v) Define alarm management philosophy.

It is recommended that functions, activities and deliverables in the latter phases of the SDLC be traceable to the ConOps. Descriptions of the functions and the interfaces definition are a significant portion of the ConOps along with Suppliers' packages data.

During this phase the Integrity Levels (IL) are assigned to the functions and carry this IL assignment to the Software Modules, refer to Subsection 3/5. Components of the integrated system, Human Machine Interfaces (HMI) and integrated system's suppliers connected packages are identified.

1.1 Concept Phase Activities (1 September 2012)

Verification scenarios for the ISQM integrated system are to be defined in the ConOps to the extent the scenarios are known.

Derived with reference to IEEE 12207-1-2008 Second edition, 2008-02-01, IEEE *Systems and Software Engineering – Software life cycle processes*, these activities correspond to the scope and objectives of the Concept phase are:

1.1.1 Concept Phase Development

The SI's, Owner's or SBI software development processes are to be mapped to the ISQM Guide's SDLC process.

Design tradeoffs, identification and resolutions of (integrated system to suppliers) conflicts are documented. Many decisions made to resolve conflicts will impact the RD Phase. Incorporated standards used, safety, security and human factors are documented. It is recommended that the documents that result from the analysis of the above factors are to be put under configuration management.

A canonical integration model provides the common basis for communication among the associated packages in the integrated system. A canonical integration model benefits the involved parties in identifying integration issues and determining solutions.

- i) It is recommended that the SI define a canonical integration model to be used throughout the project and provide the canonical integration model to all stakeholders and Suppliers at the beginning of the Concept Phase.

1.1.2 Systems Requirements Analysis

It is recommended that SI perform the systems requirements analysis. The system requirements analysis is an activity for the development of the ConOps. The system requirements analysis focuses on the determination of integration system requirements and the associated tradeoffs.

- a) These specifications describe:
 - i) Functional requirements, capabilities of the overall system;
 - ii) Accessibility
 - iii) Reliability
 - iv) Maintenance
 - v) Safety

- b) Additional considerations for Accessibility, Reliability, Maintenance and Safety (ARMS or RAMS) are:
 - i) Security
 - ii) Human-factors engineering interface requirements
 - iii) Design constraints
 - iv) Qualification requirements
- c) System integration requirements are evaluated using:
 - i) Traceability
 - ii) Consistency
 - iii) Testability
 - iv) Feasibility of operations and maintenance (ARMS)

1.1.3 System Integration Architectural Design

The system integration architectural design is an activity for the development of the ConOps. The system integration architectural design activity results in the creation of the top-level architecture of the system. This architecture identifies and facilitates grouping. The **recommended** groups are:

- i) Hardware
- ii) Software
- iii) Manual operation items

It is **recommended that** all software requirements are to be shown on a traceability matrix.

1.1.3(a) System Integration Architecture Evaluation Criteria. The recommended system integration architecture evaluation criteria are:

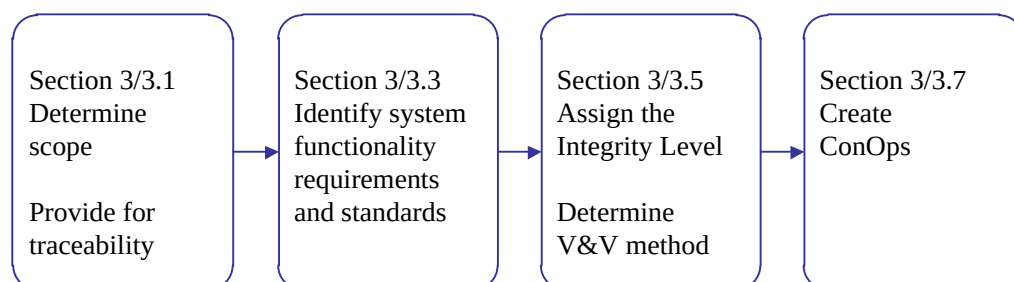
- i) Traceability
- ii) Consistency
- iii) Appropriateness
- iv) Feasibility

1.3 Concept Phase Organizations Activities

Each organization has assigned activities to facilitate successful completion of this phase. The Concept Phase activities for all organizations are listed in Appendix 1.

3 Example Concept Phase Process Flow for ISQM

FIGURE 1
General Flow of Work During the Concept Phase (1 September 2012)



Section 3, Figure 1's section references are below.

3.1 Scope and Magnitude (1 September 2012)

The limitations and boundaries of the integrated system are defined to include any interfaces with hardware and infrastructure components. Traceability is introduced in the software development process via function identification.

- i) Issues related to functions are to be identified and traceable through all SDLC phases and safety reviews.
- ii) The Owner, with input from the DCO is to state the purpose and scope of the integrated system in the ConOps.

3.3 Identify Functionality of Functions

Each computer-based controlled or monitored package, unit or device is to be identified with a method to allow for tracking of the function. Determine the standards to be used for this project and document the standards to be used.

3.5 Integrity Level Assignment

Refer to Subsection 3/5, "Risk Management", for Integrity Level (IL) assignments. An Integrity Level number is assigned to every function assigned to the ISQM control system. The IL assignment provides for enhanced visibility based on the criticality of the function and may add additional verification scenarios.

3.7 Write Concept of Operations Documents (ConOps)

Refer to Appendix 3 for an example ConOps Table of Contents.

5 Risk Management (1 September 2012)

A safety review is to be performed on the defined functions to facilitate identification of important functions such as essential, and safety functions. The techniques used in ANSI/ISA-84 and IEC61508 process may be used for the assessment of Integrity Level (IL), if desired. The safety review may be combined with other safety or operability reviews, hardware FMEA, or software FMECA.

5.1 Safety Reviews and New Technology

5.1.1 SIS Safety Systems

SIS Safety systems, integrated or not, are to follow ANSI/ISA-84 or IEC61508 for assessment of the Safety Integrity Level (SIL).

- i) When ANSI/ISA-84 or IEC61508 are used for safety systems, the IL assessment does not apply to the SIS functions.
- ii) The ISQM Guide does not specify a process for the assignment of the SIL (as per IEC61508 or ANSI/ISA-84) or IL (per ISQM) numbers. The Owner is to choose a logical and recognized process or standard to assign the IL numbers.

5.1.2 Safety Review

Safety review(s) are to be performed on the integrated system and associated packages, units and connected instrumentation.

It is recommended that SI, Owner, DCO, IA, SBI and ABS be present during the safety reviews.

5.1.3 ConOps Reviews

- i) SI, IA and the DCO are to review the ConOps. Review comments and accepted recommendations are to be documented. If the SI developed the ConOps then the Owner, IA and DCO are to review the ConOps. Review period as per contract or other agreement with the contracting party.
- ii) Comments of the review(s) are to be submitted to ABS.

5.1.4 New or Unproven Technology

New or unproven technology carries additional risk. Refer to the *ABS Guidance Notes on Novel Concepts* and the *ABS Guidance Notes on Risk Assessment Applications for the Marine and Offshore Oil and Gas Industries* for additional information. The new or novel technologies may be hardware, mechanical equipment, interface protocol or the Software Module coding.

- i) New or novel essential systems or essential functions are to be assigned a minimum Integrity Level of IL2.
- ii) New or novel SIS functions are to be assigned the minimum Integrity Level of IL3.
- iii) New or novel non-essential systems and non SIS functions are to be assigned a minimum Integrity Level of IL1.

5.3 Integrity Level (IL) Assessment

The Integrity Level (IL) is assessed by evaluating the consequences of a failure of the function. The Integrity Level represents how important a function is to the operation of the system. The IL number represents the degree of confidence the Owner and/or DCO desires for the function to operate as specified including fail safe state(s). IL numbers are assigned by Owner, with input from the DCO and SI, being attentive to the requirements of national and international authorities and classification societies.

The Integrity Level derives from the desired confidence of performance and severity of failure consequence. The IL assessment is based upon:

- i) Safety consequences
- ii) Environmental consequences
- iii) Business impact (optional)

5.3.1

Functions are to be rated in Safety and Environmental categories. Business impact is optional.

- Business impact is optional and will not be reviewed by ABS.

Potential safety and environmental consequences are to be considered when assessing functions for IL assignment. Integrity Level assignment may be increased due to company's risk tolerance and for potential business impact.

5.3.2

There are four Integrity Levels (IL). Each carries increasingly more severe consequences from IL0, which is considered as having little to no impact on safety, environment or business outcomes, to IL3 which could have significant or severe consequences affecting safety, the environment or business issues. The ISQM control system carries the number of the highest IL rated software function. A control system with IL0 to IL2 functions and a single IL3 software function is assigned an overall rating of IL3. It is not recommended to assign IL3 rating to all functions within the ISQM control system unless the risk analysis indicates this rating for the other functions.

5.3.3

Essential systems and functions:

- i) Essential systems and functions are assigned IL2 or IL3. Essential systems may be assigned an IL1 rating with justification, redundancy, etc., provided to ABS for special consideration.
- ii) SIS systems are to be IL3, as SIS is defined by IEC61508 or ANSI/ISA 84, IMO and optional assignment by Owner to non-SIS functions or systems. SIS systems may be assigned an IL2 with justification, redundancy, etc., provided to ABS for special consideration.
- iii) Refer to 4-9-3/7.1 of the *Steel Vessel Rules* for additional guidance.
- iv) ESD systems utilizing software functions are to be IL3. ESD systems maybe assigned an IL2 with justification, redundancy, etc. provided to ABS for special consideration.

An implementation of the IL assignment in the Concept Phase allows for scrutiny of the individual functions and the system as a whole. The goal is to provide a more reliable and stable integrated system. The risks include schedule, obsolescence of hardware and/or software and reliability (quality) of the software development. The IL assignment conveys to the Software module (code) of the function.

5.3.4

The overall IL number of the integrated system is to equal the highest IL number assigned to any of the functions controlled by the ISQM control system.

TABLE 1
Integrity Level Table (1 September 2012)

IL	Potential Consequences			Examples, not inclusive
	Safety	Environmental	Business	
0	Negligible	Negligible	Minor impact on operation. Might affect supporting process system but not main process system.	Entertainment System, Administrative computer systems, office network, Data Collection system (non-Authority required)
1	Might eventually lead to marginal safety incident	Might eventually lead to a marginal environmental incident	Might lead to maintenance shutdown of non-critical system. Main process continues to operate.	Non-essential control of systems, BPCS, Non-essential communication systems, Vessel Management System. New or unproven non-essential technologies minimum rating.
2	Within a short time could cause critical injury, lost time, accident or loss of a life.	Critical environmental impact	Shutdown of main system, excessive time for repair.	Drilling control system, BPCS, SIS systems (minimum rating), PMS, essential systems, DP control system, main engine control system, safety systems, new or unproven essential technologies minimum rating.
3	Immediate and Catastrophic lost time injuries, or multiple loss of life.	Catastrophic environmental impact	Significant repair time or loss of the marine or offshore asset.	Drilling Blowout Preventer control system, SIS or safety control systems, boiler firing control system, etc.

Catastrophic: Loss of human life, loss of asset, loss of system safety or security, or extensive financial or social loss.

Critical: Permanent injury or multiple lost time injuries, mission critical system damage, or significant financial or social loss.

Marginal: Lost time injury or illness, degradation of ship or units performance, or some financial or social loss.

Negligible: First aid injury or illness, non-mission critical system(s) shutdown or degraded, or DCO inconvenience.

5.3.5

Owner and DCO are to provide criteria used for IL assessment of the functions to ABS. Owner and DCO may refine terms as used above to fit company's risk tolerance.

5.5 IL Assignment Functions Documentation Requirements

5.5.1 ILO

Generally, control and monitoring of non-essential and relatively unimportant functions. Monitoring of important or essential functions where the information is not used by DCO's personnel to make essential decisions and where the data is not used in algorithms (Software Modules) for safety, important, and essential Software Modules.

- i) Descriptions of the operational or normal condition (not required for degraded or failed conditions) of the functions are to be specified in the ConOps or FDD.
- ii) The data displayed on an HMI for the DCO to make essential or important decisions are not IL0. This may apply to drilling operations where human experience and knowledge is used for the safe operation of the process.

iii) Interface description

Requirement for ARMS: Specify the requirement for testing, repair and restarting without interference with the redundant running system.

5.5.2 IL1

Generally monitoring and/or control of non-essential functions:

- i) Descriptions of the normal (operational) condition, of the function are to be specified in the ConOps or FDD.
- ii) Descriptions of the failed condition (Failure state(s)) are to be specified in the ConOps or FDD
- iii) Interface description
- iv) Requirement for ARMS. Specify the requirement for testing, repair and restarting without interference with the redundant running system.
- v) If system is redundant, specify the requirement for testing, repair and restarting without interference with the redundant operating component or part.
- vi) Obsolescence risks are defined and option selected for ARMS with replacement component(s) or part(s).

5.5.3 IL2

Essential and important systems and functions:

- i) Descriptions of the normal, condition of the functions are to be specified in the ConOps or FDD.
- ii) Descriptions of the degraded condition (state) of the functions are to be specified in the ConOps or FDD.
- iii) Descriptions of the failed condition (Failure state(s)) are to be specified in the ConOps or FDD.
- iv) Interface description
- v) Requirement for ARMS. Specify the requirement for testing, repair and restarting without interference with the redundant running system.
- vi) Specify the requirement for testing, repair and restarting without interference with the redundant operating component or part.
- vii) Obsolescence risks are defined and option selected for ARMS with replacement component(s) or part(s).

5.5.4 IL3

Essential, SIS, and important systems and functions:

- i) Descriptions of the normal, condition requirements are to be specified in the ConOps or FDD.
- ii) Descriptions of the degraded condition (state) of the functions are to be specified in the ConOps or FDD.
- iii) Descriptions of the failed condition (Failure state(s)) are to be specified in the ConOps or FDD.

- iv) Interface description
- v) Requirement for ARMS. Specify the requirement for testing, repair and restarting without interference with the redundant running system.
- vi) Specify the requirement for testing, repair and restarting without interference with the redundant operating component or part.
- vii) Obsolescence risks are defined and option selected for ARMS with replacement component(s) or part(s).

5.5.5

Refer to Section 3, Table 2 for recommended overall control system IL assignments.

TABLE 2
Recommended Safety and Environmental Overall Control System
IL Assignments (1 September 2012)

Control System	Description	IL0	IL1	IL2	IL3	Notes and Recommendations
Acoustic BOP control	Fixed and/or portable unit(s)	N/A	N/A	Note 1	X	
Acoustic DP input		N/A	X	X	N/A	
Ballast Control System		N/A	X	X	Note 1	
Ballast Water Treatment		X	X	Note 1	N/A	
BOP	Blow Out Preventer. Includes Diverter and Choke and Kill functions	N/A	N/A	Note 1	X	All Functions
Cement Pump		N/A	X	Note 1	N/A	
Chemical, gas or oil processing or separation system		N/A	X	X	Note 1	
Drawworks		N/A	Note 1	X	Note 3	ESD Functions only
Drilling Control System		N/A	Note 1	X	Note 3	See Note 3
Drilling Heave Control	Drawworks or active heave compensation lifting appliances	N/A	X	X	Note 1	
Drilling Power System	Drilling Variable Frequency Drives, Switchboards, etc.	N/A	X	X	N/A	
Drilling Top Drive		X	X	Note 1	N/A	
Dual Fuel Engine Fuel System		N/A	Note 1	X	Note 1	
Dynamic Positioning		N/A	Note 1	X	N/A	
EDS	Emergency Disconnect	N/A	N/A	X	X	
Engine Control System		N/A	X	Note 1	N/A	
ESD	Emergency Shutdown	N/A	N/A	Note 1	X	See Note 2
Fire and Gas		N/A	N/A	Note 1	X	All Functions
Fixed Rig Power Management	Jack ups, or any anchored asset	N/A	X	X	N/A	
Fuel Treatment		N/A	X	X	Note 1	
Governor		N/A	X	Note 1	N/A	
Horizontal Pipe Handling System		N/A	X	X	N/A	
Ice Load Monitoring		N/A	X	X	Note 1	

TABLE 2 (continued)
Recommended Safety and Environmental Overall Control System
IL Assignments (1 September 2012)

Control System	Description	IL0	IL1	IL2	IL3	Notes and Recommendations
Lifting Appliances	Braking function, Hoisting and Lowering function, and Heave Compensation function, non drawworks functions	N/A	Note 1	X	N/A	
LNG Refrigeration		N/A	Note 1	X	Note 1	
Marine Riser System	Includes Riser Tensioner	N/A	X	X	Note 1	
Mud Monitoring Control System	Low pressure system	N/A	X	Note 1	N/A	
Mud Pumps	High pressure system	N/A	X	Note 1	N/A	
Process Safety System (SIS)	IEC 61508, ISA 84	N/A	N/A	Note 1	X	All Functions
Production Subsea ESD		N/A	N/A	Note 1	X	
Production Subsea monitoring	Includes pressure, temperature and flow, hydrate, wax, etc.	Note 1	X	Note 1	N/A	
Thruster		N/A	Note 1	X	N/A	
Vertical Pipe Handling System	Includes finger boards, Articulated tubular handling system	N/A	X	X	N/A	
Vessel Management		N/A	X	X	N/A	
Vessel Power Management		N/A	Note 1	X	N/A	
Vessel Stability		N/A	X	X	N/A	
Zone Monitoring System		N/A	X	X	Note 1	

Notes:

- 1 Contact ABS for special consideration with justification to have this rating
 - 2 If the control system contains emergency shutdown (ESD) functions, these functions are to be rated IL2 or IL3 based upon consequences of a failure to the crew or asset and the environment. Many systems have separate and independent ESD systems that allow the Owner to lower the IL rating of the ISQM control system. The BOP (choke and kill) is considered the backup for the drilling control system and mud control system.
 - 3 The simplex software initiated ESD functions located within the Drilling Control System are IL3 if the functions are simplex. If the software initiated ESD functions are redundant, i.e. located within other control systems or hardwired, recommend IL2. It is recommended that other functions within the Drilling Control System are IL2 or less.
- N/A: Not available. ABS may not agree to offer a notation for the chosen control system based on the overall IL rating. Contact ABS
- X Available selection without contacting ABS

5.7 Software Quality Management

The Owner is to specify the verification method to be followed. There are three options of verification of the integrated system software. In the V V&T Phase, the software for the system, at a minimum, is to operate as specified in the SRS and SDS or FDD (verification). It is permissible to use all three methods of verification where the Owner-selected method is to verify the IL2 and IL3 functions, where feasible.

- i) *Closed Loop:* ABS to specially consider this option
- ii) *Software-In-the-Loop:* The integrated system software is executed on a non-native platform and the simulation may reside on the same machine
- iii) *Hardware-In-the-Loop:* The integrated system software is executed on its native platform and the simulation is running on a separate machine of different technology

The selection of the verification method is to include considerations of complexity of the functions and associated Software Modules, the functions' Integrity Level and the quantity of supplier's packages to integrate. The development of the simulation is performed in parallel with the integrated system software development and not at the conclusion of the software development.

Refer to Section 6 for a description of the V&V methods.

5.9 Obsolescence Plans

5.9.1

The SI is to **provide a high-level** hardware obsolescence plan for the integrated system. Accessibility, Reliability, Maintenance and Safety (ARMS) are to be considered **when developing** the plan.

5.9.2

The SI is to **provide a high-level** software obsolescence plan for the integrated system software.

7 Concept of Operations Document (ConOps) (1 September 2012)

An example ConOps Table of Contents is provided in Appendix 3. The ConOps is to be reviewed by the Owner (if not developed by the Owner), **SBI, DCO, SI (if not developed by the SI), IA, and ABS**. The ConOps is to contain the information listed in 3/7.1. **Review period as per contract or other agreement with the contracting party.**

7.1 General Topics

- i) Overall scope and goals of the project
- ii) Supplier's packages, if applicable
 - a) Manufacturer **or the SI's or Supplier's part number**
 - b) Model Number, if possible
 - c) Interface protocol
 - d) Constraints
- iii) Function's description including:
 - a) Sufficient detail to develop the RD Phase documents.
 - Integrator may have input on the word "sufficiently". For common and well understood functions, the detail could be "sufficient" with a one line statement.
 - b) Every function is to have a description and an assigned Integrity Level (IL0 to IL3).
 - c) **Fail safe state(s).**
- iv) Number and description of Human Machine Interfaces to include:
 - a) Manufacturer
 - b) Model Number **or the SI's or Supplier's part number**, if possible
 - c) Interface protocol
 - d) Constraints
- v) Number and description of interfaces (data collection, SCADA systems...):
 - a) **Quantity of network or direct connections to the ISQM control system**
 - b) Interface protocol **of interfaced network, control system and/or equipment**
 - c) Constraints **of interfaced network, control system and/or equipment**
- vi) Primary verification method

7.3 Definition of the Project Scope

The Owner, with input from DCO, is to state the purpose and scope of the integrated system in the ConOps.

7.5 Integrated System Major Components and Boundary

7.5.1

Major packages or components are to be preliminarily selected at a high Integrity Level.

Note At this point in the process, the SI and/or Owner know what interfaced or connected equipment packages from other vendors is needed to meet the ConOps. The Dynamic Positioning System will interface with the Power Management System from Vendor Xyz, as an example. A listing of the interfaced or connected equipment and the HMIs are included in the ConOps.

7.5.2

Control System component redundancy is not to lower the Integrity Level of the function if the redundant control system is running identical software. This includes the integrated system and the connected components. If there is a defect in the software, the function and the associated connected component or equipment under control may fail as both the primary and backup control systems are running identical code.

7.5.3

It is permissible to lower the IL number if the redundancy consists of two different technologies (i.e., PLC control and another means of control or controlled shutdown, mechanical, hydraulic, etc.).

7.7 Constraints

Constraints are to be identified and delineated in the Concept of Operations document. These can include:

- i) Supplier's package limitations
- ii) Existing, new or novel technologies to be applied
- iii) Software limitation, if known
- iv) Network or serial communications limitations of the Supplier's package (function), if known
- v) Anticipated software function risk assessment

Example: The Supplier's package may only be able to communicate using Modbus at 9600 BPS leading to the need for additional hardware module(s) for the integrated system. The process control group may suggest advanced control using unproven Software Modules (fuzzy logic, model predictive control) but the risk is judged too high by the Owner leading to using simpler proven control.

7.7.1

Suppliers' constraints are to be mitigated as necessary.

7.7.2

Supplier's verification report (V&V Report) for IL1, IL2 and IL3 ISQM control system connected packages are provided and any exceptions are noted in the FDD. Verification IL2 and IL3 functions are to be witnessed by ABS and the V&V Report may not be available at the time of FDD development.

Note: The V&V Report can be delivered during the Construction Phase. It is not necessary to have all suppliers V&V Reports for IL1, IL2 and IL3 systems to begin construction.

7.7.3

Supplier's verification plan (V&V Plan) is to be provided for IL2 or IL3 ISQM control system packages and any exceptions are noted in the FDD.

Note: The V&V Report can be delivered during the Construction Phase. It is not necessary to have all suppliers V&V Reports for IL2 and IL3 systems to begin construction.

9 Deliverables

The deliverable is the Concept of Operations phase document (ConOps).

11 Milestones (1 September 2012)

11.1 Concept Phase Complete, Milestone M2

The M2 Milestone signifies that:

- i) Components of the integrated system are identified.
- ii) Safety review report(s) are submitted.
- iii) The ConOps has been updated with safety review(s), FMEA, etc., accepted recommendations.
- iv) Integrity Levels are assigned to functions.
- v) Management of Change procedure (MOC) is applied to the ConOps.
- vi) Potential subcontractors have been consulted.
- vii) Selection of the primary V&V method for the ISQM control system
- viii) Supplier's V&V Plans are provided for IL2 or IL3 ISQM control system packages, exceptions are noted in the ConOps

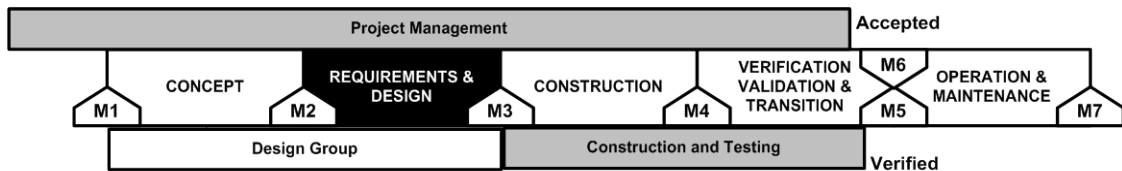
Note: The V&V Report can be delivered during the Construction Phase. It is not necessary to have all suppliers V&V Reports for IL2 and IL3 systems to begin construction.
- ix) Supplier's V&V Reports, for IL1 ISQM control system connected packages are provided, exceptions are noted in the ConOps. Verification IL2 and IL3 functions are to be witnessed by ABS and the V&V Report may not be available at the time of ConOps development.

Note: The V&V Report can be delivered during the Construction Phase. It is not necessary to have all suppliers V&V Reports for IL2 and IL3 systems to begin construction.
- x) Updated integrated system's project and overall schedules are complete.
- xi) Hardware and software obsolescence plans are included in the ConOps.
- xii) ARMS considerations are noted in the ConOps.
- xiii) Design considerations tradeoffs are complete and included in the ConOps.
- xiv) ConOps has been reviewed by DCO, SI, IA, and ABS. Review period as per contract or other agreement with the contracting party.
- xv) List of connected supplier's equipment.

11.3 Authorization from the Owner to Proceed to the RD Phase

The Owner and ABS, with input from the IA, are to approve the ConOps to proceed to the RD Phase.

SECTION 4 Software Development Life Cycle: Requirements and Design (RD) Phase



1 Scope and Objectives

(1 September 2012) At the beginning of an ISQM software project, there are two paths for developing the software detailed description, see Section 2, Figure 9. The paths are:

- Design Group (Section 9) delivering Functional Description Documents (FDD).
- Concept Phase (Section 3) delivering a Concept of Operation Document (ConOps) followed by Requirements and Design Phase (Section 4) delivering the SRS and SDS documents.

If the control system functions (code) meet the following requirements, then proceeding using the Design Group and producing the FDD is acceptable to ABS:

- The control system software to be provided to control or monitor the equipment, control system or integrated system is to be comprised of approximately 85% or more utilizing established functions and code modules or code with the remainder being configuration modifications and/or new code to meet the requirements or specifications.

And

- The control system software is to be currently in use within the industry.
 - Multiple updates or modifications that have been made to the control system software over time does not preclude the use of this section and is acceptable to ABS.

Or

- Special consideration from ABS is granted.

If the control system software meets the above requirements, see Section 9.

Below are the requirements and recommendations for the Requirements and Design Phase with the major deliverables being the SRS and SDS.

1.1 General

The Requirements and Design (RD) Phase refines the Concept of Operations document (ConOps). The focus of the RD Phase is the specification, architecture, and design of the integrated control software. The RD Phase uses the ConOps to provide guidance regarding system features. In concert with principles and quality criteria which are finalized early in the RD Phase, these ConOps inputs serve as guiding criteria for the specification, architecture, and the detailed design of the software. The resulting RD Phase documents are the basis of the Construction phase. Refer to Appendix 1 for activities and requirements for this phase.

If any new constraints are identified, they are to be documented and discussed with the Owner. Mitigation of the constraints are documented and the ConOps updated per the Management of Change (MOC) procedure. RD Phase documents are reviewed against the ConOps and, upon the Owner's approval, become the verification acceptance documents.

1.3 RD Phase Activities

(1 September 2012) During the RD Phase, focus shifts from system level description and designs to software level specification, architecture and design. From these artifacts, programmers (coders) are eventually able to convert modeled relationships and flows into **software** code. The **two** activities that are called out in IEEE 12207 that map to the scope and objectives of the RD Phase are **below as well as the two documents developed during this phase:**

1.3.1 Software Requirements Analysis *(1 September 2012)*

In software requirements analysis, the functions are de-composed into software modules. For purposes of software configuration management in the support processes, each identified software module is a configuration item. Software module's specification contains functional capability and performance specifics. Other factors **for consideration** are: interfaces external to the Software Module, qualification requirements, safety and environmental specifications, especially those involved in operations and maintenance, security requirements, human factors (ergonomics), user documentation, operation and maintenance requirements.

1.3.2 Software Architectural Design

1.3.2(a) During the software architectural design activity, the SI:

- i) Transforms software requirements into a top-level architecture that identifies software components for each of the software modules.
- ii) Assigns each of the requirements in the SRS to one or more Software Module(s).
- iii) Documents requirements and Software Modules in the traceability matrices (Refer to Appendix 3).
- iv) Documents the architecture of the Software Modules.
- v) Develops:
 - Top-level external interface designs
 - Top-level design for any database
 - The preliminary design of the user documents
 - Preliminary test requirements

1.3.2(b) It is recommended that the software architectural design be evaluated using the criteria recommended in the IEEE 12207 standard:

- i) Traceability to the requirements of the software item
- ii) External consistency with the requirements of the software item
- iii) Internal consistency between software components
- iv) Appropriateness of design methods and standards used
- v) Feasibility of detailed design
- vi) Feasibility of operations and maintenance

1.3.3 Software Requirement Specification (SRS) *(1 September 2012)*

The ISQM SRS is a specification for the integration of a defined set of functions consisting of particular software products, programs, or set of programs that perform defined functions in a defined environment. The SRS is to be reviewed by the Owner, DCO, IA organizations and ABS. **Review period as per contract or other agreement with the contracting party. The SI is to have the discretion to include or not include software functional proprietary information or intellectual property of the SI in the SRS. The SI is to describe the functions in descriptive terms.**

The SRS is to address the following, at a minimum:

- i) *Functionality:* Describe, in high-level terms, the purpose of the control system and software.
- ii) *External interfaces:* Describe, in high-level descriptive terms, how the software provides for interaction with users (user interfaces), the system execution hardware, externally interfaced system support hardware, and externally interfaced system support software.
- iii) *Performance:* Describe the availability of the control systems, scan speed if fast enough for the application, recovery or reboot time.
- iv) *Attributes:* Describe, in high-level descriptive terms, the reusability of the code, the maintainability, security, etc., considerations.
- v) *Design constraints:* Describe the constraints imposed on this implementation.
- vi) *Other:* Describe the standards that are applied to the implementation of the software, execution hardware, software language used in the implementation, policies for database integrity, resource limits, operating environment(s) etc.

1.3.4 Software Design Specification (SDS) (1 September 2012)

The ISQM integrated SDS describes the design of the system's integrated components. Typical contents include system or component architecture, control logic, data structures, input/output formats, interface descriptions, and algorithms. The SDS is to be reviewed by the Owner, DCO, IA organizations and ABS. Review period as per contract or other agreement with the contracting party. The SI is to have the discretion to include or not include software functional proprietary information or intellectual property of the SI in the SDS. The SI is to describe the functions in descriptive terms. Review period as per contract or other agreement with the contracting party.

1.3.4(a) Integrated Software Detailed Design Process. Software detail design begins in the RD Phase and continues in the Construction Phase. Software integration detailed design is the activity where software component integration of the Software Modules are refined into lower levels comprised of software integration units that will be coded in the Construction Phase. These detailed design specifications are developed during the RD Phase and refined during the Construction Phase so that the SI developers (coders) have a clear understanding of the precise nature of the task the software is to accomplish.

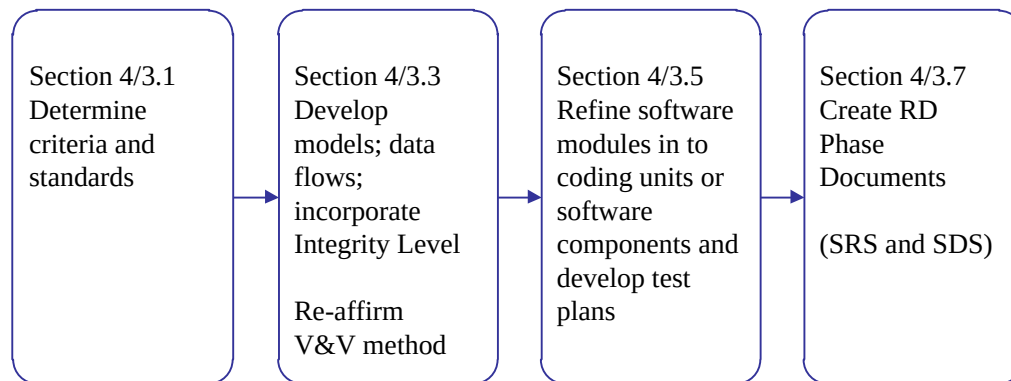
1.3.4(b) The software detailed design and test requirements are to be evaluated using these criteria recommended in the IEEE 12207 standard:

- i) Traceability to the requirements of the software item
- ii) External consistency with the architectural design
- iii) Internal consistency between software components (modules, programs)
- iv) Appropriateness of design methods and standards used
- v) Feasibility testing
- iv) Feasibility of operations and maintenance

3 Example RD Phase Design Process Flow for ISQM

Section 4, Figure 1 is a nominal depiction of a sequence that could be used to arrive at the RD Phase Documents.

FIGURE 1
General Flow of Work During the Requirements and Design Phase (1 September 2012)



Section 4, Figure 1's section references are below.

3.1 Criteria and Standards Selection (1 September 2012)

The criteria and standards are established and agreed to by the Owner and DCO organizations in step 3.1. While developing the software architecture, the assigned Integrity Levels are to be incorporated as well as the approved Owner-specified primary verification method.

3.3 Models

It is recommended that the SI develop models, data flows and other graphical support items, as needed. Refer to Appendix 4 for example models.

3.5 Identify Coding Units and Test Plans

Decomposition of Software Modules is accomplished. Identification of coding units and test plan development are completed.

3.7 RD Documents

The SRS and SDS sections of the Requirements and Design Phase document are developed.

5 Requirements and Design Phase Documents

The RD Phase documents consist of the Software Requirements Specification (SRS) and the Software Design Specification (SDS).

5.1 Software Requirements Specification (SRS)

An example SRS Table of Contents is provided in Appendix 4. The SRS, at a minimum, is to contain:

- i) The results of the software requirements analysis activity
- ii) Work Process flow Diagrams
- iii) Criteria and Standards
- iv) The Software Modules with associated functions are de-constructed into sub-software modules which make up the required function
- v) Preliminary test requirements
- vi) Functional test requirements
- vii) Top-level external interface specifications
- viii) Functions are traceable to the ConOps

5.3 Software Design Specification (SDS) (1 September 2012)

An example SDS Table of Contents is provided in Appendix 4. The SDS, at a minimum, is to contain:

- i) Top-level design for any database
- ii) Design for internal and external interfaces
- iii) Preliminary design of the user documents
- iv) Software architecture design evaluation
- v) Software design constraints
- vi) Functions are traceable to the ConOps

5.5 Risk Management

At this point, there are **two** main aspects for risks, project and operational.

5.5.1 Project Risk Management (1 September 2012)

It is recommended that metrics be collected, measured and managed during the RD and Construction Phases to notify the Project Manager of potential issues with schedule, effort, and software quality. **Recommended metrics are listed in Appendix 8. The metrics data is for the SI's internal use to manage their software quality.**

5.5.2 Operational Risk Management

Operational risks are addressed with the safety reviews, Failure Mode, Effect and Criticality Analysis (FMECA) and other reviews. New technology may come to light during the RD Phase.

5.5.3 Supplier's Package Documentation

Supplier's package documentation is to be considered in the overall plan.

5.5.4 Software Control System FMECA (1 September 2012)

The purpose of the FMECA is to determine that a single Software Module failure will not lead to failures of other Software Modules or loss of the control system.

- i) **IL2 and IL3 assigned ISQM control systems are to have a software focused functional FMECA performed.**
- ii) A Control System FMECA is to provide traceability of the Software Modules to the relevant functions in the Traceability Matrix.
- iii) A Control System FMECA of IL2 and IL3 functions is to be performed **including interfaces with integrated control systems that may have an effect upon the function.**
- iv) Update the SRS and SDS **or FDD** with FMECA recommendations.

5.5.5 New or Unproven Technology

New or unproven technology carries additional risk. ABS has Guidance Notes on risk assessment, *Guidance Notes on Review and Approval of Novel Concepts*, to assist the user. The new or novel technologies may be hardware, mechanical equipment, interface protocol or the Software Module coding. Refer to 3/5.1.4.

5.5.6 New Functionality Added in the RD Phase

- i) The Owner is to update the ConOps.
- ii) Safety reviews of the new functions are to be conducted and the results are to be documented.
- iii) If the function was added after the Software Control System FMECA, a FMECA is to be conducted to address any risks with the new functions and associated Software Modules.

5.7 Document Approval (1 September 2012)

The SRS and SDS are to be reviewed by the Owner, DCO, IA organizations and ABS for consistency with the ConOps. Review period as per contract or other agreement with the contracting party.

- i) The SI is to update and approve the SRS and SDS per the Control System FMECA and comments from reviews.

5.9 Function Requirements for ConOps with IL assignment

5.9.1 General Requirements for all Functions

- i) Unique identification of the functions for traceability
- ii) Functional description
- iii) IL assignment number
- iv) Identify function as Essential or SIS function
- v) Safety review(s) traceability or cross reference
- vi) Interface requirement(s) of the function's equipment
- vii) Process conditions
 - Temperature, pressure
 - Operating ranges
 - Alarm points
- viii) If function is a COTS
 - Supplier's identification (Model number)
 - Interface requirements
 - Constraints
- ix) Verification scenarios
 - Refer to Section 6, Figures 2 through 5 for V&V Plan requirements

7 V & V Activities during the RD Phase

The V&V organization is to develop a draft of the V&V Plan.

9 RD Phase Deliverables

- i) The Software Requirements Specifications (SRS) and Software Design Specifications (SDS).
- ii) Initial V&V Plan developed by the V&V Organization.
- iii) Variance of standards report, if variance occurred.

11 RD Phase Complete, Milestone M3

It is recognized that some RD phase activities extend into the Construction Phase.

M3 Milestone: RD Phase complete

- i) Interface or integration between components of the integrated systems is clearly defined
- ii) Detailed descriptions of functional components are complete
- iii) Alignment of the SRS and SDS with the ConOps phase document has been accomplished
- iv) Integrity Levels align per the concept scope

- v) Update software and overall project schedule
- vi) Authorization from the Owner to proceed to the Construction Phase
- vii) Variance of standards report(s)
- viii) Issue the SDS and SRS (Issue for Construction)