2021

Guidance for Integrated Software Process Management

GC-34-E

KR

APPLICATION OF "Guidance for Integrated Software Process Management"

1. Unless otherwise noted, the requirements in the Guidance apply to integrated software for which the application for process management is dated on or after July 1, 2021.
2. The amendments to the Guidance for 2020 edition and their effective date are as follows;

Effective Date : 1 July 2021

CHAPTER 1 GENERAL

Section 1 General

- 101. 6 has been added.

CHAPTER 4 PROJECT PROCESS

Section 1 Project Management Process

Section 2 Support Process

- The detailed requirements for PROJECT PROCESS in Chapter 4 have been totally revised reflecting relevant international standards.

CONTENTS

CHAPTER 1 GENERAL

Section 1 General

101. Application

1. This Guidance presents procedures and criteria applied by the Society through the review and survey of computer-based control systems related to software development. The purpose of this guidance is to reduce software-related incidents that can negatively affect system performance.
2. This Guidance specifies methods for the engineering management of software development processes for the design, development and maintenance of integrated computer-based control systems.
3. Ships or offshore structures that meet the procedures and criteria set out in this Guidance can be assigned a notation ISPM.
4. This Guidance highlights the software aspects of the control system. Security standards for hardware, failure mode and effect analysis (FMEA), and computer-based control systems are provided in other rules, guidelines issued by the Society and other standards. In addition to the ones provided in this Guidance, other criteria must be met.
5. The procedures and criteria provided in this guidance are structured processes based on best practices for the engineering management of the software development process in the design, implementation and maintenance of computer-based systems. Compliance with the process and standards of this Guidance is intended to increase the safety, accessibility, reliability and maintainability of computer-based control systems.
6. Software for purpose other than control(e.g. monitoring, management), when it affects on the performance of the control system, is to be developed accordance with the procedures and criteria in this guidance. *(2021)*

102. Definitions

The definitions of terms are to follow the Rules for Steel ships, unless otherwise specified in this Guidance.

1. **"Software Product"** means set of computer programs, procedures, and possibly associated documentation and data.
2. **"Adaptive Maintenance"** means the defect of concept error detected during the Verification process
3. **"Anomaly"** means Modification of a software product performed after delivery to keep a computer program usable in a changed or changing environment.
4. **"Artifact"** means a tangible product or by-product produced during the development of software. Some artifacts help describe the function, architecture, and design of software. Other artifacts are concerned with the process of development itself - such as project plans, business cases, and risk assessments. Much of what are considered artifacts is software documentation.
5. **"Change Control"** means Management of change as one part of the SCM process.
6. **"Closed Loop Verification"** means that the inputs and outputs of the computer-based integrated system are to be simulated with minimal interaction of the other integrated components. The V&V may require changing register values of the program to evaluate the integrated control system software response. A comprehensive understanding of the software code and functions limits this option to simple systems.
7. **"Completeness"** means that the state of software in which full implementation of the required functions is provided.
8. **"Component"** means one of the parts that make up a system. A component may be hardware of software and may be subdivided into other components. The terms “Module“, “component“, and “unit“ are often used interchangeably or defined to be sub-elements of one another in different ways depending upon the context. The relationship of these terms is not yet standardized.

9. **"Comprehensibility"** means that The quality of being able to be understood; intelligibility, conceivability.
10. **"Concept Error"** means that the interpretation of the ConOps is in error when compared to the SRS and SDS or where the intended purpose of the function was not described correctly leading to software modules not performing the intended function properly.
11. **"Concept of Operations(ConOps)"** means a group that is responsible for accepting or rejecting changes in configuration items.
12. **"Configuration Item"** means that an aggregation of hardware, software, or both, that is designated for configuration management and treated as a single entity in the configuration management process.
13. **"Consistency"** means uniformity of design and implementation techniques and notation.
14. **"Corrective Maintenance"** means reactive modification of a software product performed after delivery to correct discovered faults.
15. **"Correctness"** means the state of software in which traceability, consistency, and completeness are provided.
16. **"Cosmetic Defects"** means that these types of defects are the ones, which are primarily related to the presentation or the layout of the data. However there is no danger of corruption of data and incorrect values.
17. **"Critical Defects"** means that These are extremely severe defects, which have already halted or are capable of halting the operation of the computer-based control system.
18. **"Defect"** means a software coding error.
19. **"Deficiency"** means that software appears not to be performing the functions as listed in the ConOps, SRS and SDS.
20. **"Degraded"** means that a component or part of the control system or connected equipment is not functioning per the specification.
21. **"Emergency Maintenance"** means unscheduled corrective maintenance performed to keep a system operational.
22. **"Emulator"** means that an emulator duplicates the functions of one system using a different system. The second system “behaves” like the first system.
23. **"Essential Services"** means those services essential for propulsion and steering, and safety of the ship, which are made up of "primary essential services" and "secondary essential services" and definitions and examples are to be in accordance with Pt. Ch1 101. 4 of the Rules for the Classification of Steel Ships.
24. **"Failed"** means that The ISPM control system or significant portions of the connected equipment is not functioning normally.
25. **"FMECA(Failure Modes, Effects and Criticality Analysis)"** means that the criticality analysis is used to chart the probability of failure modes against the severity of their consequences. The analysis highlights failure modes with relatively high probability and severity of consequences.
26. **"Firmware"** means the combination of a hardware device and computer instructions and data that reside as read-only software on that device.
27. **"Flexibility Matrix"** means a method that facilitates tradeoff analysis concerning scope, schedule and resources during project definition and work planning.
28. **"Function"** means The purpose of the equipment under control (i.e., the hydraulic power unit, winch, power management system).
29. **"Hardware"** means physical equipment used to process, store, or transmit computer software or data.
30. **"Hardware-In-the-Loop"** means that the integrated system’s program is being executed on its native hardware (CPU or controller hardware) and the simulation is being executed on a separate machine. Interfaces between the two are developed for the testing. The simulation is to be of suf-

ficient fidelity to include physical real world dynamic systems to verify the central control system's programming and documenting the results of the stimulus. The real world represented by mathematical models in the simulation program.

31. **"Human Machine Interface"** means a display and operator input device.

32. **"Instrumentation"** means the attributes of software that provide for the measurement of usage or identification of errors.

33. **"Integrity Level"** means A number assigned by Owner and/or User to a computer-based function based upon the severity of the consequence of a failure of the function. Where 0 has little consequence to 3 where the consequence of a function failure is of significant concern with corresponding consequences.

34. **"Interoperability Testing"** means Testing conducted to determine that a modified system retains the capability of exchanging information with systems of different types, and of using that information.

35. **"Major Defects"** means that these are severe defects, which have not halted the system, but have seriously degraded the performance, caused unintended action or incorrect data transmitted.

36. **"Minor Defects"** means Defects which can or have caused a low-level disruption of function(s). Such defects can result in data latency but not in essential or IL2 or IL3 functions. The integrated system and the function continue to operate, although with a failure. Such a disruption or non-availability of some functionality can be acceptable for a limited period of time for IL1 functions. Minor defects could cause corruption of some none critical data values in a way that is tolerable for a short period.

37. **"Moderate Defects"** means that software function performs differently than specified in the SRS and SDS or FDD leading to a change in the Operating Manual, may be called a Moderate Defect. The Owner is to review the impact and risk of such a change.

38. **"Modification Request"** means A generic term that includes the forms associated with the various trouble/problem-reporting documents (e.g., incident report, trouble report) and the configuration change control documents.

39. **"Modularity"** means Being provided with a structure of highly independent modules.

40. **"Native Computer"** means that the program is being executed on the hardware that it will execute upon when installed.

41. **"Non-native Computer"** means that the program is being executed on an emulation of the target hardware using an emulator.

42. **"Nonoperational"** means that not in working order or ready to use.

43. **"Normal"** means that the control system, connected components and associated input and output modules are in working order.

44. **"Operational"** means (1) Pertaining to a system or component that is ready for use in its intended environment. (2) Pertaining to a system or component that is installed in its intended environment. (3) Pertaining to the environment in which a system or component is intended to be used. (IEEE Std. 610, 1990, IEEE Standard Computer Dictionary, A Compilation of IEEE Standard Computer Glossaries)

45. **"Owner"** means that the Owner is the organization which decides to develop the system, and provides funding.

46. **"Package"** means a test used to determine whether changing part of an issue has created a new issue for a different part of the application.

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

48. **"Perfective Maintenance"** means Modification of a software product after delivery to improve performance or maintainability.

49. **"Unit Testing"** means a method wherein the smallest testable portions of a module are verified. Individual units are first tested then these are tested in combination with other units within the module to assess proper interactions and outcomes. Once the module has been proven then in-

ter-module interactions can be tested.

50. **"V&V"** means Verification and Validation of the integrated software program.

51. **"V&V Organization"** means that The V&V organization is to verify the functions defined in the Software Requirement Specification (SRS) and Software Design Requirement (SDS) or Functional Description Documents (FDD) using Closed Loop (specially considered), Software-In-the-Loop or Hardware-In-the-Loop methodology. The V&V organization may be part of the System Integrator's organization or may be independent, as directed by the Owner, with limitation.

52. **"Validation"** means that Determines if the software satisfy the intended use as documented in the ConOps.

53. **"Verifiability"** means the capability of software to be verified, proved, or confirmed by examination or investigation.

54. **"Verification"** means that Demonstrate the software performs as delineated in the SRS and SDS or FDD. Also determines whether development products of a given activity conform to the requirements of that activity.

55. **"Version Control"** means management of the asset versions generated as part of the SCM process.

56. **"Virus Definition"** means Database of computer virus signature used by anti-virus programs.

103. Equivalence

The Society may consider the acceptance of alternatives to this Guidance, provided that they are deemed to be equivalent or above to those complying with the requirements of the Guidance.

104. Exclusion from the Guidance

The Society cannot assume responsibility for use of unauthorized commercial products and other technical characteristics not specified in the Guidance. ⚓

CHAPTER 2 TEST AND SURVEY PROCEDURE

Section 1 General

101. General

1. Guidance is a requirement to maintain a classification of control systems related to integrated software process management notation (ISPM). Where applicable, the requirements apply to ships or installations in addition to those specified in our classification Rules and / or Guidance.

2. The date of commissioning shall be the date when the Surveyor has issued a temporary certificate of classification for the ship or installation which has been assigned an ISPM notation.

102. Survey for integrated software quality control notation

1. Survey intervals and maintenance manuals/records

(1) All annual and periodic surveys relating to ISPM notation are periodic surveys of ships or equipment, carried out at the same time and interval and recorded on the same date of certification.

(2) Annual surveys of the integrated software relating to ISPM notation shall be carried out by the Surveyor within three months of each year of initial certification surveys. Periodic surveys of control systems related to ISPM notation shall be carried out within five years from the initial certification surveys and at intervals of five years thereafter. ISPM surveys may be provided for surveys before the desired time limit, in which case an assessment may be made after that date.

(3) Maintenance and calibration records are to be kept and reviewed at the attendance of the Surveyor. Review the maintenance records to establish the scope and content of the annual and regular inspections to be carried out by the Surveyor. During the service life of software system components, maintenance records must be updated continuously.

(a) The owner shall notify the Society whenever the IL3 software module is modified or installed in the control system by means of an ISPM designator. The Society may survey the ship after notifying of the modification or installation of the IL3 software module.

2. Annual Survey

At each annual survey, the Surveyor shall perform an integrated software and hardware configuration survey, including verification as follows.

(1) Change management procedures include periodic surveys to confirm that the procedures are being followed.

(2) Controller Registry survey

(a) Identify the control unit changed since the last surveys
(b) Record each changed equipment item
(c) a list of all software managed on the changed equipment
(d) identify all documents affected by the change
(e) record each document change
(f) Record changes not listed in the registry

(3) software registry check

(a) identify any control software that has changed since the inspection
(b) record changes to each software item
(c) All software inspections managed on modified equipment.
(d) record software changes to changed equipment
(e) identify any documents affected by the change
(f) record all changed documents in the software registry
(g) record software changes not listed in the registry

(4) review hardware registry of integrated control system

(a) Interview relevant owner / user and vendor personnel and review support documentation to assess how closely they comply with software change management.
(b) Identify possible shortcomings and recommend process improvement

(5) Review of virus and malicious software scan records

3. Periodic Survey

Periodic survey shall include the satisfaction of the Surveyor with all items listed in the Annual Survey.

103. Modification, failure and repair

1. When a modification is made to a software system that affects the ship's or equipment's ISPM code designation, details of the change should be submitted for approval, and the surveyor shall perform the work satisfactorily.
2. When the control system affecting the ISPM notation of a ship or installation is damaged that may affect the integrity level, the Society is to be notified and the integrity level reevaluated.
3. Where unexpected failures occur and the control system has been repaired or replaced without the presence of the Surveyor, details of the failure are to be left onboard for verification by the Surveyor during the following Classification Survey, as far as practicable. when the failure is considered to be the result of improper or improper maintenance, the maintenance manual shall be modified and resubmitted for approval. ⚓

CHAPTER 3 SOFTWARE PROCESS

Section 1 General

101. General

1. This guidance gives an overview of the steps and management methods that are aimed at the successful development and transition of the software. There are five phase of the Software Development Life Cycle (SDLC), management process, and support process.
2. The SDLC described in this guidance is the least acceptable process. Milestones are those items that need to be fulfilled at each phase of the process being systematically processed and that the document shall ensure that the functions convey the meaning and intent of the functions. The milestones must be met before the end of each phase.

Section 2 Roles and Responsibility of Stakeholder

201. General

1. The purpose of stakeholder requirements is to define the requirements of a system that can provide the services that users and other stakeholders need in a defined environment. Throughout the system's life cycle, it identifies the stakeholders or groups of stakeholders that are associated with the system, and identifies their needs, expectations, and desires. This common set of requirements represents the intended interactions between the system and the operational environment, and also serves as a reference for confirming the usefulness of each operational service result.
2. Development and transition of integrated software requires a variety of organizations. Each process of the SDLC includes a number of requirements, activities and deliverables, in which various organizations carry out the requirements and activities.
3. This guidance assumes that responsibility is assigned to the organization according to the activity, and that the assignment of activities clarifies the role and deliverable of the stakeholder organization at each phase.
4. Stakeholders are organizations that are interested in the success of a project. Stakeholders in the integrated software SDLC process are defined in 202. The responsibilities and roles may be combined in some cases. (For example, the Owner may be a User, and may be an Shipyard
5. Manage stakeholder interactions, information flow and timeliness of information to maintain project schedules.

202. Role of stakeholder

1. Owner

The owner is the stakeholder who acquires or procures integrated software, which is the organization that finances and initiates the project. In order to achieve the purpose of using integrated software, the requirements are presented to the developer, and the deliverables and requirements of each step are judged.

2. System Integrator (SI)

System integration organizations are responsible for the development of integrated systems. Depending on the ISPM system chosen, there may be multiple system integrators. The system integrator is an expert in the control system in charge and has an integrated awareness of the requirements of the control system to which the equipment is connected. The system integrator is responsible for the design of the integrated system, the creation of SRS & SDS, supplier management, integration and verification of the owner's permission and control system software. The owner can request information from the system integration organization as needed for the development of ConOps. The owner may select an SI to perform verification of the integrated system or the owner

may require an independent third party verification. An SI or Shipbuilder organization may not transfer its responsibility when delegating SI activities to a third party. If the project size does not warrant a system integrator, the owner, user, or supplier organization of choice must carry out this responsibility.

(1) System integrators must currently have ISO 9001 or be at least CMMI level 2.
(2) Other software quality management systems may be specially considered by the Society. System integrators and shipyards are encouraged to guide suppliers to be informed of verification requirements and activities.

3. User

An individual or group who benefit from an integrated software converted during the integration software's usage period, responsible for the operation and maintenance phase of the system. Responsibility for maintenance ensures reliable operation throughout the life cycle of the system if improvements, upgrades and replacements or new components are added to the system.

4. Quality manager (V&V)

The quality manager receives the quality criteria, which are the owner's satisfaction criteria, from the system integrator and the software is closed loop (if specially considered) and software-in-the-loop (SIL) or hardware-in-the-loop (HIL) or The combination of these three methods identifies requirements defined in the Software Requirements Specification (SRS) and Integrated Software Design Specification (SDS). Verification and verification organizations can be part of the system integrator or be independent at the owner's request.

5. Shipbuilder

Ship builder means shipyard. The department within the shipyard may be an Shipbuilder if it has entered into a contract with the system integrator or meets the requirements of 104. SI. Shipbuilder performs integration verification activities when the ISPM control system is installed. Integration activities include verifying communications (consolidation checks) between equipment connected to the ISPM control system. Shipbuilder is responsible for the conversion (supply) of the ISPM control system desired by the owner under the contract.

6. Class Society (CS)

The Society reviews the documents produced during the development of the ISPM control system independent of the SI to ensure that stakeholders comply with these guidelines. However, verification tests for control systems rated IL2 or IL3 are to be carried out in the presence of the Society. Integrated verification tests carried out by Shipbuilder or its owners are to be carried out in the presence of the Society.

7. Supplier

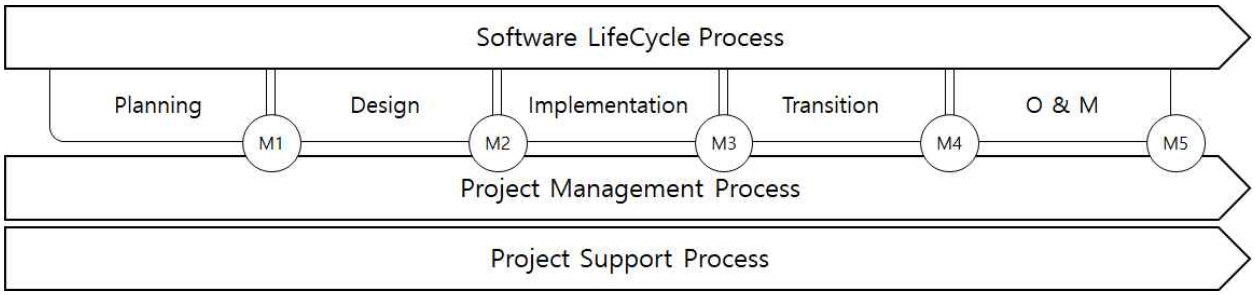
An organization that performs development tasks during a process, either as a component of integrated software or as a contracted supplier of software. The developer shall provide the specifications and constraints of the system package that the developer supplies according to the specific scope and schedule assigned by the system integrator or the ship builder. Supplier verification of IL2 and IL3 supply equipment should be verified with the Society.

(1) The Supplier organization must currently have ISO 9001 or be at least CMMI level 2.
(2) Other software quality management systems shall follow the software conformance certification guidelines, if necessary.

Section 3 ISPM Process

301. General

This section outlines the five phases of the development lifecycle process, the project support process, and the project management process.



302. Software Development Life Cycle (SDLC)

1. The software development life cycle refers to a series of engineering plans for software development, from conception to disposal of computer-based control systems. Milestones (or step gates) are associated with each step or boundary of the SDLC and with the provision of specific step products.

2. The software development life cycle is as follows:

(1) planning phase
The following activities are carried out to determine the direction and scope of the project and to define the integrated system in detail.
(a) Safety review
(b) integrity level (IL) evaluation
(c) components of the initial integrated system
(d) Major verification methods
(e) Create ConOps

(2) Development phase (RD)
Developers and programmers of system integrators write documentation that can be used to configure software for the features defined in ConOps, taking into account the system architecture.

(3) implementation phase (CON)
Emphasis is placed on converting the requirements and specifications of SRS and SDS into functional integrated system code. In addition, testing activities focus on the software aspect of the system.

(4) Verification, Verification phase (V & V)
The system software aims to operate as specified in the SRS and SDS. ConOps is a document used for verification as well as commissioning and sea commissioning activities, and quality managers must create a verification plan and set up a simulator according to the verification method selected at the planning process.

(5) Transition phase
After verification of the finished software, all the work required to convert the integrated system to owners and users should be completed. The software is installed on the hardware chosen by the owner and provided with support services. The system integrator must submit all documentation to the owner and user.

(6) Maintenance phase (O & M)
It covers operational and maintenance activities, including scheduled and unscheduled upgrade and troubleshooting activities, and includes disposal activities.

303. Project process

The project management process (planning, evaluation and engagement) is at the core of all management activities. These processes present a general approach to managing a project or process. The project support process is evident in the management of all tasks that span the entire organ-

ization, from one organization to one lifecycle process and its tasks. In this International Standard, projects are used as contexts to represent processes related to planning, execution, evaluation and coordination.

1. Project management process

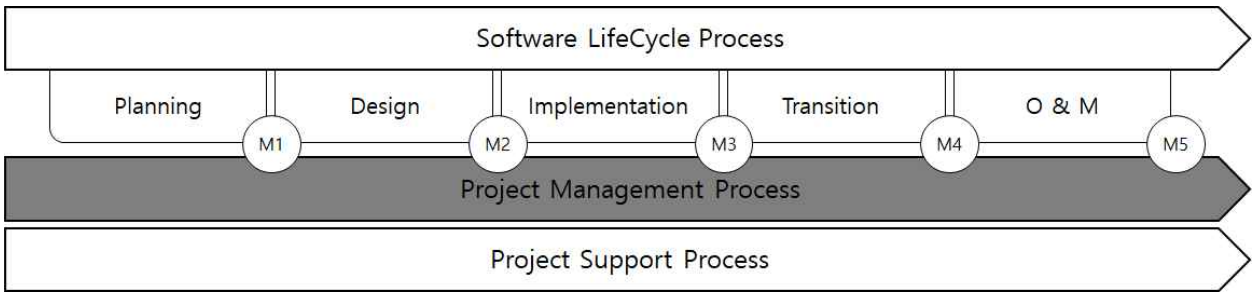
The project management process:
(1) project planning process
(2) project evaluation and control process

2. Project support process

The project support process consists of the following processes:
(1) Decision Management Process
(2) risk management process
(3) configuration management process
(4) information management process
(5) measuring process ⚓

CHAPTER 4 PROJECT PROCESS

Section 1 Project Management Process



101. General

The project management process consists of the following:

(1) Project Planning Process

(2) Project evaluation and control process

102. Project planning process

1. General

The project management process:

(1) The purpose of the Project Planning Process is to produce and communicate effective and workable project plans.

(2) This process determines the scope of project management and technical activities and identifies a schedule for project conduct, including process deliverable, project output, and project resources.

(3) The strategies defined in each of the other processes provide input are integrated in the Project planning process.

2. Activities

The planning process shall implement activities in accordance with applicable organization policies and procedures as follow.

(1) project definition

(A) Identify project objectives and constraints.

(a) Objectives and constraints include performance and other quality aspects, cost, time and stakeholder satisfaction.

(b) Each objective is identified with a level of detail that permits selection, tailoring and implementation of the appropriate processes and activities.

(B) Define the project scope as established in the agreement.

(a) The project includes all the relevant activities required to satisfy business decision criteria and complete the project successfully.

(b) A project can have responsibility for one or more processes in the complete system life cycle.

(c) Planning includes appropriate actions for maintaining project plans, performing assessments and controlling the project.

(C) Define and maintain a life cycle model that is comprised of processes using the defined life cycle models of the organization.

(2) Plan project and technical management

(A) Define and maintain a project schedule based on project objectives and work estimates.

(a) This includes definition of the duration, relationship, dependencies and sequence of activities, achievement milestones, resources employed and schedule reserves for risk management necessary to achieve timely completion of the project.

(B) Define project achievement criteria for the life cycle process decision gates, delivery dates and major dependencies on external inputs or outputs.
(a) The time internals between internal reviews are defined in accordance with organizational policy on issues such as business and system criticality, schedule and technical risks.
(C) Define the project costs and plan a budget.
(a) Costs are based on the schedule, labor estimates, infrastructure costs, procurement items, acquired service and enabling system estimates, and budget reserves for risk management.
(D) Establish the structure of authorities and responsibilities for project work.
(a) This includes defining the project organization, staff acquisitions, and the development of staff skills.
(b) Authorities includes, as appropriate, the legally responsible roles and individuals, e.g., design authorization, safety authorization, and award of certification or accreditation.
(E) Define the infrastructure and services required by the project.
(a) This includes defining the capacity needed, its availability and its allocation to project tasks.
(b) Infrastructure includes facilities, tools, communications, and information technology assets.
(c) The requirements for enabling systems for each life cycle stage are also specified.
(F) Plan the acquisition of materials, goods and enabling system services supplied from outside the project.
(a) This includes, as necessary, plans for solicitation, supplier selection, acceptance, contract administration and contract closure.
(G) Generate and communicate a plan for project and technical management and execution, including reviews.
(3) Activate the project
(A) Obtain authorization for the project.
(B) Submit requests and obtain commitments for necessary resources to perform the project.
(C) Implement project plans in order to meet the goal and requirements of the project.

3. deliverable

(1) project management plan
(2) Project Contract Management Plan
(3) Project change management plan
(4) Project financial management plan
(5) project control plan
(6) Project quality assurance plan
(7) software development plan
(8) documentation plan

103. Project assessment and control process

1. General

(1) The purpose of the Project assessment and control process is as follow.
(A) To assess whether the plans are integrated, aligned, and feasible.
(B) To determine the status of the project, technical and process performance
(C) To ensure that the performance is according to plans and schedules, within projected budgets, to satisfy technical objectives.
(2) This process evaluates, periodically and at major events, the progress and achievements against requirements, plans and overall business objectives. Information is communicated for management action when significant variances are detected.
(3) This process also includes redirecting the project activities and tasks, as appropriate, to correct identified deviations and variations from other project management or technical processes.
(4) Redirection may include re-planning as appropriate.

2. Activities

The process containing the Project assessment and control process shall implement the activities in accordance with applicable organization policies and procedures as follows.
(1) Plan for project assessment and control
(A) Define the project assessment and control strategy
(a) The expected Project assessment and control activities are identified including planned assessment methods and timeframes, necessary management and technical reviews.

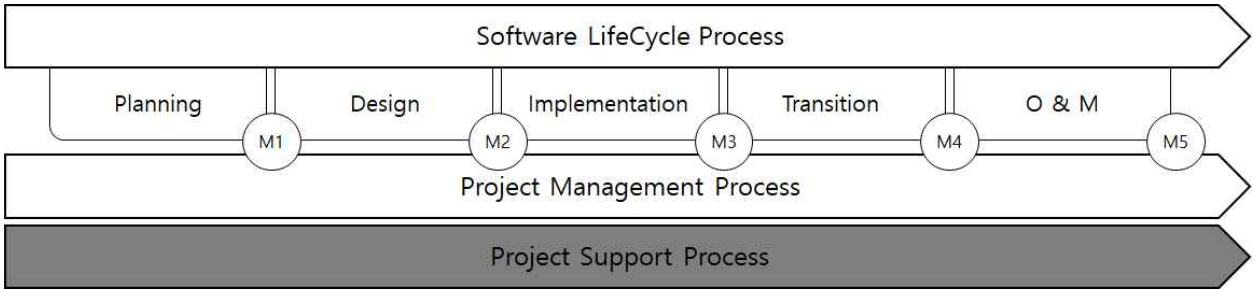
(2) Assess the project
  (A) Assess alignment of project objectives and plans with the project context.
  (B) Assess management and technical plans against objectives to determine adequacy and feasibility.
  (C) Assess project status against appropriate project plans to determine actual and projected cost, schedule and quality variations.
  (D) Assess the adequacy of roles, responsibilities, accountabilities, and authorities.
    (a) Assessment includes the adequacy of personnel competencies to perform project roles and accomplish project tasks.
    (b) Objective measures are used wherever possible like efficiency of resource use, project achievement.
  (E) Assess the adequacy and availability of resources.
    (a) Resources include infrastructure, personnel, funding, time, or other pertinent items.
    (b) Assessment includes confirming that intra-organizational commitments are satisfied.
  (F) Assess project progress using measured achievement and milestone completion.
    (a) Assessment includes collecting and evaluating data for labor, material, service costs, and technical performance as well as other technical data about objectives, such as affordability.
    (b) Assessment results are compared against measures of achievement.
    (c) Conducting effectiveness assessments is included to determine the adequacy of developing system against requirements.
    (d) The readiness of enabling systems are also included to deliver their services when needed.
  (G) Conduct required management and technical reviews, audits and inspections.
    (a) These are conducted to determine readiness to proceed to the next stage of the life cycle or project milestone;
    (b) To help ensure that project and technical objectives are being met; or
    (c) To obtain feedback from stakeholders
  (H) Monitor critical processes and new technologies.
    (a) Identifying and evaluating technology maturity and insertion are included.
  (I) Analyze measurement and make recommendations.
    (a) Measurement results are analyzed to identify deviations, variations or undesirable trends from planned values that include potential concerns, and to make appropriate recommendations for corrections or preventive actions.
    (b) Analysis includes, where appropriate, statistical analysis of measures that indicates trends, e.g. fault density to indicate quality of outputs, distribution of measured parameters that indicate process repeatability.
  (J) Record and provide status and findings from assesment tasks
    (a) The materials recorded and provided are generally designated in the agreement, policies, and procedures.
  (K) Monitor process execution within the project
    (a) This includes the analysis of process measures and review of trends with respect to project objectives.
(3) Control the project
  (A) Initiate necessary actions needed to address identified issues.
    (a) The initiation occurs when project or technical achievement is not meeting planned targets.
    (b) This includes corrective, preventive, and problem resolution actions.
    (c) Actions generally require replanning or reassignment of personnel, tools and infrastructure assets when inadequacy or unavailability has been detected, or when project or technical achievement exceeds targets or plan.
    (d) The actions often impact the cose, schedule, or technical scope or definition.
    (e) The actions sometimes require changes to the implementation and execution of the software life cycle processes.
    (f) To confirm their adequacy and timeliness, actions are recorded and reviewed.
  (B) Initiate necessary project replanning
    (a) Project replanning is initiated when project objectives or constraints have changed, or when planning assumptions are shown to be invalid.
    (b) Changing the agreement between system integrator and supplier may be considered, if necessary.

(C) Initiate change actions when there is a contractual change to cost, time or quality due to the impact of an system integrator or supplier request.
  (a) This includes consideration of modified terms and conditions for supply or initiating new supplier selection.
(D) Authorize the project to proceed toward the next milestone or event if justified.
  (a) This process is used to reach agreement on milestone completion.

2. Output

(1) project status assessment
(2) carry out quality assurance
(3) project team evaluation
(4) project progress evaluation
(5) Management and technical review and inspection
(6) Key Process / New Technology Observation
(7) data analysis and recommendations
(8) Periodic report
(9) Project control plan
(10) Project change report
(11) Requirements Status Report
(12) Project Progress Report

Section 2 Support Process



201. General

The project support process consists of as follows.

(1) Decision management process
(2) Risk management process
(3) Configuration Management Process
(4) Information management process
(5) Measurement Process

202. Decision Management Process

1. General

(1) The purpose of the Decision Management Process is to provide a structured, analytical framework for objectively identifying, characterizing and evaluating a set of alternatives for a decision at any point in the life cycle and select the most beneficial course of action.
  (A) This process is used to resolve technical or project issues and respond to requests for decisions encountered during the software life cycle, in order to identify the alternative(s) that provides the preferred outcomes for the situation.
  (B) Alternative actions are identified and selected of which are suitable for the situation of its process.
  (C) Key study results such as assumptions and decision rationale data are maintained to inform decision-makers and support future decision-making.

2. Activities

The process containing the Decision Management Process shall implement the following activities and tasks in accordance with applicable organization policies and procedures.

(1) Prepare for decisions
  (A) Define a decision management strategy.
    (a) A decision management strategy includes the identification and allocation of responsibility for, and authority to make, decisions and the identification of decision categories and a prioritization scheme.
    (b) Decisions may arise as a result of an effectiveness assessment, a technical trade-off, a problem needing to be solved, an action needed as a response to risk exceeding the acceptable threshold, a new opportunity or approval for project progression to the next life cycle process.
    (c) The degree of rigor and formality for applying to the decision analysis complies with organization or project guidelines.
  (B) Identify the circumstances and need for a decision.
    (a) Record and categorize problems or opportunities and the alternative courses of action that will resolve their outcome.
  (C) Involve relevant stakeholders in the decision-making in order to draw on experience and knowledge.
    (a) It should need to identify the subject matter expertise for the analysis and the decision.
(2) Analyze the decision information
  (A) Select and declare the decision management strategy for each decision.
    (a) The degree of rigor required to resolve these problems or opportunities is determined, as well as the data and system analysis needed for evaluating the alternatives.

(B) Determine desired outcomes and measurable success criteria.
(a) Weighting factors for each criterion of decision management are determined, and the desired value and the threshold values for all quantifiable criteria.
(C) Identify the trade space and alternatives.
(a) They are qualitatively screened to reduce alternatives to a manageable number for further detailed systems analysis when a large number of alternatives exist.
(b) The screening is based on qualitative assessments of such factors as risk, cost, schedule, and regulatory impacts.
(c) The trade space is to find alternatives for best performance under cost constraint, or optimized alternatives under an acceptable performance area.
(D) Evaluate each alternative, against the criteria.
(3) Make and manage decisions
(A) Determine preferred alternative for each decision.
(a) Alternatives are evaluated quantitatively, using the selection criteria.
(b) The selected alternative generally provides an optimization of, or improvement in, an identified decision.
(B) Record the resolution, decision rationale, and assumptions.
(C) Record, track, evaluate and report decisions.
(a) As stipulated in agreements or organizational procedures, problems, opportunities, and their disposition are recorded to permit auditing and learning from experience.
(b) The organization is able to confirm that problems have been effectively resolved, the adverse trends have been reversed, and that advantage has been taken of opportunities.

203. Risk management process

1. General

(1) The purpose of the risk management process is to identify, analyse, treat and monitor the risks continually.
(2) The Risk management process is a continual process for systematically addressing risk throughout the life cycle of a system product or service.
(3) This process applied to risks related to the acquisition, development, maintenance or operation of a system.

2. Activities

The process containing the Risk Management Process shall implement the following activities and tasks in accordance with applicable organization policies and procedures.
(1) Plan risk management
(A) Define risk management policies.
(a) Risk management policies includes the risk management process of all supply chain suppliers and describes how risks from all suppliers will be raised to the next level(s) for incorporation in the project risk process.
(B) Define and record the context of the Risk management process.
(a) Record includes a description of stakeholders' perspectives, risk categories, and a description of the technical and managerial objectives, assumptions and constraints.
(b) The risk categories include the relevant technical areas of the system and facilitate identification of risks across the life cycle of the software.
(c) The aim of this activities is to generate a comprehensive list of risks
(d) The list of risks may be capable to create, enhance, prevent, degrade, accelerate or delay the events related achievement of objectives.
(e) Opportunities, which are one type of risk, provide potential benefits for the system or project.
(f) Pursuing each opportunity has associated risks that detract from the expected benefit.
(g) This includes the associated risks not only with pursuing an opportunity but also not achieving the effects of the opportunity.
(2) Manage the risk profiles
(A) Define and document the risk thresholds and conditions under which a level of risk may be accepted.
(B) Establish and maintain a risk profile. The risk profile consists of as follows.
(a) Risk management context

(b) a record of each risk's state including its likelihood of occurrence, consequences, and risk thresholds
(c) the priority of each risk based on risk criteria supplied by the stakeholders
(d) risk management action requests along with the status of their treatment
(e) The risk profile is updated when there are changed in an individual risk's state.
(f) The priority in the risk profile is used to determine the application of resources for treatment.

(C) Periodically communicate the relevant risk profile to stakeholders based upon their needs.

(3) Analyze risks
(A) Identify risks by categories described in the risk management context.
(a) Risks are commonly identified through various analyses, readiness assessment and trade studies.
(b) Risks may be identified early in the life cycle and continue into the utilization, support, and retirement of the system.
(c) In addition, risks may be identified through the analysis of the measures of the system.
(B) Estimate the probability of occurrence and consequences of each identified risk.
(C) Evaluate each risk against its risk thresholds.
(D) For each risk that is above its risk threshold, define and recommended treatment strategies and measures.
(a) Risk treatment strategies include eliminating the risk, reducing its likelihood of occurrence or severity of consequency, or accepting the risk, but are not limited.
(b) Treatments include taking or increasing risk in order to pursue an opportunity.
(c) Measures provide information about the effectiveness of the treatment alternatives.

(4) Treat risks
(A) Identify recommended alternatives for risk treatment.
(B) Implement risk treatment alternatives for which the stakeholders determine that actions should be taken to make a risk acceptable.
(C) When the stakeholders accept a risk that exceeds its threshold, consider it a high priority and monitor it continuously to determine if any future risk treatment actions are necessary.
(D) Once a risk treatment is selected, ensure management actions in accordance with the assessment and control activities in **103. 2** of this standard.

(5) Monitor risks
(A) Continuously monitor all risks and the risk management context for changes and evaluate the risks when their state has changed.
(B) Implement and monitor measures to evaluate the effectiveness of risk treatments.
(C) Continuously monitor for new risks and sources throughout the life cycle.

204. Configuration management process

1. General

The purpose of the Configuration Management Process is to manage and control system elements and configurations over the life cycle. CM also manages consistency between a product and its associated configuration definition.

2. Activities

The process containing the Configuration management process shall implement the following activities and tasks in accordance with applicable organization policies and procedures.

(1) Plan Configuration management
(A) Define a configuration management strategy.
(a) Configuration management includes details as follows:
(i) Roles, responsibilities, accountabilities, and authorities
(ii) Disposition of, access to, release of and control of changes to configuration items.
(iii) The necessary baselines to be established.
(iv) The locations and conditions of storage, the storage media and their environment, in accordance with designated levels of integrity, security and safety.
(v) The criteria or events for commencing configuration control and maintaining baselines of evolving configurations.
(vi) The audit strategy and the responsibilities for assessing continual integrity and security of the configuration definition information.
(vii) Change management, including any planned configuration control boards, regular and

emergency change requests; and procedures for change management.
(b) The configuration management strategy needs to identify how configuration management will be coordinated across the set of system integrator, supplier, and supply chain organizations.
(B) Define the archive and retrieval approach for configuration items, configuration management artifacts and data.

(2) Perform configuration identification
(A) Identify the system elements and information items that are configuration items.
(a) Configuration items receive special attention.
(b) The items are assigned unique identifiers and are the subject of reviews and monitoring.
(c) Items generally include requirements, product and system elements, information items, and baselines.
(B) Identify the hierarchy and structure of system information.
(C) Establish system, system element, and information item identifiers.
(a) Identifiers are traceable to their specifications or equivalent, recorded descriptions.
(D) Define baselines through the life cycle.
(a) Baselines capture the evolving configuration states of system elements at designated times or under defined circumstances.
(b) Baselines form the basis for the next change.
(E) Obtain system integrator and supplier agreement to establish a baseline.
(a) The project assessment & control process is used to reach agreement.

(3) Perform configuration change management
Configuration change management establishes procedures and methods for managing change to a baseline once it is established.
(A) Identify and record Requests for Change and Requests for Variance.
(B) Coordinate, evaluate, and disposition Requests for Change and Requests for Variance.
(a) Impact assessment of proposed changes including impact on project plans, risks, and quality is to be carried out.
(b) A decision is made on whether to implement or close the change request.
(C) Track and manage approved changes to the baseline, Requests for Change, and Requests for Variance.
(a) This includes tracking, scheduling, and closing changes.
(b) Any changes and rationales are recorded.

(4) Perform configuration status accounting
(A) Develop and maintain the configuration management status information, for system elements, baselines, and releases.
(a) Configuration status accounting provides the data on the status of controlled products needed to make decisions regarding system elements throughout system life cycle.
(b) Configuration information permits forward and backward traceability to other configuration states.
(B) Capture, store and report configuration management data.

(5) Perform configuration evaluation
(A) Identify the need for configuration management monitoring and schedule for audit.
(B) Verify the product configuration meets the configuration requirements.
(C) Monitor the incorporation of approved configuration changes.
(D) Ass whether the system meets baseline functional and performance capabilities.
(E) Assess whether the system conforms to the operational and configuration information items.
(F) Record the configuration management audit results and disposition action items.

(6) Perform release control
(A) Approve system releases and deliveries.
(a) The purpose of a release is to authorize the use of a system for a specific purpose, with or without restrictions.
(b) Releases generally include a set of changes.
(c) Approval of a release generally includes acceptance of the verified and validated changes.
(B) Track and manage system releases and deliveries.
(a) Master copies of all system elements are maintained for the life of the system.

205. Information management process

1. General

(1) The purpose of the Information Management Process is to generate, obtain, confirm, transform, retain, retrieve, disseminate and dispose of information, to designated stakeholder.

(2) Information management plans, executes, and controls the provision of information to designated stakeholders that is unambiguous, complete, verifiable, consistent, modifiable, traceable, and presentable.

(3) Information includes technical, project, organizational, agreement and user information. Information is often derived from data records of the organization, system, process, or project.

2. Activities

The process containing the Information management process shall implement the following activities and tasks in accordance with applicable organization policies and procedures.

(1) Prepare for Information management

(A) Define the strategy for information management.

(a) Information about the same topic can be developed in different ways at different points in the life cycle and for different audiences.

(B) Define the items of information that will be managed.

(a) Information includes that will managed during the software life cycle and possibly maintained for a defined period beyond.

(b) When define the items is done according to organizational policy, agreements, or legislation.

(C) Designate authorities and responsibilities for information management

(a) Information is identified accordingly, where restrictions or constraints due to legislation, security and privacy.

(b) People having knowledge of such items of information specified in **(a)** are informed of their obligations and responsibilities.

(D) Define the content, formats and structure of information items.

(E) Define information maintenance actions.

(a) Information maintenance includes status reviews of stored information for integrity, validity and availability.

(2) Perform information management

(A) Obtain, develop, or transform the identified items of information.

(a) Reviewing, validating, and editing information are included per information standards.

(B) Maintain information items and their storage records, and record the status of information.

(a) Items are maintained according to integrity, security and privacy requirements.

(b) The status of information items is maintained such as version description, data of issue or validity date, record of distribution, security classification.

(c) The source data and tools used to transform information, along with the resulting documentation is placed under configuration control in accordance with the Configuration management process.

(C) Publish, distribute or provide access to information and information items to designated stake holders.

(a) Information is provided to designated stakeholders parties in an appropriate form, as required by agreed schedules or defined circumstances.

(D) Archive designated information.

(a) Archive is done in accordance with the audit, knowledge retention, and project closure purposes.

(b) The media, location and protection of the information are selected in accordance with the specified storage Information is provided to designated stakeholders

(E) Dispose of unwanted, invalid or unverifiable information.

(a) This is done in accordance with organization policy, and security and privacy requirements.

206. Measurement Process

1. General

The purpose of the Measurement process is to collect, analyze, and report objective data and information to support effective management and demonstrate the quality of the products, services, and processes.

2. Activities

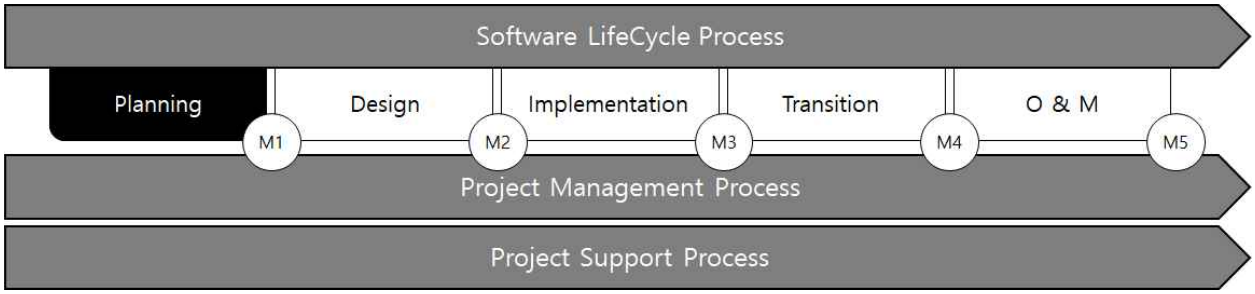
The process containing the Measurement process shall implement the following activities and tasks in accordance with applicable organization policies and procedures.

(1) Prepare for measurement
  (A) Define the measurement strategy.
  (B) Describe the characteristics of the organization that are relevant to measurement.
  (C) Identify and prioritize the information needs.
  (D) Select and specify measures that satisfy the information needs.
  (E) Define data collection, analysis, and reporting procedures.
  (F) Define criteria for evaluating the information products and the Measurement process.
  (G) Identify and plan for the necessary enabling systems or services to be used.

(2) Perform measurements
  (A) Integrate procedures for data generation, collection, analysis and reporting into the relevant processes.
  (B) Collect, store, and verify data.
  (C) Analyze data and develop information products.
  (D) Record results and inform the measurement users.
    (a) The measurement analyses results are reported to relevant stakeholders in a timely, usable fashion to support decision making and assist in corrective actions, risk management, and improvements. ⚓

CHAPTER 5 SOFTWARE LIFE CYCLE PROCESS

Section 1 Planning Process



101. General

1. The planning process identifies stakeholders who are involved with the integrated software throughout the software life cycle and identifies their needs and requirements.
2. The planning process defines the integrated software with sufficient detail to enable safety review and integrity level assessment, taking into account the needs and requirements of stakeholders.
3. The purpose of planning process is to complete ConOps, including the architecture, standards, descriptions and requirements required by the system integrator (SI) to begin the development phase and identify the suppliers of the Human Machine Interfaces (HMIs) and integrated systems connected to the package.
4. The planning process establishes an integrity level (IL) for the function, which is applied to the appropriate software module in the development process.

102. Activity

During the planning process, this process identifies stakeholders and identify and assess the requirements for integrated software configuration. The activities of this process were developed with reference to IEEE 12207-1-2008 Second Edition, 2008-02-01, IEEE Systems and Software Engineering-Software Life cycle Process.

No.	Activity
Owner	
1	Assign roles and responsibilities, Owner's team members, Users, and SI
2	Assign team member to Owner's team members
3	Update of entire project and general system requirements
4	Development of MOC Procedure for Integrated Control System
5	Development Process Tracking with SDLC
6	Coordination of work, designing conflict resolution
7	Identify integrated system components
8	ARMS consideration
9	Manage safety review, provide Result Documents
10	Provide integrity level definition
11	Independent operating means of essential systems from integrated systems
12	Assign IL Numbers to All Functions of ISPM Control System
13	Select verification method
14	Incorporate Suppliers V&V Reports &/or V&V Plans for packages
15	Develop and provide ConOps for review
16	Report of consolidated comments from ConOps Review
17	Recommended Matrix
18	Provide support information to SI during the planning process
19	Choose lifecycle Management for Integrated Systems
20	Grant authorization to Proceed to Implementation process
User	
1	Assign team member to User
2	Assign roles and responsibilities to User's team members
3	Support Owner with tradeoffs, conflict resolution
4	Support minimum requirements and design
5	Participate in safety review
6	Participate in Integrity Level assignment meetings
7	Support Owner and SI with information requests
8	ConOps Review
9	Provide component description of integrated system
10	Provide manual of functional activity during normal, degraded or failed condition

No.	Activity
SI	
1	Collect requirements from owner
2	Assign Integrator's senior technical member
3	Provide current ISO9001 or CMMI Level 2 Certificates
4	Development process tracking with SDLC
5	Collect subcontractors constraints
6	Design tradeoffs, conflict resolution
7	Provide to organizations when a canonical integration model has been developed
8	Support Owner with identifying all integrated system functions
9	System requirements analysis
10	Participate in a safety review meeting
11	Assist Owner with IL assignment
12	System integration architecture design
13	Obsolescence plan for hardware
14	Obsolescence plan for Software
15	Review selected verification method
16	ConOps Review
Supplier	
1	Provide equipment restrictions or constraints to the requesting organization
2	V&V report for packages connected to the ISPM control system
3	V&V Plan for Packages Connected to ISPM Control Systems
4	Provide current ISO 9001 Certificate
5	Provide to organizations when a canonical integration model has been developed

102. Planning process development

1. Adjustment, identification, and conflict resolution of design work (integrated system for suppliers) shall be documented. The standards, safety, security and human factors used shall be documented. It is recommended to manage the configuration of documents resulting from the analysis of the above factors.

2. The basic integration model provides a common basis for communication between relevant software modules in integrated software, helping to identify problems among stakeholders and determine solutions.

(1) It is recommended that SI define the basic integrated model used throughout the project and provide a basic integrated model to all stakeholders and suppliers early in the planning phase.

103. Integrated Model Requirements Analysis

1. The SI shall analyse the requirements of the integrated model. An analysis of the requirements of the integrated software is an activity for the development of ConOps and focuses on the compromises involved in establishing the overall requirements of the integrated software.

2. The following shall be documented..

(1) Functional requirements, characteristics of the entire system
(2) Accessibility
(3) Reliability
(4) Maintenance
(5) Safety

3. Additional considerations for reliability, accessibility, maintainability and safety (RAMS) are as follows.
   (1) Security
   (2) Human Factors Engineering Interface Requirements
   (3) Design constraints
   (4) Maintenance
   (5) Qualification requirements
4. The requirements of the integrated model shall be evaluated by considering as follows:
   (1) Traceability
   (2) Consistency
   (3) Testability
   (4) Feasibility of operations and maintenance

104. Integrated Model Requirements Analysis

1. Integrated model architecture design is an activity for ConOps development. The integrated model architecture design activity creates the system's top-level architecture. This architecture identifies and enables grouping. Recommended grouping configurations are as follows.
   (1) Hardware
   (2) Software
   (3) Manual operation items
2. All software requirements shall be presented in a traceability matrix.
3. The recommended criteria for evaluating integrated model architectures are as follows.
   (1) Traceability
   (2) Consistency
   (3) Appropriateness
   (4) Feasibility

105. Risk management

Safety reviews of defined functions shall be performed to facilitate identification of critical functions, such as essential and safety functions.
The technologies used for the integrity level (IL) assessment in the ANSI / ISA-84 and IEC61508 processes are available on demand. Safety reviews can be combined with reviews of other safety and operational possibilities, hardware FMEA or software FMECA.

1. Safety Review and New Technology

(1) SIS Safety System
Integrated or unintegrated SIS safety systems shall comply with ANSI / ISA-84 or IEC61508 for safety integrity level (SIL) assessment.
   (a) When ANSI / ISA-84 or IEC61508 is used for safety systems, the IL evaluation does not apply to SIS functions.
   (b) This guidance does not provide procedures for specifying SIL(according to IEC61508 or ANSI / ISA-84) or IL(according to ISPM) numbers.

(2) Safety review
Safety reviews shall be carried out on integrated systems and associated packages, units and connected equipment. It is recommended to carry out safety reviews in the presence of SI, owners, users, shipbuilders and the Society.

(3) Review of ConOps
   (a) The SI and User shall review ConOps. review comments and recommendations sall be documented. When the SI has developed ConOps, owners and User shall review ConOps.
   (b) The review comments shall be submitted to our Society.

(4) new or untested technology
New or untested technologies may entail additional risks. New technologies may be hardware, mechanical equipment, interface protocol, or software module coding.
   (a) A new essential system or essential functions shall be given at least an IL2 level of integrity.
   (b) The new SIS function shall give the minimum integrity level of IL3.
   (c) New non-essential systems and non-SIS functions shall be given at least an IL1 level of integrity.

2. Integrity Level (IL) evaluation

The integrity level (IL) shall be evaluated based on the results of failure of the function. The level of integrity indicates how important the function is to the operation of the system. The IL number indicates the confidence that the owner and/or the User want the function to function as specified, including the fail-safe situation. The IL number shall be assigned to the owner, taking into account the opinions of the User and SI, taking note of the requirements of the International and National Standards, and the Preference Association.

The level of integrity derives from the expected reliability of performance and the severity of the failure results.

(1) The IL evaluation is as follows:
   (a) Safety result
   (b) Environmental results
   (c) Business impact (optional)

(2) The functions shall be evaluated in the categories of safety and environment. The business impact is considered optional. The business impact is optional and not reviewed by our Society. Potential safety and environmental impacts shall be considered when assessing functions for IL designations. Designation of levels of integrity may increase due to the impact of the company's risk tolerance and potential business.

(3) There are four levels of integrity (IL). Each has increasingly serious consequences from IL0, which is considered to have little or no impact on safety, environment or business outcomes, to IL3, which can have a significant impact on safety, environmental or business issues. ISPM control systems apply the highest IL of software functions. A control system consisting of functions listed in IL0 to IL2 and a control system with one software function called IL3 shall be designated in all functions as IL3. However, an IL3 rating may not be assigned to all functions within the ISPM control system unless a higher IL is required for other functions depending on the outcome of the risk analysis.

(4) Important systems and functions:
   (a) Important systems and functions are specified as IL2 or IL3. Critical systems may be assigned IL1 in consideration of justification, redundancy, etc.
   (b) SIS shall be designated as IL3 by IEC61508 or ANSI/ISA 84, IMO and the owner's selective demand for non-SIS functions or systems. The SIS system may be assigned IL2 in consideration of justification, redundancy, etc.
   (c) ESD systems utilizing software functions shall be IL3. ESD systems may be assigned IL2 in consideration of justification, redundancy, etc.

   Implementation of IL assignments at the planning process may scrutinize individual functions and systems as a whole. The goal of the IL allocation is to provide a reliable integrated system. Risks shall include scheduling, hardware and/or software obsolescence, and reliability (quality) of software development. The assigned IL shall be applied to the software module (code) of the function.

(5) The IL of the overall integrated system shall be applied in the same way as the highest IL number assigned among functions controlled by the ISPM control system.

(6) The owner and the User shall provide to our Society the criteria used in the evaluation of the IL of the function. Owners and User may improve the terms used above to meet the Company's risk tolerance.

Table 1 Integrity level table

IL	Potential Consequences		
	Safety	Environmental	Business
0	Negligible[1)]	Negligible[1)]	Minor impact on operation. Might affect supporting process system but not main process system.
1	Might eventually lead to marginal[2)] safety incident	Might eventually lead to a marginal[2)] environmental incident	Might lead to maintenance shutdown of non-critical system. Main process continues to operate.
2	Within a short time could cause critical[3)] injury, lost time, accident or loss of a life.	Critical[3)] environmental impact	Shutdown of main system, excessive time for repair.
3	Immediate and Catastrophic[4)] lost time injuries, or multiple loss of life.	Catastrophic[4)] environmental impact	Significant repair time or loss of the marine or offshore asset.

(Note)
1) Negligible: first aid injury or illness, termination of non-workable systems or degradation of performance or User discomfort.
2) Marginal: Lost time damage or disease, degradation of ship or unit performance, or some financial loss or social loss.
3) Critical: Permanent damage or multiple roast time damage, job critical system damage or serious financial loss or social loss.
4) Catastrophic : Loss of life, loss of assets, loss of system safety or security, or extensive financial or social loss.

3. IL Assignment Function Document Requirements

(1) IL0

In general, control and monitoring of non-essential and relatively insignificant functions is required. The User monitors important or essential functions that do not use data in safety or in algorithms (software modules) of critical and critical software modules without using information to make critical decisions.

(a) A description of the operational or normal state of the function (not required for degraded or failed conditions) shall be given in ConOps.

(b) Data displayed in HMI for the User to make an essential or important decision is not IL0. This data can be applied to drilling where human experience and knowledge are used for safe operation of the process.

(c) Interface Description

ARMS requirements for testing, recovery, and restart shall be specified without interfering with the redundant execution system.

(2) IL1

In general, monitoring and/or control of non-essential functions

(a) A description of the normal (operational) condition of the function should be specified in ConOps.

(b) A description of the failure condition (failure condition) shall be given in ConOps.

(c) Interface Description

(d) ARMS requirements for testing, recovery, and restart shall be specified without interfering with the redundant execution system.

(e) Specify testing, repair and restart requirements without interference with redundant operating components or components.

(f) Aging risk is defined and options are selected for ARMS with alternative components or parts.

(3) IL2

Essential and critical systems and features :

(a) A description of the normal state of the function shall be given in ConOps.

(b) A description of the degraded state of function (state) shall be given in ConOps.

(c) A description of the failure condition (failure condition) shall be given in ConOps.

(d) Interface Description

(e) ARMS requirements for testing, recovery, and restart shall be specified without interfering with the redundant execution system..
(f) Specify testing, repair and restart requirements without interference with redundant operating components or components.
(g) Risk of aging is defined and option is selected for ARMS with alternative components or components.

(4) IL3

Essential, SIS and critical systems and features:

(a) Description of steady-state requirements shall be given in ConOps.
(b) A description of the degraded state of function (state) shall be given in ConOps.
(c) A description of the failure condition (failure condition) shall be given in ConOps.
(d) Interface Description
(e) Requirements for ARMS. Specify testing, recovery, and restart requirements without interrupting the redundant execution system.
(f) Specify testing, repair and restart requirements without interference with redundant operating components or components.
(g) Risk of aging is defined and option is selected for ARMS with alternative components or components.

4. Software quality management

(1) The owner shall specify the verification method to be followed. There are three options for verifying integrated system software. At the V & V level, system software shall at least function as specified in SRS and SDS. When the method of the owner's choice is possible, all three verification methods may be used to verify IL2 and IL3 function.
(a) Closed Loop
(b) Software-in-the-Loop
(c) Hardware-in-the-Loop
(2) The selection of the verification method includes consideration of the complexity of the function and associated software modules, the level of integrity of the function, and the quantity of supplier packages to be integrated. The development of the simulation is carried out in parallel with the development of the integrated system software, not the conclusion of the software development.

5. Aging plan

(1) SI is to provide a high level of hardware Aging plan for integrated systems. Accessibility, reliability, maintainability and safety (ARMS) shall be considered in planning.
(2) The SI is to provide a high level of software Aging plan for integrated system software.

106. Concept of operation(ConOps)

ConOps shall be reviewed by owner (if not developed by owner), Shipbuilder, User, SI (if not developed by SI) and our Society. ConOps shall contain the information listed in **106. 1**. Review the period in accordance with the contract or other agreement with the contracting party.

1. General

(1) The overall scope and goals of the project
(2) Supplier Package (if applicable)
(a) the part number of the manufacturer or SI or supplier
(b) Model number (if possible)
(c) Interface Protocol
(d) Constraints
(3) Functional description:
(a) Sufficient detail to develop Design process documents.
Integrator can enter the word "sufficient." Details of the common and well understood functions may be "sufficient" in a single line of statement.
(b) All functions shall have a description and an assigned level of integrity (IL0 to IL3).
(c) Failure safety status.
(4) The number and description of the human machine interface shall include as follows
(a) Manufacturer
(b) Model number or SI or Supplier's part number (if possible)
(c) Interface Protocol
(d) Constraints

(5) The number and description of the human machine interface shall include as follows
  (a) Quantity of network or direct connection to ISPM control system
  (b) Interface protocols for interface networks, control systems and/or equipment
  (c) Restrictions on interface networks, control systems and/or equipment
(6) Major verification methods

2. Definition of project scope

Owners who have comments from the User shall specify the purpose and scope of the integrated system in ConOps.

3. Main components and boundaries of integrated systems

(1) Major packages or components shall be pre-selected at a high level of integrity. At this point, SI and / or owners are aware that to meet ConOps, they need an interface or a package of connected equipment from other suppliers. Dynamic Positioning System will interface with Power Management System from Vendor Xyz. ConOps includes a list of interfaces or connected equipment and HMI.
(2) Redundancy of control system components does not reduce the level of functional integrity if redundant control systems run the same software. This includes the components associated with the integrated system. When the software is defective, the functions under control and associated components or equipment may fail because the primary and backup control systems are executing the same code.
(3) When redundancy consists of two technologies (PLC control and other means of control or controlled shutdown, mechanical, hydraulic, etc.), the IL number may be lowered

4. Constraints

(1) Constraints shall be identified and described in the concept of operating documents. This may include:
  (a) Supplier's package restrictions
  (b) Current existing technology, new technology to be applied;
  (c) Software restrictions (if known)
  (d) Network or continuous communication limitations of the provider package (function) (if known)
  (e) Evaluate the expected software function risk
    Supplier's package shall be able to communicate using Modbus at 9600 BPS leading the demand for additional hardware modules for the integrated system. Process control groups may propose advanced controls using unproven software modules (fuzzy logic, model predictive control), but risks are judged too high by the owner, resulting in simpler, more proven controls being used.
(2) Supplier restrictions shall be eased as necessary

107. Output

1. The main output of the planning process is ConOps according to **105.** The owner may request information from the SI or Shipbuilder for ConOps development if necessary. ConOps shall include at least the following.

(1) Provide traceability of functions for use in SDLC and identify functions.
(2) Include the recommendations of a safety review in the description of the function and in ConOps(If applicable).
(3) Assign the integrity level for each function.
(4) Identify the components of the integrated system
(5) Define alarm management policy.

2. In ConOps, it is recommended that functions, activities and outputs be traceable in the subsequent SDLC phase.

3. The definition of functions and interfaces is an important part of ConOps, along with the package data from the provider.

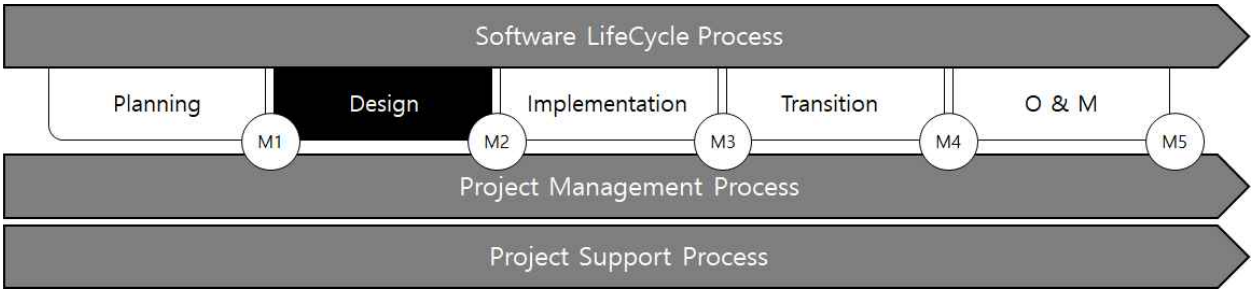
108. Planning Process Milestone (M1)

1. The components of the integrated system are identified.

2. A safety review report is submitted.

3. ConOps is updated with safety reviews and FMEA. (Approved Recommendations)
4. The level of integrity shall be assigned to the function.
5. The Change Management Procedure (MOC) applies to ConOps.
6. Consultation with potential subcontractors.
7. Choose the main V & V method of ISPM control system
8. Supplier's V&V plans are provided for packages of IL2 or IL3 ISPM control systems and exceptions are specified in ConOps. V & V reports may be delivered at the Design process. V & V reports need not be produced by all suppliers for IL2 and IL3 systems to begin development.
9. Supplier's V & V reports on IL1 ISPM control systems associated with packages are provided and exceptions are given in ConOps. Verification IL2 and IL3 functions are demonstrated by our Society and V & V reports may not be available at the time of ConOps development. V & V reports may be delivered at the Design process. V & V reports need not be produced by all suppliers for IL2 and IL3 systems to begin development.
10. The project and the overall schedule of the updated integration system are completed.
11. Hardware and software aging plans are included in ConOps.
12. ARMS considerations are specified in ConOps.
13. Compromise of design considerations is completed and included in ConOps.
14. ConOps has been reviewed by the User, SI and our Society. Review the period in accordance with the contract or other agreement with the contracting party.
15. List of equipment from the connected supplier.

Section 2 Design Process



201. General

1. The design process focuses on the specification, architecture and design of integrated control software.
2. The design process uses ConOps to provide guidance related to system characteristics. In accordance with principles and quality criteria that were completed early in the design process, the content of ConOps is used as guidance for the specification, architecture and detailed design of the software. The outputs of the design process form the basis for the implementation of integrated control software
3. When new restrictions are identified, they shall be documented and discussed with the owner. Mitigation of constraints shall be documented and ConOps updated in accordance with Change Control (MOC) procedures. Documents in the design process will be reviewed based on ConOps and will become verification acceptance documents upon owner's approval.

202. Activity

The design process shifts from system-level description and design to software-level specifications, architectures, and designs. In this process, the programmer organizes the modelling relationship and prepares the software coding through two documents. The activities of the design process have been developed with reference to the IEEE 12207-1-2008 Second Edition, 2008-02-01, IEEE Systems and Software Engineering - Software Lifecycle Process, as follows:

No.	Activities
Owner	
1	Update ConOpns according to MOC. provide to the Society with SRS and SDS
2	Review and approve SRS and SDS
3	Participate in FMECA
4	Safety review of added functions for suppler's packages
5	Grant Authorization to proceed to implementation process
User	
1	Review SRS and SDS
2	Owner and SI activity support
SI	
1	SI team member assignment
2	Update canonical integration model(if developed), pass to Suppliers
3	Enhancement and detail of functions in SRS
4	Enhancement and detail of functions in SRS
5	Added V&V scenarios for operational and non-operational from ConOps
6	Internal functionality may be tracked through ConOps and safety reviews
7	V&V Plan and/or V&V Report for Supplier's packages
8	SI to facilitate and participate in Software Control System FMECA meetings
9	Provide Software Control System FMECA report(s)
10	SI to update and approve the SRS and SDS per the functional FMECA and comments from reviews
11	Supplier's package documentation
12	Variance from standards report(s)
13	Publish SRS
14	Publish SDS
15	Provide consolidated SRS and SDS review report
Supplier	
1	Support the SI activities
2	If not previously provided, current ISO 9001 certificate.
3	Participate in the software FMECA
V&V	
1	Draft initial V&V plan

203. Software requirements analysis

1. Stakeholder requirements are analyzed to translate the stakeholder representation based on the requirements for the desired services into the technical representation of the product to which they will be provided. This process establishes a representation of the integrated software that satisfies the requirements of stakeholders within the tolerance of the constraints and does not imply any particular implementation. The result is a set of measurable system requirements that specify, from the developer's point of view, what characteristics and how much the system must possess to meet stakeholder requirements.
2. In the software requirements analysis process, functions are separated into software modules. The specification of the software module includes functional capability and performance details. In addition, consideration shall be as follows.
   (1) Interface outside the software module
   (2) Qualification requirements
   (3) Safety and environmental specifications;
   (4) Operation and maintenance
   (5) Security requirements
   (6) Human factors (human engineering)
   (7) User documentation

204. Software Architecture Design

1. The purpose of the architectural design is to find solutions that meet the integrated software requirements as follows.
   (1) The area of the solution is divided and defined, but expressed as a set of manageable, conceptual and ultimately feasible sets of separate problems.
   (2) Identify and explore one or more implementation strategies at a level of detail consistent with the technical and commercial requirements of the system and their risks, i.e. the requirements as a whole.
   (3) The architecture design solutions are defined from this, expressed in the form of requirements regarding the set of system components to form the system.
   (4) The design requirements defined as a result of performance provide the basis for validating the implemented system and form the basis for planning assembly and verification strategies.
2. During software architectural design activities, system integrators shall:
   (1) Translate software requirements into top-level architectures that identify software components for each software module;
   (2) Assign each requirement of the SRS to one or more software modules.
   (3) Document the requirements and software modules in the traceability matrix;
   (4) Document the architecture of the software module
   (5) Development
      (a) Design of top-level external interfaces;
      (b) Top-level design for all databases;
      (c) Drafting user documents
      (d) Requirements for pre-testing
3. It is recommended that the software architecture design conforms to the criteria recommended by the IEEE 12207 standard.
   (1) Traceability to the requirements of the software item;
   (2) External consistency with respect to the requirements of the software item;
   (3) Internal consistency between software components;
   (4) Conformity with the design methods and standards used;
   (5) Feasibility for detailed design
   (6) Feasibility of operation and maintenance;

205. Risk Management

In the design process, there are two main aspects of risk, project and operation

1. Project risk management

   In order to guide project managers on potential issues related to schedule, capacity and software

quality, the design process recommends collecting, measuring and managing the matrix. The data in the indicators are internally used by System Integrators (SI) to manage software quality.

2. Operation risk management

Operational hazards are identified through safety reviews, failure mode effects and materiality analyses (FMECA) and other reviews. New technologies may be identified and presented at the design process.

3. Supplier Package Document

Supplier's package documentation shall consider the overall plan.

4. Software control system FMECA

The purpose of FMECA is to ensure that failure of a single software module does not result in failure of other software modules or loss of control systems.

(1) When IL2 and IL3 are assigned to an ISPM control system, a software focused functional FMECA shall be performed

(2) The control system FMECA shall provide traceability of the software module to the relevant functions of the traceability matrix.

(3) The control systems FMECA in IL2 and IL3 shall be performed including interfaces with integrated control systems that may affect their functions.

(4) SRS and SDS shall be updated in accordance with FMECA recommendations.

5. New or unproven technology

New or unproven technologies entail additional risks. New technologies may be hardware, mechanical equipment, interface protocol, or software module coding.

6. New features added in the design process

(1) Owner must update ConOps.

(2) a safety review of new functions shall be made and the results shall be documented;

(3) Where a function has been added after the software control system FMECA, the FMECA shall be carried out to address all risks posed by new functions and related software modules.

206. Software Requirements Specification (SRS) and Software Design Specification (SDS)

1. Software Requirements Specification

The ISPM Software Requirements Specification (SRS) is a specification for the integration of specific software products, programs, or sets of programs so that they may perform defined functions in a given environment. The SRS shall be reviewed by the Owner and User organization and our Society. Review the period in accordance with the contract or other agreement with the contracting party. The SI has discretion in the SRS regarding the ownership of software functions or the inclusion of intellectual property. The SI shall describe its function in technical terms.

(1) The SRS should address at least the following:

(a) Functionality: describe the purpose of the control system and software in the top-level terms.

(b) External Interface: describe the software interaction with the user (user interface), system execution hardware, external interface system support hardware, and external interface system support software.

(c) Performance: Describe the availability of the control system and the speed of navigation if the application, recovery or reboot time is fast enough.

(d) Attribute: Describe in terms of the code reusability, maintainability and security.

(e) Design Constraints: Describe the constraints imposed on this implementation process.

(f) Other: Describe the standards that apply to the software implementation, the execution hardware, the software language used in the implementation, database integrity policies, resource limits, and the operating environment, etc.

2. Software Design Specification

ISPM Integrated SDS describes the design of integrated components of the system. Common content includes system or component architectures, control logic, data structures, I/O formats, interface descriptions, and algorithms. SDS shall be reviewed by the owner, the User organization and our Society. Review the period in accordance with the contract or other agreement with the contracting party. The SI has discretion in SDS regarding the inclusion of software functional ownership information or intellectual property rights of the SI. The SI shall describe the function in detail.

(1) Integrated software detailed design process

Software detailed design is performed throughout the implementation phase, starting with soft-

ware requirements analysis at the design process. Software integration detailed design is an activity to refine the software component integration of the software module to a lower level consisting of unit integration software to be coded. SDS is written during the design process so that SI developers (coders) may clearly understand the exact nature of the work the software shall perform.

(2) The detailed design and test requirements of the software shall be evaluated using criteria recommended by the IEEE 12207 standard as follows
(a) Traceability to the requirements of the software item;
(b) External consistency with Architecture Design
(c) Internal consistency between software components (modules, programs)
(d) Appropriateness of the design methods and standards used;
(e) Feasibility test
(f) Feasibility of operation and maintenance

207. Output

1. Software Requirements Specification (SRS)

The SRS shall include at least the following, taking into account the provisions of paragraph **1.** of **206.**
(1) Results of software requirements analysis activities
(2) Work process flow diagram
(3) Criteria and Standards
(4) Reconfigure a software module with related functions as a sub-software modules that make up the required functions
(5) Preliminary test requirements
(6) Functional test requirements
(7) Top-level External Interface Specifications
(8) The functions shall be traceable in ConOps.

2. Software Design Specification (SDS)

The SDS shall include at least the following, taking into account the provisions of paragraph **2.** of **206.**
(1) Top-level design of all databases
(2) Design for internal and external interfaces
(3) Design of user documents in advance
(4) Design evaluation of a software architecture
(5) Software design constraints
(6) The functions shall be traceable in ConOps

3. Initial V & V Plan Established by V & V Organization

4. Changes in standard reports (if changes occur)

208. Document Maintenance

SRS and SDS shall be reviewed for consistency with ConOps by Owner, User organization and our Society. Review the period in accordance with the contract or other agreement with the contracting party.

1. The SI shall update the SRS and SDS according to the review comments of the control system FMECA.

209. Design Process Milestone M2

Some design process activities extend to the implementation process.

1. Interface or integration between integrated system components shall be clearly defined.

2. A detailed description of the functional component shall be completed.

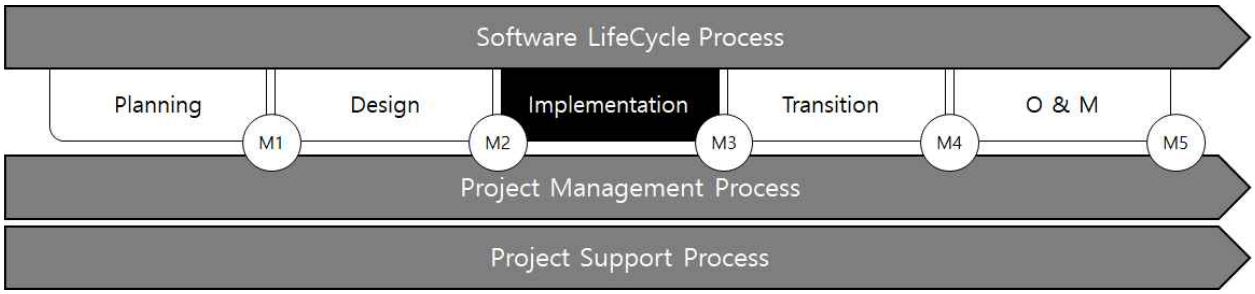
3. SRS and SDS shall be completed consistent with ConOps documentation.

4. Integrity levels shall be sorted according to the scope of the Concept

5. Software and Full Project Schedule Updates

6. Authorization to proceed from Owner to implementation process
7. Changes in standard reports
8. Issue SDS and SRS (issue Implementation process)

Section 3 Implementation Process



301. General

1. The implementation process aims to realize the integrated software specified through SRS and SDS and to assemble the software components to match the architectural design. This process objectively demonstrates that all features of SRS and SDS work satisfactorily in the integrated software and achieve their intended use in the operational environment conceptualized in the planning process.
2. The implementation process provides the information necessary for remedial work when the implemented integrated software is not satisfied with the defined requirements, and performs remedial activities against the requirements of stakeholders. Once the calibration is complete, the stakeholder confirms.

302. Activity

The implementation process implements integrated software through the integration of SRS and SDS segmentation, software module coding, and COTS product configurations, and establishes verification and verification plans to perform unit tests, integration tests, and software system-level acceptance test. Activities in the implementation process are described in ISO / IEC / IEEE 12207 First Edition, 2017-11, System and Software Engineering-Software Lifecycle Processes and ISO / IEC / IEEE 15288 First edition 2015-05-15, Systems and Software Engineering- Software Lifecycle Process ", as follows.

No.	Activities
Owner	
1	Change Request Management for MOC Policy
2	Track risk
3	Project progress monitoring for the plan
4	SI Activity Support
5	Review the overall test results of the SI
6	Review and approve updates for SRS and SDS
7	ConOps review for updates in SRS and SDS
8	Reissue ConOps when programming is 90% complete
9	Review V & V Plan
10	It is recommended that the Owner participate in the V&V verification activities.
11	When a Moderate Defect is detected on an IL2 assigned function, a safety review is to be performed on the proposed workaround. solutions are not permitted for IL3 assigned functions.
12	Defect Rating Review
13	Review V & V Report
14	Review and approve V & V plans
User	
1	Change Requirements Management for MOC
2	SI activity support
3	Review of the overall test results
4	Review updates for ConOps
5	Review updates for SRS and SDS
6	Review V&V Plan
7	The User's Recommendation to Attend V & V Activities
8	V&V Plan
9	V&V Report
10	Provide Information on defect ratings by the V & V organization

No.	Activities
SI	
1	Monitoring of issues among stakeholders, suppliers and subcontractors.
2	Issue contracts to subcontractors
3	Subcontractor Monitoring
4	Peer Review of Coding
5	Management of Development Activities
6	Review and initiate MOC (requirement changes)
7	Provide integrated test results for review
8	Forecast to complete reports
9	Deliverable summation reports noting any open issues
10	Provide updated or current SRS and SDS
11	Issue schedule update requested by owner
12	Review V & V Plan
13	Report any variance to standard
14	Attending V & V Verification Activities
15	Software is locked after passing verification tests
16	When a Moderate Defect is detected on an IL2 assigned function, a safety review is to be performed on the proposed workaround. solutions are not permitted for IL3 assigned functions.
17	Correct coding defects
18	Provide information to rank defects in V&V organizations
Supplier	
1	Review and initiate MOC (requirement changes)
2	Development and delivery of contracted package equipment and related software
3	Develop and provide the required documentation
4	Provide requested information to support anomaly identification

No.	Activities
V&V	
1	Monitor and include approved SRS and SDS changes
2	V & V Plan
3	Issue V&V plans during and after review, during implementation
4	V&V's project management to monitor V&V configuration management for plan
5	Simulation software development
6	Simulator software or configuration management peer review
7	Generate integrated reports from all V & V plan comments
8	Simulation Verification
9	Simulation configuration management peer review
10	Provide V&V plans for comments and approved V&V plans
11	V & V Plan Execution
12	Note the deviation from the V & V plan
13	Create a V & V report of all the anomalies discovered and consolidate comments from other reviewers.
14	Results of the virus scan
15	The simulator shall include component data (monitoring and control) commands connected to the integrated system, signals, software interlocks and alarms as needed.
16	Generate Intermediate V & V Report
17	Support the safety reviews of the proposed moderate defects solution for IL2 assigned functions
18	Rank defects
CS	
1	Review V&V Plan
2	Monitor SI and subcontractors for compliance with the guide
3	Perform independent selected design reviews
4	Review ConOps, SRS, and SDS
5	Review V & V Plan
6	Monitor V & V organization when executing the V&V plan
7	Review Interim V & V Report
8	Review Final V & V Report
9	Review the results of virus scans
10	Provide information about ranking of defects
11	Witness the verification

1. The system integrator is managed in the implementation process as follows.
   (1) The owner shall correct, review and approve the errors or descriptions identified in the SRS and SDS before writing the code.
   (2) The SI shall provide documentation certifying that all software modules developed by SI have been reviewed and unit tested.
   (3) Once the unit modules of the integrated software have been reviewed, they shall be placed under configuration management and integrated into the baseline project.
   (4) After all individual software modules have been successfully integrated, a SI integration test of comprehensive software system level shall be conducted to ensure that the software meets the requirements of SRS and SDS.
   (5) The owner and / or DCO shall periodically review the software development activities of the system integrator (SI) and / or contractor. The results of the review are to be notified to the Society.

303. Software coding and testing

This activity consists of development of custom software modules and the use of library modules, integration of COTS products and interfaces. SI completes the software architecture using models, diagrams and functional specifications, SRS and SDS. Based on SRS and SDS, the programmer makes the software module code of specification content and sets the order of software development. Internal test of individual software modules is performed.

1. A programmer of SI who is not involved in the functions assigned by IL2 and IL3 shall have a peer review of the integrated software module code. A peer reviewer shall evaluate an integrated software module using standard methods for
   (1) Correctness: SRS, SDS functions work correctly.
   (2) Complete: there is no missing function.
   (3) Clearness: The logic is clear and not unnecessarily complex.
   (4) Maintenance: Source code logic is easy to read and annotate. For COTS configurations, clear information about integration, registers, and configurations shall be recorded.
   (5) Efficient: There shall be no unacceptable performance bottleneck.
2. During the final detailed design, coding and unit/database testing, the SI recommends that the results of the assessment be documented as follows.
   (1) Traceability for the requirements and design of software items
   (2) Consistency between unit requirements, standard integration model
   (3) Consistency between unit requirements, standard integration model
   (4) Unit test range
   (5) Feasibility of software integration and testing;
   (6) Feasibility of operation and maintenance;

304. Software Integration

This activity develops an integrated plan that details the level of integration testing to be achieved. The test plan aims to ensure that the code developed complies with the requirements, architecture and specifications developed in the previous process. An integrated plan is part of the V & V plan.

1. It is recommended that the integrated plan include test requirements, procedures, data, responsibilities and schedules.
2. Each requirement shall be subjected to a series of test types, test cases and test procedures.
3. Each test case shall be documented and traceable to the requirements of the SRS and SDS.
4. The SI shall evaluate the integration plan, test results and user documentation as follows.
   (1) Traceability to system requirements
   (2) Consistency of system requirements
   (3) Consistency between unit requirements
   (4) Scope of testing for the requirements of software items
   (5) Conformity with the test standards and methods used;
   (6) Conformity with expected results
   (7) Feasibility of a software qualification test
   (8) Feasibility of operation and maintenance

305. Software Integration Test

The SI shall test all software modules internally for SRS, SDS requirements (function and integration requirements) through peer review or other means, and it is recommended that an integrated test be performed to ensure that each software module interacts correctly with the rest of the software whenever software module is integrated into the baseline.

1. The detailed design and test requirements of the software are to be evaluated as follows.

(1) Test range of software item requirements
(2) Conformity with expected results
(3) Feasibility of a software acceptance test
(4) Feasibility of operation and maintenance

306. Document Maintenance

Updates to ConOps, SRS, and SDS shall be reviewed at the Owner, User organization. ConOps shall be approved by the Owner. The results of the comprehensive test shall be reviewed by the Owner, the User organization. Review the period in accordance with the contract or other agreement with the contracting party.

307. V & V Plan

The V & V plan complies with the current V & V requirements of SRS and SDS.

1. Explanation of V & V plans

The V & V plan describes the purpose, goals, and scope of software V & V efforts. The plan follows the requirements listed in the current SRS and SDS.

(1) Satisfy standards, practices and conventions;
(2) The scenarios shall be traceable to the current SRS and SDS.
(3) The V & V plan shall include a process for collecting evidence that the software meets the requirements of the software system.
(4) It is recommended that ConOps be reviewed to make it easier to understand the intent of the requirements listed in the current SRS and SDS.
(5) The V & V plan is a document that specifies the scope, approach, resources and schedule of testing activities.
(6) The design of the test is a document that specifies the details of the test methods for the software module.
(7) The V & V plan is a document that specifies a series of tasks for testing.
(8) Document results and create a V & V report.

2. V & V plan approval

Owner, User and SI organizations and our Society shall review the V & V plans. The owner and our Society shall collect the reviewer's comments and approve the V & V plan. Review the period in accordance with the contract or other agreement with the contracting party.

308. V & V Method

1. The main verification method of software is as follows.

(1) Closed loop verification (if specially considered)
(2) Software in the loop verification
(3) Hardware in the loop verification

2. The minimum objective of V & V process is to verify software performance as specified in SRS and SDS. Simulation shall have sufficient accuracy to test control system software.

3. When simulation is necessary, it includes data from connected components (monitoring and control), commands, signals, software interlocks, and alarms with integrated systems to identify the code of the integrated system, and clearly show the control system software to stakeholders as specified in SRS and SDS. The intention is to identify an integrated control system, and the software of the connected components need not be checked.

4. Closed loop verification

The inputs and outputs of computer-based integrated systems are simulated with the minimum interactions of other integrated components. closed loop verification may require changing the register value of the program to evaluate the integrated system software response. A comprehensive understanding of the software code and its functions is required, which limits the application to a simple system. special considerations and prior approval of our advance are required before verification of closed loop is carried out. SI, Owner and User shall provide documentation that these closed loop verification requirements have been met.

(1) Requirements for verification of closed loop ver:
  (a) Simple integrated or stand-alone computer-based systems.
  (b) 3 or fewer integrated components;
  (c) complex software modules associated with a few complex functions.
  (d) The integrated system does not control essential or safety functions. If essential or safety functions are monitored by the system and this data is used for human decision making, then closed loop testing may not be appropriate.
  (e) The IL1 function does not result in safety or environmental effects.
  (f) The system does not have IL2 or IL3 functions.

5. Software in the roof verification

Control system software is running on native hardware and simulations are running on the same or separate computers. it shall have sufficient accuracy, check the code of the integrated system, including the actual system, and document the stimulation results to the extent necessary. The accuracy of the simulations shall be sufficient to permit verification of the control system software for the current SRS and SDS.

6. Hardware in the loop verification

(1) Programs in the integrated system run on native hardware(CPU) with interface cards for communication between the available components and the motherboard of the simulation computer and the control system.
(2) The simulator runs on separate computer hardware connected to interface card of control system.
(3) The simulator supports emulating components of the integrated system.
(4) The simulation shall have sufficient accuracy and shall identify the code of the integrated system, including the actual system, and document the stimulation results within the required scope.
(5) The accuracy of the simulations shall be sufficient to permit verification of the control system software for the current SRS and SDS.

309. Scan for Viruses and Other Malicious Software

The V & V organization runs a virus scan in the control system software before performing all V & V activities and the scan results shall be reported to the Owner, the User, the SI and our class.

1. V & V organizations shall state that they are using the latest virus definitions available in the virus testing program.

2. Provide a virus definition number or identifier in the virus check report.

3. The SI shall state when compiled software of SI is known to contain scripts detected by the virus scanning program as potentially malicious.

(1) The SI provides the name or type of malicious software that the script was detected (spyware, Trojan horse, etc.) and the number of instances reported. This enables identification of potentially different malicious software at the Management process.

4. Where an SI, supplier or sub-supplier provides antivirus software to a control system, conflicts with the owner's security plan shall be resolved between the owner and the SI, supplier or sub-supplier.

(1) Where anti-virus software is installed in a control system, SI, Supplier or Sub-supplier recommends providing details on how and when virus definitions are updated on board.

310. V & V in the Implementation Process

1. The V & V organization is responsible for performing activities during the implementation process as follows.

(1) The V & V organization shall refine the V & V plan and Detailed V & V plans are reviewed by

the Owners, the Users, and the SI. The reviewed V & V plan report shall be submitted to our Society.
(2) The V & V organization is to peer review the V & V plan.
(3) V & V organizations shall construct simulators at the implementation process.
(4) Program the simulator.
(5) Verifies the simulator program.

311. V&V review of Simulation

1. When simulator is necessary, it includes component data (monitoring and control) commands associated with integrated systems, signals, software interlocks, and alarms, to verify the code of the integrated system as specified in SRS and SDS and clearly demonstrate the control system software to stakeholders.

2. Simulation shall have sufficient accuracy and shall reasonably include actual dynamic systems and effects to verify the code of the integrated system and the V & V organization documents the results of the verification.

3. Reasonable is defined as providing sufficient accuracy to test control system software functions and programming while providing sufficient feedback to V&V organizations that the software is operating under SRS and SDS.

4. Validity is determined by the V&V organizations with inputs from the SI.

5. Equivalence Evaluation of V & V for Simulation

Before verification, the simulation configuration shall be evaluated equally by V & V organizations for the following:
(1) Traceability to requirements using the current traceability matrix.
(2) Feasibility of simulation
(3) provide the report to the Shipbuilder, the Owner and our Society.

312. Defect Ranking

SI shall determine whether the defect is a control system code defect, a simulation code defect or a planning error based on information from the V&V, the Owner organization

1. Integrity level and fault category

Table 2 includes requirements and recommendations for correct defects or errors.

313. Verification and Verification Report (V & V Report)

1. Reports are generated by V & V organizations using traceable notation for passing or failing each function currently described in SRS and SDS. This report includes as follows.

(1) Abnormalities found in software modules.
(2) Cause of defect, error, or abnormality (if known)
(3) Impact of a defect, error, or abnormality on a function and other functions have been affected
(4) Simulation design, simulation scenario, simulation procedure, and simulation results.
(5) Differences from V & V plans. to include function identifiers, what is deviated from and why there was a deviation.
(6) Recommendations

314. Review of V & V Reports

Ther Owner and The User review V&V reports and resolve them to identify any concept error. SI corrects coding defects and our Society is to review V&V report. Review the period in accordance with the contract or other agreement with the contracting party.

Table 2
IL Ranking and Defect Categories, Requirements and Recommendations (may be required to correct Owner Defects)

IL	Requirements and recommendations				
Defect Category	Cosmetic[1)]	Minor[2)]	Moderate[3)]	Major[4)]	Critical[5)]
0	D	D	D	R	R
1	D	D	D (Review)	R	R
2	R (Essential)	R (Essential)	R (Essential)	R	R
3	R (Essential)	R	R	R	R

(Notes)
D : Correction may be delayed
D (Review) : Correction may be delayed (Review results and risks of the Owner and the User)
R (Essential) : Requires correcting and retesting if essential function, may be delayed if IL consequence are business related only. On non-essential functions, review results and risks of the Owner and the User
R : Requires correcting and retesting

1) Cosmetic Defects are the ones which are primarily related to the presentation or the layout of the data. However, there is no danger of corruption of data and incorrect values. If essential or safety functions are monitored on the system and this data is used for human decision making then Cosmetic ranking may not be appropriate. Depending upon the IL rating of the function, the Software Module may be released with the permission of the Owner and the User. HMI graphic colors may not be a Cosmetic Defect.

2) Minor Defects are defects that may or have caused a low level disruption of function. Such defects may result in data latency but not in essential, safety or IL2 or IL3 functions. The integrated system and the function continue to operate, although with a failure. Such a disruption or non-availability of some functionality may be acceptable for a limited period of time for IL1 functions. Minor defects may cause corruption of some noncritical data values in a way that is tolerable for a short period. Essential or SIS functions assigned IL2 or IL3 assigned functions are to be corrected. Non-essential and non SIS IL2 or IL3 assigned functions are to be corrected at the Owner's option. IL0 or IL1 assigned functions are to be corrected at the Owner's option.

3) Moderate Defects are major defects that have a solution acceptable to the Owner and the User. Such defects may result in data latency but not in essential or IL2 or IL3 functions. The integrated system and the function continue to operate, although with a failure. Such a disruption or non-availability of some functionality may be acceptable for a limited period of time for IL1 functions. Moderate defects could cause corruption of some non-critical data values in a way that is tolerable for a short period. Changes to the Operating Manual may be called a Moderate Defect. The Owner is to review the impact and risk of such a change. When a Moderate Defect is detected on an IL2 or IL3 assigned function, the SI is to facilitate a safety review on the proposed workaround involving the Owner, User and SI organizations. Society is to be notified of the safety review meeting. Provide report of the safety review to our Society. It is recommended that safety reviews be performed on IL0 and IL1 functions.

4) Major Defects are serious defects that have not halted the system, but have seriously degraded the performance, caused unintended action or incorrect data transmitted. There exists no acceptable (to Owner and User) solution. All Major defects are to be corrected and the control system retested.

5) Critical Defects are the extremely severe defects, which have already halted or are capable of halting the operation of the computer-based control system. Critical defects are also defects that are capable of unsafe operation of the Equipment Under Control (EUC). All Critical defects are to be corrected and the control system retested.

315. Deliverables

1. The deliverables of the implementation process include detailed code specifications and unit test results for functions assigned IL2 and IL3, integration plans and overall integration software test results. However, it is not necessary to include the actual code in the documentation at this time.

2. At least the implementation process shall have the outputs as follows.
   (1) An integrated report on the results of the test plan. Include IL2 and IL3 results
   (2) Completed integrated software module code
   (3) Updated V & V plans by verification organization
   (4) Issuing updated ConOps
   (5) Issuing Updated SRS and SDS
   (6) Integrated V & V Report Summary
   (7) Simulation Equivalence Assessment Report

316. Risk Management

1. Risk management includes project and operational risks.
   (1) Project risk management
   It is recommended to collect the matrix.
   (2) Operational risk management
   Operational risks address safety reviews, FMECA and reviews performed early in the process. New technologies may be identified and presented at the implementation process.
   (3) Software Control System FMECA
      (a) The control system FMECA shall provide traceability of the software module to the relevant functions of the traceability matrix.
      (b) The control system FMECA shall perform the functions changed in the implementation phase as a whole in the integrated system.
      (c) The control systems FMECA in IL2 and IL3 shall be performed including interfaces with integrated control systems that may affect their functions.
   (4) New or unproven technology
   New or unproven technologies entail additional risks. New technologies can be hardware, mechanical equipment, interface protocol, or software module coding.

317. Implementation Process Milestone M3

1. Complete the code development.

2. Complete the integration and SI tests.

3. Adjustment of functional test strategies and plans and test results shall be reviewed and verified based on the traceability matrix.

4. The SI releases integrated system programming for the transition process.

5. Complete the V & V plan. (developed by V & V organization)

6. Complete the simulation. (Verified by V & V Organization)

7. Verification is completed and the SRS and SDS requirements of the control system software are met.

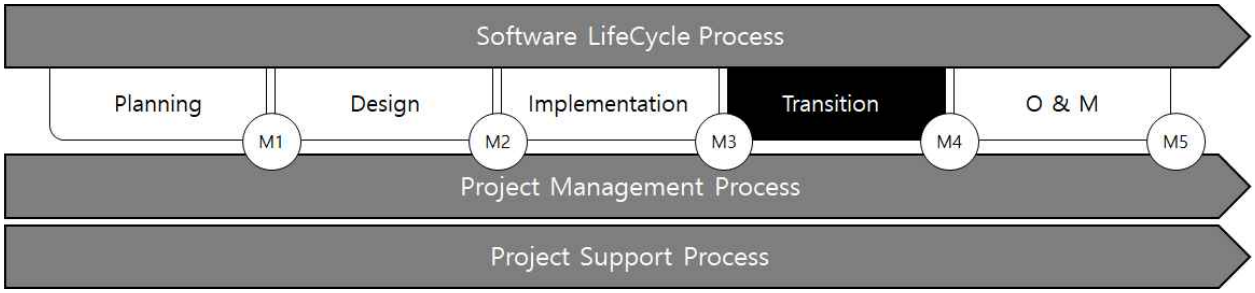
8. A V & V Report is prepared and delivered to stakeholders.

9. Before shipping the software, the software is checked for viruses.

10. The owner confirms that the software meets the current ConOps. This includes the concepts that have changed in the course of the project.

11. All components and subsystems shall be updated as defined in ConOps.

Section 4 Transition Process



401. General

1. The transition process establishes the ability to provide the services specified in the requirements of stakeholders within the operational environment and ensures that the Owner and User integrated software meets the requirements.
2. In the transition process, the User is responsible for the operation and maintenance of the integrated software. The SI shall deliver the final document to the User and its Owner, including manuals, ConOps, SRS and SDS.

402. Activity

The transition process provides supplying and installing the integrated software to the user, ensuring that the installed integrated software works with SDS, and the Owner shall develop a maintenance plan. The activities of the transition process have been developed by reference to ISO/IEC/IEEE 12207 First Edition, 2017-11, "System and Software Engineering - Software Life Cycle Process" and ISO/IEC/IEEE 15288 First Edition 2015-05-15, "System and Software Engineering - Software Life Cycle Process."

No.	Activity
Owner	
1	Transfer of change management to users after the takeover phase.
2	Operation manual review
3	O & M Planning
4	Review O & M Plan
User	
1	Install new / modified integrated software
2	Initialization, execution, and termination testing of installed integrated software
3	Identify integrated software maintenance manager
4	Review O & M plan
SI	
1	Operation manual development
2	Identify integrated software maintenance manager
3	Provide to the Owner and the User, including operation manuals, ConOps, SRS and SDS
4	Integrated software update change management
5	Provide training to the Owner and the User
6	Integrated software operation test
7	Integrated software distribution

403. Maintenance plans and operation manuals

1. The SI shall develop and provide operation manuals to the Owner and users. The operation manual shall identify the integrated software maintenance manager.

2. The Owner and/or the User shall use documents from SI, suppliers and sub-suppliers to establish maintenance plans, if possible. The SI shall provide to the Owner and the user what is necessary to produce an maintenance plan. the User is advised to review maintenance plans established by owners.

3. The maintenance plans are recommended to include as follows.
   (1) The stakeholders responsible for maintenance shall be identified.
   (2) The components of maintenance are defined.
   (3) Where planned operations and maintenance take place is identified.
   (4) When specific operations and maintenance occur is defined.
   (5) The SI shall recommend training periods and courses for the maintenance of the system.
   (6) The maintenance activities to be performed shall be described.
   (7) The checks to be performed and the data to be collected for health and performance monitoring shall be described.
   (8) Feedback shall be provided to manage maintenance effectiveness, including a schedule of reporting system health and performance.
   (9) All documents to be provided by the SI shall be specified.
   (10) System test and configuration documentation updates are covered as configuration changes, repairs and upgrades are made.
   (11) The expected life of the software and the end-of-life replacement, upgrade and retirement are addressed in detail.
   (12) It is recommended that the Owner or User identify the human resources, facilities and tools necessary for operation and maintenance.
   (13) The plan refers to individual safety security and software/firmware configuration management plans, and the Owner shall add to the list of necessary documents not provided by the SI.

404. Reviewing Operational and Maintenance Items

1. Stakeholders shall review items based on completeness and entry into the next Maintenance process. Items to be considered are as follows and it is recommended not to initiate the O & M process if these modules are missing or incomplete.
   (1) Control Equipment Registry
   (2) Management of change (MOC) Policy
   (3) Procedure for management of change (MOC)
   (4) Vessel software registry
   (5) Software configuration management plan
   (6) Software change control process

405. Change Management (MOC) Policy

1. The MOC policy shall be reviewed by the User to determine the completeness of integrated software. The review records shall be kept on the vessel for review by our Society.

2. Management of software changes is to follow the MOC procedures of the Owner or User for installation approval. The SI maintains change management of software updates internally. Owners and/or users may install new or updated software according to the MOC.

3. Users shall at least review Change Management (MOC) policies for items and activities as follows.
   (1) Definitions of various roles and responsibilities within the MOC process.
   (2) Process for software validation of changes in IL2 and IL3 components
   (3) MOC reviewed and defined milestones and life cycles;
   (4) Evaluation of the change process should be performed as part of the process.
   (5) Define formal approval procedures.
   (6) Owner or DCO must comply with the MOC for new restrictions and process safety updates. Changes should be recorded.
   (7) Notice of official ships or offshore plants shall be part of the owner's or DCO's MOC procedure.
   (8) The DCO shall manage software changes within the MOC policy of the asset.

(9) The DCO shall manage software changes within the MOC policy of the asset.
(10) It is recommended to review the effects of software changes, updates, deletions, or new functions on the scope of the control system, including subsystems.

406. Software Registry

1. The registry shall contain at least the following information:
(1) File size
(2) The physical location of the backup(if provided by the SI and/or supplier)
(3) Location of recovery procedures for control systems and components, HMI, server, etc.
(4) Date the latest software was installed

407. Control equipment Registry

1. The registry shall contain information at least as follows.
(1) Installed control equipment
(2) Integrity Level
(3) Traceable unique tags of control equipment
(4) Interacting software modules

408. Software configuration management plan

1. It is recommended that the Owner and User review the software configuration management plan at least as follows.
(1) The software configuration management activities shall be planned.
(2) All software work assets shall be identifiable, controlled and available.
(3) All changes to identified software work assets shall be managed.
(4) Inform all interested parties of the status and contents of the software base line.
(5) A mechanism shall be used to control changes in software requirements.
(6) A mechanism shall be used to control changes in software design.
(7) A mechanism shall be used to control code change.
(8) Mechanisms are used in the maintenance process to manage the configuration of software tools.
(9) Regression test libraries shall be included to accept maintenance
(10) The software configuration management plan may be part of the owner/DCO MOC procedure.

409. Scanning for viruses and other malicious software

1. Prior to the installation of the integrated software, all software code, executables and physical media used for installation on ships shall be checked for viruses and malicious software.

2. The test results are documented and kept in the software registry.

410. Transition Process Milestone M4

1. Operation manual provided

2. Operation management plan development

3. Control system software approval

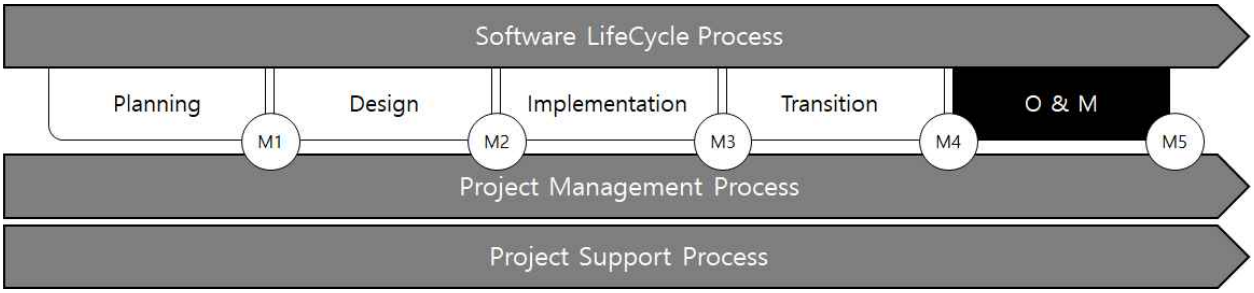
4. Ship software registry update by Shipbuilder, Owner, User and/or SI.

5. Control equipment registry update by Shipbuilder, Owner, User and/or SI.

6. Commissioning test

7. Authorize the Owner to proceed to Maintenance process

Section 5 Operation and Maintenance



501. General

1. The operational and maintenance process covers all operational and maintenance activities, including scheduled and unexpected upgrades and troubleshooting activities. This process may even apply to the decommissioning activities of ISPM control systems.
2. The operation and maintenance process uses integrated software and ensures that its capabilities persist. Ultimately, the integrated software is discontinued, decommissioned, and removed to restore the environment in which it is installed to its original state or to an acceptable state by Owner or User.

502. Activity

The activities of the operation and maintenance processes are under the responsibility of the User and the Supplier according to their instructions. After the conversion process, such as the integration software accepted by the Owner and presented to the User, the Owner or User observes the performance of the integration software based on the information and documentation provided by the SI, supplier and sub-supplier. The activities of the operational and maintenance processes have been developed by reference to ISO/IEC/IEE 12207 First Edition, 2017-11, "System and Software Engineering - Software Life Cycle Process" and ISO/IEC/IEE 15288 First Edition 2015-05-15, "System and Software Engineering - Software Life Cycle Process."

No.	Activities
Owner	
1	Development and management of MOC procedures. MOC requirements management.
2	Obsolescence monitoring
3	O&M plan review
4	MOC review
5	O&M plan development, issue for review and then for implementation
User	
1	Changes to system software are managed in a controlled manner
2	The impact of software changes on the system as a whole shall be reviewed.
3	Perform verification tests after upgrades or source code changes(integrators may conduct peer review)
4	Perform regular software audits of user schedules
5	O&M plan update (if needed)
6	O&M plan review
7	ISPM integrated software resister maintenance
8	controller registry maintenance
9	Obsolescence monitoring
SI	
1	Operation manual development

1. Identify and analyze operational problems associated with organizational constraints.

(1) Observe the ability of the system to provide the service, record the problem, take corrective activities, coordination activities, adaptation activities, preventive activities, and check the recovered ability.

(2) This process reproduces, stores and destroys system elements or waste in an environmentally sound manner in accordance with laws, conventions, organizational constraints and stakeholder requirements. If required, records should be maintained to monitor the health of operators, users, and the safety of the environment.

503. Scan for viruses and other malicious software

Regularly check the integrated software in operation for virus and malicious software. Survey results are documented and stored in the Software Registry.

504. Maintenance of Integrated Control System

1. Scheduled Upgrades – New Features

New functional upgrades of integrated control systems are usually due to the replacement of critical computer systems, the addition or replacement of major system functions. Due to known nature and significant effects on units, these upgrades are managed in the same way as initial system integration. To use the new control system functions, processes and outputs shall be updated in the previous SDLC process. The activities of SDLC may be reduced to match the scope of the project. The distinction between important and minor upgrades depends on the unit and application of the control system.

(1) Project management

Establish a project management plan for the new scheduled functions.

(2) planning process

(a) Review existing ConOps and update to reflect new functionality

(b) Define all new functionality.

(c) Safety review of new functionality.

(d) Review the results of a function failure and specify a new level of integrity with inputs from other organizations and groups.
(e) The verification method for the new function is as applicable as the method used for the original verification.
(f) Update all traceability matrices

(3) Requirements and design process
(a) update existing SRS to reflect new functionality;
(b) update existing SDSs to reflect new requirements;
(c) Update all existing performance, safety, database and security requirements and comply with standards, ergonomic considerations and capabilities.
(d) Define new integration tests for all new commercial off-the-shelf (COTS) packages.

(4) Implementation process
(a) Develop integrated code to support new features.
(b) SI shall complete all levels of testing specified in the Implementation process in accordance with SRS and SDS.

(5) Verification & verification process
(a) Update the verification plan (V&V plan) and configure the simulation for the verification method.
(b) Carry out an updated V & V plan.
(c) Transition the Integrated System to the Owner and the User.

(6) Transition process
(a) Install the software on the target hardware.
(b) Functionally test all support services.
(c) All documentation updates at O & M process.

2. Unscheduled upgrade

(1) Unscheduled upgrades occur when the equipment manufacturer releases hardware, firmware, or software upgrades to the control system, or when the computer hardware manufacturer releases a series of modifications.
Software upgrades with ISPM control systems or integrity levels IL0 to IL3 shall be upgraded using the following steps.
(a) Follow the safety procedures related to lockout / tagout.
(b) Follow the manufacturer's instructions when upgrading hardware / software.
(c) Use the software and control equipment registry to identify all hardware / software modules that interact with the upgraded hardware / software.
(d) At least the SI shall review the software code or perform regression tests on all identified hardware / software.
(e) When all tests pass, bring the upgraded hardware / software to operation.
(f) When the test fails, contact the supplier before attempting the upgrade and return the system to the previous version of hardware / software.
(g) Update all documents.

(2) When any IL2 or IL3 software functionality is upgraded, the Owner or the User shall follow the "scheduled upgrade" procedure possible.

(3) When a scheduled upgrade has not been performed prior to an unscheduled upgrade, significant or minor upgrades shall be performed according to the "scheduled upgrade" procedure for IL2 and IL3 ISPM control systems as determined. To update ConOps, SRS & SDS, the process defined in **504. 1** (1) and (2) shall be followed at least.

(4) For IL0 and IL1 ISPM control systems, it is recommended to comply with **504. 2** (1) (a) to (f) or at the owner's discretion.

505. Scanning viruses and other malicious software

Disposal or replacement of the control system shall take into account the following disposal or replacement plan.

1. Control and monitoring are reduced or eliminated during disposal or replacement activities. Disposal plans shall consider safeguards on equipment and processes during removal and / or replacement.

2. The control system to be replaced shall not affect the functioning of the control system assigned the ISPM code.

506. Operation and Maintenance Process Milestone M5

1. Disposal of the integrated control system. ⚓

GUIDANCE FOR SOFTWARE CONFORMITY CERTIFICATION

Published by
KR
36, Myeongji ocean city 9-ro, Gangseo-gu,
BUSAN, KOREA
TEL : +82 70 8799 7114
FAX : +82 70 8799 8999
Website : http://www.krs.co.kr