OCEAN OBSERVATORIES INITIATIVE

SYSTEMS ENGINEERING MANAGEMENT PLAN

Version 3-12-P
Document Control Number 1100-00000
2010-07-27

Consortium for Ocean Leadership
1201 New York Ave NW, 4th Floor, Washington DC 20005
www.OceanLeadership.org

in Cooperation with

University of California, San Diego
University of Washington
Woods Hole Oceanographic Institution
Oregon State University
Scripps Institution of Oceanography

Document Control Sheet

Version	Description
3-12-P	Public version

Note: This document has been edited to remove information that is considered confidential and/or sensitive to ongoing or future financial negotiations for OOI procurements. Information removed has been replaced by the insertion of “[redacted]”.

Table of Contents:

Table of Figures

Table of Tables

1 Introduction

1.1 Purpose

The *OOI System Engineering Management Plan* (SEMP) describes the overall plan for systems engineering management of the OOI program and the processes invoked to accomplish the plan. The organization of this document follows guidance provided by American National Standards Institute/Electronics Industries Alliance (ANSI/EIA)-632-1998, Processes for Engineering a System, as shown in Figure 1.

Technical Management, Supply & Acquisition, System Design, Implementation (Realization), and Technical Evaluation are the five major process categories shown in the figure along with the sub-processes within each of the major process categories. These processes and sub-processes are used for the level one and level two headings within this SEMP starting with Section 3.0.

The Systems Engineering processes used for the Ocean Observatories Initiative (OOI) System of Systems (SoS) are multi-dimensional in nature. There is a vertical dimension of systems engineering processes and procedures that, in their application, decompose the system from statements of user needs into SoS, System, Subsystem, Component, and finally product definitions, and then support the integration, testing, and delivery of the integrated systems. This is interwoven with a horizontal dimension that deals with the System Development Life Cycle (SDLC). Ocean Leadership (OL) and the Implementing Organizations (IOs) have selected an Iterative SDLC for OOI, which demands the repetitive application of the systems engineering process within iterations. The third dimension is the knowledge and skills of our systems engineering staff developed through their experiences on previous projects, formal systems engineering training, and specific OOI-provided training.

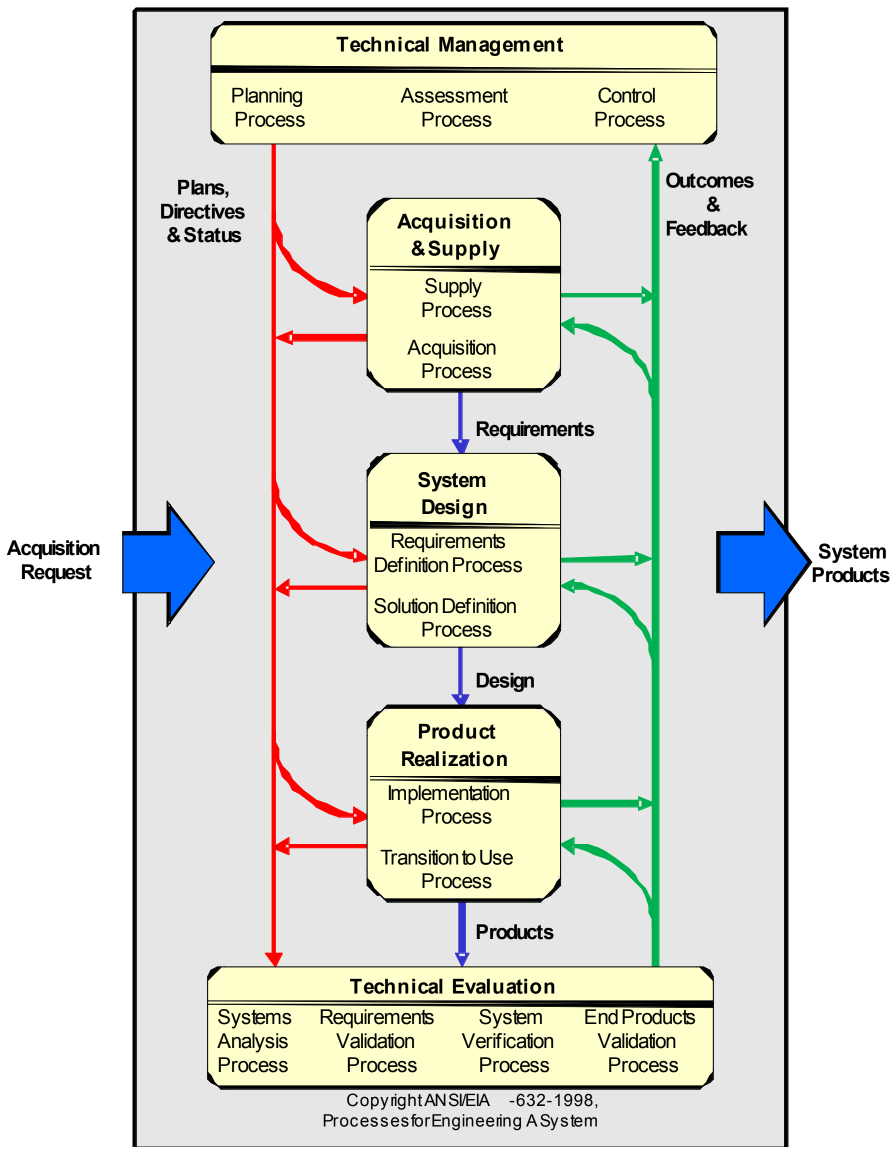

Figure 1, Processes for Engineering a System

The Systems Engineering "V", shown in Figure 2, identifies a few of the ANSI/EIA-632 processes (identified by the requirement numbers in the white circles) the OOI Team uses to define, implement, deliver, and sustain systems that fully satisfy customer and stakeholder needs and illustrates the vertical nature of our processes.

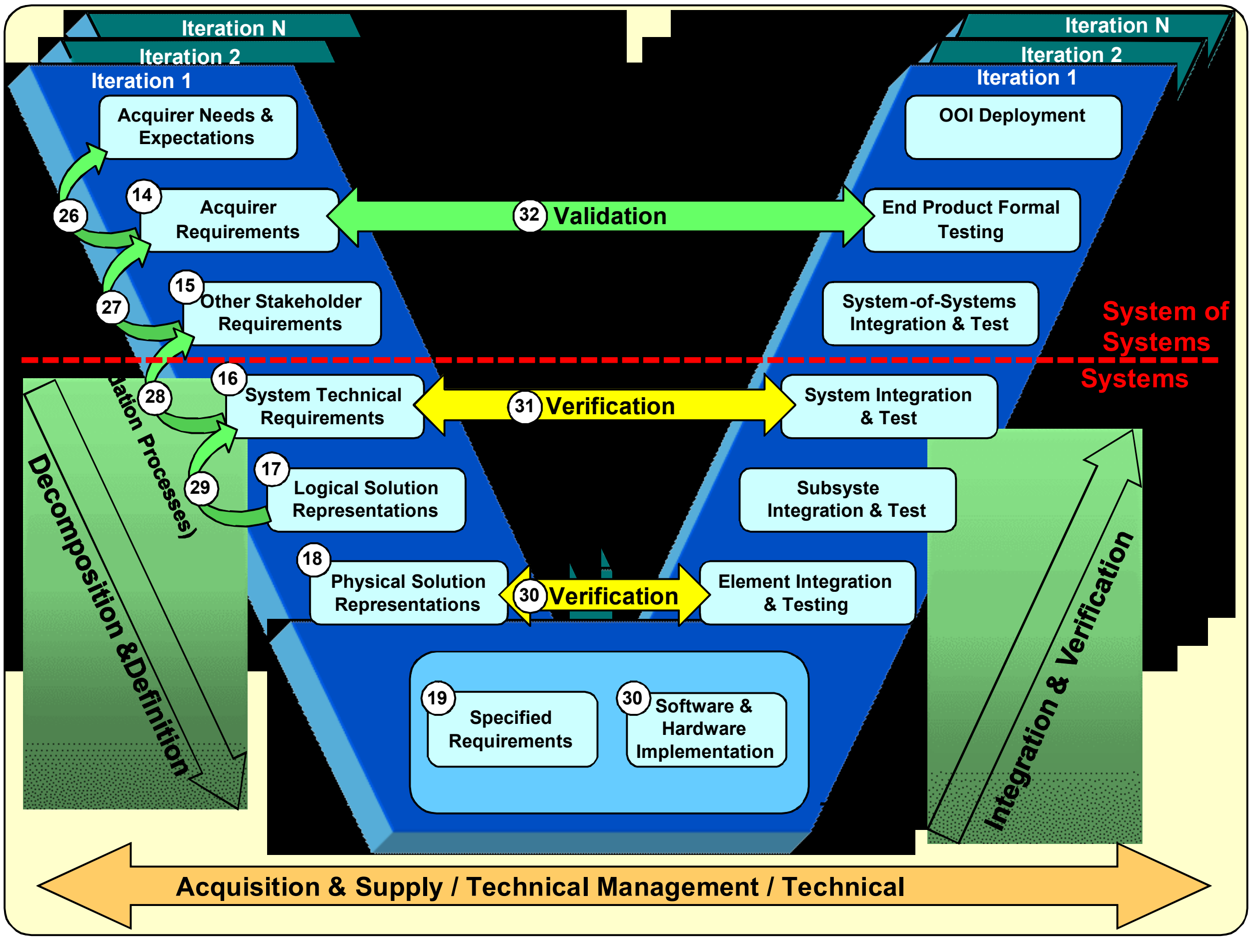

Figure 2, Systems Engineering "V"

Figure 2 also illustrates a line of demarcation between the integrated program level management responsibilities of OL and those of the IOs. Since responsibility for developing individual Systems are assigned to the IOs, this same line of demarcation also marks the cooperative intersections between OL as the Prime awardee and the sub-awardees of the Regional Scale Nodes (RSN), Coastal/Global Scale Nodes (CGSN), and Cyberinfrastructure (CI) Systems.

This SEMP presents the OOI processes for:

- Acquisition and Supply – Section 3
- Technical Management – Section 4
- System Design – Section 5
- Technical Evaluation – Section 6

1.2 Scope

This document is applicable to all OOI Systems, Subsystems and component engineering efforts (hardware and software) accomplished throughout the program. It includes the Systems Engineering processes used by OL and all of the IOs and as a result, the IOs do not maintain separate or subordinate SEMPs. This SEMP addresses a series of questions regarding the OOI deliverables:

- What systems will be delivered?
- What tasks must be accomplished to deliver them?
- What is the order in which the tasks must be completed?
- What are the task dependencies?
- What are the final acceptance criteria?
- Who will be responsible for each task?
- How will each task be carried out?

This SEMP incorporates and combines relevant aspects of traditional System Engineering Management Plans and Software Development Plans. It covers all stages in both hardware and software system life cycles, and the integrated OOI life cycle from requirements definition through deployment and into operations.

1.3 Precedence and References

1.3.1 Precedence

In the event of conflict between/among plans, policies and guidelines, the following precedence shall exist when not specifically identified. First, the OOI PEP, then the OOI SEMP, then the remaining OOI pertinent documents as equal importance. The SEMP spawns all other engineering plans on the project. The OOI Program Director, or designee, shall have authority to resolve any conflict between/among guidelines/direction.

1.3.2 References

The following documents are provided for guidance and reference. The only "official" version of any document is the most recent CCB approved version. They are maintained in the OOI Document Management System (DMS).

1.3.2.1 Guidance and Reference Documents

The following documents shall exist and be retained in the OOI DMS.

1001-00000 Project Execution Plan (PEP)
1100-00000 Systems Engineering Management Plan (SEMP)
1040-00000 Integrated Master Schedule (IMS)
1000-00000 Configuration Management Plan (CMP)
1002-00000 Cost Estimating Plan (CEP)
1003-00000 Quality Assurance and Quality Control (QA/QC) Plan
1004-00000Commissioning Plan (CP)
1005-00000 Earned Value Management System (EVMS) Plan
1006-00000 Environmental Health and Safety (EH&S) Plan
1101-00000 Final Network Design (FND)
1007-00000Risk Management Plan (RMP)
1008-00000 Acquisition Plan (AP)
1010-00000 Operations and Maintenance (O&M) Plan
1011-00000 Property Management Plan (PMP)
1020-00000 Schedule Management Plan (SMP)
Transition to Operations (T2P) Plan

Integrated Logistics Support (ILS) Plan
1001-00100 Annual Work Plans (AWP)
Test Plan
Build Plan
Integration, Verification and Validation (IV&V) Plan
1012-00000 Security Management Plan (aka Cybersecurity Plan)
Documentation Tree
1041-00000 WBS Dictionary

1.3.2.2 References

Department of Defense Architecture Framework (DoDAF) 1.5 Volume 1 (http://www.defenselink.mil/cio-nii/docs/DoDAF_Volume_I.pdf)
DoDAF 1.5 Volume 2 (http://www.defenselink.mil/cio-nii/docs/DoDAF_Volume_II.pdf)
DoDAF 1.5 Volume 3 (http://www.defenselink.mil/cio-nii/docs/DoDAF_Volume_III.pdf)
DoDAF 1.0 Deskbook
Processes for Engineering a System, ANSI/EIA-632-1998

1.4 Responsibility and Authority

The SEMP defines the technical organization, the roles and responsibilities of that organization, and establishes the high level guidelines (and root of procedural work instructions) for technical control of the project. The SEMP ensures that the management and engineering processes include the necessary discipline and participation to effectively perform the complete, integrated engineering functions.

The Project Manager for OOI has the authority and responsibility to appoint an OOI Chief Systems Engineer, who shall have the authority and responsibility to carry out the policies and activities described herein.

The OOI Systems Engineers have primary responsibility for all system level issues. The OOI Chief Systems Engineer works with IO Systems Engineers to implement the systems engineering process as described herein across the collaboration; to ensure that requirements and interfaces are fully defined; and that all technical issues affecting more than one system are efficiently resolved.

The approval of the OOI Chief Systems Engineer or designee is required on all documents and decisions that have the potential to impact the ability of the delivered systems, including instruments, to meet their allocated science requirements.

2 Ocean Observatories Initiative (OOI) System Overview

The OOI comprises three interconnected systems spanning global, regional and coastal scales.

- Costal-Global Scale Nodes (CGSN) - The global nodes address planetary-scale problems via a network of moored buoys linked to shore via satellite for command and control plus limited near-real time data access. The coastal nodes of the OOI will expand existing coastal observing assets, providing extended opportunities to characterize the effects of high frequency forcing on the coastal environments.
- Regional Scale Node (RSN) - A regional cabled observatory will 'wire' a single region in the Northeast Pacific Ocean with a high-speed optical and power grid.
- CyberInfrastructure (CI)- The CI constitutes the integrating system that links and binds the two types of marine observatories and associated sensors into a coherent system-of-systems. The CI is not an overlay, but integrated functionality imbedded deep into the design of each scale of the observatories.

The OOI will enable powerful new scientific approaches by capitalizing on a confluence of disruptive technologies that are often related to exponential growth in fields including telecommunications, computer science, and genomics. The OOI will build a networked sensor grid that will collect ocean and seafloor data at high sampling rates over years to decades. Researchers will make simultaneous, interdisciplinary measurements to investigate a spectrum of phenomena including episodic, short-lived events (tectonic, volcanic, biological, severe storms), and more subtle, longer-term changes or emergent phenomena in ocean systems (circulation patterns, climate change, ocean acidity, ecosystem trends). Through a unifying Cyberinfrastructure, researchers will control sampling strategies of experiments deployed on one part of the OOI in response to remote detection of events by other parts of the OOI. Distributed research groups can form virtual collaborations to collectively analyze and respond to ocean events in near-real time. The long-term introduction of ample power and data rate capability to remote parts of the ocean by the OOI will provide the ocean science community with unprecedented access to detailed data on multiple spatial scales. This enables studying the coastal, regional, and global-scale ocean, and using mobile assets (autonomous underwater vehicles, gliders, and vertical profilers) to complement fixed-point observations. Additional information regarding OOI design and deployment is found in the OOI Final Network Design (FND)

3 Acquisition and Supply

3.1 Product Supply Process

3.1.1 OOI Organizations as Suppliers

Ocean Leadership stands in the position of supplier (Product Supply Process) to the National Science Foundation (NSF) providing the OOI System of Systems. The OOI Systems Engineering organization is responsible for establishing the requirements for the OOI System, assessing the Request for Proposals (RFPs) to determine the capability to meet the acquisition requirements, supporting the establishment of a cooperative-agreement with the NSF, and satisfying the agreement.

The IOs stand in the position of supplier to OL providing the underlying systems, subsystems and components of the OOI System of Systems. The IO Systems Engineering organizations are responsible for establishing the requirements for the IO Systems, subsystems and components; assessing the RFPs to determine the capability to meet the acquisition requirements, supporting the establishment of an agreement with Ocean Leadership, and satisfying the agreement.

The OOI and IO Systems Engineering Organizations at all levels are responsible for implementing the processes enumerated in this SEMP, as applicable, to meet the requirements and to deliver the products and other deliverables as specified in the established agreements. Each IO will follow a defined Acquisition Plan that specifies the role of Systems Engineering within the acquisition process. For example, the Requirements Working Group (RWG), lead by Ocean Leadership's Requirements Lead, establishes the OOI System Requirements baseline (Level 2), and recommends changes to Level 3 and Level 4 requirements. Traceability is maintained in the Dynamic Object Oriented Requirements System (DOORS) tool to reflect the requirements allocation from System of Systems to Systems to Subsystem to component. This forms the "agreement" between the organizations at each level.

3.1.2 Contracts Management - Supply

Contract Management processes govern the Product Supply activities. The Contract Management organizations in the NSF, OL, IOs, and IO subcontractors record the established agreements in the form of formal contracts within legal, regulatory, enterprise, and project bounds. The contracts incorporate Statements of Work (SOWs), Concept of Operations (ConOps), requirements, and systems designs that have been generated and baselined by the OOI Systems Engineers. The IO System Engineers, System Architects, Project Scientists, and other members of the OOI community participate on the Requirements Working Group, the Interface Working Group, and other OOI level activities to gain an understanding of the allocated requirements.

3.2 Acquisition Process

3.2.1 OOI Organizations as Acquirers

Ocean Leadership stands in the position of acquirer (Product Acquisition Process) obtaining products from the Implementing Organizations. The OOI Systems Engineering Group is responsible for:

- Technical inputs to aid the IOs in preparing applicable RFPs, Specifications, or Source Control Documents (SCD) to obtain a supply of work or delivery of desired system products
- Assistance in evaluating supplier responses to the RFP, Specification, or SCD
- Recommending acceptance of delivered products.

The IOs stand in the position of acquirer obtaining products from second tier subcontractors and vendors. The IO Systems Engineering organizations are responsible for:

- Technical inputs for preparation of the applicable RFP, Specification, or Source Control Document (SCD) to obtain a supply of work or delivery of desired system products;
- Evaluating supplier responses to the RFP, Specification, or SCD;
- Recommending acceptance of delivered products.

3.2.2 Contracts Management - Acquisition

Contract Management processes also govern the Product Acquisition activities. The Contract Management organizations at OL, the IOs, and IO subcontractors record the established agreements in the form of formal contracts within legal, regulatory, enterprise, and project bounds. The contracts incorporate Statements of Work (SOWs), Concept of Operations (ConOps), requirements, and systems designs that have been generated and baselined by the OL, IOs, and IO subcontractor's Chief Systems Engineers.

3.2.3 Acquisition Documentation

A good design must not only perform all of the allocated functions in a reliable manner, it also must be possible to efficiently purchase or manufacture the quantity needed. The end result of all engineering development effort is the creation of a documented baseline with sufficient information to support the purchase or manufacture of needed system elements.

Simple items can be purchased with high confidence using only a vendor's part number, whereas complex items may require a carefully detailed specification to achieve reasonable confidence that a competitive selection will yield the expected result.
Figure 3 presents a flow diagram illustrating the decisions involved and resulting documentation required. All acquisitions shall be consistent and follow the OOI Acquisition Plan.

3.2.4 Source Control Document

Source Control Documents (SCDs) are used when the manufacturer's literature does not completely define the required configuration or behavior of the item being acquired. The SCD supplements the existing standard item documentation by defining any missing or unique design attributes that are required. The SCD is prepared, reviewed, released, controlled, and maintained in accordance with the CMP.

3.2.5 Specifications

Specifications are used when the needed items must be defined in detail to support vendor selection. The specification establishes the complete set of detailed characteristics of the item to be delivered, and is typically much more comprehensive than an SCD. Specifications are prepared, reviewed, released, controlled and maintained in accordance with the CMP.

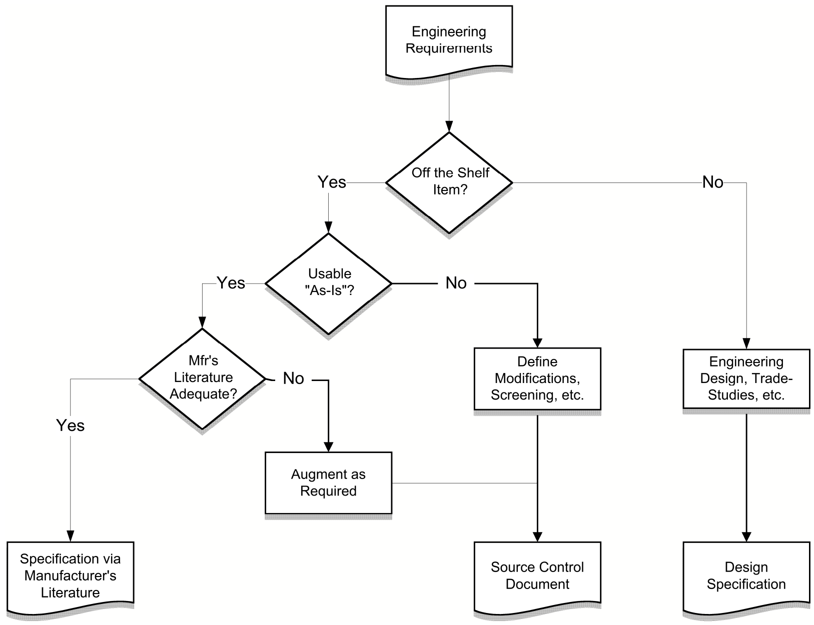

Figure 3, Purchasing and Production Documentation Method

3.3 Supplier Performance

The Supplier Performance process is used by an organization when acting as an acquirer to monitor the execution of an agreement that has been established with an organization acting as a supplier. Ocean Leadership stands in the position of acquirer obtaining products from the IOs. The IOs are acquirers for obtaining products from the second-tier subcontractors and vendors.

Contracts, Purchase Orders, Source Control Documents, and other forms of OOI agreements define the required acquirer-supplier contractual and technical relationships including the people, information to be provided and interface activities to be performed.

As part of an acquirer organization, the OOI Systems Engineering Group (along with COTRs and COs) monitors performance of the Contractors, Subcontractors, vendors, and suppliers to ensure they provide end products that satisfy the requirements laid out in the agreements. This is accomplished by system engineers through:

- Participating in appropriate supplier teams.
- Participating in appropriate supplier Technical Interchange Meetings (TIMs)
- Monitoring supplier performance against Technical Performance Measures (TPMs) and other Key Performance Parameter product metrics.
- Flowing down changes in requirements or operational concepts that might affect the supplier's product or project.
- Controlling changes to requirements made by the supplier that would affect the acquirer's project or other related projects or products.
- Assessing supplier performance against assigned requirements, including conduct of, or participation in, appropriate technical reviews.
- Verification and/or Validation of products delivered from the supplier, or ensuring that products have been validated before delivery and prior to integration with other products that form a composite end product intended to meet the acquirer's specified requirements.

4 Technical Management

4.1 Planning Process

4.1.1 Process Implementation Strategy

Following industry best practices, Ocean Leadership, the University of California, San Diego (UCSD), the University of Washington (UW), and Woods Hole Oceanographic Institution (WHOI) and their subcontractors, will follow a comprehensive set of written processes and procedures for system development, production, test, deployment/installation, training, support, and disposal that are tailored for the OOI project. These organizational processes are selected and arranged to form the system development life cycle for a particular project. The tailored processes and procedures are published and monitored to ensure compliance.

4.1.1.1 Stakeholder Identification

Stakeholders who have an interest or stake in the outcome of the project have been identified and their needs are the driving force behind the OOI System Requirements. The primary stakeholders are scientists, modelers, and educators that use the system for a variety of reasons. A series of formal workshops have been conducted to elicit stakeholder requirements and to identify and acquire applicable documents, and the requirements therein, that could affect the project.

To sustain stakeholder involvement, Science meetings, Technical Interchange Meetings (TIMs) and systems engineering work sessions are scheduled and conducted any time the parties involved have a need to interact on a more formal basis. TIMs have published agendas and meeting minutes are retained in the project files. Action items recorded at these events are reflected in the Project Level Action Item tracking system and monitored through closure.

Formal and informal coordination with stakeholders and system engineering peers, as well as periodic interaction with a larger topic related workgroup are all useful methods to help reduce development risk. Comparison against allocations, adherence to established interface specifications, and careful consideration of derived requirements all contribute to remaining focused on the overall system goals.

4.1.1.2 OOI Integrated Master Schedule (IMS)

The OOI Integrated Master Schedule (IMS) identifies contractual events and the significant accomplishments that must be achieved by those events for the complete technical effort. It also clearly reflects the OOI Iterative Life Cycle and how the efforts of the IOs are integrated. When taken as a whole, the OOI IMS illustrates and defines a major portion of the Life Cycle for the OOI System between Final Design Review (FDR) and the Operations and Maintenance (O&M) phase. The events, accomplishments, and accomplishment criteria directly relate to Work Breakdown Structure (WBS) elements.

Each of the major IMS accomplishments, which can also be referred to as a life-cycle phase, culminates with a Formal Management Review for which specific work products are expected to be produced and reviewed. Each of the Formal Management Reviews has measurable exit criteria for successful completion of the review, which provides a definitive measure or indicator that the required level of maturity or progress has been achieved and also denotes the successful completion of that life-cycle phase. Section 4.2.3 of this SEMP provides information about each of the Formal Technical Reviews used in the OOI Program with specific details on input products, entry criteria, and exit criteria. The IMS separates the phases for each of the OOI systems and the OOI System of Systems as a whole. It depicts the process implementation strategy for developing individual systems of the OOI and how the IO systems are integrated together into a cohesively fielded OOI System of Systems.

4.1.1.3 Cyberinfrastructure System Life Cycle

The Cyberinfrastructure system life cycle is described in Section 2.2 of the Cyberinfrastructure PEP, and is based on the spiral development management model. Each Spiral (Figure 4) is a four-month-long inception phase, a four-month-long elaboration phase, a six-month-long construction phase, and a two-month-long transition phase. Each phase terminates in a milestone review. The details and impact of the risks (whether technical, management, operational, or stakeholder) drive the number of spirals, the level of detail, and effort within each phase of a spiral. The riskiest items and issues are brought forward as early in the development process as possible. Each spiral includes management, engineering, and support activities in proportion to the risks. Each spiral expands system definition and results in a deployed representation of the CI.

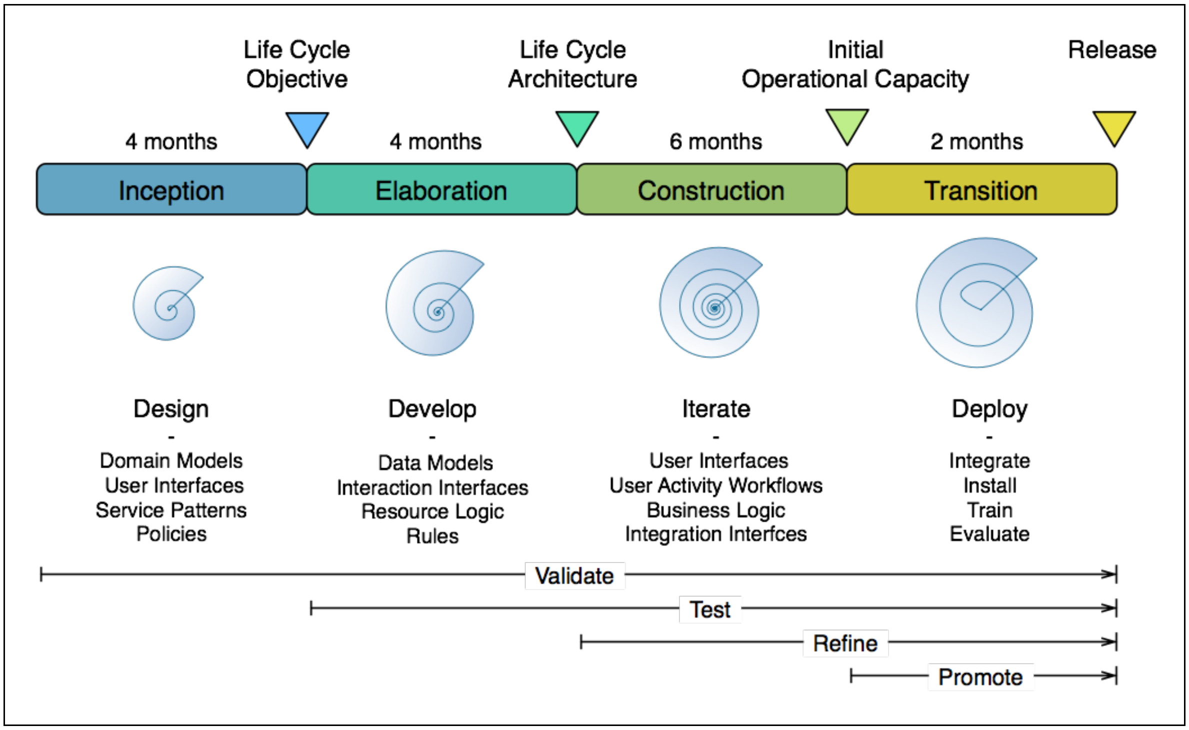

Figure 4, Spiral Development Life Cycle

The CI project master schedule consists of five full development spirals.
Figure 5 shows multiple Spiral Development Life Cycles applied in an overlapping manner to each of the CI Subsystems. The Cyberinfrastructure system life cycle consists of five overlapping sixteen month spiral cycles. Beginning with the second cycle, the inception phase starts four months prior to the end of the preceding construction phase, so that a full development cycle and major software release occurs every twelve months beginning eighteen months after project start. Figure 4 shows in a simplified manner how each of the five Cyberinfrastructure spirals coordinate with the life cycles of the other subsystems and contribute to successive releases of the OOI System of Systems.

The system life cycle consists of a set of planning, requirements definition, and system-level design, prototyping, integration, and verification activities. Under the spiral development model, these activities can occur during any system life cycle phase, although typically they are dominant during particular phases as described throughout this section of the SEMP. In addition, the project is being managed in an agile manner, and in reality, several elements of the system life cycle may occur iteratively during a single phase of a given spiral. For example, requirements and architecture definition are iterative activities that are most productive when carried out over relatively short (order one month) periods. The key system life cycle activities are the responsibility of and under the supervision of the CI System Engineer, Senior System Architect and Software Development Manager, as defined in Section 2.1 of the CI-PEP.

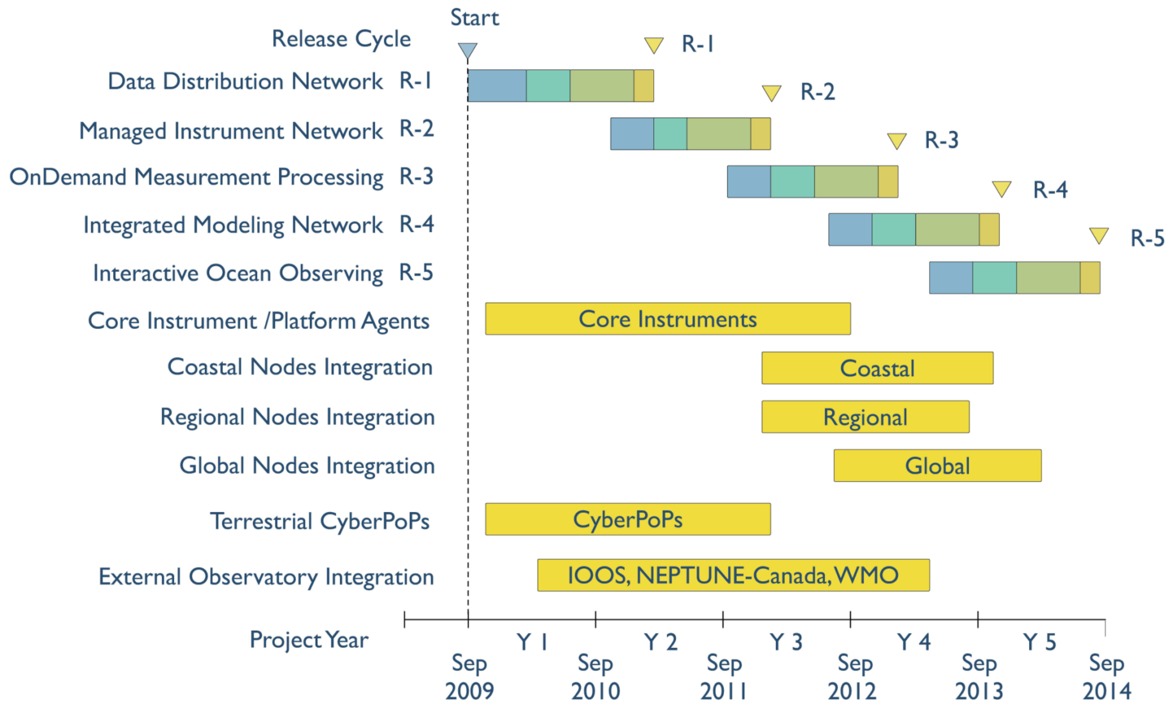

Figure 5, Application of Spiral Development to Subsystems

Figure 6 maps the system life cycle onto the spiral model shown in
Figure 5, and describes it through a series of activities in each spiral phase that produces a set of artifacts, ending in a milestone review with a defined set of principal assessors. The CI System Engineer drives the entire process through management of the system life cycle. During the inception phase at the start of each spiral, the main activities are highly iterative requirements gathering and architectural design activities. These terminate with the Life Cycle Objective (LCO) milestone review in which the assessors are the Software Development and System Engineering teams. The elaboration phase is dominantly carried out by the System Architecture and Software Development teams, and involves rapid prototyping to minimize risk. It terminates in the Life Cycle Architecture (LCA) review for which the assessors are the stakeholders and Project Scientist. The construction phase is primarily carried out by the Software Development team and has the key goal of building and integrating a functional system that meets the requirements. It ends with the Initial Operational Capacity (IOC) milestone review during which the evaluation activities are testing and verification led by the System Engineer and Quality Assurance team assessing the former. During the transition phase, the activity is integration of the CI and the marine IO systems carried out by the System Integration team with the goal of producing a deployed system. Validation also occurs during the transition phase by the Project Scientist and stakeholders. The phase terminates with a release and is evaluated through the acceptance

process carried out by the OOI Program Office and stakeholders. Under the alignment of successive spirals shown in Figure 4, the LCO and release milestones are coincident.

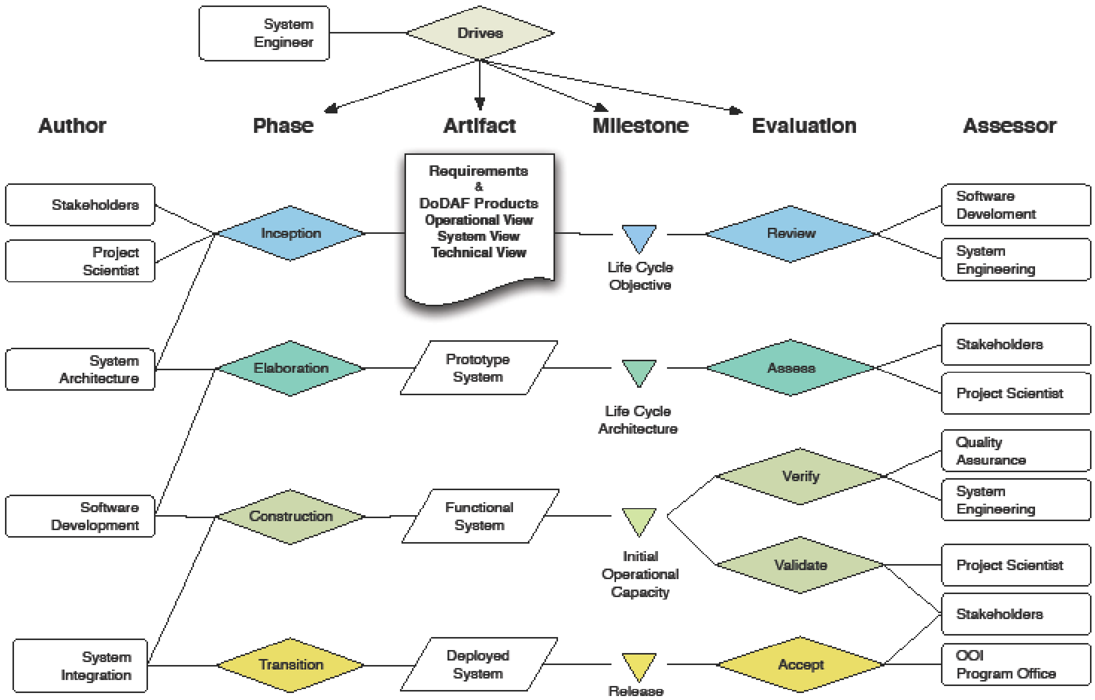

Figure 6, Engineering Process Model, Software

4.1.1.3.1 Inception Phase

System and subsystem requirements definition is the dominant activity in each inception phase (Figure 4), but continues at reduced levels throughout each development spiral. The CI System Engineer and requirements working group extract system requirements from the user requirements and other sources. Requirements definition involves the stakeholder communities organized through the Project Scientist and EPE Manager, the entire CI development team, and the Program Office. Additional elements of the system requirements are the policies that govern use of OOI resources, which must be negotiated with the marine IOs, OOI Program Office and stakeholders.

4.1.1.3.2 Elaboration Phase

System architecture definition is the dominant activity during each elaboration phase, although it continues at a reduced level in the other spiral phases. With input from the Subsystem Development IPTs, the architecture working group defines and refines the system architecture according to the evolving requirements. Architecture specification activities may include prototyping and trade studies. Quality assurance is a cross-cutting activity throughout system development.

4.1.1.3.3 Construction Phase

During the construction phase of each development spiral, the newly created architectural components are integrated into any existing CI release by the Software Development Manager and verified for compliance with the system requirements by the System Engineer. Upon completion, the integrated and verified CI is deployed into the marine IOs, and then undergoes a second verification process led by the CI System Engineer and OOI Test Lead. The System

Integration team carries out both activities to provide continuity, and the Operations Manager oversees deployment to give a seamless transition to the operations and maintenance phase.

Near the end of each construction phase, the newly integrated and verified CI is validated to show that the result meets stakeholder needs through compliance with user requirements. The Project Scientist is responsible for validation with assistance from the Chief Systems Engineer and selected stakeholders.

4.1.1.3.4 Transition Phase

During each transition phase, the integrated and verified system is delivered to the Operations Manager for deployment. After deployment, the CI is available for operations and use by the scientific and educational communities. During this phase, the newly integrated and verified CI is validated to show that the result meets stakeholder needs through compliance with user requirements. The Project Scientist is responsible for validation with assistance from the CI Systems Engineer and selected stakeholders. Subsequent to these activities, the system is accepted by the OOI Program Office using specified criteria.

4.1.1.3.5 CI Software Development Processes

Cyberinfrastructure software and system engineering activities follow a highly iterative process. Development iterations define a number of development products that are delivered with a prescribed state and content. Some deliverables are external only, and are subject to review and acceptance. The dates for deliverables must be coordinated and consistent with project milestones.

The Cyberinfrastructure Software Development team, consisting of the Software Development Manager and Subsystem IPTs, together with the System Engineer and architecture working group, leverage and further develop existing technologies to ensure both the rapid availability of an initial CI implementation and the systematic, iterative, and incremental implementation of the full set of CI capabilities in accordance with the release schedule. At its core, the OOI software development effort is a system-of-systems integration challenge, with software development primarily focused on subsystem adaptation and integration of best-of-breed, proven technologies.

4.1.1.4 Coastal/Global Project Life Cycle

The CGSN project life cycle is broken down into two major subcategories: Subsystem Development and Implementation. During subsystem development the subsystems identified in CGSN Level 3 and Level 4 requirements are brought from detail design to production-ready. These subsystems are then utilized in the implementation phase where the coastal array and global array components are integrated and accepted. The arrays are then moved into the deployment and commissioning phase, completing the NSF's Major Research Equipment and Facilities Construction (MREFC) project. Major areas of project life cycle monitoring include the General CGSN Project Life Cycle, the Global Arrays Project Life Cycle, the Endurance Array Project Life Cycle, and the Pioneer Life cycle.

Subsystem Development includes three (3) stages:

- **Development and Documentation:** Qualified manufacturers – internal and commercial - participate in subsystem development.
- **Prototype (as required):** In conjunction with RSN and CI as appropriate, CGSN will perform prototype development and performance evaluation.
- **Preproduction:** Suppliers develop and implement Manufacturing Plans and Verification Plans which include the input for the qualification test and manufacturing test plans.

Implementation has four (4) stages, including:

- **Production:** CGSN will work in conjunction with the vendors to finalize Manufacturing Test Requirements, Manufacturing Reporting Requirements, Manufacturing QA/QC Compliance Requirements, and develop a Continuous Improvement Plan with periodic engineering and cost reviews in the manufacture of components.

- **Platform Integration:** Prior to the Integration Phase CGSN, in conjunction with RSN and CI as appropriate, will develop a Platform Integration Plan and a Platform Integration Test Plan for each of the configuration items and conduct these integration and test activities.
- **Incremental Installation and Acceptance:** During the incremental Installation Phase, each of the configuration items will be deployed and tested as outlined in the schedules.
- **Array Commissioning:** The Array Commissioning Phase begins upon completion of the incremental installation and acceptance and when all logistics support and operational systems are developed and in place.

These items and specific project life cycles are documented and managed in the *CGSN Project Life Cycle* Document, which consolidates and further refines the information that can be found in the *CGSN Operations Plan and Maintenance Strategy.*

4.1.1.5 Regional Scale Node Project Life Cycle

The RSN project life cycle consists of two major subcategories: Primary Infrastructure and Secondary Infrastructure. The Primary Infrastructure is defined as the entire transmission terminal and power equipment in the Shore Station, the Primary Nodes, and all of the interconnecting submarine cable. The Secondary Infrastructure refers to all of the infrastructure and cables from the Primary Nodes to the actual instruments or sensors.

Because of the differences between the Primary Infrastructure and Secondary Infrastructure, there are different project life cycles associated to their respective categories.

The Primary Infrastructure project life cycle includes:

- **Contractor Selection**
- **Development**
- **Construction**
- **Installation**
- **Commissioning**

The Secondary Infrastructure project life cycle includes:

- **Subsystem Development**
    - Prototype Developed
        - Requirements Analysis
        - Allocations
        - Develop Prototype and Create Build Documentation
        - Review Documentation
    - Prototype Evaluated
        - Build Prototype Documentation
        - Test Prototype
    - Production Development
        - Develop Production Build Documentation
        - Review Documentation
    - Production Evaluated
        - Build Evaluation Unit
        - Evaluation Unit Review
        - Test Evaluation Unit
- **Subsystem Production**
- **Subsystem Integration by Site**
- **Installation by Site**
- **Acceptance by Site**
- **Commissioning by Site**

These items and specific project life cycles are documented and managed in the *RSN Acquisition Strategy* Document, which consolidates and further refines the information that can be found in the *RSN Operations Plan and Maintenance Strategy.*

Insert 4.1.1.6 Education and Public Engagement Infrastructure Life Cycle

4.1.2 Technical Effort Definition

4.1.2.1 Goals, Objectives, and Expectations

Elicitation of user requirements through Formal Workshops, TIMs, and SE Work Sessions is the initial phase of an ongoing stakeholder oversight and interface process that continues through the deployment and acceptance phases of the system life cycle. Extracting requirements from diverse stakeholder communities presents a challenge, as the typical user may not be familiar with many of the relevant information technologies, and is not able to readily quantify present and future needs in a manner that leads to a formal design. The Project Scientist, Education and Public Engagement (EPE) Manager, System Engineers and architecture working group work with domain scientists and educators to overcome this issue. Outputs from formal workshops have been captured in the following set of OOI Level 1 and Level 2 Requirements documents:

- L1 Science Themes
- L1 Programmatic Requirements
- L2 Science Questions
- L2 Science Requirements
- L2 Cyber-User Requirements
- L2 Educational Requirements
- L2 Operational Requirements
- L2 Common Requirements
- L2 Reference (Acronyms, Glossary)

These OOI Level 2 Requirements include: agreement requirements; other stakeholder requirements; and enterprise, project, and associated process constraints.

In order to achieve this goal, the requirements working group constructed a wide range of use scenarios (i.e., operational concepts) and concepts of operations incorporating representative suites of sensors and platforms in close collaboration with a representative group of domain users. A complementary process involves a Concept of Operations Document (ConOps), developed by the Operations Manager and Systems Engineers in collaboration with the Science Team. The ConOps describes what the systems do from the user perspective, while stimulating stakeholder ideas with feasible OOI System capabilities and applications, as well as enabling the use case scenario development effort.

4.1.2.2 Risk Management Strategy

The OOI Project has developed a risk management approach to identify risks to the appropriate level and to avert or remedy them when possible. Within the framework of the risk management process is also an opportunity management to identify positive opportunities that will reduce cost and schedule while maintaining scope. This risk management approach has been published as a separate document called the *OOI Risk Management Plan*, that provides detailed guidance on the OOI Risk Management processes, and flows to the IOs. The *OOI Cost Estimating Plan (CEP)* incorporates the concept of estimating the necessary level of contingency funds to be held for risk mitigation activities. Figure 7 depicts the basic set of five processes that are executed in an iterative manner to perform risk management for the OOI Project.

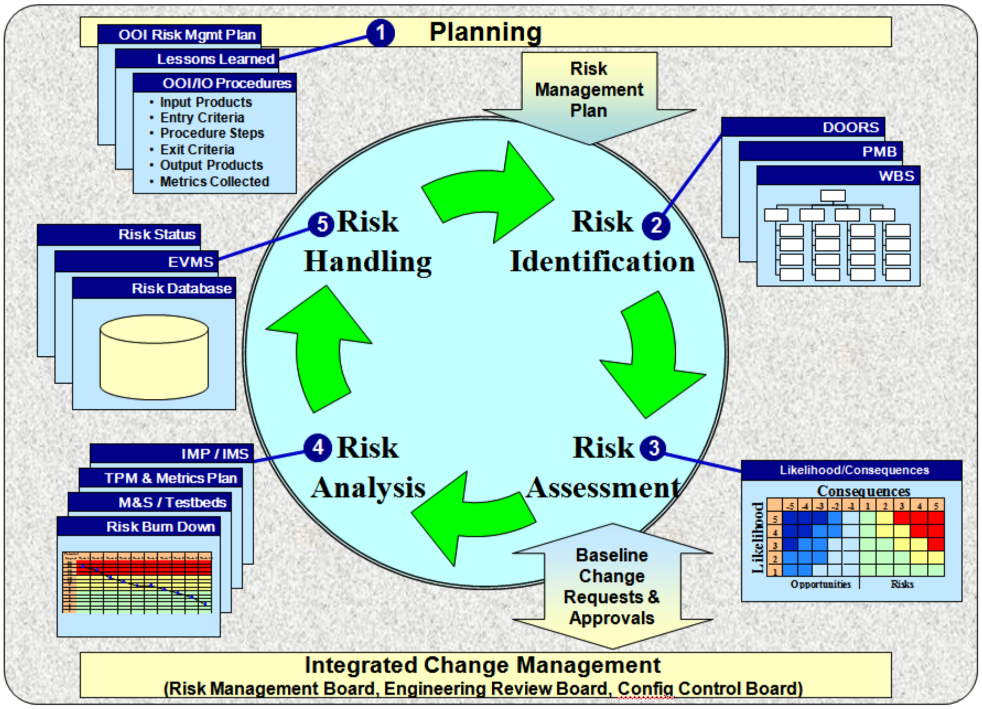

Figure 7, Risk Process Steps

The five processes of Risk Planning, Risk Identification, Risk Assessment, Risk Analysis, and Risk Handling, plus the additional Contingency Estimating process, are explained in the subparagraphs of this section.

- **Risk Planning**: is the umbrella term for the systematic process of reducing or eliminating the undesirable occurrences inherent in programs.
- **Risk Identification:** is the process of exposing the risks that have a realistic potential of harming the program.
- **Risk Assessment:** is the process of quantification, characterization and prioritization of program risk after identification.
- **Risk Analysis:** is the process of evaluating alternatives for handling the assessed risks.
- **Risk Handling**: is the action (or inaction) taken in response to an identified risk after it has been identified and assessed.

The primary organizations charged with Risk Management responsibilities are the Program Management and Systems Engineering organizations. Systems engineering identifies the technical risks on the project while Program Management administrates the Risk Management Process, approves risk handling plans and allocates the requisite amount of Management Reserve.

It is strongly emphasized that this process, to be effective, must be used in conjunction with established processes for requirements analysis, verification & validation, quality assurance, quality indicators, management indicators, document production, Configuration Management and project planning.

4.1.2.3 System Engineering Metrics

The OOI Program has selected the following set of product metrics by which quality is evaluated and process metrics by which efficiency and effectiveness of technical efforts are measured. These system engineering metrics are implemented and integrated with the project-level metrics outlined in the OOI PEP, and include:

- Complete set of earned value metrics that encompass cost and schedules in technical areas
- Total number of requirements
- Number of requirements associated with an approved baseline change
- Change in number of requirements
- Total number of design elements
- Change in number of design elements
- Total software size: Equivalent source lines of code (ELOC), source lines of code (SLOC) or function point analysis (FPA)
- Change in software size (ELOC, SLOC or FPA)
- Total number of test cases & test procedures
- Change in number of test cases & test procedures
- Total number of defects
- Number of defects detected per test case
- Defects open during a reporting period
- Defects closed during a reporting period
- Set of Technical Performance Measurements (TPM) that are derived directly from the performance requirements

4.1.2.4 Technical Performance Measurements (TPM)

TPMs are used to identify and flag the importance of a design deficiency that might jeopardize meeting a system level requirement that has been determined to be critical, TPMs are the continuing verification of the degree of anticipated and actual achievement of technical parameters.

The OOI Project has established a TPM process that identifies Key Performance Parameters (KPPs), which in turn are used to determine success of the system, or portion thereof. Failure to achieve a KPP may constitute system failure or unacceptable degradation. KPPs also identify what should receive management focus and items to be tracked using TPM procedures. The OOI TPM process tracks the TPMs assigned and/or allocated to the IOs to ensure they are considered in the design, properly addressed in the implementation, and thoroughly tested before the products are incorporated into the OOI Baseline. Figure 8 depicts the basic OOI TPM approach, and associated variables, with definitions given below it.

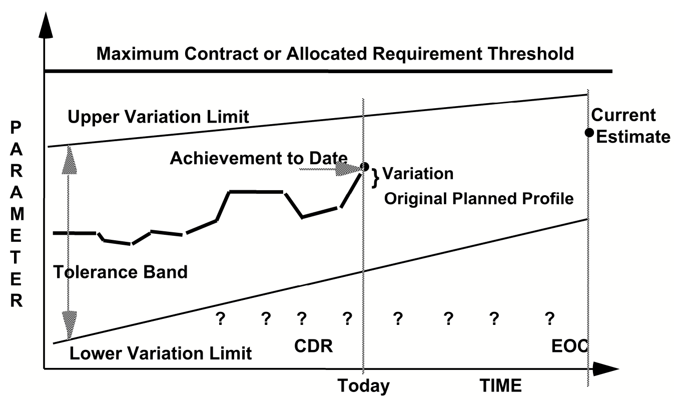

Figure 8, Technical Performance Measurement Profile

Achievement to Date: Measured progress or estimated progress plotted/compared with planned progress at designated milestone dates.
Current Estimate: Value of technical parameters predicted to be achieved with existing resources by End of Contract (EOC).
Planned Profile: Profile representing the projected time-phased demonstration of a technical parameter requirement.

Tolerance Band: Management alert limits placed each side of the planned profile to indicate the envelope or degree of variation allowed. The tolerance band represents the projected level of estimating error.
Threshold: The limiting acceptable value of a technical parameter; usually a contractual performance requirement.
Variation: Difference between the planned value of the technical parameter and the achievement-to-date value derived from analysis, test, or demonstration.

TPMs are jointly developed and agreed to by both the OL and the IOs. The IOs may select to “elevate” their respective TPMs to “IO specific KPPs” where failure to satisfy any KPP may be cause to deem the specific IO as inoperable. Examples of “IO specific KPPs” may include, but are not limited to:

RSN KPPs

- Accuracy of Pulse Per Second Timing System
- Reliability of Primary Infrastructure
- Maximum Speed of Shallow Profiler
- Maximum number of full profiles/day for Deep Profiler.
- MVC Output Power

CGSN KPPs

- Instrument availability by platform, instruments operating within specification when powered
- Power availability by platform and power subsystem
- Data and telemetry availability by platform
- Instrument data integrity (effectiveness and bio-fouling mitigation) by platform
- Platform configurability, for event driven tasking (human in loop and automated)
- Operational design life
- Operational costs
- Integration operation (design stability)

CI KPPs

- Availability
- Reliability
- Message processing rate
- Message latency

4.1.2.5 System Breakdown Structure

The System Breakdown Structure (SBS) is shown in **Error! Reference source not found.**. Based on the OOI requirements, these are the three systems and associated subsystems of the OOI. (A fourth system, Education and Public Engagement, will be added in the future.)

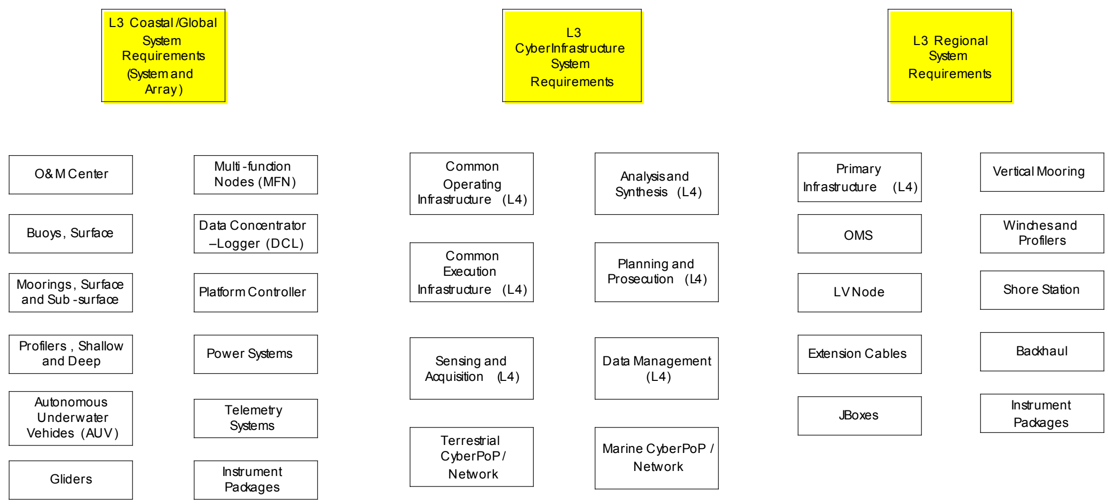

Figure 9, System Breakdown Structure

The sub-systems in the SBS (Figure 9) under CI are:

- **Sensing and Acquisition:** provides the life cycle and operational management of sensor network environments, as well as observing activities (i.e., scheduling, collecting, processing) associated with sensor data acquisition;
- **Analysis and Synthesis:** provides the life cycle and operational management of community models, ensembles of models and the virtual ocean simulator, as well as modeling activities (i.e., assimilation, analysis, evaluation) using observed and derived data products;
- **Planning and Prosecution:** provides the mission and campaign planning and prosecution (execution through completion) activities to carry out simultaneous coordinated multi-objective observations across the resources of the OOI;
- **Data Management:** provides life cycle management, federation, preservation and presentation of OOI data holdings and associated metadata via data streams, repositories and catalogs;
- **Common Operating Infrastructure:** provides the services and distributed infrastructure to build a secure, scalable, fault-tolerant federated system of independently operated OOI components;
- **Common Execution Infrastructure:** provides the services to manage the distributed, immediate mode execution of processes.
- **Marine CyberPoP/Network:** provides the agent architecture and implementation to interface to marine IO infrastructure, including instruments.
- **Terrestrial CyberPoP/Network:** provides the networked management, distribution, acquisition and distribution points along with the OOI backbone network

The sub-systems in the SBS (Figure 9) under RSN are:

- **Primary Infrastructure:** includes all equipment needed to provide power at 10 KV and data rate at 10 Gbps from the Shore Stations on the coast of Oregon to the RSN Sites across the Juan De Fuca Plate.
- **Observatory Management System (OMS):** is a software application with interfaces to all of the Primary and Secondary Infrastructure Element Management Systems (EMS) to provide a single point of interface for command and control of the RSN infrastructure for the Cyberinfrastructure and for the RSN Operations Center.
- **Low Voltage Node (LVNode) Subsystem:** is a power, timing and communication distribution and aggregation node in the Secondary Infrastructure that is a junction between the Sensor connected to Junction Boxes and Primary Nodes.

- **Junction Box (JBox):** provides connection points for instruments to the RSN infrastructure. The JBox provides power and timing to the sensors and communication between the sensor in its native format (RS232/RS485/TCP/IP) and the RSN TCP/IP communication system.
- **Vertical Mooring:** provides the infrastructure needed to support continuous profiling of a water column from sea-floor to just below the sea-surface. The Vertical Mooring includes an EOM cable anchored to the seafloor and a fixed buoyant platform at 200 meters below the sea surface.
- **Profilers:** includes two components of the Vertical Mooring. The Deep Profiler allows for sampling the water column from the seafloor to the 200 meter platform along the EOM cable. The Shallow Profiler allows for sampling the water column from the 200 meter platform to just below the sea surface.
- **Shore Station:** includes the physical building and support needed for the shore based equipment of the Primary Infrastructure. It includes providing conditioned Utility Power with backup systems and access to the cable beach terminations and backhaul access points.
- **Backhaul:** provides a high reliability, high bandwidth link between the Shore Stations and the Cyberinfrastructure CyberPoP in Portland.
- **Instrument Packages:** includes all of the sensors and interfaces needed to measure the environment at rates, locations and accuracy needed to fulfill user requirements.
- **Extension Cables:** provides the secondary infrastructure links between the Primary Nodes, LVNodes and JBoxes. It encompasses the full cable assemblies including cable, connectors and cable terminations.

The sub-systems in the SBS (Figure 9) under CGSN are:

- **Moorings, Surface and Subsurface:** are designed to keep the surface and water column fixed measurement stations on station between maintenance intervals, each configured specifically for a site and its functional requirements.
- **Surface Buoys:** provide the necessary buoyancy to support surface moorings by resisting mooring weight and drag forces. In the CGSN they are also used as platforms for meteorological sensors, RF telemetry equipment, power generation and storage systems, and data collection and control subsystems.
- **Autonomous Underwater Vehicles (AUVs):** are used to collect data in the general vicinity of the Pioneer Array. AUVs will operate unattended for extended durations, utilizing docking stations at the base of Pioneer Array EOM moorings to offload data and recharge batteries between missions.
- **Multi-Function Node (MFN):** incorporated at the base of each EOM mooring, MFNs are capable of supporting multiple onboard (e.g., frame-mounted) sensors as well as external sensor packages connected to the MFN frame by ROV wet-mateable connectors. MFNs can be configured to incorporate an AUV docking station.
- **Platform Controller:** or Communications and Power Monitor (CPM), provides the intelligence aboard platforms to acquire sensor data, monitor the state of health of the platform, provide the means for telemetry of data and command information to a shore facility, and to maximize the life of the platform according to predetermined operability rules.
- **Data Concentrator Logger (DCL):** is a microcomputer based element that is the hardware interface to sensors, responsible for configuring, powering and monitoring health of sensors, acquiring, and storing data and forwarding data as requested either directly to a telemetry device or via the Communications and Power Manager (CPM).
- **Power Systems:** are designed to provide continuous power to a buoy based data collection and telemetry system in all weather and seasons. Power systems may contain fuel cell, photovoltaic, and wind generators as well as primary and secondary battery banks.
- **Profilers**: consist of a suite of sensors that are raised and lowered through the water column on a regular basis. The profiler body may travel through the water column using

wire-crawler for deep measurements or winched technique for surface piercing measurements.

- **Gliders:** are autonomous vehicles that profile vertically by controlling buoyancy and move horizontally on wings. Within the CGSN, gliders will be employed for two general purposes: providing horizontal context to horizontally fixed platforms and communicating with subsurface instruments and relaying their data to shore.
- **Telemetry Systems:** are comprised of a set of telemetry devices operating through satellite links, local radio links, and in some cases acoustic modems. The telemetry systems allow communications between platforms and the shore station or nearby UNOLS ship as well as platform to platform communications.
- **Operations & Management Center:** operates 365 days a year and supports operational staff. Systems will be automated as much as possible with operator alerts available around-the-clock. Each facility will provide space for the operations staff, computers and communications equipment, and will have internet connectivity, a firewall, a GPS time server, air conditioning, and emergency backup power.
- **Instrument Packages:** include all of the sensors and interfaces needed to measure the environment at rates, locations and accuracies needed to fulfill user requirements.

4.1.2.6 Work Breakdown Structure

The OOI Work Breakdown Structure (WBS) derives its structure from the OOI System Breakdown Structure (SBS). The major products that comprise the OOI correlate to the cornerstone WBS Elements. A product-based WBS includes a program management branch, a system engineering branch, a system integration and test branch, and an operations planning branch.

The primary WBS elements have been decomposed to reflect hardware sub-products / assemblies and software that comprise the OOI System of Systems. Decomposition was continued until the WBS elements identify applicable tasks that can be accomplished by a team of two or three people in one or two months following organizational procedures with specific entry and exit criteria.

The result is similar to the OOI WBS shown in Table 1, which along with the WBS Dictionary establishes the individual elements of work that are managed. Because of their size, the OOI WBS and OOI WBS Dictionary are maintained as an application in the Software Application Framework (SAF) and a separate document respectively that are subject to configuration control.

Outline Level	WBS	Name
1	1	OOI
2	1.1	System Integration (Project Management Office)
3	1.1.1	PMO Project Management
3	1.1.2	PMO System Engineering
3	1.1.3	PMO Operations Planning
3	1.1.4	PMO Education and Public Engagement
3	1.1.5	PMO Environmental Management
2	1.2	Cyberinfrastructure
3	1.2.1	CI Project Management
3	1.2.2	CI System Engineering
3	1.2.3	CI System Development
3	1.2.4	DEPRECATED
3	1.2.5	CI Implementation
2	1.3	Coastal / Global Infrastructure
3	1.3.1	CG Project Management
3	1.3.2	CG Systems Engineering
3	1.3.3	CG Subsystem Development
3	1.3.4	CG Implementation

Outline Level	WBS	Name
2	1.4	Regional Scale Infrastructure
3	1.4.1	RSN Project Management
3	1.4.2	RSN System Engineering
3	1.4.3	RSN Subsystem Development
3	1.4.4	RSN Site Implementation
2	1.7	Education and Public Engagement
3	1.7.1	EPE Project Management
3	1.7.2	EPE System Engineering
3	1.7.3	EPE System Development
3	1.7.4	EPE Implementation

Table 1, OOI Work Breakdown Structure

With a robust WBS and WBS Dictionary established, Technical Description / Basis of Estimates (TD-BOEs) can be created to estimate the cost of accomplishing the work in each WBS element. With the costs associated, the WBS now becomes a cost work breakdown structure with established cost objectives (e.g., ownership, acquisition, operating, support, and disposal) that can be used in tradeoff analyses. Tradeoffs may be required if the total cost obtained by summing up the individual WBS element cost estimates exceeds the budget.

To properly estimate the costs associated with each WBS Element, the estimator identifies the appropriate methods and tools, required facilities and equipment, and training required to be able to complete defined tasks and meet event exit criteria. The estimator also identifies applicable or potential technology constraints and develops an approach for overcoming each constraint by using an appropriate mitigation approach and by technology insertion at the appropriate time in the enterprise-based life cycle.

4.1.2.7 Methods and Tools

To support the technical effort in accordance with the process implementation strategy, a System Development Environment (SDE) has been constructed that consists of selected methods and tools (Table 2). These tools establish an information database that allow capture of project data and are able to securely retain and make information available. These include tools that aid in collaboration, project management and configuration management.

Configuration Management tools are used to ensure the integrity of the configuration management process. The software configuration management tools have been selected specifically to implement and enforce restrictions of the controlled items, thus making control of project materials significantly easier and more effective. They are used to: 1) enforce pre-determined access restrictions; 2) direct user class privileges; 3) perform data collection, retrieval, storage, and manipulation; 4) provide online reporting capabilities; and 5) facilitate interaction between parties. Finally, Configuration Management tools support control of project materials by providing repositories for controlled items, controlling software code and other software materials, maintaining status accounting records, and providing Project Repository inventory management.

Collaboration Tools are used to provide the OOI Program Office and all IOs the ability to digitally centralize the creation, control and distribution of information and assets. This includes, but is not limited to: information management, document management, issues management, software versioning and control, as well as requirements management, all of which fall under the purview of the Collaboration Tools.

Process Result Product	Category	Tool
Project Planning	Project Management	Microsoft Project
Requirements Specification & Management	Configuration Management	DOORS
Software Architecture Design (CI)	Configuration Management	Software Architect

JAVA Software Development (CI)	Development	Eclipse IDE
Software Configuration Management (CI)	Configuration Management	GIT, Subversion
Action Tracking System (System Level /CI)	Collaboration	JIRA, Atlassian
Data Management / DMS	Configuration Management	Alfresco
Collaboration Wiki	Collaboration	Confluence, Atlassian
Documentation Authoring	Project Management	MS Word/Excel/PowerPoint
System Architecture	Collaboration	Enterprise Architect, Visio, AutoCAD

Table 2, System Development Environment Tools

Requirements Specification & Management: Driven by project management best practices and programmatics, OOI uses Dynamic Object Oriented Requirements System (DOORS) as a Requirements Management system. DOORS supports an emphasis on the relationships between, and orchestration of, activities across all OOI lifecycle aspects, including program management, system acquisition, development, transition/deployment, sustainment, and operational use.

Based on Telelogic's (an IBM company) DOORS platform, OOI DOORS is a Requirements Management system that regulates requirements as modules containing trees of text objects, qualified by an arbitrary number of user-defined attributes, and cross-linked by directional links. It enables requirements traceability through its ability to store multiple documents and tables containing project requirements, attributes, cross-links as well as other information, with no loss of overview, visibility, control or responsibility in the allocating element(s).

OOI DOORS enables these types of capabilities to requirements management:

- All individual requirements may be tagged with multiple attributes and filtered from the rest without losing the remainder of information.
- Requirements may be categorized.
- Requirements from separate documents may be linked showing one-to-one, one-to-many, etc. relationships. This is an important feature allowing traceability through the project lifecycle.
- Any OOI-related project, project affiliate or participant may use DOORS Links to individual standards, such as to demonstrate compliance with mandatory category testing requirements.

OOI DOORS is more than a requirement management platform. It is a multi-user, multi-access database environment. It ensures that all information, including historical versions, is stored. Long-term, this ensures a full audit-trail of the justification and reasoning behind any particular mandated requirement. DOORS also allows coverage and gap analysis, through its ability to give OOI an aggregate level view of requirements and the respective states. It also provides strict configuration management and change control facility. As an additional capability, OOI can readily import and export DOORS-related information into and out of Microsoft Word and Excel documents and Access Tables.

Action Item Tracking: As part of the OOI Collaboration Tool Set, JIRA will be used for Action Item Tracking and for the OOI Issues Tracking and Management System. Issues Tracking and Management Systems are used to prioritize, assign, track, report and audit issues, related to tasks, projects or any number of engagements, including software and hardware bugs, as well as help desk tickets and change requests.

Issues Tracking and Management Systems also implement a workflow foundation, which in turn regulates entered issues into "states." Issues move from state to state, such as "submitted," "open," "evaluation," "working," "in testing," "closed," and moves can be bidirectional. Moves in state can initiated by those with proper authority, or through well defined inputs and outputs, can be automated via business logic.

The typical process flow is:

1. An issue is submitted by a scientist, engineer, or test engineer, via a web browser or e-mail submittal.
2. The issue management system logs the issue and relocates the issue to a predefined representative's inbox.
3. The representative evaluates the issue and assigns it to an appropriate team member.
4. Work is done on the issue, documented in the system, and closed.
5. The originator is notified that the issue has been resolved.

The OOI Issues Tracking and Management (ITM) System allows for a series of reporting and auditing, which will be able to provide basic statistical analysis, but will also be able to give true trend analysis, enabling business intelligence. Reporting capabilities include:

- Unresolved high-priority issues
- Number of issues per customer
- Average resolution time
- Estimated time vs. actual time taken
- Number of issues created per day/week/month/year
- Customizable reports

The ITM/JIRA System is hosted and maintained by the network administrators at the OOI's CI group at UCSD. In addition to its primary role, OOI ITM will also be used by and benefit the OOI through its contribution and capabilities afforded to programmatics and the program management aspect of OOI. The JIRA-based ITM system shall be used as system of record for issues that arise concerning both technical and non-technical tasks, including performance, scope and timelines of operational, managerial, and programmatic tasks within the programs. Actions items are defined in terms of:

- A unique log number assigned to each action
- Date the action was opened
- Originator or event at which the action originated
- Action number as shown in the event minutes or other reference
- Action Title
- Responsibility
- Due Date
- Actual Completion Date
- Status
- Promise Date
- Date of last record update
- Comments

Responsible individuals are to provide up-to-date (weekly minimum) status information regarding assigned actions through closure. Periodic reviews are conducted by management to assess progress and evaluate resource priorities.

4.1.3 Schedule and Organization

4.1.3.1 Engineering Schedule

The schedule for engineering activities, accomplishments and milestones is an integral part of the OOI Integrated Master Schedule (IMS) and Program Execution Plan (PEP)..

4.1.3.2 Resource Loaded Schedule

The OOI WBS that contains the cost estimation information is used as an input to identify the resources required to complete the scheduled tasks. Labor resources and materials are loaded into the IMS using the capabilities of Microsoft Project. With this accomplished, the result is a

Resource Loaded Schedule (RLS), a network of tasks with their dependencies and required resources.

The OOI RLS is a baselined cost and schedule plan against which progress is measured using Earned Value techniques. Cost Account Managers (CAMs) report progress on specific tasks on a regular basis so that actual progress against the plan can be assessed and reported. Overall systems engineering area task status is reported monthly, and any significant variance from cost or schedule baseline is analyzed, reported, and appropriate corrective actions are initiated. Additional details on the Earned Value Management System (EVMS) are provided as part of the EVM Plan, a separate document.

4.1.3.3 Project Organization

The RLS defines the staffing and discipline needs for completing the scheduled tasks and training needs. It is also used as the basis to identify specific risks if required staff is not available. The OOI PEP defines the team (i.e., cooperative partners), organizational structure, and Roles & Responsibilities to complete the scheduled tasks within resource constraints. Agreements with the implementing organizations under the OOI cooperative agreement place further definition on expected system engineering tasking, including definition of deliverables each institution is responsible to provide. The OOI PEP, a separate document, provides details on the overall organizational structure.

The OOI Program is a hierarchy of development organizations. The Consortium for Ocean Leadership (OL) is at the peak of the hierarchy with three (eventually four) separate academic institutions as the IOs, and numerous second tier subcontractors and vendors. Figure 10, illustrates the hierarchical organizational structure of the OOI Project at the OL level and how the IOs are related.

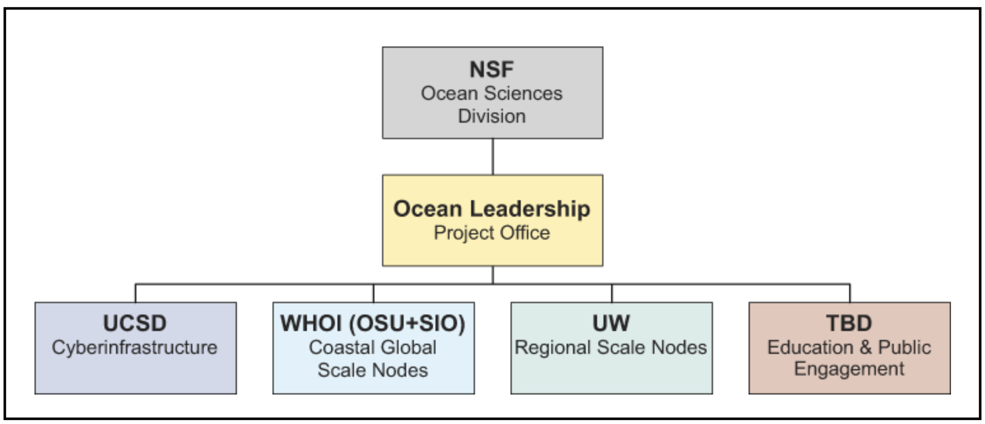

Figure 10, Program Organization Structure

4.1.3.4 Engineering Roles and Responsibilities

4.1.3.4.1 Working Groups

The OOI Chief Systems Engineer has the authority to form various working groups at the OOI level as needed to accomplish project goals and objectives. Groups may be chartered with responsibilities and schedules. Groups may be recurring (i.e., ongoing with no definitive termination schedule) or they may be formed to address specific issues. The intent of working groups is to balance the need for coordinated, focused effort against the established constraints of schedule and resources. Individual IOs may form internal working groups or product focused Integrated Product Teams (IPTs) within their program.

It is envisioned that initially the following groups will be established:

- Requirements working group- lead by the Senior OOI requirements lead
- Interface working group- led by the OOI SE Team
- Test working group- led by the OOI Test lead

4.1.3.4.2 Primary Engineering Roles and Responsibilities

The following positions exist at both the OL level and at the IO levels and that they work cooperatively to accomplish the roles and responsibilities.

Requirements Lead

- Defines requirements management process in collaboration with the OOI and IO Chief Systems Engineers; creates initial requirements management plan
- Defines requirements document (RD) template
- Defines requirements elicitation and management tool support and establishes tool support environment
- Delineates boundary between requirements and design
- Elicits requirements from source documents and requirements workshops
- Provides requirements elicitation materials as required
- Elaborates requirements to the level of detail necessary for architecture design according to priorities set by the OOI Chief Systems Engineer (system level) and Project Scientist (user level)
- Supports requirements controlling and prioritization by providing feasibility information and realization effort estimates based on conceptual system architecture and existing/projected technologies and tools. Provides prototypes to validate requirements feasibility
- Iteratively analyzes and documents requirements in RD (both user and system level)
- Prepares RD deliverables (both user and system level)
- Keeps RD artifacts under configuration and version control and performs document archival
- Performs requirements change management and issue tracking
- Submits RD (both user and system) for review to Chief Systems Engineers and Project Scientists

Engineering Lead (Chief Systems Engineer at OL; Senior Systems Engineer at IOs)

- Approves requirements management process and plan
- Approves RD template
- Provides source documents and prioritizes their importance/relevance
- Defines system scope
- Provides use case scenarios/workflows at system level
- Supports traceability identification for each requirement
- Prioritizes requirements with respect to necessary level of detail from system perspective
- Supports requirements mediation for conflicting system requirements
- Validates RD
- Completeness with respect to system scope
- Completeness with respect to use case scenarios/workflows at system level
- Utility for transition to design
- Provides process, product and quality level review comments for RD

Project Scientists

- Identifies relevant user communities for OOI
- Organizes requirements workshops with user communities and participation of Chief Systems Engineer and Chief Architect
- Provides use case scenarios/workflows at user level
- Supports traceability identification for each requirement

- Prioritizes requirements with respect to necessary level of detail from user perspective
- Supports requirements mediation for conflicting user requirements
- Reviews RD
    - Completeness with respect to use cases/scenarios/workflows at user level
    - Traceability to requirements workshops

Project Manager

- Monitors execution of the requirements management process
- Defines and validates scope and level of project detail with respect to budget
- Reviews requirements management plan for coherence with overall project management and system engineering processes
- Reviews RD with respect to overall project vision
- Approves system RD
- Oversees requirements related risk management

Associate / Deputy Project Director

- Resolves user-system requirements conflicts that cannot be negotiated between stakeholders
- Approves science user RD

Test Lead

- Identifies and develops system of systems test requirements, procedures, processes and work instructions
- Determines test schedules in coordination with Program Controls, Chief Systems Engineer, IOs, Project Manager
- Leads conduct of all OOI level tests
- Reviews and approves IO level test procedures and test if such tests and procedures are part of requirements verification/validation

Operations Manager

- Carries out the integration of all verified subsystems in conjunction with the OOI Chief Systems Engineer and Test Lead.
- Oversees the deployment process to give a seamless transition to the operations and maintenance phase.
- Prepares a Deployment and Acceptance Report after each deployment or acceptance.
- During each transition phase, receives the integrated, verified, and validated system for deployment.
- May sit on the CCB, as applicable.

4.1.4 Technical Plans

4.1.4.1 System Engineering Management Plan (SEMP)

The SEMP identifies the plans and schedules that all of the IOs use to perform the technical effort for the OOI systems development. The IOs do not create or maintain subordinate SEMPs. The various activities within this SEMP have been tailored to the needs of the OOI Project/Program and are used to control the systems development. As depicted in Figure 11, the SEMP is incorporated by reference into the OOI Project Execution Plan, to which it is subordinate. The SEMP incorporates by reference the hierarchy of Level 2 System of Systems, Level 3 System, and Level 4 Subsystem requirements specifications, Interface agreements, and test procedures.

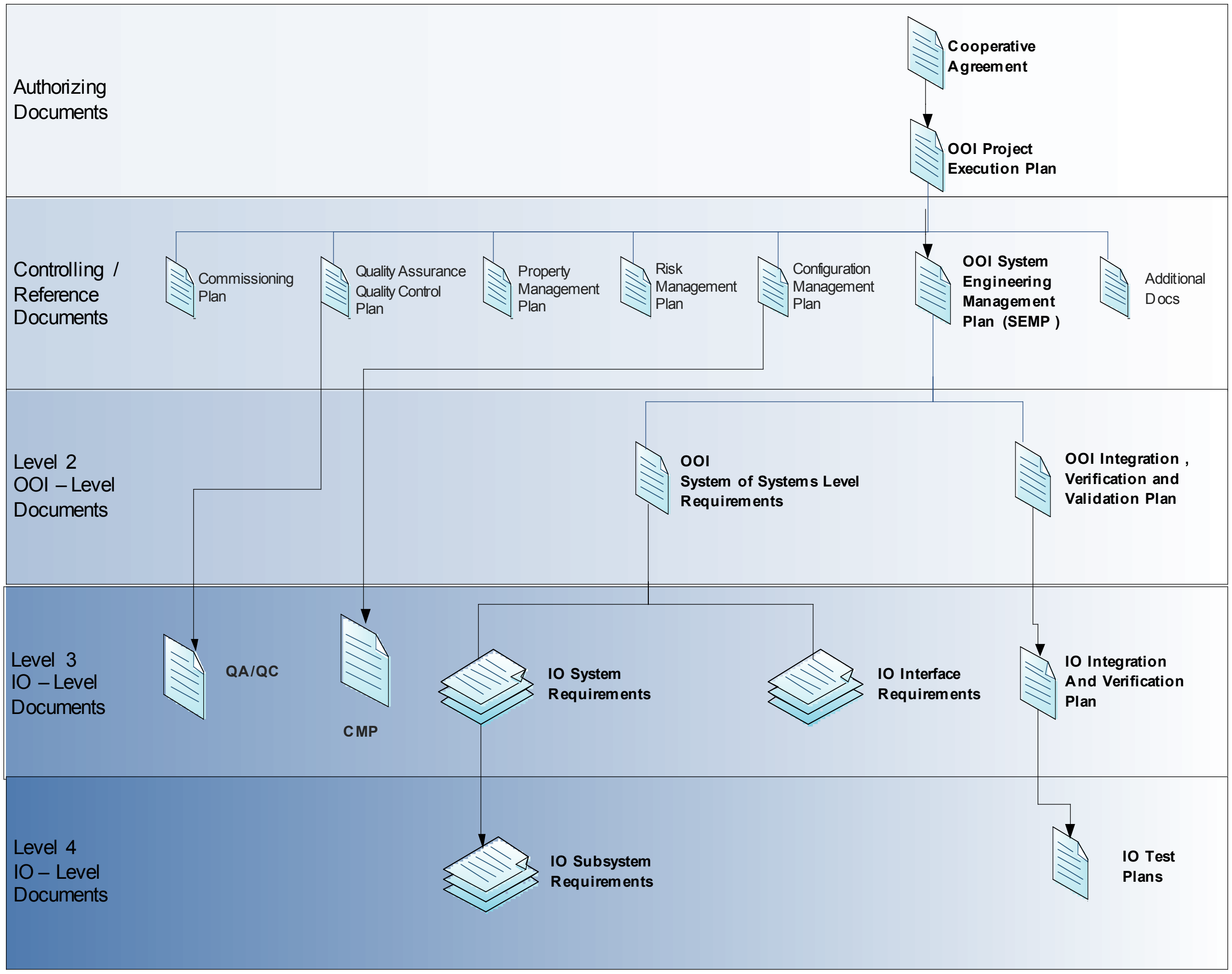

Figure 11, SEMP Location in Document Hierarchy

4.1.4.2 OOI Interoperability Document Set and Interface Control Documents

The OOI Interoperability Document Set will be developed as part of the Technical Data Package (TDP) and compiled from the process of developing the list of interfaces and interface controls for the OOI. The document set will include the interoperability of the CI both internally and with the hardware and software items produced by the marine IOs (RSN/CGSN) and key external entities, notably the national Integrated Ocean Observing System (IOOS). This includes all hardware and software interfaces between configuration items at levels from component through system of systems, internal to all IOs and between IOs (cyber and marine).

These interfaces will be described in detail in Interface Control Documents (ICDs) that describe the interfaces between all systems and subsystems internal to the IOs and external entities. Interface control documents are created in the early stages of design and mature throughout the development of the system of systems, and will be completed as an as-built design document.

The document set also incorporates the Interface Requirements Specifications (IRSs) negotiated among the Project and the marine IOs that establish interface requirements and constraints. The IRSs will reference relevant ICDs, and are negotiated, and approved by, the cognizant IO System Engineers subject to approval by the cognizant IO Project Managers. The OOI Program Office Chief Systems Engineer has final approval authority, and resolves any conflicts that may arise. Finally, IRSs may be negotiated between the project and external entities under similar conditions.

Development of the Interoperability Document Set that includes the IRSs and ICDs will be a major system engineering activity during the early development period of MREFC. The development of ICDs is initiated by the IO system engineers each drafting a list of interface categories; these will divide into three classes: intra-IO, inter-IO interfaces and external interfaces. The first is handled within a given IO, and requires that each IO system engineer work with system and sub-system designers to refine each interface category into a set of specific interfaces and then document each.

The inter-IO interfaces are handled in a like manner by pairs of IO system engineers supported by cognizant system and sub-system designers for each IO. OOI level system engineers also monitor and review these activities for program wide consistency. These activities must be standardized by the use of DOORS and a template that facilitates capturing the necessary information in a standard form. The key sections of the ICDs include descriptions of the interface design, data elements, physical elements, protocols and standards.

External interface development and documentation may require participation of all IOs. Definition and responsibility for development resides at the OOI level. This responsibility may be delegated to IOs, most notably CI and EPE.

The initial requirements for these interfaces exist throughout the requirements sets in Levels 1 through 4. During the early stages of development the list of interfaces will be completed and the corresponding documents created, all managed by the OOI SE and performed by the full SE team. Applicable interface documents will completed by the first *ifdr* of each system. The ICDs will be matured as each subsystem moves through its development phase. They will be written to specify, where appropriate, the mechanical, electrical, environmental and logical components of each interface including nominal values, maximum/minimum values, tolerances, exceptions, variations, nomenclature and markings. For logical software interfaces, full command, control, data structures, exception handling, tools and data transport mechanisms will be defined. In some cases these ICDs will be negotiated with other IOs, developed with external vendors or may be existing vendor documents for off the shelf hardware.

4.1.4.3 Risk Management Plan (RMP)

The Risk Management Plan (RMP) is published and maintained as a separate document and is the responsibility of the OOI Project Manager. The OOI Project Manager serves as risk manager for the project and chairs the Risk Management Board (RMB). The OOI Chief Systems Engineer is a member of the board. An OOI wide risk list is created during the early analysis and architecture definition phase. Potential risk items may be submitted by any project/program personnel. The list is maintained through ongoing Change Control Board activities. In the event risk mitigation activities have significant cost, schedule or scope impact, it is referred to the System Level Change Control Board using the OOI CM procedures. Changes to the baseline design resulting from risk mitigation activities must adhere to the procedures defined in the CMP.

4.1.4.4 Configuration Management Plan (CMP)

The Configuration Management Plan (CMP) is published and maintained as a separate document and is the responsibility of the OOI Chief Systems Engineer. Changes to the OOI System Baseline are managed and controlled in accordance with the procedures defined in the CMP and are evaluated for risk in accordance with the procedures defined in the Risk Management Plan (RMP). The scope of the CMP includes all hardware and software components of the OOI including, but not limited to all of the hardware deployed, or to be deployed, cabling, communications, hardware servers, network components, and software.

The CMP charters a Change Control Board (CCB) at the Ocean Leadership (OL) level that approves or rejects all changes to the OOI Level 1 or 2 requirements, cost and schedule baselines, as well as changes that have an impact between the systems (i.e., Coastal, Global, Regional, and Cyberinfrastructure). The IO CCBs refer all matters that meet this description to the OL CCB for a decision. The OL CCB consists of the OOI Contract Officers Technical

Representatives (COTRs), the OOI Chief Systems Engineer, and other design-cognizant engineering and science personnel as described in the CMP.

Defect Management: The CMP provides for the detection, tracking, and closure of system defects. The OOI Chief Systems Engineer is responsible for the management of SoS defects and indirectly, through the IO Chief Engineers and PMs, defects that substantially diminish the operation and/or quality of the data products. The IO Chief Systems Engineers are responsible for oversight of system-level activities that expose defects and for tracking the defects to closure.

Software Configuration Management: The CMP provides specific processes for software, both COTS and developed, which include:

- **Version Control:** Version control of development artifacts is provided through a specified and controlled application running on a specially protected server. Artifacts are archived on a daily basis. Each created artifact is uniquely identified by its file name and location in the hierarchical file structure that acts as the repository. A revision number is automatically associated with each version of a file. The revision number is automatically created by the application server; it uniquely identifies a file version in combination with the file name and repository location. There is always one current version of a file. Multiple users can get copies of all repository files or parts thereof on their local workstations. These copies can be edited locally and concurrently, and committed to the server when finished. The server ensures that the current versions of the files are updated consistently. The repository provides capabilities to access all versions of a version-controlled object and to compare differences between versions. Sets of files can be combined into new configurations.

- **Configuration Identification:** Version numbers for significant project deliverables and artifacts are assigned when needed. Version numbers are different from the revision numbers that are automatically created by the version control system, as they are manually assigned by the configuration manager for artifacts and groups of artifacts (configurations) that have a certain status. Configuration information is maintained by the version control system.

- **Configuration Control:** After release of a software version or document, all changes shall be recorded and associated with the description of the change and cause of the change.

4.1.4.5 Commissioning Plan

The process of commissioning systems is described in the *OOI Commissioning Plan*, which supports the OOI system commissioning policy where each IO has developed commissioning plans for any system, or subsystem to be commissioned. This commissioning plan and procedures within the plan establish the methodology and processes supporting the decision to commission OOI systems and equipment to be used in the conduct of OOI operations. It is published and maintained as a separate document and process, named the *OOI Commissioning Plan*.

The *OOI Commissioning Plan* cites a systematic process (milestone event/test) of ensuring through validation and verification that new integrated items perform according to the documented design and user operational needs. Among others, it verifies that specified documentation and training are provided to the operations and maintenance groups.

The following criteria are covered in the *OOI Commissioning Plan*:

- Configuration item(s) delivered and fully accepted.
- All support items for operations and maintenance of the Configuration Item(s) are in-place.
- Item capable of operating in a "steady state" mode.

There are four commissioning phases consisting of (a) pre-commissioning, (b) commissioning evaluation, (c) system commissioning and implementation, and (d) decommissioning of the legacy system, or subsystem. Each phase is delineated in the *OOI Commissioning Plan* as applicable to the system being commissioned. Some aspects of each phase may not be applicable because the function is not a part of the specific technology.

4.1.4.6 Quality Assessment and Quality Control Plan (QA/QC)

The QA/QC Plan is published and maintained as a separate document, named the *OOI Quality Assurance and Quality Control Plan (QA/QC)*. It is the responsibility of the OOI Project Director. It describes the quality management system that will be employed through the design, development, deployment, operations and maintenance phases of the OOI project. All personnel will use this QA/QC plan as a reference for individual IO QA/QC Plans and as OOI guidance for strategic, enterprise-level quality management and governance.

The OOI QA/QC Plan incorporates both QA and QC.

- **Quality Assurance:** QA is process-focused and preventive in nature. It is a staff function that is the responsibility of a support organization. An organization that ensures quality is defined & agreed upon, ensures processes exist to produce & measure quality products, ensures continuous improvement is sought, and is capable of providing objective analyses.

- **Quality Control:** QC is product-focused and detective in nature. It is a mainline activity that is the responsibility of the developers, operators and maintainers. It consists of mechanisms to ensure that products meet requirements (formal inspections, one-on-one peer reviews, testing).

Ocean Leadership quality policies and procedures are maintained by the Ocean Leadership Quality Management Organization. Ocean Leadership project instructions are maintained by program personnel.

The OOI QA/QC is organized into the following four sections:

- Introduction - provides the scope, document organization and change control procedure for this document.
- Related Documentation - cites other documents that provide input and reference for this plan.

- Ocean Leadership (OL) Quality Management Organization - describes the goals and objectives, independent reporting, roles and responsibilities, facilities and tools, resource allocation, and training of the quality assurance organization.
- Ocean Leadership Quality Assurance Activities - describes the activities of the OL Quality Management Organization which includes planning, conducting evaluations, developing evaluation criteria, issuing deficiency reports, status reporting, metrics reporting and schedule.

Software Quality Assurance: The QA/QC Plan defines the software quality assurance policies and procedures implemented throughout the software Inception, Elaboration, Construction, and Transition. The OL Quality Management Organization oversees QA/QC activities throughout each development phase. The key activities include monitoring the implementation of the project plans, controlling the acceptance of project deliverables, and providing input to the Project Manager on risk identification and mitigation. The OL Quality Management Organization reports to the Project Director and is responsible for system development quality assurance during each development spiral. Analytical and constructive QA measures are defined jointly by the OOI Chief Systems Engineer and IO Chief Engineers according to the criticality of components and in compliance with the QA/QC Plan. Analytical QA measures include software testing, formal inspections, code reviews, product audits, walk-throughs, and run-time monitoring. Constructive QA measures include formal methods specification, design verification and simulation.

4.1.4.7 Property Management Plan

The Property Management Plan (PMP) establishes an effective property control system for use by OL in the management of the OOI hardware, software, and associated equipment purchased with OOI funding under the Cooperative Agreement, including subawards and subcontracts. The PMP is published and maintained as a separate document, named the *OOI Property Management Plan.*

The PMP will be implemented by OL staff under the direction of the OL Director of Contracts and Grants. It will be used to audit Implementing Organizations (IOs) in the management of their property systems. Each IO will have property plans and procedures for receiving and controlling OOI property and for controlling IO subcontractor/subawardee materials purchased with OOI funding. It is essential to promptly report incidents of loss, damage, or destruction of the OOI property. It is also essential to perform internal property self audits, and to initiate corrective actions when deficiencies are disclosed.

The IOs will maintain formal written policies, plans and procedures that provide an effective property control system for each type of OOI asset for which they are responsible in accordance with the terms and conditions of their contracts. These plans and procedures will be provided to the OL Director of Contracts and Grants, to the OL Contracting Officer Technical Representatives (COTR), and to the OL Property Administrator responsible for the custody of OOI equipment. If an incident of loss, damage or destruction (LDD) occurs, the OL Director of Contracts and Grants and the OL Property Administrator will be promptly notified. Property self-audits by the IOs will be performed bi-annually and corrective actions will be taken in the event of any deficiencies. Property audits by the OL Property Administrator will be performed on an annual basis.

The PMP is not a material management (raw material tracking) requirements set.

4.1.4.8 Environmental Health and Safety Plan (EH&S)

The OOI EH&S Plan describes the processes to describe, assess, and mitigate safety-related issues. These processes include:

- Hazard analysis (the assessment and mitigation of safety-related design and implementation issues)
- Reporting of safety-related events
- Personal protective equipment
- Operational safety (lockout/tagout, fire, electrical, chemical, and use)
- Safety training

Safety is not a standalone task; it must be incorporated into the overall project design. Safety evaluations shall be conducted throughout all phases of the OOI Project, including design, development, manufacturing, deployment, use, maintenance, service, and decommissioning.

4.1.4.9 Integration, Verification and Validation Plan

The OOI Integration, Verification and Validation (IV&V) Plan establishes task sequences and strategies for iterative and incremental integration of the subsystems within an IO, of subsystems across IOs, and of IO and OOI components with external interfaces, at successive stages of development. It describes the types of testing that will be conducted at each level of integration, and establishes criteria to both verify that the system requirements have been met, and to validate that user needs have been met by the delivered products. ISO 9126 serves as a framework of verification attributes and criteria. The terms Verification and Validation have the following meanings:

- Verification: Did you build the system right? – ensures conformance to requirements
- Validation: Did you build the right system? – confirms that the system satisfies the user's needs

IV&V Plans are written at both the IO and OOI levels. IO IV&V plans include all aspects of responsibility assigned to the IO while the OOI IV&V plan focuses on system of systems perspective and functionality. IO IV&V Plans provide a more detailed description of integration and testing strategies for the IO-specific components of the OOI.

Preparation and custody of the OOI IV&V Plan is the responsibility of the OOI Chief Systems Engineer and normally delegated to the OOI Test lead. Preparation and custody of each IO IV&V Plan is the responsibility of the IO Chief Systems Engineer. Each IO Chief Systems Engineer is responsible for delivery of a quality integrated system to the OOI. At the end of each IV&V phase, the OOI and IO Chief Systems Engineers must submit an IV&V Report to their respective Project Managers that includes a Requirements Verification Compliance Matrix.

Integration, Verification, and Validation activities are described further in Section 7 of this document.

4.1.4.10 Test Plans

Test Plans will be written at the IO level and will describe in detail the test activities to be conducted by the IO. Test Plans will be written using a standard template, and will contain information regarding the type of testing to be done, the purpose of the test, the test environment, the test equipment, the list of components to be tested, the integration level of the components, the list of requirements which will be verified by the test, assumptions and constraints, expected results, and the planned schedule and time required to conduct the test. Test Plans will organize individual tests into appropriate logical groupings, with a goal of minimizing redundancy and maximizing testing efficiency. Requirements Verification Matrices will be used to map requirements to test plans and to record verification results.

Program testing is described further in Section 7 of this document.

4.1.5 Work Directives

The OOI Program Office and OL management will monitor and administer the work directives of each IO. However, each IO will be responsible for the creation and reporting of work directives that implement any OOI effort. IOs will be responsible for, but not limited to:

- Developing individual IO work packages that describe the work to be done, resource sources, schedules, budget, and reporting requirements.

- Generating work authorizations for the IO team that provide approval for applicable teams or organizations to complete their work package requirements and to release applicable resources.

4.2 Assessment Process

4.2.1 Progress against Plans and Schedules

The OOI Program Office and OL management has and will continue to administrate and monitor the processes of each IO and their associated technical efforts, against IO submitted technical plans and schedule. Each IO is responsible for the creation and reporting of plans and schedules related to any OOI effort, and to monitor actual progress against them. IOs are responsible for, but not limited to:

- Identifying events, tasks, and process metrics for monitoring progress against plans and schedules.
- Collecting and analyzing identified process metrics data and results from completion of planned and scheduled tasks and events.
- Comparing process metrics data against plans and schedule to determine technical areas requiring management or team attention.
- Determining and implementing required changes to correct variances, making changes to the plan and schedule, and redirecting work.

4.2.1.1 Process Metrics

The set of process metrics selected for the OOI Program is presented in Paragraph 4.1.2.3. These process metrics are used for monitoring actual progress against technical plans and the tasks and events on the IMS.

4.2.1.2 Process Metrics Collection & Analysis

The IOs collect and analyze identified process metrics data and results from completion of planned and scheduled tasks and events. The process metrics data is compared against the plans and schedule to determine technical areas requiring management or team attention. Assessments are scheduled at regular intervals as determined by the Project Manager, at all milestone reviews, and at other decision gates as required. The primary goal is keeping open and thorough communication within the project team and with the stakeholders.

Progress of the technical effort is evaluated from two perspectives: Self Assessment Process and System Engineering Measures. The former is carried out on a monthly basis in conjunction with earned value management reporting to the Project Office, and consists of evaluation by the OOI Chief Systems Engineer of how system level processes are functioning, identification of problem areas, and communication of lessons learned.

The principal system engineering measure is earned value, as described in the PEP and as handled by the Project Manager. The Cost Account Managers (CAMs) are responsible for reporting cost and progress information to the Project Office on a monthly basis for incorporation into the IO's Earned Value Report to the OOI Program Office. The Project Manager determines the format and content of these reports.

4.2.1.3 Process Metrics Variances

Actual progress compared against plans expose variances, which are communicated to the Project Manager for possible action or wider distribution. The IO Program Managers are responsible for determining and directing required changes to correct these variances, make changes to plans and schedules, and redirect work.

4.2.2 Progress against Requirements

The OOI Program Office has and will continue to monitor and assess the progress of OOI system and task development through a comparison of defined system/task characteristics against requirements. This is done through use of general project management principles and tools, in conjunction with OOI SDE Collaboration Tools, such as the ITM/JIRA system for tracking action items and issues, and OOI SDE Configuration Management Tools, such as OOI DOORS for monitoring and managing requirements at all levels.

Further, there are processes, such as the Configuration Status Accounting process described in the Cyberinfrastructure Configuration Management Plan (CI CMP) as well as the *System Requirement Review* and *System Functional Review* sections in this document, which individual IOs follow in performing progress against requirements measurement and management, while aiding the progress toward maturity of the system/task (or portion thereof) being engineered.

4.2.3 Technical Reviews

OOI will conduct technical reviews of progress and accomplishments in accordance with the appropriate technical plans, as developed, managed and maintained by OOI and each IO. Technical reviews look to identify the review objectives and requirements cited in the respective plan, as well as considerations given to OOI policies, procedures, and agreements, as applicable. They will also help determine progress toward satisfying the technical review entry requirements and help prepare the materials constituting technical review package and presentation package.

4.2.3.1 Technical & Management Review Process

Entry Criteria: System-level Technical reviews (herein after referred to as “Reviews”) are conducted on an aggregate product after all the reviews on subordinate products have taken place. The system-level review concentrates on aggregate system performance and external interfaces, but also serves as the vehicle to identify and resolve any remaining configuration item interface or requirements disconnects. Grouping of multiple configuration item review sessions into a larger meeting event is permissible, and strongly encouraged from a resource and travel efficiency standpoint, however, for traceability, each review is conducted and documented individually.

Review Format: Review format is matched to the complexity and risk associated with the product or products being reviewed, and may be as simple as a conference call following document review if all parties are in agreement. More typically, the review consists of an in-person document walk through and discussion lasting a few hours. If substantial issues are discovered, the review may be rescheduled as a result or accomplished in multiple stages.

Review Panel Selection: In order to provide sufficient time for planning, perhaps as much as three months before the review, members of the external review panel are identified and individually contacted to solicit their participation. Internal participants are also selected so that a comprehensive attendee list can be constructed. Representation from the following organizations should be present to conduct a review:

- Project Management
- Quality
- Systems Engineering
- System Architecture
- Hardware
- Software Development
- Other groups as may be identified for technical or programmatic expertise

Location Selection: Perhaps two months before the review, a location is selected, and arrangements with a hotel are made for meeting rooms, breakout rooms, food services, and a block of rooms at a favorable rate.

Agenda Preparation: Perhaps two months before the review, the draft agenda is prepared and the internal presenters are notified of the subjects they are responsible for at the review.

Review Invitation: Perhaps one month before the review, all attendees are provided with a formal invitation that includes details about the meeting location(s), hotel accommodations, an updated agenda, when & where the review package is to be made available, and other administrative data.

Review Package: At least three days prior to the review, the review package, containing supporting materials, is assembled and loaded into a common work area for review. Additional lead time and technical content is encouraged whenever circumstances permit.

Conduct Review: The review is conducted at the appointed time and place beginning with the distribution of the final agenda.

Common Review Items: Certain items are revisited and evaluated at every review, including:

- System requirements documentation related to the products being reviewed are evaluated to confirm they are complete and current:
    - Controlled document format
    - All interfaces identified
    - Environments identified
    - Modes and states identified
    - Functional requirements identified
    - Performance requirements identified
    - Verification methods are identified
    - Requirements are traceable (justified)
- System design documentation related to the products being reviewed are evaluated confirm they are complete and current:
    - Design reflects the requirements
    - Methods selected for performing the required functions are logically sound
    - Degree to which the design is ready for verification
- Risk Assessment is made based on the degree of uncertainty present in the products being reviewed and the products that provide the underlying foundation:
    - Unknown or uncertain requirements and interfaces (i.e., TBx)
    - Key assumptions, confidence level, and dissenting opinions as to validity
    - External dependencies
    - Remaining actions, responsibility, schedule, and impact

Action Items: Action items are recorded at each review. Any action items that must be completed before formal closure of the review are so noted. Action Items are entered into the OOI Action Item Tracking System and monitored through closure.

Meeting Minutes: Within one week after the review, a set of meeting minutes is prepared that includes the following information:

- Meeting date, location, and purpose
- A summary of key findings and discussions
- Determination of configuration item development status
- A copy of the pre-meeting agenda for reference
- A list of all attendees, including position and institution represented
- A detailed list of all action items arising during the meeting

Meeting minutes are controlled by CM and placed in the DMS. The CM organization notifies participants of their location and availability.

4.2.3.2 Preliminary Design Review (PDR)

PDR is the external sponsor and science community review conducted to evaluate the progress, technical adequacy and risk associated with the emerging design approach. Emphasis is on complete understanding of the requirements, including environments and operating modes and states, to ensure that subsequent detailed engineering design activities can be initiated with minimum risk of rework or wasted effort. Unlike informal peer interaction or periodic meetings, the PDR is specifically structured for the purpose of validating the requirement set and assessing initial design progress.

The PDR scope ranges from the system level concentrating on aggregate system performance and external interfaces, but also serves as the vehicle to identify and resolve any remaining configuration level item (configuration item) interface or requirements disconnects. Configuration item reviews focus on required behavior within the configuration item and establishing defined interfaces

PDR is conducted after preliminary design efforts, but before the start of detail design.

Evaluation Elements of the PDR include:

- Evaluating the progress, technical adequacy, required behavior, and risk resolution (on a technical and schedule basis) of the selected design approach.
- Determining its compatibility with performance and engineering specialty requirements.
- Evaluating the degree of definition and assessing the technical risk associated with the selected manufacturing methods/processes.
- Establishing the existence and compatibility of the physical and functional interfaces among the configuration item and other items of equipment, facilities, computer software, and personnel.

For software, the PDR focuses on:

- The evaluation of the progress, consistency, and technical adequacy of the selected top-level design and test approach.
- Compatibility between software requirements and preliminary design.
- The preliminary version of the operation and support documents.
- Preliminary performance estimates

4.2.3.3 *ifdr* – Internal Final Design Review

The *ifdr* is an internal **Engineering Technical Design Review** (not to be confused with the NSF Final Design Review process) conducted by the OOI Program Office to evaluate the progress, technical adequacy, and risk associated with the detail design solution **prior to the release of drawings/specifications for manufacture or purchase of materials**. Emphasis is on complete representation of the design; to the degree to which the proposed design meets the associated requirements, the nature, and extent of any derived requirements that are introduced as a result of specific design choices, and the overall risk to proceed into implementation.

The *ifdr* may be incremental, provided the capstone *ifdr* takes into account the inter-relation of the entire system and addresses issues that arise with respect to conflicts in module fit and operation with relation to each other and the system. For large complex configuration items, the *ifdr* may be a progressive review, culminating in a system level FDR which essentially reviews the completeness of preceding *ifdr*s and ensures adequate interfaces between the configuration items. For the product or products under review, the complete subsystem design is presented, highlighting all design changes made with respect to the design disclosed in the PDR, providing rationale for the changes.

All OOI systems are required to undergo an *ifdr* after the external FDR and start of the MREFC Program. This type of *ifdr* is commonly referred to as a critical design review.

Entry Criteria:

- Successful completion of all action items related to the previous review (PDR, external FDR)
- Advanced scheduling and published agenda
- Acceptance of all applicable requirements
- Successful demonstration of the prototype system or critical components

Exit Criteria:

- Acceptance of published minutes to include list of attendees
- Completion of all action items assigned to the IOs
- Acceptance of any requirements due at the ifdr
- Concurrence from the OOI Program Office/IO members that all issues in the review agenda have been addressed

The Project Manager is the final arbiter of unresolved issues.

Evaluation Elements:

1) Evaluate the progress, technical adequacy, required behavior, and risk resolution (on a technical and schedule basis) of the selected design approach.
2) Determine its compatibility with performance and engineering specialty requirements.
3) Evaluate the degree of definition and assess the technical risk associated with the selected manufacturing methods/processes.
4) Establish the existence and compatibility of the physical and functional interfaces between the configuration item and other items of equipment, facilities, computer software, and personnel. N2 diagrams must be developed for major sub-systems and configuration items.
5) For new development hardware configuration items, evaluate producibility analyses conducted on system hardware.
6) For new development hardware configuration items, review preliminary hardware product specifications.
7) The IOs shall supply a copy of all existing engineering calculations related to calculating design life. COTS supplied data sheets and COTS supplied calculations for their

equipment design life shall be included with the design life calculations as they become available.

For software, the review has and will focus on:

1) The evaluation of the progress, consistency, and technical adequacy of the selected top-level design and test approach.
2) Compatibility between software requirements and preliminary design.
3) The updated versions of the operation and support documents.

4.2.3.4 FDR – Final Design Review

FDR is the external sponsor's review, conducted to validate the design, cost, schedule and program management control systems. FDR scope includes assessment of the technical and project-management components of the program, in order to assess the full readiness for construction, and the level of confidence that the project can be delivered within the parameters defined in the project baseline.

FDR Criteria are:

Note: Bold items indicate direct reference to the NSF Large Facilities Manual (NSF 07-38)

1) **Final construction-ready design**: delivery of designs, specifications and work scopes that can be placed for bid to industry, including:
   a) Key functional (science, system and sub-system) requirements and performance characteristics, including internal interfaces and interconnections
   b) System architecture and equipment configuration, including how the OOI interfaces with other systems
   c) Operational concept
   d) Reliability criteria, analysis, and mitigation
2) **Tools and technologies needed to construct the project**
   a) Technical maturity of critical components (including core sensors)
      i) Industrialization of key technologies needed for construction (made consistently, not necessarily COTS)
   b) Overall development and production schedule (within resource loaded schedule) of outstanding components in pre-construction phase, including
      i) Milestone reviews
      ii) Design reviews
      iii) Major tests
3) **Project execution plan** including
   a) Project organization/governance including
      i) Organizational structure (tied to WBS includes roles, responsibilities, reporting)
      ii) Governance, including advisory structure
      iii) Completion of recruitment of key staff and cost account managers needed to accomplish the project
      iv) Managing sub-awardees

b) Acquisition-Acquisition plans, sub-awards and subcontracting strategy including
   i) Competition strategy
   ii) Types of contracts to be awarded
   iii) Contractor(s) responsible for developing and implementing the system, where feasible
c) Internal and institutional oversight plans, advisory committees, and plans for building and maintaining effective relationships with the broader research community that will eventually utilize the facility to conduct research [Governance]
d) Education and outreach plans
e) Environmental compliance (NEPA) [see #7 below]
f) Plans for transitioning to operational status
g) Configuration control plans
h) Working with interagency and international partners
   i) Finalization of commitments with interagency and international partners

4) Fully implemented Project Management Control System, includes:
   a) Baseline version of resource-loaded schedule
   b) Mechanisms to generate reports-using EVMS-on monthly basis and use as a management tool
   c) Path dependencies, schedule float, and critical path are defined

5) Updated budget and contingency, including risk analysis, presented in a detailed WBS format with WBS dictionary defining scope of all entries
   a) Refined bottom-up cost and risk estimates and contingency estimates
   b) Refined description of the basis of estimate for budget components
      i) Majority of cost estimates derived from external information
      ii) Basis of estimates integrated in WBS dictionary/cost book
   c) Refined project risk analysis and description analysis methodology
      i) Risks include cost escalation and volatility in OMB escalators, etc.
   d) Refined contingency and contingency management (budget, scope, schedule)
      i) Prioritized scope [to achieve science, time vs. dollars, critical points where in schedule decisions are made to ensure zero cost overruns. Plan with Front-End options]
      ii) Integration of prioritized scope in schedule and cost (including O&M for upscope)

6) Fit-up and installation details of major components and commissioning strategy [Fit-up synonymous with interface integration, hardware and software]
   a) Systems integration
   b) Testing and acceptance
      i) Number of tests
      ii) Criteria for entering into testing
      iii) Exit criteria for passing test
      iv) Where tests are to be conducted
   c) Commissioning
   d) Operational readiness criteria-by component and by project

7) **Plans for QA and EHS-reporting and mitigation**

   Plans relative to the construction period including OL management of IO policy and procedures implementation.

8) Updated operating estimates

4.2.3.5 Test Readiness Review (TRR)

This review ensures that a subsystem or system is ready to proceed into formal test. The TRR assesses test objectives, test methods and procedures, scope of tests, and safety, and confirms that required test resources have been properly identified and coordinated to support planned tests.

The TRR is an internal review conducted to evaluate the overall readiness to enter formal verification testing. Emphasis is on complete definition of the unit under test and the environment needed to conduct the test, availability of resources and facilities, and on establishment of clear pass and fail criteria.

TRRs are conducted as early as a high fidelity design article and associated test planning data become available.

As a minimum, the necessary supporting materials shall include the system requirements document and Verification Matrix for each configuration item, together with the test plan.

Any TRR issues, however slight, introduce a risk that the verification results are only partially transferable to the final article and must be carefully weighed during the TRR.

4.3 Control Process

4.3.1 Outcomes Management

OOI achieves Outcomes Management through a variety of tools and processes. Much of Outcomes Management is a natural derivative from use of the OOI SDE Configuration Management and Collaboration Tools, such as OOI DOORS, OOI DMS, ITM/JIRA, GIT or Subversion. The culmination of use of the tools and processes enable the capture the outcomes, descriptions of methods and tools used, decisions and assumptions, lessons learned, and other data that allow for tracking requirements.

For example, the OOI DOORS platform is used to manage and track stakeholder requirements, system technical requirements, derived technical requirements, specified requirements, approved changes, and validation results, while the OOI DMS based on Alfresco allows for data and document management such as logical and physical solution representations.

Further, processes have been set in place for OOI and within each IO outlining how to perform configuration management in accordance with the Configuration Management Plan, such as the *OOI Configuration Management Plan* and the *CI Configuration Management Plan*.

4.3.1.1 Requirements Management

Requirements definition constantly evolves throughout the project life cycle, and hence is an ongoing activity. Requirements and their provenance are captured and managed using the Telelogic-based OOI DOORS tool.

The requirements definition process results in a hierarchy of documents. At the top of the requirements hierarchy are the Level 1 Requirements, which are encompassed in the National Science Foundation Cooperative Agreement and NSB Guidance. Level 2 (L2) Requirements, that annunciate key OOI requirements, are found in the set of Level 2 requirements modules that are under configuration control with the OOI Chief Systems Engineer as custodian. These include:

- L2 Science Questions
- L2 Science Requirements
- L2 Cyber-User Requirements
- L2 Educational Requirements
- L2 Operational Requirements
- L2 Common Requirements
- L2 Reference

L2 Requirements modules serve as the top-level description of the OOI desired capabilities. Requirements Traceability is maintained within DOORS linking the L3 and L4 IO-specific requirements to the L2 acquirer requirements. The Chief Systems Engineer for each IO is responsible for ensuring that all requirements are stated in an atomic, clear, verifiable manner with source traceability. The IO Chief Systems Engineers and IO Chief Architects are responsible for trade studies, constraint evaluation, and cost-benefit analyses that affect IO specific requirements. Requirements review is a key purpose of each Life Cycle Objectives milestone review for the Cyberinfrastructure IO, that is roughly analogous to the waterfall model Concept Design Review.

System requirements are at Level 3 (L3), which in the requirements hierarchy correspond to IO system specific requirements. Level 3 requirements include –

- The *L3 IO System Requirements*: under configuration control with each of the IO Chief Systems Engineers as custodian.
- The *L3 CI-CG Interface Requirements Specification*: under configuration control with the IO Chief Systems Engineers sharing joint custody.
- The *L3 CI-RSN Interface Requirements Specification:* under configuration control with the IO Chief Systems Engineers sharing joint custody.
- The *L3 CG-RSN Interface Requirements Specification:* under configuration control with the IO Chief Systems Engineers sharing joint custody.
- The *L3 CI-EPE Interface Requirements Specification:* under configuration control with the IO Chief Systems Engineers sharing joint custody. (to be developed)

The IO requirements modules are subject to review by the stakeholder communities and approval by the OOI Program Office. It is the responsibility of the IO Project Scientist and IO EPE Manager to communicate user-initiated proposed changes to the IO Chief Systems Engineer and IO Chief Architect on an ongoing basis. It is also the responsibility of the IO Project Scientist and IO EPE Manager to communicate changes in IO capabilities to the stakeholder communities, all of which is described in detail in *Section 5.1* of this document

Subsystem requirements reside at Level 4 (L4), and individual system elements are captured in all lower levels.

The OOI Requirements Management System: The OOI DOORS platform is hosted and maintained by the network administrators at the OOI's CI group at the University of California, San Diego. It incorporates all of the inherent capabilities and general functionality of object-oriented requirement management systems, and benefits from OOI-specific configurations requirements.

OOI DOORS is comprised of various major interlinked objects, including levels, modules, components and views.

Levels (of a Project)	Levels are the top aggregate of objects within a Project. They define the basic structure and hierarchy of the requirements. For example: **1.** Level 1) OOI **2.** Level 2) Project **3.** Level 3) System **4.** Level 4) Subsystem Intermediate levels are often useful, for example, Levels 2a, 2b or 2.5, 3.5 etc. are acceptable as it acknowledges hierarchy within a level
Modules	A database collection of requirements, headings, info, tables, figures, TOC, etc for a specific project entity. • **Module Tree:** shows levels and modules based on the project's organization and work breakdown structure • **Module:** An electronic collection of requirements, headings, info, tables, figures, TOC, etc., formerly called a "document" • **Element:** A general term used to specify a project entity that can be assigned requirements and whose data resides in a module. • **Custodian:** Person responsible for each module
Components	Components are within modules, and usually are considered the individual "requirement". Components in DOORS contain - • ID: A unique number identifying each object. – Created automatically by DOORS sequentially upon entry of any new OBJECT TEXT • Header: Section number and a title describing the contents of that section • Requirement: A verifiable shall statement (usually linked for traceability) • OBJECT TEXT: The text of a header, information or requirement • OBJECT SHORT TEXT: A brief summary of the requirement (optional) • Attribute: A DOORS term for data items associated with objects and links, used for additional information, control and filtering
Views	A display of selected information in a specified format. A view resides in a module, but can draw and display information from other linked modules (higher level, lower level, same) and is named to reflect what attributes are visible to the user of the view
Documents	Any view may be defined as a "document" for a specific need, and exported to a Word or PDF file for distribution. A document is typically a collection of requirements, headings, information, tables, figures, TOC, etc., created by a view of a module which may include information from one or more other modules. Documents are for reference only; they are not necessarily controlled under OOI Configuration Management.

4.3.1.2 Information Database

The OOI Information Database consists of several different database tools and repositories, including those in the OOI DOORS platform and the Software Application Framework (SAF). OOI records are maintained, including the following key products that are used for managing the outcomes of the system development effort.

- Science Requirements Baseline
- Science Traceability Matrix
- Engineering Design Baseline
- System Level Engineering Requirements Document
- Configuration Level Item Engineering Requirements Documents
- Configuration Level Item Interface Control Documents

- Configuration Level Item Verification Results
- System Level Verification Results

4.3.1.3 Verification Matrix

DOORS is also used to maintain Test Procedures in the form of Test Procedure Modules. Links are established between individual requirements maintained in the Requirements Modules and individual Test Procedures maintained in the Test Procedure Modules. This provides a Verification Matrix between each individual requirement contained and the specific verification method that was utilized. The Verification Matrix is prepared, reviewed, released, controlled, and maintained in accordance with the CMP.

4.3.2 Information Dissemination

OOI and the OOI Program Office ensure that required and requested information is disseminated in accordance with agreements with the IOs, OOI project plans, policies, and procedures. OOI uses not only set communication and information processes, but also software and system tools to help disseminate information, such as, but not limited to, program/progress status, planning information; requirements, technical data material; design data and schemas, lessons learned; data deliverables and work directives resulting from management decisions, planning, or approved changes.

The OOI Collaboration Tools play a major factor in how information is disseminated not only within OOI, its IOs and its members, but also to external communities, key third parties, and the general public. For information dissemination, OOI Collaboration Tools such as the OOI DMS (based on the Alfresco platform) and the OOI Wiki (based on the Confluence platform) have played pivotal roles in accomplishing this.

4.3.2.1 OOI Wiki

Atlassian's Confluence Enterprise is the Wiki used by the OOI. The OOI Wiki is used not only as social software, allowing for collaborative communication throughout various associated communities, but also as an information portal where a vast amount of disparate information can be collected, jointly authored, collated, managed and distributed from a single source. Acting as a singular source of dynamic information creation, editing, posting and storage, Wikis create a community of users and information seekers, allowing for a simplified view of important information, while also enabling a feedback mechanism which not only allows for additional input, but also foster continual community interest, communication, and growth.

The OOI Wiki enables enterprise information management, allowing contributors from across organizations and geographic locations to pool and share all of their information together using a simple but effective interface, boosting general information sharing within an organization and out. As a main collaboration tool, the enterprise-level OOI Wiki incorporates functionality necessary for multiple users and groups, with access and security considerations. Different levels of permissions, either based on user or group, can be fine-grained to decide who is able to view, create, edit and comment on particularly information. The OOI Wiki is hosted and maintained by the network administrators at OOI's CI group at the University of California, San Diego.

"Spaces" have been defined within the OOI Wiki for the sake of hierarchically arranging information based on Program Office or specific topic areas. The naming convention for "Spaces" is designated by Group or IO, and then topic area. For example, one "space" has been designated as the "OOI Engineering Space", which denotes that this OOI space belongs to any topic area related to systems engineering efforts, and deals with their education and public engagement topics. Once you have entered a space, you will not only see the creator of the space, but also the last person who has edited the space, or articles within.

4.3.2.2 OOI DMS

The Alfresco Document Management software is the basis for the OOI Document Management System (DMS) portion of the Collaboration Tools. Document Management software enables a unified, extendible digital solution of how documents are created, stored, filed, retrieved, secured, recovered, retained, archived, distributed and authenticated; all of which span near-unlimited locations (only limited by connectivity).

The central repository aspect of the OOI DMS efficiently store libraries of documentation, as well as past revisions and versions. This central repository not only allows for disparate groups and individuals to gain access to the proper documentation, but also provides an easy to use, single source of access to all of the documentation they require. It also enables various policies that documents within the repository are subject to, including but not limited to organizational security, disaster recovery, retention, and archive policies.

Version Controls with Document Management software give strong support to the change process within tasks and the project, that the OOI DMS automatically inherits from the Alfresco base. This allows for previous version of documents to be archived, thus not only preserving previous versions, but also enabling better program oversight as documentation can be monitored within its iterative states.

Document Management software also enables a true sense of workflow associated to each critical document within a project and/or organization, thereby allowing documents to be controlled in a fashion where creation, editing, and deletion is tracked, monitored and managed. Workflow is defined more narrowly as the automated movement of documents or items through a sequence of actions or tasks that are related to a business process. Workflows are used to consistently manage common business processes within an organization by enabling the organization to attach business logic to documents or items in a DMS or library. Business logic is essentially a set of instructions that specifies and controls the actions that happen to a document or item.

OOI also utilizes its OOI Configuration Management Tools to aid in information dissemination. This includes the OOI DOORS platform, the ITM/JIRA system, and the OOI Subversion/GIT platform.

4.3.2.3 Deficiency Management

The OL Chief Systems Engineer is responsible for oversight of system-level activities to detect problems and for the maintenance of the Deficiency List. The Deficiency List is conveyed to the Project Manager together with a monthly report on the system for inclusion in the corresponding report to the Program Office.

4.3.2.4 Waivers and Deviations

Waivers can be requested if there is a preponderance of evidence that the degree to which a particular requirement is met does not materially impact higher level functionality. Deviations are associated with accepting a performance level other than that normally required. Both are legitimate design and risk management tools, but must be very carefully reviewed and approved based on the merits of each individual situation.

Waivers and deviations are prepared, reviewed, released, controlled, and maintained in accordance with the CMP. Any proposed waiver or deviation with impact to basic Science Requirements shall require the approval of the Principal Investigator and the Project Director before implementation. All waivers, including waivers from safety or design standards must be formally documented and submitted for approval.

5 System Design

System Design processes provide validated system definitions in the form of requirement specifications, logical solutions, and physical solution representations that can be efficiently implemented with acceptable risk. The OOI system design sub-processes, shown in **Error! Reference source not found.**, produce functional and physical designs from the program high-level requirements and concepts.

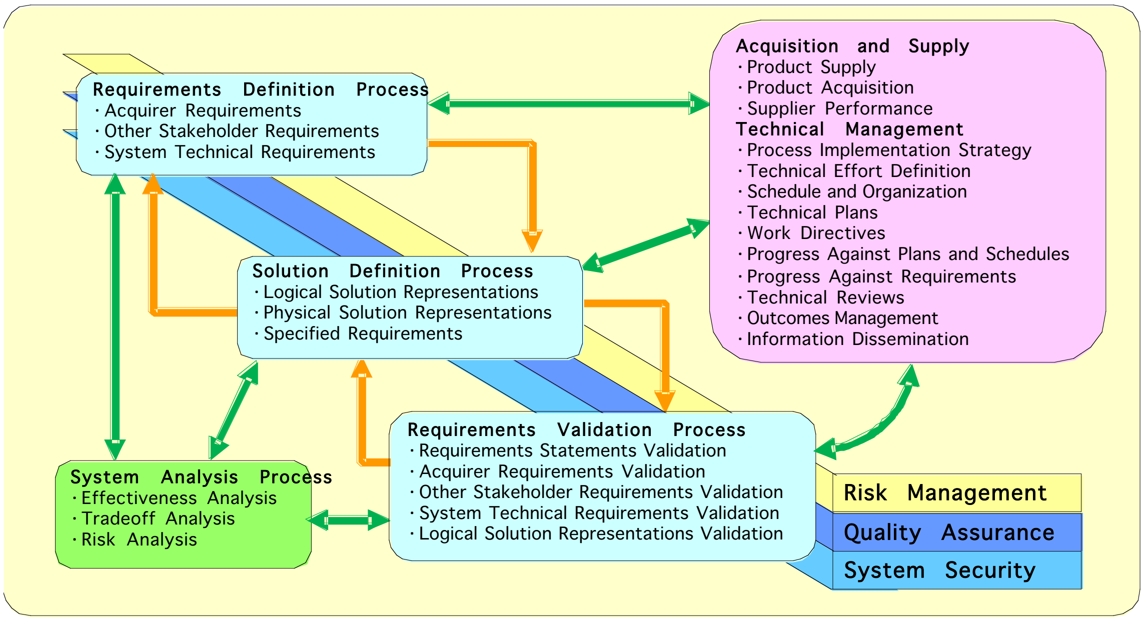

Figure 12, System Design Processes

The System Design process followed by the OOI Team has six steps:

1. Acquirer Requirements are gathered from workshops, published literature, and the experience of the OOI Team and captured in the set of L2 requirements modules/documents. For OOI, L2 contains the OOI or system of systems requirements. The Acquirer Requirements drive the System Technical Requirements.
2. Other Stakeholder Requirements are also gathered and captured in the set of L 2 system of systems requirements modules/documents. Other Stakeholder Requirements also drive the System Technical Requirements.
3. System Technical Requirements are developed from the L2 requirements that include Acquirer and Other Stakeholder Requirements and captured in the set of Level 3 requirements modules/documents. For OOI, L3 contains the system requirements for the CI, CG, RSN and EPE Systems, as well as the Interface Requirements Specifications documenting inter-IO interfaces and agreements. The System Technical Requirements drive the logical and physical solution representations.
4. Logical solution representations are driven by the System Technical Requirements and iterate with the physical solution representations until convergence on an optimal design solution.
5. Physical solution representations are driven by the System Technical Requirements and iterate with the logical solution representations until convergence on an optimal design solution. The design solution identifies the physical components, or subsystems, for each of the systems; the System Technical Requirements are allocated or assigned and, where appropriate, additional requirements are derived.
6. Specified Requirements are the allocated or assigned System Technical Requirements combined with the derived requirements for each subsystem and are captured in the set of

L4 requirements modules. The L4 requirements modules correspond to configuration items that are independently developed and maintained under configuration control. L4 requirements modules can be further decomposed into lower levels (e.g., elements, components, units) that can be either developed or used as part of the acquisition process.

Use of an iterative life cycle does not alter the function of system engineering, and in fact it becomes the key activity that binds the cyclically growing system into a coherent whole. The system engineering framework used by the project is a tailored version of that defined in the System Engineering Handbook Version 3 issued by the International Council on Systems Engineering (http://www.incose.org).

System engineering is a triumvirate of processes that places equal emphasis on Requirements Analysis, Operational Analysis, and Architectural Analysis. As shown in Figure 13, the three primary processes and their sub processes are continuously executed in a spiral manner that defines progressively more detailed levels of the system during each loop through the triumvirate.

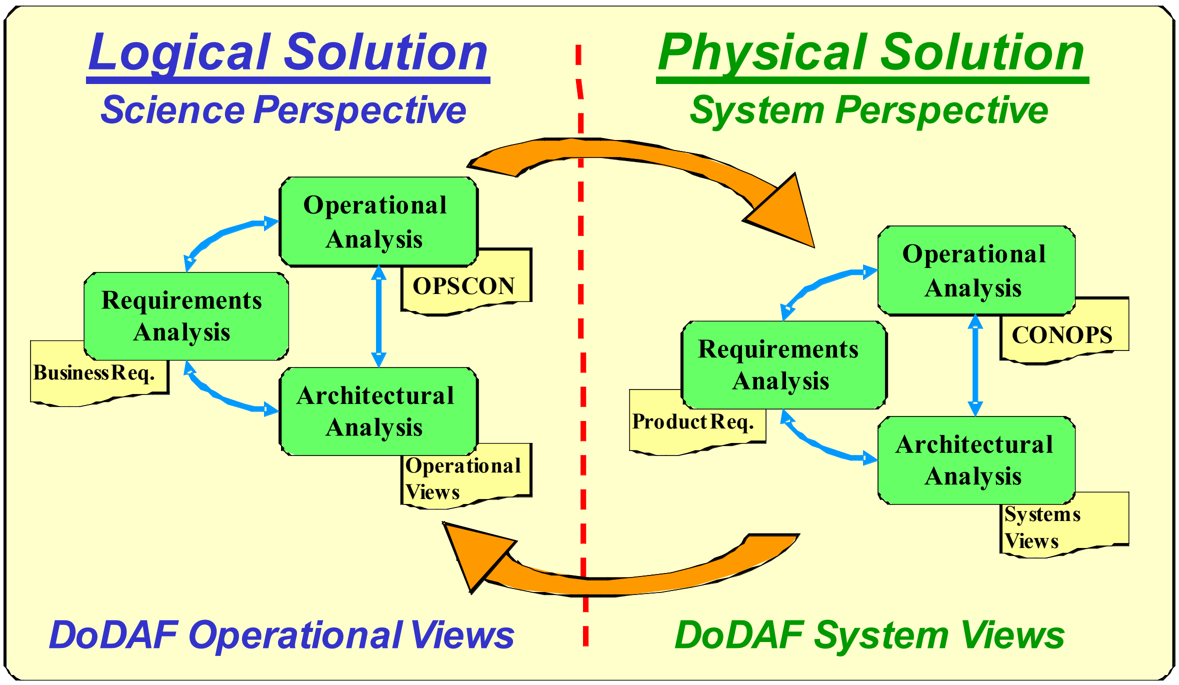

Figure 13, System Engineering Triumvirate

The entire process begins with an examination of user requirements. Iterations through the triumvirate of processes are executed until the science perspective is thoroughly understood and the operational views, which represent the logical solution, have been fully developed. This is followed by additional Iterations through the triumvirate of processes until the system perspective is thoroughly understood and the system views, which represent the physical solution, are fully developed. As concepts are exposed or developed, iterations back and forth between the science and system perspective are executed until the operational views and the system views are balanced.

Under the triumvirate approach as implemented for the OOI project, the IO Chief Systems Engineer is responsible for IO Requirements Analysis, including the OOI Level 2 System Requirements, and for system perspective Operational Analysis. The IO specific architects, assisted by both OOI and other IO engineers and architects as necessary,, are responsible for the architectural design of the system, including production of the design documentation. The IO project scientist is responsible for science perspective operational analysis, including devising use case scenarios that can be used by system and project test groups for validation that user requirements have been met at the time of deployment.

5.1 Requirements Definition Process

Generally, the OOI requirements originate from the user requirements. The IO System requirements present more detailed requirements than the OOI Level 2 Requirements, and enable the science requirements for the system.

The process for discovering and tracing requirements has been described and demonstrated in the OOI Level 2 Requirements (L2), OOI Science Prospectus, and elsewhere. The science drivers are captured in the OOI Science Prospectus through a series of science questions that are traced down to a particular location and a list of sensors necessary to answer the science questions. Requirements are refined and carried through to the subsystems and components in subsequent requirements development meetings with scientists, other users, and the IOs.

All requirements, starting with the OOI L1 Requirements at the top level, are maintained in a DOORS database. OOI follows a standard systems engineering approach for setting requirements at successive levels of detail, maintaining traceable relationships between them, and testing them appropriately. The relationships between science requirements, system requirements (at all levels), and conformance tests will be maintained using DOORS.

5.1.1 Acquirer Requirements

OOI Acquirer Requirements define a validated set of acquirer requirements for the OOI, and all portions thereof. They encompass much of the L2 Requirements and identify, collect, and prioritize assigned, customer, user, or operator requirements for OOI, including any requirements for development, production, test, deployment/installation, training, operations, and support/maintenance.

5.1.1.1 Stakeholder Engagement

The OOI is based upon a community vision resulting from two decades of workshops, meetings, and reports, which has established science drivers for the proposed infrastructure investment. Examples of science questions are:

- What processes control volatile exchange at the air-sea interface and within the ocean?
- Do severe mixing events, such as large storms or eruptions, affect water column processes?
- Do plate tectonics and seafloor roughness modify fluxes and mixing and influence biological communities in the deep ocean?

These and other topics are explored further in the science traceability matrices in the *Ocean Observatories Initiative Science Objectives and Network Design: A Closer Look* (OOI Science Prospectus), that are graphical representations showing the logical flow from high-level science questions to the overall design of the proposed OOI infrastructure.

An important element of system-level stakeholder engagement is the process of eliciting user requirements from representatives of the science and education user communities through formal workshops, technical interchange meetings, or systems engineering work sessions. Stakeholders who have an interest or stake in the outcome of the project have been identified and their needs are the driving force behind the OOI Requirements. The primary stakeholders are scientists, modelers, and educators that use the system for a variety of reasons. For example, the CI IO has held a series of formal workshops have been conducted to elicit stakeholder requirements and to identify, collect, and prioritize assigned, customer, user, or operator requirements for the system, and portions thereof, including any requirements for development, production, test, deployment/installation, training, operations, support/maintenance, and disposal of the system's products. Each of the Formal Workshops was crafted to have a particular technical emphasis, for example:

- Ocean Observing Programs Requirements
- Data Product Generation Requirements
- Integrated Observatory Management Requirements
- Education and Public Engagement Requirements
- Ocean Modeling Requirements
- User Applications Design

A second key element of stakeholder engagement is the inclusion of selected stakeholders at milestone reviews, especially all Initial Operating Capability Reviews where the previous software release is evaluated and the requirements and plans for the next one are described.

5.1.1.2 OOI Acquirer Requirements Set

The composite set of OOI Acquirer Requirements, gathered from science, programmatic, environmental, and other sources, is captured and controlled in a hierarchically organized manner. The set of OOI Acquirer Requirements is at the top (Levels 1&2), system requirements at Level 3 (L3), subsystem requirements at Level 4 (L4), and individual subsystem components captured in lower levels. The acquirer requirements are recorded in the DOORS in the following set of Level 2 Requirements modules:

- L2 Science Questions
- L2 Science Requirements
- L2 Cyber-User Requirements
- L2 Educational Requirements
- L2 Operational Requirements
- L2 Common Requirements
- L2 Reference Module

Each of these OOI DOORS modules is a configuration item that contributes to the definition of individual items that must be developed. The acquirer requirements captured in each of the Level 2 modules are coordinated to facilitate traceability of requirements from the system-of-systems to any lower level. Acquirer requirements are prepared, reviewed, released, controlled, and maintained in accordance with the *OOI Configuration Management Plan (CMP)*.

5.1.1.3 L2 Science Questions

Multiple workshops and reports have identified the OOI Level 2 (L2) Science Questions and high priority areas of ocean research that require the infrastructure envisioned in a state-of-the-art ocean observing network area. These topics have been described in the *OOI Science Plan*, *Ocean Sciences at the New Millennium*, and *Ocean Research Interactive Observatory Networks (ORION) Workshop Report*. The science in these reports mirrors many interdisciplinary themes described in *Charting the Course for Ocean Science in the United States for the Next Decade: An Ocean Research Priorities Plan and Implementation Strategy*.

The main research areas, which constituted the basis of how the OOI L2 Science Questions were developed, are listed below. These OOI L2 Science Questions also bear the ultimate goals of which all OOI-related requirements support, and are maintained by the OOI Program office within DOORS:

- Ocean-Atmosphere Exchange.
- Climate Variability, Ocean Circulation, and Ecosystems.
- Turbulent Mixing and Biophysical Interactions.
- Coastal Ocean Dynamics and Ecosystems.
- Fluid-Rock Interactions and the Sub-seafloor Biosphere.

- Plate-Scale, Ocean Geodynamics.

5.1.1.4 L2 Science Requirements

Project science requirements provide the foundation of the design process, and establish the functions and performance levels the installed instrument delivers. The OOI Level 2 (L2) Science Requirements are the first order design variables and are carefully protected throughout the development period. The OOI L2 Science Requirements have been derived from the *OOI Science Plan* and traceability matrices, and are maintained in OOI DOORS.

Modifications to the science requirements shall be made only based on specific authorization by the Principal Investigator (PI), and all changes shall require approval by the CCB in accordance with the process set forth in the CMP, with OOI Level 2 Science Questions driving rationalization.

5.1.1.5 L2 Cyber-User Requirements

The basis for the OOI Level 2 (L2) Cyber-User Requirements were part of the initial OOI system requirements that are part of the CI Conceptual Architecture, and were developed from an examination of existing observatory projects (LEAD, SIAM, SSDS, IOOS DMAC, and VENUS/NEPTUNE Canada) along with input from the OOI advisory structure and the OOI Science Plan. Further OOI L2 Cyber-User Requirements definition involves stakeholder communities organized through the CI Project Scientist and CI Education and Public Engagement (EPE) Manager, and the entire CI development team. Additional inputs to the Cyber-User Requirements are the policies that govern use of OOI resources. Their specification follows a parallel process, but may involve negotiation with the marine IOs, and may require OL Program Office approval. The OOI L2 Cyber-User Requirements are divided into four major categories (functional requirements, performance requirements, design principles, and interface requirements), and then further sorted into categories that are consistent with the CI subsystems.

The OOI L2 Cyber-User Requirements are captured throughout the project through direct stakeholder involvement. The OOI L2 Cyber-User Requirements capture process is iterative in nature to provide immediate stakeholder feedback and requirements adjustment. The creation of infrastructure prototypes provide further feedback for stakeholders and validate selected requirements. With early prototypes, it is possible to detect technology risks expeditiously and constrain stakeholder expectations.

5.1.1.6 L2 Educational Requirements

OOI Level 2 (L2) Educational Requirements were developed through a mission to reshape the way ocean science is conducted by providing ocean researchers with access to near real-time data, the ability to control/configure sensors and mobile assets, high data rate capability for images, powerful Cyberinfrastructure , and data visualization and modeling tools to conduct their research. In a parallel trend, recent advances in the delivery of web-based education, and use of visualization technology and data visualization tools in educational contexts, have lead to development of on-line platforms for instruction that engages students in active scientific inquiry, incorporates computer simulations of real-world phenomena, and involves collecting and analyzing data. Capitalizing on the burgeoning fields of information and visualization technology and the increasing power of the Internet, OOI education and public engagement (EPE) programs will use technology to advance ocean science education and outreach in much the same way that the OOI will advance ocean research. By investing in education infrastructure for the OOI, the ocean research and education community will be positioned to establish an ocean science EPE program of unprecedented technical sophistication.

OOI has sought guidance through leading academics, white papers, and agencies intimately familiar with education and ocean sciences, These OOI L2 Educational Requirements stem directly from the community consensus established during the OOI Education Drivers and Requirements Workshop (June 2008) and vetted at Final Design Review. They are well aligned with National Science Board (NSB) priority recommendations for an NSF Science, Technology, Engineering, and Mathematics (STEM) education roadmap. Developed requirements are based in these primary goals:

- Support research on learning and educational practices and the development of instructional materials.
- Develop human capital (e.g., STEM workforce development).
- Increase public appreciation for and understanding of STEM.

NSF has offered guidance that education infrastructure for OOI would be something that depreciates over time and needs to be bought, developed, and/or maintained.

OOI L2 Educational Requirements are maintained in the OOI DOORS requirements repository.

5.1.1.7 L2 Operational Requirements

OOI stakeholders have identified Level 2 (L2) Operational Requirements by identifying requirements and the concept of operations for data product generation, ocean observing programs, education and public engagement, and integrated observatory management.

The OOI L2 Operational Requirements, system and subsystems specification efforts have and will deliver white papers, requirements, and artifacts depicting the operational aspects of the OOI. The white papers are framed as executive summaries that provide the high–level view of the operations and subsystems interconnections. The set of artifacts will be scoped to the available time frame.

5.1.1.8 L2 Common Requirements

The OOI Level 2 (L2) Common Requirements contain requirements that apply to all IOs and are fundamental to achieving the goal of the OOI. These requirements reflect that the OOI is designed from the start to provide key features for ocean science:

- Persistence: Designed for long-term (greater than 25-year) operation, support, and data access
- Geographic Range: Consistently occupying larger volumes of multiple oceans to adaptively observe ocean processes on multiple scales
- Mobility/Portability: Able to go where the action is and the science demands
- Control/Adaptability: Responsive to commands addressing real-time needs
- System Interoperability: Common ways to exchange information and do science
- Intercommunication: Connected systems
- High Power/Bandwidth: Experiments and observations freed from traditional limits
- Sensor Capability: Increased spatial, temporal, and measurement resolution
- Community: Building sharing and interactions across all scientific endeavors

5.1.2 Other Stakeholder Requirements

Should there be any additional requirements needed outside of the capture and management through the aforementioned text, OOI shall identify all other possible OOI stakeholders in the same manner that it already has, by:

- Identifying, collecting and recording other stakeholder requirements that may affect development, production, test, deployment/installation, training, support/maintenance of OOI
- Ensuring that the resulting set of requirements agrees with other stakeholder needs and expectations

5.1.2.1 Security Management

The OOI Chief Systems Engineer is responsible for preparing and implementing the Security Management Plan that covers all aspects of operational and CI security for the systems, including defining the software and hardware “best practices” (e.g., firewalls, one-time passwords, anti-virus software) that are used to protect against intrusion and the processes used to define and manage reportable incidents both within OOI and at the federal level. It also describes the authorization and auditing policies for each of the IOs at different levels of access and the ongoing process for ensuring that repositories remain free from external aggression. Compliance with national security requirements is also described. The Security Management Plan incorporates any additional requirements imposed by the Program Office and NSF.

5.1.2.2 Programmatic Requirements

While science requirements form the core of the design process, a host of additional requirements must also be simultaneously satisfied. OOI programmatic requirements include, but are not limited to, fulfilling international treaty obligations, compatibility with existing transportation and handling resources whenever possible, user safety, and many other aspects critical to the instrument design yet not directly tied to specific science requirements.

5.1.2.3 Additional Requirements Sources

Many other sources of requirements exist that must be captured and managed during the overall development period. Examples include compatibility with existing development tools and test equipment, safety and ergonomic provisions, and the need for test and repair access.

5.1.2.4 Parts, Materials, Process Selection

In accordance with the OOI Physics of Failure methodology, parts materials are constrained to match the deployed environments.

- **Determination of Prohibited Materials:** The *OOI L2 Common Requirements* will contain the overall list of prohibited materials, and individual subsystem requirements are free to impose additional restrictions as dictated by the application, as they are derived.
- **Use of Commercial and Industrial Parts:** The use of commercial off-the-shelf (COTS) products is becoming increasingly commonplace in high reliability programs. Accelerating rates of COTS product enhancement is a major driver of this process. Wherever possible, electronic parts are selected from “Manufacturer High Reliability” parts or “industrial” parts qualified and screened in accordance with applicable military and IEEE (Institute of Electrical and Electronics Engineers) standards.

5.1.3 System Technical Requirements

While the Science Requirements present the primary intent of the OOI, the System Technical Requirements contain some of the more detailed specifications and constraints on achieving that overall goal. Because of the wide breadth of systems, software, hardware, operations, and services required for the OOI, the OOI System Technical Requirements are defined by and within each IO’s System Requirements, maintained within the OOI DOORS.

The individual IO System Requirement documents establish required transformation rules, priorities, inputs, outputs, states, modes, and configurations, as appropriate to each system product. They also define operational requirements to include operational profiles, and for each operational profile the utilization environment, events to which system end products must respond, frequency of use, physical and functional interfaces, and system functional requirements as well as performance requirements, including identification of critical performance parameters. These documents, in their entirety, not only define the OOI System Technical Requirements, but are used to weigh against all Common requirements of OOI, acquirer and other stakeholders requirements, as well as used to resolve conflicting requirements.

The OOI System Technical Requirements approach emphasizes minimizing the overall cost, while maximizing reuse and collaboration. The overall cost is analyzed in terms of the complete life cycle of OOI, including all operational costs. Design, installation, implementation, operating, and maintenance costs are to be considered for the purpose of minimizing life-cycle cost. This is done through:

- Maximize collaboration and cooperation between all IOs via the Systems Engineering function.
- Maximize use of common components between OOI systems.

The open design requirements inherent in all OOI Systems Technical Requirements strongly emphasize the open nature of the OOI. Not only will science data from the OOI be openly available, but the work performed in building the OOI will be made available for public reuse. This approach will maximize the impact of the OOI development, by making its concepts more visible and reusable, and also by making other environmental science projects economically feasible, since they will not have to redevelop the components. Furthermore, the direct benefit to projects adopting this technology will be matched by the interoperability across all the compatible projects.

OOI Systems Technical Requirements also account for cost-effective system reliability and maintainability, as they are critical to ensuring a long operational lifetime for the system. Individual observatories carry these concepts further with additional diagnostic and reporting requirements. Examples include:

- OOI shall be single fault tolerant.
- To the extent practical, provide sufficient fault isolation to ensure that failures can be isolated to individual instruments nodes/elements/branches of the network.

Finally, within the OOI Systems Technical Requirements, there are support services requirements that focus on the interactions of potential OOI participants, particularly those building instruments. Required services include interface simulators, testbeds, and instrument calibration. This also emphasizes the integration of the OOI components to:

- Maximize integration of support services between IOs as perceived by the end-user, and
- Provide standard, simulated test interfaces and testbeds for instruments users/designers.

5.1.3.1 L3 CG System Requirements

The Level 3 (L3) Requirements, also known as the System Requirements for the Coastal and Global Scale Nodes (CGSN) component of the OOI project are captured and maintained in the "*L3 CGSN System Requirements*" module within the OOI DOORS. These requirements are derived from the *OOI Level 2 (L2) Requirements* and the original *CGSN L3 System. Requirements*, and describes the CGSN system architecture and details the data measurement requirements at each of the Coastal and Global Nodes. These requirements shall be used to derive the subsystem requirements for the fixed and mobile assets from which the arrays are comprised, and is in the control of the CGSN IO to develop, refine, and maintain requirement and document integrity.

The CGSN IO shall maintain the Level 3 (L3) CGSN System Requirements, which outlines specific requirements necessary to design, build, and operate an integrated network of offshore infrastructure to facilitate ocean science over the next three decades. The requirements of this network shall be part of a larger network that includes the Regional Scale Nodes (RSN), and shall be fully integrated by a shared Cyberinfrastructure (CI) that is designed and implemented by the CI IO. CGSN Level 3 Requirements include system requirements for, but not limited to, Global Array, Pioneer Array, Endurance Array, the Operations Management Center, and Shore-Side Test Mooring.

All L3 CGSN System Requirements are and will be captured, monitored, and managed through the OOI Information Database- DOORS. OOI DOORS has these requirements and their relationships between, and orchestration of, activities across all OOI lifecycle aspects, including program management, system acquisition, development, transition/deployment, sustainment, and operational use in the context of system of systems.

5.1.3.2 L3 CI System Requirements

The CI IO shall maintain the CI Level 3 (L3) System Requirements that details the information technology capabilities, structure and development plans required to integrate the three OOI components (i.e., the Coastal, Regional and Global Scale Nodes) of the OOI into a coherent system-of-systems providing marine infrastructure, and user environment management services.

The set of System Requirements for the Cyberinfrastructure system are captured and maintained in the "*L3 Cyberinfrastructure System Requirements*" module within the OOI DOORS. The set of CI System Requirements specifies the requirements for the CI System and the methods to be used to ensure that each requirement has been met. Requirements pertaining to the interfaces with the RSN and CG Systems are captured and maintained in the *L3 CI & RSN Interface Requirements Specification* and *L3 CG & CI Interface Requirements Specification* OOI DOORS modules referenced by the L3 CI System Requirements module. The CI System Requirements, supplemented by the Interface Requirements Specifications, is used as the basis for design and qualification testing of the Cyberinfrastructure System. The set of CI System Requirements are derived from, and can be traced to, governing requirements at the OOI System-of-Systems level (Level 2).

The L3 CI System Requirements are the parent requirements used to derive the Level 4 requirements for each of the CI Subsystems that are also captured and maintained in DOORS modules. Traceability is maintained from the L4 requirements to the parent L3 requirements and to the grandparent L2 requirements using inherent DOORS capabilities that allows both bottoms-up and top-down analyses of proposed changes and potential risks.

The CI IO shall maintain the hierarchy of CI requirements from the *OOI L2 Cyber-User Requirements* at the top to the L4 subsystem requirements in accordance with established Configuration Management and Systems Engineering procedures.

5.1.3.3 L3 RSN Requirements

The Level 3 (L3) Requirements, also known as the System Requirements for the Regional Scale Node (RSN) component of the OOI project are captured and maintained in the "*L3 RSN System Requirements*" module within the OOI DOORS. These requirements are derived from the OOI Level 2 (L2) Requirements and original RSN System Requirements, which describe the RSN system architecture and details the data measurement requirements at the Regional Scale Nodes. These requirements are used to derive the subsystem requirements for the fixed and mobile assets from which the arrays are comprised, and are in the control of the RSN IO to develop, refine, and maintain requirements and document integrity.

The L3 RSN System Requirements include specific system requirements for, but not limited to: communication systems, power systems, time distributions system, OOI control systems, land based facilities, primary infrastructure, secondary infrastructure (e.g., vertical moorings, network interfaces, etc), core instruments, backhaul, and shore stations. They describe general system requirements such as expandability, maintainability, security, operations, reliability and environmental consideration.

All L3 RSN System Requirements are and will be captured, monitored, and managed through the OOI DOORS system.

5.1.3.4 Interface Control

As project scale increases, the work becomes too large for any single individual or group to accomplish in a timely manner, and the overall system must therefore be decomposed into parts. Splitting the project into a set of subordinate elements creates the very favorable possibility of adding resources and conducting parallel development, but at the price of introducing the need to control and manage the resulting interfaces.

The challenge of effective interface control is significant, and interface control represents a key project risk area that must be carefully managed. The fewer, and simpler, the interfaces that are introduced, the lower the overall risks are to the project.

5.1.3.5 L3 CG-CI Interface Requirements Specification

The interface agreement between the CGSN IO and the CI IO is outlined specifically in the *L3 CG & CI Interface Requirements Specification* OOI DOORS module. In consideration for the development of the CG-CI Interface Requirements Specification within the OOI DOORS, the CGSN IO and CI IO have defined and outline the responsibilities of each implementing organization to their interface.

All Level 3 (L3) CG-CI Interface Requirements Specification requirements are and will be captured, monitored, and managed through the OOI DOORS system.

5.1.3.6 L3 CI-RSN Interface Requirements Specification

The interface requirements specification established between the CI IO and the RSN IO is outlined specifically in the *L3 CI & RSN Interface Requirements Specification* OOI DOORS module. The CGSN IO will also be involved in the creation of this specification. The IRS also outlines the agreement between the CI IO and RSN IO, specifying the responsibilities of each organization.

All Level 3 (L3) CI-RSN Interface Requirements Specification requirements are and will be captured, monitored, and managed through the OOI DOORS system.

5.1.3.7 L3 RSN-CG Interface Requirements Specification

The interface agreement between the RSN IO and the CG IO is outlined specifically in the *L3 RSN & CG Interface Requirements Specification* OOI DOORS module. In consideration for the development of the CI-RSN Interface Requirements Specification (IA) within the OOI DOORS, the RSN IO and CGSN IO will define and outline the responsibilities of each implementing organization to their interface.

All Level 3 (L3) RSN-CG Interface Requirements Specification requirements are and will be captured, monitored, and managed through the OOI DOORS system.

5.1.3.8 L3 CI-EPE Interface Requirements Specification

As OOI develops and deploys transformative tools necessary to pursue national research priorities, it must also enable the “effective translation of results into readily understandable information usable by decision-makers, resource managers, educators, and potential workforce participants” (NSTC-JSOST, 2007). The draft interface agreement between the CI IO and the Education and Public Engagement (EPE) IO is outlined in the *L3 CI & EPE Interface Requirements Specification* OOI DOORS module. In consideration for the development of the CI-EPE Interface Requirements Specification (IA) within the OOI DOORS, the CI IO and EPE IO will define and outline the responsibilities of each implementing organization to their interface. Typically, the EPE IO provides derived requirements according to the needs of the EPE applications, and once finalized, the CI IO shall incorporate the requirements in the design of the interface, and provide the means for accessing them through the CI, subject to OOI policies.

These responsibilities are also reflected within the EPE *Request for Proposal*.

5.2 Solution Definition Process

5.2.1 Logical Solution Representations

5.2.1.1 OOI Logical Solution Process

The typical process for arriving at a set of logical solutions is to perform a functional analysis that begins with analysis of the high level system requirements and their placement into functional groups and then establishment of a set of logical solution representations, to which the requirements can be allocated. The Logical Solution process is iterated with the Physical Solution process to converge on an optimal design solution. The optimal logical solution is selected by performing trade studies; identifying and defining interfaces, states and modes, timelines, and data and control flows; analyzing behaviors; and analyzing failure modes, and defining failure effects. Functional and performance requirements and constraints are assigned to the elements of the logical solution representations, e.g., subfunctions, groups of subfunctions, objects and data sources.

The OOI Team follows the typical process for arriving at a set of logical solutions with one notable exception. The OOI System Breakdown Structure is based on more than 10 years of workshops and other groundwork in the ocean observing domain. The conceptual design for the OOI infrastructure is well documented in the *OOI Conceptual Network Design* and is the design baseline for the *OOI Preliminary Network Design* (PND), with refinement in the *OOI Final Network Design* (FND). The OOI System-of-Systems is composed of the Regional Scale Nodes, Global Scale Nodes, Coastal Scale Nodes, and Cyberinfrastructure Systems. The subsystems for all of these systems are also well understood, so the OOI Functional Analysis process begins with this base as a starting point. The IOs start at the System level and use the standard functional analysis process to identify configuration items that are generally characterized by specific functional role and well-defined interfaces, and are identified to facilitate management of the development process.

A flow-down process is used to break up and assign the system requirements to specific Configuration Items and component items. Included within the system-level engineering requirements documents are complete allocations of power, reliability, timing, and other requirements. The net result is that the original set of requirements contained in the system requirements documents are spread across a network of interacting lower-level elements and interfaces such that if each of the pieces meets assigned requirements, then there is confidence that the system as whole does so as well.

This coordinated "divide and conquer" approach is essential to enable parallel development effort and minimize downstream integration risks. Because of the incremental nature of development, it is inevitable that additional requirements are introduced as a by-product of ongoing decision-making. These "derived" requirements further constrain the remaining design space and may impact other internal and interface documentation.

5.2.1.1.1 System Architecture

The overall OOI project architecture has been divided into a nested hierarchy of system of systems, systems, subsystems, and components. Each layer is built from a set of individual lower level items plus the interface rules of how those items interact.

The net result is a list of all items and interfaces that must be developed, along with their logical relationships and dependencies to one another. This collection of n-dimensional puzzle pieces, together with the interface rules of how they fit together, represent the full set of system attributes that are to be developed.

At any time, the formal System Architecture is defined by the released and controlled set of baseline documents, engineering drawings and artifacts. These items show the subordinate content at any given level, reference the next higher assembly, and provide an easily followed architecture view.

5.2.1.1.2 Identifying Interface Relationships

To allow parallel configuration item development (or even serial development without extensive rework) it is essential that the interfaces be comprehensively identified and carefully managed.

Comprehensive interface identification is accomplished by use of a tool known as an N2 (n-squared) diagram, shown below in Figure 14. This elegantly simple tool places a finite number of system components along a diagonal and then supports discovery and documentation of every possible internal interface relationship in the remaining cells of the matrix.

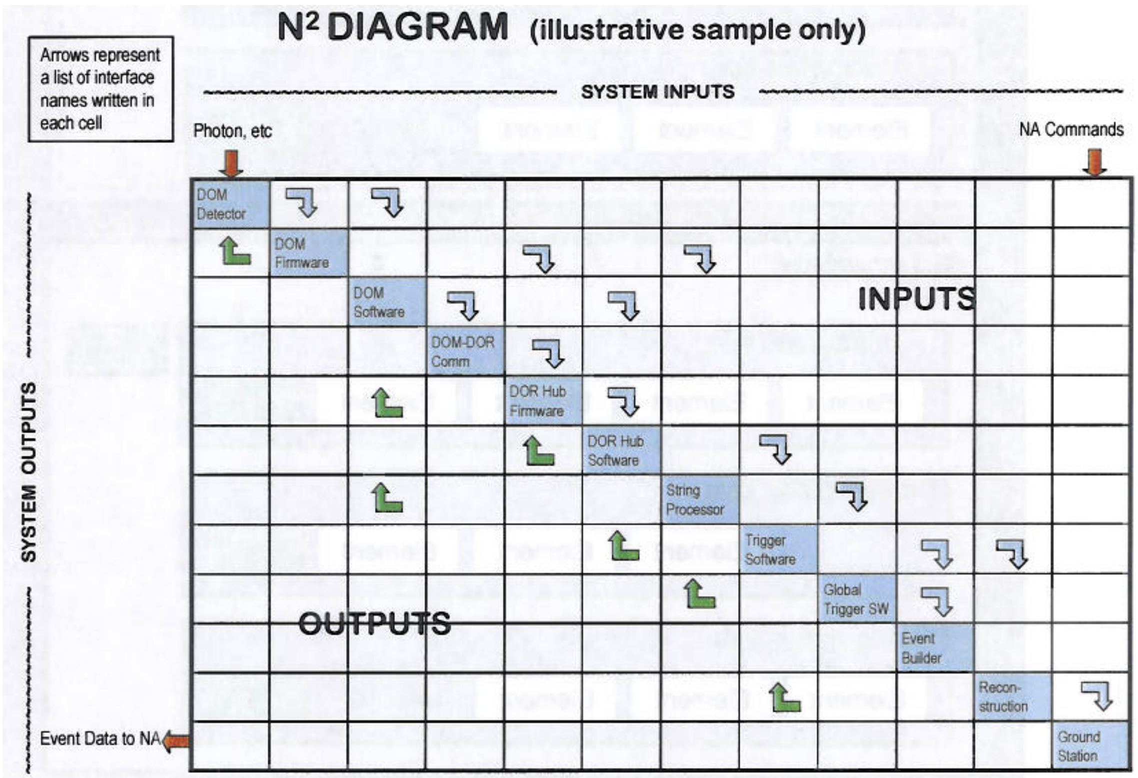

Figure 14, N2 Diagram Sample

Interface Control Document: The Interface Control Document (ICD) establishes the context of how lower level system elements interact to form the composite element the ICD covers. ICDs explain, in detail, all aspects of each interface including, but not limited to, physical, logical, data, data formats, rate, environment, ranges and responses. If the subordinate elements are the bricks, then the ICD is the mortar that holds them together in the manner needed to build the overall item. ICDs are structured around the N2 diagram described above. Use of the N2 approach ensures comprehensive consideration of all interface behaviors.

N2 diagrams are required as part of the *ifdr* (critical design) review prior to release of manufacturing drawings. ICDs are prepared, reviewed, released, controlled, and maintained in accordance with the *OOI Configuration Management Plan*.

5.2.1.2 Marine Implementing Organizations (CGSN/RSN) Logical Solution Process

Both the CGSN and RSN IOs follow the typical OOI Logical solution process, including standard functional analysis processes, to identify functional roles and well-defined interfaces. This also facilitates management of the development process. The CGSN and the RSN IOs have incorporated into their approach to the Logical Solution process, whether solved by COTS products or by OOI-specific development efforts, three major phases: specification, research, and result documentation; with appropriate documentation appearing at each phase. Much of this process is standard research and development protocol. By incorporating these steps into the marine IOs Logical Solutions Process, it helps mitigate approaching a problem with a box of familiar but inappropriate tools and partial completion of a somewhat different problem by imitating known solutions to similar problems.

The goal is that through the Logical Solutions Process, CGSN and RSN IOs accomplish their tasks in totality, though one or more avenues of approach, including new data-exploration tools and mathematical techniques, may be available to do so. Through a comprehensive examination of the various avenues of approach, one will typically result in the creation of valuable solution, reducing significant barriers, and seamless integration to other OOI tasks and initiatives.

1. **Specification**
    1. **Logical Solution description:** CGSN and RSN IOs will define one or more validated sets of logical solution representations that conform with the technical requirements of the system.
    2. **Context description:** Both IOs will then assign system technical requirements (especially performance requirements and constraints from the system technical requirements) to elements of the logical solution representations, such as sub-functions, groups of sub-functions, objects, and data structures.
2. **Research**
    1. **Tradeoff Analysis:** Continuing to follow the Logical Solution process, CGSN and RSN IOs will also establish sets of logical solution representations by doing tradeoff analyses, identifying and defining interfaces, states and modes, timelines, and data and control flows, analyzing behaviors, and analyze failure modes and defining failure effects.
    2. **Technical Requirement Analysis:** IOs shall then identify and define derived technical requirement statements resulting from tasks in Specification and Research Phase. This will help ensure that the derived technical requirements are stated acceptably in accordance with general OOI requirements.
3. **Result Documentation**
    1. **Recording:** CGSN and RSN IOs will record the resulting sets of logical solution representations, the set of derived technical requirement statements, and any unassigned system technical requirements, along with source rationale and assumptions in the established information database and OOI change management tools
    2. **Refinement:** In the refinement phase of Result Documentation, IOs shall optimize the Logical Solutions for their target platforms, yielding an embodiment of the technology, operations, requirements, and solutions that meets all OOI specifications and constraints.

Once these steps are followed, CGSN and RSN will then have numerous sets of logical solution representations that conform with the technical requirements of OOI, selecting appropriate representations to proceed to their respective Physical Solution Process.

5.2.1.3 Cyberinfrastructure Logical Solution Process

The ORION CI Conceptual Architecture forms the original baseline for the CI architecture development activity. The pertinent elements from the CI Conceptual Architecture were transferred into the CI architecture document and version management system and toolset. This includes, in particular, the Conceptual Architecture’s DoDAF All Views (AVs) and Operational Views (OVs), but also the pertinent information contained in the Conceptual Architecture requirements document.

5.2.1.3.1 *CI Architectural Approach*

The CI architecture makes a clear distinction between the activities that users engage in (collection, assimilation, surveillance and adaptive response) and the resources (data, instruments, networks, analysis processes, computational models and behavior systems) they employ to complete the activities. The interactive nature of the activities and the constraints imposed on the resources represent a substantial extension to data analysis systems as typified by existing data Grid architectures. While data management and analysis are essential elements of the CI, they are not sufficient to support interactive observation and response activities in cyber-physical coupled systems. The architecture extends the capabilities of data and computational Grid architectures by incorporating the ability to employ, couple, and control shared resources operating across the OOI enterprise in real-time over extended periods.

Throughout the OOI network, strategically placed computation and storage infrastructure is provided at Cyberinfrastructure Points of Presence (CyberPoPs). These include integrated real-time data processing and archive sites located at a few central facilities and at marine shore stations or control centers. In situ computation and storage resources are located within science instrument interface modules (SIIMs) and selectively within the marine networks. Large computational models are run on the national Grid infrastructure (e.g., the Teragrid and the Open Science Grid). Finally, OOI participants are able to securely incorporate computation and storage capabilities within their instruments, instrument platforms (e.g., AUVs and gliders) and research facilities.

The resource elements extending beyond storage, data and computation needed to realize the high level CI capabilities can be generalized as:

- Dynamic data sources (e.g., data, product and event streams).
- Taskable elements (e.g., instruments, AUVs, and ocean modeling systems).
- Executable processes (e.g., behaviors, workflows, scripts, and compiled code).

The organization and structuring of resources taken in the planned architecture recognizes the process-driven nature necessary for OOI, ranging from simple data collection protocols to a complete investigation model. **Error! Reference source not found.** illustrates the relationships between OOI activities (upper left) and the five core resource networks it employs: the Control, Data, Processing, Instrument, and Modeling Networks (upper right). The Knowledge Network is not currently funded, although provision is made to extend the CI to incorporate it.

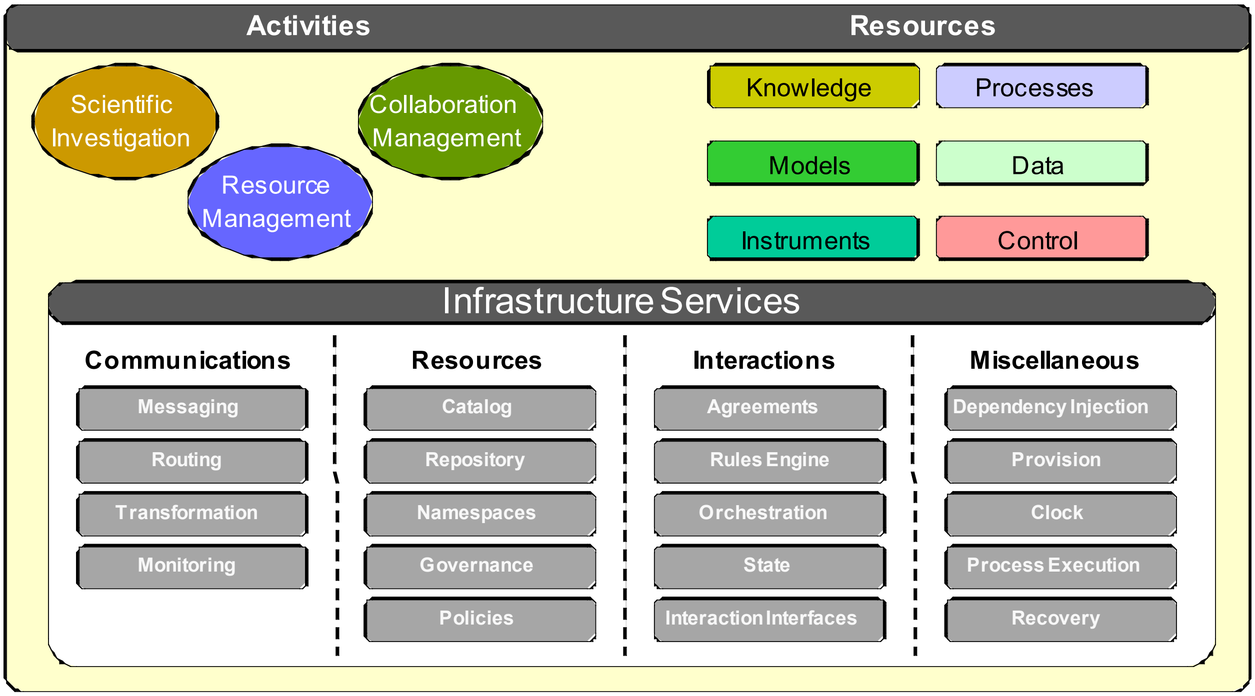

Figure 15, Core CI Architecture

The purposes of the five resource networks are:

- The Control Network establishes standard models for the management of stateful and taskable resources. It provides the semantics to monitor and control the operating state of an active resource as well as to initiate, monitor, and amend the tasks of a taskable resource.
- The Data Network provides an automated data distribution and preservation network with pervasive and universal access subject to OOI Data Policy. It provisions a federated system of data streams, repositories, and catalogs that supports the distributed organization of resources.
- The Process Network provides scheduling of processes at specified locations within the integrated network based on explicit time requirements and/or event triggers.
- The Instrument Network provides interactive and coordinated relations with real and/or synthetic environments through the use of transducers (sensors or actuators). It ensures the safe and secure operation of individual sensing platforms, and provides reliable delivery of acquired data with their associated metadata. These capabilities must be integrated with network-wide resource allocation and observation planning.
- The Modeling Network establishes baseline processes and tools comprising a coherent framework for the analysis and assimilation of data. The capability to network and interact with multiple community-based numerical ocean models for parameter estimation/optimization and data assimilation is integrated into the framework.

5.2.1.3.2 CI Service Oriented Architecture (SOA)

The CI architectural concept rests on a rigorous Service-Oriented Architecture (SOA) design approach to project subsystem capabilities and integration into system capabilities. The CI leverages service-oriented implementation techniques to yield a seamless software and system engineering project framework. Intuitively, every OOI entity (examples range from instruments to laboratories to data repositories to coastal, regional, and global observatories to the computational Grid) represents itself as a set of services that can be located and accessed via the CI. Web services and related technologies enable rapid implementation, provisioning, and integration, along with flexible configuration of these services to yield the CI.

The development effort is structured into six subsystems based on the major activities of scientific investigation and the two infrastructure elements. The subsystems are:

a. Sensing & Acquisition,
b. Analysis & Synthesis,
c. Planning & Prosecution,
d. Data Management,
e. Common Operating Infrastructure,
f. Common Execution Environment.

Each subsystem project has a duration of either two or three 16-month development cycles. They are staggered across the five release cycles of the overall proposed project. Their ordering is based on a prioritization of their value to the OOI community and their interdependency. The projects deliver complete subsystems and have a prescribed set of deliverables. These deliverables, starting with the domain models and ending with deployed code, are essential for the long-term viability of the system. Close attention has been paid to the shared architectural elements that can be assembled by one team, enhanced by another and used by most. This strategy of “implement, enhance, use” across teams is employed to ensure sustainability of the interaction interfaces across the duration of the OOI, and drive the quality of the implementations behind them.

In addition to the teams identified for each subsystem, architectural leadership, domain modeling, software design, and user interface resources have been allocated to work alongside each project. This ensures coherence of the design and products generated across the projects while giving the proposed work the ability to engage the expertise of the ocean sciences and CI communities in a very targeted and cost effective manner to the OOI vision.

The CI subsystem IPTs develop, at a minimum, the following artifacts to prepare for integration into the overall systems:

- Requirements & use cases
- DoDAF-style domain models and other pertinent architecture products
- A service framework, consisting of
    - Presentation Interfaces
    - Service patterns
    - Governance logic
- Capability block framework, consisting of
    - Presentation binding
    - Service binding
    - Logic and state
    - Resource binding
- Resource technology descriptions, consisting of
    - System technology
    - Community-supported technologies
    - Externally-provided technologies

Particular emphasis is placed on the precise specification of Interaction Interfaces (i.e., service interface specifications *including* interaction protocol). This facilitates the creation of test-plans and informed acceptance decisions to prepare and perform system integration.

5.2.1.3.3 CI DoDAF Development Methodology

CI Software Architecture development follows the process suggested for the Department of Defense Architectural Framework (DoDAF) 1.5, as documented in [DoDAF 1.5 Volume 1], tailored for the needs of the CI project. In particular, this entails development of a sequence of architectural products, structured into:

- All Views Products (AVs): Executive Summary & Glossary
- Operational Views (OVs): Logical Architecture
- System Views (SVs): Deployment Architecture & Implementation Considerations
- Technical Views (TVs): Technical Standards, Constraints and Evolution.

DoDAF Operational Views (OVs) constitute the CI Logical Solution derived from user and system requirements, as well as from the corresponding concepts of operations. The L2 CI System Requirements serves as the top level description of desired CI capabilities, and is a key guide for the architecture development process. The products to be developed for the Operational Views are:

1. High Level Operational Concept Graphic (OV-1)
2. Operational Node Connectivity Description (OV-2)
3. Operational Information Exchange Matrix (OV-3)
4. Organizational Relationships Chart (OV-4)
5. Operational Activity Model (OV-5)
6. Operational Rule Model (OV-6a)
7. Operational State Transition Description (OV-6b)
8. Logical Data Model (OV-7)

The core of the Operational Views consists of OV-5, OV-6 and OV-7. These products are collectively referred to as the “domain model”. The domain model is the basis for all operational view products (except OV-1) and all system views products.

The architecture team enriches this list of products to address service-oriented views, including end-to-end policy and governance specifications to the degree they are needed and not explicitly called out in the DoDAF standard.

5.2.2 Physical Solution Representations

5.2.2.1 OOI Physical Solution Process

The typical process for arriving at a preferred set of physical solution representations is analysis of the logical solution representations, derived technical requirements, and any unassigned system technical requirements to determine which ones provide requirements for enabling products. The Physical Solution process is iterated with the Logical Solution process to converge on an optimal design solution. Logical Solution representations, unassigned system technical requirements, and derived technical requirements are assigned to entities in the physical solution representations that make up a physical solution. Alternative physical solutions are generated by the identification and definition of physical interfaces, identification and analysis of critical parameters, identification and assessment of physical solution options, and performance of systems analysis. The optimal physical solution representation for further characterization into a design solution is selected from the evaluation of results from each physical solution representation.

Again, the OOI Team follows the typical process for arriving at a set of physical solutions with one notable exception, the OOI System Breakdown Structure is based on more than 10 years of workshops and other groundwork in the ocean observing domain. This foundation provides an advanced point of departure for defining the design solution.

5.2.2.2 Marine IO Physical Solution Process

Once specific logical solutions representations are agreed upon, both the CGSN and RSN IOs will have a set of physical solution processes that will analyze logical solution representations and derived technical requirements to determine which ones provide requirements for enabling products, can be done best manually or by facilities, materials, data, services, or techniques, and can be done best by hardware, software, or firmware products (new or existing).

The marine IO Physical Solution Process encompasses CGSN and RSN engineering design considerations, which aggressively defines common system components across the GSN, CSN, and RSN that will reduce development and construction costs and simplify maintenance. The marine IO Physical Solution Process path is as follows:

- Preparation
  - Analyze logical solution representations, derived technical requirements, and any unassigned system technical requirements
- Define Requirements
  - Assign representations from requirements, unassigned system technical requirements, and derived technical requirements to physical entities that will make up a physical solution
- RFP/RFQ Development
- Vendor Evaluation
  - Identify and define physical interfaces
  - Identify and analyze critical parameters
  - Identify and assess physical solution options
  - Perform of systems analysis
- Negotiations to Develop a Final Executable Contractual Agreement
  - Identify and define derived technical requirement statements resulting from the previous steps
- Approval to Award
  - Select the preferred physical solution representation for further characterization into a design solution from the evaluation of each physical solution representation results
- Award

For the RSN IO, the acquisition of material and services for the RSN project including, but not limited to, the Primary Infrastructure, Shore Station and Backhaul will be in accordance with the UW Purchasing Policy and Procedure Manual, Washington State Law, and OL subaward.

The RSN IO will also have its Physical Solution Process encompasses RSN design considerations, which in turn incorporates the findings of two trade-off studies completed by the RSN IO to investigate optimal configuration of the cabled backbone infrastructure and shore station location(s). These studies include the *Regional Scale Nodes Wet Plant Primary Infrastructure White Paper* and the *Regional Scale Nodes Shore Station Options White Paper*. Further definition of the RSN design is developed in the *RSN Secondary Infrastructure White Paper.*

5.2.2.3 Cyberinfrastructure Physical Solution Process

CI Physical Solution Representations are developed using the DoDAF Systems Views (SVs). These are derived from Acquirer Requirements and System Technical Requirements, as well as from the Logical Solution Representations developed using the DoDAF Operational Views (OVs). The products to be developed for the deployment and implementation views are:

1. Systems Interface Description (SV-1)
2. Systems Communication Description (SV-2)

3. Systems-Systems Matrix (SV-3)
4. Systems Functionalities Description (SV-4)
5. Operational Activities to System Functionalities Traceability Matrix (SV-5)
6. Systems Data Exchange Matrix (SV-6)
7. Systems Performance Parameters Matrix (SV-7)
8. Systems Evolution Description (SV-8)
9. Systems Technology Forecasts (SV-9)
10. Systems Rules Model (SV-10a)
11. Systems State Transitions Description (SV-10b)
12. Systems Event-Trace Description (SV-10c)
13. Physical Schema (SV-11)

5.2.3 Specified Requirements

From the System Technical Requirements, the OOI specified requirements are referred to as subsystem requirements that are in turn derived for each of the OOI Systems. These subsystem requirements are captured in the Level 4 modules/documents. The Level 4 requirements modules/documents correspond to platforms, assemblies, and components that are independently developed and maintained under configuration control, and are integrated together to form configuration items. The Level 4 requirement modules/documents are developed and maintained by each IO and managed by the OOI Program Office.

The Level 4 requirements look to fully characterize the design solution, while ensuring that the design solution is consistent with its source requirements, including but not limited to selected physical solution representation requirements, associated system technical requirements, and derived technical requirements. Level 4 requirements also are more specific, including information on functional and performance requirements, physical characteristics, and test requirements for the system, system end products, and subsystems of each end product, as applicable to the engineering life cycle phase.

Level 4 requirement modules/documents are incorporated and universally captured, stored, monitored and managed using DOORS. This DOORS-maintained information is also referenced in various documents (generated from DOORS).

5.2.3.1 L4 CI Requirements

The Level 4 (L4) CI requirements are recorded in DOORS and are used to define the design solution work products. All tradeoff analyses results, design rationale, assumptions, and key decisions to provide traceability of requirements up and down the system structure are recorded in whitepapers and trade study reports.

.

The L4 CI Requirements also establish tasks that require development, and/or tasks that require procurement of off-the-shelf or reused solutions that satisfy identified requirements for associated processes (production, test, deployment/installation, training, support or maintenance, and retirement or disposal) related to the system’s end products.

5.2.3.2 L4 Coastal / Global (CGSN) Requirements

The Level 4 (L4) CGSN requirements are recorded in DOORS and are used to define the design solution work products. All tradeoff analyses results, design rationale, assumptions, and key decisions to provide traceability of requirements up and down the system structure are recorded in whitepapers and trade study reports.

The L4 CGSN Requirements also establish tasks that require development, or tasks that require procurement of off-the-shelf or reused solutions, which satisfy identified requirements for associated processes (production, test, deployment/installation, training, support or maintenance, and retirement or disposal) related to the system's end products.

5.2.3.3 L4 RSN Requirements

The Level 4 (L4) RSN Requirements reflect the OOI emphases: connectivity (of power and communications) and persistence at the typical installation depths for most instruments. The requirements call for a system capable of expansion, anticipating regular upgrades to instrumentation and occasional upgrades to core systems. The Level 4 (L4) RSN requirements are recorded in DOORS and are used to define the design solution work products. All tradeoff analyses results, design rationale, assumptions, and key decisions to provide traceability of requirements up and down the system structure are recorded in whitepapers and trade study reports.

5.3 Implementation Process

5.3.1 Implementation

OOI employs an Implementation Process that assures accordance with the specified requirements to obtain a verified end product, and successful implementation. In order to do this, each IO has developed and maintains separate documents and processes, in particular the *IO Project Execution Plan (PEP)* and supporting documents. They also validate the subsystem products received or reused against their acquirer requirements (input requirements to the subsystem development) using the OOI verification processes.

Each OOI implementation may involve an assembly of the validated subsystem products, or physical integration of such products, into the respective test article or end product to be verified. Once assembled and/or integrated, each IO will also verify each test article or end product against its specified requirements, acquirer requirements, input/output requirements and ensure that the enabling products for each associated process will be ready and available to perform their intended support functions required by the overall OOI requirements and goals.

Use of OOI SDE Configuration Management tools and OOI SDE Collaboration tools, such as OOI DOORS, ITM/JIRA, GIT and Subversion will be used to monitor and manage each step in the Implementation Process and ensure that all steps and requirements are met.

5.3.1.1 Regional Scale Nodes Build Process

RSN has developed and maintained separate documents and processes, such as the *RSN Project Execution Plan (PEP) to* outline the specifics the RSN Build Process. The RSN Build Process follows the general tenants of the System Design process, the Project Lifecycle, as well as the Logical and Physical Solution processes. They are divided into primary and secondary infrastructure considerations

Primary Infrastructure

Components Built, Tested, Installed, by ISO-9000 Contractor to telecom industry standards, with oversight by members of the RSN Quality, SE, Engineering and Project Management team. The project schedule will be included in the contract with critical milestones tracked and tied to contract payments over the life of the project.

Secondary Infrastructure

All components, other than the vertical mooring, which will be built by a suitable contractor based on production documentation, will be produced by the University of Washington Applied Physics Laboratory (APL)/RSN with oversight by members of the RSN Quality, SE, Engineering and Project Management team. Extensive monitoring of the production line, sub-system testing and final acceptance testing is used to maintain quality needed to maintain overall system reliability.

The Vertical Mooring infrastructure components will also be built at APL with oversight by members of the RSN Quality, SE and Project Management team. Appropriate environmental and stress testing will be performed to ensure suitability of final product produced for the RSN system.

5.3.1.2 Coastal and Global Scale Nodes Build Process

CGSN has developed and maintains separate documents and processes, such as the CGSN Project Execution Plan (PEP) and FND to outline the specifics of the CGSN build process. The PEP defines the management processes and responsibilities for implementation while the FND, derived from the Preliminary Network Design (PND), describes the specifics of the CGSN design. A Technical Data Package (TDP) details the design and along with the FND is reviewed at the Final Design Review.

5.3.1.2.1 CGSN Development Tools

All design documentation is controlled internally using commercial Document Management software that utilizes a single threaded check-out/check-in version control system that also includes workflow controls. Software development is controlled separately using Subversion, where software developers can get local copies of the software source code using the version control system, and can build software components as required.

CGSN utilizes both commercial and custom platform development tools. For static mooring analysis of subsurface moorings and for initial design of surface moorings CGSN uses WHOI-developed software called NOYFB. For dynamic analysis of surface mooring designs as well as any general cable analysis CGSN uses WHOI-developed nonlinear 3d cable dynamics software called WHOI Cable. Mechanical solid modeling is primarily Autodesk Inventor with FEA performed using COSMOS/M. Electrical schematic capture, simulation and layout are performed using several commercial software packages, such as OrCAD and LTSPICE. Additionally, controller specific development packages, such as Codewarrior-C, are used for embedded controller design.

System simulation and use case simulation tools include Matlab and the Microsoft Excel. System and subsystem hardware tests are designed around National Instruments hardware utilizing LabVIEW graphical programming software.

5.3.1.2.2 CGSN Standards and Technologies

CGSN follows ASME Y14.1 documentation standards. All documentation conforms to configuration management requirements per the OOI CMP. Calibration of manufacturing test equipment and other critical measurement devices are detailed in the CGSN QA/QC plan.

5.3.1.2.3 CGSN Verification Plan

The CGSN Verification Plan aligns requirements with objective evidence of compliance. Verification methods will be analysis, inspection, analysis and test. Verification will further be defined as type - Engineering Qualification or Production Test. Verification will occur at levels of assembly appropriate to confirm compliance as early as possible. The Verification Plan will define the method, level and type of testing for the complete system.

5.3.1.2.4 CGSN Subsystem Development

CGSN has defined cross-cutting subsystems to foster commonality between platforms and arrays to the greatest degree possible. Subsystem performance, interface, and other requirements are combined in a detailed specification which fully defines all verification requirements. Subsystems are then independently verifiable using an appropriate combination of verification techniques and levels, e.g. one-time qualification test vs. production unit test.

The TDP will be expanded during subsystem development and will form the basis for a series of Production Readiness Reviews (PRR). The PRR will evaluate drawings below the subsystem level for procurement/piece-part production readiness as well as subsystems and integration tests and requirements verification plans, and QA/QC requirements. Completion of the PRR will be the gate for purchase requisitions for material, unless prior, written pre-authorization is requested and received.

The organizational structure of the CGSN team has been established to provide clear understanding of roles within subsystem development as well as within the array development and build. This is important to maintain the subsystem and integrative requirements alignment for commonality.

5.3.1.2.5 CGSN Subsystem Testing

Unit testing will follow written procedures developed from the subsystem qualification test plans and requirements verification plans. The subsystem test plan will define both the level and method of testing for the subsystem. Test records will be maintained by the QA/QC engineer per the QA/QC Plan. The test records will be reviewed against requirements and when all requirements have been met the readiness assessment report for the subsystem will be completed.

5.3.1.2.6 CGSN Integration Test/Burn-in

Prior to installation and acceptance, CGSN plans to perform integration testing and burn-in for platforms for a defined period. The burn-in period is established to weed-out infant mortality of sensors and other equipment, thus improving overall availability of deployed systems. The complete system for the configuration line item must be available for the burn-in cycle, including any externally provided software, to provide the needed level of system confidence. Integration testing will be performed using simulated use case scenarios and will utilize the entire system with the exception of telemetry, where satellite communications will be minimized for cost reasons. The burn-in periods will be determined using institutional best practices. Test records will be maintained by the QA/QC engineer per the QA/QC Plan. The test records will be reviewed against requirements and when all requirements have been met the Installation Readiness Review (IRR) for the configuration item will be completed.

5.3.1.2.7 CGSN Installation Readiness Review

CGSN will conduct an IRR of the build and test documentation following Integration test/burn-in. The purpose of the review will be to ensure the objective documentation of the build and test process is complete and accurate. The IRR will evaluate the Installation Test Plan for each configuration item that will be deployed at the site. The IRR is the gate for initiation of ship and field engineering activities for installation.

5.3.1.2.8 CGSN Installation Test

CGSN will conduct an Installation Test of each deployed platform to ensure operation at the site. Installation Test will be the gate for Acceptance for configuration line items and will culminate in commissioning of the array once all assets have been deployed and accepted at each site, as defined in the Commissioning and Operation and Maintenance Plans.

5.3.1.2.9 CGSN Operations and Maintenance (O&M)

CGSN O&M maintains a sustaining engineering presence to deal with obsolescence, interface and overall improvement issues for the life of the project. Maintenance of the requirements, particularly as they relate the Verification Plan and resulting test procedures, is imperative to continue delivery of fully capable equipment.

5.3.1.3 Cyberinfrastructure Build Process

CI has develops and maintains separate documents and processes to outline the specific CI Build Process. The CI Build Process follows the general tenants of the System Design process, the Project Lifecycle, as well as the Logical and Physical Solution processes.

5.3.1.3.1 CI Methodology

Software Implementation is driven by service-oriented and component-oriented concepts, emphasizing modularization of software units, loose coupling and interface specification.

A given software unit is developed using a test-first strategy. Tests need to be specified, designed and developed first, according to the software architecture and design.

Rapid prototyping is applied together with frequent requirements/design iterations and software build cycles in order to identify and mitigate implementation risks and obtain stakeholder involvement early in the project.

5.3.1.3.2 CI Tools

All software development occurs under full version control. Software developers can get local copies of the software source code using the version control system, and can build software components as required. Appropriate hardware and middleware installations are required to deploy and execute the system or parts thereof. Software developers are able to run automatic unit and integration tests for software units and components on their development workstations.

A testing environment provides the capabilities for testing individual system components in isolation from the other parts of the system, in order to establish full testability. Test drivers, test harnesses and test containers simulating actual system infrastructure provide the test environment. Tests are version controlled in a similar manner to software, and need to be automatically executable.

An automatic build environment is used that creates builds of the software on demand and each night. Nightly builds are subject to automated testing. Build and test results are published for access by the software development team.

5.3.1.3.3 CI Standards and Technologies

Using the ILS process, supportability is a fundamental consideration in selection of state-of-the-art industry standards, infrastructure technologies and products for the basis for implementation of the OOI Cyberinfrastructure . Such technologies include, but are not limited to, Java SE and EE 6, Enterprise Service Bus (ESB) solutions, ActiveMQ and AMQP messaging middleware, Spring, PicoContainer, Ruby on Rails, and AJAX-enabled Web Frontends.

All source code developed for the OOI Cyberinfrastructure must follow industry standard source code format guidelines. In the case of the Java programming language, this is the Code Conventions for the Java Programming Language, available at http://java.sun.com/docs/codeconv/ .

5.3.1.3.4 CI Unit Testing

Unit testing is required for every software unit and component. Unit tests need to be provided by the software developers using a “test-first” approach, following the software architecture definition and design. Unit tests define the acceptance criteria for each software unit. The Software Development Manager is responsible for checking the existence and quality of the unit tests. Tests should be engineered towards low footprint and automatic execution in order to enable short turnaround times. Only software units with appropriate test coverage, passing all tests can be included in software releases.

5.3.1.3.5 CI Integration

During the construction phase of each development spiral, the newly created architectural elements are integrated into the existing CI release using the roadmap defined in the Integration, Test and Verification Plan. The responsibility for each subsystem lies with its subsystem IPT lead, and the Software Development Manager is responsible for integration of the subsystems into a coherent CI. The subsystem IPT leads are also responsible for any defects pertaining to their subsystems and their timely removal. Integration of subsystems can occur when all tests are passed.

The architecture and design of the subsystems must follow the DoDAF framework and be consistent with the CI overall architecture and design documentation. Particular emphasis must be placed on the design of suitable subsystem interfaces that establish a loose coupling but high coherence.

5.3.1.3.6 CI Verification and Validation

The verification process for the integrated CI is described in the *Integration, Test and Verification Plan*, and is carried out by the CI Chief System Engineer. Integration of the verified CI with the physical and logical infrastructure produced by the marine IOs is also described in that document, and is carried out by the CI Chief System Engineer and CI Operations Manager with oversight from the OOI Chief Systems Engineer/Test lead and OOI Operations Manager. Each CI release is evaluated for correctness, completeness, security, and quality using the criteria established in the Integration, Test and Verification, Security Management, and QA/QC Plans.

5.3.1.3.7 CI Deployment and Acceptance

The deployment process is described in the CI Deployment and Acceptance Plan, and is carried out by the CI Operations and System Integration teams with oversight by the OOI Chief Systems Engineer and Operations Manager. The acceptance process is described in the Transition to Operations Plan, and is carried out by the OOI Program Office.

5.3.1.3.8 CI Operations and Maintenance

The Operations and Maintenance team carries out operations and maintenance activities on the CI after deployment and acceptance. The IO Chief Systems Engineer and System Architecture team, along with the cognizant Subsystem IPTs, provide necessary support to facilitate the transition to operations during each development cycle transition phase, including the final six month transition phase.

5.3.2 Major Technology Risk Decision Points

The final design of the OOI incorporates various levels of technology maturity. The major technology risks identified in the risk register have been listed in the master schedule and tied to review decision points. These go / no-go decision points provide a clear timeline for determining whether to continue with technology that had been identified as a risk or to engage mitigation options for the technology solution selected. These decision points are identified in the Integrated Master Schedule.

5.4 Transition to Use Process

5.4.1 Transition to Use

OOI has and will continue to develop its Transition to Use Process through a framework designed to transition verified system, subsystems and tasks to the acquirer of the systems in accordance with processes such as the *OOI Project Execution Plan, OOI Operations and Maintenance Plan* and the *OOI Commissioning Plan.*

The *OOI Operations and Maintenance Plan*, incorporated by reference, also outlines the OOI Transition to Use Process through establishing a framework and shared vision in which Ocean Leadership and the various IOs established requirements for governance, daily operations, maintenance, administration, policies and procedures. This plan establishes two groups, the Facility Governance Group (FGG) and the Facility Operators Group (FOG). The responsibilities of Ocean Leadership, the FGG, the FOG, the Network Operations Center, and each of the IOs, are delineated; policies and procedures will be promulgated within this framework.

The *OOI Project Execution Plan (PEP) and OOI Commissioning Plan* outlines sites where end products systems will be located, installed, used, maintained, and serviced. It also discusses how transportation of the systems will be accomplished, how installation will occur, as well as how commissioning will occur, as required by the OOI Commissioning Plan, to bring delivered or installed end products to operational readiness with appropriate acceptance and certification tests completed.

5.4.1.1 Readiness Assessment (Production Readiness)

Readiness assessment (testing) is an internally validated ready for deployment and acceptance test. The OOI Program Office will attend and witness any readiness assessment testing, and at the appropriate level will request NSF involvement. The standard process is to perform Acceptance Testing – Paragraph 6.3.1.5, followed by a formal review such as the Operational Test Readiness Review (OTRR).

5.4.1.2 OL/NSF Acceptance

The "ownership" of a tested configuration item transfers to OL upon "acceptance".

- Acceptance (with Conditions if one or more non-critical items were not delivered, and the configuration items is operable at a less than full operating state)
- Acceptance (Full, validation of scope, verification of quality product delivered)

Acceptance of items operating in a near-steady state or non-logistics supported mode is planned as the incremental deployment of sub-systems and arrays are completed, and the systems are commissioned leading to a full system-of-systems commissioning. Accepted configuration items and sub-systems will be operating under O&M support, pending system commissioning and will remain under the design and engineering domains during the pre-commissioning period.

5.4.1.3 Commissioning

Validation and verification that the support systems are in place, operational and the configuration items are operating in a controlled "steady state" and providing data, are all part of the OOI Commissioning process. This includes ensuring that delivered or installed end systems are at operational readiness level, backed with completed appropriate acceptance and certification tests. The transfer of responsibility from Engineering to Operations will occur in accordance to the Commissioning discussed in *Section 7.3.1.5* of this document, and the *OOI Commissioning Plan*.

Systems eligible for commissioning must meet the qualifications below:

- Configuration item delivered and fully accepted.
- All support systems for operations and maintenance of Configuration Item in place.
- System capable/demonstrated operation in a steady state mode.
- O&M Management capable.

5.4.1.4 Deployment and Acceptance Management

The OOI Chief Systems Engineer is responsible for developing a Deployment and Acceptance Plan that defines the process for each IO deployment and the criteria for its acceptance by the OOI Program Office. The Plan describes the documentation that allows the system to make the transition to operations and specify the training required for operations personnel. The acceptance process complies with requirements imposed by, and is overseen by, the OOI Program Office, which has ultimate responsibility for accepting individual IO deliverables. The deployment and acceptance process follows on the integration, verification, and validation processes described in this plan. Deployment is carried out by the O&M and the System Integration teams, with oversight by the Operations Manager and OOI Chief Systems Engineer. The Operations Manager prepares a Deployment and Acceptance Report after each development / acceptance.

6 Technical Evaluation

6.1 Systems Analysis Process

6.1.1 Effectiveness Analysis

OOI shall perform effectiveness analyses to provide a quantitative basis for decision making that is embedded within each level of validation, verification, and testing activities. Both OOI and each IO will plan effectiveness analyses to include purpose, objectives, execution and data collection, schedule of tasks, resource needs and availability, and expected outcomes.

As further discussed in *Section 7.2* of this document, each validation level will not only test systems, subsystems and tasks against requirements, but also analyze alternatives for system and cost effectiveness, based on factors such as accuracy, availability, capacity, maintainability, reliability, responsiveness, operability, safety, security, spares requirements, survivability, transportability, cost, impact and vulnerability.

OOI Effectiveness Analysis is also discussed in other developed and maintained documents and processes, in particular the OOI and IO *Configuration Management Plan (CMP)*. Use of OOI SDE Configuration Management tools and OOI SDE Collaboration tools, such as OOI DOORS, ITM/JIRA, GIT and Subversion will be used to record effective analysis outcomes, including assumptions, details of the analysis, findings, lessons learned, models used, rationale for decisions made, and other pertinent information that affects the interpretation of the effectiveness analysis results.

6.1.1.1 Reliability Engineering

OOI's operating environment and inaccessibility of major system elements following deployment place a high priority on careful reliability engineering. The primary reliability engineering analysis for OOI is based on a Physics of Failure (PoF) assessment of the factors that introduce stress on system elements, supplemented by statistical analysis of failure rate predictions when meaningful data is available. Available failure history is examined for insight and experience from similar systems such as Monterey Accelerated Research System (MARS) and utilized where applicable.

6.1.1.2 Physics of Failure Method

PoF is an approach for the development of reliable products that uses knowledge of root cause failure processes to prevent product failures through robust design and manufacturing practices. The basic premise is that it is equally important to understand how equipment works and fails in the environment for which it is expected to operate.

Unlike statistical analysis, which requires a prior database of comparable experience, PoF methods can be applied effectively in environments such as OOI. By carefully understanding the sources, types, and levels of available energy that may cause harm, one can identify the system elements most at risk. Applying this insight into how the design interacts with environmental stressors enables a proactive risk response and results in significantly higher reliability.

6.1.1.3 Role of Statistical Analysis

Statistical analytical methods shall be used as a supplement and extension of PoF reliability analysis whenever appropriate source data is available or can be reasonably developed using probabilistic methods. Failure rate estimates are made for purposes of system availability estimation. Data collected during developmental and production testing are captured for analysis and predictive value.

6.1.1.4 Criticality Analysis of Failure Modes and Effects

Select system elements are examined in terms of possible failure modes and root cause -- an activity closely integrated with PoF reliability philosophy and methods. As each failure mode is identified, the anticipated effect is determined and associated with a criticality level. This information is central to reliability modeling activities and to creating designs that are fault tolerant or at least fail gracefully through gradual degradation rather than exhibiting outright loss of functionality.

6.1.1.5 System Reliability Modeling

System modeling tools are limited to their direct applicability on a program such as OOI due to the unique operating conditions, but are still useful to generate guidance. A system reliability model that extends to the component level for critical system elements is developed as part of the detail design.

6.1.1.6 Failure Review & Corrective Action

Although failures are always unwelcome, they offer a wealth of information that can be used to modify the design or environment to address the underlying cause. Thorough root cause analysis often identifies corollary risks with much higher potential impact than the one just encountered. This valuable information is lost if the circumstances cannot be recreated for analysis, such as when the user has tried to repair or hide the failure.

In the event of any failure, the failed item is carefully maintained in its "as failed" state until root cause analysis can be completed. The results of the analysis are used to determine the root cause of the condition, and a corrective action to eliminate the cause is developed and implemented. Periodic checks after the corrective action implementation take place to assess the effectiveness of the corrective action and to further evaluate other actions that could improve the effectiveness and efficiency of the process, component, or material.

6.1.1.7 Safety

The *OOI Environmental Health and Safety Plan* describes the processes to describe, assess, and mitigate safety-related issues. Safety is not a standalone task; it must be incorporated into the overall project design. Safety evaluations shall be conducted throughout all phases of the OOI Project, including design, development, manufacturing, deployment, use, maintenance, service, and decommissioning.

6.1.2 Tradeoff Analysis

OOI performs tradeoff analyses to provide both decision makers and those defining requirements with recommendations, predictions of the results of alternative decisions, and other appropriate information. This allows selection of the best course of action when the original path is no longer available. Each IO performs tradeoff analyses considering their respective project life cycles, as well as their logical and physical solution.,

Selection criteria may include:

- Cost
- Schedule performance and risk
- Life-cycle outcomes
- Producibility, Testability, Maintainability
- Size weight and power consumption
- Effectiveness
- Analysis outcomes

Weighting factors for each selection criterion are used to distinguish its degree of importance.

The WBS and resource loaded IMS of each IO will also aid in determining the availability of required resources, execution and data collection requirements, expected outcomes, defined conditions (triggers and rigor), level of importance, objective, schedule of tasks, and type of analysis (formal, informal or judgmental).

The OOI SDE Configuration Management tools and OOI SDE Collaboration tools are used to record outcomes of the tradeoff analysis, including assumptions, details of the analysis, lessons learned, models used, rationale for decisions made, recommendations and effects, and other pertinent information affecting the decisions made.

While much of the design process is an incremental conversion of requirements into straightforward solutions, there are frequently a number of alternatives to be considered. The use of simple, but logically sound, trade study methods to define and contrast options provides not only a timely decision aid but also traceability as to the resulting outcome. Further, the documented trade studies and analysis can be easily revised if underlying assumptions change or are proven to be incorrect.

6.1.3 Risk Analysis

Risk Management is central to the development effort and involves the systematic discovery and elimination of uncertainty. The criticality of any given risk is related to the dependence that other design decisions have on that input, and a large fraction of overall Risk Management takes place as a by-product of applying good engineering practices.

There exist, however, more fundamental classes of uncertainty that have much wider impact, and therefore require elevation to higher visibility levels for appropriate resolution. OOI Risk Analysis is discussed in another OOI developed and maintained document and process, called the *OOI Risk Management Plan (RMP)*. Cost-based analysis of risk, as well as contingency planning and funding is documented and managed through the *OOI Cost Estimation Plan*.

Risk management is defined as a systematic approach to identifying, analyzing, and controlling areas or events with a potential for causing unwanted change. It is through risk management that risks to the program are assessed and systematically managed to reduce risk to an acceptable level. The OOI program has established the following risk management objectives:

a) To develop and implement a risk management process with risk assessment, handling, and monitoring functions; to define and generate risk watch lists; and to apply metrics to assess the implementation of alternative concepts.
b) To establish quantified acceptable risk levels to be achieved and to define the risks and proposed risk mitigation steps to be addressed during design and construction.

6.1.3.1 Risk Identification

Risks can only be tracked and mitigated if they are known. Therefore, it is essential to establish a working culture wherein individuals freely share their risk awareness and to ensure that the full range of viewpoints and experience are applied to the discovery of risk. In a manner similar to brainstorming, risks must be easy to nominate for consideration, then subjected to specific analysis to determine the nature, severity, and proposed mitigation method.

OOI, as described in the *OOI Risk Management Plan (RMP)*, has identified/classified six types of risk that could affect the OOI Program:

- Technical Risk
- Cost Risk
- Schedule Risk
- Programmatic Risk
- Operational Risk
- Support Risk

6.1.3.2 Risk Tracking

Once a risk or an opportunity has been identified, it must be captured and tracked through conclusion. Meeting minutes provide the lowest formal level of risk tracking, capturing a summary of the discussions and a list of associated action items that need to be addressed. This process is managed and described i in the *OOI Risk Management Plan (RMP).*

The subset of those risks that represent significant cost, schedule, or technical impact to the project are elevated for appropriate management attention, tracked using a database, and closely monitored through closure.

A central repository of risks is established in the Software Application Framework to facilitate management and tracking through closure. The OOI SDE Configuration Management tools and OOI SDE Collaboration tools will be made to capture, track, monitor and manage risks as defined in terms of (as applicable):

- A unique log number assigned to each risk
- Date the risk was opened
- Title
- Reference
- Status
- Actual Closure Date
- Risk Type
- Related Work Breakdown Structure
- Root Cause
- Description and Impact Summary
- Corrective Action
- Closure Approach
- Responsibility
- Impact
- Date of last Record Update
- Planned Closure Date
- Comments

Responsible individuals, Risk Managers, are to provide up-to-date status information regarding assigned risks through closure. Periodic reviews are conducted by management to assess progress and evaluate resource priorities.

6.1.3.3 Risk Mitigation

In all cases the goal of Risk Management is either to avoid the risk in the first place or to minimize the potential impact. Every risk is associated with a responsible owner, who is charged with analysis and mitigation of the underlying root cause.

Root cause analysis is essential not only to differentiate between the observable symptom and the underlying concern, but to understand the full potential impact and thus properly prioritize resources and overall effort to be applied.

6.2 Requirements Validation Process

The OOI Program Office shall ensure that defined technical requirements, defined acquirer requirements, defined other stakeholder requirements, defined system requirements and specified requirement statements, individually and as sets, are well formulated and agree with needs and expectations.

The OOI System Integration, Verification and Validation Plan outlines how OOI and each IO will analyze and compare identified and collected requirements to the set of defined requirements to determine downward and upward traceability, analyze and compare the set of validated system technical requirements with the sets of defined logical solution representations and derived technical requirements, and make sure the systems, subsystems and tasks are consistent with the level of system structure, enterprise based life cycle phase, and each Validation Process.

Use of OOI SDE Configuration Management tools and OOI SDE Collaboration tools will be made to monitor and manage each step in the Validation Process and ensure that all steps and requirements are met.

6.3 System Verification Process

6.3.1 OOI Verification and Testing Process

The OOI shall perform thorough and appropriate testing throughout the Construction and Operations and Maintenance phases of the program, to verify that each end system, subsystem, and component defined and implemented by each IO functions properly and conforms to the requirements of the IO and OOI logical and physical design solution. **Error! Reference source not found.** shows an overview of the types of verification and testing that will occur on the program, and indicates when each type of verification or testing occurs in relationship to the system development life cycle.

Throughout all verification and testing activities, the IOs and OL shall use OOI SDE Configuration Management tools and OOI SDE Collaboration tools to monitor and record verification and test results, including: variances identified (untraceable requirements and constraints, anomalies, variations, voids, and conflicts), corrective actions taken; lessons learned; outcomes achieved; tradeoff, effectiveness, and risk analyses completed with resulting key decisions; test activities completed; and the verified design solution.

If the cause of an identified variance was failure to properly complete the fully characterized design, the design and development is re-worked and the verification and testing procedures are then re-run against the modified product.   If the cause of an identified variance was an inadequate test plan or test environment, the test plan or test environment is corrected and the verification and testing procedures are re-run.

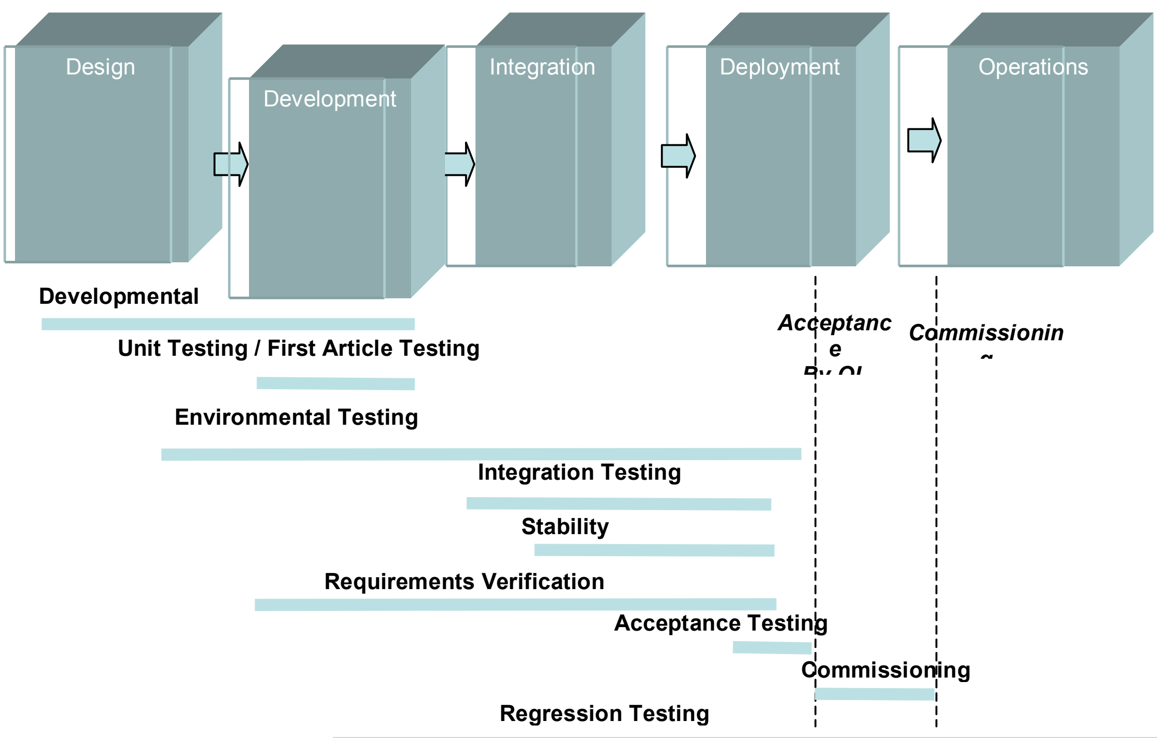

Figure 16, Verification and Testing Activities Throughout the System Development Life Cycle

6.3.1.1 Developmental Testing

Developmental Testing is conducted during the Design and Development stages of the system development life cycle. The purpose of this type of testing is to investigate and prove feasibility of design options, to develop and test prototype solutions, to demonstrate proof of concept, and to manage and reduce design and implementation risks. Developmental testing is conducted at the IO level. In the Cyberinfrastructure IO spiral development methodology, Developmental testing occurs primarily during the Inception Phase of the spiral development model.

Results of Developmental testing are documented and used to inform the ongoing design and development of the associated product.

6.3.1.2 Unit Testing / First Article Testing

Unit Testing / First Article Testing is conducted during the Development phase of the system development life cycle. It is the first level of functional testing performed on the lowest level production units which are produced or procured by the IOs. Unit Testing / First Article Testing confirms that there are no remaining design changes needed prior to production and deployment of the unit or second and subsequent articles. Successful unit testing of all component units must be completed before integrating the units into the next level of assembly for integration testing.

Unit Testing / First Article Testing is conducted at the IO level. In the Cyberinfrastructure IO spiral development methodology, unit testing occurs during the Elaboration and Construction Phases of the spiral development model.

During the formal test itself, all items except the Unit Under Test (UUT) are considered test equipment and must be carefully managed to avoid errors in interpretation of test results.

6.3.1.3 Environmental Testing

Environmental Testing is an optional type of testing conducted during the Design, Development and Integration phases of the system development life cycle. It is important to obtain *in situ* deployment and operating experience as early in the project as possible, especially for the critical elements of the system; thus Environmental Testing is sometimes necessary. In Environmental Testing, hardware components tested previously in Unit or Integration testing are tested again in a “wet environment,” with pressure, temperature, and other environmental factors as similar to those at the deployment site as practicable. The achieved performance of the product being tested is measured against the required performance.

In most cases water tanks and near shore testing are used for environmental testing of hardware components, and while simulating the deployment site environment, environmental testing is still considered testing in a non-deployed test. Additional refinements indicated by the environmental testing effort are incorporated into the product design during this cycle.

Environmental testing is conducted at the IO level, and each IO is responsible for the documentation, maintenance, performance, and monitoring of its environmental tests.

The Initial Operating Capability (IOC) CI spiral development milestone is a gate to the Environmental Testing described above. The IOC occurs at the end of the Construction phase of the spiral development model (see 4.1.1.3), and transitions the construction activities into the deployment activities. Success criteria include the requirement that a functioning system be delivered that implements the functional specification and external integration criteria from the LCA, documentation of unit tests for all system components and system tests for functionality, and a plan for deployment metrics and integration points. The IOC review/test is performed internally to the CI IO with participation from the Program Office and other IOs as needed.

6.3.1.4 Integration Testing

Integration Testing is conducted during the Integration and Deployment phases of the system development life cycle. Integration is the incremental and iterative process of combining lower-level parts or components into higher-level assemblies. Testing of assembly functionality, performance and interfaces is conducted at each level of integration. Some levels of integration can only be tested fully after actual deployment of the integrated assembly.

Integration testing is conducted by individual IOs, and at higher levels of OOI integration, is conducted jointly by two or more IOs who are contributing components to the integrated assembly being tested. Integration test plans and procedures are documented and integration results are recorded. Interface requirements, interface diagrams, and interface control documents are used to inform the Integration test plans and to evaluate Integration testing results.

In the Cyberinfrastructure IO spiral development methodology, integration testing occurs during the Construction Phase of the spiral development model.

6.3.1.5 Stability Testing

The purpose of stability testing is to show that the product being tested can perform as intended over an extended period of time with no significant degradation in performance, functionality, or usability. Hardware burn-in testing and software memory growth testing are examples of stability tests.

Stability testing is conducted by the IOs during the Integration and Deployment phases of the system development life cycle. In the Cyberinfrastructure IO spiral development methodology, stability testing occurs during the Construction and Transition Phases of the spiral development model.

6.3.1.6 Requirements Verification

Requirements Verification is conducted during the Development, Integration, and Deployment phases of the system development life cycle. It is conducted by the IOs, and may be witnessed by OL personnel. In the Cyberinfrastructure IO spiral development methodology, requirements verification occurs during the, Construction, Phase of the spiral development model.

Requirements Verification is the formal process of assessing a product to determine whether it complies with its documented requirements. Individual requirements are verified according to the verification method assigned to them (see section 7.3.3). Requirements Verification results are tracked on the Requirements Verification Matrix. Requirements verification is a superset of other types of testing; i.e., requirements may be verified during unit testing, environmental testing, integration testing, or stability testing, or in several or all of these instances. All product requirements must be verified as a prerequisite to formal Acceptance of an IO product by OL.

6.3.1.7 Acceptance Testing

As the first Ocean Leadership (OL) and OOI led verification and testing activity, Acceptance Testing seeks to validate and verify that the requirements were met and that the subsystem, system or item to be accepted is a quality product. Successful completion of Acceptance Testing results in formal Acceptance of the delivered product, and transfer of "ownership" of the product to OL. Acceptance criteria require that the system, subsystem or item be operating in a near-steady state or non-logistics-supported mode.

Acceptance Testing occurs during the Deployment phase of the system development life cycle. In the Cyberinfrastructure IO spiral development methodology, Acceptance Testing occurs during the Transition Phase of the spiral development model.

The act of Acceptance constitutes acknowledgment that the supplies or services offered to Ocean Leadership (OL) conform to applicable contract or sub-award quality and quantity requirements and are subject to and conform to other terms and conditions of the contract or sub-award.

Verification of all requirements related to the delivered product is a prerequisite to formal Acceptance. Other Acceptance testing includes stability testing, usability testing, and the execution of use case scenarios which demonstrate that the system fulfills end user needs.

Acceptance Testing and its process is described and maintained in the *OOI Quality Assurance and Quality Control Plan (QA/QC)*, the *OOI Operations and Maintenance Plan (O&M),* and as part of required documentation of any supplier/contractor issued contract.

6.3.1.8 Commissioning Evaluation

The final stage of the OOI verification and testing process, the Commissioning Evaluation is a full deployment test at the Array level, against a fully integrated Array (including software). The Commissioning Evaluation includes the validation and verification that all required logistical and support systems are in place and operational, and that the Array is operating in a controlled "steady state." Commissioning criteria are formally documented, and include that the Array is ready to use in routine operations, operations staff has been trained, and operational troubleshooting procedures have been developed and documented. Demonstration that the Array meets all of the formal commissioning criteria marks the transfer of responsibility from the Engineering to the Operations domain.

With the OOI Program Office managing and maintaining processes of Commissioning, with input and collaboration with each IO, the Commissioning Evaluation tests are performed by Array, lowest level item through component, assembly, element, sub-system and system as appropriate for each category of test. Commissioning and its process is described and maintained in the *OOI Commissioning Plan* and *Quality Control Plan and OOI Quality Assurance and Quality Control Plan (QA/QC)*, *OOI Operational and Maintenance Plan (O&M),* and as part of required documentation of any supplier/contractor issued contract. Full Operational Capability (FOC) is achieved as of the completion of the deployment and commissioning cycle.

6.3.1.9 Regression Testing

Regression testing is conducted throughout the Development, Integration, Deployment, and Operations phases of the system development life cycle. In the Cyberinfrastructure IO spiral development methodology, regression testing occurs during the Elaboration, Construction, Transition, and Operations Phases of the spiral development model. Regression tests repeat previously-conducted unit, integration, environmental, stability, or requirements verification tests, and are conducted when hardware or software design or implementation changes are made after the original test is conducted. Regression tests verify that the design or implementation change not only fixed the problem or provided the improvement it was intended to address, but also that the change did not cause any unintended adverse side effects in other capabilities.

Regression tests are conducted by the IOs. Each IO documents and maintains a suite of regression tests, and chooses the correct regression tests to run when system design or implementation changes are made.

6.3.2 Configuration Item (Config-I) Verification

Each IO has a set of Configuration Items (Config-I) which they must monitor, assess, manage and maintain throughout each OOI project lifecycle phase. Configuration items are defined at a level of product aggregation that is appropriate for managing and testing changes, modifications, or upgrades. *ifdr* reviews are conducted at the Configuration Item level, and Integration Test Plans within an IO are written at the Configuration Item level.

The list of Configuration Items for each IO is maintained in document 1100-00001, the Configuration Item Table.

6.3.3 Requirements Verification Methods

All OOI requirements must be verified as a prerequisite to system acceptance and commissioning. Verification answers the question “Did you build the system right?”, i.e., verification is the process by which it is determined that the delivered product conforms to its stated requirements. The DOORS database is used to assign verification methods to requirements. Once a requirement is properly stated, the goal is to select the verification method most suited to obtaining the needed confidence at the lowest cost and schedule impact to the project. Note that verifiability is only one of several key characteristics that a good requirement must possess, but few other activities have as much beneficial impact as considering verifiability at the same time the requirement is being written.

Verification methods are associated primarily with Level 4 requirements in DOORS. Generally, Level 3 and Level 2 requirements are considered to be verified when all of their child requirements have been verified, making it important that the linkage of Level 2, Level 3, and Level 4 requirements be correct and complete. In cases where the full intent of a Level 3 requirement cannot be completely verified through verification of its child Level 4 requirements, a verification method will be assigned to the Level 3 requirement and supplemental verification procedures will be developed for the Level 3 requirement.

For OOI, four verification methods have been defined: Analysis, Inspection, Demonstration, and Test. Each of these methods is described in more detail below, but all compare the stated requirement against some external criteria. The difference between methods lies in the degree of confidence obtained and the effort expended to achieve. When Demonstration or Test is selected, the tasks of defining the demonstration or test environment and associated pass/fail criteria must be also accomplished.

Analysis: Analysis is the use of mathematical, narrative, graphical, or physical models to verify the requirement. It may include estimation of execution times and estimation of system resources. This category encompasses a wide range of possible techniques, ranging from formal engineering analysis to historical analogy. Formality of the analysis should be matched to the criticality and fundamental nature of the requirement. Examples of requirements for which

Analysis is an appropriate verification method include Reliability/Maintainability/Availability (RMA) requirements.

Inspection: Inspection is the examination, by visual or other means, of a product's physical characteristics, processes, or documentation, to confirm that the stated requirement has been met. The product is not used during the inspection; it is only examined. Examples of requirements for which Inspection is an appropriate verification method include requirements for the existence or inclusion of a component part (e.g., AUVs shall include a satellite-based recovery beacon), requirements for a physical characteristic or attribute (e.g., Global Surface Buoy Buoyancy material shall be made of foam), and requirements for adherence to a process (e.g., CI services shall utilize a naming scheme that is compliant with the OOI naming convention).

Demonstration: Demonstration is the use of the product in some operation that verifies the product's capability to meet the functional objectives expressed in the requirement. Demonstration is a qualitative process. Success of the demonstration is determined by observation alone or by simple measurements. Requirements for which Demonstration is an appropriate verification method are those requirements which describe functionality of a product without expressing quantitative goals (e.g., Gliders shall obtain GPS position when surfaced.).

Test: Test is the most formal verification method for a requirement. It is the process of submitting a product to an operating, instrumented examination under a controlled, repeatable set of conditions. Quantitative results are obtained from the test, which are evaluated against specified limits or responses in the requirement language. Formal tests are planned and documented using a formal written test procedure.

It is essential that any unique requirements associated with the test itself such as interface cables, test equipment (and associated calibration requirements), software, scripts, terminations, or any other non-operational behavior of the system be captured in the test plan and test results. Each of these test-support elements must also be documented, validated, and verified prior to being available as a means for verifying the original requirement. This additional effort must be carefully scheduled and managed so that mature test environments are available in time to perform verification.

Requirements for which Test is an appropriate verification method are those requirements which specify quantitative limits or responses (e.g., The Power System Controller shall be capable of maximum output power of 500 W).

6.3.4 Array, System, and Subsystem Readiness

OOI shall determine readiness of arrays, systems, subsystems and items for development, production, test, commissioning, training, support/maintenance, as well as retirement or disposal.

OOI testing, verification and validation processes enabling product readiness determination and associated process proofing in accordance with the appropriate processes, maturity of the related system, life cycle phase, and level in the system structure. It includes selection and definition of the appropriate method for the enabling array and system readiness determination and for proofing for each applicable associated process.

Readiness determination procedures are to be followed for the method selected, and the purpose and objective of each procedure, pre-test and post-test actions, and the criteria for determining the success or failure of the procedure shall be recorded.

OOI testing, verification and validation will also ensure adequacy and completeness of the arrays, system, subsystems and items, including its environment readiness and methods and procedures will be implemented. Further testing will afford assurance that required information regarding the status and maturity of enabling array, system and subsystem development and requirements definition are available, if appropriate, integrated with the environment according to appropriate plans and schedules.

Use of OOI SDE Configuration Management tools and OOI SDE Collaboration tools will collect and evaluate readiness determination outcomes to either show compliance or identify variances (untraceable requirements and constraints, anomalies, variations, voids, and conflicts); thus enable array, system and subsystem readiness determination and associated process proofing, using the selected methods and procedures within the established environment.

6.3.4.1 Stakeholder Engagement

An important element of system-level stakeholder engagement is the process of eliciting user requirements from representatives of the science and education user communities at meetings or workshops. The roles and processes for this purpose are described in Section 6.

A second key element of stakeholder engagement is the inclusion of selected stakeholders at milestone reviews, especially the annual IOC where the previous software release is evaluated and the requirements and plans for the next one are described.

6.3.4.2 Integrated Logistics Support Management

Integrated Logistics Support (ILS) defines all of the elements required to support the OOI program and associated systems throughout its life cycle. It is usually divided into ten components:

- Maintenance planning
- Supply support
- Test equipment/equipment support
- Manpower and personnel
- Training and training support
- Technical data
- Computer resources support
- Facilities
- Packaging, handling, storage, and transportation (PHS&T)
- Design interface.

The ILS process and products are to be developed jointly with the Operations and Maintenance team. The objective of the ILS process is the design, development, and delivery of supportable, reliable, sustainable, maintainable and affordable OOI systems and subsystems that meet the required operational performance, availability and Total Ownership Cost (TOC) goals. The ILS process:

- Identifies, defines and incorporates appropriate supportability characteristics into the OOI and individual IO system and subsystem designs
- Develops and delivers the OOI focused product support to sustain TOC goals

6.4 End Products Validation Process

6.4.1 End Products Validation

OOI shall ensure that systems, subsystems and items (or an aggregation thereof), conform to their validated acquirer requirements. To accomplish End Products Validation, OOI will determine the type of system, subsystem and/or item validation required and the exit criteria, including reference to the acquirer requirements applicable to the system end products being validated.

OOI conducts End Products Validation in accordance with the IV&V Plan, showing conformance with appropriate requirements. The System Verification Process, discussed above, enables and allows for acquisition of test articles for the validation process, as appropriate to the OOI-based life cycle phase and level of the system structure.

The Validation Process establishes the criteria and process for evaluating the completed system at each release against the user requirements by asking “was the right system built?” The process is the responsibility of the Project Scientists, who carry out the validation process with the assistance of the OOI Chief Systems Engineer and selected stakeholders. Upon completion, the Project Scientists prepare a Validation Report for submission to the Project Manager, who has approval authority. Validation involves the creation and execution of use case scenarios which represent the end user needs from the system.

Use of OOI SDE Configuration Management tools and OOI SDE Collaboration tools such as DOORS will allow for the collection, analysis, and validation of outcomes to identify any variances; resolve variances and repeat any appropriate verifications and validations. Use of such systems will also allow for the recording of assumptions, lessons learned, and other pertinent information about the validation and results to provide traceability.