OOI CYBERINFRASTRUCTURE
NSF OCEAN OBSERVATORIES INITIATIVE

OOI – CyberInfrastructure

Architecture & Design

Organizational Relationships Chart

OV-4 PDR CANDIDATE

November 2007

NSF
JOI Joint Oceanographic Institutions
UCSD

Document owner: OOI CI Design Team

Document History

Date	Version	By	Description of Changes
2007-08-03	1.0	CI ADT	Conceptual Architecture Update Initial Draft. Reframed, replaced ORION with OOI
2007-09-20	1.1	CI ADT	Addressed review comments, replaced ORION with OOI in figures, revised. Added impact of authority domains.
2007-10-04	1.2	CI ADT	Updated fig 1, 2, and 4 and the related text
2007-11-12	1.3	CI ADT	Updated fig. 1, addressed review comments

Preamble

The set of documents named AV*, OV*, SV*, TV* are all part of the OOI CyberInfrastructure Architecture & Design (CIAD), in the structure prescribed by the DoDAF (Department of Defense Architecture Framework). Each document has a designated title, an identifier (such as AV-1) and covers a specific topic in a self-contained way. Document AV-1 provides further explanations and a summary. A glossary of the terms used in these documents and their context can be found in AV-2.

The figure below suggests an intuitive reading flow through the provided documents. Other documents will be added to the figure as they emerge during the design of the CI (for the complete set of documents see AV-1). The thick arrow suggests a reading order through the core documents (AV-1, OV-1, OV-5 and SV-1). The red rectangle highlights the current document.

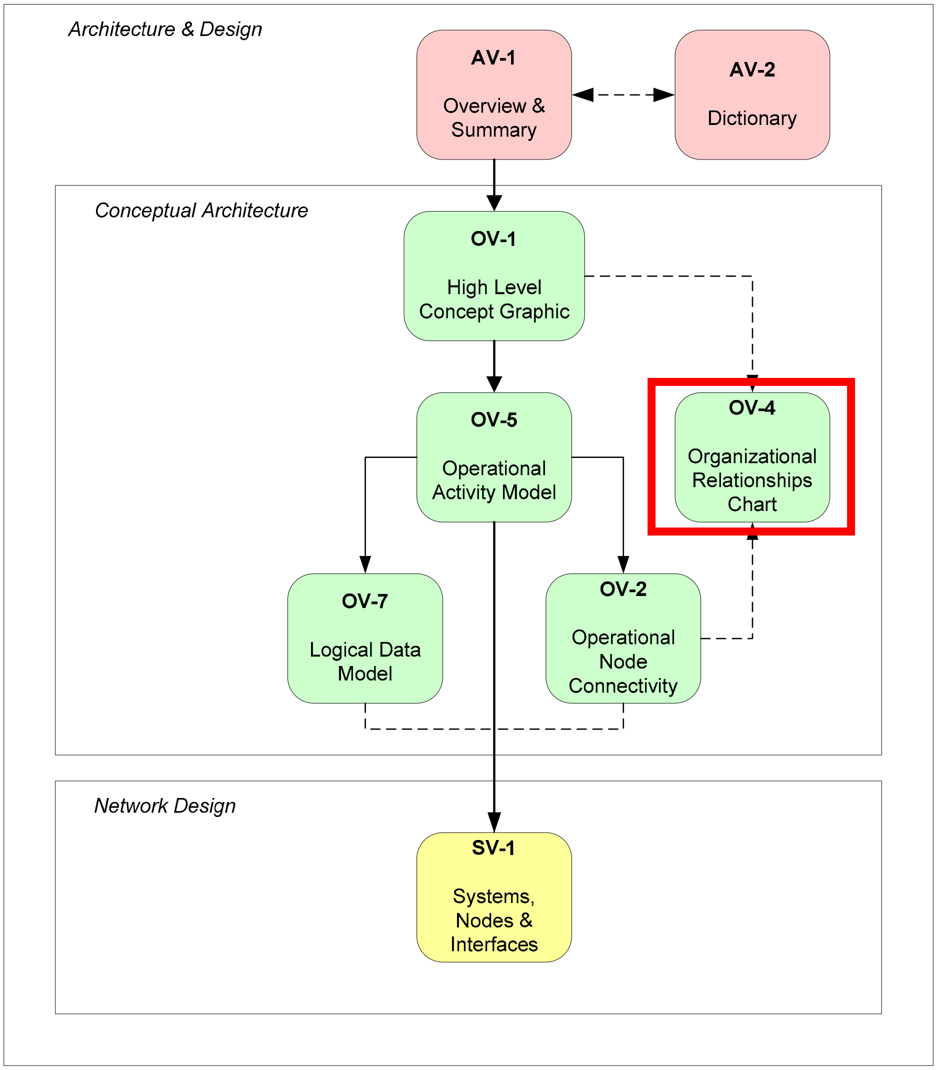
Architecture & Design
AV-1
Overview & Summary
AV-2
Dictionary
Conceptual Architecture
OV-1
High Level Concept Graphic
OV-5
Operational Activity Model
OV-4
Organizational Relationships Chart
OV-7
Logical Data Model
OV-2
Operational Node Connectivity
Network Design
SV-1
Systems, Nodes & Interfaces

Table of Contents

OOI - CyberInfrastructure

Architecture & Design
Organizational Relationship Chart (OV-4)

1 Introduction

1.1 Product Overview

The Organizational Relationships Chart illustrates the command structure or relationships among human roles, organizations, or organization types (as opposed to relationships with respect to process flow) that are the key players in an architecture (adapted from [DoDAF-vII 2007]).

1.2 Product Purpose and Description

OV-4 illustrates the relationships that exist between organizations and sub-organizations within the architecture and between internal and external organizations. Organizational relationships are important to depict because they can illustrate fundamental human roles (e.g., who or what type of skill is needed to conduct operational activities) as well as management relationships (e.g., command structure or relationship to other key players). These can include supervisory reporting, command and control relationships, and command-subordinate relationships. Another type of relationship is between equals, where two organizations coordinate or collaborate without one having a supervisory or command relationship over the other. The key players in OV-4 correspond to the operational nodes of OV-2, which in turn contains added detail on how they interact in order to conduct their corresponding operational activities in OV-5 (adapted from [DoDAF-vII 2007]).

2 Representations

Five figures illustrate the external and internal organizational relationships at two levels: that of reporting and communication relationships, and that of provisioning and consuming relationships under policy constraints. The five figures are:

1. External relationship to IOOS and other major observing systems
2. Internal OOI organizational chart
3. OOI external operational relationships
4. OOI internal operational relationships
5. Authority Domains

The first two diagrams address reporting and communication, while the latter three address provision, consumption, and policy relationships.

2.1 Relationship to Major Observing Systems

Figure 1 shows the relationship of the proposed Integrated and Sustained Ocean Observing System (IOOS) management and reporting structure and of other terrestrial environmental observatories to that of OOI. IOOS is an operationally-oriented national system managed by Ocean.US (http://www.ocean.us), that receives federal sponsorship and oversight from many agencies, with NOAA taking the lead role. IOOS is the key US contribution to the international Global Ocean Observing System (GOOS; http://www.ioc-goos.org) and the Global Earth Observing System of Systems (GEOSS; http://www.earthobservations.org).

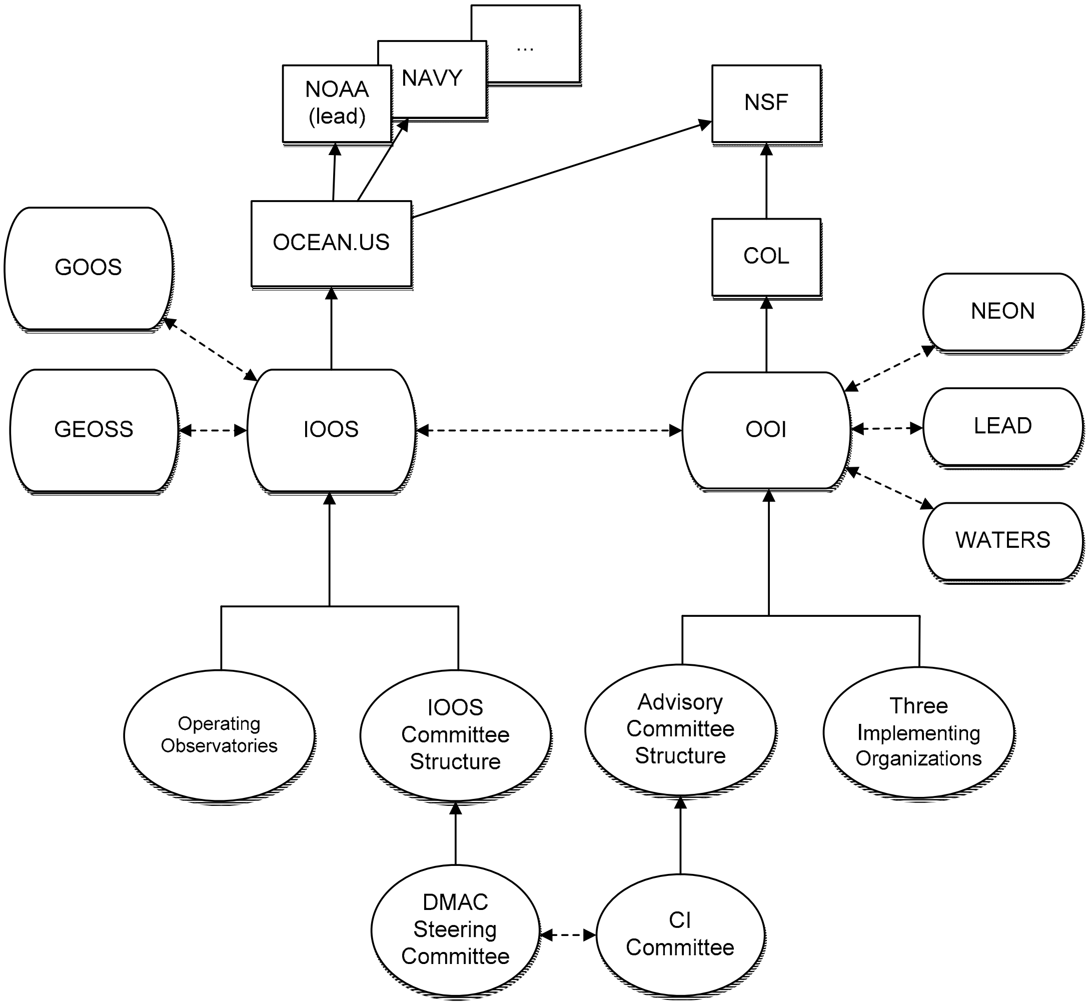

Figure 1. Reporting and coordination structures of IOOS and OOI showing their corresponding management organizations and the principal pathways for communication, along with related terrestrial observatory efforts. The solid lines with single arrows depict a reporting relationship, while a dotted line with double arrows shows a coordination relationship

IOOS has an advisory committee structure whose most pertinent component is the Data Management and Communication (DMAC) activity, and a number of regional associations that integrate ocean observing activities in their geographic areas. Related terrestrial observatory efforts include the National Ecological Observatory Network (NEON; http://www.neoninc.org), Linked Environments for Atmospheric Discovery (LEAD; http://lead.ou.edu), and the WATer Environmental Research Systems Network (WATERS; http://www.watersnet.org).

OOI is the research-oriented component of IOOS. It is managed separately, as indicated in Figure 1. OOI has an advisory committee structure reporting to the OOI Program Office, and it has formulated three Implementing Organizations for the regional scale observatory, coastal-global scale observatory, and cyberinfrastructure components of the Ocean Observing Initiative. OOI is managed by the Consortium for Ocean Leadership (COL) receiving federal sponsorship and oversight from the National Science Foundation (NSF). Further details on the internal OOI relationships are given in Section 2.2.

OOI and its advisory committees have informal relationships with IOOS and various IOOS committees, and notably between the OOI CI Committee and the DMAC Steering Committee and expert teams. These contacts were expanded during the development of the OOI Conceptual Architecture, but were necessarily limited due to resource constraints on both sides and to the IOOS desire to minimize cross-contamination of its two ongoing conceptual architectural investigation activities.

NEON, LEAD, and WATERS all have cyberinfrastructure definition components at differing states of maturity, with LEAD being in the implementation phase and NEON and WATERS being at the concept level. As with IOOS, the primary focus is on data resources and their archiving and dissemination.

A major element of system coordination lies in the interoperation of data resources, so that publicly-available data products from any project will be accessible to all communities. It is anticipated that, at a minimum, registration, discovery, and access services to OOI data resources will be supported according to IOOS standards and best practices. Note that the OOI standards and best practices will likely extend beyond those of IOOS, as OOI anticipates considerably broader functionality for its cyberinfrastructure. Data resource coordination with NEON, LEAD, and WATERS needs to be established.

2.2 OOI Organizational Chart

Figure 2 shows an expanded view of the OOI organizational structure that occupies the right hand side of Figure 1. The central element is the OOI Program Office, run by the Consortium for Ocean Leadership (COL), which provides overall project management and oversight functions for the implementing organizations, houses the educational and public awareness efforts, and sponsors an extensive advisory committee structure.

The Program Office (details not shown in Figure 2) is headed by a Program Director and reports both to the JOI Board of Governors and to the National Science Foundation. The three implementing organizations for the regional scale node, coastal-global scale node, and cyberinfrastructure elements report to the project office through the OOI Director of Engineering.

The OOI Advisory Committees advise the Program Office on policies and procedures for observatory operations, usage, and data management, approve annual OOI Science and Operations Plans, and carry out program planning and development functions. Originally, the top-level group was an Observatory Steering Committee (OSC) that supervised a Science and Technology Advisory Committee (STAC), and in turn had subcommittees for Sensors, Cyberinfrastructure (CI), Engineering (EC), and Education and Public Awareness (E&PA). The original advisory structure has been replaced temporarily with the Interim Observatory Steering Committee, and future changes will be accommodated within Figure 2.

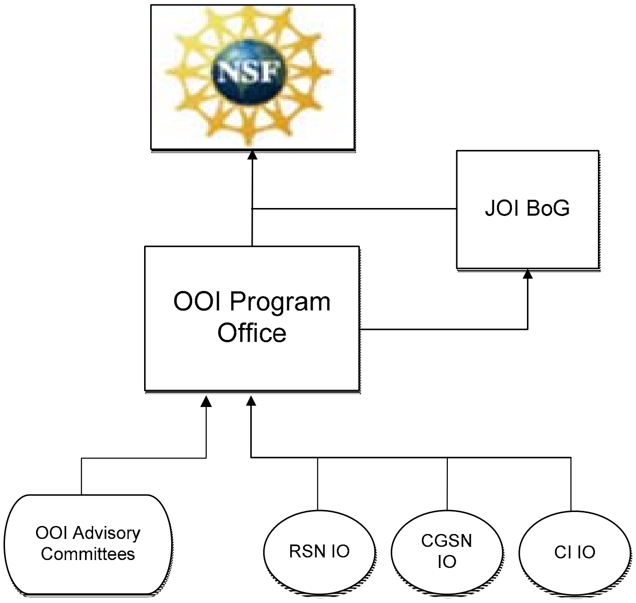

Figure 2. Internal organizational chart for OOI showing reporting relationships

2.3 OOI External Operational Relationships

Figure 3 shows the external provisioning, consumption, and policy relationships for OOI. The central element is the OOI node (including a human management component) that has two types of relationships with external entities.

In the first instance (at the top of the diagram), OOI publishes data and data products and provides them to external users. OOI also consumes externally produced data and data products via a mediation layer, which transforms them into OOI-compatible formats. These data and data products are in turn distributed to Laboratories, Observatories, and other collaborations that are internal to OOI, and those collaborations also provide their own data and data products to the OOI system (see Figure 4).

In the second instance, OOI has analogous relationships with two classes of actors: Members and Resource Providers. OOI defines membership agreements to which members must agree and after which they may access OOI resources and services. OOI also defines service level agreements to which external resource providers must agree, as well as service templates to which the provided external resources must adhere. Upon accepting the agreements and following the templates, the resource provider’s resource(s) may be integrated into the OOI system, and thereby become available to OOI members.

Agreements are intended to assure effective operation of the OOI system for all of its users and providers. They are analogous to negotiated interface protocols that allow the effective exchange of data among different components of the system.

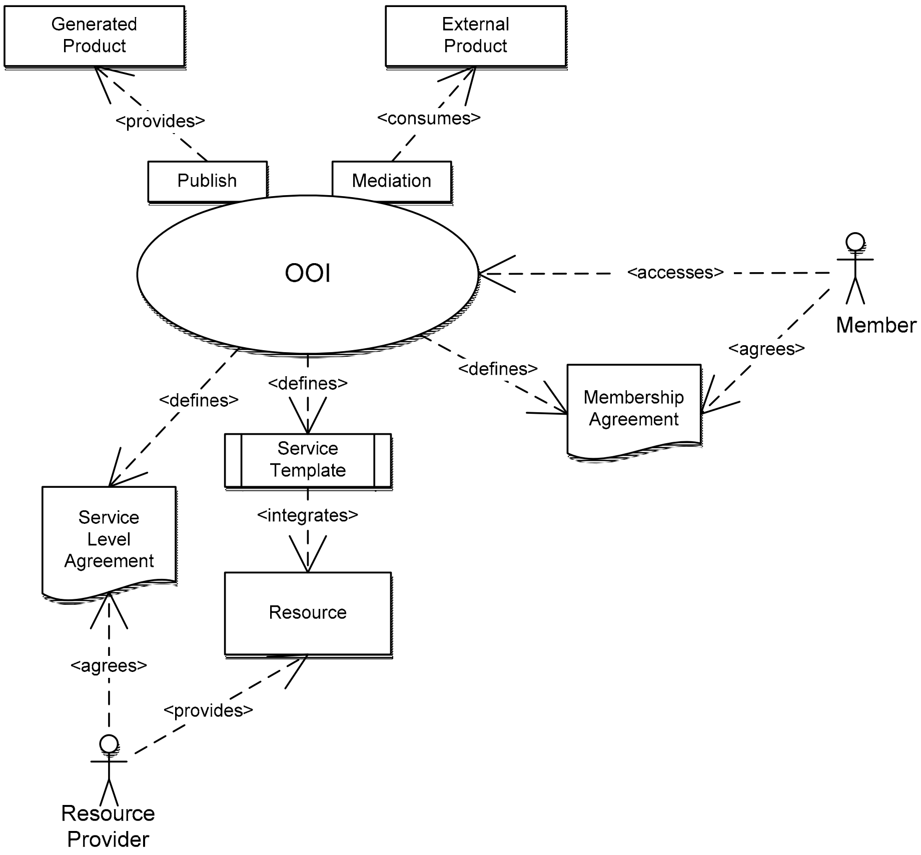

Figure 3. OOI External Operational Relationships

2.4 OOI Internal Operational Relationships

Figure 4 shows the internal organizational relationships among the classes of actors and nodes, as well as the services that mediate these relationships.

The two key nodes in Figure 4 are the Marine Observatory at the left and the Laboratory at the upper right whose connectivity to other nodes is described in OV-2. The Marine Observatory is governed by the Marine Operator, who uses Policy defined by the OOI Program Office Oversight actor and contracts with the CyberInfrastructure Operator for CyberInfrastructure services that he or she uses to operate a network of instruments. The Marine Observatory uses control, processing, and resource management services to operate and govern a suite of Instruments, and provides real-time or near real-time Data Products, Event Detection and Instrument services for use in Laboratories.

Laboratories are a second principal organizing node, and allow participants to collaborate in a dedicated virtual space. Instrument Providers, Collaborating Investigators, and other invited participants share infrastructure resources under the supervision of the Principal Investigator, who governs the collection of resources. The Laboratory makes use of a wide range of CyberInfrastructure services and produces Data Products and some modeling services that can then be made available by OOI.

The CyberInfrastructure Operator governs the CyberInfrastructure and contracts with Resource Providers for Resources such as computing, storage, networking and their associated services. The CyberIn-

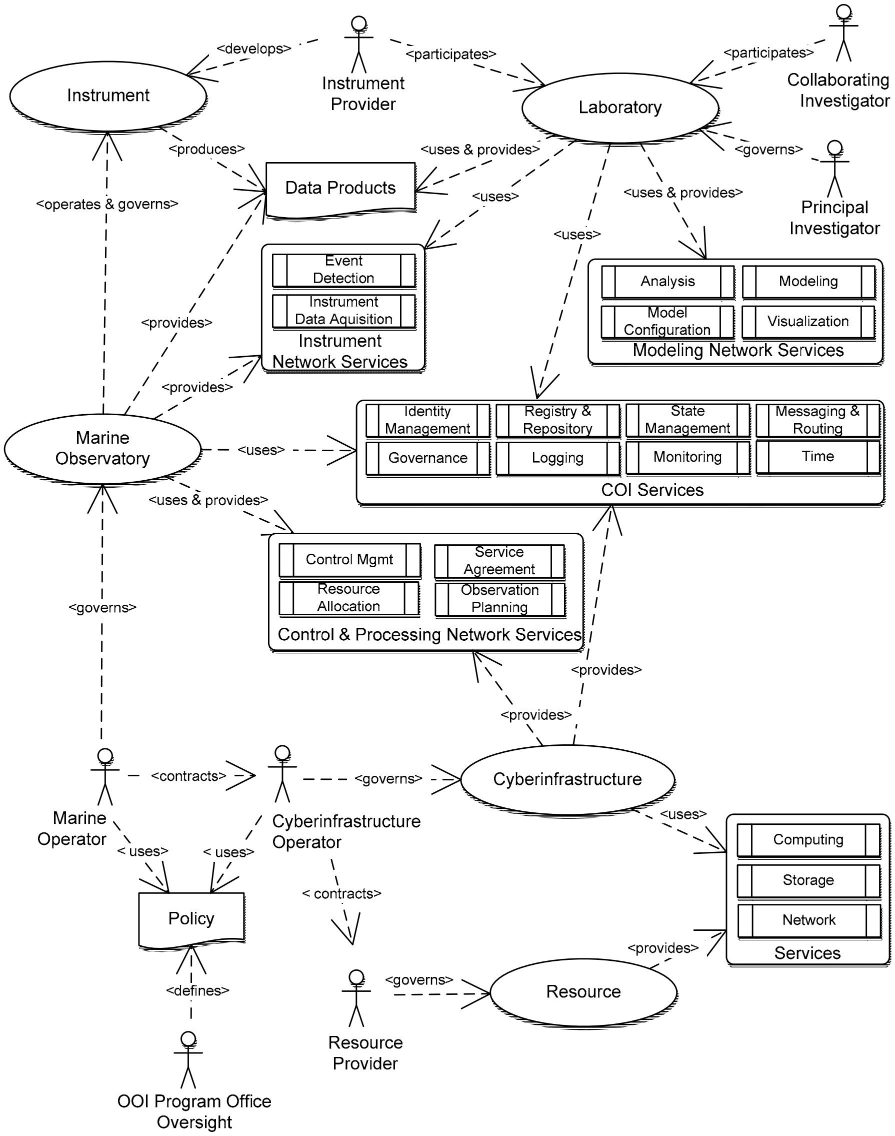

Figure 4. OOI internal operational relationships

frastructure both uses resource services and provides a wide range of core services to Observatories and Laboratories, including identity management, governance, security, policy enforcement, logging, messaging and routing, service orchestration, interaction monitoring, resource cataloging and persistence, and accurate synoptic time.

The Instrument Provider develops Instruments for use in the Observatory, and may participate in Laboratories through an expert role. The Instrument node receives instructions through services provided by the Marine Node, and produces data products for use by Laboratories and other members of OOI. Availability of Instruments,and the Data Products they produce to the community is governed by the policies of OOI, as expressed via the Marine Observatory and Laboratory.

2.5 Impact of Authority Domains on the Architecture

Figure 5 shows three different authority domains involved in oceanographic operations: marine domain, CyberInfrastructure domain, and instruments in the domain of the researcher. For example, a Researcher may want to access an instrument that belongs to the marine community. Even when the Researcher accesses their own instrument, they still have to obey the set of policies regarding the power usage, allowed research activities, and timing of activities at the observatory node. Because each party has its own set of policies, the operations are constrained by all policies. Therefore, the CyberInfrastructure has to provide for the management and governance of resource access across authority domains. This requires contract agreements, access policies, identity federation, and resource usage tracking. The architecture has to support the deployment, operation, and distributed management of resources across a cyber-infrastructure operated by independent stakeholders. It facilitates a seamless communication along the levels of hierarchy without the Researcher or Instrument being aware of the fact that they are communicating with entities out of their authority domain.

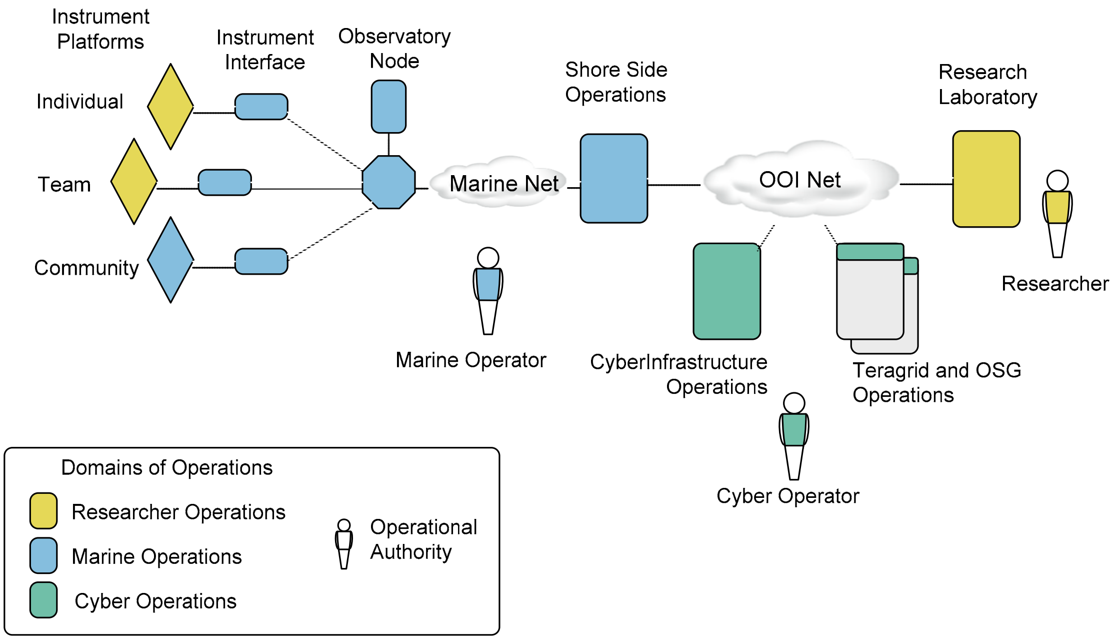

Figure 5. Authority Domains