Designation: F2594 – 07

Standard Guide for Unmanned Undersea Vehicle (UUV) Communications[1]

This standard is issued under the fixed designation F2594; the number immediately following the designation indicates the year of original adoption or, in the case of revision, the year of last revision. A number in parentheses indicates the year of last reapproval. A superscript epsilon (ε) indicates an editorial change since the last revision or reapproval.

INTRODUCTION

ASTM has prepared this series of standards to guide the development of autonomous unmanned underwater vehicles (UUVs). The standards address the key capabilities that a UUV system must possess in order to be considered autonomous and reconfigurable:

Autonomous— Capable of operating without operator input for extended periods of time. Implicit in this description is the requirement that the UUV's sortie accomplishes its assigned goal and makes the appropriate rendezvous for a successful recovery.

Reconfigurable— Capable of operating with multiple payloads. The top level requirement is established that the UUV systems will consist of:

Payloads to complete specific system tasking such as environmental data collection, area surveillance, mine hunting, mine countermeasures, intelligence/surveillance/reconnaissance (ISR), or other scientific, military, or commercial objectives.

Vehicles that will transport the payloads to designated locations and be responsible for the launch and recovery of the vehicle/payload combination.

While the payload will be specific to the objective, the vehicle is likely to be less so. Nevertheless, commonality across all classes of UUV with respect to such features as planning, communications, and post sortie analysis (PSA) is desirable. Commonality with regard to such features as launch and recovery and a common control interface with the payload should be preserved within the UUV class.

In accordance with this philosophy, ASTM identifies four standards to address UUV development and to promote compatibility and interoperability among UUVs:

F2541 Guide for UUV Autonomy and Control,
WK11283 Guide for UUV Mission Payload Interface,
F2541 Guide for UUV Communications, and
F2595 Guide for UUV Sensor Data Formats.

The relationships among these standards are illustrated in Fig. 1. The first two standards address the UUV autonomy, command and control, and the physical interface between the UUV and its payload. The last two ASTM standards address the handling of the most valuable artifacts created by UUV systems: the data. Since there are many possibilities for communications links to exchange data, it is expected that the UUV procurement agency will provide specific guidance relative to these links and the appropriate use of the UUV communications standard. In a similar manner, specific guidance is expected for the appropriate use of the UUV data formats.

F2541–Standard Guide for UUV Autonomy and Control—The UUV autonomy and control guide defines the characteristics of an autonomous UUV system. While much of this guide applies to the vehicle and how the vehicle should perform in an autonomous state, the relationship of the payloads within the UUV system is also characterized. A high level depiction of the functional subsystems associated with a generic autonomous UUV system is presented. The important functional relationship established in this guide is the payload's subordinate role relative to the vehicle in terms of system safety. The payload is responsible for its own internal safety, but the vehicle is responsible for the safety of the vehicle-payload system. Terminology is defined to provide a common framework for the discussion of autonomous systems. System behaviors and capabilities are identified that tend to make a system independent of human operator input and provide varying levels of assurance that the UUV will perform its assigned task and successfully complete recovery. A three-axis sliding scale is presented to illustrate the system's level of autonomy (LOA) in terms of situational awareness,

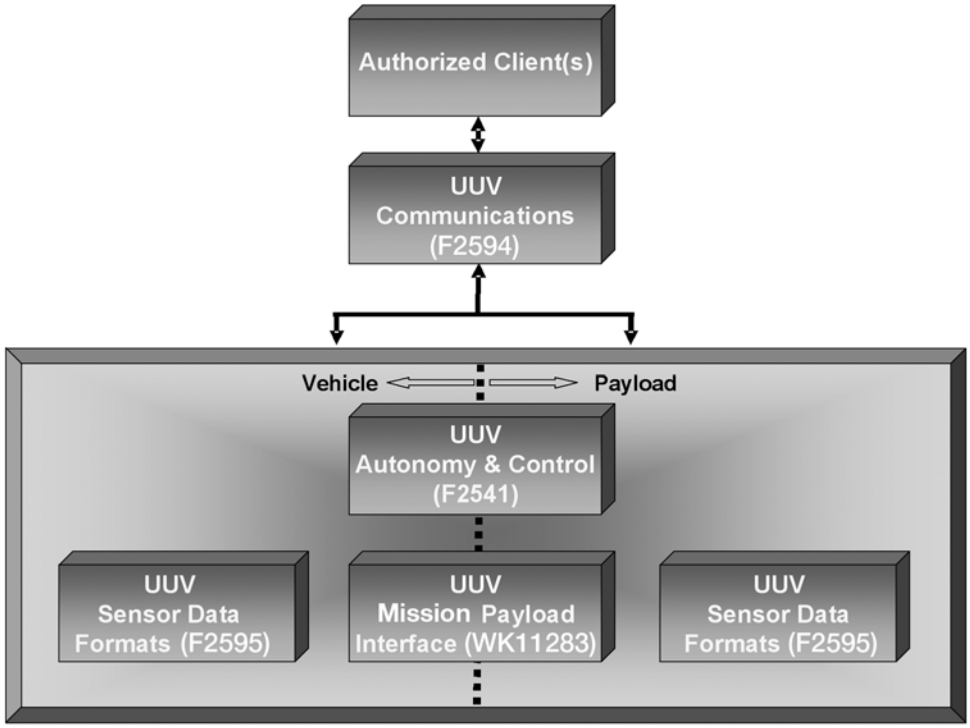

FIG. 1 Notional System Interfaces and Governing Standards

decision-making/planning/execution, and external interaction. The control interface (messages exchanged between the vehicle and the payload) is described and instantiations of this interface for the various classes of UUV are presented in associated appendixes.

WK11283–Standard Guide for UUV Physical Payload Interface—The UUV physical payload interface guide is a physical and functional interface standard that guides: the mechanical and electrical interface between the vehicle and the payload, and the functional relationship between the vehicle and the payload. In-as-much-as a single physical interface standard cannot address all classes of UUVs, this guide describes the physical interfaces in the body of the guide and provides appendixes to guide the instantiation for each of the classes. This guide reinforces the relationship between the vehicle and the payload and confirms the permission-request responsibility of the payload and the permission-granted/denied authority of the vehicle.

F2594–Standard Guide for UUV Communications—The UUV communications standard guides the development of offboard communications between the UUV system and the authorized clients, that is, those agents designated by the UUV operational authorities with responsibility for programming, operating, or maintaining a UUV, or a combination thereof. An authorized client may also represent an end user of UUV and payload mission data. Such a standard is required to provide for UUV interoperability with multiple authorized agents and to provide the authorized agents with interoperability with multiple UUVs (preferably across the different classes of UUVs). Optical, RF and acoustic methods of communication are considered. While RF communication is a matured communications mode and existing standards are referenced and adopted for offboard surface communication, underwater acoustic communication (ACOMMS) is an evolving field and interoperability between the different ACOMMS systems is also evolving. Typical ACOMMS systems and protocols are described with typical applications related to bandwidth and range. General comments are provided for optical communication as the use of this mode of communication may evolve in the future.

F2595–Standard Guide for UUV Sensor Data Formats—The UUV sensor data formats guide provides the UUV and payload designer with a series of commonly accepted data formats for underwater sensors. These formats provide the opportunity for two-way interoperability. Their use

[1] This guide is under the jurisdiction of ASTM Committee F41 on Unmanned Maritime Vehicle Systems (UMVS) and is the direct responsibility of Subcommittee F41.02 on Communications.

Current edition approved April 15, 2007. Published May 2007. Originally approved in 2006. Last previous edition approved in 2006 as F2594 – 06. DOI: 10.1520/F2594-07.

facilitates the UUV system's ability to process historical environmental data for mission planning purposes. Likewise, use of these formats facilitates the end users' ability to catalog, analyze, and produce recommendations based on current field data. Fig. 1 suggests that both vehicle-specific data as well as payload sensor data should be stored in these data formats.

1. Scope

1.1 This guide establishes the basic communications requirements for Unmanned Undersea Vehicles (UUVs). In its first instantiation, this guide serves as only a guideline, and not a definitive directive on acceptable UUV communication standards. In fact, this initial version is more accurately considered a compendium that addresses myriad communication modalities, where the selection of listed standards is determined after communication requirements are tailored to specific UUV applications and payloads.

1.2 This guide is intended to influence the design and development process for the acquisition and integration of vehicles, payloads, and communication system components, while at the same time to avoid specifying particular solutions or products. In its initial release, an additional intent of this guide is to address the communication standards required for operation of the U.S. Navy's planned 21-in. Mission Reconfigurable UUV System (MRUUVS) which is representative of its heavy weight class of UUVs. Guidance provided by the newly mandated and continually evolving, DoD IT Standards Registry (DISR) in the realm of existing military communication standards is also provided as a reference. Although there is a certain emphasis on U.S. Navy UUV missions, there is broad utility across the spectrum of commercial applications as well.

1.3 The breadth of standards addressed within this guide encompasses widely recognized Network standards and RF communications standards, including line of sight (LOS) and beyond line of sight (BLOS). Discussion of optical laser and underwater acoustic communications standards that are in development is also included. Besides identifying existing communication infrastructure, waveforms, and standards, this guide also briefly addresses related issues, security considerations, and technology forecasts that will impact fleet communication systems in the near future (5 to 10 years).

1.4 For ease in reading and utility, specific recommendations of existing standards are captured in tables segregated by communication domain. In some cases where standards are still under development or do not yet exist, details have been reserved for future revisions to this guide. Similarly, in various sections, elaboration of certain topics has either been determined to be beyond the scope of this guide or more appropriate for forthcoming revisions.

1.5 Readers of this guide will also find utility in referencing the related Committee F41 Guides on UUV Sensor Data Formats, UUV Payload Interfaces, and UUV Autonomy and Control. There is a clear relationship that exists in terms of communication systems, external interfaces, data formats, and information/data exchange which can be applied in context with the standards invoked in those documents.

1.6 The values stated in SI units are to be regarded as the standard. The values given in parentheses are for information only.

1.7 *This standard does not purport to address all of the safety concerns, if any, associated with its use. It is the responsibility of the user of this standard to establish appropriate safety and health practices and determine the applicability of regulatory limitations prior to use.*

1.8 *Table of Contents:*

2. Referenced Documents

2.1 *ASTM Standards:*[2]

F2541 Guide for Unmanned Undersea Vehicles (UUV) Autonomy and Control

F2595 Guide for Unmanned Undersea Vehicle (UUV) Sensor Data Formats

WK11283

2.2 *DoD Documents:*[3]

DoD Directive 8100.1 Global Information Grid (GIG) Overarching Policy, 09/19/2002

DoD Directive 8100.2 Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)

DoD Directive 8320.2 Data Sharing in a Net-Centric Department of Defense, December 2, 2004

DoD IT Standards Registry (DISR) Generated 21 in. MRUUVS[4]

Technical Standards Profile (TV-1)

2.3 *Other Documents:*

CCITT 84 Consultative Committee on International Telegraphy and Telephony[3]

CCSDS401.0-B-6 Radio Frequency and Modulation Systems-Part 1: Earth Stations and Spacecraft, May 2000, Consultative Committee for Space Data Systems

CJCSI 6251.01 Ultrahigh Frequency Satellite Communications Demand Assigned Multiple Access Requirements[5]

Common Data Link Communications Standard Waveform Specification for the Standard Common Data Link, Rev (F)

FIPS 140-1 Security Requirements for Cryptographic Modules[6]

HAIPE IS 1.3.5 High Assurance IP Encryption Interoperability Specification

HAIPE IS 3.0.1 High Assurance IP Encryption Interoperability Specification

ICD-GPS-227 Navstar GPS Selective Availability and Anti-Spoofing (SA/A-S) Host Application Equipment (HAE) Design Requirements with the Selective Availability Anti-Spoofing Module (SAASM), 26 November 2003

IEEE 802.3 IEEE Standard for Information Technology-Telecommunications and Information Exchange Between Systems-Local and Metropolitan Area Networks—Specific Requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications[7]

IEEE 802.16 Standard for Local and Metropolitan Area Networks - Part 16: Air Interface for Fixed Broadband Wireless Access Systems[7]

IEEE 802.20 Local and Metropolitan Area Networks - Standard Air Interface for Mobile Broadband Wireless Access Systems Supporting Vehicular Mobility - Physical and Media Access Control Layer Specification[7]

IESS-309 Rev. 7 QPSK/FDMA Performance Characteristics for INTELSAT Business Services, 10 February 2000

IESS-310 Rev. 2 Performance Characteristics for Intermediate Data Rate Digital Carriers using rate 2/3TCM/8PSK and Reed-Solomon Outer Coding (TCM/IDR), 10 February 2000

IETF Standard 5 Internet Protocol, September 1981. With RFCs 791 / 950 / 919 / 922 / 792 / 1112

IETF Standard 6/RFC 768 User Datagram Protocol, 28 August 1980

IETF Standard 7/RFC 793 Transmission Control Protocol, September 1981

IETF Standard 41/RFC 894 Transmission of IP Datagrams Over Ethernet Networks, April 1984

IETF RFC 2460 Internet Protocol, Version 6 (Ipv6) Specification, December 1998

IETF RFC 2464 Transmission of Ipv6 Packet Over Ethernet Networks, December 1998

IS-GPS-200D NAVSTAR GPS Space Segment/Navigation User Interfaces, 7 December 2004

ISO 12171 (CCSDS201.0-B-2) Space Data and Information Transfer System-Telecommand, Channel Service, Architectural Specification, 1998

ISO 12173 (CCSDS202.1-B-1) Space Data and Information Transfer System-Telecommand, Command Operation Procedures, 1998

ISO 12174 (CCSDS203.0-B-1) Space Data and Information Transfer System-Telecommand, Data Management Service, Architectural Specification, 1998

MIL-STD-188-181C Interoperability Standard for Access to 5-kHz and 25-kHz UHF Satellite Communications Channels, 30 January 2004

MIL-STD-188-182B Interoperability and Performance Standard for UHF SATCOM DAMA Orderwire Messages and Protocols

MIL-STD-188-183B:2 004 Interoperability Standard for Multiple-Access 5-kHz and 25-kHz UHF Satellite Communications Channels, 30 January 2004

MIL-STD-188-184(1) Interoperability and Performance Standard for the Data Control Waveform, 20 August 1993, with Notice of Change 1, 9 September 1998

MIL-STD-188-185(2) DoD Interface Standard, Interoperability of UHF MILSATCOM DAMA Control System, 29

[2] For referenced ASTM standards, visit the ASTM website, www.astm.org, or contact ASTM Customer Service at service@astm.org. For *Annual Book of ASTM Standards* volume information, refer to the standard's Document Summary page on the ASTM website.

[3] Available from U.S. Government Printing Office Superintendent of Documents, 732 N. Capitol St., NW, Mail Stop: SDE, Washington, DC 20401.

[4] Resident in the Joint C4I Program Assessment Tool-Empowered (JCPAT-E) online data base available through DISA DoD C3I Common Data Link Policy and Tactical Data Link Policy.

[5] Available on the web at http://www.dtic.mil/cjcs_directives/cdata/unlimit/6251_01.pdf.

[6] Available from National Institute of Standards and Technology (NIST), 100 Bureau Dr., Stop 1070, Gaithersburg, MD 20899-1070, http://www.nist.gov.

[7] Available from Institute of Electrical and Electronics Engineers, Inc. (IEEE), 445 Hoes Ln., P.O. Box 1331, Piscataway, NJ 08854-1331, http://www.ieee.org.

May 1996, with Notice of Change 1, 1 December 1997; and Notice of Change 2, 9 September 1998
MIL-STD-188-220B Interoperability Standard for Digital Message Transfer Device (DMTD) Subsystems, 22 May 2002
MIL-STD-188-243 Tactical Single Channel (UHF) Radio Communications, 15 March 1989
MIL-STD-6011C Tactical Data Link (TDL) 11/1 1B Message Standard
MIL-STD-6016C:2 005 Tactical Data Link (TDL) 16 Message Standard, 28 March 2005
MIL-STD-6020 Data Forwarding Between Tactical Data Link (TDL), 31 March 2004
PEO C4I Undersea Acoustic Communication Information Exchange Rate Performance Regimes[3]
SEIWG-005 Interface Specification, Radio Frequency Transmission Interfaces for DoD Physical Security Systems, 15 December 1981
STANAG 4175 Technical Characteristics of the Multifunctional Information Distribution System (MIDS), Edition 3, 6 February 2001
STANAG 4294 NAVSTAR Global Positioning System (GPS)-System Characteristics plus Summary of Performance Requirements (Part 2, Edition 2, June 1995), Part 1, Edition 2, December 1997
STANAG 4586 Standard Interfaces of the Unmanned Control System (UCS) for NATO UAV Interoperability Ed. 2
STANAG 5522:200 1 Tactical Data Exchange-LINK 22, Edition 1, September 2001

3. Terminology

3.1 *Acronyms:*

3.1.1 *ACTD*—Advanced Concept Technology Demonstration

3.1.2 *API* —Application Program Interface

3.1.3 *ARQ*—Automatic Repeat Request

3.1.4 *ASW*—Anti-Submarine Warfare

3.1.5 *AUV*—Autonomous Undersea Vehicles

3.1.6 *BAMS*—Broad Area Maritime Surveillance

3.1.7 *BER*—Bit Error Rate

3.1.8 *BGPHES*—Battle Group Passive Horizon Extension System

3.1.9 *BLOS*—Beyond Line of Sight

3.1.10 *C2*—Command and Control

3.1.11 *CAS*—Collaboration at Sea

3.1.12 *CDL*—Common Data Link

3.1.13 *CHBDL*—Common High Bandwidth Data Link

3.1.14 *CJCS*—Chairman, Joint Chiefs of Staff

3.1.15 *COMSEC*—Communications Security

3.1.16 *CONOPS*—Concept of Operations

3.1.17 *COTS*—Commercial Off-the-Shelf

3.1.18 *CRC*—Cyclic-Redundancy Check

3.1.19 *CTS*—Clear-to-Send

3.1.20 *DAMA*—Demand Assigned Multiple Access

3.1.21 *DCGS*—Distributed Common Ground System

3.1.22 *DISA*—Defense Information Systems Agency

3.1.23 *DISR*—DoD IT Standards Registry

3.1.24 *DMR*—Digital Modular Radio

3.1.25 *DoD*—Department of Defense

3.1.26 *DSCS*—Defense Satellite Communications System

3.1.27 *DSP*—Digital Signal Processor

3.1.28 *DVL*—Doppler Velocity Log

3.1.29 *DWTS*—Digital Wideband Transmission System

3.1.30 *EHF*—Extra High Frequency

3.1.31 *EMC*—Electromagnetic Compatibility

3.1.32 *EMD*—Engineering and Manufacturing Development

3.1.33 *EMI*—Electromagnetic Interference

3.1.34 *EMSS*—Enhanced Mobile Satellite Services

3.1.35 *EO*—Electro-optical

3.1.36 *FH-FSK*—Frequency Hopped-Frequency Shift Keying

3.1.37 *GCCS-M*—Global Command and Control System-Maritime

3.1.38 *GFP*—Generalized Framing Protocol

3.1.39 *GOA*—Generic Open Architecture

3.1.40 *HDR*—High Data Rate

3.1.41 *HF*—High Frequency

3.1.42 *HAIPE*—High Assurance IP Encryption

3.1.43 *ICD*—Interface Control Document

3.1.44 *IEEE*—Institute of Electrical and Electronic Engineers

3.1.45 *IER*—Information Exchange Rate

3.1.46 *IETF*—Internet Engineering Task Force

3.1.47 *INMARSAT*—International Maritime Satellite

3.1.48 *IOC*—Initial Operational Capability

3.1.49 *IR*—Infrared

3.1.50 *ISO*—International Standards Organization

3.1.51 *ISR*—Intelligence, Surveillance, and Reconnaissance

3.1.52 *JAUS*—Joint Architecture for Unmanned Systems

3.1.53 *JCPAT-E*—Joint C4I Program Assessment Tool-Empowered

3.1.54 *JHU APL*—Johns Hopkins University Applied Physics Laboratory

3.1.55 *JMCIS*—Joint Maritime Command Information Systems

3.1.56 *JMCOMS*—Joint Maritime Communications Systems

3.1.57 *JRP*—Joint Robotics Program

3.1.58 *JSIPS-N*—Joint Service Imagery Processing System-Navy

3.1.59 *JTIDS*—Joint Tactical Information Distribution System

3.1.60 *JTRS*—Joint Tactical Radio System

3.1.61 *LAN*—Local Area Network

3.1.62 *LLC*—Logical Link Control

3.1.63 *LMRS*—Long-Term Mine Reconnaissance System

3.1.64 *LOS*—Line of Sight

3.1.65 *LPD*—Low Probability of Detection

3.1.66 *LPI*—Low Probability of Intercept

3.1.67 *MAC*—Media Access Control

3.1.68 *MCM*—Mine Counter Measures

3.1.69 *MFSK*—M-ary Frequency Shift Keying

3.1.70 *MPA*—Maritime Patrol Aircraft

3.1.71 *MP-CDL*—Multi-Platform Common Data Link

3.1.72 *MRUUVS*—Mission Reconfigurable Unmanned Undersea Vehicle System

3.1.73 *MP-CDL*—Multi-Platform Common Data Link

3.1.74 *MUOS*—Mobile User Objective System

3.1.75 *NCO/W*—Network-Centric Operations and Warfare

3.1.76 *NIMA*—National Imaging and Mapping Authority

3.1.77 *NM*—Nautical Mile

3.1.78 *NSMA*—Neighbor-Sense Multiple Access

3.1.79 *ONR*—Office of Naval Research

3.1.80 *OPCON*—Operational control

3.1.81 *ORD*—Operational Requirements Document

3.1.82 *OSI*—Open System Interconnection

3.1.83 *OTH*—Over the Horizon

3.1.84 *OUSD*—Office of the Under Secretary of Defense

3.1.85 *PNT*—Positioning, Navigation, and Timing

3.1.86 *PPS*—Precise Positioning Service

3.1.87 *RF*—Radio Frequency

3.1.88 *RMS*—Remote Minehunting System

3.1.89 *RT*—Real Time

3.1.90 *RTS*—Request-to-Send

3.1.91 *SAE*—Society of Automotive Engineers

3.1.92 *SAHRV*—Semi-autonomous Hydrographic Reconnaissance Vehicle

3.1.93 *SATCOM*—Satellite Communications Equipment

3.1.94 *SCA* —Software Communications Architecture

3.1.95 *SDR*—Software Defined Radio

3.1.96 *SIGINT*—Signals Intelligence

3.1.97 *SNR*—Signal-to-Noise Ratio

3.1.98 *SRQ*—Selective Repeat Request

3.1.99 *SSC SD*—Space and Naval Warfare Systems Center, San Diego

3.1.100 *SPS*—Standard Positioning Service

3.1.101 *STANAG*—Standardization Agreement

3.1.102 *TACON*—Tactical Control

3.1.103 *TCDL*—Tactical Common Data Link

3.1.104 *TCP/IP*—Transmission Control Protocol/Internet Protocol

3.1.105 *TES-N*—Tactical Exploitation System-Navy

3.1.106 *TIC*—Technical Information Center

3.1.107 *TRANSEC*—Transmission Security

3.1.108 *UAV*—Unmanned Aerial Vehicle

3.1.109 *UHF*—Ultra-high Frequency

3.1.110 *UUV*—Unmanned Undersea Vehicle

3.1.111 *UWT*—Underwater Telephone

3.1.112 *WGS*—Wideband Gap Filler Satellite

3.1.113 *Wn W*—Wideband Networking Waveform

3.1.114 *WHOI*—Woods Hole Oceanographic Institution

3.1.115 *WiMAX*—Worldwide Interoperability for Microwave

4. Significance and Use

4.1 *Interoperability:*

4.1.1 Achieving interoperability is the goal of any standards initiative. In terms of UUV operations, it is critical for effective UUV communications. From a military perspective, interoperability is defined by the U.S. Joint Chiefs of Staff as the ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to use the services so "exchanged" to enable them to operate effectively together (**4**).[8] In the strictest sense, effective communications is the basis for this "exchange" of services and the achievement of interoperability. With the publication of this guide, ASTM Committee F41 has initiated an effort to establish UUV communication standards in the pursuit of promoting interoperability.

4.1.2 The communications requirements for general UUV operations encompass a wide range of potential modes dependent on mission requirements. Both the source and destination of the communication must be considered, as well as the content of the communications. It is important that the UUV be able to operate within the existing communications infrastructure. This includes leveraging communications across all modes in the traditional RF and network realms, as well as the emerging acoustic and optical domains. While the nuances of operating in the RF and network environment are generally more familiar to most users, acoustic- and optical-based node-to-node and networked communication modes between UUVs, host platforms, and other destinations also need to be better understood. This is of particular importance for a multi-mission UUV, which is envisioned to be deployed from a variety of platforms. The vehicle must be able to communicate with the host platform, as well as to transmit data on a path to the eventual users.

[8] The boldface numbers in parentheses refer to the list of references at the end of this standard.

4.2 *U.S. Navy UUV Master Plan*—The U.S. Navy UUV Master Plan[9] calls for the use of standardization and modularity in the design of UUVs. The ultimate goal is to provide for communications interoperability so that all UUVs can be a functional part of the Net-Centric battle-space. Although the aforementioned Master Plan describes four general classes of UUVs (man portable, light weight, heavy weight, and large displacement variants), the intended focus of this guide is to recommend basic communications standards compatible with the 21-in. diameter MRUUVS, a heavy weight vehicle.

4.3 *FORCEnet and DISR Compliance:*

4.3.1 *Global Information Grid (GIG) and FORCEnet* (**6**)—In an effort to ensure information superiority in the future Net-Centric battle-space, the U.S. Department of Defense has embarked on several transformational communications initiatives. Among these are the creation of the GIG as outlined in DoD Directive 8100.1, the GIG Bandwidth Expansion (GIG-BE), and the Transformational Communications Architecture (TCA). More specifically, the U.S. Navy has embraced FORCEnet as its component of the GIG and the way to operate within this Network-Centric Operations and Warfare (NCO/W) environment. Clearly, effective end-to-end communications are an integral part of FORCEnet. All UUVs conducting military missions that expect to operate in future battle-space environments must therefore embrace the tenets of the GIG, TCA, and FORCEnet. The U.S. Navy's Chief of Naval Operations Staff (OPNAV N71)[10,11] has drafted an initial list of Technical Standards (TV-1) devised for FORCEnet that specifically addresses the communications and networks service areas, among many others.

4.3.2 *DISR*—The DoD IT Standards Registry (DISR) is a Defense Information Systems Agency (DISA) generated compendium of mandated and emerging IT standards required for use in the acquisition and design of new U.S. military systems. Universal use of the DISR standards ensures and facilitates open systems and interoperability. Due to constantly changing technology and the standards upon which it is based, DISR is an evolving database that requires a controlled change process and continuous input from its various stakeholders.[12] The aforementioned FORCEnet TV-1 database includes many of these DISR standards, in addition to several others not contained in the DISR repository.

4.3.2.1 *MRUUVS Technical Standards Profile (TV-1)*—The current 21-in. MRUUVS Technical Standards Profile (TV-1) was created from the DISR online database. It is posted online at the SIPRNET site of the Joint C4I Program Assessment Tool-Empowered (JCPAT-E).[13] Since all the RF and network communication standards recommended in Section 5 have been extracted directly from the MRUUVS TV-1, and therefore, the DISR repository, the adoption of any of these relevant UUV communications standards by the ASTM Committee F41 UUV community ensures conformance with this unique U.S. military requirement levied by DISA. In addition, there is no conflict with the governing FORCEnet TV-1 either, ensuring conformance with the unique U.S. Navy requirement.

4.3.3 *Undersea FORCEnet Process Implementation Working Group* (**6**)—Valuable work done by the U.S. Navy's Undersea FORCEnet Process Implementation Working Group is leveraged in this ASTM Committee F41 UUV standards effort to codify UUV communication standards. Fig. 2 captures the communication domains that UUVs can expect to operate in with notional communication paths between various sources and destinations. In the case of UUV communications, expected UUV data and information exchanges are anticipated to take place between vehicles and their host platforms, as well as vehicles and other unmanned systems including UUVs, USVs, UAVs and myriad remote sensor and communication nodes. The Undersea FORCEnet working group (**6**) segregated the above-water, underwater-air interface, and underwater domains and identified the anticipated methods of communication in each. They were then able to address scalable architecture specifications by ascribing specific attributes for: standard Navy/Joint waveforms for RF BLOS and LOS (above-water), laser, acoustic, MF gateway buoys and submarine gateways (for the underwater-air interface); and direct acoustic communications and acoustic gateway buoys (for underwater). The resulting attributes include: data rates, ranges, speed, covertness, persistence, depth, latency, and network configuration. Access to these attributes is available through the Navy's Technical Information Center (TIC) for the 21-in. MRUUVS.[14]

4.4 *Security*—Information Security awareness and DoD directives mandating Communications Security (COMSEC) impact commercial and DoD UUV development at multiple system engineering levels because of the impact of information surety, requiring multiple analyses to identify potential weaknesses of systems, subsystems and components which manifest in Information Assurance (IA) planning, certification and accreditation. From a broad position, vulnerability analysis would categorize:

(1) System operations facilitating a vulnerability to unauthorized access.

(2) Host Platform or UUV System operating software vulnerability which may allow the unauthorized transfer of operating system code or recorded data.

(3) Exploitation of the Host Platform or UUV's internal data bus network allowing unauthorized monitoring of subsystems and access.

(4) CONOPS weakness affecting overall system security.

4.4.1 *Guidance*—Director of Central Intelligence Directive 6/3, Protecting Sensitive Compartmented Information within Information Systems (1), defines levels of protection and necessary steps in developing a system at the highest classification levels. DoD Directive 8100.2 is used for systems at

---

[9] The Navy Unmanned Undersea Vehicle (UUV) Master Plan, November 9, 2004.

[10] OPNAV N71 is available at http://cno-n6.hq.navy.mil/Director_Net-Centric_Warfare/OPNAV_N71/FORCEnet/.

[11] Accessed from http://cno-n6.hq.navy.mil/Director_Net-Centric_Warfare/OPNAV_N71/FORCEnet/.

[12] The latest DISR online baseline is version 06-1.1, dated March 1, 2006.

[13] Access to DoD IT Standards Registry (DISR) generated 21 in. MRUUVS Technical Standards Profile (TV-1) resident in the Joint C4I Program Assessment Tool-Empowered (JCPAT-E) online data base available through DISA.

[14] Access available through Naval Sea Systems Command (NAVSEA), PMS 403 Unmanned Undersea Vehicles.

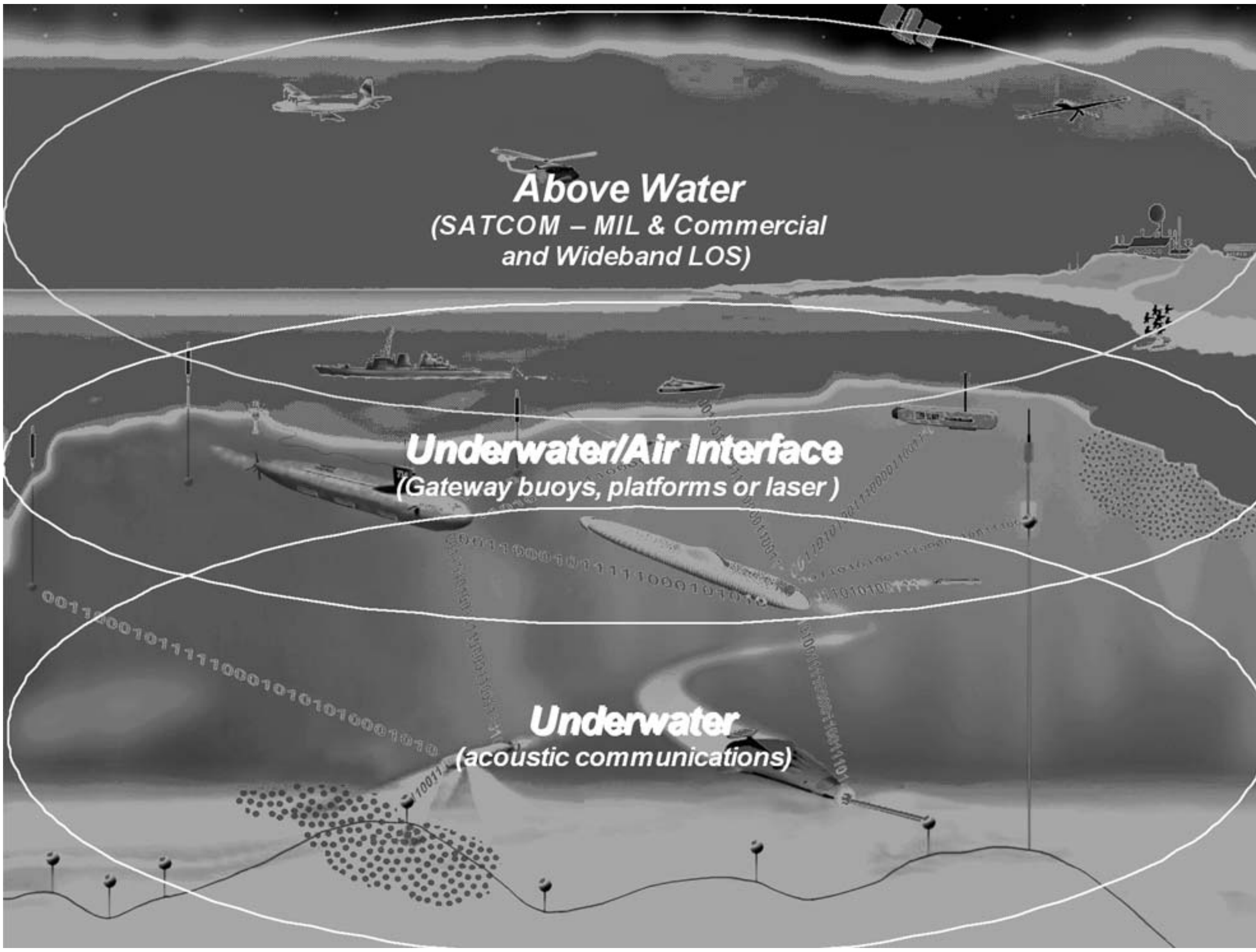

FIG. 2 UUV Communications Domains

Secret and below. Where mission drivers warrant, the UUV control architecture will need to satisfy information assurance requirements involving multilevel security classification information. The interface between the vehicle autonomy module and payload controller is the recommended interface at which UUV information assurance requirements can be accommodated through a combination of operating system, hardware, and middleware safeguards.

4.4.2 *Cryptography*—Cryptography is used to protect data while it is being communicated between two points or while it is stored in a medium vulnerable to physical theft and dissemination. It is considered as a supporting role in the overall information security awareness aspect but in itself not a validation policy measure. Cryptography compliments the overall security posture under Information Assurance planning, certification and accreditation, and compliancy to a system vulnerability assessment, measured in time cycles required to break the encryption code as a measure of effectiveness. Cryptology equipment serves as a part of an overall defense of unauthorized intrusion, denial, and assured data requirements. COMSEC provides protection to data by enciphering it at the transmitting point and deciphering it at the receiving point. File security provides protection to data by enciphering it when it is recorded on a storage medium and deciphering it when it is read back from the storage medium. A key must be available at the transmitter and receiver simultaneously during communication or a key must be maintained and accessible for the duration of the storage period. Cryptographic modules must meet FIPS 140-1 standard. The transmission security algorithm can be implemented in software, firmware, hardware, or in combination.

4.4.3 *DoD Encryption*—Data encryption is used by both the US Government and commercial industry. In communications environments, it is utilized to shield and deny unauthorized dissemination of the information sent via radio frequency, acoustic, optical, or wire methods. The DoD has mandated specific direction to use NSA approved communication security algorithms because a majority of DoD developed equipment is destined to support operational forces. At this time, there are few exceptions not to follow National Security Agency (NSA) guidelines. Only when the DoD material developer is not considering a production and deployment milestone or the item remains within the concept development cycle can one utilize sensitive but unclassified, non-assured channels for RF transmission security and data surety. Depending upon the overall system vulnerability or threat, commercial encryption is considered a viable option to achieve a level of data surety required. Only NSA approved or NSA authorized equipment supporting assured communications channels satisfies transmission security for systems classified at the secret level or above for US military systems.

4.4.4 *Considerations*—When a UUV RF system is actively transmitting or receiving a transmission it can become vulnerable to unauthorized intrusion. Information Assurance is the process used to analyze and mitigate the potential of intrusion through links such as the RF physical layer. Enabling data monitoring through frame analysis, network device monitoring, and providing software assurance between components, subsystems, and data exchanges, are good examples of methods used for quantifying the level of vulnerability imposed on the subject system. COMSEC is the DoD icon to deny system intrusion through the physical layer, the most likely point of intrusion. Designation of the security systems and protocols required are beyond the current scope of this guide. However, if the system is to be used to transmit information that is governed by security regulations, the security requirements must be addressed at the earliest point in the architecture design phase.

4.5 *Data*—A general discussion of data sharing in a DoD Net-Centric environment can be found in DoD Directive 8320.2. Specific UUV sensor data format standards are addressed in Guide F2595. The following discussion simply identifies certain data types and general data characteristics that may impact the transfer rates of UUV communication systems.

4.5.1 *Environmental Measurements*—Environmental measurements support an understanding of typical physical characteristics of the ocean environment such as salinity, temperature, ambient noise, and so forth. Many types of sensor systems are available to measure these characteristics and the majority of them utilize low data rate information transfer. The exception might be directional wave spectra, but here private industry has developed *in situ* signal processing supporting modest data transfer rates.

4.5.2 *Anti-submarine Warfare (ASW) Related Data*—On the assumption that cooperating groups of UUVs will be used for ASW purposes, the use of asynchronous, multi-access, low probability of detection (LPD) communications may be required. This is inherently a low data rate methodology. Information likely will include estimates of range, bearing, frequency, SNR (combined, perhaps 8 bytes of data), and UUV self-identifying information such as geoposition.

4.5.3 *Geopositions*—Transmission of geoposition requires that approximately 8 bytes of data be transmitted. As with the ASW problem, this may require low data rate, asynchronous, multi-access, LPD communications.

4.5.4 *Imagery*—Imagery, either optical or by sonar, should be supported by advanced image compression technology. As an example, a single 640 by 480 pixel image contains 3.1×10^5 bytes. With a reasonable 100:1 compression ratio, this reduces to approximately 3 Kbytes. When transmitted at a modest rate of 600 bps, this requires approximately 40 s to transmit. At a rate of 2560 bps, the time is reduced to less than 10 s.

4.5.5 *ISR Data*—Signals Intelligence (SIGINT) including Electronic Intelligence (ELINT) and Communications Intelligence (COMINT) is expected to be collected from U.S. Navy UUVs. Formats for this data are amplified in Guide F2595, the UUV Sensor Data Formats Standard.

TABLE 1 Notional UUV Communication Modes

Mode Type	Modality	Node Types				
		Submarine	Relay Buoy	Ship	Aircraft	Satellite
Optical	Laser	X	X		X	
Acoustic	Acoustic	X	X	X		
RF (LOS)	UHF LOS	X		X	X	
RF (BLOS)	UHF SATCOM	X		X		X
Local Area Network	Ethernet	X		X		

4.5.6 *Command and Control*—Command and control data will generally be transmitted to the vehicle. Peer to peer (vehicle to vehicle) command and control information exchanges are also anticipated. This will be low bandwidth and low-to-modest data rate. Typical command and control information will be at low data rates in the 100 to 1000-bps range.

4.5.7 *Data Gathering*—The primary data-gathering function requiring a communications link will be collecting GPS information. This requires a GPS antenna that may be integrated with other RF and SATCOM antenna equipment. There are also methods being developed which provide geopositioning via acoustic communications means that would not require the UUV to surface.

4.5.8 *Data Off Loading*—The communications modes and requirements for data off-loading are driven by three main factors: type of data, data destination, and timeliness of the data required (real-time versus post-mission download). The nature of a specific mission will dictate the required communications suite or protocol. Significant considerations are range, platform relative speed, channel conditions (for example, multi-path), and LPD requirements.

4.6 *Timing*—A crucial piece of information required for accurate data collection is timing. Latencies in electronic subsystems can greatly affect high sample rate systems such as attitude sensors and multibeam sonars and their correlation to other sensors. On many platforms, precision clocks updated using precision timing services or GPS, or both, are common. Distributed timing networks aboard some platforms can be used to insure accurate time is available to all sensors (facilitating exact correlation between data types collected). All data collected aboard UUVs should similarly have timing accuracy and precision standards that meet end user requirements for temporal resolution and accuracy. As a result, formats such as the American Inter Range Instrumentation Group (IRIG) Time Code Formats and Network Timing Protocol (NTP) should be followed where applicable to ensure timing accuracy and precision for collected sensor data is known to end users. IRIG accommodates accuracies down to 10 usec and NTP, using 64-bit stamps, has even greater potential. The National Institute of Standards and Technology, Time and Frequency Division, has readily available information on NTP and relevant standards.

5. Recommended UUV Communication Standards

NOTE 1—As discussed in 4.1, UUVs should be able to leverage communications across all modes: RF, network, acoustic, and optical. The choice of communication mode will depend upon the type and amount of data to be exchanged and the platforms or nodes involved. Table 1

TABLE 2 Layers of a Notional Undersea Acoustic Communication System

No.	Layer Name	Example/Detail
7	Application	UUV Control System
6	Presentation	Compact Control Language
	Encryption	Hardware Encryption Device
5	Session	Combat ID, Acknowledgement
4	Transport	TCP
3	Network	Table-driven routing
2	Data Link Layer	Framing and Error-Control
	Logical Link Control	Automatic Repeat Request
	Media Access Control	Access Arbitration
1	Physical	FH-FSK, PSK, M-FSK, etc.

identifies the basic UUV communication modalities, highlights the likely source or destination nodes, and provides notional means or conduits of communication. The subsequent discussion in this section amplifies the use of all five of these modes to varying degrees. Ultimately, for each communication mode, recommended standards are tabulated where established specifications exist.

5.1 *Introduction*—UUV communication standards can utilize the nomenclature of the telecommunications industry's Seven Layer Open System Interconnection (OSI) reference model shown in Table 2 (CCITT 84). This inaugural standards document begins to address the requirements associated with the OSI layers as these apply to UUV underwater communications using optical, RF, and acoustic modes, and it also touches on the challenges of future network considerations. Modern communication systems that employ networks are typically described using an approach similar to the OSI Reference Model[15] which was defined by the International Standards Organization (ISO). The layered approach is generally accepted as an appropriate means to describe a complete communications system. The model description described in Table 2 is used to frame the subsequent requirements summary.

5.1.1 *Physical Layer*—The physical layer includes the modulation and actual transmission. Examples of details addressed at the physical layer include selection of a carrier frequency and the type of encoding. While error-correction coding is not traditionally a part of the physical layer, error-prone RF and acoustic links commonly have this functionality built into the physical layer.

5.1.2 *Data Link Layer*—The data link layer has traditionally been associated with framing (breaking larger segments into frames) and error-control through use of a cyclic-redundancy check (CRC). RF ad-hoc networks often include two additional sub-layers. Logical Link Control (LLC) performs functions such as automatic repeat request (ARQ) to ask for additional transmissions of frames received with unrecoverable errors. The Media Access Control (MAC) layer provides arbitration in a multi user network where collisions are possible.

5.1.3 *Network Layer*—The network layer includes routing functions and potentially the maintenance of routing information.

5.1.4 *Transport Layer*—The transport layer connects user systems together, that is, it is host-to-host level.

[15] A summary of the OSI Reference Model is available at http://en.wikipedia.org/wiki/OSI_model.

5.1.5 *Session Layer*—The session layer addresses data such as Combat ID, and terse acknowledgements.

5.1.6 *Presentation Layer*—This layer is present in the OSI model, but not in the TCP/IP model. It is included here because it includes data representation and potentially data encryption as sub-layers or functions.

5.1.7 *Application Layer*—The software that is the end user of the data is the highest layer typically defined in the model. An example of this layer is a graphical user interface displaying UUV information.

5.2 *Optical Communications Standards*—There are several optical communications methods being developed. Fiber optic cable has been used on a number of systems, although generally on a "stove-piped" system with specific mission requirements. To date, the specificity of these requirements does not lend itself to a general purpose standard. If the high bandwidth provided by fiber optic systems proves to be a driving factor for future fleet systems, the development of a UUV system standard would be warranted. A functionally oriented discussion of laser providing quantitative values. Expansion of the scope of this laser section will be addressed in future revisions to this guide. Further optical communication discussion is beyond the scope of this guide.

5.2.1 *Laser Communications:*

5.2.1.1 UUVs should support wideband, on-demand FORCEnet laser communication connectivity with laser-equipped submarines, manned and unmanned undersea vehicles, and gateway communication buoys. The UUV shall support communications with laser-equipped airborne platforms, including Maritime Patrol Aircraft (MPA), manned helicopters, tactical Unmanned Air Vehicles (UAVs) or small "organic" submarine launched communication UAVs.

5.2.1.2 In a notional communications CONOPS between an aircraft and a laser equipped UUV, the aircraft must over-fly the UUV in a pre-selected rendezvous area, a subset of the full UUV operating area. The aircraft's laser system then scans the ocean surface with a short (coded) SPOTCAST message to initiate communications. The UUV receives and authenticates the call-up, transmits a coded "handshake" signal, then the aircraft initiates uplink spot tracking and duplex, high data rate information transfer. The aircraft will determine and transmit the location of the center of the communication cone to the UUV. The UUV should determine its position and transmit it to the aircraft.

5.2.1.3 To establish underwater communications between a Laser UUV and another underwater vehicle or buoy, the UUV must approach the pre-selected rendezvous location within approximately 150 m. The UUV's laser system then scans with a short (coded) call-up message to initiate communications. The other laser system receives and authenticates the call-up, transmits a coded "handshake" signal, and initiates duplex, high data rate information transfer.

5.2.1.4 A table of recommended optical communications standards for UUVs will be added to this section to capture future optical standards in subsequent revisions of this guide.

5.3 *Acoustic Communications Standards:*

5.3.1 *Introduction*—Since there is no pre-existing, community accepted, acoustic communications specifications from

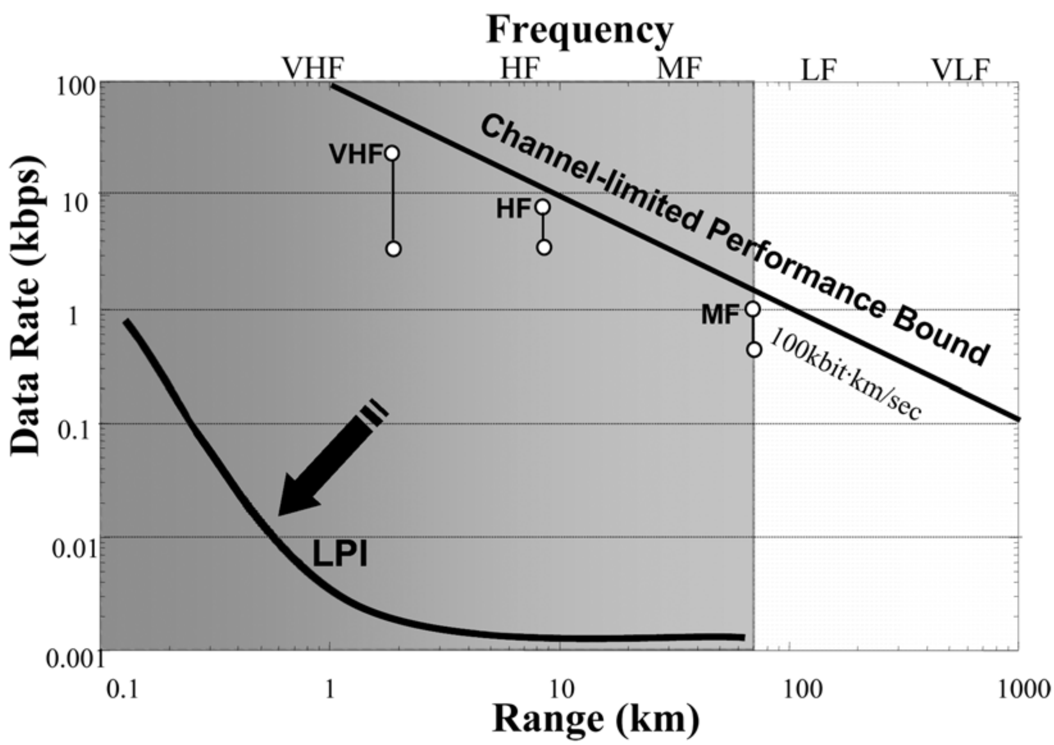

FIG. 3 ACOMMS Performance Regimes

which to draw for this guide, a descriptive approach to acoustic systems requirements is taken below. The objective of the standard is to describe the variety of approaches to acoustic communications and provide the user a means for selecting their own approach that supports their application's needs. In order to promote interoperability, the standard establishes a method to enable the user to engage another vehicle and establish a connection within the performance envelope of a given modulation method. The user can then either utilize a common communication protocol or even establish an asymmetric communication session. The asymmetric session would enable systems to possibly transmit in the receiver's native format. This assumes that the variety of proprietary formats are available to the user to transmit and maintains the proprietary nature of the receive algorithms.

5.3.2 The basis for this interoperability is the use of control and data packets where the physical layer format is common to all platforms. These packets will require the development of a standardized physical layer and link layer that allows all modems to query another. Once initial communications are established through the control packet, the user can determine the preferred communication method, i.e., symmetric or asymmetric links. The establishment of this common interface requires a method for describing the architecture behind a given acoustic communications interface. Therefore, it is generally agreed that acoustic communication standards can utilize the nomenclature of the telecommunications industry's Seven Layer Open System Interconnection (OSI) reference model shown in Table 2 (CCITT 84). This inaugural standards document begins to address the challenges and requirements of the OSI physical, data link, and network layers. Thus the standard will enable a method to accurately describe a communication protocol in a common nomenclature. Additional requirements addressing interfacing to external networks (i.e., RF or optics) in surface/near surface gateway applications will also be addressed.

5.3.2.1 *Constraints*—Unlike digital communications through RF means, underwater acoustic communications are hampered by the propagation speed (reduced by several orders of magnitude) and attenuation (ranging from 1-30 dB/km across the 10-100kHz) (3). The result of these environmental effects impacts the propagation delay (latency) and available bandwidth that can be utilized for the communication link. The bandwidth and data rate limitations of current acoustic systems can support the transfer of download host commands and off-load of mission data/vehicle status between the UUV and host platform. File sizes of up to 40–100 Kbytes have been transferred reliably in past experiments (3). Example systems typically have data rates of 100 to 2400 bps at up to 100 km range. Some developmental systems have demonstrated capabilities up to 50 kbps at distances of 5 km. As these systems are proven, additional standards will be developed to provide for higher rate communications and data transfer. The performance regime guidelines for the ACOMMS acoustic communication system are included in Fig. 3 and empirical results are documented (3). Another possible constraint includes on-board available power that could impact acoustic communications.

5.3.2.2 *Information Exchange Rates (IER)*—A general rule of thumb for acoustic communication IERs in today's state of the art is 10 Kbps-Kyd. Typical information exchange rates (IERs) for standard acoustic Command and Control (C2) data are captured in Table 3.

5.3.2.3 *Acoustic Networks*—There have been several U.S. Navy initiatives in the undersea network including AOSN,

TABLE 3 Undersea Acoustic Communication Information Exchange Rate Performance Regimes (see PEO C4I)

IER	C2 Product	Data Rate	Typical Range	Example C2 Products
1	Bellringer	1 bps	100 Kyd	Contact Report: Submarine Call Up
2	Text Messaging	100 bps	40 Kyd	Combat ID ASW Coordination
3	Track Data	500 bps	20 Kyd	Rainform Gold
4	Chat	2400 bps	4000 yd	Operation Note Chat (RF-like Chat)
5	Chat + Attachments	10 Kbps	1000 yd	ASW Gram Snippet: MIW Change Detect Snippet
6	Streaming Sensor Data	100 Kbps	100 yd	ISR sensor data, SOF Planning Update

Seaweb, and PLUSnet networks interconnect fixed and mobile nodes distributed across wide areas in the undersea environment (6,7). The unusual characteristics of the physical-layer medium constrain the design of the link and network layers. Link-layer methods including forward error correction, handshaking, and automatic repeat request provide reliability. Network-layer mechanisms such as distributed routing tables, neighbor-sense multiple access, packet serialization, and return receipts enhance quality of service.

(1) As depicted in Fig. 4, enables data telemetry and remote command and control for undersea sensor grids, autonomous instruments, and vehicles. Links to manned control centers include adaptations to submarine sonar systems and radio/acoustic communication gateway buoys with links to sky or shore.

(2) UUV undersea networking provides acoustic ranging, localization, and navigation functionality, thereby supporting the participation of mobile nodes including submarines and collaborative swarms of autonomous undersea vehicles (AUVs).

(3) Undersea acoustic network development demands attention to the underlying critical issues of adverse transmission channel (SNR and Multipath), asynchronous networking (propagation delays), battery-energy efficiency (life cycle or endurance), information throughput, and cost.

5.3.2.4 *Tactical Paging Undersea Systems*—Tactical paging undersea systems are comprised of untethered surface gateway buoys designed to operate on the surface with an RF link to a satellite or other surface or aerial platforms and have the capability to deploy an acoustic transducer(s) down to a fixed depth. The depth and distance at which the buoy's signals can be received depend on the buoy transducer and undersea platform (submarine, UUV, etc.) being within the same ocean thermalcline boundary layer with ranges that could be in excess of 50 km dependent on the specific mission. Thus, a tactical paging buoy might enable a strike commander to tactically alert/queue a submarine or UUV in low data rate regime (i.e., Table 3 minimum data rate of IER 1), either in a one- or two-way fashion acoustically. The return communication path could be acoustic or via other means (RF, optics).

5.3.3 *Acoustic Communications Architecture*—The communication architecture described by the OSI layers (Table 2) include existing open standards and description of functions supported through current initiatives.

5.3.3.1 *Baseline Physical Layer*—At the physical layer, an understanding of the transmission channel is gained through propagation theory and ocean testing. Tools include: numerical physics-based channel models, channel simulations, and portable telesonar testbeds for controlled sea measurements with high-fidelity signal transmission, reception, and data acquisition. Knowledge of the fundamental constraints on signaling translates into increasingly sophisticated digital communications techniques matched to the unique characteristics of the underwater channel. Variable amounts of forward-error correction allow for a balance between information throughput and bit-error rate. At the core of the physical layer is the type of modulation method (frequency-shift keying, phase-shift keying, and so forth).

(1) The WHOI FH-FSK Protocol—The Woods Hole Oceanographic Institution (WHOI) Frequency Hopped Frequency Shift Key (FH-FSK) Protocol (5) is demonstrated as a baseline standard for interoperability at the physical layer. FH-FSK describes a protocol for low-rate, multi-user communication in the underwater acoustic environment. The modulation physical layer allows for flexible hardware implementations for transmit and receive striving to be hardware independent (that is, allow linear/clipped power amplification implementations and a low computational load on receive) with respect to implementation. The principal characteristics of the protocol include:

(a) Data framing of variable length information segments with header information and CRC for error detection.

(b) Error-correction coding utilizing a rate 1/2 convolutional code.

(c) Symbol rates of: 160 symbols/s and 80 symbols/s.

(d) Three frequency regimes: 7.6 to 12 kHz, 12.5 to 17 kHz, and 23 to 30 kHz. (Note that the A-band overlaps the NATO STANAG 4413 Underwater Telephone (UWT) of 8–11 kHz. This can facilitate implementation on many Navy platforms and it must be implemented in order not to preclude UWT operation.)

(e) Low-coincidence frequency hopping patterns that provide code-division multiple-access and channel clearing time in multipath environments. The protocol addresses the physical modulation layer of the FSK, data layer frame structure, and error correction methods, and provides example protocols that have been used in the past.

(f) In addition, a Matlab toolbox has been written to demonstrate and document the system's implementation of the physical layer. The Matlab modules include the segmenter, the error-correction coding, and frequency-hop modulation layers.

(2) SEAWEB M-FSK Protocol—The M-ary Frequency Shift Keying (MFSK) has been demonstrated as an effective option for the physical layer and is used in Seaweb (7). Presently, the Seaweb physical layer is based exclusively on MFSK modulation of acoustic energy in any 5120 Hz band with center frequency between 10-30 kHz. Seaweb typically utilizes the 9–14 kHz band. A raw symbol rate of 2400 samples/s is reduced to an effective information bit-rate based on the degree of coding, redundancy, and channel tolerance desired. At present, 800 bits/s is the nominal information bit-rate, with provision for reduction to 300 bits/s if so required by the

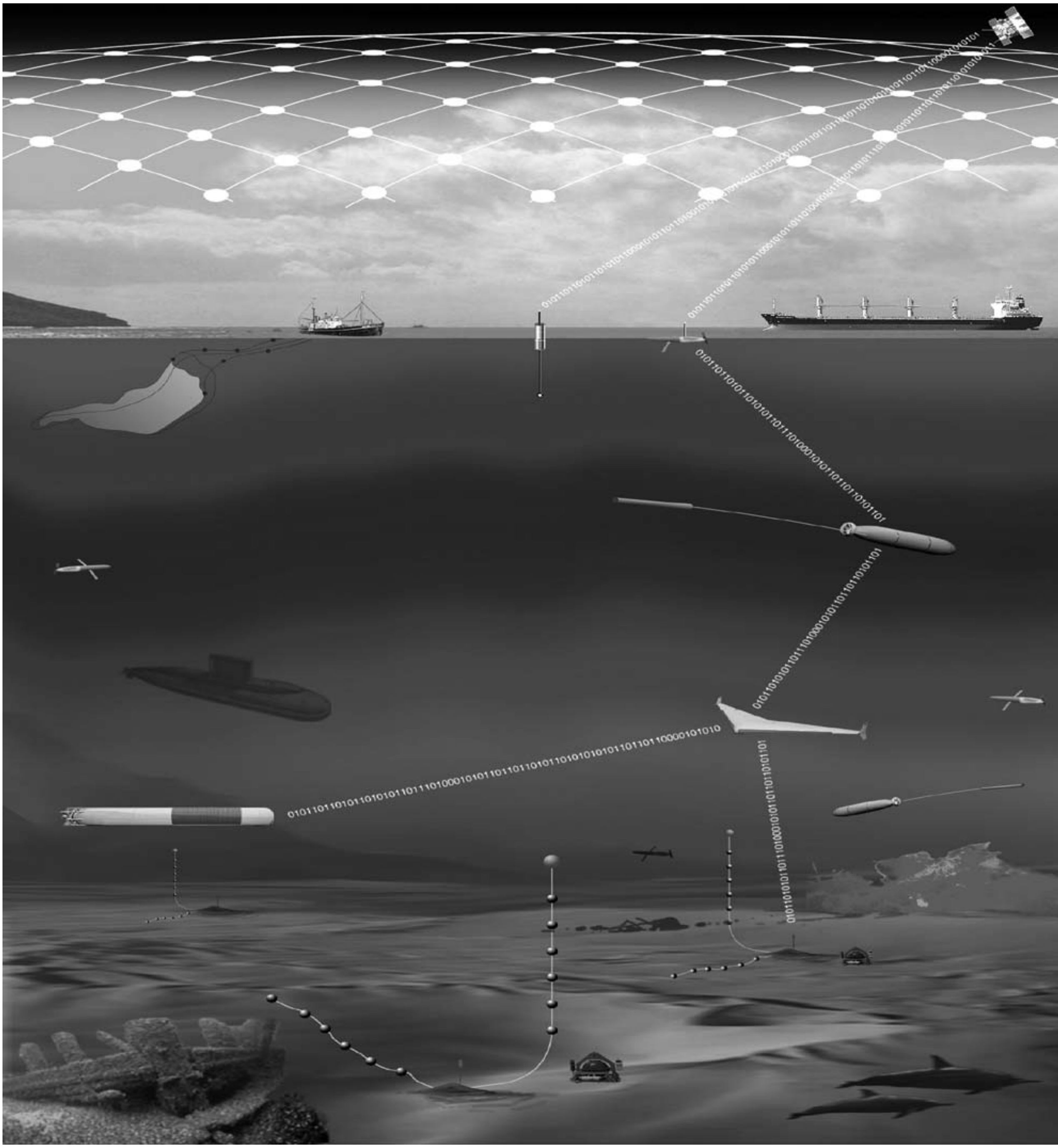

FIG. 4 Undersea Acoustic Networking

prevailing channel conditions. In addition, for increased interoperability, the Seaweb modems (Teledyne/Benthos Model 885) can support the low-data-rate frequency hopping technique, FH-FSK Protocol (5). Current FH-FSK implementation only supports physical layer point-to-point communications, modifications required to implement the other network layer functions following.

5.3.3.2 *Link Layer:*

(1) The link layer assures reliable communications between adjacent nodes. At the link layer, compact utility packets are well suited to meeting the constraints of slow propagation, half-duplex modems, limited bandwidth, and variable quality of service. The handshaking process automatically addresses and ranges the hailed node. Reliability is enhanced through the implementation of negative acknowledgements, range-dependent timers, retries, and automatic repeat requests. Example features of the Seaweb link layer are illustrated in Fig. 5 and Fig. 6.

(2) In Fig. 5, the Seaweb link-layer handshake protocol for data transfer involves Node A initiating a request-to-send

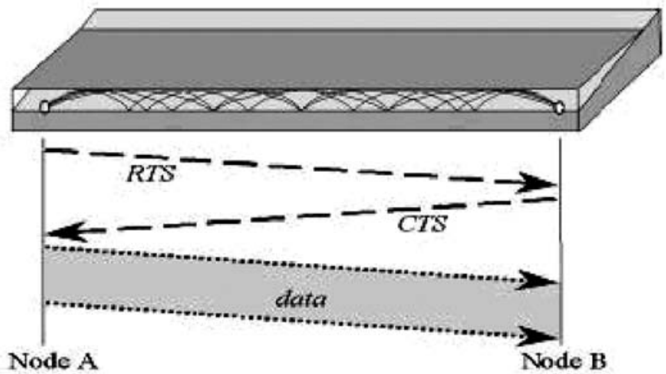

FIG. 5 Seaweb Link-Layer Handshake Protocol

(RTS) utility packet. So addressed, Node B awakens and demodulates the RTS. Node B responds to A with a clear-to-send (CTS) utility packet that fully specifies the modulation parameters for the data transfer. This protocol anticipates the spiral development of adaptive modulation wherein Node B uses the RTS as a channel probe and estimates the channel scattering function. With this knowledge, Node B then specifies optimal signaling parameters for the data packet as part of the CTS handshake.

(3) In Fig. 6, selective ARQ (SRQ) is a link-layer mechanism for reliable transport of large data files between neighboring nodes even when the physical layer suffers bit errors uncorrectable by forward error correction, as depicted in the example here. Purple arrows are Seaweb utility packets. Red arrows are data sub-packets.

(a) Utility Packet Functionality—The existing Seaweb Utility Packet described in Table 4 is a proposed standard that with some minor adaptation, could fit within the previously described FH-FSK standard of the physical layer. In the below implementation, the OSI model is violated in several ways as a matter of efficiency. Network layer addresses are contained in the layer 2 packet header, and ping/receipt packets are implemented in layer 2 utility packets even though they are essentially layer 3 concepts. The reason for this is efficiency—if replaced with a formal OSI model we would require an extra 14 byte network utility packet that would need to be embedded in the payload of the link layer DATA packet. In some important instances, these data would be preceded with RTS/CTS, further increasing the power and latency requirements. This approach demonstrates that adherence to formal models is not always in the best interests of efficiency, although there are other considerations that may argue for a different emphasis. The following utility packet description supports link layer as well as the network layer that follows.

5.3.3.3 *Network Layer*—The network layer handles end-to-end communications from source to destination node. At the network layer, routing and navigation are accomplished through embedded data structures distributed throughout the network. Seaweb neighbor tables maintain information about adjacent nodes within a 1-hop range. Seaweb routing tables dictate the neighbor nodes having networked connectivity with the intended destination node. Neighbor-Sense Multiple Access (NSMA) is a network layer function that passively monitors Seaweb traffic as a means of ascertaining the communications status of neighbor nodes. NSMA provides a means for avoiding unnecessary collisions by politely waiting for Seaweb dialogs to conclude before initiating new dialogs. At the command center, a Seaweb server maintains the neighbor table and routing table data structures, supports network configurability, manages network traffic at the gateways, and provides the graphical user interface for client workstations. Seaweb is an inherently long-latency communication system. Critical source-to-destination delivery can be confirmed through the use of return receipts implemented efficiently as Seaweb utility packets.

5.3.3.4 *Application Programming Interfaces (API)*—The OSI layered description of 5.1 does not define the interfaces, either content or syntax, that must exist for the entire stack to function. Typically these are defined by documents that describe specific services, such as socket services used for TCP/IP networking. Although this guide does not mandate any specific interfaces that may be used in layers 1 to 3 of an actual acoustic communications system, examples are listed. Layers 4 to 6 may utilize standard interfaces, but this depends on the components (services) that are used. In the case of the application layer the Compact Control Language (CCL) which includes data format descriptions suitable for operating UUVs over very low bandwidth links may be employed.

5.3.3.5 *Acoustic Communication Standards*—As acoustic communications standards are identified, a table will be inserted to list the standards for applicable layers, as well as general acoustic standards, in subsequent revisions of this guide.

5.4 *RF Communications Standards:*

5.4.1 *RF LOS Standards:*

5.4.1.1 RF LOS communications are very dependent upon the height of antenna. Transmit power is not generally the limiting factor for LOS communications; it is usually the LOS horizon. A UUV operating on the surface with an antenna mast 1.5 m (5 ft) above the surface would have a maximum LOS horizon of less than 5.49 km (3 nm) on a flat ocean.[16] That horizon is considerably less with even a moderate surface wave state. A navy surface combatant's antennas are typically 30.5 m (100 ft) above the surface, which gives an LOS horizon of 21.95 km (12 Nm). When talking to a surfaced UUV, whose antenna is so close the surface conditions, the effective communications range will probably be less the 18.28 km (10 Nm), quite possibly a lot less. Ranges are greatly improved when able to leverage other unmanned systems, including UAVs and USVs as communication relays.

5.4.1.2 Tactical Common Data Link (TCDL) and to a lesser extent due to size constraints, the directional Common Data Link (CDL), are also options for RF LOS communications. DoD has mandated that these systems transmit Intelligence, Surveillance and Reconnaissance (ISR) data.[17] Utilizing X-Band and Ku-Band, they could be made compatible with

[16] Line of Sight (LOS) Distance = 1.77 times the square root of antenna A + 1.77 times the square root of antenna B.

[17] DoD, "C3I Common Data Link Policy," June 19, 2001 and "C3I Tactical Data Link Policy," December 20, 2005.

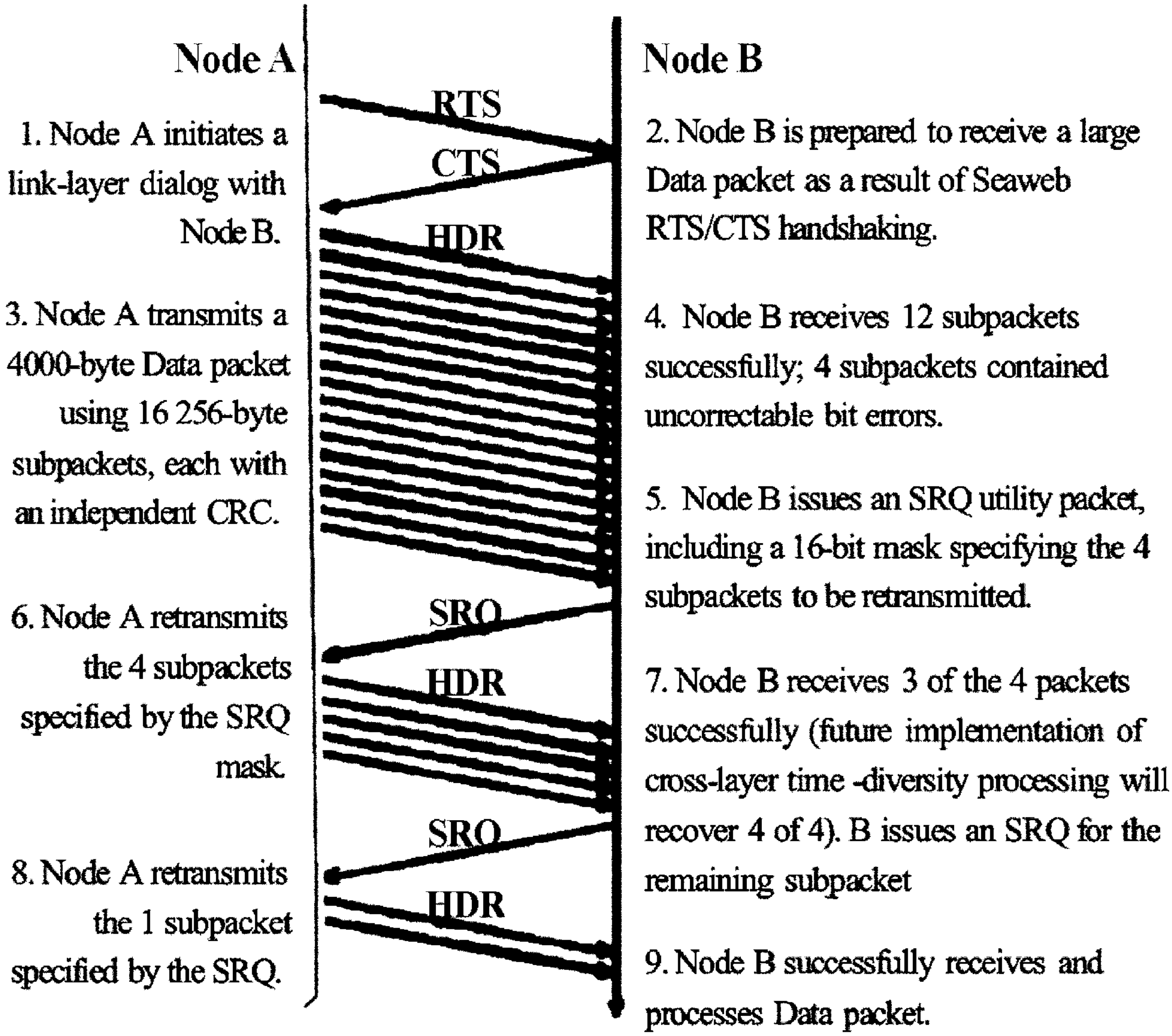

FIG. 6 Selective ARQ (SRQ)

UUV form, fit and function. Additionally, Ethernet over Generalized Framing Protocol (GFP) using the IEEE 802.3 specification; and as an emerging open standard waveform, Gigabit Ethernet over GFP as the single data framing convention for future Standard CDL are options. Finally, multiplatform CDL (MP-CDL) is an emerging waveform that may ultimately show promise for RF LOS UUV communications.

5.4.1.3 Consideration should also be given to utilizing Software Defined Radio (SDR) waveforms. As DoD transitions from its legacy communication systems, it is developing the Joint Tactical Radio System (JTRS). This future, single source of communications between 2 KHz and 2 GHz is designed to be SDR compliant. Additionally, DoD has directed that all future waveforms over 2 GHz must also be SDR compliant.

5.4.1.4 Table 6 captures a number of well established U.S. military and NATO standards for UHF LOS systems. For commercial and scientific applications, the inclusion of system specifications and protocols described in other RF LOS frequency bands is left open in this version of the guide. Future revisions to this guide may address such standards.

5.4.2 *RF BLOS Standards:*

5.4.2.1 For those operations in which UUVs are not supporting or supported by other platforms, command and control information must be exchanged with the element that currently has tactical control (TACON). Communication with these nodes BLOS must make use of a relay site, which could be a satellite, aircraft, UAV, or a ground or surface station.

5.4.2.2 The Global Positioning System (GPS) enables the ability of a GPS receiver to determine position in three dimensions and current time. GPS offers two types of service, the Standard Positioning Service (SPS) and the Precise Positioning Service (PPS). PPS is designed to be used by operational military users, and is generally reserved for U.S. military forces. It is cryptographically protected, and offers the most precise positioning information, as well as enhanced antijamming protections. SPS is widely available for general use,

TABLE 4 Existing Seaweb Utility Packet Functionality

NOTE 1—The utility packets are 9 byte messages containing several data fields, some of which are common to all packet types and others are specific to each type. The packet type dictates how the message is handled in the protocol. The data fields within the packet types give additional information.

Modem Addressing	Link-layer transmit and receive addresses are used to indicate the source and intended recipient of an acoustic packet. A receive address of 0 indicates the message is a broadcast packet and shall be handled by all recipients. The transmit and receive addresses-The fields are common to all types.
Network-Layer Addresses	The network-layer Source, Destination and Cell (last hop) addresses are used in specific utility packets that move data/commands through multiple hops in a network. These addresses indicate the final destination and the originating modem identifiers. The Cell address is used by a data originator to attempt communications to a destination address via a Cell address. This Cell address is useful when communicating with non-stationary destination nodes.
CRC Field	A forward error correction field using an 8 bit cyclic redundancy check field is used to for all packet types.
Link-layer Handshake	Preceding the transmission of data packets, a message handshake consisting of a Request-To-Send (RTS) and Clear-To-Send (CTS) is utilized. This handshake allows the transmitting modem to prepare the recipient modem to receive a message. The RTS message indicates the size of the pending packet, the number of RTS attempts that will be tried, the number of Selective Repeat Requests (SRQs) that should be attempted, and the Receipt Request indicator.
Packet Size and Modulation Indicator for Data Types	The Data Header utility type indicates the amount of data and modulation used transmitting the data packet. Both the packet size and modulation are 16 bit fields to allow for a wide range of packet sizes and modulation options.
Selective Repeat Request (SRQ)	A method of automatic repeat request (ARQ) is used called SRQ. This SRQ allows a receiving modem to a corrupted part of a received data packet to be retransmitted. This is useful when a small portion of a received data packet becomes corrupted. Instead of discarding what was received without errors, the receiving modem keeps those parts and only requests the affected segments of the data to be retransmitted.
Receipt Requests	The Receipt Request allows a modem sending data to request an acknowledgement of receipt from the destination modem. Two packets types, the RTS and Data Header, contain the Receipt Request flag which indicates to the destination modem that upon receiving a message a “Receipt” type packet shall be transmitted back to the source of the message. Furthermore, if a packet cannot be transmitted to the destination modem due to link failures, then the last modem holding the packet before the failure shall send a Receipt packet indicating failure to deliver the packet to its destination.
Node Ranging	A means of obtaining a 2-way range calculation between modems is available via the Ping and Echo message types. The Ping type contains a destination address thus indicating to the receiving modems which node is the intended recipient. The recipient of the Ping packet responds with an Echo packet after a constant response time. Once the Echo packet is received, a range in tenths of meters is calculated between nodes.
Broadcast Ranging	A special case of node ranging is the broadcast range. In this case, the broadcast address is used and all recipients of the broadcast Ping message shall respond with Echo packet type. A random time interval is selected by each recipient for transmission of the Echo response. The usage of time intervals on the response is the method used to prevent all nodes from transmitting at once and thereby acoustically corrupting the Echo response.
Brevity Packets	A special packet type noted the Brevity packet transmits packets with up to 64 bytes of data without using RTS-CTS handshake before the data. This packet type is acknowledged via a positive acknowledgement protocol. This positive acknowledgement is transmitted for every successfully received packet.
Sequence Numbers	8-bit sequence numbers are used in the RTS, Data, and Brevity packets to yield a chronological sequence to data transmissions. The modem originating the data creates a sequence number and increments that number for each new packet carrying application data.
Neighbor Sensing	A concept called “Neighbor Sense Multiple Access” is used by the modems when enabled to track the state of communications among neighbors. This allows a modem to hold off from sending data to a neighbor that is currently exchanging messages to other modems.

but does not offer the positioning accuracy or jamming protections of PPS. The Chairman, Joint Chiefs of Staff (CJCS) has declared that the GPS will be the primary radio navigation system source of positioning, navigation and timing (PNT) for DoD.[18]

5.4.2.3 Table 6 specifies the recommended RF BLOS standards for UUVs. In this initial guide, specifications and protocols for systems operating in the SHF and EHF frequency bands have been intentionally omitted from this table due to the current impracticality of antenna space requirements for UUVs.

5.5 *Network Standards*—These UUV Network standards focus primarily on layers 3 and 4 of the OSI model, allowing them to integrate with the RF and Optical standards which were focused on layers 1 and 2. For U.S. military applications (IAW FORCEnet and the GIG), all communications between the UUV and external entities must be IP enabled. The exception to this rule will probably be Acoustic Communication, due to its physical limitations. The use of this protocol will extend the network into the RF and Optical communication realms, as well as its traditional role in wire communications. A wired communications connection, either optical or electrical, will enable downloading large data files after a mission. Electrical Wired communications have not been included in this standard, but if incorporated it is assumed to be Ethernet compatible. Table 7 lists recommended standards that will enable IP network connections over the various communication mediums that the UUV will employ.

5.6 *COMSEC/TRANSEC Standards:*

5.6.1 Communications Security (COMSEC) and Transmission Security (TRANSEC) will be required to enable operations with particular military assets, to safeguard classified material, and to protect the communications signal from detection, interception, and jamming.

5.6.2 In terms of networks, DoD has developed High Assurance IP Encryption (HAIPE) specifications. The current HAIPE Interoperability Specification, version HAIPE IS 1.3.5 describes requirements for IPv4 Inline Network Encryption systems. HAIPE IS 3.0.1 addresses IPv4 and IPv6 traffic within the fixed, wireless, and SATCOM infrastructure. This version leverages bandwidth efficient IETF standard compliant encapsulation formats and shows increased alignment with commercial (IETF) standards.

[18] CJCSI 6130.01A, 1998 CJCS Master Positioning, Navigation, and Timing Plan.

TABLE 5 Recommended RF LOS Communication Standards for UUVs

Standard ID	Standard Title	Standard Description
Common Data Link Communications Standard	Waveform Specification for the Standard Common Data Link, Rev (F)	The foundation for CDL originated in 1979 as a collaborative effort between the United States Air Force/Assistant Secretary of Defense (USAF/ASD) and the National Security Agency (NSA) in support of the U-2 collection mission. Success onboard this and other platforms subsequently resulted in the Office of the ASD (OASD)/Command, Control, Communications, and Intelligence (C3I) issuing a December 1991 policy memorandum mandating CDL as the DoD interoperability standard for line-of-sight (LOS) communications of airborne ISR sensor data to surface-based (land/sea) processing terminals. A June 2001 policy update further extended the CDL standard to include air-to-air and beyond-line-of-sight (BLOS) relayed ISR applications. A December 2005 update reinforces prior directives.
MIL-STD-188-220B	Interoperability Standard for Digital Message Transfer Device (DMTD) Subsystems, 22 May 2002	Combat Net Radios (CNRs) are a family of radios that allow voice or data communications for mobile users. These radios provide a half-duplex, broadcast-transmission media with potentially high BERs. The method by which IP packets are encapsulated and transmitted is specified in MIL-STD-188-220C. With the exception of High Frequency (HF) networks, MIL-STD-188-220C is mandated as the standard communications net-access protocol for CNR networks. For IPv4, this standard is mandated. This standard is currently being updated to work in an IPv6 environment. This document promulgates the minimum essential technical parameters in the form of mandatory system standards and optional design objectives for interoperability and compatibility among DMTDs, and between DMTDs and applicable C4I systems. These Technical parameters are based on the data communications protocol standards specified herein to ensure interoperability. ***This standard will be deleted when JTRS WNW or equivalent waveform provides the same functionality.
MIL-STD-188-243	Tactical Single Channel (UHF) Radio Communications, 15 March 1989	The purpose of this document is to establish the minimum essential interoperability and performance requirements necessary for tactical single channel UHF radio communications equipment. This standard addresses ground-to-air, air-to-air, ship-to-shore and ship-to-ship tactical single channel UHF radio communications equipment. The requirements established by this document may be exceeded in order to satisfy specific operational requirements or to incorporate technological improvements, provided that interoperability is maintained. This standard is mandatory within the Department of Defense (DoD) in the design and development of new tactical single channel UHF radio communications equipment. Major modifications to existing tactical single channel UHF radio communications equipment shall comply with the requirements contained in this document. The term ″single channel″ refers to radios that are capable of transmitting, receiving or transmitting and receiving only one discrete RF envelope at a time per transmit or receive section. This document encompasses radios that may be tuned or selected to a preset channel, but is not applicable to multi-channel radios (a multichannel radio is defined as having two or more complete transmit or receive RF portions capable of operating on multiple frequencies simultaneously). *** This standard will be deleted when JTRS WNW or equivalent waveform provides the same functionality.
MIL-STD-6011C	Tactical Data Link (TDL) 11/1 1B Message Standard	This standard describes the approved standards to achieve compatibility and interoperability between command and control and communications systems and equipment of U.S. military forces employed in joint tactical operations. This publication is complemented by CJCSM 6120.01, Joint Multi-Tactical Data Link (TDL) Operating Procedures (JMTOP), which provides for planning and procedures to be used in the joint tactical environment using Link 11 as an augmentation to the overall TDL information exchange. Ref CJCSM 3115.01, the Joint Data Network (JDN) Operations document relies on a Multi-TDL Network (MTN), and Link 16 is the major component of that network. Its tactical data is shared on other JDN networks, as well as J-GCCS. DISA-GE332 is the Preparing Activity (PA) and Lead Standardization Activity (LSA), and it is published under the INST standardization area, ref DOD 4120.24-M.
MIL-STD-6016C:2 005	Tactical Data Link (TDL) 16 Message Standard, 28 March 2005	This standard describes the approved J-series messages and transmission/receipt protocols to achieve compatibility and interoperability between command and control and communications systems and equipment of U.S. military forces employed or intended to be employed in joint tactical operations. This publication is complemented by MIL-STD-6020 (Data Forwarding Between Tactical Data Links (TDL) for systems/platforms implementing a TDL gateway functionality, and CJCSM 6120.01, Joint Multi-TDL Operating Procedures (JMTOP), which provides for planning and common procedures to be used by forces in the joint tactical environment using Link-16 as the basis for information exchange.
MIL-STD-6020	Data Forwarding Between Tactical Data Link (TDL), 31 March 2004	This standard describes the approved message formats to achieve compatibility and interoperability between command and control and communications systems and equipment of U.S. military forces employed or intended to be employed in joint tactical operations. MIL-STD-6020 specifies the rules, messages translation requirements, and data element translations required to exchange data between tactical data systems. This publication is complemented by MIL-STD-6011, MIL-STD-6016, MIL-STD-6017, STANAG 5522, and CJCSM 6120.01, Joint Multi-Tactical Data Link (TDL) Operating Procedures (JMTOP), which provides for planning and procedures to be used in the joint tactical environment using Link-16 as the basis for information exchange. Ref CJCSM 3115.01, the Joint Data Network (JDN) Operations document relies on a Multi-TDL Network (MTN), as well as J-GCCS. DISA-GE332 is the Preparing Activity (PA) and Lead Standardization Activity (L SA), and it is published under the INST standardization area, ref DOD 4120.24-M.
SEIWG-005	Interface Specification, Radio Frequency Transmission Interfaces for DoD Physical Security Systems, 15 December 1981	The SEIWG-005 standard specifies the frequencies, data formats, and protocols for this class of sensors in order to relay the data back via communication links and data relays, to a common exploitation station.

TABLE 5 *Continued*

Standard ID	Standard Title	Standard Description
STANAG 4175	Technical Characteristics of the Multifunctional Information Distribution System (MIDS), Edition 3, 6 February 2001	MIDS is an advanced information distribution system that provides Communications, Navigation, and Identification (CNI) capabilities in an integrated form for application to air, land and maritime tactical operations. Various classes of MIDS terminal equipment will be provided with the characteristics of each class specified to satisfy the needs and capabilities of the various types of user systems, particularly with respect to size and weight. The principal purpose of the STANAG is to define the general technical characteristics required to: (1) achieve interoperability among MIDS terminals employed by the military services of the nations belonging to the North Atlantic Alliance; (2) ensure that the electromagnetic emissions from MIDS will not unduly interfere with other users of the frequency bands employed by MIDS; (3) establish minimum interface specifications in order to minimize problems associated with integrating MIDS terminals with appropriate operational CNI systems; (4) implement network management procedures of STANAG 5516 required for effective system operation; and (5) comply with other relevant NATO specifications, such as TEMPEST and data security. *** This standard will be deleted when JTRS WNW or equivalent waveform provides the same functionality.
STANAG 4586	Standard Interfaces of the Unmanned Control System (UCS) for NATO UAV Interoperability Ed. 2	STANAG 4586 proposes to use standards that will be NATO compliant and non-proprietary, and outlines a functional architectural standard for future UAV systems. The systems foundation will be based on the following three interfaces, which are standardized within the STANAG: a. The CUCS and the air vehicle (Data Link Interface, DLI), b. The CUCS and external C4I systems (Command and Control Interface, CCI), and c. The CUCS and the UAV system operator(s) (Human Control Interface, HCI).
STANAG 5522:200 1	Tactical Data Exchange-LINK 22, Edition 1, September 2001	Link 22 is a secure, ECM resistant NATO tactical data link conforming to interface standards which have been developed to fulfill the operational requirement to exchange tactical data between tactical data systems (including operators) and to exchange necessary network management data. Link 22 incorporates F-series message standards (formats and protocols), a Time Division Multiple Access (TDMA) architecture, specific communications media and protocols, and specific procedures. Link 22 equipped units are also known as NILE Units (NUs). NUs can exchange tactical data with units fitted with another tactical data link, for example, Link 16, via a Data Forwarding unit. STANAG 5522 provides a specification for Link 22, including message standards, operational procedures, data link protocols and network management procedures. STANAG 5522 is the governing document with respect to Link 22 network management, messages, protocols and procedures. ADatP-22 specifies the NATO Standard Operating Procedures for all organizations operating Link 22. (distributed as ADSIA(DLWG)-RCU-C-74-95)

5.6.3 Table 8 lists the current governing HAIPE specifications. This table will expand beyond HAIPE in future versions of this guide.

6. Issues

6.1 *General UUV Constraints*—UUVs offer significant constraints on the communication systems to be used. Current and planned systems such as the 21-in. MRUUVS are limited in payload space and power available. This in turn limits the range of communication systems available for use. In addition to the physical constraints, the environment also heavily influences the communications modes. RF transmission requires operation at the surface, with the attendant problems of getting sufficient height above the waves and aligning the antenna during UUV movements (vehicle pitch and roll) for a clear line of sight. RF transmission is also greatly affected by wave slap and splash, further limiting the potential range and utility. With regard to underwater acoustic communication capabilities, there are also environmental constraints affecting Sonars and their spectrum allocation. Further discussion of acoustic constraints is presented in 5.2.

6.2 *Optical Communication Issues*—The continued progress of developing optical systems' technologies, concepts of operations (CONOPS) and demonstrations should be monitored for standardization and eventual inclusion into this guide. As a frame of reference, DoD has stated that UUV Optical Communication Standards must be developed to meet the Submarine Laser Communications initial operational capability (IOC), currently scheduled for fiscal year 2010. The ONR/PMW 770 sponsored program SEADEEP represnts the U.S. Navy's current effort in this direction.

6.3 *Acoustic Communication Issues:*

6.3.1 *Interoperability*—A number of approaches are currently being investigated for underwater acoustic communications. With recent developments in acoustic communications proceeding without reference to widely accepted standards and spectrum allocation, it is critical to proceed on a path that will at the very least, ensure interoperability of these independent acoustic communications systems. Interoperability might be achieved by two means: *(1)* use one modem for all applications, or *(2)* define/document a modulation methodology that can be implemented across receivers which is not technology dependent (that is, relatively simple implementation). There will be cases which require technology to improve performance (that is, data rate and robustness), but the application of an interoperability standard is a divergent requirement made for a subset of these applications. Soliciting Interface Control Document (ICD) information on all vendors' implementations is also an option.

6.3.2 *Interference*—While the nuances of operating in the RF environment are generally more familiar to users, acoustic-based undersea networks (Seaweb) or node-to-node acoustic communications with host platforms, or both, also need to be better understood. This is of particular importance for a

TABLE 6 Recommended RF BLOS Communication Standards for UUVs

Standard ID	Standard Title	Standard Description
CCSDS401.0-B-6	Radio Frequency and Modulation Systems-Part 1: Earth Stations and Spacecraft, May 2000, Consultative Committee for Space Data Systems	This document recommends standards for radio frequency and modulation systems operated by the Consultative Committee for Space Data Systems (CCSDS) member and observer agencies. Recommendations contained in this document, Radio Frequency and Modulation Systems, Part 1, focus upon the standardization of RF and modulation systems for earthstations and spacecraft. Part 2, when completed, will comprise recommendations relating to datarelay satellite systems. Unlike the CCSDS Radio Frequency and Modulation Report, Reference (**2**), these recommendations describe the capabilities, policies, and procedures that the CCSDS agencies believe will be needed in future years. By proposing specific characteristics and attributes for subjects in these categories, the CCSDS hopes that the ensuing designs will be sufficiently similar so as to permit cross support of one agency's spacecraft by another agency's network. These recommendations are complementary to the information contained in the RF and Modulation Report. To obtain a complete understanding of an agency's tracking facilities, readers should consult both documents. The Report describes the RF and modulation characteristics of spacecraft tracking systems that the CCSDS member and observer agencies are planning for the mid-1990 time period. It comprises a multiplicity of tables summarizing the technical characteristics of those systems. These recommendations do not provide specific designs. Rather they describe certain capabilities and provide technical characteristics in sufficient detail so that an agency may design compatible equipment. Guidelines are also provided for the use of agencies' RF and modulation systems, as well as their use of the RF spectrum. Because an ability to provide cross support implies some standardization of design and operations, certain procedural recommendations have been included to assist in these areas, recommendations are assigned to one of three sections depending upon whether their primary focus is technical, policy, or procedural in nature. These recommendations are intended to promote an orderly transition to RF and modulation systems that are internationally compatible. The CCSDS believes that this course will not only assure better engineering practices but, also, that it will facilitate international cross support agreements.
IESS-309 Rev. 7	QPSK/FDMA Performance Characteristics for INTELSAT Business Services, 10 February 2000	A description of this standard was not readily available. This block will be updated in future versions of this guide.
IESS-310 Rev. 2	Performance Characteristics for Intermediate Data Rate Digital Carriers using rate 2/3TCM/8PSK and Reed-Solomon Outer Coding (TCM/IDR), 10 February 2000	A description of this standard was not readily available. This block will be updated in future versions of this guide.
ISO 12171 (CCSDS201.0-B-2)	Space Data and Information Transfer System-Telecommand, Channel Service, Architectural Specification, 1998	The purpose of this document is to establish a recommendation for source-coding data-compression algorithm applied to digital data and to specify how these compressed data shall be inserted into source packets for retrieval and decoding. Source coding for data compression is a method utilized in data systems to reduce the volume of digital data to achieve benefits in are as including, but not limited to, reduction of transmission channel bandwidth; reduction of the buffering and storage requirement; education of data-transmission time at a given rate.
ISO 12173 (CCSDS202.1-B-1)	Space Data and Information Transfer System-Telecommand, Command Operation Procedures, 1998	This recommendation contains the detailed specification of the logic required to carry out Command Operation Procedure-1 (COP-1) of the Transfer Layer. The recommendation for Telecommand, Part 2: Data Routing Service, contains the standard data structures and data communication procedures used by the intermediate telecommand system layers (the Transfer and Segmentation Layers). In particular, it contains a brief description of the Command Operation Procedure (COP) within the Transfer Layer. This recommendation contains the detailed definition of COP-1 in the form of state tables, along with definitions of the terms used. It is assumed that the reader of this document is familiar with the data structures and terminology of Part 2. In case of conflict between Part 2 and this recommendation, this recommendation will take precedence.
ISO 12174 (CCSDS203.0-B-1)	Space Data and Information Transfer System-Telecommand, Data Management Service, Architectural Specification, 1998	The purpose of this document is to establish a common recommendation which defines the systems architecture of a spacecraft telecommand "Data Management Service." The intent of this architecture is to provide a common framework within which the Agencies participating in the Consultative Committee for Space Data Systems (CCSDS) may implement compatible future spacecraft telecommanding systems. This recommendation primarily addresses the data unit formats and functions which are implemented within the Application Process layer, the System Management layer and the Packetization layer of the CCSDS telecommand Data Management Service. Recognizing that much future work remains to be done relative to these top layers, their specification has been deliberately minimized by the CCSDS. In particular, the detailed operational protocols which operate across these layers, and the flow of control information required to initialize the layers and direct the transfer of data between them, are not presently addressed within this document: these remain items for potential extension of this recommendation.
MIL-STD-188-181C	Interoperability Standard for Access to 5-kHz and 25-kHz UHF Satellite Communications Channels, 30 January 2004	This standard establishes mandatory requirements applicable to satellite communications (SATCOM) terminals required to operate over single-access 5-kHz and 25-kHz ultra high frequency (UHF) SATCOM channels. In addition, this standard establishes mandatory requirements, including modulation, coding, and preamble patterns to be used by UHF SATCOM terminals when operating over multiple-access 5 and 25-kHz channels.
MIL-STD-188-182B	Interoperability and Performance Standard for UHF SATCOM DAMA Orderwire Messages and Protocols	This standard is mandatory within the DoD and will be invoked by equipment specifications for all future terminals required to communicate on multiple-access 5 and 25-kHz UHF SATCOM channels on a demand-assigned (DA) basis. Existing terminals undergoing major modification, and terminals under development, will conform to this standard if access to multiple-access and single-access channels over UHF SATCOM channels using demand-assigned mode is required.

TABLE 6 *Continued*

Standard ID	Standard Title	Standard Description
MIL-STD-188-183B:2 004	Interoperability Standard for Multiple-Access 5-kHz and 25-kHz UHF Satellite Communications Channels, 30 January 2004	This standard establishes mandatory requirements applicable to SATCOM terminals required to access pre-assigned (PA) or demand-assigned (DA) user-to-user communications (UCOM) services that operate on either 5-kHz or 25-kHz UHF SATCOM channels. The TDMA frame structure, timing requirements, and protocols for accessing the UCOM and overhead services are defined and represent the minimum requirements that must be implemented. *** Will be replaced by MIL-STD-188-183B.
MIL-STD-188-184(1)	Interoperability and Performance Standard for the Data Control Waveform, 20 August 1993, with Notice of Change 1, 9 September 1998	This standard defines an interoperable waveform standard for data controllers required to operate over single-access, 5 and 25-kHz ultra high frequency (UHF) satellite communications (SATCOM) channels. These channels are known as dedicated channels, per MIL-STD-188-181. Data controllers use data compression, adaptive error-correction, and packet communications techniques to reliably control the flow of data over noisy communications channels at high-throughput rates. The requirements specified herein represent the minimum set required for interoperability and performance. Such requirements may be exceeded by equipment developers to satisfy specific Service requirements, provided interoperability and performance are maintained. *** Will be replaced by MIL-STD-188-184A.
MIL-STD-188-185(2)	DoD Interface Standard, Interoperability of UHF MILSATCOM DAMA Control System, 29 May 1996, with Notice of Change 1, 1 December 1997; and Notice of Change 2, 9 September 1998	This standard establishes mandatory interface requirements for military satellite communications (MILSATCOM) equipment that control access to demand assigned multiple access (DAMA) and demand assigned single access (DASA) ultra high frequency (UHF) 5-kHz and 25 kHz MILSATCOM channels. The requirements specified herein represent the minimum set required for interoperability.
IS-GPS-200D	NAVSTAR GPS Space Segment/ Navigation User Interfaces, 7 December 2004.	This ICD defines the requirements related to the interface between the Space Segment of the Global Positioning Systems (GPS) and the Navigation User Segment (US) of the GPS. The CJCS (CJCSI 6130.01A, 1998 CJCS Master Positioning, Navigation, and Timing Plan) has declared that the GPS will be the primary radio navigation system source of positioning, navigation and timing (PNT) for DoD. GPS is a space-based, worldwide, precise positioning, velocity, and timing system. It provides an unlimited number of suitably equipped passive users with a force-enhancing, common-grid, all-weather, continuous, three-dimensional PNT capability. The NAVSTAR GPS provides two levels of service a Standard Positioning Service (SPS) and a Precise Positioning Service (PPS).
ICD-GPS-227	Navstar GPS Selective Availability and Anti-Spoofing (SA/A-S) Host Application Equipment (HAE) Design Requirements with the Selective Availability Anti-Spoofing Module (SAASM), 26 November 2003.	This ICD defines the requirements related to the GPS data that is outputted from the Key Data Processor (KDP) of the SAASM. The interface defined by ICD-GPS-227 is actually three in total: a) the interface between the KDP and the SAASM Application Micro Processor, b) the interface between the KDP and the PPS HAE, and c) the interface between the KDP and the Host.
STANAG 4294	NAVSTAR Global Positioning System (GPS)-System Characteristics plus Summary of Performance Requirements (Part 2, Edition 2, June 1995), Part 1, Edition 2, December 1997	This document defines the system characteristics of the NAVSTAR GPS essential to the design of receivers and the use of the system by all military services.

multi-mission UUV, which is envisioned to be deployed from a variety of platforms. The vehicle must be able to communicate with the host platform as well as to send data on the path to the eventual user. It must be compatible with and not interfere with ambient noise sources or signals generated by other acoustic systems resident on the host platform.

6.3.2.1 *Acoustic Frequency and Time Interference Management*—Managing UUV acoustic systems operations of several onboard systems in both frequency and time are important for mission success. Appropriate frequency separation and ping timing (sequencing) from a synchronized controller are needed to minimize interference. UUV acoustic systems might include a Doppler Velocity Log (DVL), range tracking systems, forward and side looking sonar systems, acoustic communications system, and an acoustic command system. Some acoustic command systems utilize highly interference resistant coding schemes to help eliminate false commands. Ping management might require acoustic systems to utilize, where possible, shorter pulse lengths with greater inter-ping intervals. The problem is made more arduous in scenarios of multiple UUVs operating in close proximity to each other.

6.3.3 *Common Software Interface/Application Program Interface (API)*—The API for the various systems should strive for common interface language to become host independent. Past examples of embedded modem implementations have used the Hayes serial/UDP commands or NEMA serial/UDP commands. The API should define the middle ware to support a given command set to be determined. API/System issues to be resolved impact the physical layer utility/supervisory packet implementations (size, synchronization, etc.).

6.3.4 *Deficiencies in this Guide*—Admittedly, additional work is required to more fully explain the rationale and mechanisms involved with the approach taken in this guide. Cross-layer implications complicate a more straightforward approach. Among the topics not adequately addressed here, but expected in future versions of this guide, are:

6.3.4.1 *Physical Layer*—Performance envelopes.

6.3.4.2 *Media Access Control Layer*—Time and frequency division.

6.3.4.3 *Link Layer*—Asymmetric links, neighbor tables, routing tables, cellular addressing, and utility packet implementation.

6.3.4.4 *Presentation Layer*—Compact control language.

TABLE 7 Recommended Network Standards for UUVs

Standard ID	Standard Title	Standard Description
IEEE 802.3-2005	IEEE Standard for Information technology— Telecommunications and information exchange between systems— Local and metropolitan area networks— Specific requirements Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications	Ethernet local area network operation is specified for selected speeds of operation from 1 Mb/s to 10 Gb/s using a common media access control (MAC) specification, management information base (MIB), and capability for Link Aggregation of multiple physical links into a single logical link. The Carrier Sense Multiple Access with Collision Detection (CSMA/CD) MAC protocol specifies shared medium (half duplex) operation, as well as full duplex operation. Speed specific Media Independent Interfaces (MIIs) allow use of selected physical layer (PHY) interfaces for operation over coaxial, twisted pair or fiber optic cables. System considerations for multisegment shared access networks describe the use of Repeaters which are defined for operational speeds up to 1000 Mb/s. Local Area Network (LAN) operation is supported at all speeds. Other specified capabilities include: various PHY types for access networks, PHYs suitable for metropolitan area network applications, and the provision of power over selected twisted pair PHY types.
IETF Standard 5	Internet Protocol, September 1981. With RFCs 791 / 950 / 919 / 922 / 792 / 1112	IP is a basic connectionless datagram service. All protocols within the IP suite use the IP datagram as the basic data transport mechanism. Currently, IP Version 4 (IPv4) is the mandated internetworking protocol for networks carrying operations traffic within DoD. IPv6 is the next-generation, network-layer protocol of the Internet and DoD. IPv6 has been designed to provide better internetworking capabilities than are currently available within IPv4. IPv6 includes supports for the following: expanded addressing and routing capabilities, authentication and privacy, auto-configuration, and traffic-class and flow-label fields to facilitate implementation of quality of service capabilities. All implementations of IPv4 must pass the 8-bit Type-of-Service (TOS) byte transparently up and down through the transport layer as defined in IETF Standard 3, Requirements for Internet Hosts, Communication Layers, October 1989. For IPv4, this standard is mandated.
IETF Standard 41/RFC 894	Transmission of IP Datagrams Over Ethernet Networks, April 1984	This RFC specifies a standard method of encapsulating Internet Protocol (IP) datagrams on an Ethernet. This RFC specifies a standard protocol for the ARP A-Internet community. This memo applies to the Ethernet (10-megabit/s, 48-bit addresses). The procedure for trans mission of IP datagrams on the Experimental Ethernet (3-megabit/s, 8-bit addresses) is described in RFC-895, "A Standard for the Transmission of IP Datagrams over Experimental Ethernet Networks."
IETF Standard 6/RFC 768	User Datagram Protocol, 28 August 1980	This User Datagram Protocol (UDP) is defined to make available a datagram mode of packet-switched computer communication in the environment of an interconnected set of computer networks. This protocol assumes that the Internet Protocol (IP) is used as the underlying protocol. This protocol provides a procedure for application programs to send messages to other programs with a minimum of protocol mechanism. The protocol is transaction oriented, and delivery and duplicate protection are not guaranteed. Applications requiring ordered reliable delivery of streams of data should use the Transmission Control Protocol (TCP).
IETF Standard 7/RFC 793	Transmission Control Protocol, September 1981	The Transmission Control Protocol (TCP) is intended for use as a highly reliable host-to-host protocol between hosts in packet-switched computer communication networks, and in interconnected systems of such networks. This document describes the functions to be performed by the TCP, the program that implements it, and its interface to programs or users that require its services.
IETF RFC 2460	Internet Protocol, Version 6 (Ipv6) Specification, December 1998	IP version 6 (IPv6) is a new version of the Internet Protocol, designed as the successor to IP version 4 (IPv4) [RFC-791]. The changes from IPv4 to IPv6 fall primarily into the following categories: (1) Expanded Addressing Capabilities. IPv6 increases the IP address size from 32 bits to 128 bits, to support more levels of addressing hierarchy, a much greater number of addressable nodes, and simpler auto-configuration of addresses. The scalability of multicast routing is improved by adding a "scope" field to multicast addresses. And a new type of address called an "anycast address" is defined, used to send a packet to any one of a group of nodes. (2) Header Format Simplification. Some IPv4 header fields have been dropped or made optional, to reduce the common-case processing cost of packet handling and to limit the bandwidth cost of the IPv6 header. (3) Improved Support for Extensions and Options. Changes in the way IP header options are encoded allows for more efficient forwarding, less stringent limits on the length of options, and greater flexibility for introducing new options in the future. (4) Flow Labeling Capability. A new capability is added to enable the labeling of packets belonging to particular traffic "flows" for which the sender requests special handling, such as non-default quality of service or "real-time" service. (5) Authentication and Privacy Capabilities. Extensions to support authentication, data integrity, and (optional) data confidentiality are specified for IPv6. This document specifies the basic IPv6 header and the initially-defined IPv6 extension headers and options. It also discusses packet size issues, the semantics of flow labels and traffic classes, and the effects of IPv6 on upper-layer protocols. The format and semantics of IPv6 addresses are specified separately in [ADDRARCH]. The IPv6 version of ICMP, which all IPv6 implementations are required to include, is specified in [ICMPv6].
IETF RFC 2464	Transmission of Ipv6 Packet Over Ethernet Networks, December 1998	This document specifies the frame format for transmission of IPv6 packets and the method of forming IPv6 link-local addresses and statelessly auto-configured addresses on Ethernet networks. It also specifies the content of the Source/Target Link-layer address option used in Router Solicitation, Router Advertisement, Neighbor Solicitation, Neighbor Advertisement and Redirect messages when those messages are transmitted on an Ethernet. This document replaces RFC 1972, "A Method for the Transmission of IPv6 Packets over Ethernet Networks," which will become historic.

TABLE 8 Recommended COMSEC / TRANSEC Standards for UUVs

Standard ID	Standard Title	Standard Description
HAIPE IS 1.3.5	High Assurance IP Encryption Interoperability Specification	An open description of this INE standard was not readily available. This block will be updated in future versions of this document.
HAIPE IS 3.0.1	High Assurance IP Encryption Interoperability Specification	An open description of this standard was not readily available. This block will be updated in future versions of this document.
TBD	TBD	TBD

6.3.4.5 Other topics that would benefit from further discussion include: spectrum utilization, point-to-point applications, and adaptive modulation. An analysis of assumptions may also be warranted. For instance, the assumption that an 80 bit/s physical layer can support the minimal vehicle information for acoustic communication data representative of typical UUV missions requires continued validation. Although it has its shortcomings, this guide's discussion of acoustic communications does provide a framework for defining a complete repertoire of physical layer options that can be part of what is ultimately required: an adaptive modulation standard.

6.4 *RF Communication Issues:*

6.4.1 *General*—As described in 6.1, UUV RF communications must contend with significant environmental factors and physical limitations (space, size, and power). The primary focus of physical constraints includes RF antenna issues such as:

6.4.1.1 Antenna height and resultant instability which represent technical and engineering challenges.

6.4.1.2 Space in that smaller UUVs make disadvantaged ground plane and transmission platforms. Potential corrections such as electronic (antenna gain shaping) and physical (platform stabilization) might be used to facilitate an RF solution.

6.4.1.3 Radar Cross Section (RCS) where minimal is desired.

6.4.1.4 Similar to the discussion of acoustic interference, UUVs can suffer significant communication repercussions while operating in the RF realm. For a multi-mission UUV, deployed from a variety of platforms, the vehicle must be able to communicate with the host platform and to send data on paths to the eventual users. UUV RF communication systems must effectively transmit and receive without interference from other systems resident on host platforms, particularly in regard to electromagnetic interference and compatibility (EMI and EMC).

6.4.1.5 Co-site EMI and EMC issues are significant onboard U.S. Navy ships and submarines because of the myriad organic communication and radar equipment resident on board. Integrating completely new communication systems into the shipboard environment requires careful planning and often custom-designed RF filters to effectively eliminate interference between any new and existing equipment. While further discussion of EMI and EMC studies are beyond the scope of this guide, rigorous testing should be performed before planned UUV RF equipment installation.

6.4.2 *RF LOS Communication Constraints and Issues:*

6.4.2.1 *Ultra-High Frequency (UHF)*—The infrastructure to support narrow band UHF circuits, both LOS and SATCOM, is the most prevalent within the joint community. The biggest drawback to UHF is that it is narrow band. Maximum data rates are 64 kbps, and realistic link budgets usually limit operations to fewer than 30 kbps, frequently to 1.2 Kbps or even less. As previously mentioned, the advantage of UHF is the large existing infrastructure within DoD.

6.4.2.2 *Common Data Link (CDL)*—With the CDL specification mandated as the DoD standard for airborne ISR platforms,[19] the UUV community should plan to leverage this developing infrastructure where feasible on a volume and weight basis. It can provide wideband connectivity to C2 systems and support sensor data download and delivery to exploitation systems. However, in some cases, there are known interoperability deficiencies that still exist when using equipment built by different manufacturers.

6.4.2.3 *Link-16/ Joint Tactical Information Distribution System (JTIDS)*—This is a tactical networking system used to connect strike and support aircraft. It provides bandwidth in the 15 to 243-Kbps range depending on assigned priority and current usage. Limited sensor product can be moved in the system, for example, thumbnail imagery of a target area. The ability to communicate with this system would provide UUVs the capability to support strike operation s directly and use available air assets to pass priority sensor products.

6.4.3 *BLOS RF Communication Constraints and Issues:*

6.4.3.1 *Ku Band Commercial*—Since existing Ku band satellite communications are commercially owned and operated, the capacity is directed at the major landmasses where the customers are located. There is no current or planned maritime coverage. There is some capability in the littorals, although it does not extend very far out to sea. As technology improves, the sharpness of the antenna beam cutoff improves, further degrading the already limited littoral capability.

6.4.3.2 *UHF Satellite Communications (SATCOM):*

(1) Within the military UHF spectrum, there are a number of existing and follow-on satellites that provide transponder (RF relay) services. Some of these channels are 5 kHz; most are 25 kHz. It is possible to have a transponder assigned to a mission; however, with the high demand for UHF circuits worldwide, this is unlikely. Both the 5 and 25-kHz channels make use of Demand Assigned Multiple Access (DAMA), a method of sharing the available bandwidth among multiple users. This allows users to use available bandwidth and guarantees a minimum bandwidth to each user.

(2) UHF SATCOM provides military users with a long-haul data and voice communications capability. The demand for this service greatly exceeds the capacity of the system in its current single network per satellite channel mode. In an effort to provide the UHF capability to all users, the Chairman, Joint

[19] DoD, "C3I Common Data Link Policy," June 19, 2001 and "C3I Tactical Data Link Policy," December 20, 2005.

Chiefs of Staff Instruction CJCSI 6251.01 has directed that all terminals operating over non-processed UHF SATCOM transponders will be capable of employing Demand Assigned Multiple Access (DAMA) waveforms unless a waiver is granted.

6.4.3.3 *Super High Frequency (SHF) Satellite Communications (X-band)*—The Defense Satellite Communications System (DSCS) is used by the military services and many other U.S. Government agencies for secure voice and data. The third generation of satellites is currently in orbit. A number of previous generation satellites still continue to function. In most cases, antenna constraints aboard UUVs currently preclude installation of required support equipment to utilize DSCS SHF SATCOM (X-band).

6.4.3.4 *Ka Band Satellite Communications:*

(1) With an initial launch scheduled in 2006, Wideband Gapfiller Satellites (WGS) will provide early transformational capabilities supporting DoD objectives for its TCA in the next decade and beyond. WGS supports communications links within the U.S. Government's allocated 500 MHz of X-band and also, 1 GHz of Ka-band spectrum. The WGS payload can filter and route 4.875 GHz of instantaneous bandwidth. Depending on the mix of ground terminals, data rates and modulation schemes employed, each satellite can support data transmission rates ranging from 2.4 Gbps to more than 3.6 Gbps.

(2) Using reconfigurable antennas and a digital channelizer, WGS also offers added flexibility to tailor coverage areas and to connect X-band and Ka-band users anywhere within the satellite field of view. The X-band and Ka-band spot beams will almost certainly be directed at high-capacity, always-on, user areas such as bases and mobile surface platforms. As with DSCS, the WGS X-band antenna requirements are thought to be too restrictive for most UUVs. However, small autonomous vehicles may be able to take advantage of bandwidth on the Ka-band spot beams once this system becomes fully operational.

6.4.3.5 *L-Band:*

(1) The International Maritime Satellite (INMARSAT) System is an internationally owned commercial consortium:

(a) The legacy system provides worldwide coverage between 70 N and 70 S. Two types of circuits are currently available; narrowband phone (2.4 kbps) and 32 to 64-kbps data. Both types of circuits are in use by DoD. UUVs can certainly leverage the narrowband for command and control (C2). Other unmanned systems such as Global Hawk make use of this link for backup C2. However, for the 64 kbps data, the system requires a directional antenna pointed at the geosynchronous satellite. In this case, the physical dimensions of the antenna and supporting equipment become problematic for use aboard most UUVs.

(b) INMARSAT BGAN System is designed to be among the most powerful commercial communications spacecraft in orbit . It will beam broadband data and voice services covering approximately 85 % of the globe's landmass.

(2) The coverage of BGAN's first satellite is available across Europe, the Middle East, Africa and Asia. Coverage will be extended North and South America, expected by June 2006, with the planned entry into service of the second Inmarsat-4 satellite. BGAN service is accessed via small, lightweight satellite terminals, about the size of a notebook PC (typical terminal is approximately 8 by 8 in., weighing 3 to 4 lb), with broadband speeds of up to 492 kbps. The satellites will eliminate dish-dependent designs of other broadband networks with precise spot beams. Within its footprint, each spacecraft will blanket one-third of the Earth's surface with a single global beam, plus 19 wide-spot beams and 228 narrow-spot beams. The spot beams beneath the satellite are cone-shaped, so a large beam could cover several cities and a narrow beam could focus on an individual city. The smaller beams provide a more compact, more powerful broadcast signal to a smaller area. The spot beams can be refocused on any region in the satellite footprint to accommodate evolving network bandwidth demand. For example, if the number of subscribers logging on in a given area should suddenly spike, the smaller spot beams can be trained on that area to provide a stronger signal to meet the increased demand. BGAN will offer two types of IP service:

(a) Standard IP—Typically used for accessing corporate networks via a secure VPN connection at speeds up to 492 kbps.

(b) Streaming IP—BGAN offers guaranteed data rates on demand. This is ideal for applications where quality of service is paramount, such as live video in the media industry or videoconferencing. You can select Streaming IP on a case-by-case basis, with the flexibility to choose the data rate appropriate to your application requirements. Streaming IP will be available on selected BGAN terminals.

(3) Inmarsat has long been augmenting DoD's organic mobile satellite services and resources, providing the U.S. Government with mobile satellite communications that, when combined with NSA-certified Type 1 encryption devices, can be secured to the highest level. Inmarsat and ViaSat are collaborating to explore ways in which to better serve U.S. Government requirements, with specific emphasis on the Department of Defense. Use of HAIPIS encryption devices, such as the NSA-certified KG-250, to secure the Inmarsat BGAN network has been demonstrated. (2) DoD also makes use of L-band SATCOM services through Enhanced Mobile Satellite Services (EMSS). EMSS is currently operational via the commercial Iridium system; with selected enhancements providing improved security and control for DoD applications. As another strictly commercial option, the Globalstar system offers almost the same capabilities as Iridium. DoD currently has a contract with Iridium through 2007 open ended with a 12 month option to renew: contract number (HC1047-06-C-4008). Both EMSS and Globalstar provide worldwide mobile phone coverage. The satellite constellations are composed of many spacecraft in low earth orbit (LEO). This is true worldwide coverage, which includes the polar regions. The ground terminal problem is greatly simplified given that a satellite is never more than 50° away from directly overhead and operates at a relatively low altitude. Lower required transmit power and simple antennas allow for easy connectivity with handheld devices. The telephone nature of the system, with dial on demand, offers certain opportunity for UUV operations. As

with Inmarsat, the phone line data rates should be acceptable for C2. However, these data rates are likely insufficient for most UUV data transmissions.

6.5 *Network Issues*—None specified in this version of the guide. Future network issues may be addressed in revisions to this document. For example, if the current transition from IPv4 to IPv6 experiences significant difficulties or delays.

6.6 *COMSEC/TRANSEC Issues*—Continued reliance on HAIPE specifications will be the basis for network security. While myriad COMSEC and TRANSEC issues have an impact on UUV operations outside the network, a dedicated discussion of these is beyond the scope of this initial standards document.

7. Technology Forecast

7.1 *Joint Architecture for Unmanned Systems (JAUS):*

7.1.1 The Joint Architecture for Unmanned Systems (JAUS) Working Group continues to plan for the impending merge with the Society of Automotive Engineers (SAE) Aerospace Systems Division (ASD). As part of being incorporated into the SAE community, the former "JAUS Working Group" will transition to "AS-4 Unmanned Systems Technical Committee." The existing JAUS documentation is being updated and finalized to support transition to SAE standards. This ASTM effort will leverage, where appropriate, the work of SAE AS-4 in the pursuit of UUV command and control standards which are currently being developed using the JAUS version 3.2 format. As the developing SAE/JAUS message formats are formally adopted and information becomes available, this ASTM document will be updated to reference the current JAUS specifications.

7.1.2 As background, JAUS is sponsored by the U.S. Office of the Under Secretary of Defense (OUSD) for Acquisition, Technology and Logistics. JAUS is mandated for use by all of the programs in the Joint Robotics Program (JRP). This initiative will develop an architecture for the Domain of unmanned systems. JAUS is an upper level design for the interfaces within the domain of Unmanned Ground Vehicles. It is a component based, message-passing architecture that specifies data formats and methods of communication among computing nodes. It defines messages and component behaviors that are independent of technology, computer hardware, operator use, and vehicle platforms and isolated from mission.

7.1.3 JAUS uses the Society of Automotive Engineers Generic Open Architecture (SAE GOA) framework to classify the interfaces. It complies with the Joint Technical Architecture as well as the Joint Technical Architecture-Army. JAUS is prescriptive, as opposed to descriptive, and is sufficiently flexible to accommodate technology advances. JAUS can be used by any Unmanned System—Air, Ground, Surface, or Underwater—be it commercial or military.

7.1.4 OSD chartered the JAUS Working Group (WG) in 1998. Since then, the WG has made significant progress in developing the architecture. The WG consists of members from the Government, industry and academia. The JAUS documentation produced to date include the Reference Architecture Specification, the Domain Model, a Document Control Plan, and the JAUS WG Standard Operating Procedures (SOP). A Master Plan, Compliance Plan, Transport Plan and User's Handbook are under development.

7.1.5 JAUS will achieve wide acceptance and use as a flexible, robust, easy -to-use domain level architecture for consumer, military and industrial Unmanned Systems. It will promote competition, enable insertion of technology advancements, and provide industry and government a sound business case for its use. It will remain viable and relevant as advancements in system engineering and architecture design occur. As stated, JAUS will be adopted by SAE and become the standard domain architecture for military unmanned systems.

7.2 *Joint Tactical Radio System (JTRS):*

7.2.1 The Joint Tactical Radio System (JTRS) is a U.S. military initiative to develop a family of software programmable and modular communications systems that will become the principal means of communications for warfighters in the digital battlefield environment. All waveforms, protocols, encryption, and communications processes will be implemented in software defined radio (SDR) technology. The software application waveforms, including the Wideband Networking Waveform (WNW), network services, and the programmable radio set (that is, the traditional radio box) form the JTR set. The JTR sets, when networked with other JTR sets, become the JTRS.

7.2.2 JTRS WNW holds tremendous promise for interoperability and flexibility. Multiple waveforms will be available in a compact package. It portends the ability to link UUVs dynamically into a surface network, seamlessly handling the issues of vehicles entering and exiting the network, while providing enough bandwidth to offload collected sensor data in a reasonable amount of time.

7.2.3 The functionality and expandability of JT RS is built upon the Software Communications Architecture (SCA). The SCA is an open architecture framework that governs the structure and operation of the JTRS, enabling programmable radios to load waveforms, run applications, and be networked into an integrated system. Standards detailed in the SCA definition document, address both hardware and software. JTRS compliant radios and networked systems, when designed in compliance with the SCA, will meet JTRS standards for interoperability. Once established, the evolving standards invoked in the SCA will be specified in this guide for UUV communications.

7.3 *Multi-Platform Common Data Link (MP-CDL)*—The Multi-Platform CDL standard may provide a high-capacity pipe that could be used for UUV operations. Interconnecting UUVs to UAVs would help overcome the low antenna height horizon limits when communicating with surface platforms. Future versions of this guide may include MP-CDL standards as part of the RF LOS section.

7.4 *Mobile User Objective System (MUOS)*—The Mobile User Objective System (MUOS) is a next-generation narrowband tactical satellite communications system which shows great promise for UUV operations. The new communications system, slated to become operational in 2010 is being developed as a replacement to the UFO (UHF Follow On) constellation. It will provide global SATCOM narrowband (64 kpbs and below) connectivity for voice, video and data. Key trade analyses are needed for waveform selection (DS-SS CDMA, TDMA, DAMA, etc.), effects of real world interference and fading (ionospheric scintillation, etc.), antenna and multi-element beam array and active phased array beam designs. When MUOS is operational, future versions of this guide will include the UUV RF BLOS communication systems standards that leverage MUOS system protocols.

7.5 *Wireless Standards*—There are many emerging commercial wireless standards that bear consideration for inclusion in future versions of this guide. Wireless wide area network and metropolitan area networks such as IEEE 802.16, IEEE 802.20, and forth, and even personal area network standards applicable to the transmission of data at very close ranges which could support UUV data off-loading operations, have intentionally been excluded from this initial communications guide. Currently, DoD has not approved such emerging standards for Fleet or operational use, other than being restricted for Engineering and Manufacturing Development (EMD) or other developmental programs. The only exception thus far has been SecNet 11 developed by Harris Corporation which features NSA Level 1 encryption. With the obvious utility of wireless standards to future UUV operations, revisions to this guide will address this area by necessity.

8. The Way Ahead

8.1 Prior to the universal adoption of any near-term UUV communication standards, the community must recognize that there are several parallel communication efforts that will continue to upgrade technology and refine CONOPS as commercial and scientific applications are expanded and as the military evolves the concept of Network-Centric Operations and Warfare (NCOW) across the battle-space environment. Once these initial ASTM Committee F41 UUV communications standards are established, care must be taken to incorporate any such advances in technology or operations in a timely fashion. For instance, the recent independent developments in acoustic communications capability should have any associated spectrum utilization issues resolved and address any other compatibility issues to ensure future interoperability of systems and modems. Similarly, current developments in establishing a Joint Architecture for Unmanned Systems (JAUS) must be tracked closely to leverage valuable work in regard to UUV communications and data formats. Parallel unmanned systems' standards development initiatives from such bodies as SAE's AS-4 and NATO's STANAG teams should also be closely coordinated in order to attain the broader goal of complete and seamless unmanned systems' interoperability.

8.2 Although it represents an approach not adopted in this initial guide, the idea of standardizing the interfaces of a unique "communications component" for vehicles merits consideration. The communications component would have control interfaces to establish and control an off-board IP connection. The component would be able control the RF and acoustic communications capabilities. Profiles of the type of RF or acoustic communications, or other types of off-board communication links could be set up so that multiple variants of UUVs could be specified. For example, a profile with commercial standards such as IEEE 802.16 covering Worldwide Interoperability for Microwave (WiMAX) broadband wireless technology could be specified. Another profile could contain particular military communications specifications. In this model, UUV developers would have the communications links dictated and then most likely be capable of leveraging Commercial off-the-shelf (COTS) equipment. In this approach, controlling the interfaces and functionality of the UUV communications component would appear to be more useful. This would also make the governing standard guide applicable to numerous different user domains. Potential expansion of this idea will be based on feedback received during the periodic update and balloting stages of this guide's evolution.

9. Keywords

9.1 acoustic communications; FORCEnet; RF communications; unmanned undersea vehicle; UUV

REFERENCES

(1) Director of Central Intelligence Directive 6/3, Protecting Sensitive Compartmented Information within Information Systems, June 5, 1999.

(2) Exley, G. M., et al, *Submarine Communications Assessment: End to End Assessment of Current and Future Submarine Communications Systems*, Space and Naval Warfare Systems Command, San Diego, CA, September 1999.

(3) Freitag, L., and Singh, S., *Multi-User Frequency—Hopping Underwater Acoustic Communication Protocol*, Woods Hole Oceanographic Institution, Woods Hole, MA, May 25, 2000.

(4) Joint Chiefs of Staff Publication 1-02, "DOD Dictionary of Military and Associated Terms," as amended through 31 August 2005.

(5) Kilofyle, D. B., and Baggeroer, A. B., "Start of the Art in Underwater Acoustic Telemetry," *IEEE J. Oceanic Eng*., Jan 2000.

(6) Undersea FORCEnet Process Implementation Working Group, Undersea FORCEnet Process Implementation Working Group, Phase II Out-brief to the Executive Steering Group, 7 July 2005 .

(7) Coryer, M., et al, Protocol Specification: Benthos Frequency Hopped Multi-Access Signaling, 7 April 2006.