Designation: F 2594 – 06

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

This standard is issued under the fixed designation F 2594; 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:

F 2541 Guide for UUV Autonomy and Control,
WK11283 Guide for UUV Mission Payload Interface,
F 2594 Guide for UUV Communications, and
F 2595 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.

F 2541–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,

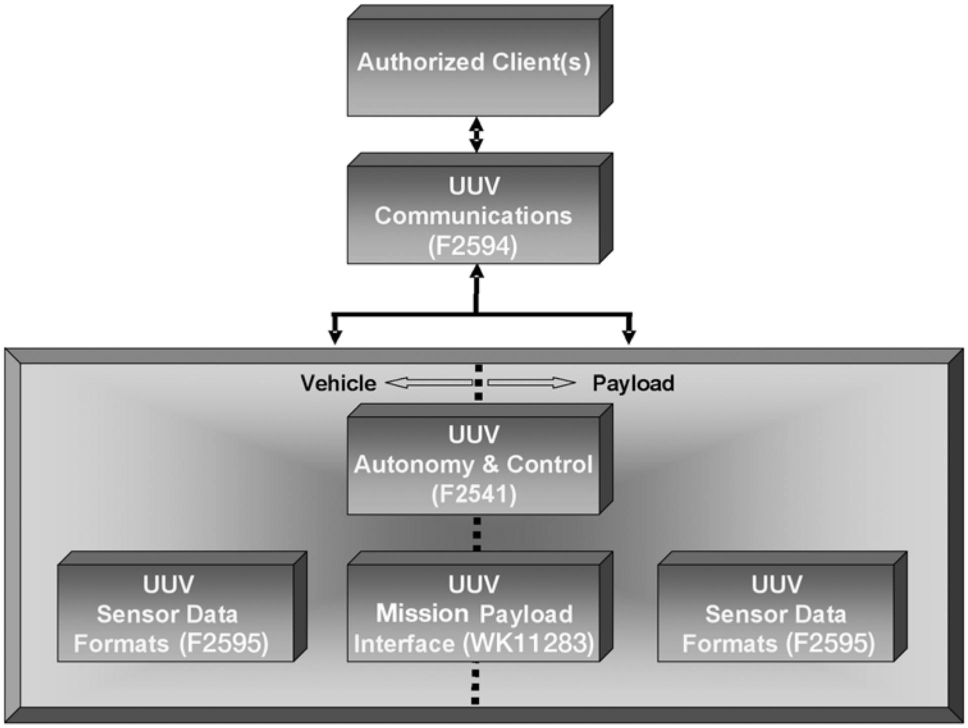

FIG. 1 Notional System Interfaces and Governing Standards

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.

F 2594–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.

F 2595–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 Undersea Vehicle (UUV) Systems and is the direct responsibility of Subcommittee F41.02 on Communications.

Current edition approved Sept. 1, 2006. Published December 2006.

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]

F 2541 Guide for Autonomy and Control for Unmanned Undersea Vehicles (UUV)

F 2595 Guide for Unmanned Undersea Vehicle (UUV) Sensor Data Formats

WK11283 Guide for Unmanned Undersea Vehicle (UUV) Mission Payload Interface

2.2 *DOD Documents:*[3]

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

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

DoD IT Standards Registry (DISR) Generated 21 in. MR-UUVS[4]

Technical Standards Profile (TV-1)

2.3 *Other Documents:*[3]

CCITT 84 Consultative Committee on International Telegraphy and Telephony

PEO C4I Undersea Acoustic Communication Information Exchange Rate Performance Regimes

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

[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.

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**).[5] 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.

4.2 *U.S. Navy UUV Master Plan*—The U.S. Navy UUV Master Plan[6] 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 (DoD) has embarked on several transformational communications initiatives. Among these are the creation of the GIG, 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

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

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

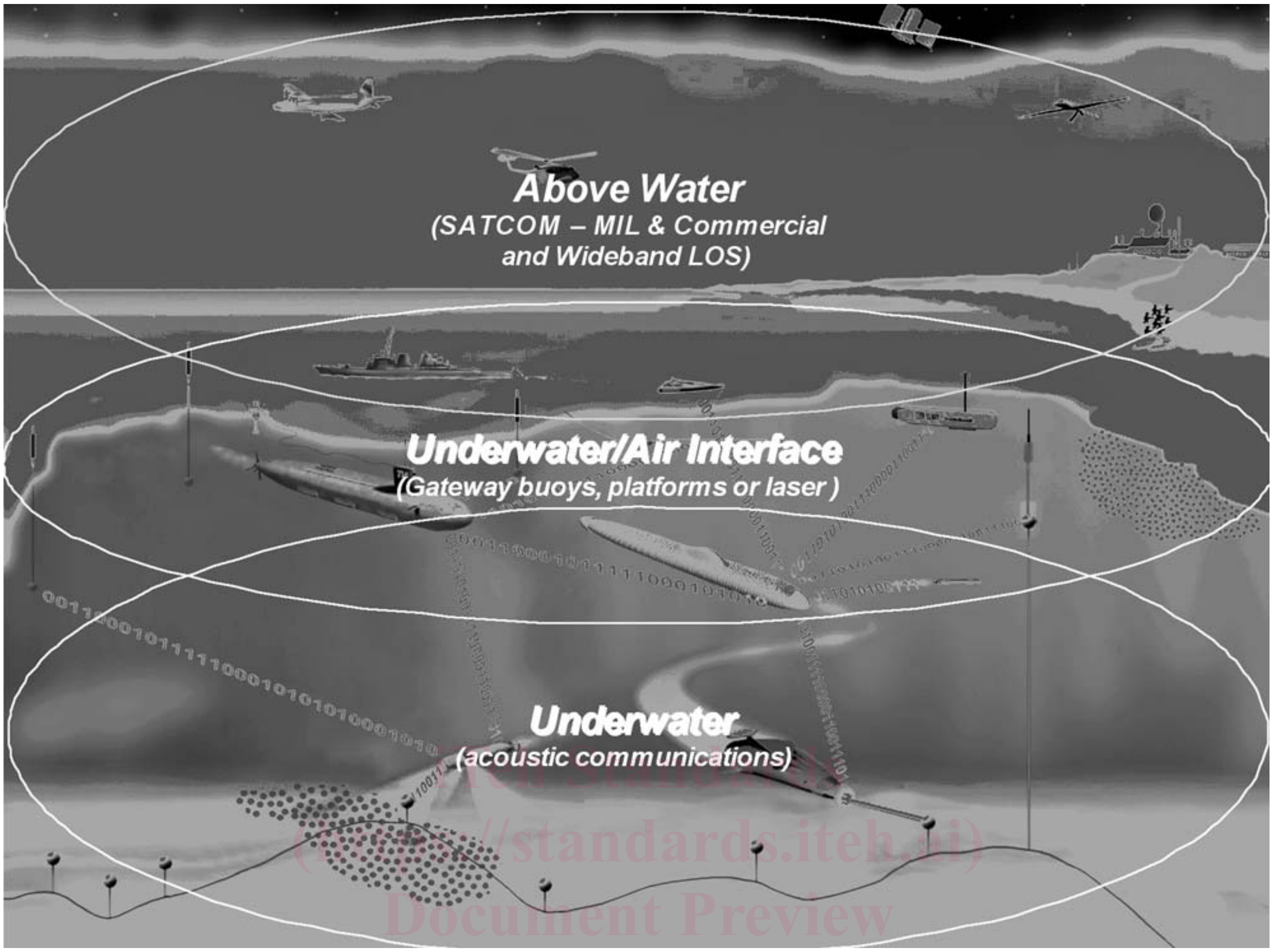

FIG. 2 UUV Communications Domains

N71)[7,8] 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.[9] 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).[10] 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,

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

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

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

[10] 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.

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.[11]

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:

System operations facilitating a vulnerability to unauthorized access.

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

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

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 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. FIPS 171 standard provides methods for managing the keys. 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.

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

4.5 *Data*—Specific UUV sensor data format standards are addressed in Guide F 2595. 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 x 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 F 2595, the UUV Sensor Data Formats Standard.

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.

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		

4.6 *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 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[12] which was defined by the International Standards Organization (ISO). The layered approach is generally accepted as an appropriate means to describe a complete

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

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.

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.

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 which to draw for this guide, a descriptive approach to acoustic systems requirements is taken below. The objective of the guide 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 guide establishes a method to enable the user to engage another vehicle and potentially establish a connection. 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 maintain the proprietary nature of the receive algorithms. The basis for this interoperability is the use of a control packet format that is common to all platforms. The control packet 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. 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

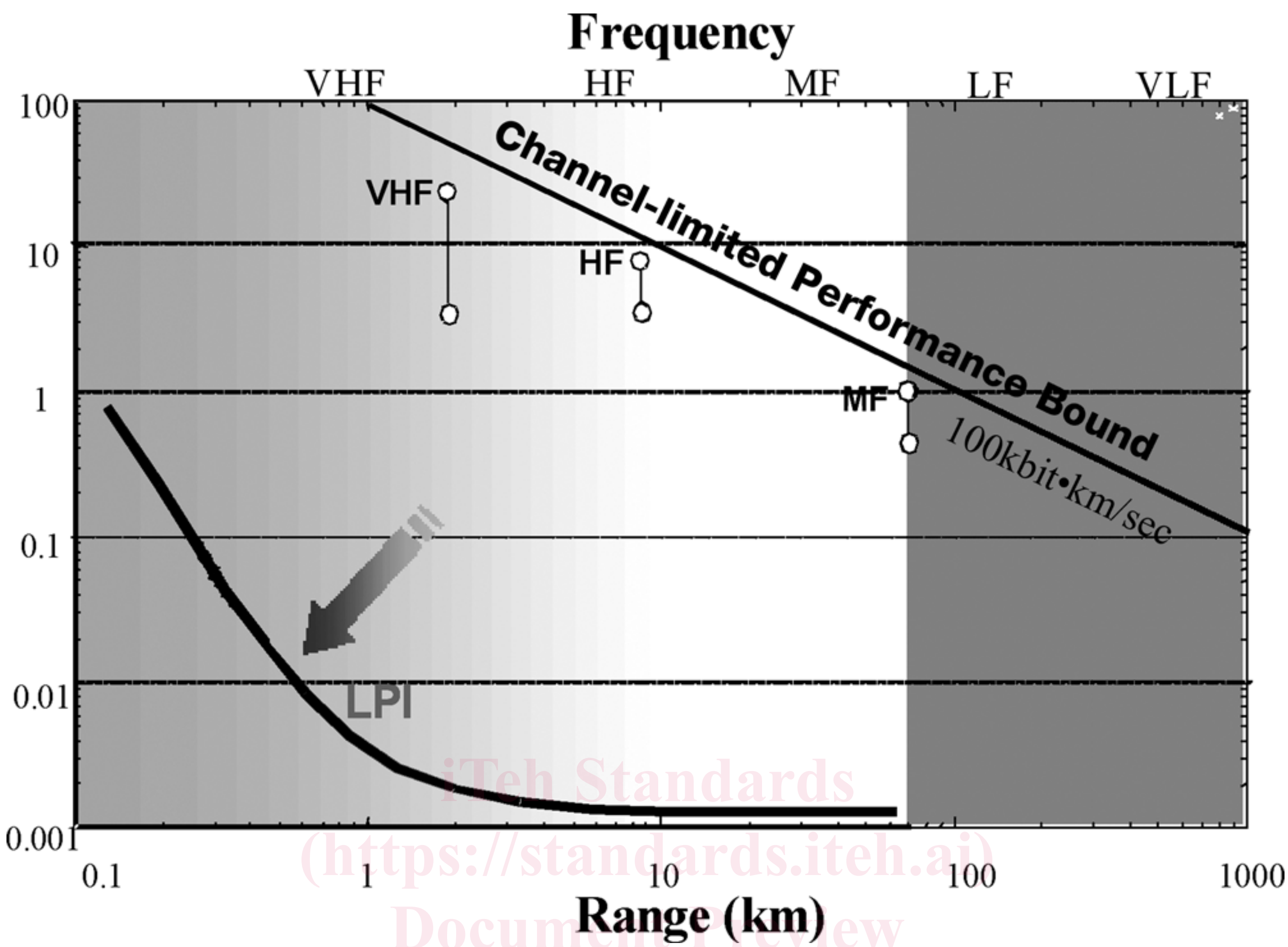

FIG. 3 ACOMMS Performance Regimes

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 physical, data link, and network layers and also touches on the challenges of future network considerations. Thus, the guide will enable a method to accurately describe a communication protocol in a common nomenclature.

5.3.1.1 *Constraints*—The bandwidth and data rate limitations of current acoustic systems 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 to 100 Kbytes have been transferred reliably in past experiments (**5**). Example systems typically have data rates of 100 to 2400 baud at up to 100 km range. Some developmental systems have demonstrated capabilities up to 50 kbaud 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 is included in Fig. 3 and empirical results are documented (**5**). Another possible constraint includes on-board available power which could impact acoustic communications.

5.3.1.2 *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.

5.3.1.3 *Acoustic Networks*—U.S. Navy undersea wireless network development is following a concept of operations (CONOPS) called Seaweb. Seaweb networks interconnect fixed and mobile nodes distributed across wide areas in the undersea environment. Through-water telesonar (that is, telecommunications sound navigation ranging) using digital communications theory and digital signal processor (DSP) electronics is the basis for the physical layer of these underwater networks. Node-to-node ranging is a by-product of telesonar signaling, permitting localization of sensor nodes and navigation of mobile nodes such as submarines and autonomous vehicles. The unusual characteristics of the physical-layer medium constrain the design of the link and network layers. Seaweb data-packet communications are achieved through the ancillary use of compact channel-tolerant utility packets. Measuring the available acoustic channel permits link optimization by adapting the data-packet signal parameters to the prevailing channel attributes. 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.