Designation: F 1756 – 97a (Reapproved 2002)

An American National Standard

Standard Guide for Implementation of a Fleet Management System Network[1]

This standard is issued under the fixed designation F 1756; 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.

1. Scope

1.1 This guide provides an overview and guide for the selection and implementation by shipowners and operators of a Fleet Management System (FMS) network of computer services in a client/server architecture (see Fig. 1). The FMS is based upon a wide area enterprise network consisting of an unspecified number of Shipboard Information Technology Platforms (SITPs) and one or more shoreside Land-Based Information Technology Platforms (LITPs), which provides management services for the shipping enterprise. The FMS can be understood as a computer system comprised of one or more LITPs and one or more SITPs. It can be characterized as mission critical 24 × 365 (24 h/day, 365 days/year).

1.2 The SITP (see Fig. 1) provides a set of software services, including:

1.2.1 *Communications Services*, to communicate between vessels and with shore via multiple wireless communication technologies;

1.2.2 *Data Acquisition Services*, providing access to shipboard system data as required for use by other systems and management purposes; and,

1.2.3 *Executive Services*, providing software process administration and control.

1.2.4 In total, the SITP provides the capability for multiple shipboard computer systems to share data with each other and to communicate with shore-based management or other vessels or both.

1.3 The SITP is understood to consist of integrated hardware, software, a data repository, and standardized procedures, which provide the ability to send, receive, process, transfer, and store data or messages in digital form in a common mode from shipboard systems or administrative utilities or both, and from designated sources outside the network, for example, systems accessed through wireless communication services, such as satellite, VHF, HF, and so forth. Shipboard systems include navigational, machinery control and monitoring, cargo control, communications, and so forth. The SITP also will provide the capability for the remote administration and maintenance of associated computer systems aboard the vessel.

1.4 The SITP requires an underlying hardware and network infrastructure, including a shipboard computer local area network (LAN), file servers, workstations, wireless communications transceivers, cabling, other electronic and optical devices, video display units, keyboards, and so forth.

1.5 The SITP also requires underlying system software providing network operating system (NOS) services, DBMS services, and other system software.

1.6 There also is a layer of shipboard application systems, which are designed to capitalize on the FMS infrastructure to share data with other shipboard systems and management ashore. Those systems also would be able to capitalize on the remote management capabilities of the FMS.

1.7 The LITP is an asset that can exchange operating and administrative data from individual ships and maintain a DBMS to support fleet management and other maritime applications. The LITP will support data repositories, file servers, workstations or personal computers (PCs), and a communication hub providing connectivity to distributed satellite services, VHF (very high frequency), HF/MF (high frequency/medium frequency), and land lines. The DBMS makes possible the development of knowledge-based "decision aids" by providing the ability to retrieve, process, and analyze operational data.

1.8 This guide does not purport to address all the requirements for a SITP, which forms a path for data for direct control of the operation or condition of the vessel or the vessel subsystems.

1.9 In all cases, it shall be possible for all units of navigation equipment resident on the Navigation Equipment Bus to operate and display essential operating data independently of the FMS.

1.10 In all cases, it shall be possible for all units resident on the Control, Monitoring, and Alarm Bus to operate and display essential operating data independently of the FMS.

1.11 In all cases, it shall be possible for all units resident on the Communications Bus to operate and display essential operating data independently of the FMS.

1.12 Values shown in this guide are in SI units.

[1] This guide is under the jurisdiction of ASTM Committee F25 on Ships and Marine Technology and is the direct responsibility of F25.05 on Computer Applications.

Current edition approved Nov. 10, 1997. Published October 1998. Originally published as F 1756 - 97. Last previous edition F 1756 - 97.

Copyright © ASTM International, 100 Barr Harbor Drive, PO Box C700, West Conshohocken, PA 19428-2959, United States.

1.13 *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.*

2. Referenced Documents

2.1 *ASTM Standards:*

E 919 Specification for Software Documentation for a Computerized System[2]

E 1013 Terminology Relating to Computerized Systems[2]

F 1166 Practice for Human Engineering Design for Marine Systems, Equipment, and Facilities[3]

F 1757 Guide for Digital Communication Protocols for Computerized Systems[3]

2.2 *ANSI Standards:*[4]

X3.172 Dictionary for Information Systems

X3.172a Dictionary for Information Systems (Computer Security Glossary)

2.3 *IEEE Standards:*[5]

IEEE 1028–1988(R1993) Standard for Software Review and Audit

IEEE 1012–1986(1992) Standard for Verification and Validation Plans

IEEE 45 Recommended Practice for Electrical Installations on Shipboard

IEEE 802 Standards for Local and Metropolitan Area Networks—Overview and Architecture

IEEE 802 Standards for Local and Metropolitan Area Networks—Interoperable LAN/MAN Security

IEEE 802.10e and 10f Supplements to IEEE 802.10

IEEE 1003

IEEE 1063 Standard for Software User Documentation

2.4 *IEC Documents:*[4]

IEC 50 International Electrotechnical Vocabulary (IEV)

IEC 92–504 Electrical Installations in Ships; Special Features–Control and Instrumentation

IEC 533 Electromagnetic Compatability of Electrical and Electronic Installations in Ships and of Mobile and Fixed Offshore Units

IEC 945 Maritime Navigation and Radiocommunication Equipment and Systems

IEC 1069 Industrial–Process Measurement and Control—Evaluation of System Properties for the Purpose of System Assessment, Part 1: General Considerations and Methodology; Part 2: Assessment Methodology

IEC 1162 Maritime Navigation and Radiocommunication Equipment and Systems—Digital Interfaces

IEC 1209 Integrated Bridge Systems (IBS) for Ships

2.5 *NMEA (National Marine Electronics Association) Standard:*[6]

NMEA 0183 Standard for Interfacing Electronic Marine Navigational Devices

[2] *Annual Book of ASTM Standards*, Vol 14.01.

[3] *Annual Book of ASTM Standards*, Vol 01.07.

[4] Available from American National Standards Institute (ANSI), 25 W. 43rd St., 4th Floor, New York, NY 10036.

[5] Available from Institute of Electrical and Electronics Engineers, Inc. (IEEE), 445 Hoes Ln., P.O. Box 1331, Piscataway, NJ 08854–1331.

[6] Available from the National Marine Electronics Association (NMEA) Seven Riggs Ave., Severna Park, MD 21146.

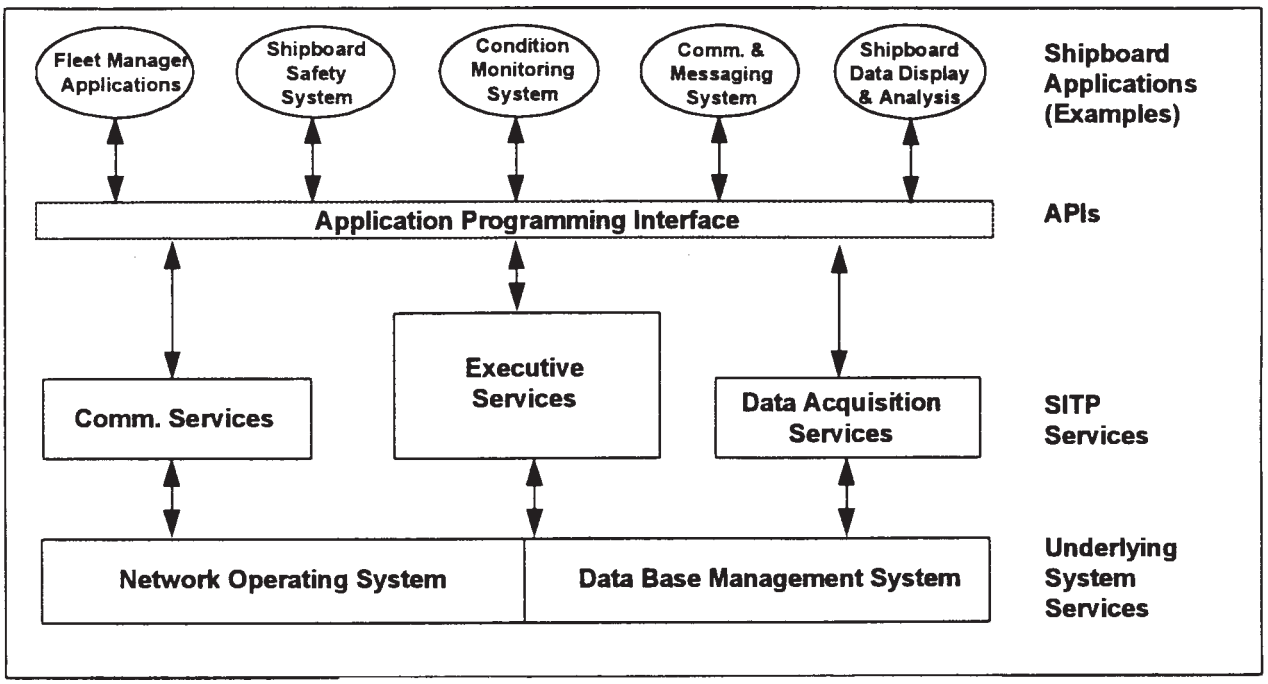

FIG. 1 Typical Architecture

3. Terminology

3.1 *Definitions:* Definitions of terms in this guide and described below are in accordance with Terminology E 1013 and ANSI X3.172 and X3.172a.

3.1.1 *application program*, *n*—a computer program that performs a task related to the process being controlled rather than to the functioning of the computer itself.

3.1.2 *application programming interface (API)*, *n*—an API is a set of rules for linking various software components of a network.

3.1.3 *automatic information system (AIS)*, *n*—automatic distribution of a ship's voyage information to all interested parties, that is, other ships, port state, owner, and so forth.

3.1.4 *baseband network*, *n*—only one transmission can be on the network at any given time.

3.1.5 *black box test*, *n*—black box tests are based on the design specification and do not require a knowledge of the internal program structure.

3.1.6 *certification*, *n*—the process of formal approval, by an authority empowered to do so, of arrangements or systems for the reception, storage, or transmission of data and intelligence relative to the management, operation, or control of vessels.

3.1.7 *client server database engine*, *n*—a commercial data base management system serving as a repository for all critical ship operating and configuration information.

3.1.8 *computer program*, *n*—a set of ordered instructions that specify operations in a form suitable for execution by a digital computer.

3.1.9 *computer system*, *n*—a functional unit, consisting of one or more computers and associated software, that uses common storage for all or part of a program and also for all or part of the data necessary for the execution of the program.

3.1.10 *configuration manager*, *n*—utilities that determine the data to be collected, the processing and storage rules, the standard software functions that facilitate the interfaces between systems and the FMS process servers and other configuration parameters.

3.1.11 *data replicator/message processor*, *n*—a software module that is responsible for receiving, decoding, and storing communications and transmissions received from ships. This module also prepares data for transmission to a ship through the land-based communications hub.

3.1.12 *document management system*, *n*—an application that allows procedures manuals to be stored and accessed electronically on shipboard and to be updated electronically.

3.1.13 *electronic mail system*, *n*—a messaging and file transfer system for both ship and shore.

3.1.14 *fault tolerance*, *n*—the built-in capacity of a system to provide continued correct execution in the presence of a limited number of hardware of software faults.

3.1.15 *fleet management system (FMS)*, *n*—a system of computer services in a client/server architecture, based on a wide area enterprise network consisting of an unspecified number of SITPs and the LITP. The FMS can be understood as a computer system comprised of one or many shipboard systems and one of many shoreside systems. It can be characterized as mission critical 24 × 365 (24 h/day, 365 days/year).

3.1.16 *independent*, *n*—independent as applied to two systems means that either system will operate with the failure of any part of the other system excluding the source of power.

3.1.17 *interface*, *n*—the interface attribute describes the methods and rules governing interaction between different entities.

3.1.18 *integration tests*, *n*—tests performed during the hardware/software integration process before computer system validation to verify compatibility.

3.1.19 *land-based communications hub*, *n*—a land-based computer system that provides uniform access to multiple maritime satellite services, as well as access to public telephone networks, e-mail, and the internet.

3.1.20 *local area network (LAN)*, *n*—a network that connects computer systems resident in a small area. For purposes of this guide, the SITP is considered a shipboard LAN with access to similar shoreside and shipboard units through radio and satellite telecommunication services.

3.1.21 *MSAT*—satellite communications service covering North America

3.1.22 *multitasking*, *n*—the capability to handle more than one task at a time

3.1.23 *NAVTEX*, *n*—a system for the broadcast and automatic reception of maritime safety information by means of a narrow-band direct-printing telegraphy.

3.1.24 *network interface unit (NIU)*, *n*—the network interface units (NIUs) provide for connection and message translation to enable data streams from systems, both hardware and software, which may use various standard and proprietary communication protocols to be stored and accessed in the FMS database in a standard format.

3.1.25 *ship information technology platform (computing)*, *n*—an integrated system of software, hardware, communication links, and standardized procedures that provide the ability to collect, process, and store information in digital form.

3.1.26 *ship earth station*, *n*—a mobile earth station for maritime service located aboard a ship. Typically, a small lightweight terminal with omnidirectional antenna with interfaces for a personal computer or any other data terminal equipment for message generation and display, for example, Inmarsat C, or a steerable antenna mounted on a stabilized platform, for example, Inmarsat A and B and M.

3.1.27 *single failure criterion*, *n*—a criterion applied to a system such that it is capable of performing its safety task in the presence of any single failure.

3.1.28 *software*, *n*—programs, procedures, rules, and associated documentation pertaining to the operation of a computer system.

3.1.29 *software cycle*—the software cycle typically includes a requirements phase, a design phase, an implementation phase, a test phase, an installation and checkout phase, and an operation and maintenance phase.

3.1.30 *validation*—the test and evaluation of the integrated computer system, hardware and software, to ensure compliance with the functional, performance, and interface requirements.

3.1.31 *verification*, *n*—the process to determine if the product of each phase of the digital computer system development process satisfies the requirements set by the previous phase.

3.1.32 *voyage data recorder (VDR), n*—a store of information, in a secure and retrievable form, concerning the position, movement, physical status, command, and control of a vessel over the period leading up to a marine casualty.

3.1.33 *white box test, n*—white box tests require a knowledge of the internal program structure and are based on the internal design specification.

3.1.34 *workstation, n*—a computer and associated visual display unit (monitor) configured as an I/O unit to perform certain tasks.

4. Significance and Use

4.1 Competent information management is essential for safe and productive operation and regulatory compliance. A short list of the functions affected includes decision aids for navigation, communications, ship handling, machinery control, cargo operations, maintenance and repair, personnel records, and environmental protection.

4.2 The shipbuilding and shipping industries have identified a need to develop comprehensive standards and guides for implementing computer-based shipboard data management systems.

4.3 The FMS may include single or multiple SITPs and single or multiple LITPs and provides the means to integrate shipboard and shoreside computer systems with multivendor connectivity, distributed processing, and electronic data interchange between noncompatible networks, computers, workstations, and peripherals and maintain databases, which promote safety of life at sea, protection of the environment, and operational efficiencies throughout the life cycle of the vessel/fleet. The FMS may incorporate satellite gateways to coastal communication hubs providing access to land-based networks, such as telephone lines, facsimile, e-mail, and expanded satellite services through land earth stations.

4.4 The SITP can be configured to provide the ship's control center with access to local control centers, such as for cargo operations, which may be located on the main deck.

4.5 This guide has provisions relevant to all components of the FMS platform including the ship earth station, interface devices for subsystems and administrative systems connected to or forming part of the network, communication services, and certain land-based facilities under the direct control of the ship's management.

4.6 It is the intent of this guide to provide guidelines for the design and implementation of open client/server architecture for computer and communication networks for shipboard and shore-based applications.

4.7 This guide is intended to assist vessel owners, designers, shipyards, equipment suppliers, and computer service providers in the development of contract technical specifications, which detail the services to be supported, performance required, and criteria for acceptance for specific FMS installations.

5. FMS Architecture

5.1 *Network Design*—There is an underlying computer network to support the FMS. The functions of the FMS enable a communication network that provides for the exchange of information between nodes or devices capable of transmitting or receiving information in the form of electronic or optical signals. The process is enabled by communication protocols, which define the rules that must be implemented in the hardware and software. The text of this guide is predicated on a network architecture conforming to the Open Systems Interconnection Reference Model (OSI/RM). See Guide F 1757.

5.2 *Network Management:*

5.2.1 The FMS is based upon a wide area network (WAN) consisting of a number of LANs, which are dispersed geographically over large areas and are linked through wireless communications by bridges and gateway devices. The group responsible for managing the FMS will normally be located in the principal shoreside office. The primary task of the network management system is to oversee and report on the operation of the network, which may comprise products from many different vendors.

5.2.2 *Security*—A security function should be provided that is responsible for the following:

5.2.2.1 Data confidentiality;

5.2.2.2 Data integrity;

5.2.2.3 Data authentification; and,

5.2.2.4 Access control.

5.3 *Database Model*—Database maintenance and availability are key features of the FMS. Each SITP and the LITP will maintain separate databases. Each FMS site will incorporate a database management system, including replication capability, as part of each SITP and LITP installation.

6. Shipboard Information Technology Platform (SITP) Connectivity

6.1 A key objective of the SITP is to facilitate sharing of data among shipboard systems (see Fig. 2). The shipboard systems, which are candidates for connection to an SITP include, but are not limited to, the following:

6.1.1 *Shipboard Operating Systems*—Shipboard operating systems are active systems and may acquire information from sensors or databases and exercise control internally or transmit data for administrative purposes or for application in knowledge-based decision aid systems.

6.1.1.1 *Integrated Bridge System*—This system comprises the integrated bridge system bus, the navigation equipment bus, and the control, monitoring, and alarm bus.

6.1.1.2 *Integrated Bridge System Bus*—The integrated bridge system bus provides connectivity for the navigation equipment bus and the control, monitoring, and alarm bus and is a controlled gateway to the administrative network.

6.1.1.3 *Navigation Equipment Bus*—The navigation equipment bus provides systemwide connectivity for any or all of the following or any additional units associated with the navigation of the vessel: gyro compass/autopilot; global positioning system (GPS); dead reckoning (DR) navigation system; speed and distance indicator (Doppler log); sonic depth finder; electronic chart system (including, but not limited to, ECDIS); rate of turn indicator (ROTI); radar/ARPA (automatic radar plotting aids); radio direction finder; and voyage data recorder (VDR).

6.1.1.4 *Control, Monitoring, and Alarm Bus*—The control, monitoring, and alarm bus provides systemwide connectivity for any or all of the following or any additional units associated

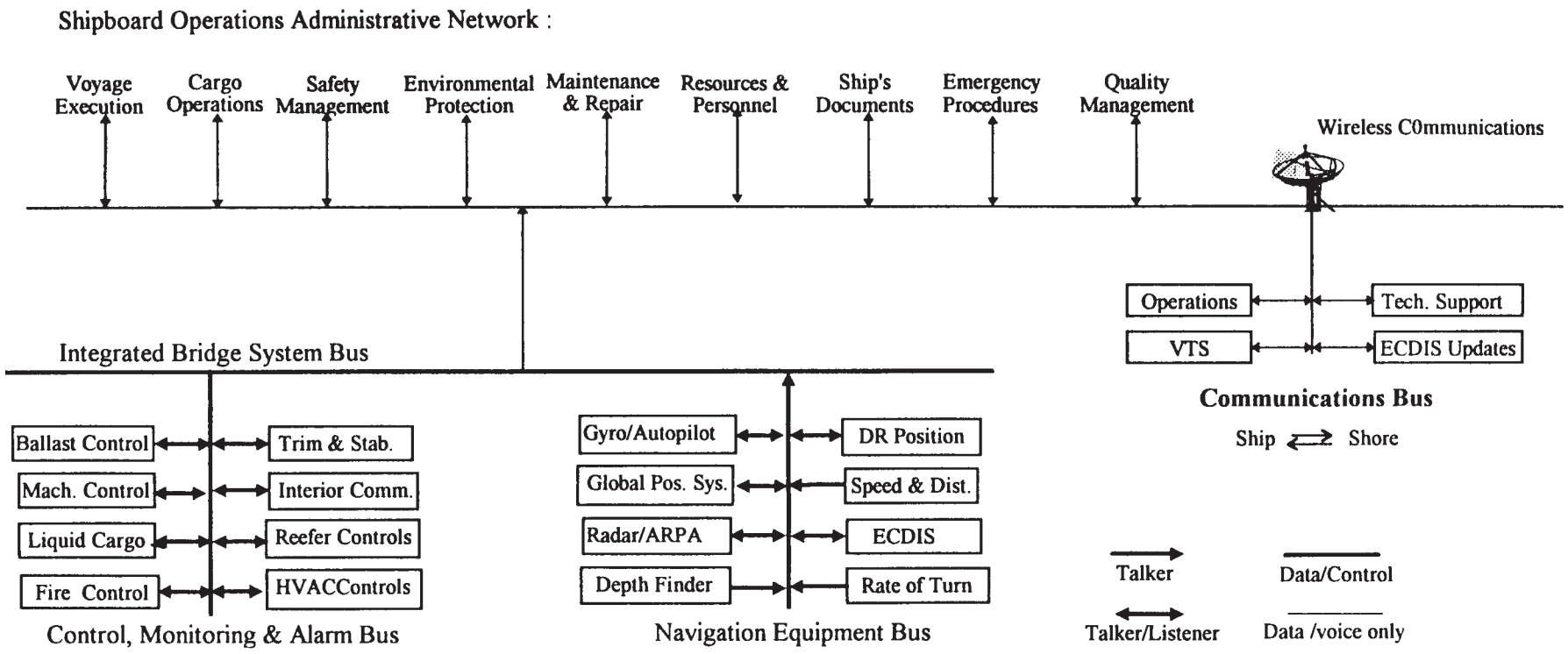

FIG. 2 SITP Data Flow (Typical)

directly with control of the vessel: machinery control, monitoring, and alarm; liquid cargo control; inert gas control; ballast control; fire detection and alarm; loading (trim and stability; hull stress); internal communications; WT door and fire door controls; controls for refrigerated cargo; and HVAC controls.

6.1.2 *Communications Bus*—The communications bus provides connectivity for any or all of the following or any additional units providing communication facitilities on board the vessel: Inmarsat A, B, M; Inmarsat C; VHF radiotelephone; MF/HF SSB radiotelephone; cellular; and GMDSS (Global Maritime Distress Safety System–see Appendix X3).

6.1.3 *Administration System:*

6.1.3.1 *Ship-to-Shore Communications:*
Electronic mail and file transfer,
Connection to local telephone systems, and
Sailing instructions (weather routing).

6.1.3.2 *Cargo Planning:*
Stability and trim,
Container ordering,
Cargo manifests,
Custody transfer procedures and records, and
International Maritime Dangerous Goods Code.

6.1.3.3 *Fuel Management—Speed/Distance/Consumption:*
Fuel rate,
Running inventory,
Fuel quality records,
Bunkering checklist,
Bunker planning—grades and quantities, and
Cargo heating.

6.1.3.4 *Inspections, Maintenance, and Repair:*
Inspection schedules,
Maintenance and repair (M and R) schedules and records, and
Spare parts inventory control (use, ordered, received, and cost).

6.1.3.5 *Quality Management:*
ISM Code compliance,
Quality procedures and records (ISO 9000), and
Auditing.

6.1.3.6 *Personnel and Safety Management:*
Employment records management—payroll,
Training and certification,
Hazard communication (benzene, asbestos),
Respiratory protection, and
Occupational health monitoring.

6.1.3.7 *Ship's Documents:*
Predeparture and prearrival checklists/documents,
Bridge manual,
Muster cards and checklists,
Stability book,
Bunkering records,
Engine manual, and
Fire and damage control.

6.1.3.8 *Reports:*
Automatic information system (AIS) and
Voyage data recorder (VDR).

7. Shipboard Information and Technology Platform (SITP)

7.1 The SITP consists of the software and hardware required to support a distributed computing network based on the client/server model. In general, the SITP will be optimized to respond to a single LITP. For cases in which the SITP will respond to multiple shoreside platforms, a hierarchy should be defined. The SITP consists of layers of computer services and underlying layers of system services, including a network operating system and a database management system.

7.1.1 *Computing Model*—Client/server computing is expected to be the computing model for the SITP. Client/server is a joint operation in which specific computers perform specific tasks. Server tasks generally involve file sharing, database management, communications management, and so forth. Client tasks, on the other hand, are generally active and are defined by the application.

7.1.1.1 *Server(s):*

(*a*) Comprises software that is resident on an intelligent machine (a computer);

(*b*) Is a provider of services. The services may include database services (DBMS), communication services, and processes;

(*c*) Is a shared resource. One server can serve several clients;

(*d*) Is transparent to the user. Clients and servers communicate by a messaging interface; and,

(*e*) Is normally a dedicated PC.

7.1.1.2 The client(s) is normally software that is resident on a PC or work station.

7.1.1.3 *Quality*—Design, development, modification, replication, and installation should be subject to a documented quality plan. At a minimum, the areas of responsibility, performance, and acceptance criteria should be addressed in the quality plan.

7.1.1.4 The design and testing of the computer services should ensure that:

(*a*) The implementation satisfies the applicable requirements, which may also include statutory and classification requirements;

(*b*) Design documentation will show that specification requirements can be traced through all levels;

(*c*) Module interfaces and dependencies are clearly defined and identified;

(*d*) Estimates of memory capacity, central processor unit, and bandwidth are reliable and can support hardware selection;

(*e*) Test procedures are defined and carried out in parallel with the design process; and,

(*f*) Documentation is subject to formal review.

7.1.2 *Required Underlying System Services:*

7.1.2.1 *Network Operating System*—A network operating system supports the following services that should be transparent to the user:

(*a*) Initialization of the system services;

(*b*) Enables applications throughout the network;

(*c*) Provides for multiple user access to programs and database and file services;

(*d*) File and print services—remote access, read, write, download, and upload;

(*e*) Gateways to independent networks—the ability to access a remote system; and,

(*f*) Network management.

7.1.2.2 *Security Management*—Security management provides an integrated platform-wide, including network operating system and compliant applications, security system that includes:

(*a*) Discretionary access control (DAC) in which the users may protect their own objects;

(*b*) Mandatory access control (MAC) in which users may read or write objects for which they have clearance. Users may read objects at the same or lower class and write objects at the same or higher class;

(*c*) Isolation of the security kernel from noncritical systems;

(*d*) User authentification/identification;

(*e*) Audit and log of security-related transactions—log-ins, read or write operations on objects, and log-outs;

(*f*) System testing;

(*g*) Users' guide;

(*h*) System manual; and

(*j*) System documentation.

7.1.2.3 *Encryption*—Radio communications between SITPs and LITPs are exposed to electronic monitoring, and messages transmitted in clear text will be exposed to eavesdropping and intrusion. Data encryption is the most effective protection against such intrusions and should be available for security-sensitive communications. The encryption protocol should provide for multiple algorithms and the assignment of separate algorithms for different types of data. A critical element of the encryption program is the control of data encyphering and data decyphering keys, a key management system. This system is responsible for key origination, application, recording, assignment, and deletion.

7.1.2.4 *Virus protection*—Includes programmed virus scanning software and floppy disk control.

7.1.2.5 *Miscellaneous*—Includes automatic checking and reporting of memory errors and automatic reset and reboot after power interruption.

7.1.3 *Database Management System:*

7.1.3.1 The database management system supports a data repository that provides for storage of data in digital form and manages:

(*a*) Data acquisition and storage;

(*b*) Data replication on demand, scheduled or event driven;

(*c*) Integration of information at multiple remote sites;

(*d*) Open database connectivity;

(*e*) Query language;

(*f*) Concurrency/multiple users; and,

(*g*) Referential integrity.

7.1.3.2 *Database Security*—The DMBS should incorporate protection against improper access, improper modification of data (ensure data integrity), and improper denial of access. It should provide for:

(*a*) *Operational Integrity*—This addresses the serialization and isolation properties of transactions. Serialization means that the concurrent run of a set of transactions will give identical results as a sequential run of the same set of transactions.

(*b*) *Logical Integrity of Data*—Allowed range.

(*c*) *Accountability and Auditing*—Record of all read or write access to data.

(*d*) *Privacy*—Control of employment, medical records, and so forth.

(*e*) *Delimitation*—Control of information transfer between programs.

7.2 *SITP Services*

7.2.1 The SITP services, as shown in Fig. 1, are required to provide overall command and control of the SITP. The executive has overall responsibility to monitor the SITP and control the distributed processes that operate as platform services. The SITP executive itself is a series of services each of which are responsible for specific tasks. The SITP provides a layer of insulation and control between high- and low-level processes. It uses a set of structured APIs and internal communication channels for message exchange.

7.2.2 *Executive Services*—The following sections describe the services provided by the SITP executive. These services are each responsible for the orderly registration, control, audit, and monitoring of SITP compliant software processes on the server and supported workstations for their specific function.

7.2.2.1 *Process Management*—Process control refers to starting, staging, pausing, resuming, and stopping. An SITP process may be an SITP internal process, network operating system process, or an SITP compliant application. The process management interfaces with the SITP compliant process through the SITP APIs and with the process management database. Each physical computer within the SITP will have a process management function. All SITP processes are registered in the SITP process management database that describes the important attributes of the process. All process information is available to SITP compliant applications.

7.2.2.2 *Health Management*—Health management is used to check, on an ongoing basis, the current health of all SITP compliant processes and record that finding in the health management database. This information is available to SITP compliant applications.

7.2.2.3 *Performance Management*—Performance management is used to observe the efficiency of any particular entity in the system. It is through the SITP performance management facilities that a process can make application-specific data available for monitoring. Furthermore, the data is modeled in such a way as to allow a general purpose monitoring application to display performance data for any participating monitored object.

7.2.2.4 *Logging Management*—The logging management interfaces with the SITP compliant process through the SITP APIs and with the logging management database. An SITP compliant process, locally or remotely, may send unsolicited events to the logging management for processing. The logging management directs the logging management database to store the event in the event history.

7.2.2.5 *Alarm Management*—The alarm management interfaces with the SITP compliant process through the SITP APIs and with the alarm management database. An SITP compliant process, locally or remotely, may send an unsolicited alarm of

a particular alarm type to the alarm management for processing. The alarm management directs the alarm management database to store the alarm in the alarm history.

7.2.2.6 *Schedule Management*—The SITP schedule management will define a standard API for applications to schedule future running of programs, either as one-time or recurring jobs. A history of requests and execution will be maintained. Compliant applications will have access to this data for display, reporting, audit, or diagnostic purposes. Programs can be scheduled to run based on several criteria, such as time and data, or a range of times. Programs also can be configured to run on a recurring basis. The SITP schedule management also will keep a history of execution.

7.2.2.7 *Time Management*—The SITP will define a standard API for applications to synchronize with a master clock. This will counter the time drift encountered in computer real-time clocks and allow for the synchronization of time stamps for remote systems. In a shipboard system in which distributed systems execute autonomously, synchronization of events is a critical function. The time management is responsible for maintaining the master clock and providing an API for various SITP services to access that information. To present a uniform reference point, the time management should operate in Z (Zulu) Time and date stamp in an accepted international format and arranged to display world local times on demand.

7.2.2.8 *Localization Management*—The SITP localization management interfaces with the SITP compliant process through the SITP APIs and with the localization management database. An SITP compliant process can request localization information, such as language type, collating sequence, date and money formats, system messages, application strings, and any other locale-related information.

7.2.2.9 *Debug Management*—The SITP debug management interfaces with SITP compliant processes through the client APIs and with the debug management database. An SITP compliant process can send debug data to the debug management for processing. The debug management will record this debug information in the debug management database.

7.2.2.10 *Backup Management*—The backup management will service client backup requests. It interfaces with SITP compliant processes through the client APIs and with the backup management database. The SITP platform will define a standard API for the backup and restoration of application files and file sets. A history of backup and restore operations for volumes and sets will be retained. Compliant applications will have access to this data for display, reporting, audit, or diagnostic purposes.

7.2.2.11 *Test Management*—The testing management will intervene between client test requests and targets. It interfaces with the SITP compliant process through the client APIs and with the testing management database. An SITP compliant process can request test execution or test history information.

7.2.2.12 *Messaging Management*—The SITP messaging management will define a standard API for applications to transport data among all registered entities on the global SITP network. This will allow applications to send and receive arbitrary data to and from any other SITP application. This includes ship to shore, ship to ship, and shore to ship. A hierarchical naming scheme is supported by the messaging management allowing for orderly classification of communication endpoints. The messaging management will use communications facilities as a transport mechanism for interapplication messages. The communication abstraction provided by the messaging management allows for additional transport mechanisms to be used in the future.

7.2.2.13 *Replication Management*—The SITP replication management is a generalized mechanism that may be used by SITP application providers to build distributed applications that operate within the SITP environment. The services provided by this facility include the following:

(*a*) *Rules-Based Distribution*—Configurable distribution of transactions, at the table level, between ship- and shore-based system sites. SITP can be configured to send all, or selected subsets of, information between system sites at flexible intervals. Further, a redistribution feature allows transactions to be forwarded to multiple sites based on system configuration parameters.

(*b*) *Distribution Control Mechanisms*—To maintain data integrity, strong control mechanisms are required to serialize, log, and archive all incoming and outgoing transmissions. Disaster recovery mechanisms are required to resend failed transmissions or allow a complete refresh synchronization between system sites. Confirmation of sent and received transmissions must be passed between system sites to ensure data integrity.

(*c*) *Batched Distribution*—As sustained real-time connections between system sites can be costly, the platform will support batched groups of transactions to be transmitted in compressed packets during low-cost time windows.

7.2.2.14 *Enterprise Management*—Several of the services offered by the executive system provide a means of managing various aspects of the SITP system. The enterprise management allows SITP interfaces to be available for use by remote users. The enterprise management would enable a user at a shore site to invoke SITP APIs on a specific ship.

7.2.2.15 *Configuration Management*—The configuration management handles requests from client processes via API calls. These requests will either request particular configuration settings or a change to a configuration setting. These client processes can be any SITP compliant process. This service is responsible for updating the configuration database as required and notifying other processes affected by the configuration change.

7.2.3 *Data Acquisition Services:*

7.2.3.1 The SITP data acquisition module is responsible for communicating with the various shipboard control systems or data collection units to acquire data. The SITP data acquisition is responsible for the orderly registration, control, audit, and monitoring of SITP compliant software processes on the server and supported workstations for data acquisition. The SITP data acquisition will provide a framework in which custom interfaces can be developed to a variety of control systems and data acquisition units.

7.2.3.2 Data acquisition from the monitoring and control bus and the navigation equipment bus generally will be read only. A gateway will be interposed between the integrated

bridge system bus and the administrative and communications networks. The gateway will provide the necessary hardware and software to enable dialog between the integrated bridge system and the administrative and communication networks platform and to enforce the one-way communication where required. Data flow on the administrative and communication networks generally is unrestricted except as may be limited by the security mode. Access to the integrated bridge system bus will be regulated as noted.

7.2.4 *Communications Services*—The communications manager must serve both remote and local users. To avoid connect-time client server blocking, it should provide for asynchronous dialog with the database server that queues client requests, establishes a link, confirms receipt, and satisfies the queries according to priority without blocking either the client or server. The communications manager provides a common systems interface and support for:

7.2.4.1 Multiple wireless communication services, which may include Inmarsat A, B, M and C; MSAT; ARGOS; Orbcomm; and Mobile Datacom.

7.2.4.2 Radio communications include VHF, HF/MF, and cellular.

7.2.4.3 Route diversification, least cost routing, and carrier choice.

7.2.4.4 Message log and cost allocation.

7.2.5 *SITP Compliance*—SITP compliance is required for software applications to have access to the services of the SITP. APIs will allow SITP compliance for third-party software applications. An SITP compliant software entity will allow for seamless integration into the platform. There will be four levels of compliance based upon the extent of SITP services used:

7.2.5.1 *Level 1:*
Process management,
Logging management,
Messaging management, and
Replication management.

7.2.5.2 *Level 2*—Includes Level 1 plus the following:
Alarm management,
Time management, and
Configuration management.

7.2.5.3 *Level 3*—Includes Level 2 plus the following:
Debug management,
Backup management,
Test management, and
Enterprise management.

7.2.5.4 *Level 4*—Includes Level 3 plus the following:
Health management,
Performance management,
Schedule management, and
Localization management.

7.3 *Application Programming Interfaces*—APIs will be required for third-party applications to use SITP services.

7.3.1 *Overview of APIs*—The term "application programming interface" (API) is defined as a software tool kit that can be used as a building block that facilitates connections primarily between applications and other constituent network software, but that also can provide linkages for other elements of the network (see Fig. 3). The function of the network operating system is to control shared resources and establish transactions among applications. In multivendor networks without commonality, APIs provide the required link.

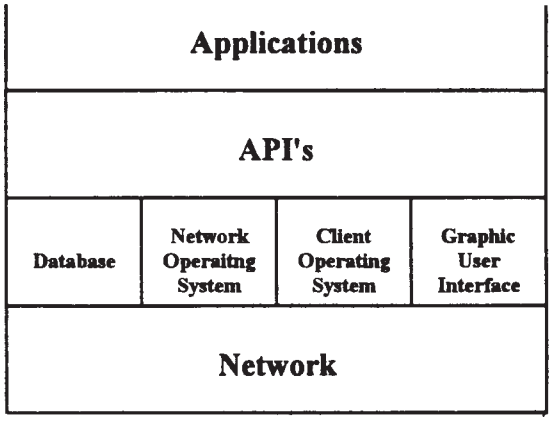

FIG. 3 Conceptual Overview of API Linkages

8. Land-Based Information Technology Platform (LITP)

8.1 The LITP is the control and communication center of FMS. It provides the infrastructure, software, and hardware, necessary to provide computing and communication services for the management of a wide area network (WAN) of SITPs and any auxiliary shoreside installations. The design profile generally will replicate that of the SITPs it manages, expanded, and optimized as required by the size of the fleet. The underlying service, that is network operating system and database management system, as well as the LITP services, provide the same functions as corresponding services of the SITP described in 7.1.2 and 7.2 except as follows:

8.1.1 *Data Acquisition Services*—Typically for the LITP, data acquisition from control systems will not be required.

8.1.2 *Data Management*—The LITP data management function will include acquiring, processing, and warehousing operating data from the various SITPs under its direction. It also may acquire data from any associated shoreside version or from other sources. It will oversee the flow of data to SITPs or LITPs.

8.1.3 *Communications Manager*—The communications manager will support a communications hub with access to land lines that may include telephone, telefax, e-mail, cellular, and land earth stations.

8.1.4 *Configuration Manager*—The configuration manager for the LITP responds to requests to reconfigure elements of the WAN, that is, the SITPs and subsidiary shoreside platforms, as well as to its local network.

9. System Hardware

9.1 The selection of system hardware for both the SITP and the LITP must consider a number of factors that are dependent on the nature and the criticality of the applications supported by the FMS. Guidance to assist the designers in the selection of hardware is provided in Appendix X4.

10. Fault Tolerance

10.1 The level of fault tolerance necessary for each FMS installation should be determined as a function of the criticality

of the applications supported by the system. A description of varying levels of fault tolerance is provided in Appendix X5.

11. Communications Bus

11.1 The communications hub provides the physical interface between the communications software and the various transceivers may include, but are not be limited to, the following:

11.1.1 *Satelite Communications:*

11.1.1.1 *Circuit-Switched Mode*—Inmarsat A, Inmarsat B, Inmarsat M, and MSAT.

11.1.1.2 *Store and Forward Mode*—Inmarsat C and Orbcomm.

11.1.2 *Radio Communications:*

11.1.2.1 *Medium and Long Range*—MF (300 kHz to 3 Mhz); HF (3 to 30 MHz); emergency communication (500 kHz); weather fax; and radio telex.

11.1.2.2 *Short Range*—VHF (30 Mhz to 300 mhz) and cellular.

11.1.3 *GMDSS*—See Appendix X3.

12. Demonstration and Validation

12.1 *General*—Evidence of a satisfactory degree of reliability in the design, manufacture, and installation of the equipment and systems comprising the FMS is to be demonstrated. In general, this demonstration consists of series of certifications, verifications, validations, tests, and trials.

12.2 *Test Philosophy*—Testing shall be of hierarchical nature, moving from the equipment unit level through testing at the integrated system level to final user testing in the installed environment.

12.3 The system hardware will be tested to ensure that no part of the system can be overstressed as by voltage transients during operation or testing, that components are electrically rated compatible with other design constraints to allow for part and parameter variations and transient conditions, and a safe margin in operating temperature.

12.4 *LAN Software Assessment:*

12.4.1 As used in this guide, software assessment refers to the methodology for verification and validation of the FMS software. Verification focuses on the functional design, whereas validation focuses on whether the system satisfies the requirements. Software is difficult to test. In contrast to hardware, it does not wear out, it does not operate within discrete parameters, and testing is largely qualitative and inferential. In addition, redundancy is not an effective backup.

12.4.2 Verification and validation of software products should be carried out for individual products and for the integrated system. There will be a defined software demonstration and validation test plan created for each installation, and the SITP and FMS infrastructure will be tested against that plan. In general, software testing shall be formalized at three points in the development.

12.4.2.1 *Unit Tests*, of individual modules in isolation to verify logic and interface characteristics. This is accomplished concurrently with software development.

12.4.2.2 *Integration Tests*, of the different units to validate interoperability in accordance with design criteria.

12.4.2.3 *Acceptance Tests*, of the complete system, including all features and elements of the software in a fully configured hardware state without any element of simulation and in a normal operating environment.

12.5 *Tests and Trials:*

12.5.1 *Unit Tests (Alpha Testing)*, are white box tests required for testing individual modules and combinations of modules in isolation to verify logic and interface characteristics. They may focus on the lower levels of the protocol and should be started as soon as the software design will permit.

12.5.2 Integration tests are white box tests, the purpose of which is to bring together the various layers or segments of the software and hardware, including communication links and gateways, and to test them step by step as the integration proceeds.

12.5.3 *End User (Acceptance) Tests*—These are tests of the complete system including software and hardware, as well as communication links and gateways. They should be conducted as installed or in simulated environment (mock-up). For the FMS, this will normally include at least one SITP and one LITP. These are black box tests requiring multiple iterations. At a minimum, the following should be included:

12.5.3.1 *Load/Stress Testing*—To confirm the system can handle the peak load conditions, internal and external traffic.

12.5.3.2 *Security Testing*—To reveal weak spots in the system by repeated attempts to defeat the security controls.

12.5.3.3 *Performance Testing*—These tests exercize all of the software applications, communications links, and database management systems.

12.5.3.4 *Hardware Compatability Testing*—To determine the margin of hardware resources, memory, disk space, speed, and so forth, over requirements.

12.5.3.5 *Configuration Testing*—To determine how the systems respond to required alternative configurations in hardware or software.

12.6 *Operation and Maintenance*—This phase will focus on all aspects of system management including:

12.6.1 System configuration and modification,

12.6.2 Anomaly identification and resolution,

12.6.3 Document control (updating),

12.6.4 Communication interfaces,

12.6.5 Latencies, and

12.6.6 Hardware replacement.

13. Human Interface

13.1 In the design of the user interface to the SITPs and the LITP, reference may be to recognized standards.

13.2 *Visual Display Unit (VDU):*

13.2.1 The size, color, contrast, and density of text and graphics should be read or interpreted easily from the operator position under all operational lighting conditions. Typeface should be an internationally recognized simple, clearcut design similar to Helvetica medium.

13.2.2 VDU pages should have a standardized format. Information and functional areas should be presented in a consistent manner.

13.2.3 An overview page or pages should be available to explain the paging system.

13.2.4 Each page should have a unique identifying label shown on the screen.

14. Training and Documentation

14.1 *General*—Regardless of the technical excellence of the FMS software and hardware, operator training is essential to its successful application. The disconnected nature of ship operations serves to emphasize the need for shipboard personnel to be trained in depth on the operation and maintenance of the system.

14.1.1 It is a condition of this guide that formal training in the operation of the FMS is available.

14.1.2 Administrators and users should be trained in and demonstrate their knowledge of step-by-step procedures for operation of the FMS including, to the extent necessary, instructions for associated subsystems, the administrative network functions, ship earth stations, and the land-based communications hub. The program of instruction should include the following at a minimum:

14.1.2.1 Management of local area networks,

14.1.2.2 Management of wide area networks,

14.1.2.3 Client server systems,

14.1.2.4 Network operating systems,

14.1.2.5 All installed hardware,

14.1.2.6 Maintenance and repair,

14.1.2.7 Knowledge of the regulations concerning telecommunications, and

14.1.2.8 Administration of the SITP and FMS systems.

14.2 *Documentation:*

14.2.1 Documentation can be defined as "the aids provided for the understanding of the structure and intended uses of an information system or its components" (ANSI) and system documentation as "the collection of documents that describe the requirements, capabilities, limitations, design, and operation of an information processing system" (ISO). Both definitions are relevant for the purposes of this guide. In addition, the documentation should comply with the provisions of ANSI/IEEE 1063 as a minimum.

14.2.2 User documentation for the SITP may be presented in a tutorial mode and should include detailed instructions for all permitted operations and for such system adjustments or repairs as may be practicable for on board personnel.

14.2.3 Administrator documentation for the FMS should include, in addition to the user documentation, complete reference material necessary to administer the system.

15. Keywords

15.1 communications service; data acquisition service; DBMS (database management system) service; executive services; fleet management system network; land-based information technology platform; network operating system; shipboard information technology platform

APPENDIXES

(Nonmandatory Information)

X1. ACRONYMS

MTS	Automated Maritime Telephone Service
ANSI	American National Standards Institute
AOR	Atlantic Ocean Region (E–East, W–West)
API	Application Programming Interface
ARPA	Advance Research Projects Agency
ASCII	American Standard Code for Information Interchange
BIOS	Basic Input/Output System
CCITT	Consultative Committee for International Telegraphy and Telephony
CES	Coast Earth Station
CISPR	Comité International Special des Peturbations Radioelectrique (International Special Committee on Radio Interference)
CMIP	Common Management Information Protocol
CRS	Coast Radio Station
DMA	Direct Memory Access
DSC	Digital Selective Calling
EBCDIC	Extended Binary Coded Decimal Interchange Code
EGC	Enhanced Group Call
ECMA	European Computer Manufacturers Association
EDI	Electronic Document Interchange
EIA	Electronic Industries Association
EMI	Electromagnetic Interference
EPIRB	Emergency Postion-Indicating Radio Beacons
FCC	Federal Communications Commission
FDDI	Fiber Distributed Data Interface
FIPS	Federal Information Processing Specification
FMS	Fleet Management System
FTP	File Transfer Protocol
GMDSS	Global Maritime Distress and Safety Systems
GOSIP	Government OSI Profile
GUI	Graphical User Interface
HF	High Frequency (see Appendix X2)
HVAC	Heating, Ventilation and Air Conditioning
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronic Engineers
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ITE	Information Technology Equipment
ITU	International Telecommunications Union
IVD	Integrated Voice and Data
Kbps	Kilo bits per second
KBps	Kilo bytes per second
LAN	Local Area Network
LF	Low Frequency (see Appendix X2)
MAC	Medium Access Control (OSI physical layer)
MAN	Metropolitan Area Network
MAP	Manufacturing Automation Protocol
MAPI	Message Application Programming Interface
Mbps	Million bits per second
MBps	Million bytes per second
MF	Medium Frequency (see Appendix X2)
MIPS	Million Instructions per Second
MTBF	Mean Time Between Failure
NBDP	Narrow Band Direct Printing
NETBIOS	Network Basic Input Output System
NFS	Network File Server
NFT	Network File Transfer

NMEA	National Marine Electronics Association
OS/2	Operating System/2
OSIRM	Open Systems Interconnection Reference Model
PC	Personal Computer
POSIX	Operating system developed by IEEE as Standard 1003
PSDN	Packet Switching Data Network
PSN	Packet Switching Network
RAID	Redundant Array of Inexpensive Discs
RAM	Random Access Memory
RFI	Radio Frequency Interference
RISC	Reduced Instruction Set Computer
RMON	Remote Monitoring of Networks
ROM	Read Only Memory
RS-232C	An EIA standard 25-pin connector for computer/terminal interface for signal rates up to 20 kbps
RS-422	An EIA standard 5-pin connector for signal rates up to 20 kbps
RS-449	An EIA standard for 9- and 37-pin connectors for signal rates up to 2 Mbps
Rx	Receiver
SART	Search and Rescue Transponder
SCSI	Small Computer Systems Interface
SES	Ship Earth Station
SITP	Shipboard Information Technology Platform
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSB	Single-Side Band
UHF	Ultra High Frequency (see Appendix X2)
VHF	Very High Frequency (see Appendix X2)
VTS	Vessel Traffic Service
WAN	Wide Area Network

X2. RELATED DOCUMENTS

X2.1 *ISO Standards:*[4]

ISO 9000 Quality Management and Quality Assurance Standards–Guidelines for Selection and Use

ISO 9001 Quality Systems–Model for Quality Assurance in Design/Development, Production, Installation and Servicing

ISO 9000-3 Quality Management and Quality Assurance Standards–Guidelines for the Application of 9001 to the Development, Supply and Maintenance of software

ISO/IEC 8802-3 Information Technology–Local and Metropolitan Area Networks–Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications (Ethernet)

ISO/IEC 8802-4 Information Processing Systems–Local Area Networks–Part 4: Token Passing Bus Access Method and Physical Layer Specifications

ISO/IEC 9075 Information Technology–Database Languages–SQL

ISO 8073 Transport Layer Connection-Oriented Services for the OSI Reference Model

ISO 8602 Transport Layer Connectionless Services for the OSI Reference Model

ISO 8326/27 Session Layer Connection-Oriented Services for the OSI Reference Model

ISO 9548 Session Layer Connectionless Services for the ISO Reference Model

ISO 8822/23 Presentation Layer Connection-Oriented Services for the OSI Reference Model

ISO 9576 Presentation Layer Connectionless Services for the OSI Reference Model

ISO 10020/21 ISO Standard for Message Handling Services Based on the CCITT X.400 Standard

ISO 8571 ISO Definition of the File Transfer, Access and Management (FTAM) Application

X3. OVERVIEW OF RADIOCOMMUNICATIONS EQUIPMENT REQUIRED FOR GMDSS

X3.1 See Fig. X3.1 for an overview of radiocommunications equipment required for GMDSS.

Sea area - A1 (Approx. 20-30 miles from land within VFH Range)	Sea area - A2 (Approx. 100 miles from land within VHF Range	Sea area - A3 Within Coverage of INMARSAT Sattelite	Sea area - A4 (All other areas outside A1, A2 and A3)
1. VHF Radiotelephone	1. VHF Radiotelephone	1. VHF Radiotelephone	1. VHF Radiotelephone
2. VHF DSC on channel 70 and printer	2. VHF DSC on channel 70 and printer	2. VHF DSC on channel 70 and printer	2. VHF DSC on channel 70and printer
3. VHF DSC watch receiver	3. VHF DSC watch receiver	3. VHF DSC watch receiver	3. VHF DSC watch receiver
4. SART - minimum of two	4. SART - minimum of two	4. SART - minimum of two	4. - minimum of two
5. NAVTEX	5. NAVTEX	5. NAVTEX	5. NAVTEX
6. EGC if outside NAVTEX coverage	6. EGC and printer if outside NAVTEX coverage	6. EGC and printer if outside NAVTEX coverage	
7. 406 MHz EPIRB	7. 406 MHz EPIRB	7. 406 MHz EPIRB	6. 406 MHz EPIRB
8. VHF two-way radiotelephone apparatus a. two req'd. for ships 300 < grt < 500 b. three req'd. for ships ≥ 500 grt	8. VHF two-way radiotelephone apparatus a. two req'd. for ships 300 < grt < 500 b. three req'd. for ships ≥ 500 grt	8. VHF two-way radiotelephone apparatus a. two req'd. for ships 300 < grt < 500 b. three req'd. for ships ≥ 300 grt	7. VHF two-way radiotelephone apparatus a. two req'd. for ships 300 < grt < 500 b. three req'd. for ships ≥ 300 grt
9. 2182 kHz watch keeping Rx - until 1999-02-01	9. 2182 kHz watch keeping Rx - until 1999-02-01	9. 2182 kHz watch keeping Rx - until 1999-02-01	8. 2182 kHz watch keeping Rx - until 1999-02-01
	10. MF radiotelephone with DSC Rx and controller	10. MF radiotelephone with DSC Rx and controller	9. Auto. direction finder 2182 kHz
	11. MF watch receiver dedicated to 2187.5 kHz	11. MF watch receiver dedicated to 2187.5 kHz	10. Two MF/HF radiotelephones with DSC
	12. Auto. direction finder 2182 kHz	12. Auto. direction finder 2182 kHz	11. Telex using narrow band direct printing
	13. MF DSC encoder/decoder	13. MF DSC encoder/decoder	12. MF DSC encoder/decoder
		14. Plus either a) Two Inmarsat A SatComs or b) Two Inmarsat C SatComs or c) Inmarsat A & C d) Inmarsat A+ MF/HF + telex or e) Inmarsat C + MF/HF radiotelephones + telex or f) Two MF/HF radiotelephones with DSC receiver and controller for HF	

FIG. X3.1 Overview of Radiocommunications Equipment Required for GMDSS

X4. SYSTEM HARDWARE

X4.1 *Electromagnetic Interference (EMI)*—Equipment to be situated in a shipboard open deck environment must be considered as exposed to high levels of radiated and conducted EMI. Because of a large glass area, the enclosed navigating bridge is treated as an open deck area. The sources of EMI can be classed as intentional emitters and nonintentional emitters. Nonintentional emitters are limited by standard to a level of 10V/m radiated EMI under test conditions. Intentional emitters, which include radar, radio, and so forth, generally are not limited as to radiated strength or direction. In addition to fixed emitters, the navigating bridge area routinely is exposed to radiation from mobile emitters, such as, walkie talkies, with levels of EMI potentially hostile to sensitive electronic equipment. See IEC 945 and IEC 533.

X4.2 *Physical Layer:*

X4.2.1 *Topology*—The topology of a network is defined by the logical configuration of the nodes and the interconnecting branches.

X4.2.1.1 *Star*—In practice, the practical execution for both bus and ring topologies is often star shaped with arms radiating from a central hub to each node or station. The wiring within the hub is connected so that logically the system behaves as a bus or ring. This arrangement allows for diagnosing and isolating faulted circuits or equipment without closing down the entire network.

X4.2.1.2 *Bus*—The bus (see Fig. 1) is the predominate topology found in LANs generally in conjunction with the Ethernet protocol and using STP cabling. The nodes share the bus, and as a result, only one station can broadcast at a time requiring some form of access control, which is provided by the Ethernet protocol. In the simplest form, transmissions from one node can be read at all the other nodes. The effective maximum transmission speed for the standard Ethernet configuration is about 8 Mbps, and this drops rapidly as traffic increases. This speed can be doubled by duplexing. Switched Ethernet provides each device with its own segment so that it has access to 10-Mbps bandwidth without contention.

X4.2.1.3 *Ring*—The ring network is characteristic of the token ring protocol. Although commonly shown in ring form, the practical execution is a star-shaped assembly which behaves logically like a ring. Arms from a central concentrator, the multistation access unit (MSAU), radiate to each station. Implementation should be in accordance with IEEE 8802.5 at 16 Mbps over STP.

X4.2.2 *Cabling*—The type of cable to be used will be governed by the length of the cable, the electromagnetic environment, and the bandwidth.

X4.2.2.1 *Copper:*

(*a*) *Twisted Pair*—Available as "Unshielded Twisted Pair"—UTP or as "Shielded Twisted Pair"—STP. UTP is not protected against noise caused by radiated EMI and generally is not suitable for shipboard use for this reason. STP is provided with a shield of copper foil or copper braid to reduce system noise as a result of radiated EMI.

(*b*) *Coax*—The cable consists of insulated central conducting solid copper core surrounded by one or more foil or mesh shields separated by insulation. The central conducting core carries the signal and the shield provides the ground. Coax cable is available as thick coax (10Base5 has been applied as the network backbone) or thin coax (10Base2).

X4.2.2.2 *Optical Fibers*—Optical fibers possess three important advantages over copper conductors:

(*a*) Immunity to noise from radiated or conducted EMI;

(*b*) Very high transmission speeds—100 Mbps over paths of up to 2 km for glass fibers. This is the medium of choice for backbone service; and,

(*c*) Improved security.

Also available with plastic fibers, but with speeds limited to under 10 Mbps and paths of less than 100 m.

X4.3 *Servers*—The standard configuration for the shipboard local area network will comprise a process server, a communications server, and a database server, which may be allocated to one or more computers. Estimated minimum requirements for the computer(s)/servers are:

X4.3.1 *Processor:*

X4.3.1.1 Speed—90 mhz,

X4.3.1.2 Two instructions per clock cycle,

X4.3.1.3 45 MFLOPS (floating point operations/second), and

X4.3.1.4 Scalable.

X4.3.2 *Memory (RAM)*, 40-MB ECC (error, checking, correcting, and reporting).

X4.3.3 *Storage Devices:*

X4.3.3.1 1.05-GB hot swap fast SCSI-2 disk,

X4.3.3.2 3.5-in., 1.44-MG floppy disk drive, and

X4.3.3.3 CD-ROM—internal SCSI-2, E.4X.

X4.3.4 *Network Interface Card.*

X4.3.5 *Color Monitor (Video Display Unit):*

X4.3.5.1 15 in., high resolution, integrated 800 × 600, noninterlaced, refresh rate 72 MHz; and,

X4.3.5.2 512-KB standard video memory.

X4.3.6 *Graphic Card.*

X4.3.7 *Multimedia Sound System Support.*

X4.4 *Workstations*—Two workstations should be provided. While nominally acting as client, workstations may in addition be configured as servers. When configured in this manner, the requirements of X4.3 would apply. The following apply to a stand-alone workstation:

X4.4.1 *Processor:*

X4.4.1.1 Speed 75 MHz and

X4.4.1.2 Scalable.

X4.4.2 *Memory (RAM)*, 16-MB ECC.

X4.4.3 *Storage Devices:*

X4.4.3.1 540-MB fast SCSI-2 hard disk;

X4.4.3.2 3.5- in., 1.44-MB floppy disk drive; and

X4.4.3.3 CD-ROM, internal SCSI-2, quad speed.

X4.4.4 *Network Interface Card.*

X4.4.5 *Graphic Card.*

X4.4.6 *Multimedia Sound Support System.*

X4.4.7 *Color Monitor*, see X4.3.5.

X4.5 *Power Sources*—The power supply from the ship's mains may be subject to the variations given in Table X4.1 (see also IEC 92.101):

X4.5.1 Power supply to SITP may be arranged as follows:

X4.5.1.1 From ship's main or emergency power supply with power conditioner as required to provide the required quality and backed up by a closed transition uninterruptible power supply with a minimum reserve capacity of 15 min.

X4.5.1.2 An on-line uninterruptible power supply with a minimum reserve capacity of 15 min supplied from the ship's main with closed transition backup.

X4.6 *Embedded Programs*—Embedded programs should be documented using the following format:

X4.6.1 The procedure's actual calling name from within the program should be listed along with a one-line description statement for the calling name. The statement's purpose is to describe clearly the task associated with the procedure's name.

X4.6.2 A list of input/output parameters, a description statement for each parameter that describes the task associated with the parameter's name, a statement as to whether the parameter is an input or an output of the procedure, and a range of valid values for each parameter that may be passed into or out of the procedure.

X4.6.3 A list of calling/called procedures, a description statement for each procedure that describes the task associated with the procedure's name (this statement should be the same as the one describing the procedure's calling name), a statement as to whether the procedure is called from within the routine or is the caller of the routine, and the name of the module in which the calling/called procedure can be found.

TABLE X4.1 Power Sources Variations

NOTE 1—Voltage and frequency variations may occur simultaneously. Total harmonic loading—5 %. Harmonic loading at any single frequency—3 %.

Parameter	Permanent, %	Transient	
		%	Recovery Time, s
Voltage	+6, −10	±20	1.5
Frequency	±5	±10	5

X4.6.4 A synopsis describing the program flow for the procedure. This synopsis should be a detailed, plain language narrative of what the code is doing.

X4.6.5 A revision history for the procedure that includes the data and a description of the change. The description should include the new revision level for the overall program that has resulted from the module modification.

X4.7 *Environmental Conditions*—The following are to be considered minimum levels. If the equipment is to be part of a system subject to regulatory body approval, then the requirements of the regulatory body, if stricter, will apply.

X4.7.1 *Temperature Range*, operating: 5 to 40ºC.

X4.7.2 *Humidity*, operating (5 to 40ºC): 15 to 80 % relative humidity.

X4.7.3 *Vibration*, operating random: 0.2 g for 5- to 100-Hz survival random: 2 g for 5 to 100 Hz.

X4.7.4 *Electromagnetic Compatibility (EMC)*, to meet CISPR 22 Class B ITE or equivalent.

X4.7.5 *Ship's Motion*, operational in any position up to 90°.

X5. FAULT TOLERANCE

X5.1 The purpose of fault tolerance is to minimize the impact of hardware or software failures on the network and particularly to prevent the loss of data. The following is a description of several of the methods of backup that may be considered.

X5.2 *"Hot Swap" Backup*—This allows continuous use while replacing a failed drive.

X5.2.1 *Disk Mirroring*—This system provides for everything to be written to two disks simultaneously; if the primary disk fails, the standby disk can take over automatically. In this system, both disks are served by a single controller.

X5.2.2 *Disk Duplexing*—This system provides for everything to be written to two disks simultaneously as in disk mirroring, but each disk has a dedicated controller for an added level of protection.

X5.2.3 *RAID 1*—This is the same as disk mirroring (see X5.2.1).

X5.2.4 *RAID 5*—RAID 5 can read and write blocks of information to different disks in an array, and it distributes parity information over all disks in the array. Parity is a mathematical representation of data held in the array.

X5.3 *Tape Backup*—On-line tape backup is an option for multitasking operating systems. Tape backup does not provide "hot swap" capability, and data must be reentered after a drive failure. Also on-line tape backup may slow the system operation to an unacceptable degree.

X5.3.1 *¼-in. Tape*, capacities to about 500 Mbytes.

X5.3.2 *Digital Audio Tape (DAT)*, capacities to about 4 Gbytes (8 Gbytes with data compression).

X5.3.3 *Video*, 8 technology, capacities to about 5 Gbytes. This is based on 8–track, 8–mm tape cartridges used in video camcorders.

X6. FIXED ANTENNAS

X6.1 *Scope*—This appendix is intended to provide information of the types of fixed antennas commonly provided for navigation, communication, and collision avoidance.

X6.2 *Classes*—For purposes of this appendix, the following classes of antennas are considered:

X6.2.1 *Omnidirectional Transmitting.*

X6.2.2 *Omnidirectional Receiving.*

X6.2.3 *Directional Transmitting.*

X6.2.4 *Directional Receiving.*

X6.2.5 *Rotating Transmitting/Receiving.*

X6.3 *Required Antenna Installations for Ocean Area A3 (Typical):*

System	Type Antenna
Statcom A and B, suitable for telex, telephony, data and voice communication	Automatic directional transmitting/receiving, 1.5 to 1.65 GHz
Statcom C, telex only	Omnidirectional, 1.5 to 1.65 GHz
Satnav	Omnidirectional whip antenna
X-band radar system	Rotating transmitting/receiving—10 cm
S-band radar system	Rotating transmitting/receiving—3 cm
MF/HF transceiver for telephony, digital selective calling, direct printing telegraphy, general communications, range <500 km	Large whip antenna as main with wire antenna as reserve
MF/HF watch receiver 2182 kHz	Same as above
MF alarm generator	Whip antenna
MF 2182-kHz direction finder	DF loop aerial and a short wire or whip
Navtex system	Whip
Inmarsat EGC receiver	Whip
VHF transceivers	Whip
VHF watch receiver	Whip

X6.4 *References:*

X6.4.1 *Radio Regulations of the International Telecommunication Union*, Geneva 1976.

X6.4.2 *CCIR Recommendation 45*, avoidance of interference from ship's other radio communication apparatus on board.

X6.4.3 *International Convention for the Safety of Life at Sea*, 1974 as amended, Chapters III and IV.

X6.5 *Types of Antennas:*

X6.5.1 *Omnidirection Antennas.*

X6.5.2 *Radio Transmitting Antennas:*

X6.5.2.1 *Wire Antennas:*
(*a*) LF communication, 30 to 300 kHz.
(*b*) MF communication, 300 kHz to 3 MHz.
(*c*) Emergency communication, 500 kHz.
X6.5.2.2 *Whip and Dipole Antennas:*
(*a*) MF communication, 300 kHz to 3 MHz.
(*b*) HF communication, 3 to 30 MHz.
(*c*) VHF communication, 30 to 300 MHz.
(*d*) UHF communication, 300 MHz to 3GHz.
(*e*) Facsimile receiver, 3 to 30 MHz.
X6.5.3 *Radio/Television Receiving Antennas:*
X6.5.3.1 *Wire Antennas:*
(*a*) LF communication, 30 to 300 kHz.
(*b*) MF communication, 300 kHz to 3 MHz.
(*c*) Emergency communication, 500 kHz.
X6.5.3.2 *Omnidirectional Radio and Television Central Antennas.*
X6.5.4 *Satellite Communication:*
X6.5.4.1 *Satcom A and B*, telex, telephony, data and voice communication, automatic 1.5 to 1.65 GHz.
X6.5.5 *Directional Transmitting/Receiving Antennas:*
X6.5.5.1 *Satcom C*, data and telex only, omnidirection antenna, 1.5 to 1.65 GHz.
X6.5.6 *Navigational Antennas*
X6.5.6.1 *Hyperbolic Navigation Antennas:*
(*a*) Omega System, 10 kHz.
(*b*) Loran System, 100 kHz.
(*c*) Decca System, 84 to 130 kHz.
X6.5.7 *Global Positioning System (GPS):*
L1 band—1575.42 MHz
L2 band—1227.6 MHz
X6.5.8 *Navigational Radar Antennas.*
X6.5.9 *Rotating Transmitting/Receiver Antenna:*
X band navigation radar, 8 to 12 GHz
S band navigation radar, 3 to 4 GHz

ASTM International takes no position respecting the validity of any patent rights asserted in connection with any item mentioned in this standard. Users of this standard are expressly advised that determination of the validity of any such patent rights, and the risk of infringement of such rights, are entirely their own responsibility.

This standard is subject to revision at any time by the responsible technical committee and must be reviewed every five years and if not revised, either reapproved or withdrawn. Your comments are invited either for revision of this standard or for additional standards and should be addressed to ASTM International Headquarters. Your comments will receive careful consideration at a meeting of the responsible technical committee, which you may attend. If you feel that your comments have not received a fair hearing you should make your views known to the ASTM Committee on Standards, at the address shown below.

This standard is copyrighted by ASTM International, 100 Barr Harbor Drive, PO Box C700, West Conshohocken, PA 19428-2959, United States. Individual reprints (single or multiple copies) of this standard may be obtained by contacting ASTM at the above address or at 610-832-9585 (phone), 610-832-9555 (fax), or service@astm.org (e-mail); or through the ASTM website (www.astm.org).