INTERNATIONAL STANDARD

ISO 15849

First edition
2001-11-01

AMENDMENT 1
2003-09-01

Ships and marine technology — Guidelines for implementation of a fleet management system network

AMENDMENT 1: Annex A

Navires et technologie maritime — Lignes directrices pour la mise en œuvre d'un système de management d'une flotte par réseau

AMENDEMENT 1: Annexe A

Reference number
ISO 15849:2001/Amd.1:2003(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

Amendment 1 to ISO 15849:2001 was prepared by Technical Committee ISO/TC 8, *Ships and marine technology*, Subcommittee SC 10, *Computer applications*.

Introduction

Annex A indicates an example of the specifications for the design of the software of the Application Program Interface (API) when it is applied to the SITP and the LITP, as required by the main text of ISO 15849 (Guidelines for the Fleet Management System Network, FMSN) to secure the effective execution of the mutual connectivity with transparency.

Ships and marine technology — Guidelines for implementation of a fleet management system network

AMENDMENT 1: Annex A

Annex A
(informative)

Example of specifications for the design of the software of the Application Program Interface (API) when it is applied to the SITP and LITP

A.1 Scope

The scope of this Annex is the software design guide for the purpose of applying the API for the functions of the SITP and the LITP that are specified in the main text of ISO 15849.

In this Annex, the concept is based on the use of CORBA (A.2.3) as the specification of a distributed object for a model.

A.2 Terms and definitions

For the purposes of this Annex, the following terms and definitions apply.

A.2.1
acquire data list
operation of acquiring the data list from the database, on the specified server

A.2.2
acquire ship information
polling operation from the specified server

A.2.3
CORBA
Common Object Request Broker Architecture
standard of distributed object model as defined by the Object Management Group

A.2.4
database server
station which became independent of the LITP-installed system and the SITP-installed system, when a database is arranged on this station

A.2.5
IDL
Interface Definition Language

language to define interface in each operation

NOTE CORBA's primary tool to insulate language.

A.2.6
IDL skeleton
when CORBA is used and the client and server communicate, a program (as a part of API) on the server side to provide an application program to start the operation directly

A.2.7
IDL stub
when CORBA is used and the client and server communicate, the client program that accesses the operation on the server side provided with the corresponding pseudo-object (as a part of API) on the client side

A.2.8
naming service
common reference service provided by CORBA

NOTE The naming service responds to the inquiry from the object, relating the name of the object to its location in the network.

A.2.9
naming service interface
program, which executes the API request from the user application, in the series of processes when a naming service is used

A.2.10
OMG
Object Management Group
international standardization group which prescribes technology for the infrastructure which is necessary for the development of the application in the environment of the dispersion of object oriented architecture and independent of the hardware

A.2.11
ORB
Object Request Broker
software which provides the tasks of communication between stub and skeleton

A.2.12
read data
operation of reading one particular datum from the database, on the specified server

A.2.13
user application
program, which is established by the user of the FMSN in accordance with the requirement by the LITP-installed system to realize the functionality on the FMSN

NOTE The functionality on the FMSN serves to acquire the operational management information and/or the ship management information.

A.2.14
user-application interface
interface in the API opened between the API and user application

NOTE This also defines four kinds of operation (Read data, Write data, Acquire data list and Acquire ship information) as described in the A.4.1.2 to A.4.3.2.

A.2.15
write data
operation of writing one particular datum to the database, on the specified server

A.3 Objectives

See 7.2 “Overview of APIs” in the main text.

For design of the software of the API, the following objectives should be considered:

a) make the system platform transparent to the programming language and development environment of the application;

b) provide links to external operating system;

c) provide links to external networks;

d) provide transparency to distributed objects;

e) provide an easy interface between the user application and the API;

f) provide a data structure of the information that is used for the communication between an application and the API, using a common method of data exchange.

A.4 Software configuration

A.4.1 LITP

A.4.1.1 Illustration

The LITP software configuration is schematically shown in Figure A.1, surrounded by a dotted line.

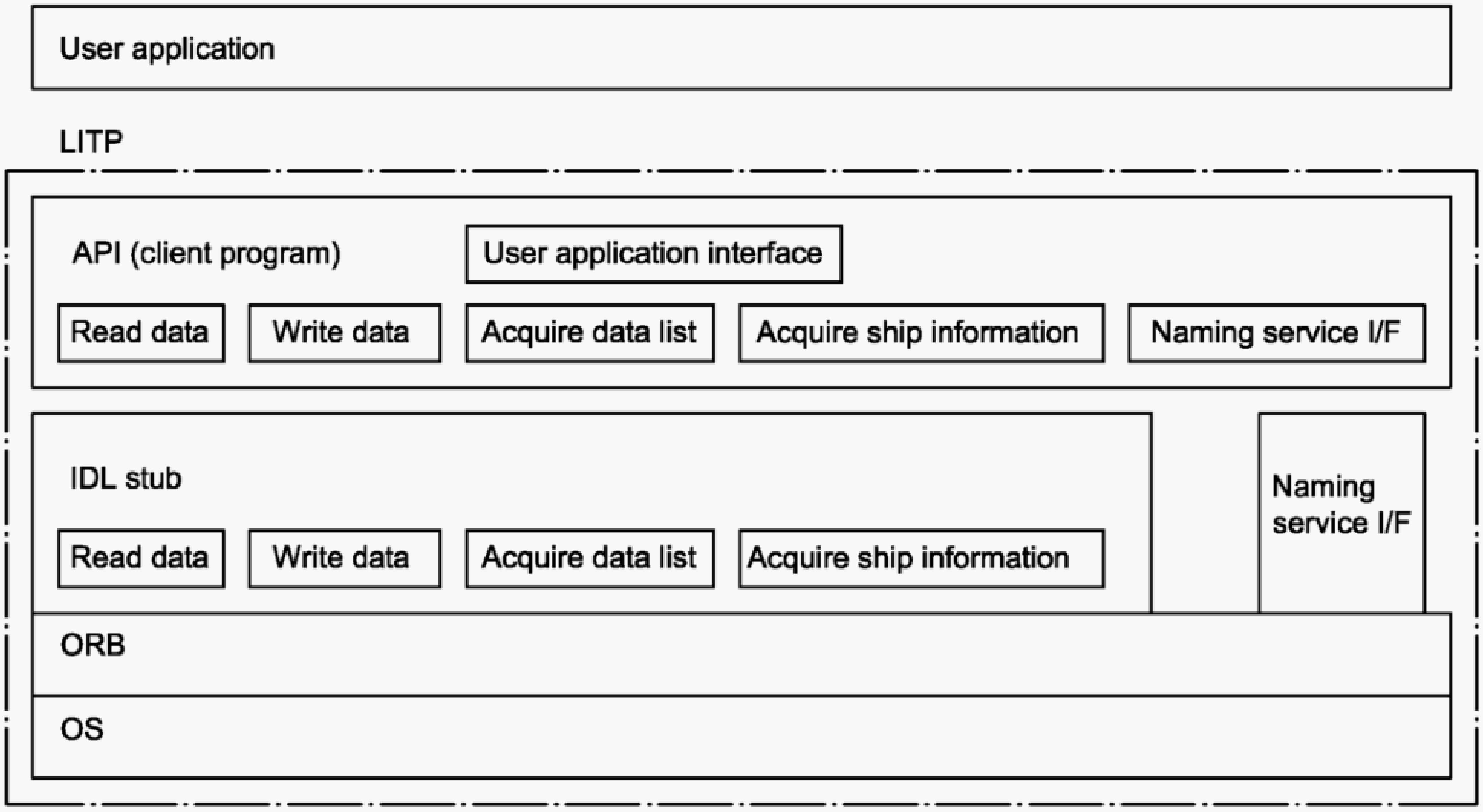


Figure A.1 — Example of construction of software of the LITP-installed system

A.4.1.2 API software block

— User application interface

A requirement from the user application invokes the operation.

— Read data

Invokes a program for accesses for the read data operation in the IDL stub block.

— Write data

Invokes a program for accesses for the write data operation in the IDL stub block.

- Acquire data list

  Invokes a program for accesses for the acquire data list operation in the IDL stub block.

- Acquire ship information

  Invokes a program for accesses for the acquire ship information operation in the IDL stub block.

- Naming service interface

  Naming service provided by ORB is invoked and Object reference of the server is assigned.

A.4.1.3 IDL stub block

- Read data

  It requests the invocation of an operation program for the read data on the server (SITP-installed system) to the ORB.

- Write data

  It requests the invocation of an operation program for the write data on the server (SITP-installed system) to the ORB.

- Acquire data list

  It requests the invocation of an operation program for the acquire data list on the server (SITP-installed system) to the ORB.

- Acquire ship information

  It requests the invocation of an operation program for the acquire ship information on the server (SITP-installed system) to the ORB.

A.4.1.4 Naming service

It acquires the Object reference for the server (SITP-installed system or on the network of one's station).

A.4.2 SITP

A.4.2.1 Illustration

The SITP software configuration is schematically shown in Figure A.2.

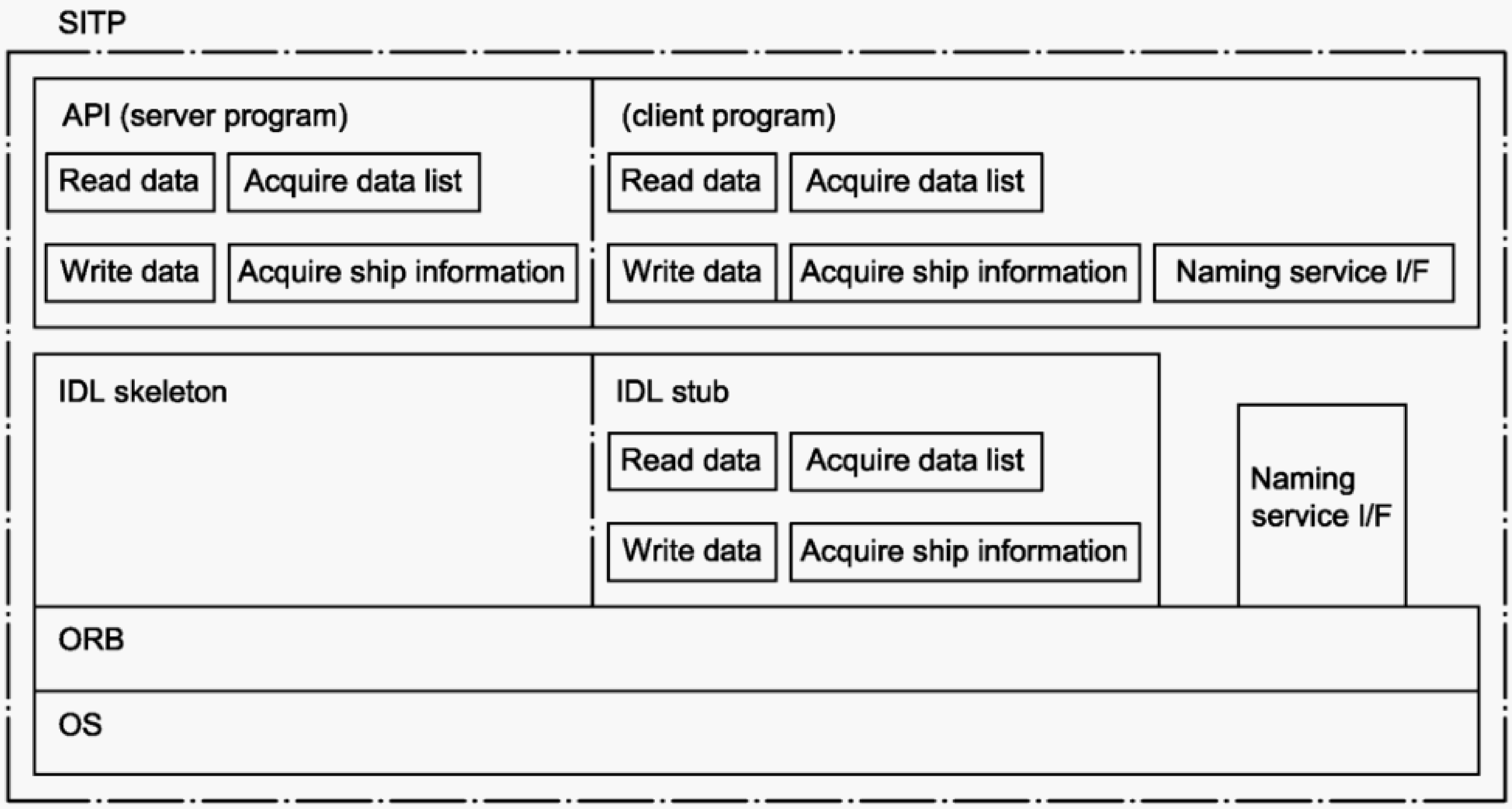


Figure A.2 — Example of construction of software of the SITP-installed system

A.4.2.2 API server program block

- Read data

  The read data operation requests, which are received from the client of the LITP-installed system, are then transmitted to a client program.

- Write data

  The write data operation requests, which are received from the client of the LITP-installed system, are then transmitted to a client program.

- Acquire data list

  The acquire data list operation requests, which are received from the client of the LITP-installed system, are then transmitted to a client program.

- Acquire ship information

  The acquire ship information operation requests, which are received from the client of the LITP-installed system, are then transmitted to a client program.

A.4.2.3 API client program block

- User application interface

  A requirement from the user application is transmitted to the server, and invokes the operation.

- Read data

  Invokes a program for accesses for the read data operation in the IDL stub block.

- Write data

  Invokes a program for accesses for the write data operation in the IDL stub block.

- Acquire data list

  Invokes a program for accesses for the acquire data list operation in the IDL stub block.

- Acquire ship information

  Invokes a program for accesses for the acquire ship information operation in the IDL stub block.

- Naming service interface

  Invokes a Naming service operation, provided by ORB, and acquires the Object reference for the server.

- IDL skeleton

  Requirements of each operation, which are issued from the client program of the LITP-installed system, are transmitted to the API server program.

A.4.2.4 IDL stub block

- Read data

  It requests the invocation of an operation program for the read data on the database server to the ORB.

- Write data

  It requests the invocation of an operation program for the write data on the database server to the ORB.

- Acquire data list

  It requests the invocation of an operation program for the acquire data list on the database server to the ORB.

- Acquire ship information

  It requests the invocation of an operation program for the acquire ship information on the database server to the ORB.

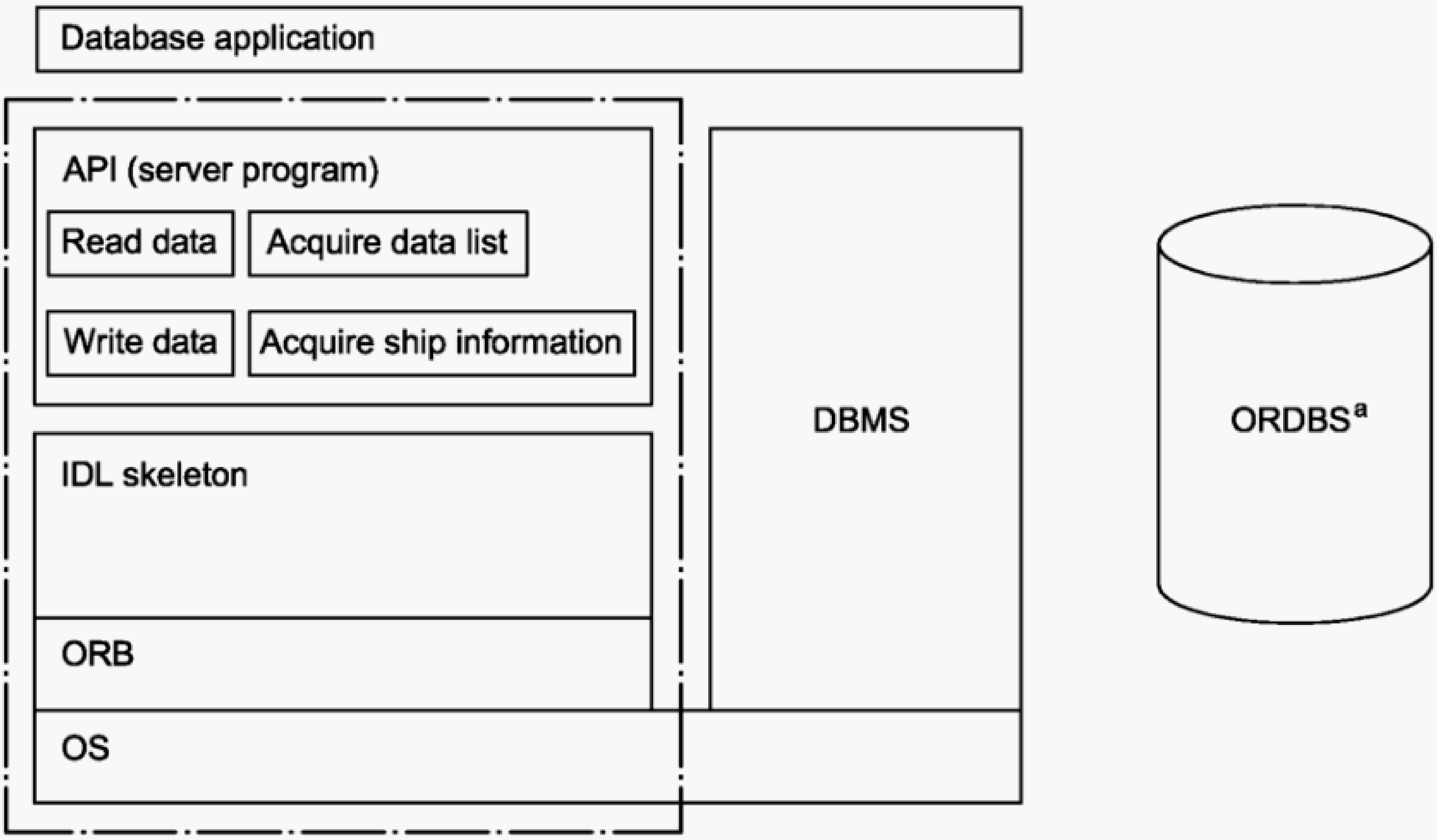
A.4.2.5 Naming service

It acquires the Object reference for the database server.

A.4.3 Database server

A.4.3.1 Illustration

The database server software configuration is schematically shown in Figure A.3, surrounded by a dotted line.



[a] ORDBS: Object Relational Data Base System

Figure A.3 — Example of construction of software of the data base server

A.4.3.2 API server program block

- Read data

  It requests the operation of the read data from the database with transferring the requirement of the read data operation from the client to the User application.

- Write data

  It requests the operation of the write data from the database with transferring the requirement of the write data operation from the client to the User application.

- Acquire data list

  It requests the operation of the acquire data list from the database with transferring the requirement of the acquire data list operation from the client to the User application.

- Acquire ship information

  It requests the operation of the acquire ship information from the database with transferring the requirement of the acquire ship information operation from the client to the User application.

A.4.3.3 IDL skeleton

Operation requests, which are issued from the client program, are transmitted to the API server program.

A.5 Function of the Software block

For convenience in this Annex, the examples assume that the transmission and reception of the FMSN data on the LITP and the SITP are evoked by the client requirement from the LITP only.

As for the SITP-installed system, both the client function, which transfers the requirement to the data base server, and the server function, which accepts a requirement from the LITP-installed system, are implemented. The server station does not always have the data items which FMSN handles.

An example of an operational timing chart on the system is shown in Figure A.4.

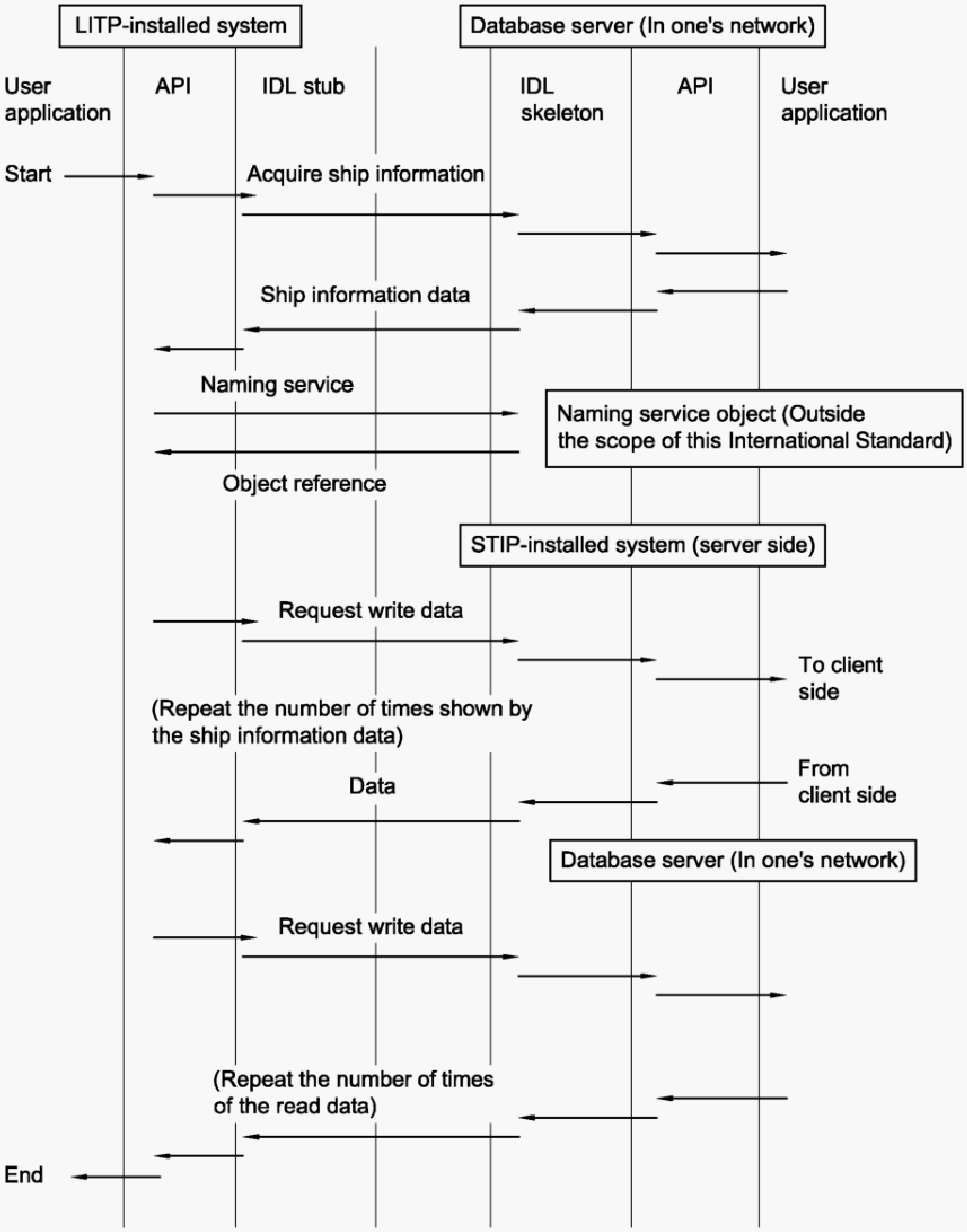

LITP-installed system
Database server (In one's network)
User application
API
IDL stub
IDL skeleton
API
User application
Start
Acquire ship information
Ship information data
Naming service
Naming service object (Outside the scope of this International Standard)
Object reference
STIP-installed system (server side)
Request write data
To client side
(Repeat the number of times shown by the ship information data)
Data
From client side
Database server (In one's network)
Request write data
(Repeat the number of times of the read data)
End

Figure A.4 — Example of system operation

ICS 35.240.60; 47.020.99

Price based on 9 pages

INTERNATIONAL STANDARD

ISO 15849

First edition
2001-11-01

Ships and marine technology — Guidelines for implementation of a fleet management system network

Navires et technologie maritime — Lignes directrices pour la mise en oeuvre d'un système de management d'une flotte par réseau

Reference number
ISO 15849:2001(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.ch
Web www.iso.ch

Printed in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

International Standard ISO 15849 was prepared by Technical Committee ISO/TC 8, *Ships and marine technology*, Subcommittee SC 10, *Computer applications*.

Introduction

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

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

It is the intent of this International Standard to provide guidelines for the design and implementation of an open client/server architecture for computer and communication networks for shipboard and shore-based applications, as well as guidelines to application software providers to allow ready integration of software applications.

Furthermore, it is the intent of this International Standard to provide guidelines that will promote and enable remote support of the shipboard data systems/networks from support offices ashore.

This International Standard is also 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 installations.

Ships and marine technology — Guidelines for implementation of a fleet management system network

1 Scope

This International Standard provides an overview and guide for the selection and implementation by shipowners and operators of a fleet management system (FMS) network of computer services. This includes

a) guidelines for the general infrastructure, including wide area network, data transmission services and common database facilities,

b) guidelines for the shipboard installations, including services to application programs, and

c) guidelines for land-based installations, including services to application programs.

This International Standard does not purport to address the requirements for safety-related systems, e.g. navigation, radio communication as well as systems used to control the operation of the ship.

This International Standard does not purport to address any of the environmental considerations associated with the use of the fleet management system.

2 Terms and definitions

For the purposes of this International Standard, the following terms and definitions apply.

2.1
application program
computer program that performs a task related to the process being controlled rather than to the functioning of the computer itself

2.2
application program interface
API
software tool kit that can be used as a building block that facilitates connections primarily between applications and other constituent network software, but that can also provide linkages for other elements of the network

2.3
black box test
test that is based on the design application and does not require a knowledge of the internal program structure

2.4
certification
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

2.5
client/server database engine
commercial database management system serving as a repository for all critical ship operating and configuration information

2.6

client/server architecture

architecture of computers called servers that manage shared resources and provide access to those shared resources as a service to their clients

2.7

computer system

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

2.8

fault tolerance

built-in capacity of a system to provide continued correct execution in the presence of a limited number of hardware or software faults

2.9

independent

independent, as applied to two systems, means that either system will operate with the failure of any part of the other system

2.10

interface

interface attribute describes the methods and rules governing interaction between different entities

2.11

land-based communications hub

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

2.12

ship earth station

mobile earth station for maritime satellite service located aboard a ship

2.13

software

programs, procedures, rules and associated documentation pertaining to the operation of a computer system

2.14

validation

test and evaluation of an integrated computer system (hardware and software) to ensure compliance with the functional, performance and interface requirements

2.15

ship information technology platform

SITP

integrated system of software, hardware, communication links and standardized procedures that provide common services to shipboard systems in a standardized form

2.16

verification

process to determine if the product of each phase of the digital computer system development process satisfies the requirements set by the previous phase

2.17

white box test

test where the test plan is based on knowledge of the internal structure of the module being tested

See **black box test** (2.3)

2.18

workstation

computer and associated visual display unit (monitor) configured as an input/output (I/O) device to perform certain tasks

3 Abbreviated terms

For the purposes of this International Standard, the following abbreviated terms apply.

ANSI	American National Standards Institute
API	application program interface
CCITT	Consultative Committee for International Telegraphy and Telephony
DAC	discretionary access control
DBMS	data base management system
FMS	fleet management system
FMSN	fleet management system network
IBS	integrated bridge systems
IEV	International Electrotechnical Vocabulary
LAN	local area network
NOS	network operation system
LITP	land-based information technology platform
NMEA	National Marine Electronics Association
SITP	shipboard information technology platform
STEP	standard for the exchange of product data (ISO)
VDU	visual display unit
WAN	wide area network

4 FMS network architecture

4.1 General architecture

The FMS architecture is shown schematically in Figure 1. The FMS is based upon a wide-area enterprise network, consisting of an unspecified number of SITPs and one or more shoreside LITPs which provides management services for the shipping enterprise. In total, the SITP enables multiple shipboard computer systems to share data with each other and to communicate with shore-based management and/or other vessels.

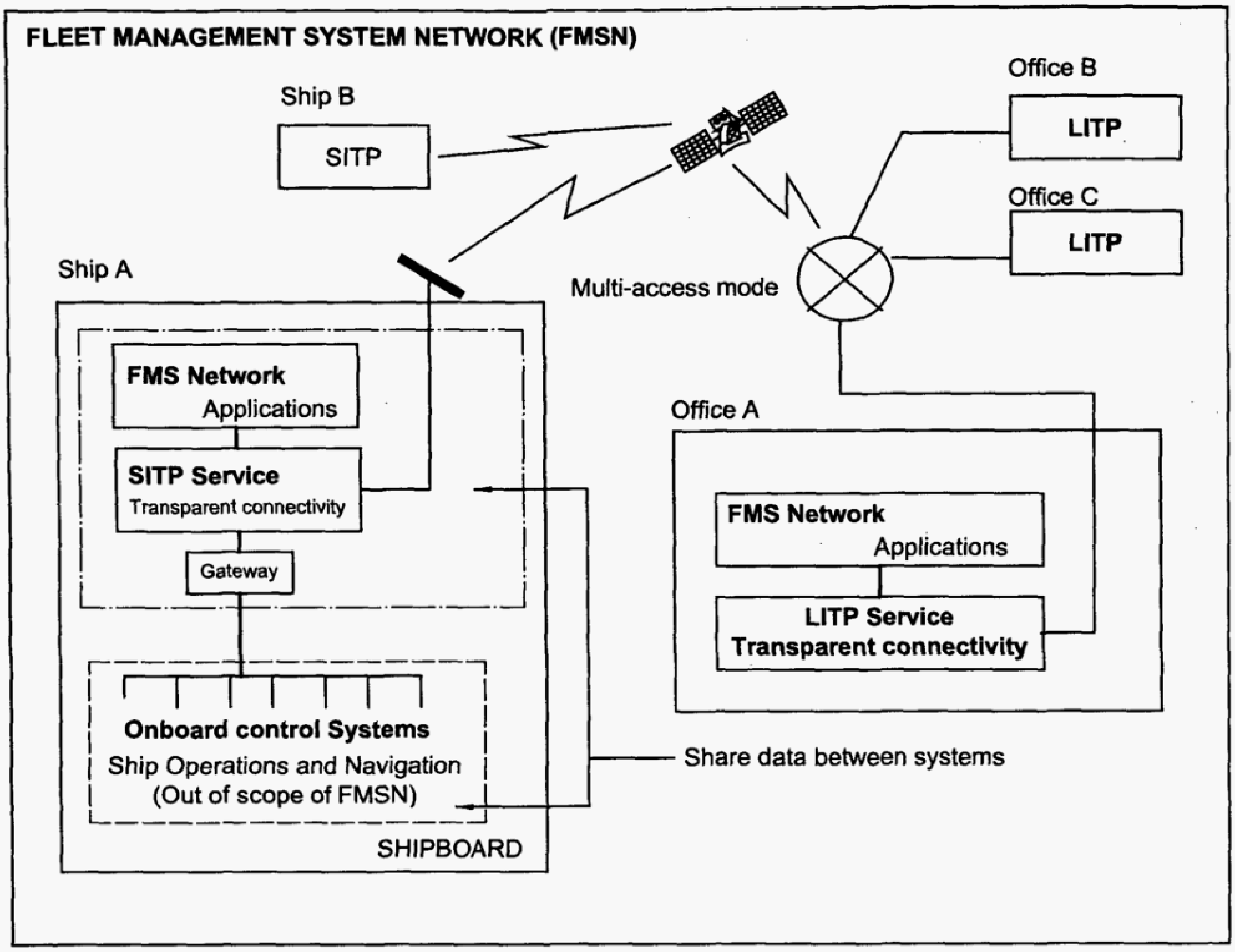


Figure 1 — Schematic of SITP / LITP connectivity

The FMS provides multi-vendor connectivity, distributed processing and electronic data interchange between networks, computers, workstations and peripherals. It also maintains databases and computer applications software that 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 communications hubs providing access to land-based networks such as telephone lines, facsimile, e-mail Internet services, and expanded satellite services through land-earth stations.

4.2 Network design

An underlying computer network is assumed 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 communications protocols, which define the rules that must be implemented in the hardware and software.

4.3 Network management

The FMS is based upon a WAN consisting of a number of LAN which are geographically dispersed over large areas and which are continuously or intermittently linked through wireless communications by bridges and gateway devices. The group responsible for managing the FMS will normally be located in the principle 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.

It is the responsibility of the user of this International Standard to establish appropriate safety and health and environmental practices and to determine the applicability of the various regulatory instruments.

4.4 Network security

A security function should be provided which is responsible for the following:

a) data confidentiality;

b) data integrity;

c) data authentication;

d) access control.

4.5 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.

4.6 Database model

Database maintenance and availability are key features of the FMS. Each SITP and LITP will maintain separate databases. Each site will incorporate a DBMS, including replication capability, as part of the SITP or LITP installation. This DBMS should be independent of the core management software. Data modelling embraces the concept that data should be structured in a neutral format separate from the applications software allowing for the exchange of data between applications using the same data model.

4.7 Database management system (DBMS)

4.7.1 General

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

a) persistent storage of data collected by the system,

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,

g) referential integrity, and

h) translators for applicable data models.

4.7.2 Database security

The DBMS should incorporate protection against

- improper access,
- improper modification of data (ensure data integrity), and
- improper denial of access;

It should provide for the following features.

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, etc.

e) Delimitation – control of information transfer between programs.

5 Shipboard information technology platform (SITP)

5.1 Introduction

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 where 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 NOS and a DBMS.

5.2 The SITP data acquisition service

The SITP data acquisition service is responsible for communicating with the various shipboard control systems or data collection units in order to acquire operating 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 should provide a framework in which custom interfaces can be developed to a variety of control systems and data acquisition units. Data from the control systems should be stored in the SITP database and be available for analysis and diagnostic applications software on the network. This data can also be transmitted to shore-based monitoring services through the communications network using gateways to provide one-way communications where required for control system isolation. A key objective of the SITP is to facilitate sharing of data among shipboard systems.

The SITP data acquisition service allows the shipboard fleet management systems to acquire information from sensors or databases in protected systems, e.g navigation and control systems. As the protected systems are critical for the safety of the ship, access to these systems should normally be through a firewall that can guarantee the integrity of the protected systems. The firewall will normally be considered as part of the protected systems and, hence, need to comply with appropriate class and regulatory requirements. These requirements are not addressed by this International Standard.

It shall be possible to manually input any shipboard information, which is required for the purpose of fleet management, and is not available directly from other systems.

5.3 SITP executive services

5.3.1 General

The standard SITP executive services, as indicated in Figure 2, are required in order to provide overall command and control of the SITP. The SITP 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 utilizes a set of structured APIs and internal communication channels for message exchange.

The following sections describe the services that may be 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. All management data recorded through an SITP executive process is available to any other SITP-compliant process.

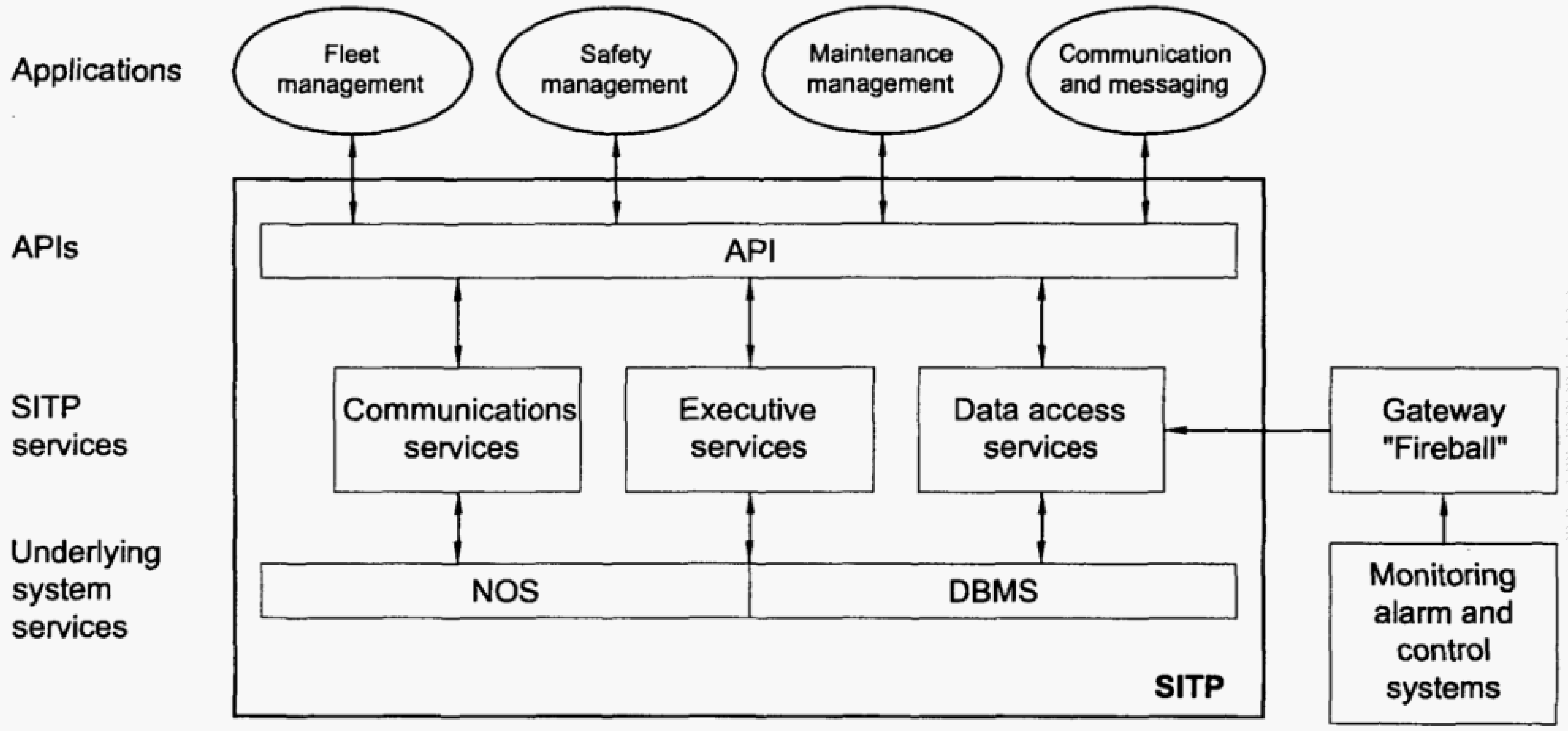


Figure 2 — SITP architecture

5.3.2 Process management

Process management refers to starting, staging, pausing, resuming and stopping a process. 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 process management database that describes the important attributes of the process. All process management information is available to SITP applications.

5.3.3 Messaging management

The SITP messaging management interfaces with an SITP-compliant process through the SITP API for applications to transport data among all registered entities on the SITP WAN. 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. The messaging management should allow for orderly classification of communication endpoints. The messaging management will use communications facilities as a transport mechanism for inter-application messages. The communication abstraction provided by the messaging management allows for additional transport mechanisms to be used in the future.

5.3.4 Replication management

The SITP replication management uses a generalized mechanism that allows SITP application providers to build distributed applications that operate within the SITP environment. This service may also be provided through the database software. The services provided 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. Furthermore, 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 re-send failed transmissions, or allow 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.

5.3.5 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.

5.3.6 Configuration management

The configuration management interfaces with SITP-compliant processes through SITP APIs. These requests will either request particular configuration settings or a change to a configuration setting. This service is responsible for updating the configuration database as required and notifying other processes affected by the configuration change.

5.3.7 Exception reporting management

The exception reporting management interfaces with the SITP-compliant process through the SITP APIs and with an exception report database. An SITP-compliant process, locally or remotely, may send an unsolicited exception report of a particular type to the exception reporting management service for processing. The management service stores the report in the exception report database where it may be accessed and processed by various monitoring systems.

5.3.8 Health management

Health management is used to check, on an ongoing basis, the current operability and availability of all SITP-compliant processes and record that finding in a historical record. This information is available to SITP-compliant applications.

5.3.9 Schedule management

The SITP schedule management interfaces with an SITP-compliant process through the APIs 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 date, or a range of times or triggered by events. Programs can also be configured to run on a recurring basis.

5.3.10 Time management

The SITP time management interfaces with an SITP-compliant process through the APIs for applications to synchronize with a master clock. This will counter the time drift encountered in computer real-time clocks and will allow for the synchronization of time stamps for remote systems. In a shipboard system, where distributed systems execute autonomously, synchronization of events is a critical function. The time management is responsible for maintaining the master clock and allowing various SITP services to access that information. In order to present a uniform reference point, the time management should operate in UTC (Universal Time Coordinated). Any information recorded by the SITP should include a date stamp in an accepted international format. The SITP should also be able to display world local times on demand.

5.3.11 Backup management

The SITP backup management interfaces with SITP-compliant processes through the client APIs and with the backup management database. An SITP-compliant process can execute backup routines and send data to the backup management for processing and where actions will be recorded in the backup management database.

5.3.12 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 performance monitoring. Furthermore, the data is modelled in such a way as to allow a general-purpose monitoring application to display performance data for any participating monitored object.

5.3.13 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 interfaces with SITP-compliant processes through SITP APIs to be available for use by remote users. The enterprise management allows users at a shore site to invoke SITP processes on a specific ship.

5.3.14 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.

5.3.15 Test management

The SITP test management interfaces with the SITP-compliant process through the client APIs and with the test management database. An SITP-compliant process can request test execution or test history information.

5.3.16 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.

5.4 Communications services

5.4.1 General

The communications manager should serve both remote and local users by providing for asynchronous dialogue with the SITP 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 common systems interface and support as described in 5.4.2 to 5.4.7.

5.4.2 Messaging

Messaging is the ability to transmit e-mail messages sent from any workstation to any other workstation in the FMS network, including the attachment of digital files. This will utilize both LANs and WANs including an interface to the Internet.

5.4.3 Digital data transfer

This is the ability to transfer digital data files between networks and workstations on a manual or automated basis.

5.4.4 Data replication

Data replication is the ability to support data replication functions of the database across the LAN and WAN so that entries on remote sites of the database can be replicated on an automatic transparent basis. Replication management should be provided at three levels.

a) **Non-session based replication**

   Transactions are replicated via e-mail, or uncontrolled file-based exchange. Success of replication is not monitored.

b) **Controlled, file-based replication**

   All transactions are tracked as a block and confirmed to have been received at the remote site. Recovery and the ability to "re-send" lost blocks is implemented. Logging is also enabled so that audits can be conducted to ensure integrity of replication.

c) **Session-based replication**

   Replication is managed by the database engine itself, which ensures integrity of the replication process. (available only under high-speed digital links), Logging and auditing mechanisms are also recommended.

5.4.5 Data consolidation and compression

Data consolidation is the consolidation of data being sent to a single address to allow multiple messages to be sent as a single file, including software at the receiving end to unconsolidate and distribute the transmission. The transmission files will be compressed to reduce data transmission time.

5.4.6 Continuation and logging

Continuation is the ability to automatically continue any message transmission from the point it was interrupted when transmission fails in mid-stream. Transmissions should be automatically logged to facilitate audits.

5.4.7 Transport medium

Data communications should be able to utilize diverse communications media including

a) satellite communications,

b) radio communications, and

c) cellular telephone.

5.5 SITP underlying system service

5.5.1 Network operating system (NOS)

A NOS supports the following services, which 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) provides multiple user access to system hardware devices;

e) file and print services – remote access, read, write, download, upload;

f) gateways to independent networks – the ability to access a remote system;

g) network management.

5.5.2 Security management

Security management provides an integrated platform-wide (including network operating system and compliance applications) security system, which includes

a) discretionary access control in which the users may protect their own objects,

b) mandatory access control in which users may read/write objects for which they have clearance,

c) isolation of the security kernel from non-critical systems (restricted access to operating system),

d) user authentication/identification for authorized access to resources without ability to bypass,

e) configuration and file server resource access restricted to administrative level logon, and

f) audit and log of security-related transactions/logins, read or write operations on objects, logouts.

5.5.3 Virus protection

As the SITP has connectivity to shore-based systems, it is important that it is protected from accidental or wilful exposure to harmful intrusion, e.g. through e-mail or transferred files. This protection should as a minimum include

a) programmed virus-scanning software, and

b) portable disc control.

5.5.4 SITP system robustness

The SITP should be equipped with mechanisms for hardware and software error detection and reporting. It should also have mechanisms that provide automatic recovery after errors. Examples of such mechanisms are

a) automatic checking and reporting of memory errors, and

b) automatic reset and reboot after power interruption.

6 Land-based information technology platform (LITP)

6.1 General

The LITP is the control and communication centre of FMS. It provides the infrastructure (software and hardware) necessary to provide computing and communication services for the management of a WAN of SITPs and any auxiliary shoreside installations. The design profile will generally replicate that of the SITPs it manages, expanded and optimized as required by the size of the fleet.

The underlying service, i.e. NOS and DBMS as well as the LITP services provide the same functions as corresponding services of the SITP described in this clause except as specified in 6.2 to 6.5.

6.2 Data acquisition services

Typically for the LITP, data acquisition from control systems will not be required.

6.3 Executive services

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

6.4 Communications manager

The communications manager will support a communications hub with access to land lines which may include telephone, telefax, e-mail, cellular and land earth stations.

6.5 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.

7 Application program interfaces (APIs)

7.1 Introduction

APIs will be required for third-party applications to use SITP/LITP services.

7.2 Overview of APIs

An API is a set of rules for linking various software components to a network. It is a software procedure that can be used as a building block to facilitate connections primarily between applications and other network software, but can also provide linkages for other elements of the network. The function of the network operating system is to control shared resources and to establish transactions among applications. In multi-vendor networks without commonality, APIs provide the links that would facilitate the following functions:

a) make system platform transparent to programming language and development environment of application;

b) provide links to external operating system;

c) provide links to external networks;

d) provide transparency to distributed objects.

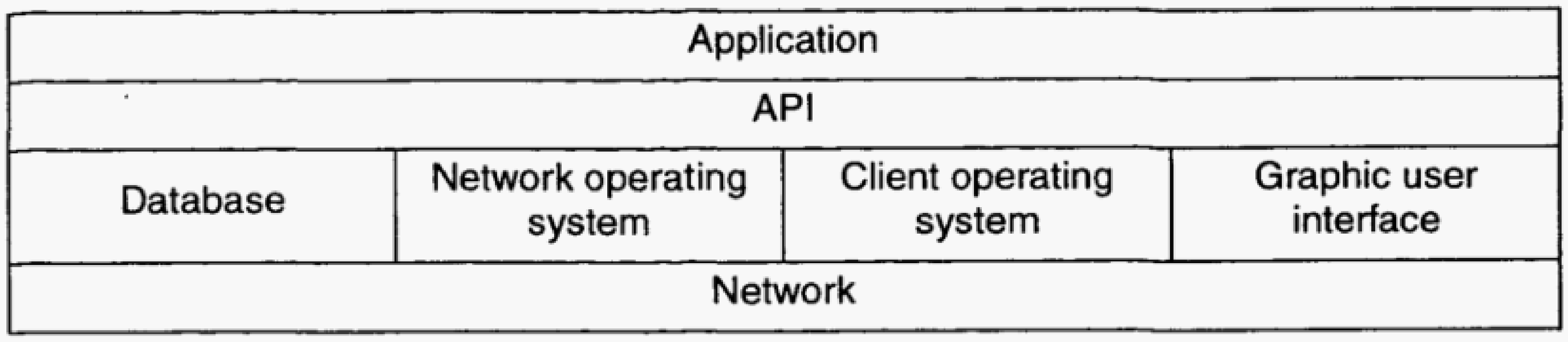


Figure 3 — Conceptual overview of API linkages

7.3 API applications

There are two types of applications:

a) SITP/LITP-compliant client application;

b) SITP/LITP system application.

A client application is any application running on the platform that wishes to take advantage of the common services. An SITP/LITP system application's purpose is to present FMS data and export system functionality. For example, an SITP/LITP client application running on the platform may be "process managed", allowing the platform to control the startup, shutdown, etc. of the application. A corresponding system application would be one that allows the user to view and control managed processes. It is possible for a system application to also be a client application of the SITP/LITP platform.

Both types of application access the platform's functionality through the APIs.

7.4 API levels of implementation

7.4.1 General

API services can be implemented to various levels. For software applications to have access to the services of the SITP, application program interfaces (APIs) will facilitate this third-party software application. An SITP compliant software entity will allow for seamless integration into the platform. There may be four levels of compliance, based upon the extent of SITP services used (see 7.4.2 to 7.4.5).

7.4.2 Level 1

a) process management;

b) logging management;

c) messaging management;

d) replication management;

e) configuration management;

f) backup management.

7.4.3 Level 2

Level 1 plus the following:

a) health management;

b) alarm management;

c) schedule management.

7.4.4 Level 3

Level 2 plus the following:

a) time management;

b) debug management;

c) performance management.

7.4.5 Level 4

Level 3 plus the following:

a) test management;

b) enterprise management;

c) localization management.

8 System hardware

8.1 System hardware

The selection of system hardware for both the SITP and the LITP must consider a number of factors which are dependent on the nature and the criticality of the applications supported by the FMS as well as the environment it must operate in. The specific hardware requirements are not covered in this International Standard.

8.2 Communications bus

The communications bus provides the physical interface between the communications software and the various shipboard transceivers that may include satellite communications, standard long-range and medium-range radio communications, and cellular communications, as well as others.

9 Fault tolerance

9.1 Fault tolerance

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.

9.2 Robustness

The FMS should be basically designed to be as robust as possible.

The design should be considered of easy recovery in the case of system loss.

If the system fails, the FMS shall not require the equipment to be complexly re-initialized by the operator.

10 Demonstration and validation

10.1 General

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

10.2 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.

10.3 System hardware test

Ensure that no part of the system can be over-stressed, e.g. as by voltage transients during operation or testing.

Ensure that components are rated electrically compatible with other design constraints to allow for part and parameter variations and transient conditions.

Ensure a safe margin in operating temperature.

10.4 LAN software assessment

As used in this International Standard, software assessment refers to the methodology for verification and validation of the FMS software.

Verification focuses on the functional design; validation focuses on whether the system satisfies the requirements.

Software is difficult to test; in contrast to hardware it does not wear out, and it does not operate within discrete parameters and testing is largely qualitative and inferential; in addition, redundancy is not an effective back-up.

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 as described below.

a) **Unit tests** of individual modules in isolation to verify logic and interface characteristics. This is accomplished concurrently with software development.

b) **Integration tests** of the different units to validate interoperability in accordance with design criteria.

c) **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.

10.5 Tests and trials

10.5.1 Unit tests (alpha testing)

These 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.

10.5.2 Integration tests

These are white box tests, the purpose of which is to bring together the various layers as the integration proceeds.

10.5.3 End-user (acceptance) tests

10.5.3.1 General

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 a simulated environment (mock-up). For the FMS, this will normally include at least one SITP and one LITP. These are black box tests requiring the type of testing described in 10.5.3.2 to 10.5.3.6.

10.5.3.2 Load/stress testing

This is used to confirm that the system can handle the peak load conditions (internal and external traffic).

10.5.3.3 Security testing

This is used to reveal weak spots in the system by repeated attempts to defeat the security controls.

10.5.3.4 Performance testing

These tests exercise all of the software applications, communication links and database management systems.

10.5.3.5 Hardware compatibility testing

This is used to determine the margin of hardware resources (memory, disk space, speed, etc.) over requirements.

10.5.3.6 Configuration testing

This is used to determine how the system responds to required alternative configurations in hardware or software.

11 Quality plan

11.1 General

Design, development, modification, replication and installation should be subject to a documented quality plan. As a minimum, the quality plan should speak to areas of responsibility for performance, and acceptance criteria in 11.2.

11.2 Design and testing of the computer services

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.

12 Operation and maintenance

The system design should include a complete plan for the operation and maintenance of the overall system, This includes the use of operations manuals in the testing of the systems. The maintenance plan should identify required maintenance procedures for the system and the applicable reference manuals.

13 Human interface

13.1 General

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

The FMSN is so designed that the operation and usability of the FMSN should be simple and not require complex operation.

13.2 Visual display unit (VDU)

13.2.1 The size, colour, contrast and density of text and graphics should be easily read or interpreted from the operator position under all operational lighting conditions. Type face should be an internationally recognized simple, clear-cut design.

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

13.3 Screen image paging

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

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

14 Training and documentation

14.1 General

14.1.1 Regardless of the technical excellence of the FMS software and hardware, operator training is essential to its successful application. The transient 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.

14.1.2 It is a condition of this International Standard that formal training in the operation of the FMS is available.

14.1.3 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 as a minimum:

a) management of local area networks;

b) management of wide area networks;

c) client server systems;

d) network operating systems;

e) all installed hardware;

f) maintenance and repair;

g) a knowledge of the regulations concerning telecommunications;

h) administration of the SITP and FMS systems;

i) database management.

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" and *system documentation* as "the collection of documents that describe the requirements, capabilities, limitations, design, operation and operation of an information processing system". Both definitions are relevant for the purposes of this International Standard.

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.

Bibliography

[1] ASME F1166, *Standard Practice for Human Engineering Design for Marine Systems Equipment and Facilities*

[2] IEC 60050, *International Electrotechnical Vocabulary (IEV)*

[3] IEC 60092-504, *Electrical installations in ships — Part 504: Special features — Control and instrumentation*

[4] IEC 60533, *Electrical and electronic installations in ships — Electromagnetic compatibility*

[5] IEC 60945, *Maritime navigation and radiocommunication equipment and systems — General requirements — Methods of testing and required test results*

[6] IEC 61162, *Maritime navigation and radiocommunication equipment and systems — Digital Interfaces*

[7] IEC 61209, *Maritime navigation and radiocommunication equipment and systems — Integrated bridge systems (IBS) — Operational and performance requirements, methods of testing and required test results*

[8] ISO/IEC 8073, *Information technology — Open Systems Interconnection — Protocol for providing the connection-mode transport service*

[9] ISO/IEC 8326, *Information technology — Open Systems Interconnection — Session service definition*

[10] ISO 8327, *Information technology — Open Systems Interconnection — Basic connection oriented session protocol specification*

[11] ISO 8571, *Information technology — Open Systems Interconnection — File Transfer, Access and Management*

[12] ISO/IEC 8602, *Information technology — Protocol for providing the OSI connectionless-mode transport service*

[13] ISO/IEC 8802-3, *Information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks — Specific requirements — Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications*

[14] ISO/IEC 8802-4, *Information processing systems — Local area networks — Part 4: Token-passing bus access method and physical layer specifications*

[15] ISO/IEC 8822, *Information technology — Open Systems Interconnection — Presentation service definition*

[16] ISO 8823, *Information processing systems — Open Systems Interconnection — Presentation service definition*

[17] ISO 9000:2000, *Quality management systems — Fundamentals and vocabulary*

[18] ISO 9001:2000, *Quality management systems — Requirements*

[19] ISO/IEC 9075, *Information technology — Database languages — SQL*

[20] ISO/IEC 9548, *Information technology — Open Systems Interconnection — Connectionless Session protocol*

[21] ISO/IEC 9576, *Information technology — Open Systems Interconnection — Connectionlless presentation protocol specification*

ICS 35.240.60; 47.020.99

Price based on 19 pages