University of Cape Town

DISSERTATION

MASTER OF SCIENCE IN ENGINEERING

Real-Time Distributed System Architecture

using

Local Area Networks

Author	:	Richard Young Pr Eng, BSc(Eng)
Supervisor	:	Mr M.J. Ventura
Prepared for	:	Department of Electrical and Electronic Engineering Faculty of Engineering University of Cape Town Private Bag **RONDEBOSCH** 7700 Cape Town Republic of South Africa
Year	:	1992
Issue	:	1
Date	:	1992-10-16

Abstract

This dissertation addresses system architecture concepts for the implementation of real-time distributed systems. In particular, it addresses the requirements of a specific mission and real-time critical distributed system application as this exemplifies most of the issues of concern. Of specific significance is the integration of real-time distributed data services into a platform-wide **Information Management Infrastructure**.

The dissertation commences with an overview of the system-level **allocated requirements. Derived requirements** for an Information Management Infrastructure (IMI) are then determined.

A generic **system architecture** is then presented in terms of the allocated and derived requirements. A specific topology, based on this architecture, as well as available technology, is described.

The scalability of the architecture to different platforms, including non-surface platforms, is discussed. As financial considerations are an important design driver and constraint, some anticipated order-of-magnitude system acquisition costs for a range of system complexities and configurations are briefly reviewed.

Finally some **conclusions** and **recommendations** within the context of the allocated and derived requirements, as well as the RSA's politico-economic environment, are offered.

Index Terms

Real-time, distributed computing, local area networks, LAN, fibre optic LANs, information management, information technology, system architecture, system integration, mission-critical, fault tolerant.

Acknowledgement

The author firstly wishes to acknowledge the support of Messrs Anton Jordaan and Brian Blackbeard whose confidence and enthusiasm were instrumental in the sponsorship of the work underlying this dissertation.

He secondly wishes to acknowledge and thank Gerhard Krüger for his participation in the requirements analysis and concept design, especially the Combat System Comparative Analysis and Dataflow Analysis.

The work performed in respect of the ICS Architecture Demonstration Model was performed at UEC Projects (Pty) Ltd by a project team of four engineers under the leadership of the author. The concept of the Architecture Concept Demonstration Model was that of the author. The work was sponsored by the SA Navy and Armscor.

The author wishes to acknowledge and thank the contributors to this exciting and rewarding project; Gerhard Krüger (system integration, FDDI, TCP/IP, Met Station, GPS), Jurie Malan (image processing), Rob Stemmett (FDDI, NetWare, TCP/IP, MIL-STD-1553B Gateway, GPS) and Louis van Alphen (SQLBase, image database and colour printer driver). He would also like to acknowledge and thank the project sponsors, Anton Jordaan of Armscor and Brian Blackbeard of the SA Navy for their critical roles in this particular aspect of the project.

The views expressed in this dissertation are those of the author and do not necessarily represent those of the South African Navy or South African Government.

CONTENTS

CONTENTS
(Continued)

CONTENTS
(Continued)

CONTENTS
(Continued)

Abbreviations and Acronyms

This section provides important abbreviations and acronyms used in the main body of this dissertation.

ACDM	Architecture Concept Demonstration Model
ADAR	Air Defense Array Radar
AJPO	Ada Joint Program Office
AMDR	Automatic Missile Detection Radar
ANSI	American National Standards Institute
APSE	Ada Program Support Environment
ASM	Anti-Ship Missile
ASR	Air Search Radar
ASW	Anti-Submarine Warfare
ASCII	American Standard Code for Information Interchange
ATM	Asynchronous Transfer Mode
BER	Bit Error Rate
BLOB	Binary Large Object
CAM	Contents Addressable Memory
BIT	Built-In Test
BSRF	Basic System Reference Frequency
CASE	Computer-Aided Software Engineering
CCD	Charge-Coupled Device
CCS	Command and Control System
CDDI	Copper Distributed Data Interface
CD ROM	Compact Disc Read Only Memory
CIWS	Close-in Weapon System
CLOS	Command to Line of Sight
CMOS	Complementary Metal Oxide Semiconductor
CPU	Central Processing Unit
CSMA/CD	Carrier Sense Multiple Access with Collision Detect
DAS	Dual-Attachment Station
DBMS	Database Management System
DID	Data Item Description
DJ	Deception Jammer
DOD	Department of Defense
DQDB	Dual Queue Dual Bus
EEZ	Exclusive Economic Zone
EFA	European Fighter Aircraft
EMC	Electro-Magnetic Compatibility
EPROM	Erasable Programable Read Only Memory
EW	Electronic Warfare
EWSS	Electronic Warfare Sub-System
FC	Fibre Channel
FCR	Fire Control Radar
FDDI	Fibre Distributed Data Interface
FDVDI	Fibre Distributed Voice, Video and Data Interface
FFOL	FDDI Follow-On LAN
FGC	Frame Grabber Card
FGU	Frame Grabber Unit
FLIR	Forward-Looking Infrared

FOM	Figure Of Merit
GCU	Gun Control Unit
GPS	Global Positioning System
GPU	Graphics Processing Unit
HiPPI	High Performance Parallel Interface
HLL	High-Level Language
HMS	Hullmount Sonar
HRC	Hybrid Ring Control
HSCC	High Speed Communication Controller
HSS	Helicopter Sub-System
IC	Integrated Circuit
ICS	Integrated Combat Suite
IEEE	Institute of Electrical and Electronic Engineers
IMI	Information Management Infrastructure
IMU	Image Monitor Unit
I/O	Input/Output
IP	Internet Protocol
IPI	Intelligent Peripheral Interface
IPX	Internetwork Packet Exchange
iRMK	Intel Real-time Multi-tasking Kernel
iRMX	Intel Real-time Multi-tasking Executive
ISA	Industry Standard Architecture
ISO	International Standards Organisation
ISW	In-System Write
IT	Information Technology
LAN	Local Area Network
LRU	Line Replaceable Unit
LSS	Lightweight Support Services
MAN	Metropolitan Area Network
MAC	Media Access Control
MAP	Manufacturing Automation Protocol
MCU	Missile Control Unit
Met	Meterological
MIB	Management Information Base
MIPS	Mega-Instruction Per Second
MMI	Man-Machine Interface
MPD	Medium Propagation Delay
NATO	North Atlantic Treaty Organisation
NDI	Non-Developmental Item
NETBLT	Network Bulk Transfer
NJ	Noise Jammer
NMS	Network Management Station
NPU	Numeric Processing Unit
NRSS	Navigation Radar Sub-System
NSS	Navigation Sub-System

OBP	Onboard Programming
OBS	Optical Bypass Switch
OFCC	Optical Fibre Cable Components
OLTP	On-Line Transaction Processing
ORT	Optical Radar Tracker
OS	Operating System
OSI	Open Systems Interconnect
PCB	Printed Circuit Board
PDL	Program Design Language
PFM	Platform
PHY	Physical Layer Protocol
PL	PHY Latency
PMD	Physical Medium Dependant
PMF	Parameter Management Frames
PC	Personal Computer
POSIX	Portable Operating System Interface Extension
RAM	Random-Access Memory
RCS	Radar Cross-Section
RINA	Royal Institute of Naval Architects
RISC	Reduced Instruction Set Computer
RAM	Random Access Memory
RAN	Royal Australian Navy
RH	Relative Humidity
RLT	Ring Latency Time
RN	Royal Navy
RTU	Remote Terminal Unit
R-T	Real-Time
SAE	Society of Automotive Engineers
SAFENET	Survivable Adaptable Fibre-Embedded Network
SAM	Surface-to-Air Missile
SAS	Single-Attachment Station
SCA	Standard Console Assembly
SCS	Standard Computing Segment
SDD	Software Design Document
SDP	Software Development Plan
SIM	Strategic Information Management
SMT	Station Management
SMU	Station Management Unit
SNC	Standard Naval Console
SNMP	Simple Network Management Protocol
SPS	Software Product Specification
SPX	Sequenced Packet Exchange
SQL	Structured Query Language
SRS	Surveillance Radar System
SRS	Software Requirement Specification
SSM	Surface-to-Surface Missile

SSR	Surface Search Radar
STANAG	NATO Standard Agreement
STP	Shielded Twisted Pair
STP	Software Test Procedure
STR	Software Test Result
STS	Software Test Specification
TAS	Towed Array Sonar
TBD	To Be Determined
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDS	Torpedo Decoy System
TFCS	Torpedo Fire Control System
TLAM	Tactical Land Attack Missile
TOP	Technical Office Protocol
TP4	Transport Protocol Class 4
TSS	Tracker Sub-System
TRT	Token Rotation Time
TTRT	Target Token Rotation Time
USN	United States Navy
WBC	Wideband Channel
WBS	Work Breakdown Structure
WORM	Write Once Read Many
UTP	Unshielded Twisted Pair
VLSI	Very Large Scale Integration
WCU	Weapon Control Unit
WER	Word Error Rate
VMTP	Versatile Message Transaction Protocol
XTP	Express Transfer Protocol

1. SCOPE

1.1 Scope

This dissertation addresses system architecture concepts for the implementation of real-time distributed systems. In particular, it addresses the requirements of an Integrated Combat Suite (ICS) for a Naval Surface Combatant as this application exemplifies a mission and real-time critical distributed application of all the issues of concern. Of specific significance is the integration of real-time distributed data services into a ship-wide **Information Management Infrastructure.**

The objectives of the work underlying this dissertation were the analysis of the information management requirements of the next generation of surface combatant, specifically a multi-purpose frigate, for the South African Navy and the synthesis of an optimal (in terms of upgradeability, flexibility and cost-effectiveness) solution using distributed computing elements and local area networks. Of particular significance was that the total platform should exhibit a high degree of integration across all its functional areas.

The work was carried out by the author under the auspices of a number of related Navy projects [9.2.39] as well as in preparation for a technical paper presented by the author at the Royal Institute of Naval Architects (RINA) International Conference on Information Technology and Warships in London during December 1991 [9.2.40].

Recognising that the application could be somewhat complex, a further objective was to adopt, adapt or formulate practical paradigms for the two fundamental issues in synthesizing a total solution, i.e. information management and communication management.

1.2 Introduction

In order to meet the ever-increasing demands for performance, effectiveness, flexibility and upgradeability, systems are being designed to rely to a greater and greater extent on computers. While computer hardware provides the computing **platform** for the required function, it is computer software which effects the actual functionality. Significant progress in the area of computer hardware technology has been made in recent years with the result that relatively inexpensive computers are readily available.

Although current computer hardware can offer considerable computing power, machines are susceptible to failure, with extensive implications in mission and safety-critical applications, especially in centralised computer architectures. Also, despite the considerable power of current computers, the demands of software, especially that of modern high-level language implementations, are rapidly beginning to outstrip the capabilities of the most powerful computers.

The solution to these apparent dilemmas is the implementation of **distributed** computer architectures where a number of distributed, but connected, computers share the processing load. While the implementation of any distributed computer architecture is non-trivial, the requirements for such a system become complex when applied to a critically **real-time** application [9.2.39].

There are fewer applications of a more mission-critical, real-time nature than that of the modern naval surface combatant. In addition, the modern warship must not only be able to survive in its hostile physical and electromagnetic environment, but it must be able to *fight hurt* after considerable battle damage.

In the modern combat environment, the force with the best access to **information** is best placed to deal effectively with its adversary, i.e. assuming a reasonable parity in weapon

capability. In fact, this can be said of almost any organisation operating competitively.

The very nature of the modern naval surface combatant and its environment demands an Information Management Infrastructure (IMI) that is distributed and can operate in real-time. This IMI needs to be constructed from the fundamental building blocks of modern Information Technology (IT).

Three areas of IT, in particular, are influencing the way in which combat systems can function with greater effectiveness; these are **networking**, **graphics** and **image processing**.

1.3 Document Overview

The dissertation commences with an overview of the **system-level allocated requirements**. **Derived requirements** for an Information Management Infrastructure (IMI) are then determined.

Various **architecture concepts** are reviewed before a generic **system architecture synthesis** is presented in terms of the allocated and derived requirements as well as the adopted information and communication management models. A specific topology, based on this architecture as well as available technology, is then described.

The scalability of the architecture to different platforms, including non-surface platforms, is discussed. As financial considerations are an important design driver and constraint, some anticipated order-of-magnitude system acquisition costs for a range of system complexities and configurations are briefly reviewed.

A description on the rapid prototyping of some of the characteristics of the system, i.e. an Architecture Concept Demonstration Model, is then presented [9.2.39]. This describes actual engineering development, performed by the author and colleagues, of an Integrated Combat System Information Management Infrastructure. The author was responsible for the

formulation of the concept as well as the architecture of the proposed system. He was also the project manager of the project team which undertook implementation (mainly in terms of software) of various aspects of the architecture concept.

Finally some **conclusions** and **recommendations** within the context of the allocated and derived requirements, as well as the RSA's politico-economic environment, are offered.

Detailed results of some specific investigations into an ICS IMI are provided in six appendices: Combat System Comparative Analysis, LAN Technology Comparative Analysis, 1st Order Dataflow Analysis, 1st Order Database Analysis, FDDI Ring Latency Time Analysis and Implementation Issues.

2. SYSTEM REQUIREMENTS

2.1 Combat System Requirements

Without regarding the user's intrinsic weapon capability, the user requirement for a highly effective combat system may be summarised as follows :

- **Fast access to accurate and informative information**
- **to provide the ability to make quick and well-founded strategic and tactical decisions**
- **to defend or attack as the operational requirement may demand.**

From this it can be derived that the user requires an **integrated**, **available** and **operable** system. Sensors, decision support systems and weapons need to be integrated to provide this capability.

The user also requires the system to be **secure**, **survivable** and **flexible.**

Deriving lower-level requirements from those above means that the system must be **reliable**, **maintainable**, **reconfigurable**, and **electro-magnetically compatible** (EMC), as well as **small in size** and **low in mass.**

Apart from these, the user organisation has further requirements of any operational system. It must be **user-friendly**, **supportable**, **expandable**, **upgradeable** and **affordable.**

In terms of the functional performance of the combat system, this can be extensively enhanced by the use of **graphics**, **shared databases**, **image processing** and **image databases.** In the medium-term future, **knowledge-based (*expert*) systems** will be required in order to give the user the critical edge over the adversary.

Apart from all the above requirements, the system must operate in a critically **real-time** environment. This demands the capability of handling **high data rates**, **vast data volumes** with **low latency times** in a **deterministic** manner.

2.2 Functional Performance Requirements

The overall functional requirements of a surface combat system can be summarised as follows :

a. Reception of surveillance information from a variety of sensors, both onboard and offboard, as well as the rest of the task force via data links.

b. Generation and display of air, surface and sub-surface situation plots identifying friend or foe.

c. Transfer of this information to other units and vessels in the task force via data links.

d. Threat analysis of the situation.

e. Simulation of potential engagements as an aid to the decision making process of the operators and commanders.

f. Target designation, target weapon assignment and the control of counter-measures against the enemy's weapons.

g. Operation and control of weapons and the release of munitions.

From these allocated requirements, it follows that information is required to be transmitted between sub-systems on the same platform and other platforms; this can be considered as a **derived** requirement as it is transparent to the user. The manner in which data and information flow is achieved has significant implications on system architecture, design and implementation and should therefore be effected

in such a manner as to optimise the design of the Combat System in areas such as functional performance, availability, maintainability, upgradeability, training, cost, etc.

Such optimisation should be achieved by effective allocation of functions to physical equipment in order to achieve minimum data flow between equipments without compromising flexibility, survivability and upgradeability.

The transfer of information must be performed in real-time which places the following requirements on the information transfer system :

a. Minimisation of the latency of information transfers.

b. Simultaneous information transfer between multiple sub-systems.

Figure 1 depicts the critically real-time environment of the modern naval surface combatant.

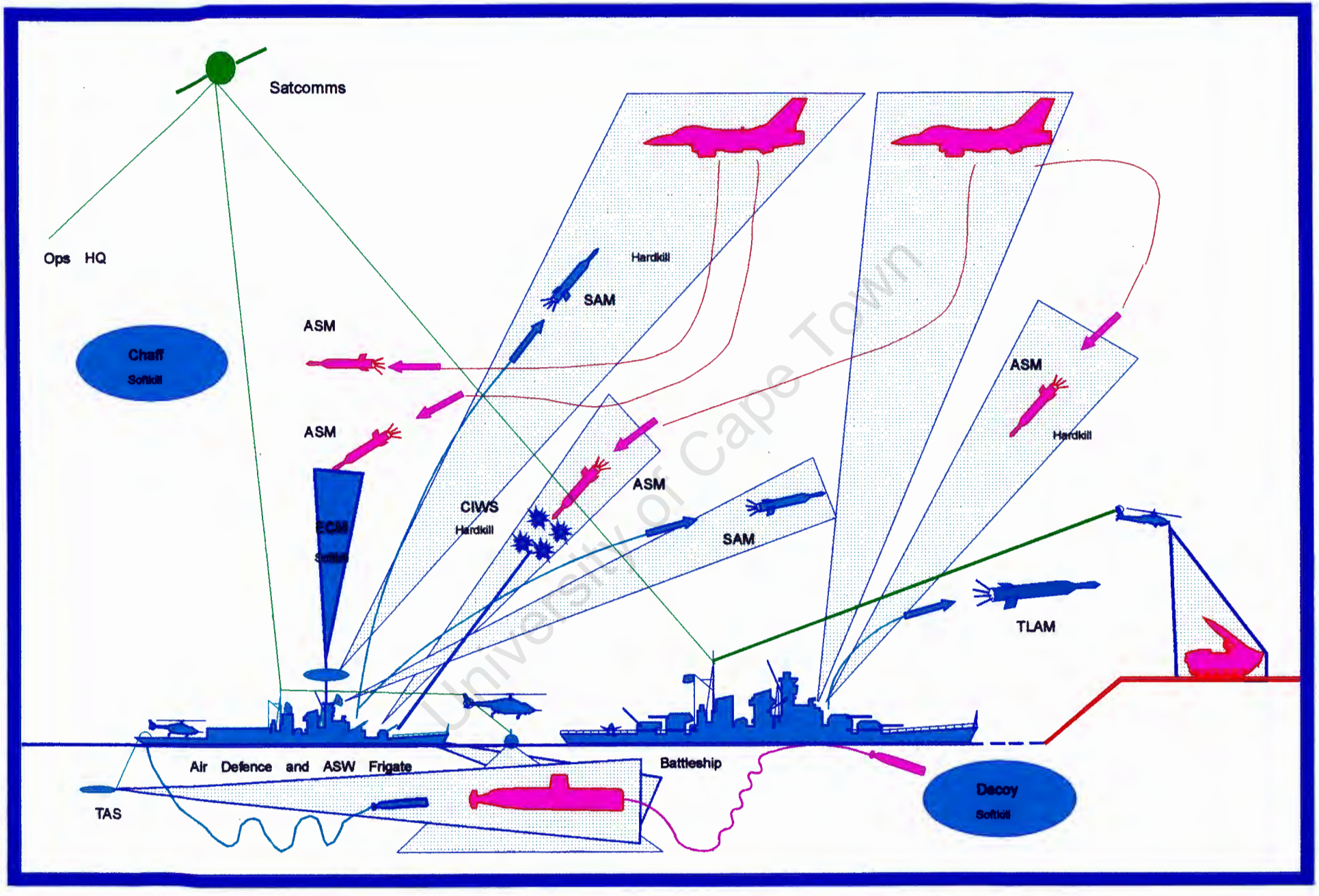


Figure 1 : Critically Real-Time Environment of Naval Surface Combat

The ICS can be described in terms of a Data Flow Model and Functional Flow Block Diagram as depicted in Figure 2 and Figure 3 below.

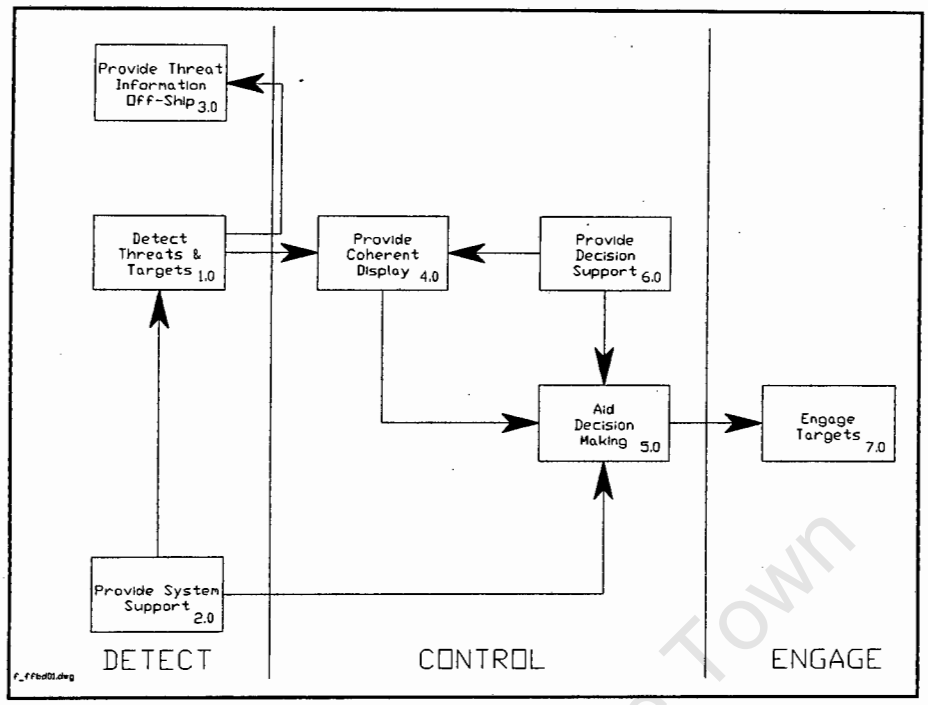


Figure 2 : ICS Data Flow Model

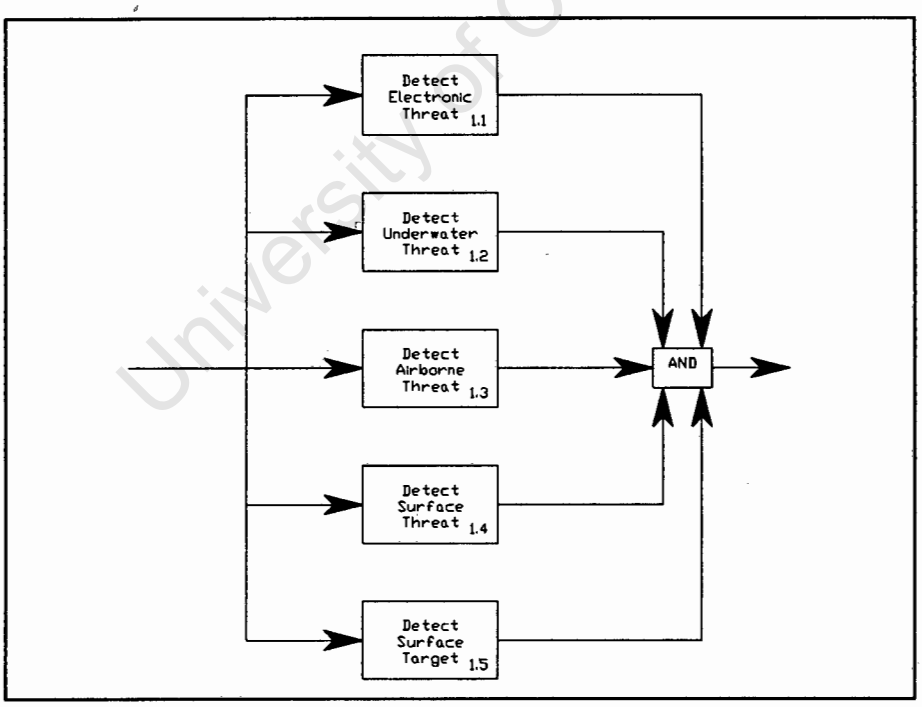


Figure 3 : Functional Flow Block Diagram for Detect Threats and Targets

2.2.1 Real-Time Data Transfer Requirements

The single most important consideration when partitioning a combat system is the time criticality of the various sensor/weapon/operator data paths.

2.2.1.1 Critical Functions

The following real-time critical functions of the ICS determine LAN bandwidth requirements :

a. Tracking of up to 400 contacts from all sensor sources including Fire Control Radar (FCR), Air Search Radar (ASR), Surface Search Radar (SSR), Anti-Submarine Warfare (ASW) suite, Electronic Warfare (EW) suite and off-ship via Data Links.

b. Providing fire-control quality tracks for up to 16 threat missiles (ASMs) of speed 3 Mach (800 ms^{-1}).

c. Engagement of up to 10 threat missiles with own ship's command-to-line-of-sight missiles (SAM) systems, capable of speed 5 Mach (1 500 ms^{-1}).

d. Engagement of up to 4 threat missiles with ship's gun systems.

e. Engagement of the balance of the threat missiles with ship's EW "weapons", i.e. jammers, chaff and decoys.

2.2.1.2 Critical Data

The applicable fire-control algorithms involve the transmission of the following time- and mission-critical data :

a. Target Track Data (≈ 32 bytes) from a Tracker Sub-System (TSS) to a Gun Control Unit (GCU) every 5 ms.

b. Platform Stabilisation Data (≈ 16 bytes) from the Navigation Sub-System (NSS) to the Weapon Control Units (WCUs) every 10 ms.

c. Target Track Data (≈ 32 bytes) from a Tracker Sub-System (TSS) to a Missile Control Unit (MCU) with a maximum latency of 20 ms.

From these mission and time-critical dataflow requirements, 1st Order Dataflow and Database Analyses can be performed (refer Appendices D and E for further detail). Appropriate LAN timing considerations can also be addressed (refer Appendix C - FDDI Ring Latency Time Analysis).

2.2.1.3 Determinism

A major requirement for the transfer of data in a real-time system is that it be deterministic, i.e. transfer of specific data messages occurs within guaranteed time 'windows'. This is so in order that algorithms implemented by distributed systems converge in real-time. Determinism is also a highly desirable attribute in test, evaluation and qualification as these

processes are difficult and time consuming in non-deterministic systems.

3. ARCHITECTURE CONCEPTS

3.1 System Architecture

The extensive array of requirements determined in Paragraph 2 focuses the resulting combat system architecture towards one with the following attributes :

Distributed system architecture integrated by means of a *system of local area networks* (LANs)

The LAN provides for sub-system interconnectivity, sub-system redundancy as well as supporting the required data throughput. The system of cross-connected LANs ['Metropolitan' Area Network (MAN)] supports a high-level of system integration across the major warfare areas and reduction of LAN dataflow, while supporting survivability in the case of localised combat damage. It also facilitates co-ordination and development of a coherent, multi-warfare, tactical picture supporting command team decision making.

Multi-platform data communication is supported by data links forming a Wide Area Network (WAN).

The chief attributes of the LAN are fibre-optics technology and intrinsic redundancy. These attributes provide the capability of high bandwidth, reliability, survivability and electro-magnetic compatibility.

In essence the LAN provides **networking services** by providing interconnectivity, operating system services and interfaces to shared resources such as input and output devices. Input devices include digital document scanners and CD ROM drives. Output devices include monochrome and colour printers, bulk storage devices such as tape streamers, optical disk drives and magnetic disk drives.

The LAN also provides an infrastructure for **data services**. Data services encompass data access services (database management services), data interchange services (gateways,

routers and bridges) and data storage services (mechanisms for interfacing to the bulk storage devices).

Together the networking services and data services provide an *Information Management Infrastructure*.

3.2 Information Management Model

It is clear that a vast amount of data and information needs to be gathered, distributed, processed and presented within the complex combat system. It is also clear that many organisations will be involved in acquiring, defining, designing, developing, using and supporting the system.

To simplify these ends, a conceptual Information Management Model is required to be defined and adopted by the parties involved.

It is proposed that the Strategic Information Management (SIM) model [9.2.9] is used in the development of the **Information Management Infrastructure**.

The SIM model addresses the areas of interconnection, distributed services, information presentation and, similarly to the ISO OSI model, utilises a layered approach.
The model consists of four layers, namely :

a. User Interface Layer.
b. Application Layer.
c. Data Layer.
d. Processing Layer.

Figure 4 below shows these layers graphically.

An important objective of the layered approach is to de-couple functionally-different services from each other. This has an advantage in development where different parties can provide functionality within their special areas of capability. The approach also allows for less troublesome functional integration. It has further advantages during

product or system upgrade where specific implementations of certain functions can be replaced by more state-of-the-art implementations i.e. effective **management of obsolescence.**

3.3 Real-Time

3.3.1 Definition

Real-Time systems are characterised by the requirement to execute multiple, concurrent tasks with **hard deadlines.** i.e. exhibit bounded and deterministic responses to external events [9.2.26]. Compromising these deadlines may have catastrophic results, including loss of life, loss of platform or mission failure.

3.3.2 Scenario

The typical, real-time nature of naval surface combat can be exemplified in the case of a attack by supersonic (800 ms^{-1}) anti-ship missiles; e.g. Styx (4 in number). In sea-state 5 (rough sea causing significant rolling and pitching motion) the limitations of radar will imply a maximum detection range of 16 km implying a time-to-impact of some 20 seconds. Threat confirmation, report and engagement orders will take at least 7 seconds. 2 seconds are required for trackers to lock-on, weapons to slew to the correct azimuth, stabilise and fire control solutions converge. At this stage the threat missile is 9 km away with 11 seconds until impact. The time of flight of the first round of the standard anti-aircraft gun (76 mm) at 8 km is 11 seconds. As the hit probability per round is significantly less than unity, a large number of rounds (≈ 20 with two guns) must be expended to achieve an acceptable (≈ 85%) kill probability. The hit probability can be enhanced if each round is afforded its own fire solution.

The case of a sea-skimming, pop-up, missile would be significantly worse; as little as 4 seconds may remain between detection and time-to-impact. In this case, the only realistic defence would be the **automatic** engagement of the threat with the Close-in Weapons Systems (CIWSs) (e.g. Goalkeeper, Phalanx).

3.3.3 System Implementation Implications

As threats will be shared amongst processing elements, multitasking will be required. This implies task switching and scheduling with hard deadlines.

With respect to data communications, real-time performance implies the requirement to transmit data and synchronisation information within **strict deadlines** via the communications media.

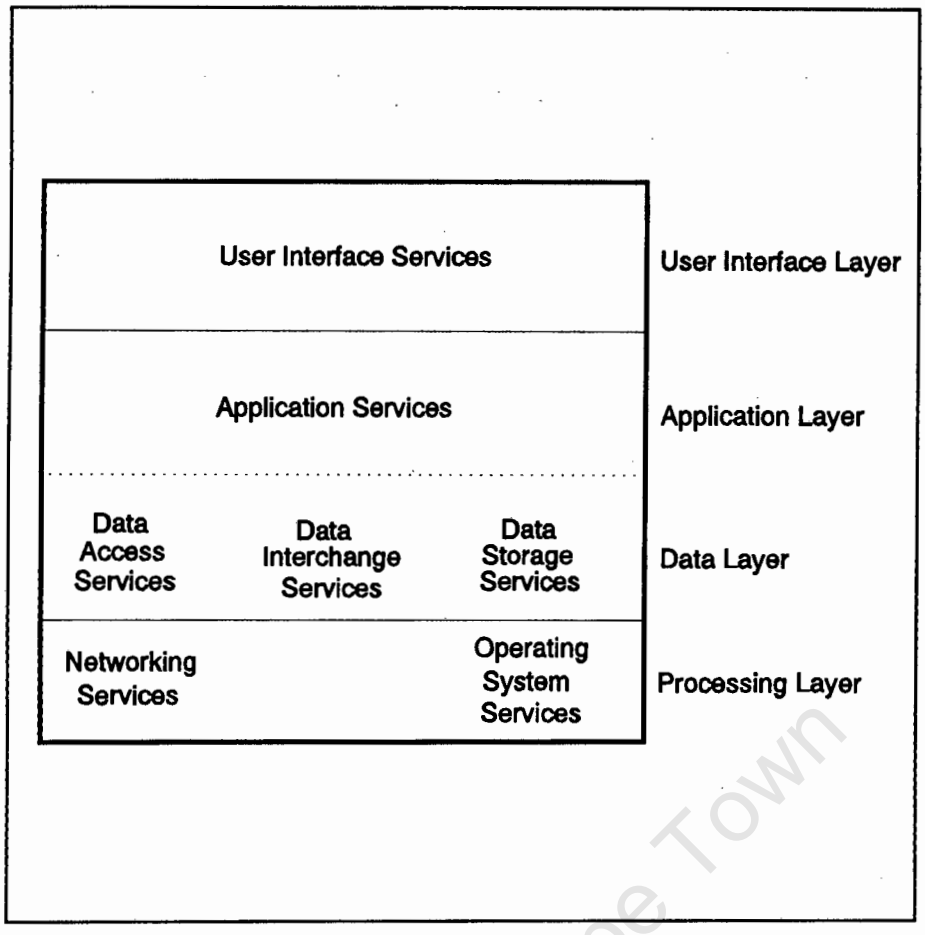


Figure 4 : Strategic Information Management Model

The Information Management Infrastructure consists of all items and services within the Data and Processing Layers.

Within the integrated combat system, the Application and User Interface Layers utilise the services of the lower layers. These layers implement the user's higher level of functional requirements.

3.4 Communication Model

As with information management, a communications model is required to be defined and adopted.

The *Survivable Adaptable Fibre Optic Embedded Network* (SAFENET) model specifically the SAFENET II [9.1.5, 9.2.1] model, as defined for the US Navy [9.2.6], is proposed.

Table I shows the SAFENET profile and its relationship to the ISO OSI 7-layer Basic Reference Model. The SAFENET profile is derived from the ISO OSI communications model [9.1.9] described in Table II.

		SAFENET I		SAFENET II	
Layer No.	**ISO OSI Layers**	**ISO Suite (Maximum Interoperability)**		**Lightweight Suite (Minimum Latency)**	
9	Application Process *	Ada Task		Ada Task	
8	Operating System *	(Selection Ongoing)		(Selection Ongoing)	
7	Application	MAP 3.0 File Transfer Private Communications Network Management & Directory Services		Lightweight Support Services (Designed to meet the needs of a specific system)	
6	Presentation	MAP 3.0 Presentation			
5	Session	MAP 3.0 Session			
4	Transport	ISO Class 4 Transport Protocol	Global Time Service	**XTP** Protocol	Global Time Service
3	Network	ISO Network Protocol			
2	Data Link	IEEE Logical Link Control Class I Protocol		IEEE Logical Link Control Class I Protocol	
		IEEE 802.5 Token Ring		ANSI **FDDI** MAC Protocol	
1	Physical	SAFENET Modification (16 $MBits^{-1}$)		ANSI **FDDI** Physical Protocol (100 $MBits^{-1}$)	
0	Cable Plant *	Common Cable Plant		Common Cable Plant	

Note : * denotes outside the scope of the 7-layer model

Table I : SAFENET I and II Standards Suites

No.	Layer	Functional Description
7	Application	Interfaces to user programs and provides specific and common services for applications
6	Presentation	Restructures data to/from format used within the network
5	Session	Sets up and controls a communication channel
4	Transport	Optimises use of the network and enhances reliability
3	Network	Provides message routing for data transfer
2	Datalink	Formats/disassembles packets, controls flow and handles error recovery
1	Physical	Encodes and physically transfers packets

Table II : ISO OSI Basic Reference Model

The reason for the applicability of the SAFENET II Model is that it is a practical, achievable implementation of the ISO OSI Model that is capable of real-time performance. It is practical because, while it redefines the 7-layer model somewhat, it leaves the major layer boundaries (i.e. the major interfaces) unchanged. It also provides the other layers required for a complete system. It is achievable because implementations (hardware and software) of all the layers exist, or are currently under full-scale engineering development.

Another reason for its applicability is that, while SAFENET II is a standard, the same approach can be taken without full adherence to the standard. This is significant in the South African context as full adherence would have extensive, possibly prohibitive, cost implications.

3.5 Relationship Between Models

The Information Management Model describes the higher order functionality of the Information Management Infrastructure while the Communication Model provides the detail of the former's Networking Services Sub-Layer. There is not, however, a strict correlation between the models. For example, the SAFENET model places the Operating System at Layer 8 while the SIM Model places Networking Services and Operating System Services on the same layer. This is not a problem, however, as the objective of defining the models is to provide a **perspective** of the problem and solution domains, i.e. they are paradigms.

4. System Architecture Synthesis

Having analyzed all the allocated and derived requirements of the Integrated Combat System as well as defined Information Management and Communication Models, the synthesis of an Information Management Infrastructure can proceed.

The approach is to allocate chosen options to each of the layers of the respective models. This is done after review of the characteristics of all the potential candidates for these layers. This is addressed in some detail in Appendices A and B.

Of specific significance to the choice of appropriate options, is their ability to support real-time performance.

4.1 Cable Plant

The chief attributes that are sought of the Cable Plant are that it :

- supports present and future functional (i.e. bandwidth and synchronisation) requirements
- meets the physical (mass and size) requirements
- meets the electromagnetic compatibility requirements
- meets the reliability requirements
- meets the supportability requirements

While copper-based cable plant can meet the latter two requirements, it falls short in meeting the first three. Fibre optic cable is the only medium that can support all the requirements. While fibre optic components such as cable, connectors, splices and interconnection systems have not exhibited adequate reliability and supportability for critical shipboard systems in the past, this situation is rapidly being overcome through research and product development. A range of products is now undergoing qualification and will be available for the next generation of warships [9.2.7, 9.2.3].

4.2 Communication Standards

A detailed analysis of communication standards is provided in Appendix B. It is concluded [Paragraph 2.1, Appendix B] that none of the currently used standards will meet all of the requirements of the next generation of ICS IMI.

It is also concluded that it is highly desirable to utilise a commercial standard that :

- meets present and future functional requirements
- is finding widespread application
- has significant reserves of data transfer capacity

The FDDI (Fibre Distributed Data Interface) is a new international standard which meets all these requirements.

As is indicated in Table I, the ANSI FDDI standard is prescribed at Layers 1 and 2 for the SAFENET II protocol suite. FDDI [9.2.8, 9.2.15] is an optical fibre network offering high speed, reliable and fault-tolerant data transfer at 100 $Mbits^{-1}$. FDDI is a commercial networking standard designed to support data-intensive applications such as image processing, image and real-time distributed databases and graphics in LAN (Local Area Network) and MAN (Metropolitan Area Network) topologies.

While FDDI does not strictly support deterministic data transfer (c.f. MIL-STD-1553), its timed-token protocol and synchronous/asynchronous message modes, as well as its throughput, does adequately support reliable networking for an ICS. FDDI also offers the low bit error rate (BER) of $2,5 \times 10^{-10}$.

The major features of FDDI, as well as an analysis of FDDI Ring Latency Time, are detailed in Appendices B and C respectively.

4.3 Communication Protocols

A detailed analysis of communication protocols is also provided in Appendix B. It is concluded [Paragraph 2.2, Appendix B] that none of the currently used protocols will meet all of the requirements of the next generation of ICS IMI.

It is also concluded that it is highly desirable to utilise a standard commercial protocol (or set of protocols) that :

- meets present and future functional requirements
- supports the chosen communication standard
- has significant reserves of routing capacity

4.3.1 XTP

The XTP (Express Transfer Protocol) [9.1.21, 9.2.14] is a developing standard which meets all these requirements.

As is indicated in Table I, XTP is prescribed at Layers 3 and 4 for the SAFENET II protocol suite. XTP is a light-weight protocol specifically designed for **parallel** operation as opposed to serial operation. XTP has also been designed for solid-state implementation, rather than firmware or software implementation. Chipsets are currently available that can handle throughputs of up to 200 $Mbits^{-1}$ or 100 000 packets per second. The major attributes of XTP are error, flow and rate control, optimised inter-network addressing mechanisms and reliable multicast support.

The major features of XTP are detailed in Appendix B.

4.3.2 TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) [9.1.4] is a set of protocols providing services that communicate between, and control,

incompatible computers and networks. It is sometimes dubbed "the Rosetta Stone of Internetworking". It provides point-to-point, guaranteed-delivery communication between networked nodes and was originally designed for packet switching communications.

Despite being somewhat dated in terms of performance and capability, there are many qualified implementations of TCP/IP for many platforms. Even if it is for this reason alone, TCP/IP cannot be discarded as an option for the short term.

4.3.3 ISO TP4

TP4 is the ISO Class 4 Transport Protocol. Layer 4 of the OSI model (Transport Layer) [9.1.9] consists of five classes of increasing capability with respect to retransmission of lost data, flow control and reordering of packets.

While not providing the highest levels of performance required for LANs and internetworks of the future, the ISO OSI protocols are amongst the most modern of which software implementations exist. Furthermore, the ISO OSI model does currently provide the most widely accepted communications model. For these reasons, ISO TP4 is also a good candidate protocol for the short to medium term.

4.3.4 Global Time Service

The SAFENET defined Global Time Service [9.2.6] will provide to processes within a node a precise Calendar Time (time of day) which is consistent over the LAN. A precision of one binary millisecond is required with provision being made to represent time to a precision of better than a nanosecond over a time span of several hundred years. It also provides a means to co-ordinate this time with an external time reference such as that which may be obtained from a

ship's navigation system and to provide the time stamp in a variety of formats including Greenwich Mean Time. There is no existing or proposed ISO standard for such a service over the LAN.

4.4 Lightweight Support Services

Lightweight Support Services (LSSs) are those services required by certain applications, but are not catered for by the other protocol layers and where latency must be minimised. LSSs are achieved by allowing the implementers maximum flexibility in tailoring communication services at the upper layers to meet the needs of a specific application (e.g. inter-task message passing).

4.5 Real-Time Operating Systems

While not quantitative, this informal analysis illustrates that ultra-high processing speeds are required with absolutely minimum task response times (task switch times) from the operating system. Proposed figures for such times are typically in the order of 100 μs to 500 μs (maximum).

In complex software systems where the functionality is implemented by many software tasks, real-time operation is most effectively implemented under control of a **real-time operating system** (R-T/OS). The R-T/OS manages all system resources including task scheduling, inter-task communication, synchronisation, interrupt handling, memory management and I/O.

Because of the onerous performance requirements of critically real-time systems, real-time operating systems were traditionally programmed using proprietary techniques. This has normally resulted in the corresponding real-time computing system being a ***closed system***, i.e. unable to interface to any system not especially developed for the purpose. Recent advances in hardware and software technology, however, have made it possible to apply the concept of **open systems** to demanding real-time systems. The attributes of

such an operating system are that they should exhibit excellent real-time performance, be compatible with industry standards and be available on a variety of hardware platforms. They should support a variety of standard features, networking and graphical user interfaces, as well as memory and mass storage management.

4.5.1 POSIX

In order to further the objective of open systems, the IEEE is developing standards that will enhance the portability of Unix across different computer environments. In particular, the IEEE is presently developing or refining nine POSIX (Portable Operating System Interface) standards [9.1.11] in specific areas.

Of specific importance to real-time systems are the POSIX 1003.1 *Compliance Test*, POSIX 1003.4 *Real-Time Extensions* and POSIX 1003.4a *Threads Interface*.

4.6 Application Software

Complex systems tend to rely more and more on software to achieve the required functionality. Correspondingly, software systems themselves have tended to become increasingly complex and the development of such systems more labour intensive. While the quality and reliability of hardware systems has increased to the extent where mission and safety critical levels of dependability can be achieved, software is only very recently beginning to achieve a similar status. One of the most important factors in this regard is that concerning **software languages**. A dilemma that exists in the design of a software language is to resolve the conflicting requirements of software productivity and software reliability. Modern languages such as **Ada**, **C** and **C++** are examples of languages which were designed to address these issues.

4.7 Proposed Communication Standards Suite

With suitable candidates and/or alternatives identified for an implementable standards suite, a specific suite can be proposed. Table III shows the RSA SAFENET II Standards Suite with the various options each appropriate level.

<table>
<tr><th>Layer No.</th><th>ISO OSI Layers</th><th colspan="4">Proposed Suite (Maximum Flexibility and Performance)</th></tr>
<tr><td>9</td><td>Application Process *</td><td>C Task</td><td>C++ Task</td><td>Ada Task</td><td>Ada 9X Task</td></tr>
<tr><td>8</td><td>Operating System *</td><td>iRMX Real-Time Operating System</td><td>VRTX Real-Time Operating System</td><td colspan="2">Unix/POSIX Real-Time Operating System</td></tr>
<tr><td>7</td><td>Application</td><td colspan="4" rowspan="3">Lightweight Support Services

(Designed to meet the needs of the specific system)</td></tr>
<tr><td>6</td><td>Presentation</td></tr>
<tr><td>5</td><td>Session</td></tr>
<tr><td>4</td><td>Transport</td><td rowspan="2">TCP/IP</td><td rowspan="2">ISO TP4 Protocol</td><td rowspan="2">XTP Protocol</td><td rowspan="2">Global Time Service</td></tr>
<tr><td>3</td><td>Network</td></tr>
<tr><td rowspan="2">2</td><td rowspan="2">Data Link</td><td colspan="4">IEEE Logical Link Control Class I Protocol</td></tr>
<tr><td>SNMP</td><td>ANSI FDDI SMT Protocol</td><td colspan="2">ANSI FDDI MAC Protocol</td></tr>
<tr><td>1</td><td>Physical</td><td colspan="4">ANSI FDDI Physical Protocol (100 MBits^{-1})</td></tr>
<tr><td>0</td><td>Cable Plant *</td><td colspan="4">Fibre Cable Plant</td></tr>
</table>

Note : * denotes outside the scope of the 7-layer model

Table III : RSA SAFENET II Standards Suite

4.8 Topology

The topology of a system will be derived from the system engineering process and will reflect the functionality and complexity of a particular implementation.

The possibilities are extensive, but one approach that is recommended [9.2.4] is a topology based on logical system segmentation into principal warfare areas. This approach offers flexibility in terms of reconfiguration and

survivability following battle-damage. It also provides for management of bandwidth allocation down to acceptable levels.

One such topology is a MAN connecting the following FDDI LANs :

- Weapons LAN.
- Control LAN.
- ASW LAN.
- EW LAN.
- Ship Management LAN.
- Task Force LAN.
- Image and Voice LAN(s).

Interconnectivity between the LANs would be provided by a **Logic Router**.

Figure 5 represents a topology for a generic, totally integrated combat suite while Figure 5 represents the topology of a single FDDI LAN.

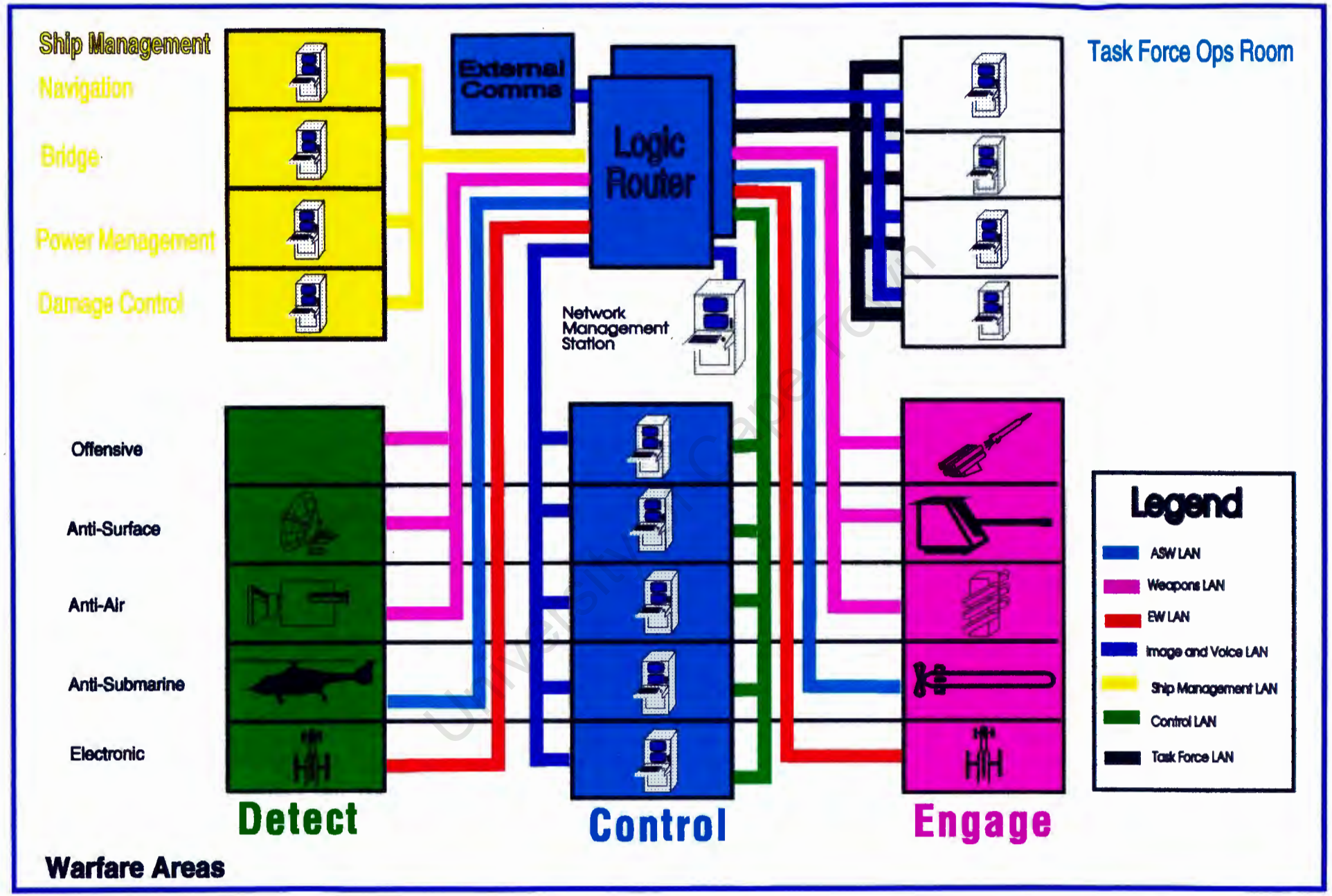


Figure 5 : Generic Fully-Integrated System Architecture

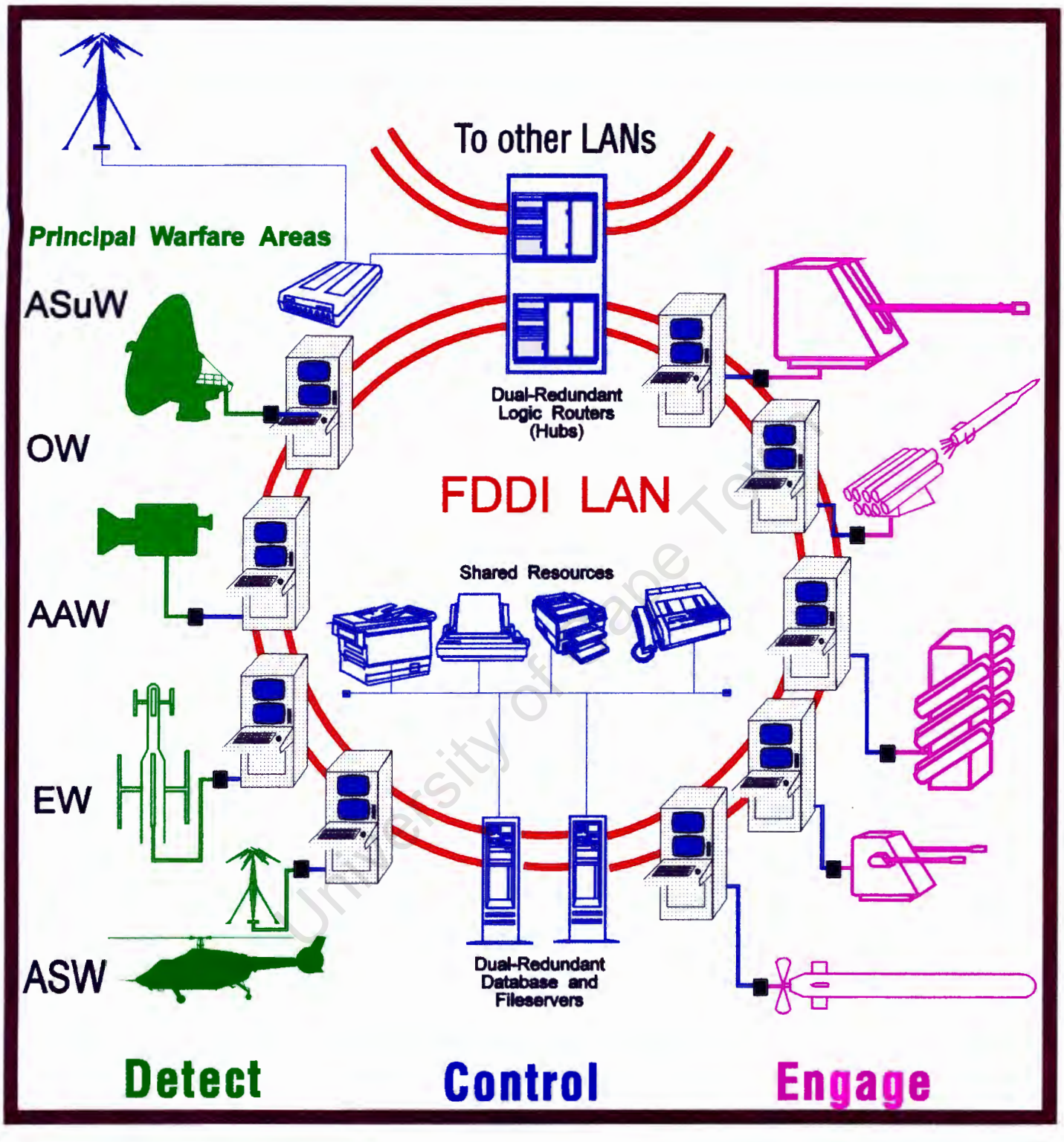


Figure 6 : Single FDDI LAN Topology

file : yfddil1.cdr

4.8.1 Weapons LAN

The Weapons LAN interconnects all surface weapon systems (guns, missiles, etc.) and their associated sensors (radars, infra-red and visible light cameras, optical trackers, etc). Dataflows between these sub-systems are characterised by short, periodic (synchronous) messages with low latency times, initiated aperiodically. Furthermore, many of the related functions involved self-defence (Close-in Weapon Systems, Surface-to-Air Missiles, etc.) and are thus of a safety and mission-critical nature. Thus reliability and timeliness of these messages are paramount.

4.8.2 Control LAN

The Control LAN interconnects all the Standard Naval Consoles (SNCs) which constitute the **Control** function. These SNCs are re-configurable according to mission mode, battle demand and fault/damage. The SNCs are warfare operator consoles and feature man-machine interfaces (MMIs) with high resolution graphic, image and real-time video displays as well as input devices such as rollerballs, joysticks, touchscreens and keyboards. Dataflows on this LAN fall into the following main categories :

- Tactical Database interrogation and update.
- Decision Support Database interrogation and update.
- Graphics sharing between consoles.
- Control Orders to the weapons and sensors.
- Alarms from sensors.

The first three categories of dataflow are characterised by very high volumes. In most cases very low latency is not required. The dataflows also tend to be mostly aperiodic, except in the case of tactical database interrogation during an engagement. These dataflows can be assigned lower priorities on the LAN.

Control Orders and Alarms, however, are critical in nature and require low latency in most cases (e.g. CLOS missile release, chaff and decoy release, etc.). These messages must be assigned high priorities on the LAN and the internetwork. These messages will also be routed by the Logic Router to the appropriate destinations on the Weapons LAN and from relevant sources on the sensor LANs.

4.8.3 ASW LAN

This LAN interconnects all sub-surface sensors and weapons. The Anti-Submarine Warfare (ASW) segment is assigned its own LAN because of the peculiarities of sub-surface warfare. Due to the nature of the submarine environment, target acquisition times are very long (typically 5 minutes to several hours) and involves correlation of data from many sensors. Extensive dataflow can occur between these sensors, the ASW Database, other general databases and the ASW operator(s) (refer Paragraph 4.1 and Paragraph 6.7 of Appendix E). Access to the general databases and the assigned SNC(s) will be via the Logic Router.

In terms of weapon control, modern wire-guided torpedoes require (or allow) regular update of status and control information between both platform and weapon. This involves periodic (typically every 1 second) duplex transmissions of a few hundred bytes of information. More modern variants, however, are able to transmit real-time sonar representation of their targets back to the platform. While copper wire limits the effective transmission bandwidth, data

rates can still be fairly high (ten to hundreds of $kbits^{-1}$). It is expected that these guidance wires will (or already have been) replaced by optical fibres whose effective bandwidth is not effected by the marine environment (c.f. copper wire). Transmissions in the order of several $Mbits^{-1}$ are then likely.

4.8.4 EW LAN

This LAN interconnects all Electronic Warfare (EW) sensors, i.e. signal interception and direction finding equipment and EW "weapons" (e.g. jammers, chaff and decoys). The EW segment is assigned its own LAN because of the time criticality necessary to invoke a jammer after threat detection. The required latencies are in the order of sub-milliseconds. Fairly high bandwidths (a few hundreds of $kbits^{-1}$) can originate from the EW sensors.

4.8.5 Ship Management LAN

The Ship Management LAN interconnects all systems associated with the **Move** function, i.e. Engine Control Room, Bridge, Navigation System and Damage Control Headquarters. Integration with the Combat System, i.e. the **Fight** function, will become an increasingly desirable capability in order to optimise fighting effectiveness and survivability. Capabilities such as **real-time** Radar Cross-Section (RCS) minimisation, power management, optimal orientation for chaff deployment and threat engagement are applicable here.

While the Navigation System provides navigation capability to the **Move** function, it also has another critical function of providing Ship Stabilisation Data (roll, pitch, yaw, velocity) to the sensors and weapon control systems. Accurate Ship Stabilisation Data (possibly including first and second derivatives) is critical to the closed-loop control

of these systems. Ship Stabilisation Data will be **multicast** to the required destinations through the Logic Router. The data will be of periodic nature with typical update rate of 5 ms; as such it should be afforded a high priority on the internetwork. The Navigation System will also include a Global Positioning System (GPS) and Real-Time Clock. The GPS will provide accurate (sub-millisecond) Calendar Time to the platform, while the Real-Time Clock will provide precision synchronisation to the entire system. Both Calendar Time and Synchronisation will be broadcast through the Logic Router to all systems which have these requirements. These two data messages should be afforded the highest priority on the internetwork.

4.8.6 Task Force LAN

The Task Force LAN is similar in function to the Control LAN and would be provided on larger vessels, i.e. frigate upwards, where the surface combatant was operating in a battle group or task force and the Task Force Commander was assigned his or her own operations room. The Task Force Operations Room would typically be equipped with a number a Standard Naval Consoles which would require interconnection between themselves as well as to certain onboard systems. Most of the data flowing between the Task Force Operations Room and the onboard systems would be extensively processed summaries of the local scenario. The Task Force Commander would obviously have a primary interest in proceedings off-ship, i.e. on other vessels of the Task Force, Air Assets as well as Operational and Naval Headquarters. For this the system would be linked to the outside world by a number and variety of data links via the Link Connection. The data links would be implemented as radio modems using a variety of technologies such as VHF, UHF, satellite and spread-spectrum communications systems.

4.8.7 Image and Voice LAN

Image and digital video onboard would arise from a number of different sources, i.e. mission-critical FLIRs (Forward-Looking Infrared device) and Optical Trackers, non-critical helicopter deck observation cameras, scan-converted radar and from various image databases. The attribute which characterises all these sources is the extensive bandwidth they require over the networks. Another capability which is required onboard is to display certain images simultaneously at different consoles. An example could be the case of an incoming threat missile being observed by a number of sensor and weapons operators as well as the Commanding Officer, Weapons Officer and Task Force Commander. There is thus the requirement to multiplex and multicast image data. For this reason it is recommended that image and digital video signals be allocated their own LAN (or LANs) where they will not saturate more critical data transmissions. Thus the Image LAN(s) interconnect(s) all nodes which are sources or destinations of such data.

Voice transmission requirements onboard are similar in nature to video because, despite extensive integration of functions across the platform, there will always be a heavy reliance on voice communications between operators, especially during critical phases of combat. The most important difference between voice and video is that the former requires some tens of $kbits^{-1}$ while the latter requires some $Mbits^{-1}$ (after compression). While voice and video may not be physically transmitted on the same LAN, they are grouped here for the sake of simplicity.

A special requirement of real-time digital video and voice is that circuit-switched services are required.

Standard FDDI does not support this facility and so either of the following must be implemented :

- Custom protocol extension to FDDI.
- Adoption of FDDI II LAN standard (when available).
- Adoption of other real-time LAN standard (when available).

4.9 Logic Router

The Logic Router would consist of an intelligent, modular, high-performance FDDI router capable of routing up to eight FDDI LANs simultaneously. In commercial networking terminology, the Logic Router could be termed a "Smart" Hub. Such devices can also cater for other LAN technologies such as Ethernet and Token Ring and the Logic Router could be used to connect such equipment should this be appropriate.

Although system operation would be possible in the case of failure of the Logic Router, this would be in a degraded mode. For this reason, the Logic Router should be dual-redundant, with two identical equipments physically situated so as to maximise survivability following battle damage.

A desirable capability of the Logic Router is that which is known as 'hot swapping'. Such a capability would allow on-line maintenance of the network by swapping of the appropriate modules within the Logic Router while it remains powered-up. This would negate the otherwise significant downtime that could result if the equipment had to be switched off and then rebooted after re-configuration.

4.10 Network Management

Another requirement for the Logic Router would be its capability of effective network management. Network Management would be effected at two levels; the lower level (up to Layer 3) by the Logic Router and the higher level by Network Management Station (NMS).

The Logic Router would provide real-time monitoring and control of the entire LAN system, statistical measurement, event reporting and low-level diagnostics facilities.

The FDDI standard provides a Station Management Layer (SMT) [9.1.11]. This, however, only offers a kernel for station management and some higher-level functionality must be provided in order to implement total network management. Two main options are available, neither being totally adequate [9.2.37].

4.10.1 Parameter Management Frames

Parameter Management Frames (PMF) is an optional station management layer of the FDDI standard. The advantage of PMF is that it has been optimised to operate in a homogenous FDDI environment. The disadvantages are that it cannot operate in a heterogeneous LAN environment and that SMT cannot be bridged or routed without a proxy agent (protocol conversion).

4.10.2 SNMP Management Information Base

Another option is SNMP (Simple Network Management Protocol - part of TCP/IP) Management Information Base (MIB) which is an emerging standard. The advantage of SNMP MIB is that it is a routable protocol that can operate in a heterogeneous LAN environment. The disadvantages are that it cannot support certain features of FDDI hubs such as multiple buses on the backplane.

4.10.3 Network Management Station

The NMS would provide on-line monitoring and control of the entire IMI, re-configuration management and high-level diagnostics (BIT) facilities. It would consist of a Naval Standard Console, either dedicated to this function, or within another item of equipment which was not required for full-time warfare

operations (i.e. it would be software function). The configuration and complexity of the NMS would be dependent on the sophistication and complexity of the combat vessel.

4.11 LAN Connectivity

All critical sub-systems on the LANs would be FDDI Dual-Attachment Stations (DASs). Non-critical sub-systems could be FDDI Single-Attachment Stations (SASs) connected by FDDI Concentrators. Non-critical, bought-out sub-systems would be connected by gateways. Gateways would typically support Ethernet, IBM Token-Ring, MIL-STD-1553B, RS-232 and RS-422 communications standards.

4.12 Wide Area Connectivity

Typical combat scenarios will involve multi-ship co-operation with the sensors of one platform providing targeting data to another's weapons. There are also requirements for concurrent, shared databases amongst a variety of on-board and off-board systems to provide for decision support for the battle group commander and his or her staff.

Such capabilities will be provided by employing gateways to RF communications systems and would be implemented by radio modems such as Link-16.

4.13 Fault Tolerance and Reconfigurability

The requirement for availability of a system is derived from two perspectives; firstly the system must be ***available*** when called into use and secondly the system must be ***fault-tolerant*** whilst in use. The attributes of reliability and maintainability contribute to the availability of a system whilst redundancy and reconfigurability contribute to fault-tolerance.

Fault-tolerance can be achieved by the implementation of multiple levels of redundancy; from integrated circuit (IC) level, through card, sub-assembly and assembly level to sub-

system level. On-line reconfiguration and **system BIT** (Built-in Test) are important mechanisms by which fault tolerance can be achieved.

Implementation of such technologies such as **Flash EPROM** [9.2.30] offers significant advantages in achieving on-line reconfigurability. Flash EPROM , in particular the capability of In-System Write (ISW), allows for the on-line download of code from a central fileserver while still maintaining code integrity in the case of power failure or LAN failure. This capability also provides for enhanced upgradeability as computer boards do not have to be removed from equipment racks, thus providing for less down and requalification time as well as increased user confidence following set-to-work.

4.14 Security

With such a high degree of data and information integration, both onboard as well as with other operational systems, including headquarters, there are critical requirements for sophisticated security features implemented throughout the Information Management System. Applications and operating systems must offer multilevel password and key control features, while all data over the LANs and data links should be encrypted.

4.15 Database Management

Knowledge is an abstraction derived from the processing of information which in turn is an abstraction derived from the processing of data. On a weapons platform, data is gathered from many and varied external sources, including on- and off-board sensors. The repository for this data, assuming an integrated system, is a number of shared databases. These databases are managed by database management systems. These are constructed from computer hardware and software building blocks. The required attributes for these database management systems are real-time and on-line capability.

Many different configurations of databases exist; i.e. distributed, centralised, relational and client-server.

Problems arise in the resolution of providing coherency, integrity and security for these databases. Specific configurations are better suited to mission-critical, real-time applications.

For a fully-integrated combat system, three types of databases will exist; these are tactical, decision support and ship support databases. While the latter may only require on-line capabilities, the tactical database will be both real-time and mission-critical.

Databases and Database Management Systems are addressed in detail in Appendix E.

4.16 Image Processing

Image processing will play an increasing role in providing enhanced war-fighting capability.

Image processing consists of the following processes :

a. Image capture from infra-red, video or low-light cameras as well as radar, sonar and other imaging systems.

b. Digitisation of the input analog signals by means of frame grabbers and scan converters.

c. Digitisation of document images by means of digital scanners.

d. Image manipulation including format conversion, image enhancement, image recognition and compression.

e. Image transmission by means of high-bandwidth media.

f. Image transmission multiplexing from various sources to various destinations simultaneously.

g. Image storage in image databases supported by high-capacity storage systems such as optical disk drives.

h. Image rendition by means of high-resolution colour display systems.

Typical image databases may contain perceived threats that may be encountered on a mission and charts of the areas where the mission is carried out. Any other digitised image, e.g. actions captured photographically during a mission, new enemy threats encountered and photographed as well as reconnaissance photographs can also be stored in the image database.

A digital scanner would provide the ability to scan threats, charts and maps as well as any illustration or document. A colour printer would be provided to print maps or images from the image database. These can be used for mission planning, debriefing procedures, intelligence gathering and operational records.

4.17 Ruggedization

It is proposed that commercial equipment be used wherever possible. There are three main reasons for this :

- Commercial products are normally more advanced than military products in terms of technology and functionality.

- The Naval environment is harsh, but not extremely so (c.f. space and avionics environments).

- The cost of commercial equipment is considerably less than that for equivalent fully military-qualified parts (sometimes an order of magnitude lower).

However, most commercial equipment is not adequately packaged for the naval environment. In these cases the equipment should be repackaged and/or ruggedised. Ruggedization is an effective and fairly inexpensive option that can be implemented without extensive technological resources (as in the RSA). Techniques that are applicable are the fitting of shockmounts (wire-rope shockmounts are very effective),

vibration dampers, cooling, anti-condensation heating, conformal coating of PCBs, etc. Connectors are often a weak point in commercial equipment and these should often be replaced with industrial, or even military specified parts where appropriate. Another consideration is the naval requirement for all equipment to exhibit low combustion toxicity and to be non-halogenoid.

5. ICS Concept Demonstration Model

5.1 Scope

The scope of the work was the development of a LAN-based, distributed processing, Naval Integrated Combat System (ICS) Architecture Concept Demonstration Model (ACDM) [9.2.39] in terms of the following **Description of Work.**

a. Acquisition and integration of commercially-available, industry-standard, hardware and software building blocks into a skeletal system representing the ICS's LAN-based, distributed processing architecture.

b. Value-added software development to support architecture concepts.

c. Characterisation of the following requirements :

i. System timing and synchronisation.

ii. Critical resource redundancy.

iii. Global data distribution i.e. broadcast of common data (Calendar Time and NAV Data).

iv. Image Transfer (i.e. digital video).

v. Reconfigurability and Station Management.

vi. Multiprotocol data transfer i.e. gateways, bridges and routers.

vii. Data transfer determinism.

viii. Resource sharing.

ix. Preliminary data transfer protocol.

x. System security.

b. The following outputs were to be generated :

i. A demonstration of the integrated system.

ii. A report on the system and the characteristics addressed above.

iii. *Preliminary Protocol Description.*

5.2 WORK COMPLETED

Work, as detailed below was completed. Refer to Figure 7 *ICS ACDM Topology* for a diagrammatic representation of the system topology and applicable technologies.

5.2.1 Network

A fileserver hosting Novell NetWare V3.11, supporting NetWare Streams and TCP/IP, was configured and set-to-work. The fileserver supported disk mirroring as disk storage was considered to be critical network resource.

The fileserver and the network workstations (386 and 486 PCs) hosted dual-attached FDDI communications controllers.

The network supported an Ethernet bridge to the branch network (two Ethernet LANs) to the external company wide-area network (WAN) via a modem gateway.

5.2.2 1553 Gateway

One FDDI network PC acted as a MIL-STD-1553B gateway to two 286 PCs on a MIL-STD-1553B bus.

One 1553 PC simulated a Navigation Sub-System ('NSS') which broadcast simulated NAV Data to the whole network. The 'NSS' received Calendar Time information

from the Global Positioning System (GPS) host via the FDDI/1553 gateway.

5.2.3 Image Transfer Infrastructure

This was implemented by using a commercial Super VHS video camera mounted on a remotely-controllable pan and tilt system. The analogue video signal was digitised by a PC-compatible frame grabber card.

The digitised images were transferred by the FDDI ring using the TCP/IP protocol from the Frame Grabber Unit (FGU) to an Image Monitor Unit (IMU) where they were displayed immediately. Software was used to convert the image formats to high-resolution VGA for display, storage and retrieval.

Images acquired from the video camera or image database could be printed on an on-line A4 Tektronix Phaser II thermal wax colour printer.

A high-resolution, A4, flatbed, colour scanner was used to capture digital images, including charts, threat images and documents for entry into the database.

5.2.4 GPS

A PC-compatible GPS system was hosted within a network workstation. The GPS provided Calendar Time and Position which was broadcast to all network workstations as well as stored in an on-line database.

The GPS Calender Time provided real-time synchronisation, by means of the broadcast capability, to the system via the network.

5.2.5 Meterological Station

An externally-mounted Meterological (Met) Station consisted of wind-speed, wind-direction, relative humidity (RH), air temperature and barometric pressure sensors as well as an RS-232 communications interface. The Met Station provided these parameters to a network workstation which in turn broadcast them to all other network workstations as well as stored them in an on-line database.

5.2.6 Database Management System

A client-server architecture SQL database (SQLBase) provided database management facilities to the system. A database server provided for data storage and manipulation facilities, while database clients provided database access.

5.2.7 Software Development

A extensive amount of software, supporting FDDI protocol, network operation and synchronisation, image processing, printing, database management, GPS, 1553 gateway, Met Station and MMI functions were developed and demonstrated.

5.2.8 Communication Protocols

The FDDI/NetWare interface was implemented by means of the TCP/IP and SPX/IPX protocols, supported by commercial PC FDDI Boards. The two protocols were proved to co-exist peacefully together.

5.3 Problems

5.3.1 Real-Time Image Transfer

The requirement for animation-quality (real-time) image transfer is some 25 frames per second. This translates to some 25 $Mbits^{-1}$, which is well within the

specified 100 Mbits^{-1} of FDDI as well as the quoted 30-40 Mbits^{-1} of the PC FDDI boards.

Extensive effort was expended in attempting to achieve transfer rates of 20 to 25 frames per second. Only 5 frames per second could be achieved successfully, however. Rates in the order of 10 frames per second were achieved, however the integrity of the image was not maintained at this rate.

It was determined that the problem lay in the limited throughput of PC ISA backplane bus and TCP protocol (< 1,2 Mbytes^{-1}).

It is concluded that an EISA (Extended Industry Standard Architecture) or Multibus II processing platform, including frame grabber and FDDI Communications Controller, would support real-time image transfer. Protocols such as XTP would further enhance real-time data communications.

Despite this, real-time image transfer was not a project objective in itself. It was mainly a mechanism of demonstrating and stressing the throughput capability of the FDDI LAN.

5.3.2 Real-Time Database Management

While SQL database management systems such as SQLBase do provide adequate **on-line** capability, these cannot provide **real-time** performance. One reason for this is that the databases are stored in serial-access, magnetic or optical storage systems. A real-time database will have to exist in random-access memory, preferably non-volatile.

5.3.3 Fileserver Mirroring

As a fileserver is a critical item within a LAN system, this should be mirrored to provide

redundancy. At present NetWare does not support fileserver mirroring, but does support disk mirroring and duplexing, the latter having been implemented. It has been determined that such operation is not totally reliable and requires further investigation into causes and solutions. Further releases of NetWare, i.e. Version 4 in early 1993, should offer better reliability and functionality in this area. Full server mirroring is also expected in this release.

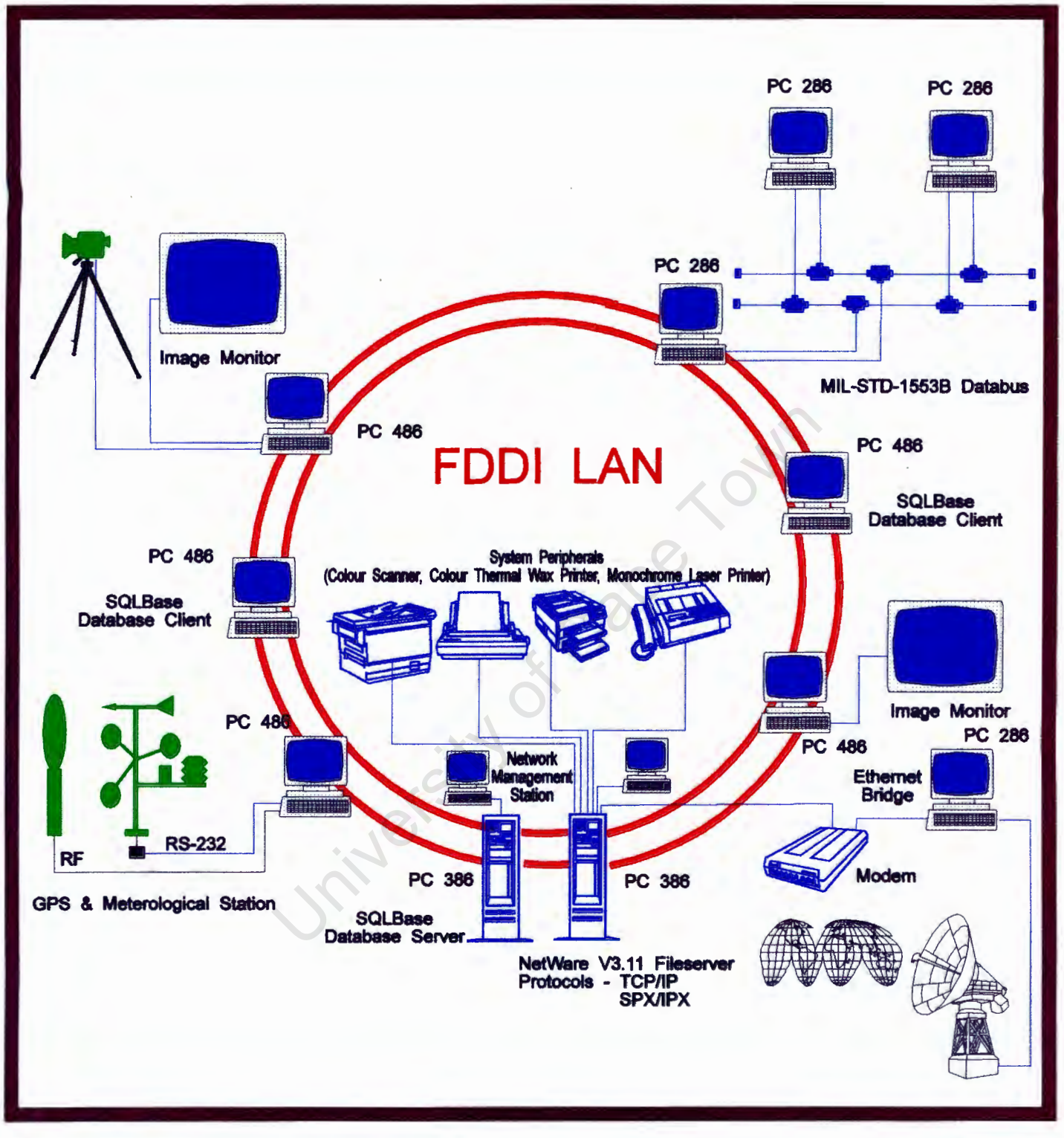


Figure 7 : ICS ACDM Topology

file : ytacdm1.cdr

6. Costs

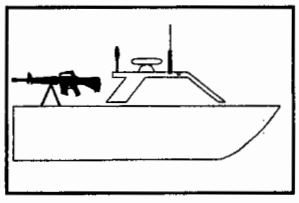
The following are typical **order-of-magnitude** costs for various implementations. The medium, high and very high complexity implementations assume some measure of value-added engineering as well as amortisation of development costs over at least four platforms.

The costs indicated are applicable to both new constructions as well as refit to existing vessels, but would be marginally higher in the latter case.

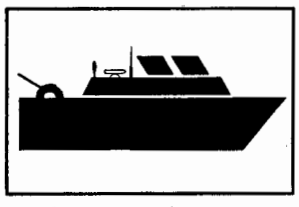
Configuration — Cost

Low Complexity — R500 000

5 x Rugged PC Workstations
Fileserver
FDDI LAN
C Software
Laser Printer
Video Camera
Facsimile
Tactical Data Link
Meterological Station
GPS (Commercial)
Navigation Radar (Commercial)
Echo Sounder (Commercial)
Laser Range Finder
Low-light CCD Camera
System Engineering
Installation
Integration
Qualification



EEZ Protection Vessel



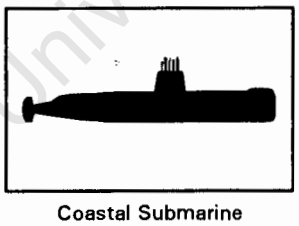
Armed Merchantman

Note : The cost **does** include the price of the PC Workstations

Medium Complexity — R2 000 000

5 x Workstations
Fileserver
On-line Database Server
FDDI LAN
C Software
Laser Printer
A4 Colour Printer
A4 Colour Scanner
Video Cameras
Frame Grabbers
System Engineering
Installation
Integration
Documentation
Qualification

Strike Craft



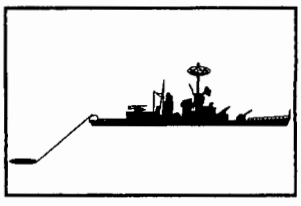
Coastal Submarine

Note : The cost does **not** include the price of the workstations

Configuration — Cost

High Complexity — R5 000 000

20 x Standard Naval Consoles
Mirrored Fileservers
Network Management Unit
SAFENET II
Real-Time Database Server
Logic Router
Gateway
Ada Software
Laser Printer
A3 Colour Printer
A4 Colour Scanner
Video Cameras
Frame Grabbers
System Engineering
Navalised Hardware
Installation
Integration
Documentation
Qualification

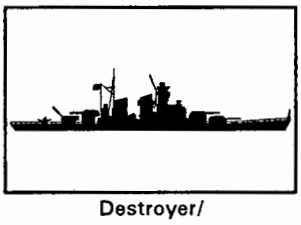


ASW Frigate

Note : The cost does **not** include the price of the Standard Naval Consoles

Very High Complexity — R15 000 000

40 x Standard Naval Consoles
Mirrored Fileservers
Network Management Unit
SAFENET II
Image LAN
Real-Time Database Servers
Logic Routers
Gateways
Ada Software
Laser Printer
A3 Colour Printer
A4 Colour Scanner
Video Cameras
Frame Grabbers
Scan Converters
Image Processing
System Engineering
Military Hardware
Installation
Integration
Documentation
Qualification
Full Integrated Logistic Support



Destroyer/ Battleship

Note : The cost does **not** include the price of the Standard Naval Consoles

7. CONCLUSIONS

7.1 Architecture Concept

It is concluded that LAN-based architecture solutions offer considerable advantages over centralised, star-wired systems. The attributes of fault-tolerance, survivability, flexibility, expandability and upgradeability are well supported by a LAN-based distributed architecture.

The specific proposed solution offers further advantages in that a higher degree of integration is possible without the inappropriate mixing of diverse data types on the same LAN. The problems associated with this, e.g. responsibility for integration, qualification, etc., have largely contributed to the very conservative approach up until recently by most major navies of the world. The proposed architecture is thus considered to be a good compromise of federalism, performance and cost-effectiveness.

The proposed architecture is also very flexible in terms of system design options, scalability, on-line and onboard reconfiguration, as well as system upgrade.

The novelty of the architecture lies in the use of the Logic Router (or 'Smart' Hub). This allows functional partitioning without retarding data throughput or latency. Such devices are available commercially and it is concluded that, ruggedised and configured for dual-redundancy, these would be suitable for most applications, specifically the future surface combatants of the South African Navy. The performance of routers is also improving rapidly with the advance of computer technology. High performance processors, including RISC processors, backplanes (e.g. Futurebus+) and CAM (Contents Addressable Memory) devices will be significant in this regard.

7.2 Relationship of Implementation and Models

It is concluded that suitable models for the management of information and communication have been identified, modified and adopted. These are the Strategic Information Management, SAFENET II and RSA SAFENET II Models respectively.

The RSA SAFENET II Standards Suite is presently achievable, flexible and has considerable scope for upgradeability without major implications to the system.

Technological solutions for each of the appropriate layers of the models have been considered (Appendix B), with at least one achievable solution being finally recommended. Where the recommended SAFENET II option is considered inappropriate for some reason, alternatives have been recommended. Thus the total Information Management Infrastructure has been synthesized in terms of these models, the allocated and derived requirements and available technology.

7.3 FDDI LAN Standard

The FDDI LAN standard offers intrinsic redundancy, determinism, low error rates and electro-magnetic compatibility while supporting high data throughput at affordable cost.

The ACDM project demonstrated that FDDI is reliable, affordable, effective and relatively simple to use.

It is interesting to note a recent announcement (March 1992) that FDDI is being adopted as the LAN standard in Royal Navy submarine combat systems [9.2.38].

7.4 War-fighting Capability

Applying Information Technology to warship combat systems greatly enhances their war-fighting capabilities. Information Technology will play an increasingly important role in providing the *critical edge* in the combat environment.

In the medium term, i.e. 5 to 15 years, a surface combatant without such capabilities could, in fact, be effectively defenceless even in a typical third-world threat environment.

The information processing capability of a surface combatant will have to be continually upgraded throughout its life. This will place a heavy burden on the Information Management Infrastructure. This implies that the IMI should be designed with considerable spare capacity (i.e. 50% to 200%).

7.5 Scalability

The architecture, technologies and topologies that have been proposed are scalable to provide value-added, cost-effective solutions to **any** class of vessel, from a multi-purpose destroyer, to an ASW frigate, a submarine, a coastguard vessel or even an EEZ protection vessel.

In the case of the latter two classes of vessel, a modest investment in an **integrated system** will provide a **force multiplication** which is affordable even to organisations of limited means.

The proposed systems are applicable to both new constructions as well as refit to existing vessels.

7.6 The Paperless Operating Environment

A paperless operating environment contributes significantly to a more effective war-fighting capability. It will also contribute to lower crew-levels and enhance supportability.

The proposed Information Management Infrastructure contributes extensively towards providing a paperless environment.

The Paperless **Operations Room** is achievable within context. Due to the operational doctrine of all navies, some paper will always be required, however.

7.7 User Commitment

The implementation of an Information Management Infrastructure is not inexpensive and requires full commitment from the user organisation in terms of planning, construction, implementation, operation and support.

7.8 Rapid Prototyping and Risk Reduction

Effective application of rapid prototyping reduces implementation timescales as well as technical risks.

Rapid prototyping also provides for performance benchmarking which is critical in the environment of off-the-shelf building blocks. Specific areas where this is critical are timing, synchronisation, throughput and interfacing.

7.9 Standard Building Blocks

There are many hardware and software products available supporting specific areas of an Information Management Infrastructure solution.

There are many organisations offering partial, proprietary solutions. When these products become obsolete, so will their systems.

Non-standard solutions have limited life-cycles.

7.10 Image Processing

Real-time image processing requires computer resources far in excess to that which can be provided by software hosted by general purpose computers. To achieve acceptable performance requires purpose-built, image processing hardware usually utilising RISC and digital signal processing techniques.

7.11 Data Transmission Determinism

FDDI is sufficiently deterministic to support real-time synchronisation, i.e. within 500 μs (where LANs are geographically small to medium in size i.e. less than 2 km in diameter).

7.12 Message Multicast

Unicast, multicast and broadcast of messages can be achieved.

7.13 Communication Gateways

Gateways to support a variety of data communication standards are easily implemented.

7.14 Integrated Data and Image

Integrated data and image is possible with FDDI.

7.15 Real-Time Video

Real-time digital video, i.e. image, with FDDI is possible although not optimum in the case of geographically-extensive LANs (i.e. in excess of 10 km in diameter).

7.16 Real-time Image Multiplexing

Real-time image multiplexing over the LAN/MAN with compression hardware is possible.

7.17 Multiprotocol Operation

Multiprotocol operation is possible. Protocols (NetWare V3.11 SPX/IPX and TCP/IP) do co-exist peacefully.

7.18 Circuit-Switched Services

FDDI only supplies packet-switched services. Real-time digital signal such as video and voice require circuit-

switched services. There is a requirement for LANs supporting these services (e.g. FDDI II and FDVDI).

7.19 High-Performance Protocols

There is a requirement for high-performance protocols e.g. XTP (Xpress Transfer Protocol).

7.20 Real-Time Operating Systems

There is a requirement for a real-time operating system e.g. Unix/POSIX.

7.21 Real-Time Database Management Systems

There is a requirement for a real-time database management system.

8. RECOMMENDATIONS

8.1 System Engineering

A system engineering effort should be applied to provide a total solution to the implementation of a combat platform's Information Management Infrastructure. This effort should be tailored strictly according to the extent of the requirements.

The solution should also be tailored according to the user's needs and means.

The provision of the Information Management Infrastructure should be co-ordinated by a single party because, despite the layered approach, the nature of the services is such that they are *closely-coupled*.

Individual capabilities, mainly in the Application and User Interface Layers, should be provided by a variety of specialists in their particular fields.

8.2 Rapid Prototyping

Rapid prototyping should be employed to aid the system engineering efforts, especially so as to involve the user's operational staff as early as possible during development. This will lead to a more appropriate system design and implementation as well as reduce development costs and timescales.

8.3 Standards

The solution should be strictly standards-based.

As far as possible, the system should be constructed from available, off-the-shelf building blocks, ruggedised if necessary.

One exception to this applies in the area of the Fibre Optic Cable Plant. It is recommended that fully qualified parts, such as cables, connectors and splices are used unless rigorous analysis shows lower quality parts to be appropriate. It is further concluded that the extra outlay in this area will prove cost-effective in terms of the platform life-cycle.

Future combat systems should be constructed from building blocks based on commercial technology, including the following standards :

Standard	Function
FDDI	Dual-Redundant Fibre-Optic LAN
SAFENET II	*Survivable Adaptable Fibre Embedded Network* Profile
Futurebus+	Parallel Backplane Bus
Unix/POSIX	Real-Time Unix Operating System
Ada	High-Level Language
TBD	Real-Time Database Management
TBD	Presentation Layer Interface

8.4 Open-Systems Architecture

The solution should be based on an open-systems architecture providing for product obsolescence management, flexibility, upgradeability and life-cycle support.

8.5 FDDI and Protocols

While full SAFENET II compliance is considered the ultimate technological objective in terms of LAN implementation, this should be achieved by a *stepping-stone* approach; i.e. by

migration through the interim solutions such as TCP/IP to a final acceptable set of standards.

8.6 Operating Systems

The POSIX operating system extension should be used to provide a portable, real-time, deterministic, multiprocessing, Ada-compatible, networkable operating system.

8.7 Future Development

While significant progress was made in certain technology areas and many potential shortcomings of presently-available implementations identified, much progress needs to be made at all layers of the Information Management Infrastructure before full confidence in local engineering capability could be justified.

Only through concerted and co-ordinated effort, with appropriate funding, can this situation be resolved and place the RSA in a position to tackle a surface combatant build programme in time to replace our present naval surface capability when it reaches the end of its life-cycle at the turn of the century.

9. REFERENCE DOCUMENTS

9.1 Standards

9.1.1 MIL-STD-1553B - Digital Time Division Command/Response Multiplex Data Bus (1978).

9.1.2 DOD-STD-1773 - Fibre Optic Mechanisation of an Aircraft Internal Time Division Command/Response Multiplex Data Bus.

9.1.3 MIL-STD-1760 - Aircraft/Store Electrical Interconnection System.

9.1.4 MIL-STD-1777 - Internet Protocol (1983-08-12).

9.1.5 MIL-STD-xxxx - Survivable Adaptable Fiber Embedded Network (Draft) (1992-01-10).

9.1.6 DOD-STD-2167A - Defense System Software Development (January 1988).

9.1.7 MIL-STD-1815A - Ada Language Reference Manual (1983-02-17).

9.1.8 STANAG 3910 - High Speed Data Transmission under STANAG 3838 or Fibre Optic Equivalent Control (1989-06-23).

9.1.9 7498-1984(E) - ISO Opens Systems Interconnection - Basic Reference Model (October 1983).

9.1.10 FIPS 146 - Government Open Systems Interconnection Profile (GOSIP) (August 1988).

9.1.11 IEEE P1003.1 - POSIX Compliance Test.

9.1.12 IEEE P1003.4 - POSIX Real-Time Extensions.

9.1.13 IEEE P1003.4a - POSIX Threads Interface.

9.1.14 IEEE 802.2 - Logical Link Control (November 1982).

9.1.15 IEEE 802.3 - Carrier Sense Multiple Access with Collision Detect Protocol (1982).

9.1.16 IEEE 802.5 - Token-Passing Ring LAN (1985).

9.1.17 X3.166-1988 - ANSI FDDI Physical Media Dependent Protocol (Rev. 9) (1989-03-01).

9.1.18 X3.148-1988 - ANSI FDDI Physical Layer Protocol (1988).

9.1.19 X3.139-1987 - ANSI FDDI Media Access Control (1986-11-05).

9.1.20 X3T9.5 Draft - ANSI FDDI Station Management (Rev. 6.2) (1990-05-18).

9.1.21 XTP Protocol Definition, Revision 3.6, Protocol Engines, Inc., January 1992.

9.1.22 Manufacturing Automation Protocol, Revision 3.0, General Motors Corporation, April 1987.

9.2 Other Documents

9.2.1 *SAFENET Executive Summary*, US Department of Defense (1991).

9.2.2 *MIL-STD-1553B and the Next Generation - Conference Volume* (ERA Technology), 1989.

9.2.3 Felisky, T., Michael, G.W., *Ships Transfer Data on Fiber-Optic Cables*, Rockwell Corp.

9.2.4 Zitzman, L.H., Falatko, S.M., Papach, J.L., *Computer System Architecture Concepts for Future Combat Systems*, Naval Engineers Journal, May 1990.

9.2.5 *Command and Control*, Navy International Magazine, November 1991.

9.2.6 Green, D.T., Marlow, D.T., *Application of LAN Standards to the Navy's Combat Systems*, Naval Engineers Journal, May 1990.

9.2.7 Knudsen, D.R., Brown, G.D., Ingold, J.P., Spence, S.E., *A Ship-Wide System Engineering Approach for Fiber Optics for Surface Combatants*, Naval Engineers Journal, May 1990.

9.2.8 Ullal, J.V., McCool, J.F., *Fiberoptic network standard delivers speed and reliability*, Computer Design, October 1987.

9.2.9 Duitsman, L.L., Pinelli, M.M. (Boeing Computer Services), *An all-purpose model to aid in all phases of network design*, Data Communication, September 1987.

9.2.10 Sevick, K.C., Johnson, M.J., *Cycle Time Properties of the FDDI Token Ring Protocol*, IEEE Transactions on Software Engineering, Vol. SE-13, March 1987.

9.2.11 Hooton, E.R., Hewish, Turbé G., *Naval command and combat systems*, International Defense Review, Vol. 6, June 1991.

9.2.12 UK MOD, *Principles of Combat System Highway Engineering on the Type 23 Frigate*, (1986-08-14).

9.2.13 European Organisation for the Safety of Air Navigation *Common Operational Performance*

Specifications (COPS) for the Future Controller Operating Environment, Report Version 5, 1991-04-15.

9.2.14 Saunders, R.M., Weaver, A.C., *The Xpress Transfer Protocol - A Tutorial*, Computer Networks Laboratory, Department of Computer Science, University of Virginia (undated).

9.2.15 Ross, F.E., *FDDI - A Perspective*, Fiber Optics Sourcebook.

9.2.16 de Vediere, C., *Naval Combat System Integration - the French Experience*, International Defense Review, 1/1986.

9.2.17 Yanis, E., Schmitt, R., *Design Techniques to Upgrade the Combat System Effectiveness of the FFG 7 Class Frigate*, Proceedings - RINA International Conference on Interaction between Naval Weapon Systems and Warship Design, December 1990.

9.2.18 Ferrerio, L., *Offboard Command Casualty Launch*, Proceedings - RINA International Conference on Interaction between Naval Weapon Systems and Warship Design, December 1990.

9.2.19 Fraser, J.H., *Design Techniques to Optimise the Combat System Effectiveness of the T23 Frigate*, Proceedings - RINA International Conference on Interaction between Naval Weapon Systems and Warship Design, December 1990.

9.2.20 Burt, T.E., *Combat System Integration in the US Navy*, International Defense Review, 1/1986.

9.2.21 de Bakker, G., *Trends in Naval Combat Systems - Part 2*, International Defense Review, 9/1989.

9.2.22 *MEKO Concept Description*, 4/1987.

9.2.23 Finkelstein, R., *Multiuser SQL Databases*, Byte, May 1990.

9.2.24 Ball, J., *Design for Down Under*, Oracle Magazine, Spring 1989.

9.2.25 Scott, K., *SQL Products Are Here, But Is NetWare Ready?*, Data Communications Magazine, 1991-06-21.

9.2.26 Stankovic, J.A., Ramamritham, K., *Tutorial - Hard Real-Time Systems*, IEEE Computer Society, 1988.

9.2.27 van Halm, R., *Real-Time in the Real World*, Unixworld Magazine, 1989.

9.2.28 LynxOS Marketing Brochure, Lynx Real-Time Systems Inc., July 1991.

9.2.29 Marketing Brochure, *GDX Real-Time Relational Database Management System*, Firmware Associates, (1989).

9.2.30 *ETOX™ Flash Memory: The Cost Effective and Reliable Firmware Management Solution*, Intel Corporation, March 1988.

9.2.31 Pinkowitz, D.C., *MIL-STD-1553B: The military standard for avionics integration*, ILC Data Device Corporation, 1984-03-28.

9.2.32 *MIL-STD-1553B Current and Emerging Standards*, ILC Data Device Corporation (1992).

9.2.33 Mazzaferro, J.F and Dell'Acqua, A.A., *FDDI Technology Report*, Computer Technology Research Corporation, April 1991.

9.2.34 *Emerging PC LAN Technologies Report*, Computer Technology Research Corporation, January 1992.

9.2.35 Ochs, T., *In defense of Ada*, Computer Language, December 1991.

9.2.36 Rodd, M.G. and Deravi, F., *Communications Systems for Factory Automation*, University of Wales, 1987.

9.2.37 Greenfield, D. and Keough, L., *Smart Hub Vendors Move In on FDDI*, Data Communications Magazine, October 1991.

9.2.38 *British Navy to use FDDI Networks*, Electronic Design Magazine, March 19, 1992.

9.2.39 Young R.M., *Project Report - Integrated Combat Suite Architecture Concept Demonstration Model*, UEC Projects (Pty) Ltd, October 1991.

9.2.40 Young R.M., *Information Management Infrastructure for an Integrated Combat Suite Architecture*, Proceedings - RINA International Conference on Information Technology and Warships, December 1991.

9.2.41 *Introduction to ATM*, SA LAN Times, September, 1992.

8.1 APPENDIX A

Combat System Comparative Analysis

1. SCOPE

The Databus Architecture study addresses the different interconnect arrangements of the sub-systems within an integrated combat system. A description of the basic philosophy behind the different topologies identified is presented, as well as the pros and cons thereof.

It also addresses the different hardware elements constituting these different topologies and the physical layer specification of different interconnect standards.

The investigation includes the different topologies of integrated naval combat systems that are either deployed at present, under development or under consideration.

2. BUS TOPOLOGIES

The following bus topologies are described and analyzed :

- Royal Navy Type 23 Frigate Bus Architecture (UK).
- MEKO Frigate Bus Architecture (Germany).
- C70AA Frigate Bus Architecture (France).
- IPN10 System Architecture (Italy).
- FFG 7 System Architecture (US Navy).
- Present Aegis Cruiser/Destroyer Combat System (US Navy).
- Next Generation US Combat System (US Navy).
- Backbone Network System Topology (proposed).
- Total Integrated System Architecture (proposed).
- Federated Integrated System Architecture (proposed).

2.1 SA Navy Minister Class Strike Craft (RSA)

The details of the Combat System of this vessel are classified. However, in general, sub-system interconnection is point-to-point using synchro and analogue links and some RS-422 digital links. The result is a closely-coupled, inflexible system, difficult to upgrade. The situation is exacerbated by the computing architecture which gives rise to the situation where information flows in loops between equipment. This results in a propagation of implications when system upgrade is considered.

2.2 Royal Navy Type 23 Frigate LAN Architecture (UK)

As shown in Figure 8 the Combat System on board the new Type 23 Frigate for the Royal Navy (RN) incorporates two different LANs [9.2.19, 9.2.12]. The one LAN which interconnects all the sensors and weapons is designated as the Combat System Highway (CSH) and the other LAN, interconnecting all the reconfigurable Multi-Purpose Consoles (MPCs), is designated as the Command and Control Bus (CCB). Both these LANs are dual-redundant.

All video information is distributed to all the MPCs via the Video Multiplexer. Each MPC has its own frame grabber and scan converter to display the raw video information on a digital monitor.

All the sensor and weapon control consoles are connected by the CSH and these consoles are not reconfigurable. Each console is permanently assigned to a sensor or weapon. Any information received by the sensor is transferred to the fileserver connected to both the CSH and the Command and Control Bus. The tactical picture is maintained within a database on this fileserver which is mirrored in the redundant backup system.

The MPCs connected to the Command and Control Bus are reconfigurable consoles. The officers responsible for each warfare area, as well as the Commanding Officer (CO), man

these consoles. When the operator switches on the MPC, the role that the MPC is required to perform is selected by the operator. The appropriate computer program is then downloaded from the fileserver with a copy of the database required for that configuration.

During operations the fileserver distributes the information required by each MPC to the respective consoles so that the officers manning them can have the same information displayed on their screens as operators in front of sensor consoles. This allows for the Sensor Compartment and the Operations Room to be partitioned, but still be in close contact. Thus the concept of "looking over the operator's shoulder" falls away. This topology allows for the autonomous operation of the sensors and weapons while battle engagement takes place within the MPCs. The battle engagement rules define target designation and weapon assignment. Once this is completed, the weapon and sensor can work autonomously without interference from the MPC. The MPC acts then as a monitor of the engagement.

The decision to use databuses within RN vessels could be considered as a breakthrough at the time. Such use has resulted in a more flexible system architecture, but the chosen implementations are considered to be severely limiting for the medium to long term. In particular, the choice of a proprietary standard for the CSH with a limited bandwidth of 2 $Mbits^{-1}$ are considered limiting. The LAN topology also does not lend itself to reconfigurability. The T23 is known to suffer "many EMC and space problems" [9.2.19] due to the choice of copper media. There is concurrence with Fraser's recommendations [same reference] that fibre optic media would have solved these problems as well as provided for significant upgradeability.

The video multiplexing arrangement is considered to be somewhat cumbersome due to its point-to-point topology and expensive due to the requirement for signal processing at each node. However, there were unlikely to have been more sophisticated alternatives at the time that this system was designed and developed.

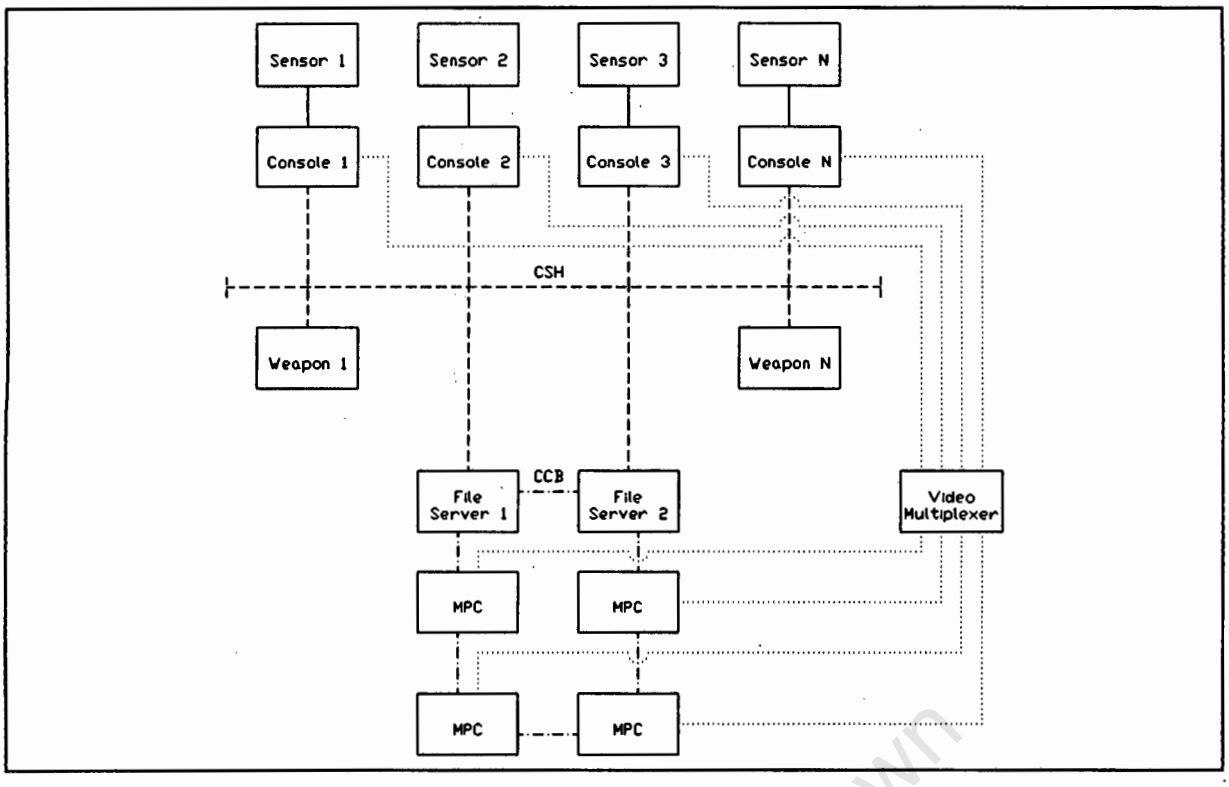


Figure 8 : Royal Navy Type 23 Frigate Bus Topology

2.3 MEKO Frigates LAN Architecture (Germany)

As shown in Figure 9, the Combat System of the MEKO class frigate, designed by Blohm & Voss in conjunction with American and European partners, consists of two data interchange LANs namely the Data Information Link (DAIL) and the Command and Control Bus (FüWES) [9.2.22].

One LAN is used as a navigation LAN for the transfer of all navigational data while the other is used as a command and control LAN to control the sensors and weapons.

These two LANs are interchangeable. Should one fail, the other will perform both functions, albeit in a degraded mode. The DAIL interconnects the sensors and weapons and is linked to the FüWES bus via a Multi-Interface Computer Einheit (MICE) (Multi-Interface Computer Unit).

The sensors and weapons are all supplied with MICE interfaces and are called Intelligente Funktionseinheit (IFE) (Intelligent Functional Units).

The MPCs are connected to the FüWES bus and are reconfigurable. Battle Engagement is controlled from these consoles.

Connected to all the LANs is the Ship's Maintenance System (SMS). This console monitors the data transfers on all the LANs and logs any errors and failures.

The MEKO architecture does provide for a considerable degree of availability and modularity. The topology does not, however, support on-line reconfigurability. The choice of Ethernet also limits the upgradeability of the system.

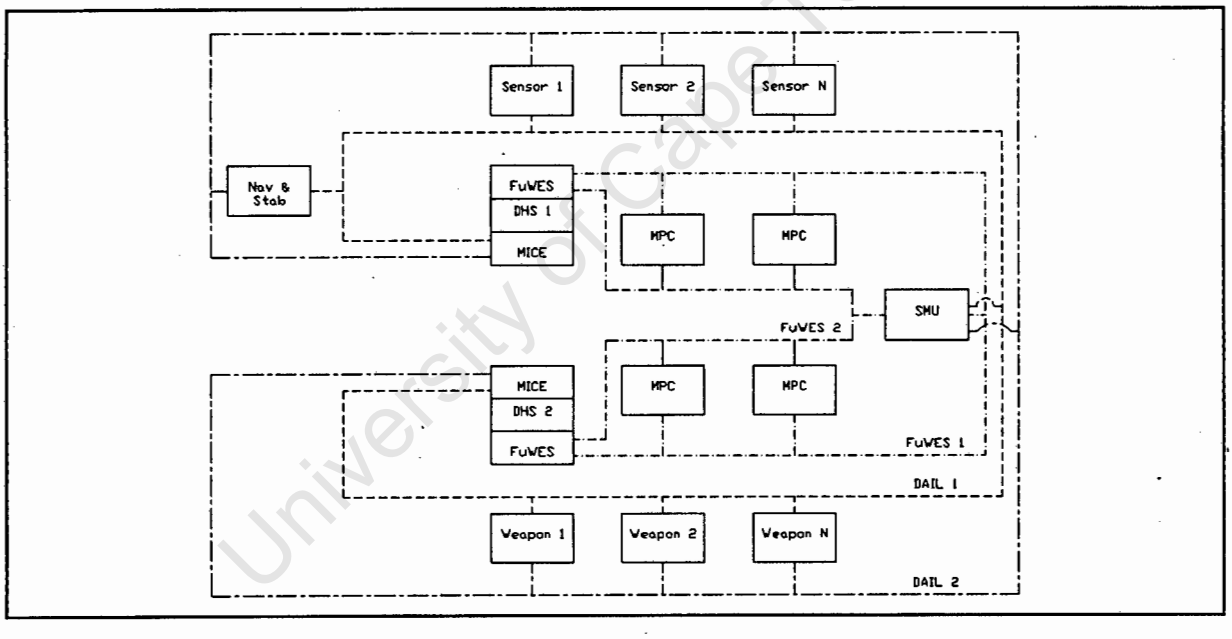


Figure 9 : MEKO Frigate Bus Topology

2.4 C70AA Frigate LAN Architecture (France)

This Combat System interconnection topology consists of six different LANs [9.2.16]. The interconnection philosophy is based on a federated system partitioned according to warfare areas.

The Display Bus connects the MPCs which are reconfigurable consoles. These MPCs are utilised for command and control of the battle situation and display of the tactical picture.

This LAN is connected to the System Bus via the Display Computer which acts as a gateway. The System Bus interconnects all the sub-systems that constitute the Combat System.

There are six sub-systems, namely :

- Surveillance Sub-System.
- Display Sub-System.
- Threat-Evaluation/Self-Defence Sub-System.
- Tartar Sub-System.
- ESM/ECM Sub-System.
- Link Sub-System.

Those sub-systems that consist of more than one unit are interconnected with their own local data link.

There are 7 MPCs of which 6 are normally in operation and one is kept in reserve. These seven MPCs are distributed in two compartments, one forward and one aft.

The C70AA architecture is considered as good architecture, supporting most of the modern combat system requirements, that was achievable at the time. The architecture reflects both a high degree of distribution as well as federalism using multiple LANs. Again, the choice of Ethernet will limit the upgradeability of the system.

2.5 IPN10 System Architecture (Italy)

As shown in Figure 10, the Combat System consists of only one LAN [9.2.21]. Only one sensor is shown here in order to describe the concept without cluttering it (the sensor shown is a radar).

The Radar Central Unit (RCU) is connected to all the MPCs in the system via dedicated links. The MPCs are divided into two groups, namely the Single Vertical Consoles (SVC) and the Multi-Horizontal Consoles (MHC). Only one operator can operate a SVC, but up to three operators can operate the MHCs. The MHCs are mostly used by the Weapons Officers and the Commanding Officer. A Combat System will normally consist of six SVCs and two MHCs.

The RCU is also directly connected to the Radar Tracking Unit (RTU). The SVCs and MHCs are mainly used as Man-Machine Interfaces (MMIs) and most of the processing of the tactical information is performed by the two Central Processing Units (CPUs). The CPUs are connected via a dedicated link to the Tape Cassette Unit (TCU) to record the tactical information for later analysis. The LAN is also connected to an In/Output Expander and Converter Unit (SDC).

The IPN10 architecture exhibits a hybrid approach of using LANs as well as point-to-point links. As such, it is considered to be somewhat inflexible with limited upgradeability and survivability. System availability will also be adversely affected by the use of only one LAN.

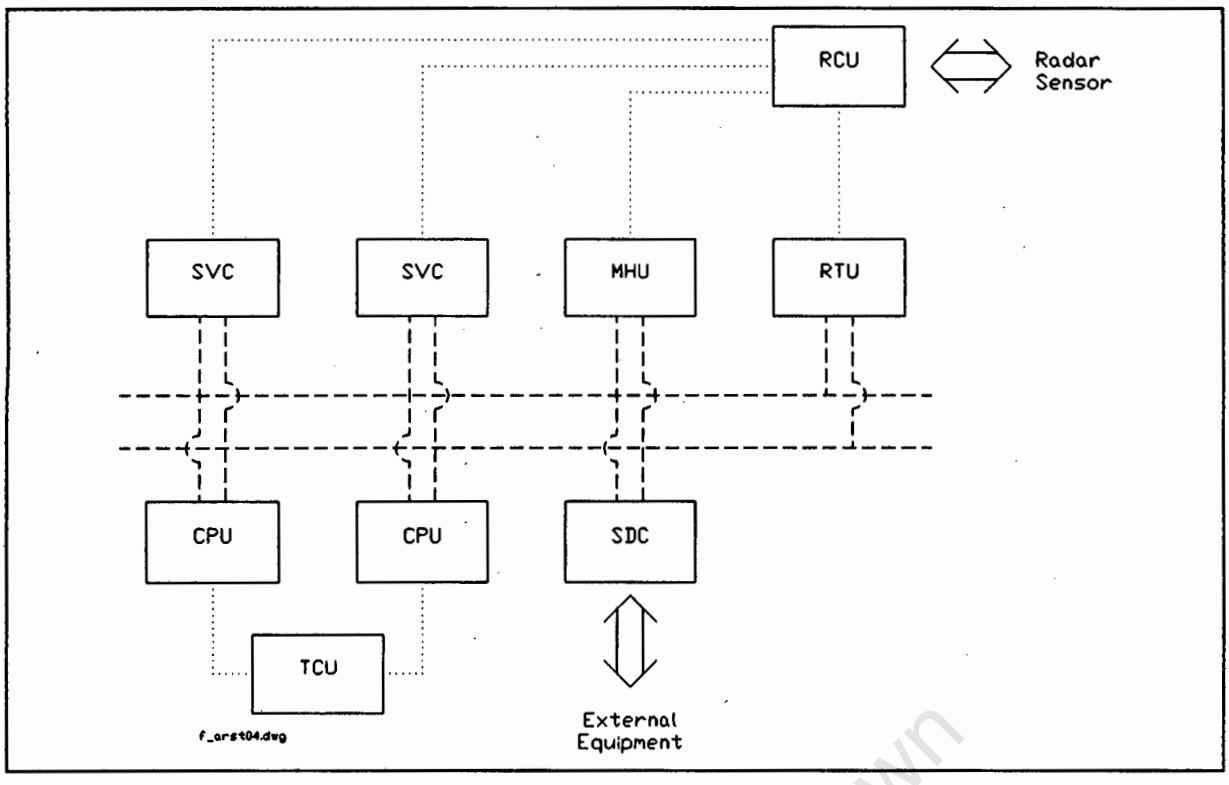


Figure 10 : Italian IPN10 Bus Topology

2.6 FFG 7 Upgraded Frigate (US Navy)

The FFG 7 is a fairly old US Navy frigate which is being considered for functional upgrade. The main mechanism for such upgrade will be the provision of an Advanced Combat System (ACS) [9.2.17].

The ACS is a modular, integrated combat system capable of multiple simultaneous operations across all warfare areas. The heart of the ACS is the Combat Direction System (CDS) consisting of reconfigurable standard workstations connected by redundant LANs. These LANs transmit data at an average of 2,5 $Mbits^{-1}$ and employ Ethernet technology. The standard workstations employ 68030 microprocessors and the VME parallel system bus.

Central to the FFG 7's very high anti-air combat capability is its Air Defense Array Radar (ADAR). The ADAR is a high-performance phased array radar capable of tracking 400 targets and providing up to 16 fire-control quality tracks while controlling up to 10 missiles in flight (midpoint guidance type). While providing very high performance, such a system places a high premium on information management resources including LAN bandwidth, database management systems and processing power.

Considering that the FFG 7 combat system is already and upgrade, this architecture can be considered as most effective. In fact, the FFG 7 possesses an awesome war-fighting capability for its size and cost (mainly due to its impressive ADAR and missiles). The capability is extensively supported by modern architecture concepts of distributed functionality extensively integrated by LANs.

Despite this, the long term requirements for a combat vessel of this type are not well supported by the implementation. The LAN employs Ethernet whose bandwidth does not support image, graphics, etc. The FFG 7 combat system is also not integrated with the rest of the platform which would enhance its combat effectiveness and will certainly be a medium to long term requirement.

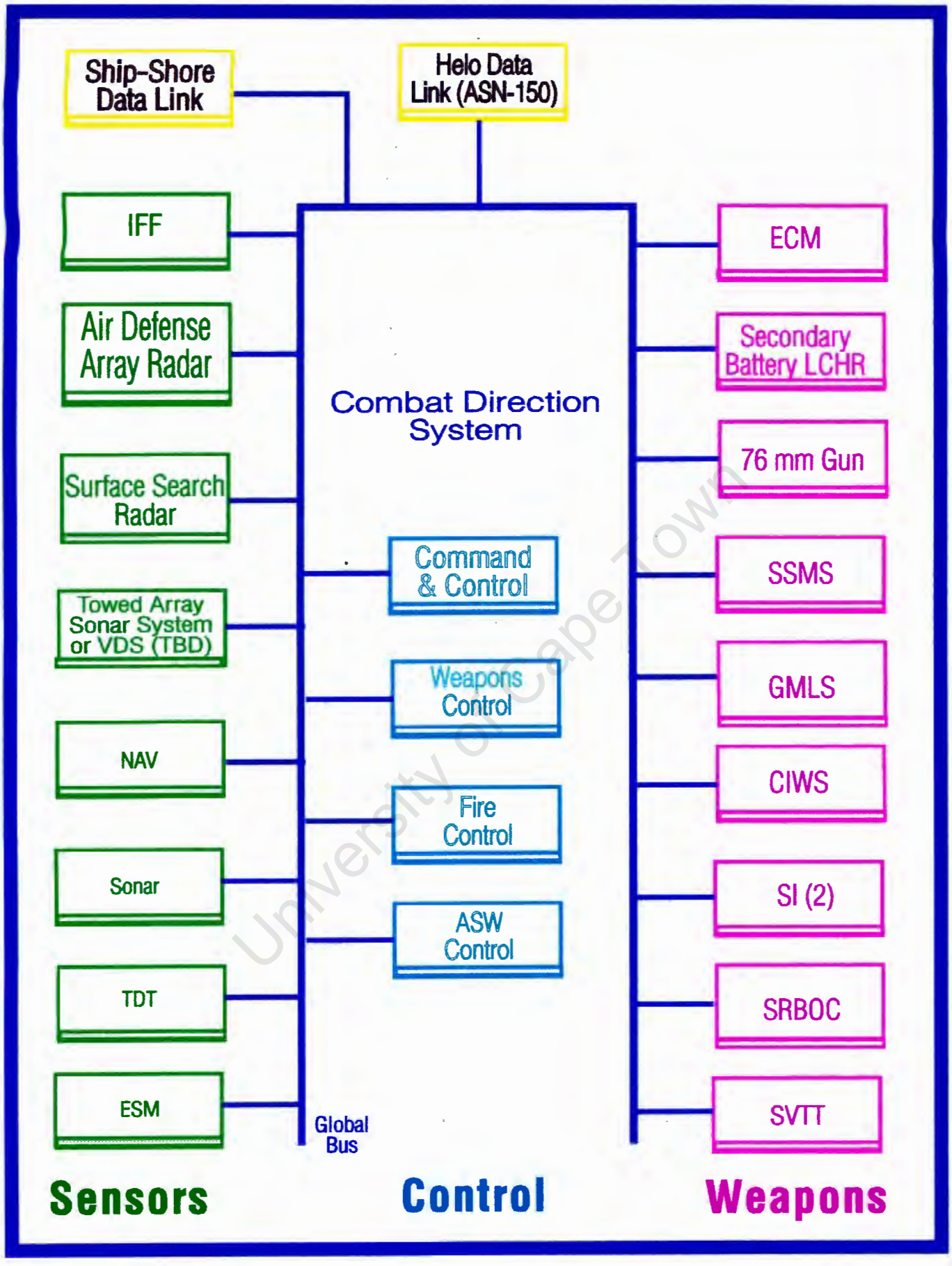


Figure 11 : FFG 7 Upgrade Combat System Architecture

file : yffg7ua.cdr

2.7 Present Aegis Cruiser/Destroyer Combat System (US Navy)

The latest operational combat system in the US Navy is the Aegis Combat System [9.2.20, 9.2.4]. The system was, however, designed some years ago and features a centralised computer system architecture. The central processing elements are the Command and Decision (C&D) unit and the Weapon Control System (WCS). A complex system of dual-redundant, point-to-point, copper-wire interconnections exists (US Navy standard NTDS channels).

Refer to Figure 12 for a diagrammatic representation of the Present Aegis Cruiser/Destroyer Combat System.

Despite that Aegis systems are currently in use, they cannot be considered as examples of modern combat system architecture. The centralised computer architecture and point-to-point data distribution topology are severely limiting in terms of availability, flexibility, reconfigurability and upgradeability.

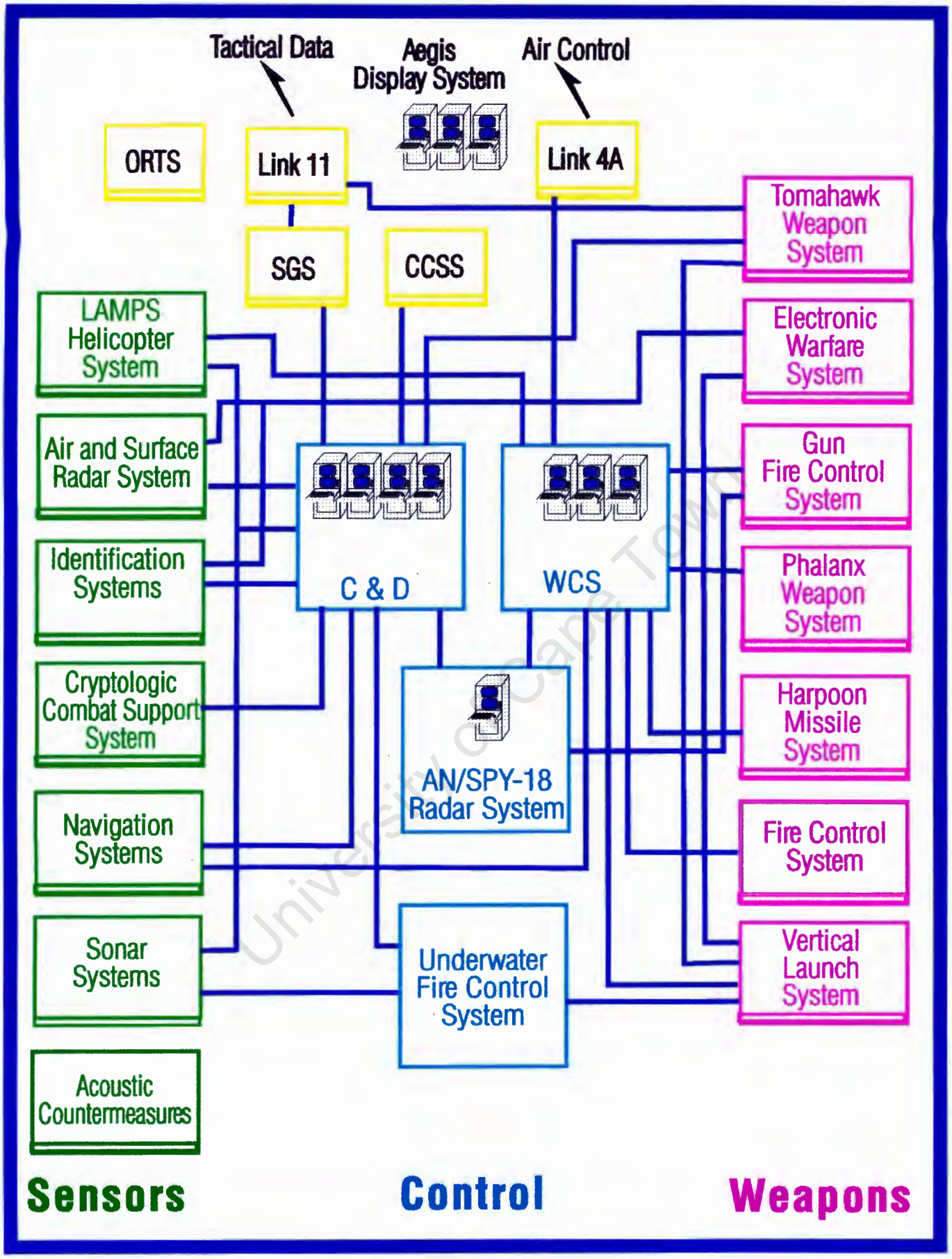


Figure 12 : Aegis Combat System Architecture

file : yaegisa.cdr

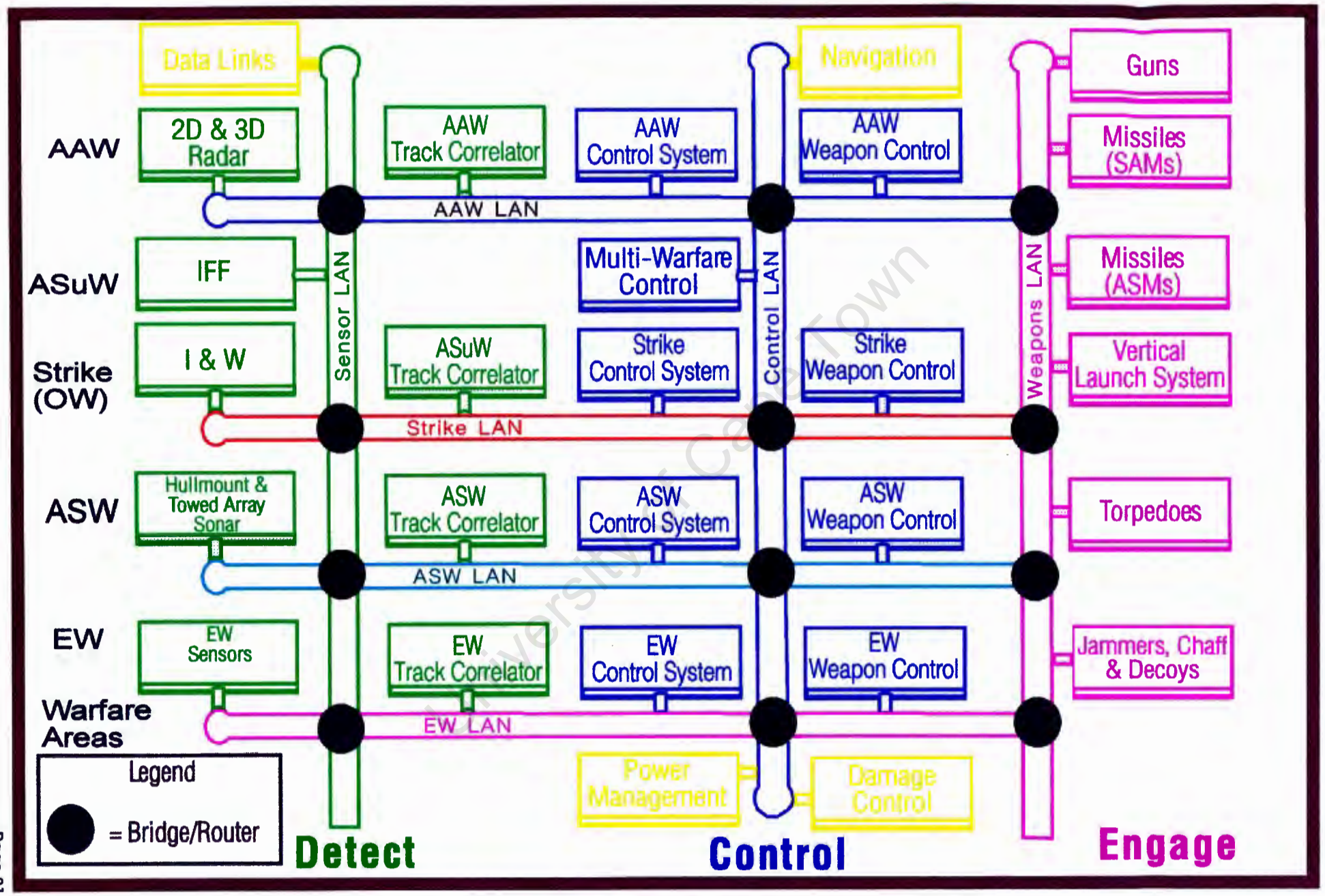
2.8 Next Generation USN Combat System (US Navy)

A group of combat system engineers and academics in the United States are presently giving consideration to the next generation of US Navy combat system requirement and architectures [9.2.4]. The work is being performed by the Aegis Computer Architecture, Data Bus, and Fibre Optics Working Group sponsored by the US Naval Sea Systems Command (NavSea). This next generation of surface combatants is destined for operational use in the 2010 to 2030 timeframe, hence many of the concepts are somewhat advanced for present consideration, while the full spectrum of operational requirements can only be speculated. However, the group recognises the requirement for *transition* and has formulated many relevant principles and philosophies, some of which are implementable in the short to medium term.

In terms of system architecture, they propose a heavily segmented approach according to the detect/control/engage/ and warfare area principle. The systems constituting each of these segments are arranged in a matrix fashion with a corresponding matrix of dual-redundant fibre optic LAN segments providing interconnection. This amounts to a system of seven LAN segments arranged orthogonally with twelve LAN interconnects which they term **gateways** (but are probably more correctly termed **bridges** or **routers**).

The system architecture and topology provides for a very flexible and upgradeable combat system. In terms of combat system engineering, it may represent the ultimate goal in this regard. One potential negative factor is that under certain conditions of system re-configuration (e.g. after equipment failure) data messages may have to be routed through two or more routers to reach their destinations. This may have timing implications (this may well be insignificant with next generation routers). The other drawback, especially for smaller vessels (such as frigates) is that the solution could tend to be expensive.

Refer to Figure 13 for a diagrammatic representation of the Next Generation USN Combat System Architecture.



file : yusnnga.cdr

Figure 13 : Next Generation USN Combat System Architecture

2.9 Totally Integrated System

As shown in Figure 14, this topology consists of one LAN only. All the sensors, weapons and MPCs are connected to the same LAN. The LAN may be dual-redundant to increase the availability of the system.

While this LAN topology is simple to conceptualise and implement, it does not support the required attributes of availability, flexibility, reconfigurability and upgradeability. Bandwidth problems are also likely to result from the requirement to integrate image, graphics and shared databases.

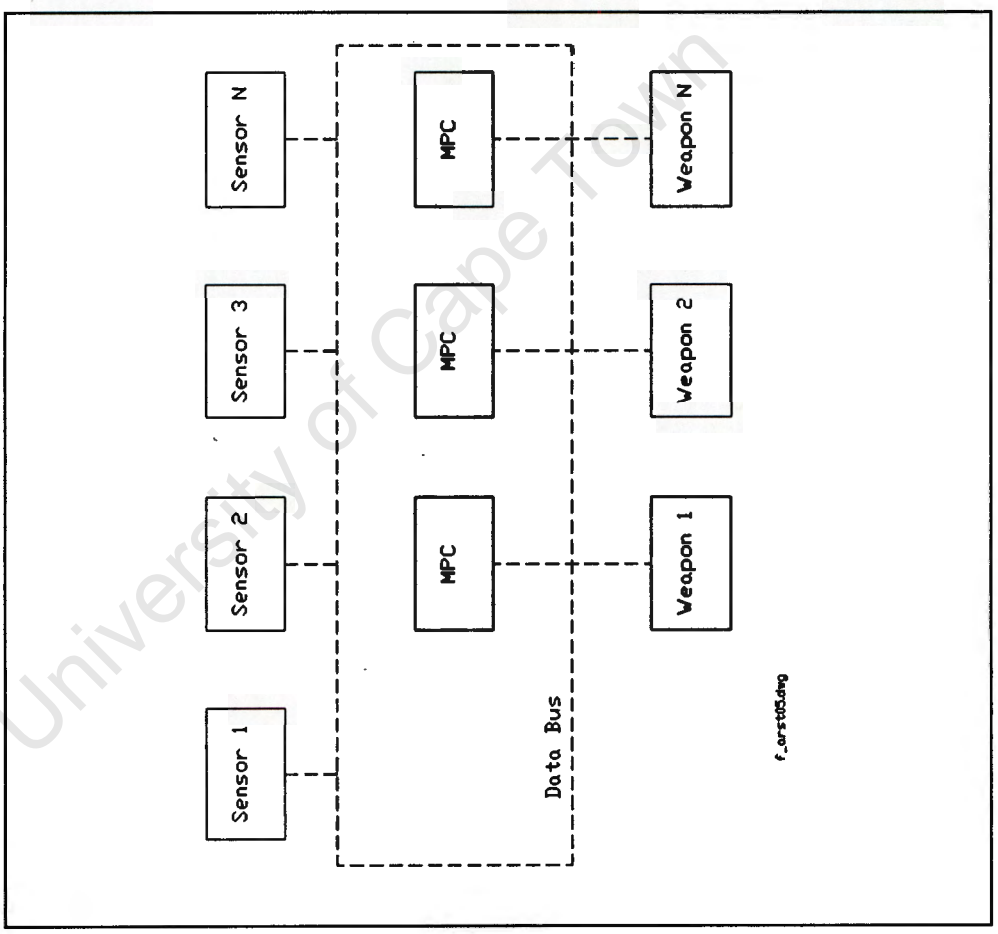


Figure 14 : Totally Integrated Bus Topology

2.10 Backbone Network System Topology

As shown in Figure 15, this topology consists of a number of largely independent LANs connected by a backbone network. LANs connect independently functional areas such that data flow on the LANs is concentrated locally while traffic to the backbone is minimised.

The advantages of this topology are that it is fairly non-complex and hence simpler to design, develop and manage. Organisations developing specific segments of the combat system may feel "more comfortable" with this arrangement as interfacing and qualification are less complex.

The disadvantages are that re-configurability is severely retarded, internetwork data will have to transit at least two routers each transmission and the costs for the multiple routers could be significant. The backbone also is a data throughput bottleneck because its bandwidth is equal to that of the LANs. A further negative factor is that, in the quest for maximum system integration, it will likely prove difficult to localise LAN traffic, especially during system upgrade.

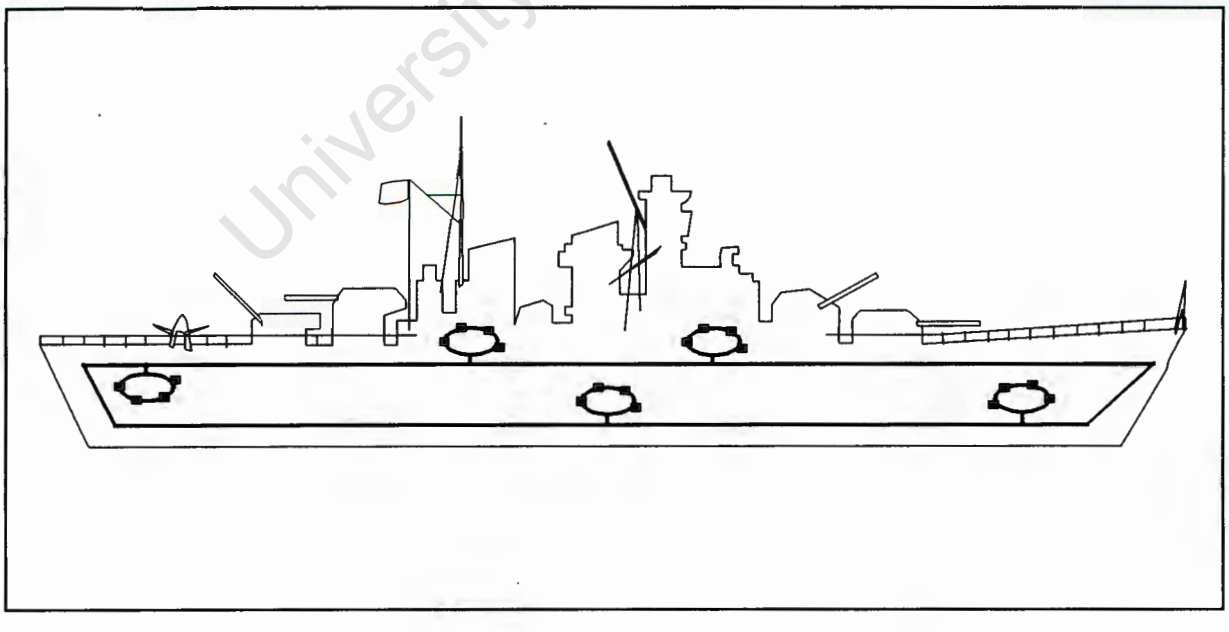


Figure 15 : Backbone LAN Topology

2.11 Federated Integrated System

As shown in Figure 16, the LAN topology is similar to the total integrated system, only differing in that segmentation is effected across warfare areas. A sensor or weapon will normally be connected to two LANs and the MPC will be connected to all three LANs.

This will decrease the overhead on a sub-system, but this implies that each sub-system has to interface to all the LANs it requires. This will increase the cost of the sub-system.

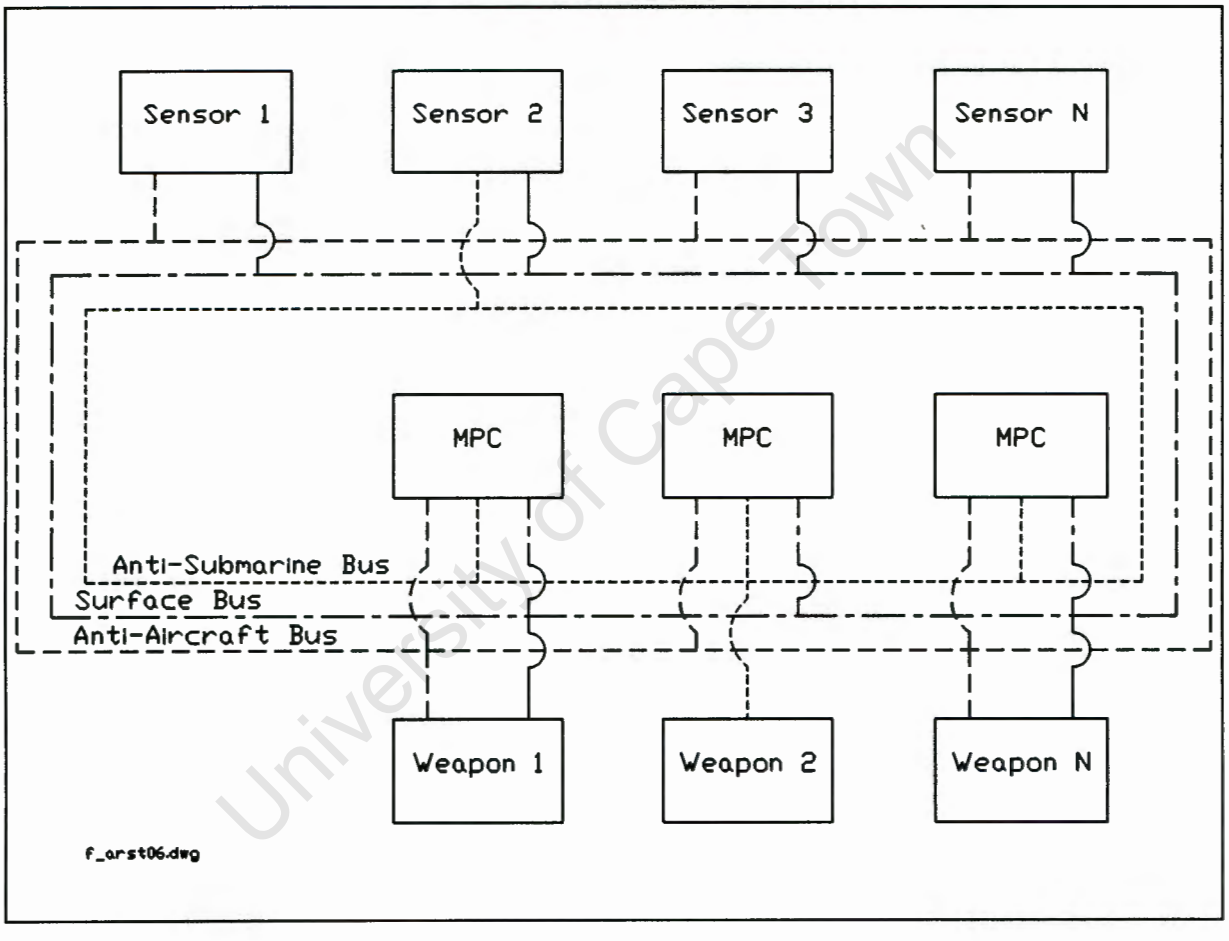


Figure 16 : Integrated Federated LAN Topology

3. CONCLUSIONS

Most of the Combat Systems being commissioned now and those that are being designed use some form of interconnecting LAN. The days of point-to-point connections are gone.

The future trend for consoles is to be reconfigurable. This enhances the availability of the Combat System and the survivability of the vessel and increases the capability of the vessel to ***fight hurt***, including the ability of launching a missile using targeting commands from another platform [9.2.18].

There is to date no clear route for a LAN or databus topology, although most of the systems seem to have more than one type of LAN. Partitioning is normally made across warfare areas, with gateways or bridges between the different types of LANs.

It is concluded that most of the current architectures have sought to support the anticipated medium to long term requirements, but have been limited by the availability of suitable technology including, high bandwidth LANs, real-time operating and database management systems, fibre optic cabling systems, digital signal processing hardware (capable of, for example real-time image processing).

It is also concluded that technology solutions have been developed, or are developing, in all these areas and it is now possible to consider architectures and topologies which support all the allocated and derived requirements.

Apart from the applicable technology developments, there has been considerable progress in commerce and industry in the implementation of reliable LANs and related information technology products and services which make the implementation of cost-effective solutions for Naval systems achievable at minimum risk.

4. RECOMMENDATIONS

Considering the present systems in operation and the future trends of naval combat systems, it is considered that a federated system partitioned on a warfare area basis, but with a dual-redundant router between all the LANs, is the most reliable and cost-effective topology and will offer the best functional performance.

As shown in Figure 17, this LAN topology consists of seven different LANs. The LANs are partitioned on the basis of warfare area with which the sensor/weapon is mostly involved.

All the LANs are interconnected to each other via the Logic Router which acts as a LAN router and logic controller. The proposed topology differs from the conventional federated system on the basis of having only one logical point of cross-over between the LANs. This arrangement allows information to be transferred from any sensor on the vessel to any MPC or weapon, while being transferred via only one routing element. This will increase the speed of transfers.

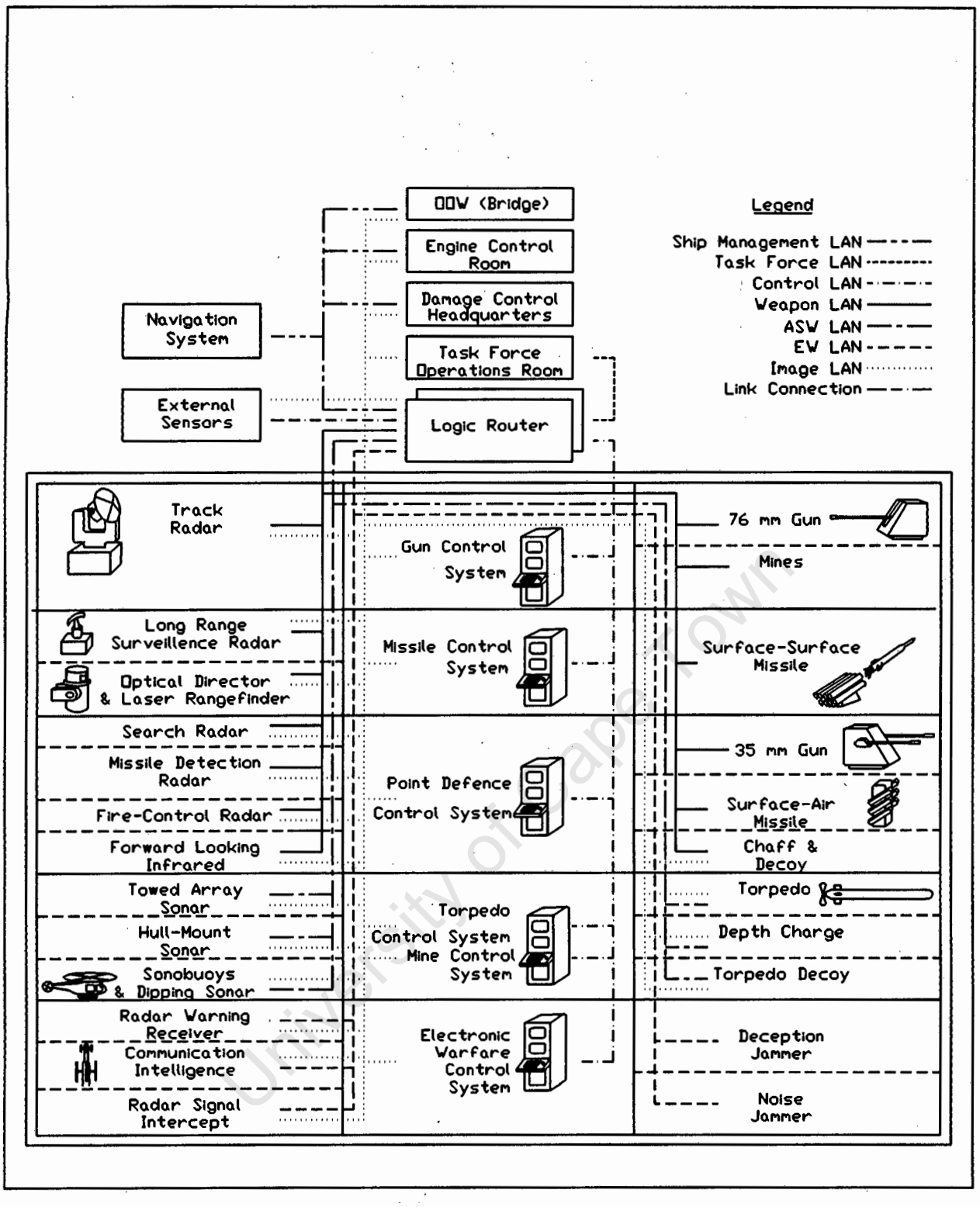


Figure 17 : Generic Fully-Integrated ICS Architecture

LAN Technology Comparative Analysis

1. LAN TECHNOLOGIES

1.1 Physical Layer Technologies

1.1.1 Collision Detect Schemes (IEEE 802.3)

In a Carrier Sense Multiple Access (CSMA) scheme a station that requires to transmit information, first "listens" for any bus activity. If no activity is sensed, the station is free to start transmitting. It may happen that two stations transmit at the same time. In this case a collision is said to occur. The simplest form of collision detection requires a higher level of protocol to detect that information has been lost. This could be accomplished by waiting for an acknowledge from the receiving station.

In IEEE 802.3 [9.1.15] a Carrier Sense Multiple Access with Collision Detect (CSMA/CD) scheme is specified. In this scheme collision detection is performed while the station is transmitting. This requires that the frame has a certain minimum length and that after a collision is detected a few additional bytes be transferred for the collision to propagate throughout the system. The minimum length and additional bytes are dependent on the length of the bus. The station will retransmit its frame after a random time delay.

If activity is detected on the bus, the station "backs off" for a predefined time (1 μs) and "listens" again. This is repeated until no activity is detected and the station is free to transmit.

The following collision detect scheme is identified :

- Ethernet.

1.1.2 Token Ring Schemes (IEEE 802.5)

A token ring scheme as defined by IEEE 802.5 [9.1.16] is a logical ring and not a physical ring. In a token ring a station may only transmit if it has the token. A token is a special type of frame. The token is generated by the master monitor station and the other station merely passes the token around the bus.

When a station requires the bus it will "grab" the token and hold it if the station has a higher priority than the priority specified in the token. If not, the station will request the token by placing its priority in the reserve bits in the token. After the station has removed the token from the bus, it then transmits its information.

In IEEE 802.5 three types of frames are defined. These are the Token Frame, Data Frame and the Abort Frame. Each station receives the frame and determines whether the frame is destined for itself. In this case the data contained in the frame is copied to memory. The station updates the frame status bits and transmits the frame back to the source station. When the source station receives the frame and has determined that the destination station has received the frame successfully, it will remove the frame from the LAN and release the token.

The following token ring schemes are identified :

- IBM Token Ring.
- FDDI.

1.1.3 Command/Response Schemes

In a command/response scheme there is always a controller controlling the scheduling on the bus. A station can only transmit if it is given the

authority by the controller. The controller verifies all bus traffic for integrity and will reschedule messages if any information was lost.

The following command/response schemes are identified :

- MIL-STD-1553B.
- HDLC.
- SDLC.

1.2 Existing LAN Standards

1.2.1 FDDI

The Fibre Distributed Data Interface (FDDI) is a high-speed LAN standard developed under co-ordination of the ANSI X3T9.5 committee. The primary medium of communication is multimode fibre in a ring topology. While single connection station attachment is optional, FDDI has been designed to support a dual-redundant counter-rotating ring topology. Further protection against node failure can be achieved using optional optical bypass switches which switch the optical signals around a failed node.

FDDI supports a data rate of 100 $Mbits^{-1}$ using 4B/5B encoding, resulting in a (bit-wise) transmission efficiency of 80%. FDDI allows for a total ring diameter of 200 km; this results in an effective ring diameter of 100 km in the dual-redundant configuration. A total of 1 000 attachments is allowed; again resulting in an effective 500 dual attachments in the dual-redundant configuration. Standard FDDI allows for intersegment lengths of up to 2 km between stations, but up to 40 km can be attained at present using singlemode fibre. FDDI also specifies a low bit error rate of $< 2,5 \times 10^{-10}$.

FDDI employs a **timed token** protocol which offers an efficient, deterministic, collision-free access to the network, regardless of the number of stations connected to the network. Such a protocol results in an overall transmission efficiency of up to 95%. Possession of the token allows a station to transmit one or more data frames of up to 4 500 bytes per frame.

FDDI, while conforming to internationally-accepted standards, also offers considerable flexibility in terms of media and station attachment. While the primary medium is multimode fibre, singlemode fibre is also supported, while 'FDDI' over both shielded/twisted pair (STP) and Unshielded/Twisted Pair (UTP) are also options. These options are sometimes termed CDDI (Copper Distributed Data Interface). While CDDI supports the data rates of FDDI, intersegment lengths are considerably reduced (≈ 30 m) while error rates are also increased.

The FDDI Standard is specified in four ANSI documents :

- FDDI Physical Media Dependent Protocol (Rev. 9) [9.1.17].
- FDDI Physical Layer Protocol [9.1.18].
- ANSI FDDI Media Access Control [9.1.19].
- ANSI FDDI Station Management (Rev. 6.2 - Draft) [9.1.20].

1.2.2 MIL-STD-1553

MIL-STD-1553 [9.1.1, 9.2.2, 9.2.31] is the document number for the US military avionics databus standard fully entitled *Digital Time Division Multiplex Command/Response Databus*. The standard was first published in 1973 and is now in its current revision

of MIL-STD-1553B (Notice II) which was published in 1978.

The standard has found extensive application in a wide variety of airborne platforms including aircraft, missiles, satellites, spacecraft and launch vehicles. It has also found application in land vehicle and smaller naval platforms such as submarines and smaller surface ships.

MIL-STD-1553 employs serial asynchronous communications over a shielded, twisted wire pair. The data rate is 1 $Mbits^{-1}$ using Manchester II biphase signalling resulting in a baud rate of 2 $Mbits^{-1}$ (i.e. 50% efficiency).

MIL-STD-1553 allows for up to 31 remote terminals plus a broadcast option. The number of data words per message is limited to 32 16-bit words. The communication protocol specifies a command/response mechanism, i.e. a bus controller schedules all messages on the bus. A dynamic bus control option is allowed, however.

MIL-STD-1553 offers both *synchronous* (state) and *asynchronous* (event) data transmission. The former are scheduled according to pre-determined message tables held by the (current) bus controller. The latter are scheduled in response to flags set in the status words of synchronous messages or by means of polling.

Traffic on a MIL-STD-1553 bus is normally organised into minor cycles and major cycles. The former derive from the repetition rate of the most frequent synchronous messages while the latter derive from the repetition rate of the least frequent synchronous messages.

As the transmission time for the longest (32-word) message is some 670 μs (that is without allowing for

any retries), minor cycle times are bounded by this figure. Practical minimum minor cycle times are in the order of 5 ms. Typical major cycle times are in the order of 1 s).

1.2.3 DOD-STD-1773

DOD-STD-1773 [9.1.2, 9.2.32] is an equivalent of MIL-STD-1553B, but specifies fibre-optic media in place of the latter's copper media. The standard provides no performance advantage other than improved electromagnetic compatibility. DOD-STD-1773 is implemented on NASA's Small Explorer Satellite (SMEX) where electromagnetic interference would degrade the platform's highly sensitive scientific instruments. The standard is also being considered for implementation in a number of satellite programmes as well as the Space Station Freedom.

1.2.4 STANAG 3910

While MIL-STD-1553 has found extensive and successful application on a wide variety of platforms, the standard only provides for an effective control bus and is ineffective as a true databus. As applications advanced, the requirement to transfer bulk data between processing nodes increased, thus saturating MIL-STD-1553's bandwidth.

While high-speed fibre optic communications systems were in existence at the time of the definition of NATO's European Fighter Aircraft (EFA), the reliability of these was not regarded as sufficient to support mission critical functions, especially fly-by-wire. It was therefore decided to develop a new bus standard STANAG 3910 [9.1.8, 9.2.2] (STANAG - Standard NATO Agreement) which exploited the trusted MIL-STD-1553 (STANAG 3838) bus as the mission-critical, low-speed bus whilst also offering a high-speed (20 $Mbits^{-1}$) data path. All traffic over

the high-speed bus is triggered by messages over the low-speed bus.

STANAG 3910 offers various options of media (copper or fibre), redundancy schemes and terminal address allocations.

While STANAG 3910 offers a significant improvement in data transfer performance, it does not offer any significant improvement in minor cycle performance due to its reliance on the MIL-STD-1553 protocol.

1.2.5 EFABus

The EFABus [9.2.32] is a subset of STANAG 3910 derived specifically for the European Fighter Aircraft by the European EFA Consortium. Specific restrictions are the specified use of 200/278 μm fibre optic media, dual redundancy and the designation of Subaddress 26 as the High Speed Subaddress.

1.2.6 MIL-STD-1760

The MIL-STD-1760 *Aircraft/Store Electrical Interconnection System* [9.1.3, 9.2.32] is a superset of MIL-STD-1553B and includes some enhancements thereto. The standard was developed mainly to interface advanced, intelligent munitions to the aircraft combat system.

There are a number of applications of MIL-STD-1760, including the Longbow Hellfire Missile, Inertially Aided Munitions and Advanced Bomb Family.

1.3 New Standards

1.3.1 FDDI II

FDDI II is an enhancement of the basic FDDI LAN protocol [9.2.33]. While FDDI (I) offers a packet

(switched) service, FDDI II offers a circuit switched service. A packet service provides for the delivery of variable length, delimited data packets to network stations on the basis of an address within the packet. A circuit switched service provides a continuous connection between two stations or between one station and multiple stations. Instead of using addresses, the connection is established between the stations based on some prior agreement mechanism such as a timeslot mechanism.

A typical timeslot mechanism is implemented using a standard timing marker such as the Basic System Reference Frequency (BSRF) which is a 125 μs clock used by public networks. As applied to FDDI II, this is termed the cycle clock.

FDDI II is capable of supporting **isochronous** data, i.e. data which occurs in precise amounts on a precise time basis. Typical examples of isochronous data are digital samples from sensors, voice data and video data.

The implementation of FDDI II constitutes a superset of FDDI (I) with the addition of one further layer known as Hybrid Ring Control (HRC).

FDDI II supports dynamic bandwidth partitioning between packet and circuit switched services to allow both modes of operation. Allocation of bandwidth is effected by means of 8 $kbits^{-1}$ sub-channels up to a 6,144 $Mbits^{-1}$ Wideband Channel (WBC). Up to 16 WBCs are assignable to isochronous services. It is possible to allocate any or all of the WBCs to one virtual service, thus satisfying the requirements for high-resolution video.

If all 16 WBCs are allocated to circuit switched service (i.e. 16 x 6,144 $Mbits^{-1}$ = 98,304 $Mbits^{-1}$), a residual 1 $Mbits^{-1}$ channel for packet traffic remains.

1.3.2 FFOL

The FDDI Follow-On LAN (FFOL) [9.2.33] is a very high performance fibre optic LAN proposed by the ANSI X3T9.5 committee for future application. Important proposed requirements for FFOL include the following :

- Ability to provide a backbone for multiple **FDDI** networks.
- Data Rates > 600 $Mbits^{-1}$, but < 1,25 $Gbits^{-1}$.
- Support for singlemode fibre.
- Ability to use existing **FDDI** cable plant.

1.3.3 Fibre Channel

Fibre Channel (FC) [9.2.33] is a proposed standard under consideration by the ANSI X3T9.3 committee. FC will be used to provide a common transport vehicle and switching environment for the extension of existing peripheral interface standards such as High Performance Parallel Interface (HiPPI), Small Computer System Interface (SCSI) and Intelligent Peripheral Interface (IPI). FC is optimised for predictable transfers of large blocks of data between large scale processors and devices such as laser printers.

FC does not follow OSI protocols, although its lower layers have functional similarities to FDDI and OSI Layers 1 and 2. FC uses a switch fabric topology, but by itself is not a general purpose LAN.

1.3.4 FDVDI

Fibre Distributed Voice, Video, Data Interface (FDVDI) [9.2.33] is a proposed new standard for simultaneous packet and circuit switched services.

As its name suggests, it is targeted to support fully integrated data, voice and video communications. FDVDI is a competitive standard to FDDI II and it is likely that only one standard will emerge as dominant in this segment.

FDVDI development is taking a three-phased approach, each phase corresponding to a particular data rate. Table IV summarises the relevant FDVDI characteristics.

Phase	Data Rate	Chip Technology
I	35/45 $Mbits^{-1}$	CMOS
II	155 $Mbits^{-1}$	BiCMOS
III	565 $Mbits^{-1}$	As yet Undetermined

Table IV : FDVDI Characteristics

1.3.5 DQDB

Dual Queue Dual Bus (DQDB) is a standard for Metropolitan Area Networks (MANs) recently developed in Australia. As its name suggests, it is based on a dual-redundant, bus topology. DQDB will feature fibre optics media and operate in the region of 155 $Mbits^{-1}$.

A summary of characteristics of LAN standards is presented below.

Military Standards

MIL-STD-1553B

Sponsor	Society of Automotive Engineers (SAE), USA, on behalf of US DOD
Developer	Many
Status	Established and widely used
Medium	Twisted-Wire Pair
Bandwidth	1 $Mbits^{-1}$
Length	100 m
Terminals	31
Topology	Linear Bus
Protocol	Command/Response

DOD-STD-1773

Sponsor	US DOD
Status	Established, but not widely used
Medium	Fibre-Optic
Bandwidth	1 $Mbits^{-1}$
Length	100 m
Terminals	31
Topology	Linear Bus
Protocol	Command/Response

STANAG 3910

Sponsor	NATO
Developer	Various European Companies
Status	Full-Scale Development
Medium	Fibre-Optic High-Speed Channel Twisted-Wire Pair Low-Speed Channel
Bandwidth	20 $Mbits^{-1}$ Data Bus 1 $Mbits^{-1}$ Control Bus
Length	100 m
Terminals	31
Topology	High-Speed Bus - Ring Low -Speed Bus - MIL-STD-1553B
Protocol	Command/Response

EFABus

Sponsor	European Fighter Aircraft (EFA) Consortium
Developer	Various European Companies
Status	Full-Scale Development
Charac-terristics	Derivative of STANAG 3910

Commercial Standards

Ethernet (IEEE 802.3)

Status	Mature Product
Developer	Xerox Corporation
Medium	Co-axial Cable
Bandwidth	10 $Mbits^{-1}$
Length	300 m (without Repeaters)
Terminals	≈ 250
Topology	Tree Network
Protocol	Carrier-sense, Multiple Access with Collision Detect (CSMA/CD)

IBM Token Ring (IEEE 802.5)

Status	Maturing Product
Developer	IBM Corporation
Medium	Co-axial Cable
Bandwidth	4 or 16 $Mbits^{-1}$
Length	≈ 500 m
Terminals	≈ 260
Topology	Ring Network
Protocol	Token Passing

FDDI

FDDI	Fibre Distributed Data Interface
Sponsor	ANSI
Developer	Many Commercial Companies
Status	Approaching Standardization
Medium	Fibre-Optic
Bandwidth	100 $Mbits^{-1}$
Length	100 km
Terminals	1 000
Topology	Dual-Redundant Counter-Rotating Ring
Protocol	Timed Token

1.4 Communication Protocols

1.4.1 TCP/IP Protocol Suite

The USA Department of Defence (DOD) commissioned the design of TCP/IP (Transmission Control Protocol/Internet Protocol) [9.1.4] before the OSI Reference Model was conceived. It provides point-to-point, guaranteed-delivery communication between networked nodes and was originally designed for packet switching communications.

TCP/IP consists of a range of protocols, providing services that communicate between and control incompatible computers and networks. The five-core military standard protocols of the TCP/IP suite are TCP, IP, FTP, SMTP and TELNET.

The TCP/IP suite consists of a four-layer communication framework with the following layers :

♦ Process Layer

The Process Layer contains the protocols needed to support various end-user applications. The three-core protocols implemented at this layer are FTP, SMTP and TELNET.

- FTP

The purpose of FTP is to transfer a file or portion thereof from one system to another. FTP must first interact with the user interface or program. FTP uses TCP to communicate with other FTPs to achieve file transfer. FTP must also interface with the local file management system. FTP can transfer ASCII text files or a transparent bit stream that can be used for any type of data to be transferred.

- SMTP

  SMTP provides the basis for a network electronic mail facility, but does not provide for the user interface. SMTP provides a mechanism for transferring messages between users by using TCP to send and receive messages anywhere on the network or internet.

- TELNET

  TELNET is a network terminal emulation standard and is a protocol used to link terminals to applications. TELNET provides reliable data exchange by means of TCP. It also allows terminals to control applications running on a remote host.

♦ Host to Host Layer

The Host-to-Host Layer uses TCP to ensure the reliability of data transfer between two hosts.

- TCP

  TCP is a connection-orientated protocol providing reliable data transfer between two transport users (eg. FTP and SMTP). Data is passed from the transport user to TCP which then encapsulates the data into segments containing the user data and control information. Outgoing segments are numbered sequentially and are acknowledged by number by the destination TCP module.

  The TCP standard defines the main levels of service as being Multiplexing

(Multiple Users), Connection Management, Data Transport and Error Reporting. TCP allows the transport user to specify the quality of transmission service and data transmission priority.

♦ Internet Layer

The Internet Layer is concerned with routing data between two hosts attached to different or multiple networks. An internet is an interconnected set of networks. Internet Protocol (IP) is used at this layer.

• IP

IP provides for the routing functions between hosts. It is a connectionless protocol and is responsible for the transmission of segmented data.

♦ Network Access Layer

The Network Access Layer is concerned with routing data between two devices on the same network. The physical protocol used to transmit TCP/IP data is independent of TCP/IP's top three layers. TCP/IP can operate over any media-access protocol including Ethernet, Token Ring (including FDDI) and Arcnet.

The advantage of this arrangement is that high-level software will function correctly regardless of the network type to which the host is attached.

1.4.2 OSI TP4

TP4 is the ISO Class 4 Transport Protocol. Layer 4 of the OSI model (Transport Layer) [9.1.9] consists of

five classes of increasing capability with respect to retransmission of lost data, flow control and reordering of packets. TP4 is frame orientated.

1.4.3 MAP/TOP

General Motors and Boeing Corporations developed the Manufacturing Automation Protocol/Technical and Office Protocol (MAP/TOP) [9.1.22]. MAP utilises multinational, interoperability standards frozen as of 1987 for the use of the manufacturing community.

1.5 Real-Time Protocols

In order to support reliable, real-time networks such as those required by the ICS, there is a requirement for light-weight protocols such as VMTP, NETBLT and XTP [9.2.14].

VMTP (Versatile Message Transaction Protocol) is being developed at Stanford University by David Cheriton, NETBLT (Network Bulk Transfer) at MIT by David Clark and XTP (Express Transfer Protocol) [9.1.21] by various developers in the USA under co-ordination of Protocol Engines, Inc.

1.5.1 XTP

The major attributes of XTP are error, flow and rate control, optimised inter-network addressing mechanisms and reliable multicast support.

1.5.1.1 Flow Control

Flow Control allows the receiver of information to inform the sender about the current state of its receiving buffers. In XTP, the receivers's flow control parameters are included in control packets sent from the receiver to the sender.

1.5.1.2 Rate Control

Rate Control allows the restriction of the size and time spacing of data from a sender in order that the ability of a data receiver (or intermediate routers) to decipher and queue data is not overwhelmed.

1.5.1.3 Error Control

Error Control provides for the detection of errors and retransmissions of data. XTP uses two checksums over the XTP packet contents to verify the integrity of the data received over the network. The XTP checksum algorithms were chosen for execution speed and VLSI implementation compatibility. The XTP checksums are also placed at the end of an XTP frame allowing concurrent checksum calculation with frame transmission or reception.

1.5.1.4 Priority Message Scheduling

XTP supports prioritization of packet processing at both the sender and receiver using **pre-emptive priority scheduling**. If a server is currently processing a low priority packet as a higher priority packet arrives for service, the server is **pre-empted** from processing the lower priority packet and begins processing the higher priority packet. Only after all higher priority packets have been completed or blocked will the server return to the lower priority packet.

In XTP, two pre-emptive schedulers exist, one for incoming packets and one for outgoing packets. For both the receiver and sender prioritization schemes, XTP supports

2^{32} different priorities. Each context is associated with a particular priority level. Multiple contexts can be assigned the same priority level simultaneously.

1.5.1.5 XTP Features

Specific features of XTP are the following :

a. It is a **transfer** (as opposed to transport) protocol and combines the functionality of the network and transport layers of the ISO OSI reference model.

b. XTP can provide user applications with multi-packet exchange sequences offering a transport-level **virtual circuit** capability and a transport-level **datagram** service.

c. XTP is specifically designed for **parallel** operation as opposed to serial operation. Address translation, context creation, flow control, error control, rate control and host system interfacing can all execute in parallel.

d. XTP can be considered as a lightweight protocol for a number of reasons. Firstly, it is a fairly simple, yet flexible algorithm. Secondly, packet headers are of fixed size and contain sufficient information to screen and steer the packet through the network. The core of the protocol is essentially contained within four fixed-size fields in the header. Additional mode bits and flags are kept to a minimum to simplify packet processing.

e. XTP is designed for **VLSI** (Very Large Scale Integration) implementation as opposed to soft- or firmware implementation.

Protocol Engines has developed the PE-1000 Series Protocol Engine Chipset featuring a CMOS VLSI XTP implementation. The chipset can handle throughputs of up to 200 $Mbits^{-1}$ or 100 000 packets per second.

Software implementations of XTP are also available. For example, Network Xpress Inc. has developed the Xpress Transfer Protocol (Version 3.6) which is compatible with Intel iAPX 80x86 processors and the DOS operating system, as well as Motorola 680x0 processors and the pSOS or pSOS+ operating systems.

1.5.2 ATM

Asynchronous Transfer Mode (ATM) [9.2.41] is a new protocol under development by many IT organisations throughout the world. At present it is envisaged for use with networks up to the 155 $Mbits^{-1}$, but will be capable of supporting bandwidths of up to several $Gbits^{-1}$. ATM is also being developed for silicon implementation and support packet and circuit-switched data transfer in MAN and WAN network topologies.

1.6 LAN Performance Comparison

Network performance can be quantified in terms of a Figure of Merit (FOM). Two such FOMs are the P-Factor [9.2.15] and Z-Factor.

The P-Factor is the product of the maximum size, maximum number of stations and peak data rate for a network :

$$P = \text{Length} \times \text{Size} \times \text{Data Rate} \qquad \text{station-km-bits}^{-1}$$

The Z-Factor is the quotient of the P-Factor and product of the Bit Error Rate (BER) and connection cost (in US dollars) for a network. The Z-Factor can be considered as a price/performance index for a LAN technology.

$$Z = \frac{\text{Length} \times \text{Size} \times \text{Data Rate}}{\text{Bit Error Rate} \times \text{Cost}} \qquad \text{station-km-bits}^{-1} \text{ per error per dollar}$$

Table VII provides P- and Z-Factors for MIL-STD-1553, Ethernet (IEEE 802.3), IBM Token Ring (IEEE 802.5) and FDDI LAN technologies.

It can be concluded that the FDDI standard offers significantly higher performance factors than all the other LAN standards, especially in the case of the Z-Factor, indicating that this technology has a very advantageous price/performance index.

2. CONCLUSIONS

2.1 Communications Standards

It is concluded that only the most recent of Communications Standards are appropriate for a next generation Naval Surface Combatant LAN infrastructure. High bandwidth, in the order of tens to hundreds of $Mbits^{-1}$ will be required to support image real-time transfer, graphics and shared databases. This clearly excludes from contention standards such as MIL-STD-1553B (1 $Mbits^{-1}$). Even Ethernet (10 $Mbits^{-1}$) and IBM Token Ring (4 and 16 $Mbits^{-1}$) are likely to find short-term useability in such applications. STANAG 3910 and EFAbus (20 $Mbits^{-1}$) provide higher levels of bandwidth, but their implementation limits effective throughput.

Apart from bandwidth, LANs should ideally support other attributes such as determinism, synchronous and asynchronous transfer modes and fibre optic media. Only the new family of LAN standards, including FDDI, FFOL, FDVDI and DQDB features these capabilities. Of these, only FDDI is currently readily available as affordable off-the-shelf equipment.

It is of interest to note that the new Type 471 diesel electric submarines of the Royal Australian Navy (RAN) employ the 50 $Mbits^{-1}$ Rockwell Multiplex Databus [9.2.3]. A submarine combat system has far less extensive LAN performance requirements than a surface combatant such as a frigate and it is concluded that it can be assumed that the latter class of vessel should be afforded a further degree of LAN capability.

A further desirable attribute of a LAN technology is that it conforms to a true, preferably international standard. Despite its performance and maturity, the Rockwell Multiplex Databus is a proprietary military and hence is not a recommended option.

It is concluded that none of the currently commercial protocol standards are appropriate for a next generation Naval Surface Combatant LAN infrastructure. To support the tens to hundreds of $Mbits^{-1}$ bandwidth requirements with real-time performance, will require protocols which have only recently been conceptualised with implementations yet to be realised.

While TCP/IP has found extensive implementation in large and sophisticated networks, it was designed in the era of 56 $kbits^{-1}$ data links [9.2.14] and is intrinsically unable to support data rates much above a few $Mbits^{-1}$ [9.2.34]. Similarly, ISO TP4, although extensive in its internetworking features, has not been designed for deterministic and real-time data transfer.

Only emerging protocols standards such as XTP, ATM, VMTP and NETBLT are capable of the throughput and other requirement on the combat vessel LANs and internetworks. Of these XTP is rapidly emerging as the leading contender for standardization for LANs while ATM appears to be doing the same for MANs and WANs.

LAN Standard	Length (km)	Size (Nodes)	Data Rate (Mbit/s)	P–Factor	Bit Error Rate	Cost per Node ($)	Z–Factor
MIL–STD–1553B	0,1	32	1	**3E+06**	1,0E–12	10 000	**3E+14**
802.3	0,5	100	10	**5E+08**	1,0E–08	700	**7E+13**
802.5	0,5	260	4	**5E+08**	1,0E–08	500	**1E+14**
802.5	0,5	260	16	**2E+09**	1,0E–08	900	**2E+14**
FDDI	100,0	1 000	100	**1E+13**	2,5E–10	3 400	**1E+19**

Table VII : P– and Z–Factors for Common LAN Technologies

Formulae

P = Length x Size x Data Rate station–kilometre–bits–per–second .....(1)

$$Z = \frac{P}{\text{Bit Error Rate} \times \text{Cost}}$$ station–kilometre–bits–per–second– per error–per dollar .....(2)

FDDI Ring Latency Time

The latency of an FDDI ring is dependant on two factors, *medium propagation delay* and *PHY latency*.

8.3.1 Medium Propagation Delay

Medium Propagation Delay (MPD) is a function of the path length i.e. FDDI ring diameter (RD) :

MPD	5,1 μs/km	(F D D I standard)
ICS	RD ≈ 1 km	(assumed)
Worst Case	RD = 200 km	(F D D I standard)

8.3.2 PHY Latency

PHY Latency (PL) is a function of the sum of the physical interface (PHY) latencies (PL). For a dual-attachment station (DAS), each DAS has two active PHYs; this case is applicable when one station has failed and the ring is in the ***wrapped*** configuration.

PL	0,6 μs per PHY	(F D D I standard)
ICS	No. of DASs (D) ≈ 30	(assumed)
Worst Case	No. of DASs (D) = 500	(F D D I standard)

8.3.3 FDDI Ring Latency Time

Thru' Ring Configuration

$RLT = MPD.RD + PL.D$

$RLT_{ICS} = 5,1 \times 1 + 0,6 \times 30$

$= \underline{23,1\ \mu s}$

$RLT_{WC} = 5,1 \times 200 + 0,6 \times 500$

$= \underline{1\ 320\ \mu s}$

$= \underline{1,320\ ms}$

Wrapped Ring Configuration

$RLT = MPD.RD + 2PL.D$

$RLT_{ICS} = 5,1 \times 1 + 2 \times 0,6 \times 30$

$= \underline{41,1\ \mu s}$

$RLT_{WC} = 5,1 \times 200 + 2 \times 0,6 \times 500$

$= \underline{1\ 620\ \mu s}$

$= \underline{1,620\ ms}$

8.3.4 ICS Cycle Times

Cycle times for the ICS are derived from the mission- and time-critical dataflows. The FDDI protocol employs a *timed-token protocol*. The **Target Token**

Rotation Time (TTRT) is a fundamental characteristic of a specific FDDI implementation and an analysis effort is required to determine a suitable value for the ICS in respect of the system-level performance characteristics.

The **Token Rotation Time** (TRT) of an FDDI ring defines the time taken for the timed-token to circumnavigate the ring and thus defines the time taken for a station to gain access to the LAN's message transfer services.

It can be proven mathematically that the timed-token protocol of FDDI has two important properties :

$TRT_{average} \leq TTRT$

$TRT_{maximum} \leq 2 \times TTRT$

The proof of these properties is somewhat complex and reference should be made to an article *Cycle Time Properties of the FDDI Token Ring Protocol* by K.E. Sevcik and M.J. Johnson [9.2.10].

8.3.5 TTRT for the ICS

The choice of TTRT for a system is not only dependent on the *ring latency time*, but also on the relative bandwidth allocation to synchronous and asynchronous traffic. Sevcik and Johnson provide two formulae to determine *Minimum TTRTs to Permit Various Fractions of Total Capacity to be Allocated to Synchronous Traffic*.

$$TTRT \geq \frac{N \times Z + P}{1 - S} \quad \text{. . . . . (Formula 1)}$$

$$N \times Z + P \approx 0{,}005 \times (RD + N) \quad \text{. . . . . (Formula 2)}$$

where N Number of PHYs

S Proportion of Synchronous Traffic

If allocation of between 50% and 70% of the bandwidth to synchronous traffic is made, it can be determined from Formulae 1 and 2 that the possible choice of minimum TTRT lies in the range 0,61 ms to 1,02 ms.

In order to effect accurate synchronization via the FDDI ring, the TTRT should be minimised, however this may have implications on sub-system interrupt processing overhead.

It is recommended that should a synchronization accuracy of better than 2 ms be required, a TTRT of 1 ms be adopted; if a synchronization accuracy of better than 10 ms is sufficient, a TTRT of 5 ms should be adopted.

TTRT min
(ms)

No. of Stations (N)	Ring Diameter (km)	N x Z + P (ms)	Synchonous Bandwith Allocation (S) 10%	20%	30%	40%	50%	60%	70%	80%	90%	95%	99,5%	99,9%
10	1	0,06	0,06	0,07	0,08	0,09	0,11	0,14	0,18	0,28	0,5	1,1	11	55
10	10	0,10	0,11	0,13	0,14	0,17	0,20	0,25	0,33	0,50	1,0	2,0	20	100
10	100	0,55	0,61	0,69	0,79	0,92	1,10	1,38	1,83	2,75	5,5	11,0	110	550
10	200	1,05	1,17	1,31	1,50	1,75	2,10	2,63	3,50	5,25	10,5	21,0	210	1 050
19	1	0,10	0,11	0,13	0,14	0,17	0,20	0,25	0,33	0,50	1,0	2,0	20	100
19	10	0,15	0,16	0,18	0,21	0,24	0,29	0,36	0,48	0,73	1,4	2,9	29	145
19	100	0,60	0,66	0,74	0,85	0,99	1,19	1,49	1,98	2,98	5,9	11,9	119	595
19	200	1,10	1,22	1,37	1,56	1,83	2,19	2,74	3,65	5,48	10,9	21,9	219	1 095
40	1	0,21	0,23	0,26	0,29	0,34	0,41	0,51	0,68	1,03	2,0	4,1	41	205
40	10	0,25	0,28	0,31	0,36	0,42	0,50	0,63	0,83	1,25	2,5	5,0	50	250
40	100	0,70	0,78	0,88	1,00	1,17	1,40	1,75	2,33	3,50	7,0	14,0	140	700
40	200	1,20	1,33	1,50	1,71	2,00	2,40	3,00	4,00	6,00	12,0	24,0	240	1 200
60	1	0,31	0,34	0,38	0,44	0,51	0,61	0,76	1,02	1,53	3,0	6,1	61	305
60	2	0,31	0,34	0,39	0,44	0,52	0,62	0,78	1,03	1,55	3,1	6,2	62	310
60	10	0,35	0,39	0,44	0,50	0,58	0,70	0,88	1,17	1,75	3,5	7,0	70	350
60	100	0,80	0,89	1,00	1,14	1,33	1,60	2,00	2,67	4,00	8,0	16,0	160	800
60	200	1,30	1,44	1,63	1,86	2,17	2,60	3,25	4,33	6,50	13,0	26,0	260	1 300
100	1	0,51	0,56	0,63	0,72	0,84	1,01	1,3	1,7	2,5	5,0	10	101	505
100	10	0,55	0,61	0,69	0,79	0,92	1,10	1,4	1,8	2,8	5,5	11	110	550
100	100	1,00	1,11	1,25	1,43	1,67	2,00	2,5	3,3	5,0	10,0	20	200	1 000
100	200	1,50	1,67	1,88	2,14	2,50	3,00	3,8	5,0	7,5	15,0	30	300	1 500
490	1	2,46	2,7	3,1	3,5	4,1	4,9	6,1	8,2	12	25	49	491	2 455
490	10	2,50	2,8	3,1	3,6	4,2	5,0	6,3	8,3	13	25	50	500	2 500
490	100	2,95	3,3	3,7	4,2	4,9	5,9	7,4	9,8	15	29	59	590	2 950
490	200	3,45	3,8	4,3	4,9	5,8	6,9	8,6	11,5	17	34	69	690	3 450
900	1	4,51	5,0	5,6	6,4	7,5	9,0	11,3	15	23	45	90	901	4 505
900	10	4,55	5,1	5,7	6,5	7,6	9,1	11,4	15	23	45	91	910	4 550
900	100	5,00	5,6	6,3	7,1	8,3	10,0	12,5	17	25	50	100	1 000	5 000
900	200	5,50	6,1	6,9	7,9	9,2	11,0	13,8	18	28	55	110	1 100	5 500
1 000	1	5,01	5,6	6,3	7,2	8,3	10	13	17	25	50	100	1 001	5 005
1 000	10	5,05	5,6	6,3	7,2	8,4	10	13	17	25	50	101	1 010	5 050
1 000	100	5,50	6,1	6,9	7,9	9,2	11	14	18	28	55	110	1 100	5 500
1 000	200	6,00	6,7	7,5	8,6	10,0	12	15	20	30	60	120	1 200	6 000

Table VIII : Minimum TTRTs for Various Fractions of Synchronous Traffic

Notes : 1. Shading indicates areas of interest.
2. Table derived from that of Sevcik and Johnson.

Formulae

$$TTRT \quad > \frac{N \times Z + P}{1 - S} \quad ms \qquad .....(1)$$

$$N \times Z + P = 0{,}005 \times (RD + N) \quad ms \qquad .....(2)$$

1st Order Dataflow Analysis

1. SCOPE

This appendix addresses a *Dataflow Analysis for an Integrated Combat Suite*. An attempt has been made to derive the dataflow requirements from the expected requirements of each of the systems identified.

The analysis was performed primarily on critical and major information flows between the sub-systems.

Finally some **conclusions** and **recommendations** are offered.

2. ASSUMPTIONS

Data throughput is a major requirement in applications such as distributed databases, shared graphics and on-line console reconfiguration where large volumes of data need to be transferred in short times.

No level of sub-system redundancy was considered.

Whatever the reliability attributes of a system, maintenance will be required. Differentiation between on- and off-board maintainability requirements is essential as this affects the design of the system and sub-systems as well as the total logistic support policy for the equipment. This was, however, seen as a **minor** requirement.

With a high degree of redundancy and reconfigurability the requirement for on-board maintenance will be significantly reduced. This will lead to other system requirements such as on-line system monitoring and tracking of configuration state and Line Replaceable Unit (LRU) status. This was also seen as a **minor** requirement.

3. DEFINITIONS AND DERIVATION

In the context of this analysis, the following definition and derivation are applicable.

Definition

Utilisation ≡ The ratio of the sum of the Bit Times of all Data Messages and the total number of available Bit Times in one second

Derivation

$$\text{Utilisation} = \frac{\Sigma\ (\text{Msg Length} \times 8 \times \text{No. of Messages})}{\text{Bit Times per Second}} \times \frac{1}{\text{Update Rate}}$$

Where :

Msg Length is the data message length in bytes.

One Byte is equal to 8 Bits.

The Update Rate is the repetition cycle for periodic (state or synchronous) messages or expected frequency for aperiodic (event or asynchronous) messages and is expressed in milliseconds.

No. of Messages is the number of times a specific message may be transmitted from one source to several destination in the absence of a multicast facility.

Bit Time is the time required to transmit one Bit of data over the communication medium.

4. CONCLUSIONS

4.1 LAN Bandwidth

The 1st Order Dataflow Analysis (Table IX) indicates a bandwidth utilisation of some 4,4% of the 100 $Mbits^{-1}$ of an FDDI LAN. While this analysis assumes a topology based on a single LAN, it considers only critical and major dataflows that are known at this time. It does not consider dataflows involved with start-up, reconfiguration, redundancy implications, non-critical database access, graphics sharing or image transmission. These requirements will have extensive implications on LAN bandwidth, especially in transient phases of ICS operation.

The bandwidth requirement of 4,4 $Mbits^{-1}$ does indicate that neither MIL-STD-1553, 4 $Mbits^{-1}$ token-ring nor Ethernet would be sufficient for the application. In the case of the latter, it should be remembered that the effective throughput of an Ethernet LAN is in the order of 30% due to the inefficiency of the CSMA/CD protocol.

The analysis does show that a single FDDI LAN can easily support the critical, steady-state dataflow requirements of the specified ICS configuration. A number of other considerations are nevertheless applicable :

a. The effective throughput of an FDDI LAN is in the region of 80 to 90 $Mbits^{-1}$ (i.e. 80% efficiency) as a result of implementation realities.

b. The bandwidth utilisation of an FDDI LAN in a time- and mission-critical application should be kept considerably below the maximum (e.g. 50% to 70%) in order to maintain deterministic throughput (refer to the *FDDI Ring Latency Time Analysis*).

c. The design bandwidth utilisation of any LAN in a long life-cycle application such as the ICS should be kept to below 40% at initial set-to-work. This is in order

to allow for the step-increase in bandwidth requirements normally experienced during system integration as well as enhancements during the life cycle of the platform.

d. The LAN infrastructure, especially the physical component, should be designed to be stable for at least 15 years after initial set-to-work.

e. Survivability of the weapons platform is considerably enhanced by 'compartmentalising' the weapons systems in such a manner that weapons operation is possible following battle damage, i.e. the capability to *fight hurt*.

The implications of this on the LAN infrastructure are the following :

i. Dual-redundant cabling systems.

ii. Geographic isolation of redundant cable paths (e.g. **port-high** and **starboard-low**).

iii. Dual-redundant critical LAN resources (e.g. logic routers, bridges, gateway, database servers, fileservers, radio modems).

iv. Geographic isolation of redundant LAN resources (e.g. **foreword** and **aft**).

f. While the provision of a Towed-Array Sonar (TAS) has not been considered for the ICS, a *fit-for-but-not-with* approach should be taken in respect of its implications on dataflow and LAN requirements. This is because a TAS requires extensive inter-sub-system and inter-database communication having a significant impact on LAN bandwidth requirements.

4.2 LAN Requirements

Analysis of the allocated and derived requirements shows that the IMI for the ICS will have extensive requirements in terms of real-time performance, throughput and number of terminals supported due to the nature of the platform as well as its threats, targets, weapons and environment.

The IMI will also be required to support on-line reconfigurability and real-time database sharing.

Although buses such as those defined by MIL-STD-1553B remain extremely effective implementations as high-reliability control buses, they fall short in their ability to transfer data at high speeds, are limited in effective length and number of available nodes.

Only high-bandwidth fibre optic networks have the attributes necessary to provide these requirements.

4.3 High-Speed Communications Controller

LAN communications should be supported by a High-Speed Communications Controller (HSCC). This should be an "intelligent" communications controller in that it can operate with minimal overhead on its host CPU. The card should provide for at least dual media redundancy i.e. support multiple physical buses with automatic message retries between these buses.

The throughput of the unit should be ≥ 100 Mbits per second in order to cope with the large number of remote terminals as well as the extreme real-time nature of the ICS.

The HSCC should support industry standards including those defining communications protocol, physical form factor and electrical backplane bus.

Messages										Parameters		No. of Messages	Utilisation (Bits/s)
Message Name	**Source Address**	**Dest Address**	**Transfer Type**	**Message Type**	**Integrity Control**	**Priority**	**Precedence**	**Msg Length (Bytes)**	**Update Rate (ms)**	**Parameter ID**	**Parameter Name**		
Target Track Data (32 Targets)	FCR	WCU	Sync	Peer–Peer	Session	0	Critical	512	5	1 2 3 4 5 6 7 8 9	Azimuth Elevation Range Azimuth' Elevation' Range' Azimuth'' Elevation'' Range''	4	3 276 800
Own Motion Data	NSS	CCS ORT 1 ORT 2 FCR TIS 1 TIS 2 Ballistics Unit 1 Ballistics Unit 2	Sync	Multicast	Session	0	Critical	32	10	1 2 3 4 5 6 7 8 9 10 11	Position Course Speed Heading Bottom Depth Roll Pitch Roll' Pitch' Roll'' Pitch''	1	25 600
Meterological Data	NSS	All	Sync	Broadcast	Session	2	Critical	16	10	1 2 3 4 5	Wind Speed Wind Direction Air Temperature Barometric Pressure Relative Humidity	1	12 800
Contact Report	SRS ASR AMDR	Target Database	Async	Peer–Peer	Session	2	Critical	32	250	1 2 3 4 5 6 7	Contact ID Report Time Bearing Range Speed Altitude Remarks	3	3 072
Threat Alarm	SRS ASR AMDR	CCS WCU	Async	Multicast	Application	2	Critical	32	250			3	3 072
Racket Report	EWSS	CCS	Async	Peer–Peer	Session	1	Critical	48	20	1 2 3 4 5 6 7 8 9 10 11 12 13 14 15	Racket ID Classification Platform Type Confidence Factor Emitter Type Bearing Bearing Error Bearing Rate–of–Change Frequency Amplitude PRF PW Scan Type Scan Rate Remarks	1	19 200

Messages										Parameters		No. of Messages	Utilisation (Bits/s)
Message Name	Source Address	Dest Address	Transfer Type	Message Type	Integrity Contro	Priority	Precedence	Msg Length (Bytes)	Update Rate (ms)	Parameter ID	Parameter Name		
Racket Alarm	EWSS	CCS	Async	Peer-Peer	Application	0	Critical	8	250			1	256
Decoy Confirmation Request	EWSS	CCS	Async	Peer-Peer	Application	0	Critical	8	250			1	256
Decoy Confirmation	CCS	EWSS	Async	Peer-Peer	Application	0	Critical	8	250			1	256
Decoy Fire	EWSS	SRDS	Async	Peer-Peer	Application	0	Critical	8	250			1	256
Decoy Confirmation Request	SRDS	EWSS	Async	Peer-Peer	Application	0	Critical	8	250			1	256
Decoy Confirmation	EWSS	SRDS	Async	Peer-Peer	Application	0	Critical	8	250			1	256
Jammer Engagement	EWSS	CCS	Async	Peer-Peer	Application	0	Critical	8	250			1	256
Jammer Confirmation	EWSS	CCS	Async	Peer-Peer	Application	0	Critical	8	250			1	256
Decoy Engagement	EWSS	CCS	Async	Peer-Peer	Application	0	Critical	8	250			1	256
Jammer Allocation	EWSS	CCS	Async	Peer-Peer	Application	0	Critical	8	250			1	256
Decoy Allocation	EWSS	CCS	Async	Peer-Peer	Application	0	Critical	8	250			1	256
Tracker Status	WCU	CCS	Sync	Peer-Peer	Session	0	Critical	32	100	1 2	Status Remarks	4	10 240
Weapon Status	WCU	CCS	Sync	Peer-Peer	Session	0	Critical	32	100	1 2	Status Remarks	4	10 240
Attack Alarm (Air)	CCS	WCU	Async	Peer-Peer	Session	0	Critical	26	250	1 2 3 4	Contact ID Bearing Range Remark	1	832
Target Designation	CCS	WCU	Async	Peer-Peer	Application	0	Critical	26	250	1 2 3 4	Target ID Bearing Range Remark	1	832
Permission to Fire (PTF)	SCA	WCU	Async	Peer-Peer	Application	0	Critical	2	250			1	64
PTF Confirm Request	WCU	SCA	Async	Peer-Peer	Application	0	Critical	2	250			1	64
PTF Confirm	SCA	WCU	Async	Peer-Peer	Application	0	Critical	2	250			1	64
Target Data	ORT 1 ORT 2 TIS 1 FCR	Target Database	Sync		Session	0	Critical	10	10	1 2 3 4 5	Tgt ID Azimuth Elevation Range 1 Range 2	4	32 000
Tactical Data	Target Database	Tactical Editor	Sync	Peer-Peer	Session	0	Critical	512	10			1	409 600
Tactical Data	Tactical Editor	Tactical Database	Sync	Peer-Peer	Session	0	Critical	512	10			1	409 600
Target Track Data	Target Database	Ballistics Unit 1 Ballistics Unit 2 CIWS SAM	Sync	Peer-Peer	Session	0	Critical	32	10	1 2 3 4 5 6 7 8 9	Azimuth Elevation Range Azimuth' Elevation' Range' Azimuth'' Elevation'' Range''	4	102 400
Manual Target Update	SCA	WCU	Async	Peer-Peer	Application	1	Critical	10	100			10	8 000
Group Tactical Data	ICS	All	Sync	Broadcast	Session	1	Critical	100	1 000			1	800
Group Tactical Data Update	Tactical Editor	ICS	Async	Peer-Peer	Session	1	Critical	32	1 000			1	256
Nav Radar Data	NRSS	CCS, NSS	Sync	Multicast	Session	1	Critical	40	1 000			1	320
Towed Array Sonar Data	TAS	SSS, CCS	Sync	Multicast	Session	1	Critical	40	1 000			1	320
Hullmount Sonar Data	HMS	SSS, CCS	Sync	Multicast	Session	1	Critical	40	1 000			1	320
Torpedo Decoy Data	TDS	SSS, CCS	Sync	Multicast	Session	1	Critical	40	250			1	1 280

Messages										Parameters		No. of Messages	Utilisation (Bits/s)
Message Name	**Source Address**	**Dest Address**	**Transfer Typ**	**Message Type**	**Integrity Contro**	**Priority**	**Precedence**	**Msg Length (Bytes)**	**Update Rat (ms)**	**Parameter ID**	**Parameter Name**		
Helo-Ship Tactical Data	HSS	CCS (via ICS)	Sync	Peer-Peer	Transport	2	Major	32	1 000	1 2 3 4 5 6 7 8	Position Course Speed Altitude Target ID Target Position Target Course Target Speed	1	256
Ship-Helo Tactical Data	CCS (via ICS)	HSS	Sync	Peer-Peer	Session	2	Major	32	1 000	1 2	Vector Data Search Data	1	256
Helo Sonar Data	HSS	CCS (via ICS)	Sync	Peer-Peer	Session	1	Major	4	10			1	3 200
Noise Jammer Data	NJ	CCS	Sync	Peer-Peer	Session	0	Critical	40	100			1	3 200
Deception Jammer Data	DJ	CCS	Sync	Peer-Peer	Session	1	Critical	40	100			1	3 200
Tactical Constructs	SCAn	SCAm	Async	Peer-Peer	Session	2	Major	50	1000	1 2 3 4 5 6	Construct Type Origin Co-ordinates/Axis Labels Symbols Remarks	5	2 000
Formation Data	SCAn	SCAm	Async	Peer-Peer	Session	2	Major	40	1000	1 2 3 4 5 6 7 8	Formation Type Axis Distances Address List Origin Course Speed Time Reference	2	640
Command and Control Info	SCAn	SCAm	Async	Peer-Peer	Session	1	Critical	5	1 000			20	800
Environmental Data	PFM	All	Sync	Broadcast	Session	2	Minor	15	1 000			1	120
Ship System Data	PFM	All	Sync	Broadcast	Session	2	Critical	64	1 000			1	512
Control Orders	SCAn	WCUn	Async	Peer-Peer	Session	0	Critical	10	500			10	1 600
Bus Synchronisation	SMU	All	Sync	Broadcast	Session	0	Critical	4	1			1	32 000
Platform Status Data	PFM	All	Sync	Broadcast	Transport	3	Major	7	10			1	5 600
Calendar Time	GPS	All	Sync	Broadcast	Session	0	Critical	8	1 000			1	64
RT Status Poll	SMU	SCAn	Sync	Multicast	Transport	3	Minor	4	10			1	3 200
RT Status Report	RTUn	SMU	Sync	Peer-Peer	Transport	3	Minor	32	1 000			20	5 120
RT Self Test	SMU	SCAn	Async	Multicast	Transport	3	Minor	4	1 000			1	32
RT Self Test Results	SCAn	SMU	Async	Peer-Peer	Transport	3	Minor	32	1 000			20	5 120
Loop Test	SMU	SCAn	Async	Multicast	Transport	3	Minor	4	1 000			1	32
Loop Test Results	RTUn	SMU	Async	Peer-Peer	Transport	3	Minor	32	1 000			20	5 120
Total												**% Utilisation FDDI 100 (Mbit/s)**	**4 402 664** **4,40%**

Table IX : 1st Order Dataflow Analysis

1st Order Database Analysis

1. SCOPE

This appendix presents a *Database Analysis for an Integrated Surface Combat Suite*. An attempt has been made to derive the database requirements for each of the sub-systems of the combat system.

The analysis has concentrated on the critical and major information flow between the sub-systems and the respective databases.

Some **conclusions** and **recommendations** in respect of database requirements and solutions are offered.

2. REQUIREMENTS

A significant proportion of ICS LAN dataflow will originate from database access.

Two main types of databases are required, i.e. mission databases and support databases.

In order to effect system data coherency, there is a requirement to maintain a centralised shared database. Working images of segments of the database may be downloaded to remote workstations on a read-only basis. The database is updated from these same workstations, as well as other sources, but not via the remote database segments.

2.1 Mission Databases

The mission databases are characterised in terms of their time criticality (priority) and mission criticality (precedence) and will consist of the Target Database and Tactical Database.

2.1.1 Target Database

The target database will contain data describing all identified targets and applicable parameters. In particular, the Target Database will contain the Master Track File for up to 400 targets. This database is a real-time database guaranteeing access times of < 10 ms.

2.1.2 Tactical Databases

These databases store the tactical information, battle actions, ship's manoeuvres, etc. and include local databases such as Electronic Warfare (EW), Sonar, Navigation, Chart and Communications databases.

2.2 Support Databases

These databases provide on-line operator and maintainer manuals, a stores management database (for managing the munitions, fuel, spares, food, electricity and water consumption, etc.). The support databases are characterised by their capability to handle an extensive number of records.

2.3 Image Databases

Image databases provide storage for representations of threats, charts, maps and other graphical files. The image databases are characterised by their capability to handle records of extensive size (binary large objects).

3. DATA STORAGE TECHNOLOGIES

Optical drives should be fitted to the servers (fileservers and database servers) for the storage of application software, databases and back-ups.

Read-Write optical drives should be used for the storage of dynamic, non-time-critical data.

WORM (write once read many) optical drives should be used for the archiving of static, non-time-critical data.

CD ROM (Compact Disk Read Only Memory) optical drives should be used for the storage of charts, maps, maintenance documentation, etc.

Time-critical segments of databases should exist in non-volatile RAM. Flash EPROM should be used for static and semi-static data while battery-backed RAM for dynamic data segments.

4. DATABASE FEATURES AND CAPABILITIES

4.1 Backups and Recovery

The DBMS should support the reliable creation of backups of the database as well as mechanisms for simple and effective database restoration from backup logs and transaction records following catastrophic DBMS failure.

4.2 Operating Host

A desirable attribute of the DBMS is portability between operating hosts, but a critical requirement is effective operation on the Standard Computing Segment (SCS) of the Standard Console Assembly (SCA) defined for the ICS. This includes compatibility with the standard operating system, standard high-level languages, standard network operating system and communication infrastructure.

4.3 Security

The DBMS should offer administrative features, especially the assignment of access rights to database users. The security mechanisms should include data encryption and a hierarchical rights system.

4.4 Concurrency Control

It is clear that it is a critical requirement of the DBMS to provide multi-user access to the databases. As such, the DBMS has to provide concurrency control mechanisms such as record locking so that two applications are prevented from updating the data simultaneously. The capability of read consistency is also important so that one application can read data while another updates it.

The DBMS must offer mechanisms for prevention of the database *deadlock* phenomenon. The *deadlock* phenomenon is a common, but non-trivial problem in database design which occurs when one

or more concurrent processes lock a record which has already been locked.

4.5 Integrity Rules

The DBMS must provide a consistent set of **integrity rules**, which guarantee the integrity of the databases. Two important rules are *entity integrity* which ensures the uniqueness of each record in a table and *referential integrity* which ensures consistency between tables.

4.6 Database Access

The DBMS must provide an efficient and effective method of access to the database by the remote processing elements, i.e. support interconnectivity.

4.7 Binary Large Objects

The DBMS should provide the capability of supporting data types such as Binary Large Objects (BLOBs) within the databases. BLOBs include data entities such as charts, maps, images and documents.

5. COMPARATIVE ANALYSIS

5.1 Database Models

Four important database models exist; *hierarchical*, *networking*, *relational* and *object-oriented*.

5.1.1 Hierarchical and Networking Models

The hierarchical and networking models store data in record structures. Application programs are tightly bound to the actual data with the implication that intimate knowledge of the associated data structures is required in order to implement or update an application, making these models somewhat inflexible.

5.1.2 Relational Model

The relational model views data as if it were formatted into tables. The actual format in which the data is stored is transparent to the application with the implication that implementation and update are simplified and more flexible.

The relational model employs a restricted range of data types, e.g. integer, string, etc.

The relational model was derived from the mathematics of set theory and first-order predicate logic thus allowing the development of well-defined optimisation rules, the ***normalisation rules***. These minimise the replication of data across tables.

Relational Databases also support **Structured Query Language** (SQL), a language interface which provides an ad-hoc query facility to access or update data. The language is designed to restrict unnecessary data traffic by specific data requests. SQL has become an industry standard for commercial database systems.

5.1.3 Object-Oriented Model

The object-oriented model views data as an object, i.e. an autonomous data entity possessing a clearly defined external interface with masking of internal functionality and data.

The object-oriented model provides an unrestricted range of user-defined data types. It does not possess any design rules or optimisation strategy.

Existing object-oriented database products are not optimised and are not standard. They do not have clearly defined architectures, nor do they support SQL.

5.2 Database Architectures

Database management systems may exist in a number of different configurations or architectures. Traditionally large databases have been implemented on mainframe and minicomputers in a centralised, star-wired architecture.

The advent of inexpensive computer hardware and local area networks (LANs) has supported the trend towards distributed processing, including database processing. Distributed architectures have many advantages over traditional ones, especially in an integrated combat suite environment, in that the attributes of fault-tolerance, survivability, flexibility, expandability and upgradeability are well supported by a distributed, LAN-based architecture.

The distributed, LAN-based system architecture in turn supports a Client-Server Database Architecture. Here the database is centralised on a dedicated processing platform, i.e. the database **server**, while access to the database is granted through intelligent workstations, i.e. the database **clients**. The clients may access the server by means of SQL which has major advantages in that network traffic is minimised.

The architecture may readily be extended to a **system** of database servers where each server holds a database of information most relevant to its local applications.

5.3 Commercial Databases

5.3.1 Oracle

Oracle (Oracle Corporation) is a commercial, SQL DBMS [9.2.23] which runs on a variety of processing platforms and LANs. Its major features are its portability and large base of application support.

Its negative characteristics are its complex relational model and difficulty in administration, as well as lack of features such as stored procedures and triggers.

5.3.2 SQL Server

SQL Server (Microsoft Corporation) is a commercial, SQL DBMS [9.2.23] which runs on a variety of processing platforms and LANs. Its major features are its mission-critical OLTP (On-line Transaction Processing) capability and effective operation in large networks.

Its negative characteristics are its overhead requirements in terms of resources and administration.

5.3.3 SQLBase

SQLBase (Gupta Technologies) is a commercial, DOS-compatible, SQL DBMS [9.2.23] which runs on a variety of processing platforms and LANs. Its major features are its LAN compatibility, ease of management and development tools.

Its negative characteristics are its lack of portability.

5.3.4 Informix

Informix (Informix Software, Inc.) is a commercial, Unix-compatible, SQL DBMS [9.2.23] which runs on a variety of processing platforms and LANs. Its major features are its Unix compatibility, portability, flexible locking mechanisms, BLOB support, disk mirroring and modest requirement for hardware and administration resources, as well as good development tools.

Its negative characteristics are its (past) poor vendor support.

5.4 General Data Executive (GDX II)

The GDX II Real-Time Relational Database Management System [9.2.29] is a set of two products: the GDX Engine and GDX Toolkit developed by the US company Firmware Associates. Together they support the development of high-performance database management systems running under the Intel iRMX II, iRMX III and DOS/RMX real-time operating systems. Operation on PC, Multibus I and Multibus II computer platforms is supported.

5.4.1 GDX Engine

The GDX Engine is a set of database utilities and system calls to PL/M and C high-level language applications.

5.4.2 GDX Toolkit

The GDX Toolkit provides an integrated CASE environment with a data dictionary, Report Generator,

Program Generator, Screen Generator, 4th Generation Database Language and additional utilities.

Programs developed for the Engine can run concurrently with programs developed with the Toolkit, with full support for inter-program communication, e.g. mailboxes.

GDX II can support databases in RAM of up to 16 Mbyte and greater than 1 GByte (multi-gigabyte) on disk. It would be possible to extend the RAM addressing capability to 1 Gbyte for the cost of a vendor-implemented engineering change.

5.4.3 Cost

The acquisition cost for a full GDX development system is in the order of $15 000 (R60 000 landed).

5.4.4 GDX Performance

Performance benchmarks have been performed on a system with the following configuration :

a.	Processor Type	:	Intel 80386DX
b.	Processor Speed	:	25 MHz
c.	Bus Type	:	AT-bus
d.	Record Length	:	80-byte
e.	Key Length	:	6-byte

RAM Database

Benchmark Result : 3,1 ms per access (**average**)

Magnetic Disk Database

Benchmark Result : 5,9 ms per access (**average**)

5.5 Comparative Analysis Summary

DBMS	Transactions per Second (TP1)	Cost	Operating Systems	4GL	Languages	Referential Integrity
Oracle	11,00	$ 2 499	OS/2 Unix VAX/VMS	SQLForms SQLReport	C Cobol Fortran	None
SQL Server	10,54	$ 2 495	OS/2 Unix VAX/VMS	ABT Workbench	C	Triggers
SQLBase	15,54	$ 2 495	DOS OS/2	SQLWindows	C Cobol	To be provided
Informix	Unknown	$ 1 600 to $10 000	Unix VAX/VMS	Informix 4GL	C Cobol	None

Table V : Multi-User SQL Databases

DBMS	Transactions per Second	Cost	Operating Systems	4GL	Languages	Referential Integrity
GDX II	322	$15 000	RMX II RMX III DOS/RMX	Proprietary	C PL/M	Unknown

Table VI : GDX Real-Time Database

Data Storage										Parameters		
Data Item	Database	Server	Source Client	User Client	Precedence	Storage	No. of Records	Record Length (Bytes)	Update Rate (ms)	Parameter ID	Parameter Name	Data Item Size (Bytes)
Target Master Track File (400 Targets)	Target	Mission	FCR ORT 1 ORT 2 SRS MDR TIS 1 TIS 2	WCU 1 WCU 2 WCU 3	Critical	NOVRAM	400	32	5	1 2 3 4 5 6 7 8 9 10 11	Azimuth Elevation Range Azimuth' Elevation' Range' Azimuth'' Elevation'' Range'' Classification Comment	12 800
Target History File (400 Targets)	Target	Mission	FCR ORT 1 ORT 2 SRS MDR TIS 1	WCU 1 WCU 2 WCU 3	Critical	Optical Disk	409 600	32	1 000	1 2 3 4 5 6 9 10	Azimuth Elevation Range Azimuth' Elevation' Range' Classification Comment	13 107 200
Own Motion Data	Tactical	Mission	NSS	CCS ORT 1 ORT 2 FCR TIS 1 TIS 2 SRS SSM 1 SSM 2 SAMS Ballistics Unit 1 Ballistics Unit 2	Critical	Optical Disk	100 000	32	10	1 2 3 4 5 6 7 8 9 10 11	Position Course Speed Heading Bottom Depth Roll Pitch Roll' Pitch' Roll'' Pitch''	3 200 000
Meterological Data	Tactical	Mission	NSS	All	Critical	Optical Disk	100 000	16	1 000	1 2 3 4 5	Wind Speed Wind Direction Air Temperature Barometric Pressure Relative Humidity	1 600 000
Tracker Status	Tactical	Mission	WCU	CCS	Critical	NOVRAM	16	32	100	1 2	Status Remarks	512
Weapon Status	Tactical	Mission	WCU	CCS	Critical	NOVRAM	16	32	100	1 2	Status Remarks	512
Tactical Data	Tactical	Mission	CCS	Tactical Editor	Critical	NOVRAM	1 024	128	10			131 072
Tactical Signals File	Tactical	Mission	CCS ICS	CCS	Critical	NOVRAM	1 024	256	1 000	1 2 3 4 5	Racket ID CPA TCPA Weapon/Sensor Range Report Flag	262 144
Tactical Plans File	Tactical	Mission	CCS	CCS	Critical	Flash EPROM	1 024	512	1 000		ATP 1 B Volume I and II	524 288
Tactics File	Tactical	Mission	CCS	CCS	Critical	Flash EPROM	1 024	512	1 000	1 2 3 4	EW MSL Gunnery AA	524 288
Group Tactical Data	Tactical	Mission	ICS	Tactical Editor	Critical	NOVRAM	1 024	128	10	1 2 3 4 5	Formations ASW/SU/AA Directions Constructs Assignments	131 072
Nav Radar Data	Navigation	Navigation	NRSS	CCS, NSS	Critical	Flash EPROM	1 024	40	1 000			40 960
Towed Arrey Sonar Data	Sonar	Sonar	TAS	SSS, CCS	Critical	Optical Disk	1 024	40	1 000			40 960
Hullmount Sonar Data	Sonar	Sonar	HMS	SSS, CCS	Critical	NOVRAM	1 024	40	1 000			40 960
Torpedo Decoy Data	Sonar	Sonar	TDS	SSS, CCS	Critical	Flash EPROM	1 024	40	250			40 960

Data Storage										Parameters		
Data Item	Database	Server	Source Client	User Client	Precedence	Storage	No. of Records	Record Length (Bytes)	Update Rate (ms)	Parameter ID	Parameter Name	Data Item Size (Bytes)
Helo-Ship Tactical Data	Sonar	Sonar	HSS	CCS (via ICS)	Major	NOVRAM	1 024	32	1 000	1 2 3 4 5 6 7 8	Position Course Speed Altitude Target ID Target Position Target Course Target Speed	32 768
Helo Sonar Data	Sonar	Sonar	HSS	CCS (via ICS)	Major	NOVRAM	1 024	4	10			4 096
Noise Jammer Data	EW	EW	NJ	CCS	Critical	NOVRAM	1 024	40	100			40 960
Deception Jammer Data	EW	EW	DJ	CCS	Critical	NOVRAM	1 024	40	100			40 960
Tactical Constructs	Tactical	Mission	SCAn	SCAm	Major	Optical Disk	2 048	50	1 000	1 2 3 4 5 6	Construct Type Origin Co-ordinates/Axis Labels Symbols Remarks	102 400
Formation Data	Tactical	Mission	SCAn	SCAm	Major	Flash EPROM	1 024	256	1 000	1 2 3 4 5 6 7 8	Formation Type Axis Distances Address List Origin Course Speed Time Reference	262 144
Mission Planning	Tactical	Mission	SMU	All	Major	Optical Disk	1 024	1 024	10 000			1 048 576
Intelligence	Tactical	Mission	SMU	All	Major	Optical Disk	1 024	1 024	10 000			1 048 576
Ovelays	Tactical	Mission	SMU	All	Major	Optical Disk	1 024	1 024	10 000			1 048 576
Environmental Data	Tactical	Mission	PFM	All	Minor	Optical Disk	1 024	15	1 000			15 360
Ship System Data	Tactical	Mission	PFM	All	Critical	Optical Disk	1 024	64	1 000			65 536
Platform Status Data	Tactical	Mission	PFM	All	Minor	Optical Disk	1 024	7	10			7 168
Stores Status	Stores Management	Supporrt	PFM	All	Major	Optical Disk	1 024	128	1 000			131 072
RT Status	Tactical	Mission	SMU	SCAn	Critical	Flash EPROM	1 024	4	10			4 096
RT Self Test Results	RT Status	SMU	SCAn	SMU	Minor	Optical Disk	1 024	32	1 000			32 768
Charts	Navigation	Navigation	SMU	All	Major	WORM Drive	256	16 777 216	10 000			4 294 967 296
Topological Maps	Navigation	Navigation	SMU	All	Major	WORM Drive	256	16 777 216	10 000			4 294 967 296
Document Images	Documents	Supporrt	SMU	All	Minor	WORM Drive	65 536	131 072	10 000			8 589 934 592
Photographic Images	Photographs	Supporrt	SMU	All	Minor	WORM Drive	65 536	131 072	10 000			8 589 934 592
Radar Images	EW	EW	EW	All	Minor	WORM Drive	1 024	131 072	10 000			134 217 728
Threat Images	Air Threats	Tactical	SMU	All	Minor	WORM Drive	1 024	131 072	10 000			134 217 728
Threat Images	Surface Threats	Tactical	SMU	All	Minor	WORM Drive	1 024	131 072	10 000			134 217 728
Threat Images	Sub-Surface Threats	Tactical	SMU	All	Minor	WORM Drive	1 024	131 072	10 000			134 217 728
Communications	Communications	Tactical	SMU	All	Major	Optical Disk	1 024	1 024	1 000			1 048 576
Spares Status	Maintenance	Support	PFM	All	Minor	Optical Disk	16 384	128	10 000			2 097 152
Spares Catalogue	Maintenance	Support	SMU	All	Minor	WORM Drive	65 536	131 072	10 000			8 589 934 592
Total												34 923 297 792

Storage Requirements Summary		
	Mission	
NOVRAM	(MBytes)	0,7
Flash EPROM	(MBytes)	1,3
Optical Disk	(MBytes)	23,5
WORM Drive	(GBytes)	32,5
Total	(Bytes)	34 923 297 792

Table X: 1st Order Database Analysis

6. CONCLUSIONS

6.1 Performance Assumptions

6.1.1 Real-Time Performance

An assumption of a guaranteed 10 ms data transaction time has been made in performing a comparative analysis and formulating conclusions. This figure has not been verified for two reasons; firstly only a first order database analysis has been completed and the exact requirement is dependent on the exact ICS architecture.

The choice of 10 ms is not entirely arbitrary however. It is derived from the requirement of updating and accessing the Target Master Track File (i.e. the target database). From the dynamic characteristic of the targets, radars and ballistics system, 10 ms has been determined as a point of departure.

6.1.2 On-line Performance

For non-time-critical data transactions there are two requirements.

a. Low OLTP time.
b. Large database size.

6.2 Real-Time Databases

While commercial multi-user databases can provide OLTP capability, they cannot offer the reliable, real-time performance such as that required by the mission databases of the ICS.

The GDX II Real-Time Relational Database System does offer the level of capability such as that required by the mission databases of the ICS. GDX II can guarantee this performance

by implementation of memory-only data tables (c.f. disk-based tables) for up to 16 Mbytes (1 GByte with a vendor-implemented engineering change). An important requirement within the ICS would be the provision of non-volatility for these data tables. Two technologies exist which offer such capability; these being battery-backed-up RAM and Flash EPROM. It is concluded that the latter technology offers considerable benefits in appropriate applications in terms of reliability and cost.

The GDX II system, while having found field applications for some 15 years, is not well-known as an industry standard. It has also been developed primarily for RMX-based systems which is considered a drawback as this operating system is not recommended as the primary choice for the ICS standard computing segment.

6.3 On-line Databases

It is concluded that any of the multi-user SQL database management systems described above are suitable candidates for the implementation of non-time-critical databases. Some of these are more suited to the application than others. The optimum choice would depend on a detailed analysis of the performance requirements.

It is concluded that no disk-based system (including so-called RAM disks) could guarantee a data transaction in less than 10 ms. The data access performance of the fastest magnetic disks is in the order of 10 ms **average** with worst-case values being several times higher. The data access performance of the fastest optical disks is in the order of 40 ms **average** with worst-case values again being several times higher.

It is suggested that DBMSs with OLTP performance ≥ 10 TPS (transactions per second) would be suitable for the ICS.

6.4 Unix Compatibility

Should a choice of a real-time Unix/POSIX operating system be made, the Informix DBMS is considered a good candidate as an on-line database.

6.5 RAN Ship Information Management System Application

It is worth noting that the Oracle DBMS is finding application within the Ship Information Management System (SIMS) on the state-of-art Type 471 diesel electric submarines of the Royal Australian Navy (RAN) [9.2.24]. The SIMS is essentially a 100- to 200 Gbyte on-line operations and maintenance database onboard the submarine itself. Another Oracle application is the associated Configuration Management Information System which contains important submarine logistics information. The two systems are integral in providing a ***paperless submarine***.

While the use of Oracle is in itself noteworthy, it is contended that the use of an industry-standard, SQL DBMS running on distributed, hardware-independent platforms, is in fact, more so.

6.6 Bulk Storage Devices

For the purposes of data storage capacity as well as mechanical, environmental and EMC integrity, it is concluded that optical disks offer far superior performance to magnetic disks for the storage of non-time-critical data.

6.7 Towed-Array Sonar Implications

While the provision of a Towed-Array Sonar (TAS) has not been considered within the ICS, a *fit-for-but-not-with* approach should be taken in respect of its implications on database and LAN requirements. This is because a TAS requires extensive inter-sub-system and inter-database communication, this having significant impact on shared database requirements.

7. RECOMMENDATIONS

7.1 Database Model, Architecture and Implementation

The DBMSs should employ the **relational model** in a **client-server architecture**. Databases should be centralised **or** distributed according to their client profiles i.e. databases with mainly common clients should be centralised (e.g. target database) while databases with different clients should be distributed, but nevertheless **locally** centralised (e.g. sonar, EW and ship databases).

Database **servers** should be redundant i.e. mirrored and also employ **disk** mirroring.

Critical segments of databases should be replicated on geographically-isolated servers where they can be accessed (through the Logic Router if necessary) to provide a down-graded mode of operation in battle-damage situations.

Time-critical segments of databases should exist in non-volatile RAM. Flash EPROM should be used for static and semi-static data with battery-backed RAM for dynamic data segments.

For the purposes of data storage capacity as well as mechanical, environmental and EMC integrity, optical disks should be employed as opposed to magnetic disks for the storage of non-time-critical data.

7.2 DBMSs from Multiple Vendors

A detailed study should determine whether the use of a single DBMS type is possible throughout the ICS (and the platform as a whole). This would be desirable from a standardisation perspective, but it may not be practical considering both the real-time requirements and the storage requirements.

7.3 Rapid Prototyping

A variety of different commercially-available DBMSs in a variety of configurations should be prototyped and benchmarked using the ICS Architecture Concept Demonstration Model (ACDM). This will reduce the risk in making the correct choice as well as provide hands-on experience to database implementers.

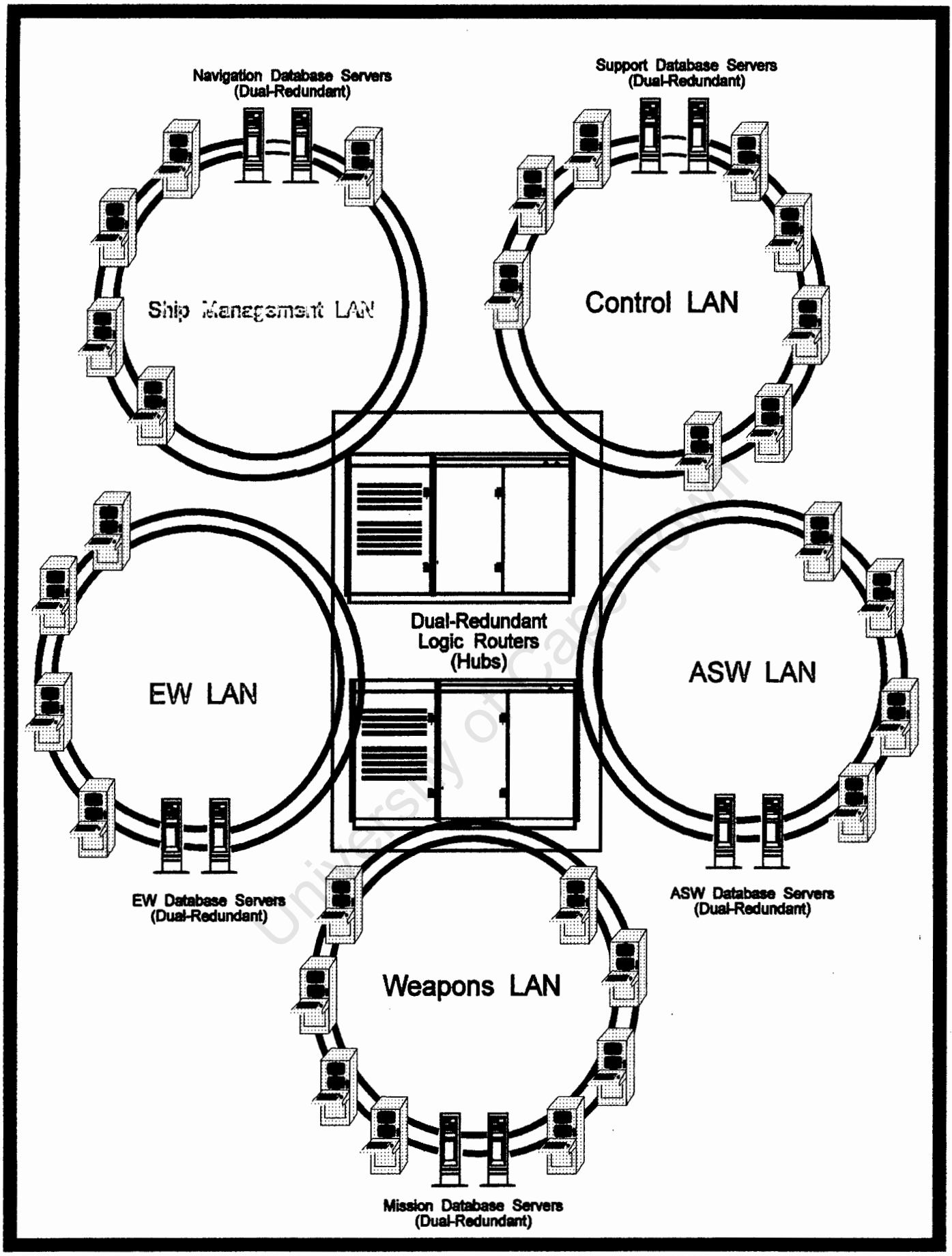


Figure 18 : ICS LAN-based Database Infrastructure

Implementation Issues

1. Scope

This appendix addresses various issues which deserve consideration in the implementation of an Information Management Infrastructure.

1.1 Cable Plant

1.1.1 Fibre Optic Cable

The recommended fibre optic cable type for critical applications consists of individual single-fibre cables called Optical Fibre Cable Components (OFCCs) laid with strength members around a central member and jacketed for environmental protection (see Figure 19). A typical OFCC cable can accommodate 12 fibres in a 15 mm cable.

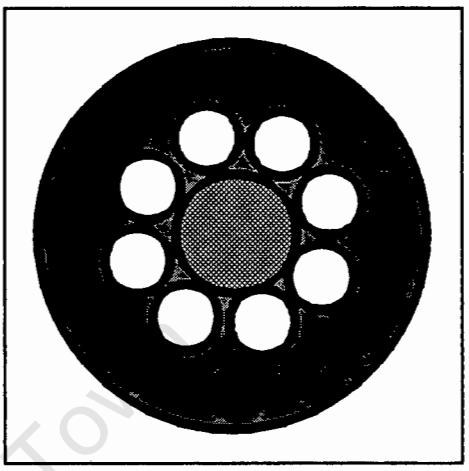


Figure 19 : OFCC Cable

1.1.2 Fibre Optic Connectors

Two types of connectors are recommended, the Single Fibre Light Duty Connector and the Multi-Fibre Heavy Duty Connector. The former are used inside interconnection boxes and equipments where they do not have to withstand the full extent of the harsh environment. They typically feature the ST (straight tip) bayonet-type design. The latter are used for main cable trunks and are designed to withstand the full rigours of the harsh environment. They consist of standard rugged-type connector housings with special optical inserts.

1.1.3 Fibre Optic Cable Splices

Single Fibre Light Duty Splices are possible inside interconnection boxes and equipment. Having this splicing capability considerably enhances onboard

maintenance and reconfiguration. Such splices are based on the commercial rotary splice and consist of a single glass tube which is broken into two pieces during the installation process. Each half of the tube is terminated in much the same way as a connector and then the two pieces are re-assembled as before they were separated.

1.1.4 Fibre Optic Interconnection Boxes

Interconnection Boxes terminate main cable trunks. They are designed to withstand the full extent of the harsh shipboard environment as well as protect the connectors and splices contained within. Boxes are modular with a typical design allowing up to three modules. Each module may contain up to 48 connectors or 144 splices. The boxes are designed to optimise onboard maintenance (refer Figure 20).

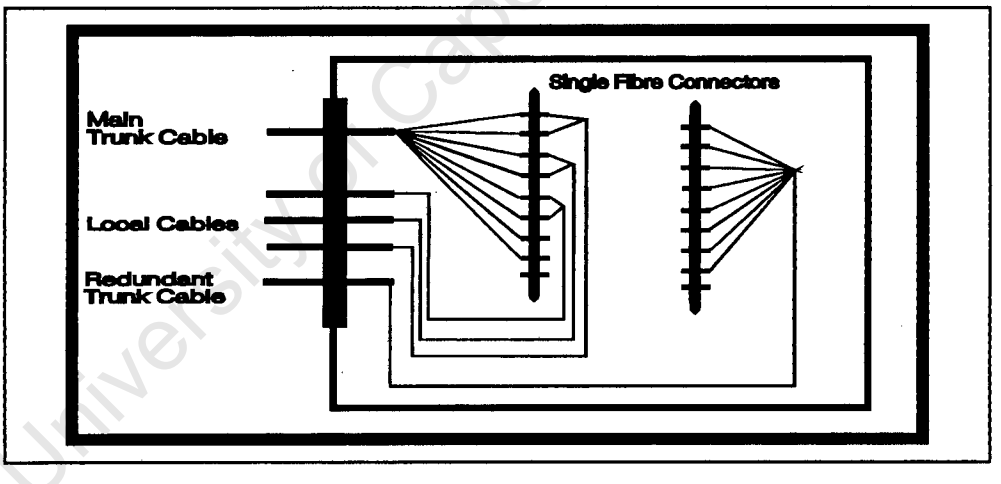


Figure 20 : Fibre Optic Interconnection Boxes

1.1.5 Optical Bypass Switches

In a high reliability environment such as the ICS IMI, a further enhancement to the cable plant is the provision of Optical Bypass Switches (OBSs) at every retransmission node. An OBS is an opto-mechanical switch which will physically re-route the optical signal around a node in the case of node failure, e.g. power failure. An OBS will stop the fibre optic

ring from "wrapping" and sub-dividing in the case of two or more node failures. Only three consecutive OBSs can be operational before optical power reaches a minimum.

1.2 Communication Protocols

1.2.1 Global Time Service

The SAFENET defined Global Time Service [9.2.6] will provide to processes within a node a precise Calendar Time (time of day) which is consistent over the LAN. A precision of one binary millisecond is required with provision being made to represent time to a precision of better than a nanosecond over a time span of several hundred years. It also provides a means to co-ordinate this time with an external time reference such as that which may be obtained from a ship's navigation system and to provide the time stamp in a variety of formats including Greenwich Mean Time. There is no existing or proposed ISO standard for such a service over the LAN.

1.3 Real-Time Operating Systems

1.3.1 Real-Time Unix

The most universally used operating system is Unix developed by AT&T. While standard versions of Unix cannot be considered as real-time operating systems, many vendors are developing versions of Unix with real-time extensions [9.2.27]. Examples are Hewlett-Packard's HP-UX and Concurrent Computer Corporation's RTU.

Another US company, Lynx Real-Time Systems, Inc., have developed the **LynxOS** real-time operating system [9.2.28]. While LynxOS is claimed to be fully Unix-compatible, it is also claimed to have been "written from scratch with performance, standards, and the

needs of the real-time developer in mind". LynxOS is also advertised as compliant to POSIX 1003.1, 1003.4 and 1003.4a. It also supports real-time Ada as well as the following processors : Intel 80386, 80486 and i860; Motorola MVME 147, 68030, 68040 and 88100; Sun SPARC 2; MIPS R3000 and R6000. For a 33 MHz 80386 (2 wait-states and 64 Kbyte cache), Lynx claim that their LynxOS/386-AT exhibits a *worst-case task response time* of 180 μs for a scenario involving 2 interrupts, or 270 μs for a scenario involving 5 interrupts.

LynxOS has found application on the US Space Station Freedom as well as in the fields of chemical, nuclear and automobile engineering and robotics.

1.3.2 Ada's Real-Time Kernel

An important feature of the Ada HLL is that it offers an optional, built-in real-time kernel. In certain applications this is sufficient to provide task scheduling, interrupt control, etc. However, in most medium to large applications, this kernel is not extensive enough to replace a full-featured real-time operating system.

1.3.3 Intel iRMX

iRMX is a Real-Time Executive developed by Intel Corporation. It is a multitasking executive designed for use as a standard software component in real-time embedded computer applications. iRMX also provides for a stripped down version of the executive, the Real-Time Kernel (iRMK). iRMX is well supported within the DOS and Intel development environments.

1.3.4 VRTX

VRTX is a real-time kernel developed by Ready Systems, Inc. It is similar in many respects to iRMX.

Like the former, VRTX is well supported within the DOS and Intel development environments.

1.4 Application Software

1.4.1 The Ada High-Level Language

The Ada High-Level Language (HLL) [9.1.7, 9.2.35] was developed to contribute towards the objective of software reliability, life cycle cost reduction, portability and reusability. Its development was sponsored by the US Department of Defense (DoD) to solve the problem of massive, software-intensive systems that present a set of specific language requirements.

The DoD mandates the use of Ada for all mission-critical applications unless the programme can justify the cost advantage of another language over the **system life-cycle.**

The design requirements for the Ada language were as follows :

- Structured constructs.
- Strong typing.
- Relative and absolute precision specification.
- Information hiding and data abstraction.
- Concurrent processing.
- Exception handling.
- Generic definition.
- Machine-dependent facilities.
- Efficiency.

Other desirable attributes of high-quality software are re-useability and maintainability. **Object-Oriented** methods are recommended to attain these ends.

Ada supports the following object-oriented characteristics :

- Data Abstraction - Types and subtypes
- Encapsulation - Packages
- Polymorphism - Generics

An Ada program consists of one or more program units. All Ada program units consist of two parts :

- Specification - Identifies the visible information to the client.

- Body - Unit implementation details which are hidden from the client.

These parts can be separately compiled. This gives a very powerful feature in using Ada as a Program Design Language (PDL). The interfaces (specifications) of a program can be verified very early in the project development cycle. With some extra coding of the program bodies which perform the calls, the flow of the program can be verified before detailed coding. These are powerful methods for the design of large software programs. They also give the design team confidence in the program's correctness very early on.

Ada includes a number of built-in attributes and constructs which support reliable software. These include structure, strong typing and exception handling.

The Ada development environment also defines what is termed the Ada Program Support Environment (APSE) which is a set of tools that assist in the implementation of effective and reliable code.

1.4.2 The C High-Level Language

The C programming language is a procedural language developed primarily by Dennis Ritchie at the University of Berkeley. C is not specified as a language, but ANSI standards are being set for various revisions of the language. It is thus a fast-developing language with many somewhat different versions.

C is a flexible high-level language that also offers low-level constructs. These features give the programmer access to the hardware in a high-level language format. The flexibility of the language often leads to cryptic, unmaintainable source code.

Some C compilers allow programmers to customise their programs for type checking, but no out-of-bounds checking is provided.

1.4.3 The C++ High-Level Language

The C++ programming language is an object-oriented extension of the C language. Again C++ is not specified as a language. C++ is a fairly new language and is neither stable nor mature.

C++ does implement more rigid type checking than C. It is, however, a true object-oriented language which implements polymorphism (run-time creation of software entities) which can lead to unreliable code.

1.4.4 Ada 9X

The next generation of the Ada language is under serious consideration by its sponsor and other interested parties. Requests for Proposal have been issued by the Ada Joint Program Office (AJPO) to compiler developers for their proposals in respect of the attributes, capabilities and features for the

next generation of Ada language and its development environment.

Due to the lengthy formalised process of the definition and acquisition process, no definite timescales have been set for the availability of next generation compiler products, hence the term Ada 9X.

While there are number of technical considerations for Ada 9X, one of the most important and controversial is the new language's support (or otherwise) for object-orientation.

1.4.5 Development Methodologies

A number of different development methodologies have arisen or been derived in order to influence software quality and reliability. The US DoD prescribes DOD-STD-2167A for most defence software acquisitions.

1.4.5.1 DOD-STD-2167A

DOD-STD-2167A is a US Department of Defense (DoD) military standard entitled ***Defense System Software Development***. The stated objective of the standard is to provide "a means for establishing, evaluating, and maintaining quality in software and associated documentation". The standard achieves this by prescribing a software engineering approach as well as a number of Data Item Descriptions (DIDs). The standard does not prescribe a dogmatic adherence to itself, however, and in fact requires appropriate tailoring in accordance with DOD-HNDK-248, ***Guide for Application and Tailoring of Requirements for Defense Acquisitions***.

The basic approach of DOD-STD-2167A is the logical phasing of the software acquisition

process and the documentation of the major activities/outputs of these phases. The major applicable phases of the software development process map closely to normal system acquisition, i.e. functional analysis and decomposition, planning, specification, design, development, integration, testing and qualification. The outputs of these phases are a set of documents: System Design Document, Software Development Plan (SDP), Software Requirement Specification (SRS), Software Design Document (SDD), Software Source Code, Computer Software Configuration Items (i.e. operational code), Software Test Specification (STS), Software Test Procedures (STPs), Software Test Results (STRs), Software Product Specification (SPS), Software Version Description (SVD). All are described by an appropriate DID (DI-MCCR-800xxA).

It is recommended that a tailored DOD-STD-2167A software development methodology should be followed. Such tailoring, as well as factors such as the use and implications of CASE, should be described in the Software Development Plan.

1.4.5.2 Computer-Aided Software Engineering (CASE)

Computer-Aided Software Engineering (CASE) is a relatively new methodology to increase the effectiveness of software development. Such increases in the overall development effectiveness will also have positive influences on software quality and reliability. One reason for this is that CASE contributes towards making software development more of a science and less of an art. It also reduces some of the drudgery associated with documentation generation,

especially back-annotation required during the iterative design and development process.

One of the most important factors in achieving high quality, reliable software is effective software documentation. CASE tools can aid significantly in achieving readable, consistent and useful documentation including the all-important logic and flow diagrams. Some CASE tools also offer I/O consistency checking and type checking as well as static and dynamic simulation. The **Statemate** package is more of the Computer-Aided **System** Engineering tools with a software orientation and offers static and dynamic simulation. It also offers DOD-STD-2167A type documentation output.

1.4.5.3 Computer-Aided System Engineering

Due to the complexity of current system designs and implementations, software tools to support Computer-Aided System Engineering are also becoming available. Such tools will lead to designs that are more correct than traditionally designed systems. Development of these systems will also be faster and less expensive.

Software packages such as Statemate can be effectively used to specify, analyze and model complex reactive systems. They enable early detection of errors through powerful visual modelling, executable specifications and early rapid prototyping. They address the behaviour of a system in its environment over time, including behavioral interactions between parts of the systems and between systems and sub-systems.