*Trans IMarE, Vol 102, pp 57–66*

# Development of a ship-wide control and surveillance system for fleet replenishment vessels

**C T Marwood**
Hawker Siddeley Dynamics Engineering Limited

## SYNOPSIS

*This paper outlines the development of onboard facilities for a new fleet support vessel with defensive capability and helicopters, with requirements similar to warships. It must also operate economically in peacetime with minimum manning, calling for remote control and surveillance of a wide range of machinery.*

*A 4000 point distributed system has been designed which allows control from five consoles using colour VDUs. Development cost and risk have been minimised by using existing designs where possible, and by providing flexibility to cope with an evolving machinery configuration.*

## INTRODUCTION

The development of a control and surveillance system for a new class of Fleet Auxiliary vessels is nearing completion. The scope of control includes propulsion, ancillary, auxiliary, cargo handling and damage containment. This paper covers aspects of the equipment design to satisfy the combination of naval and mercantile requirements which this type of vessel must meet.

The extent of remote control and automation has grown significantly, in line with recent trends in ship platform system design.[1,2] The techniques adopted to achieve the development under the constraints of a fixed-price contract are described, along with some of the problems and solutions.

## REQUIREMENTS

### Ship and machinery

The *Fort Victoria* is the first of a new class of fleet replenishment ships of 31 500t designed by Harland and Wolff for 'one-stop' replenishment. They will carry both liquid and dry stores, be able to operate several helicopters and provide facilities for vertical take off aircraft. A self-defence capability is supported by tracking radars and extensive electronic surveillance systems. Survivability is ensured by NBC defence systems, high shock resistance, and good roll stability even after partial damage.

Replenishment at sea calls for simultaneous operation of most of the ship's machinery systems. Dual purpose rigs are fitted for transfer of liquids or solids to more than one vessel at a time. While the main liquid system is pumping diesel oil, lubricating oil, aviation fuel or fresh water from one of the many storage tanks, ballast pumps are operated to a pre-planned corrective programme. Helicopters may be in use to carry out vertical replenishment and the defensive radar and surveillance systems may also be operating. Fire prevention systems will be available in case of fuel spillage and the electrical generation system will automatically increase output to ensure reserve power capacity.

The equipment to be controlled and monitored requires a total of around 4000 input or output signals, allowing for future growth. This includes:

Tim Marwood began his career as an engineering apprentice and progressed through design of electronics for engine controls and computers to ship controls. He is now Technical Consultant in the Defence Division of Hawker Siddeley Dynamics Engineering Limited and has spent the last 14 years on analogue and digital marine systems.

1. Propulsion; twin shafts with medium speed reversing diesels;
2. Ancillaries; fuel, lubricating oil, cooling, start air compressors;
3. Electrical; six diesel generators with three 3.3 kV switchboards and low voltage distribution;
4. Cargo/Ballast; approximately 70 tanks, 25 pumps and 200 valves;
5. Damage control; fire pumps and valves, ventilation clearance fans, sprinklers, foam, halon, plus flooding, door and hatch indication;
6. Auxiliaries; refrigeration, chilled water, boilers, compressed air and domestic services.

Only about one third of the signals are in the main engine room area, the remainder being spread throughout the ship as shown in Fig 1. Approximately 500 are intrinsically safe circuits associated with hazardous areas.

### Manning levels and operating positions

Manning levels for new Royal Fleet Auxiliary vessels have been reduced towards merchant ship standards when in low-level operational states. The number of operators for replenishment at sea must be kept to a minimum, although the amount of machinery is higher than in earlier ships. This requires increased use of remote control and surveillance, plus automation of some functions which were previously carried out manually. For example, sequence re-starting of essential services and motor drives following electrical black-outs to avoid overloading the generators. From Falklands experience, rapid assessment of damage or fire is essential to decide priorities and prevent the problems spreading. The ship is divided into mul-

tiple fire zones with an extensive monitoring and fire suppression system. Surveillance of doors and ventilation has been improved to reduce the time for manual checking when close-down is required.

The size of watch teams and the number of control positions in use depend largely on the ship operating state. Under most conditions the machinery control room is unmanned, following merchant ship UMS practice. In this state alarms (other than machinery alarms) are announced at the bridge. Machinery alarms alert the duty engineer on call and can be displayed in the chief engineer's office. The main positions for remote control shown in Fig 1 may be manned in the action state. They are as follows:

1. Bridge; propulsion and steering;
2. Machinery console; ancillaries and auxiliaries electrical generation;
3. Damage control headquarters; damage control including ballast monitoring;
4. Damage control console; damage control (backup control position).

In addition, local manual control is provided adjacent to each major item of machinery.

## Unusual requirements

Many of the features in this type of vessel may be found either in warships or merchant ships, but rarely in the same equipment. Shock levels in the machinery spaces are higher than for some warships and the ship must be protected against the effects of nuclear weapons. However, Lloyd's Register rules and the requirements of the British Department of Transport must be met, including safety regulations regarding fire and explosion hazards. In some cases requirements go beyond these standards.

The extent of remote control and surveillance for platform machinery is higher than in most warships, either in-service or planned. This shows the increasing trend towards more effective monitoring systems, which enable manning levels to be reduced during normal operation, and enables a quicker response to malfunctions or damage.

# DESIGN CONSIDERATIONS

## Form of distributed system

The considerations addressed here relate to the design of equipment to implement the overall ship control and surveillance systems requirements, which had already been agreed between the MOD and the shipbuilder. A distributed system had been chosen, since the widespread locations of machinery and control positions, shown in Fig 1, would clearly make a centralised system impractical and uneconomic. The choice then lies between the various forms of distributed system which can be considered as follows:

1. Distribution by function;
2. Centralised control, distributed surveillance;
3. Distribution by location;
4. Semi-distributed.

These systems are made up of processor-based intelligent units, combining control and surveillance outstations located in machinery spaces and communicating with control positions by a serial data link network with its own central data collection and display processors.

The relative merits of each of the forms of system are fully discussed elsewhere,[3] and are summarised in Table I.

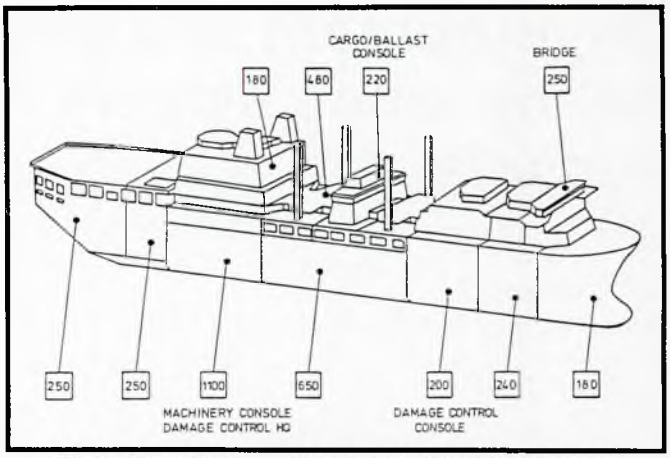


**Fig 1: Operating positions and signal distribution**

Distributed control and surveillance by location was adopted for the majority of the system, siting the outstations so that the number of signals is evenly shared regardless of function, thus minimising cabling between plant and outstations. However, important plant items, eg a propulsion engine or a switchboard, are handled by a single outstation so that they do not depend on the operability of several units. If this outstation fails, alternative backup is provided by hard-wired controls.

Other non-critical functions involving widely distributed plant connect to multiple outstations, one of which acts as co-ordinator while the rest simply act as remote input/output interfaces.

## Multiple control positions

Control positions are located at various parts of the ship and some functions need to be provided at more than one location. Damage control, for example, may be carried out from the main headquarters in the machinery control room (MCR) or the secondary headquarters or from the bridge. This requirement calls for a large amount of information to be displayed quickly, at up to nine multi-function VDUs and several dedicated panels, and for transfer of control for specific functions between locations. Display and acceptance of alarms is subdivided between the control positions, depending on the operating state.

## Cost

This was a major influence in the design of the control and surveillance equipment. It became clear that cost was one of the most important of the contract selection criteria and that a special-purpose design to full naval standards would be unlikely to win. It was essential to use as much existing developed hardware and software as possible and minimise the cost of configuring the equipment to fit the ship machinery arrangement.

At the bidding stage hardware estimates were reduced by carefully choosing components which met the environment and performance requirements without over-specifying.

Fortunately, although the equipment was designed to be capable of meeting the full warship environment, its modular structure allowed the degree of protection to be tailored to suit the ship requirements. For example, the cost of radio interference filters for a merchant ship are significantly less than for a warship. Application engineering costs were kept low using standard table-driven software for machinery interfacing together with an existing display system which offered most of the facilities needed.

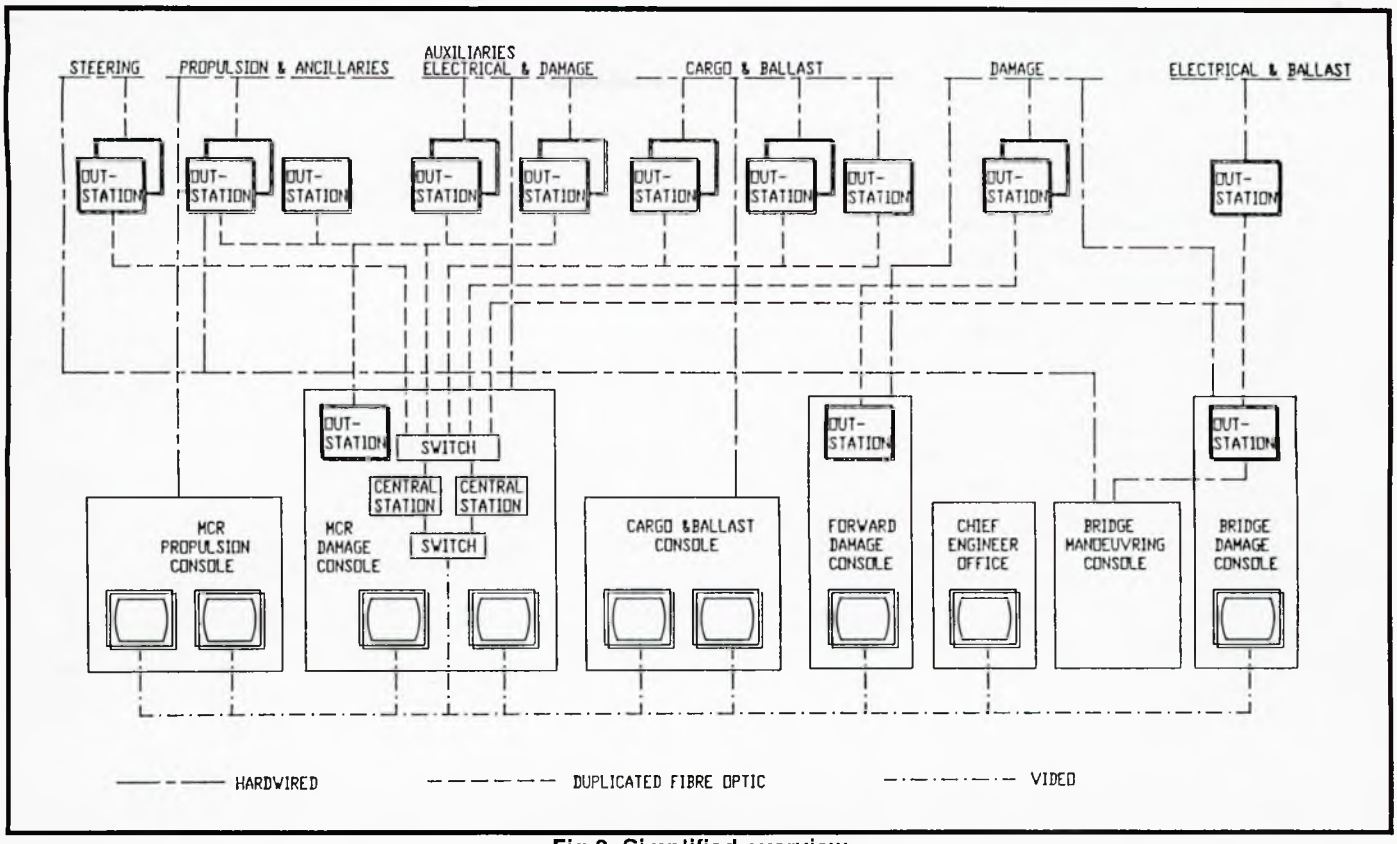


**Fig 2: Simplified overview**

**Table I: Summary; centralised/distributed comparison**

| | *Cabling cost* | *Electronics cost* | *Fault tolerance* | *Vulnerability* | *Comments* |
|---|---|---|---|---|---|
| Centralised control and surveillance | High | Low | Poor | Poor | Feasible for small systems only |
| Semi distributed control and surveillance | Low | Medium | Medium (good with duplicated central unit) | Medium | – |
| Centralised control distributed surveillance | Medium | Medium | Medium | Medium | Requires duplication for fault tolerance. Large systems not feasible |
| Distributed control and surveillance by function | Medium | High | Good | Good | Widely dispersed systems not feasible |
| Distributed control and surveillance by location | Low | Medium | Good | Good | More complex co-ordination and data traffic |

## Reliability and availability

Replenishment at sea must be carried out quickly and effectively for many reasons, including the risk of collision and the vulnerability to attack while the ships are linked. The reliability of the control equipment must be such that there is a very high probability of successfully completing a replenishment. Lloyd's rules also define the degree of independence of the control, alarm and monitoring systems necessary to ensure that no single failure can cause an unsafe condition. Essential functions within the control system must be maintained for 30 min after a total loss of electrical power.

Achieving this reliability at a realistic cost involved a careful assessment of the key items in the equipment which could affect the ability to continue replenishment, and a consideration in each case of whether duplication or backup by a simpler form of control was needed.

## Flexibility

The risks to cost and timescale due to changes in requirements were increased by the size of the system, its unusual requirements and innovations in operating methods. Since the last details were unlikely to be finalised until late in the tight delivery programme, flexibility was called for in the total number of signals and their location in the ship. Spare capacity in each unit and the communications network, plus the ability to modify displays or enter new functions quickly, were essential to keep the risks low.

# THE DESIGN SOLUTION

## Overall description

The solution shown in Fig 2 resulted from the system design

preceding the requirement specification and from the development jointly carried out with the shipbuilder (Harland and Wolff plc) and consultants (Shell Seatex) using the above design considerations.

Control and surveillance functions are combined within the distributed digital system, with a number of hard-wired backup controls. All nine displays are driven from the central station which co-ordinates and collects data from the 20 outstations. Most of the outstations are located close to machinery or other equipment, but some are used to drive hard-wired indicators and switches on dedicated control panels. Units for this purpose are fitted in the bridge console and damage control consoles, giving significant savings in ships cabling and electromagnetic filters.

High reliability and fault tolerance are ensured by duplication of the communications links and central station and by hard-wired remote controls for vital plant. An extensive monitoring and alarm reporting system presents full damage control information at the bridge when other positions are unmanned, and provides a variety of logging print-outs.

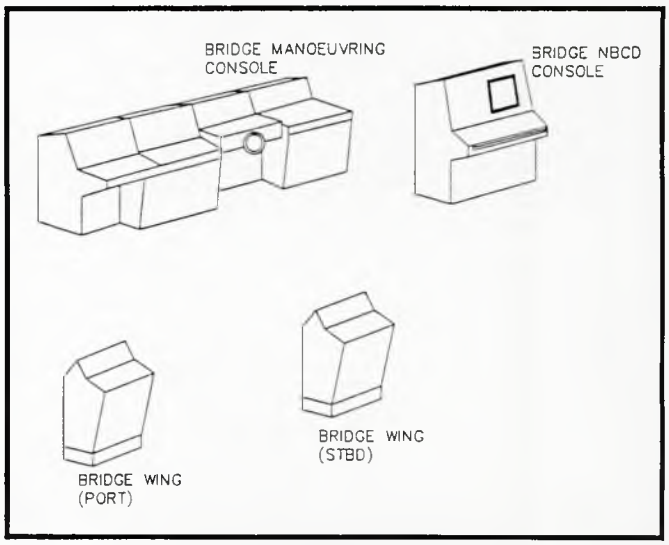


**Fig 3: Bridge and wing consoles**

## Operating positions

### *Bridge*

The bridge manoeuvring console shown in Fig 3 is fitted with all necessary controls and alarms for full automatic control of each shaft, including engine reversal and clutch control for crash stop manoeuvres. The levers are electrically linked with those on the bridge wings and compared with the MCR propulsion console lever settings, enabling rapid transfer of propulsion control. Dedicated meters and lamps show engine speed, group alarms and other prime indications, and push buttons are fitted for emergency hard-wired functions.

A separate bridge damage console provides an alternative position when the headquarters damage control console is unmanned. Alarm information and mimics from the damage system can be displayed on the colour VDU, and remote control can be carried out from a simple keypad.

### *MCR propulsion console*

Consoles in the MCR and replenishment control centre are shown in Fig 4. A propulsion panel is the primary position for propulsion control actions. Additionally, two colour displays and keyboards are fitted for control and surveillance of ancillary and auxiliary machinery. Each can call up any of the mimic or text display pages and can be independently manned in emergencies. The operator at this position can delegate control to the bridge and can limit the maximum engine speed available at the bridge and wings. Hard-wired controls include the backup engine speed demand and hard-wired emergency stop buttons.

All alarms and propulsion orders are logged automatically on separate printers.

The machinery control console also serves for monitoring electrical generation and distribution. A separate power management system supplies status and alarm information. The chief engineer's office is also provided with a VDU console to monitor propulsion, auxiliary, ancillary and electrical plant.

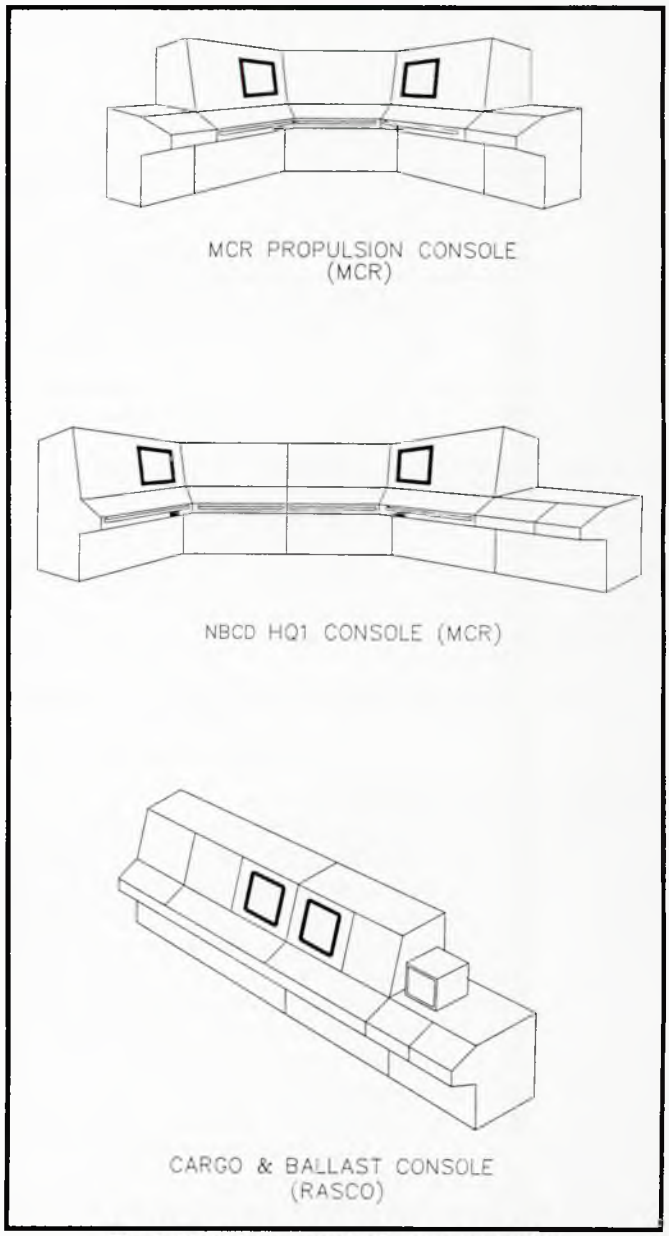


**Fig 4: Machinery control room consoles**

### *Damage control HQ*

This is the main console for all NBCD co-ordinating functions, and is provided with two colour displays and keypads as well as hard-wired fire detection mimic panels. This console is designed for peacetime incidents as well as action state conditions. The aim is to establish the ship state as quickly as possible and allow marking up of traditional incident boards by copying

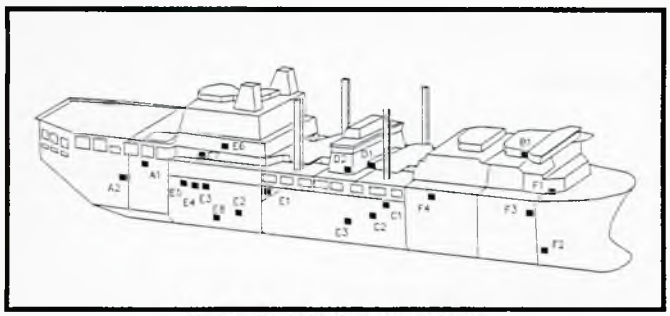

**Fig 5: Outstation locations**

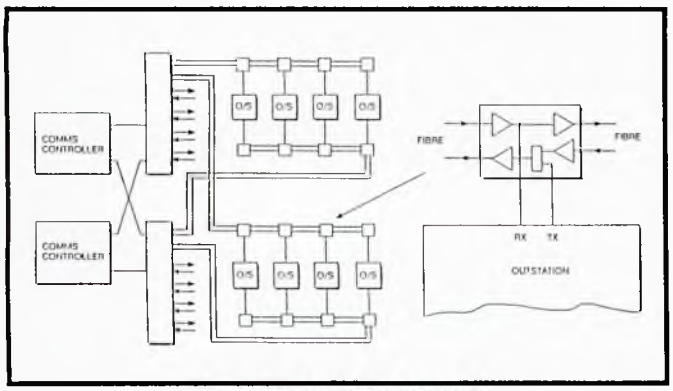


**Fig 6: Fibre optic network**

from a VDU or from hard copy print-out. Remote operation of firemain pumps and zone stop of ventilation fans can be carried out under direct operator control from this position.

### *Cargo/ballast console*

This position controls all cargo transfer operations for replenishment and cargo loading. As more than one transfer may be in progress at any one time, two colour displays with keypads are provided for controlling pumps and valves and monitoring tank contents. Loading calculations are carried out on a dedicated computer to ensure stability and optimise trim.

### *Forward damage control*

This console is only manned in the action state and provides a local damage control point if the MCR is unavailable.

## Control and data collection

Outstation distribution is shown in Fig 5. One type of outstation is used for control and surveillance throughout the ship, reducing the spares count and giving the most flexibility in allocating signals between units.

Each outstation can handle up to 256 signals and allows combinations of analogue and digital signals by fitting appropriate interface cards. Individual channels can be configured to suit most types of ship signals including voltage, current and contact inputs. Analogue and switched outputs are used for driving panel indicators or controlling machinery.

Machinery interface channels are scanned at selectable rates, in accordance with functional requirements, by a special purpose module which stores the results in memory, leaving the main processor free for higher level functions including communications, control sequencing and alarm detection. All configuration data including alarm limits are held in non-volatile memory, and can be adjusted onboard if necessary.

Although each outstation performs different functions, modules of the same type are interchangeable. The differences are defined in the configuration data, of which two copies are held in each outstation. If a processor module is changed, the data is automatically transferred.

The outstation is constructed in two main parts, one enclosing the terminals for ship cables, while the electronics is housed in the front section. This enables the terminal box to be installed separately in the ship and the wiring to be checked out fully before the electronics section is fitted, thus allowing full access to terminals without risk of damage to the electronics.

## Communication and the central station

The central station performs three key functions as follows:

1. Communication between all outstations and control consoles.
2. System level co-ordination of self check and alarm facilities.
3. Display generation and operator keyboard handling.

The first two functions are carried out by the communications processor, while all VDUs are handled by the display driver. The complete central station and all communication links are duplicated, operating in stand-by mode. The outstations are linked to both central stations in a multi-drop star network of fibre optic links (Fig 6). Each group of outstations is connected so that failure of any single unit does not affect both communication paths.

The communications processor controls all data flow through the system, polling the outstations according to a priority schedule and transferring commands and machinery status. Message frames are based on the high-level data control (HDLC) structure, with a cyclic redundancy check for error detection and recovery.

Fibre optic links give inherent galvanic isolation and immunity from interference as well as a data rate well in excess of the maximum total requirements.

Each group of outstations is connected to the data collector by two independent multi-drop chains. Each link has separate cores for transmit and receive signals. Two spur point units in each outstation provide optical/electrical interfaces and regenerate optical signal levels. The two chains for a group of outstations are connected to separate star centres. The connections are arranged so that the first outstation in one chain is the last in the other chain. This ensures that no single failure of a link, spur point or star centre can isolate any outstation. If one outstation fails, all others remain connected. The star centres are located adjacent to the data collectors and are connected to them by automatic changeover switching.

Each link in the multi-drop chain has a two-way fibre optic cable with an optical transmitter and receiver at each end. The twin core cable is reinforced with zero halogen cladding and is waterblocked so that it can safely pass through bulkheads. High efficiency light emitting diode (LED) transmitters operate at low power levels giving very high reliability, whilst the shielded receivers ensure freedom from electromagnetic interference problems.

Links can be up to 250m including allowance for two extra connectors per link, should repairs be necessary. Maximum data rates exceed 1Mbps, well in excess of the system data rate.

## The display driver

The display driver is a multi-processor system, each of its display channels having its own processor and memory to give 1s page changing and fast response to keyboard inputs. All display processors access a common dynamic database which

holds the current state of all signals in the ship system. This is under the control of a separate processor and is constantly updated by information coming from the communications processor. A separate block of memory holds the static backgrounds on which the dynamic data is superimposed.

For this vessel over 50 pages of displays include the following types:

1. Mimics of each main ship system, colour coded according to function, showing plant operating and alarm status, as shown in Fig 7. Full use is made of colour changes and blinking to highlight hazardous conditions. The three oldest unacknowledged alarms are shown at the bottom of each page.
2. Chronological alarm lists display all alarms in order of occurrence with supplementary data. When printed, time and data are added. Alarms can be acknowledged in any order from this page.
3. Hierarchical or group alarm pages provide an overview of all alarms and warnings, broken down into machinery or plant groups.
4. Status tables are used to compare plant operating states for specific groups of equipment.

## Fault tolerance

In setting out to achieve the target figure for reliability in completing replenishment, the types of faults which could affect this figure have been examined. These fall into three categories as follows:

1. Random failures of the electronics and wiring of the control system.
2. Faults in the ship power supplies to the control system.
3. Damage by fire, flood or enemy action.

The effects of a single fault are also important, for example the number of electrical generators or cargo pumps which cannot be remotely controlled. Manning levels do not allow for all functions to be carried out simultaneously in the absence of remote control, although essential services must be maintained to meet safety regulations and the basic needs to stay afloat and manoeuvre.

The design of the control and surveillance system is aimed at reducing the extent of single faults so that only a very small percentage would interrupt replenishment. The risk of these faults affecting performance is then further reduced by redundancy or backup. If a VDU display becomes unavailable, control can be transferred to another predefined position since the facilities are identical. Dual central units and data links give a very high availability, and signals are allocated among the outstations to avoid a single failure affecting more than one major function. Each outstation can operate either from the ship's ac supplies or a battery backed inverter, and power supply cables from the two sources are routed separately.

If both communication paths to an outstation are lost it can continue to operate in a 'stand alone' condition, carrying out the last orders received or reverting to a safe control state. Propulsion outstations continue controlling the engines and clutches using hard-wired lever inputs. Alarm detection continues, each outstation having indicators locally and at the MCR propulsion console.

Independent backup is provided for critical functions where remote control is essential in the event of an outstation fault. For example, the engine governor and trip controls are separately wired to the machinery console.

## Software

The software structure makes maximum use of existing proven software within a well designed framework so that the control and surveillance functions specific to the ship can be specified and implemented easily. The operating system and display software are proprietary packages with many previous applications. This approach reduces development cost and risk significantly.

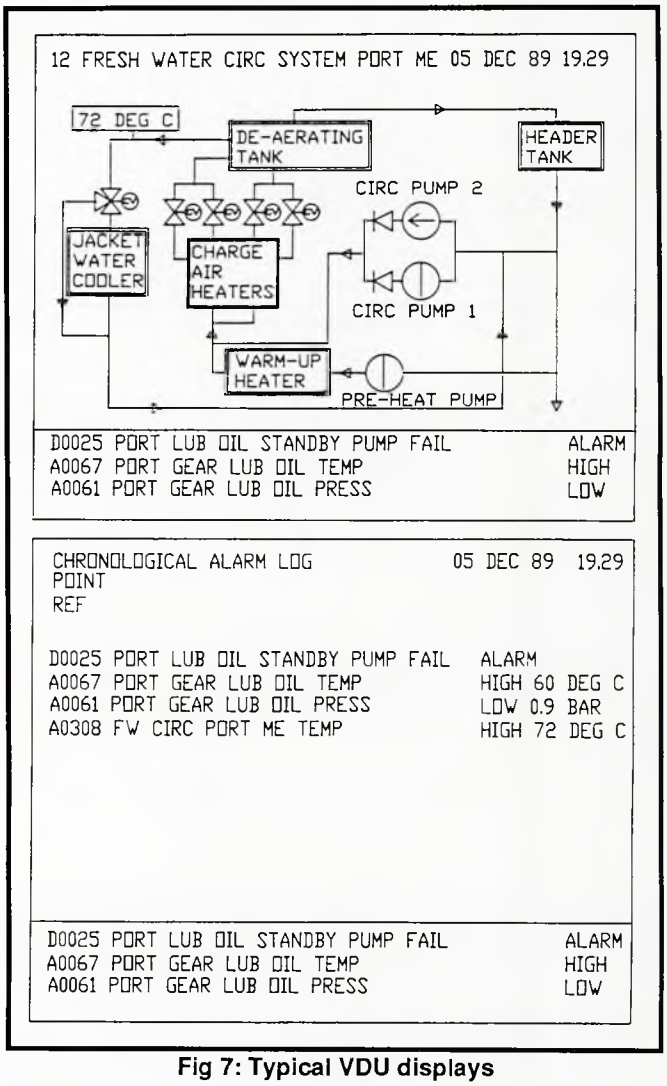


**Fig 7: Typical VDU displays**

The system software performs general functions, which need not vary greatly between types of ship, such as: data communications, input/output signal conditioning, alarm handling, internal safety checks and diagnostics. It is mainly written in PASCAL, with some assembler for efficiency of execution, and is designed to simplify the applications software by removing most aspects of data handling and system housekeeping.

Applications software implements the control and surveillance functions for each machinery group. A new approach has been made in specifying the detailed control sequences and algorithms, and generating the PASCAL code automatically. A proprietary software design package enables the systems engineers to enter the control function in the form of a flow diagram with decision tables. This accurately specifies the response to combinations of machinery and operator inputs and simplifies checking to ensure that all possibilities are considered. The flow diagram is then automatically converted into PASCAL modules for integration with the system software. This approach helps to clarify the initial definition and allows modifications to be made by changing the flow diagram, which is less prone to error than changing the code manually.

Many standard features are table-driven, using the same code with data tables containing the parameters which vary with each use on the ship. Input signal handling, for example, will contain tables of channel number, scaling and alarm levels. These can readily be changed onboard by the maintainer without the risk of affecting the program code.

The complete tables for 4000 channels make up a complex database which is held in non-volatile memory in the installed system. During development the database has been built up and modified under a database manager as each stage of information became available. Loading from the development computer into the ship hardware is an automatic process, with data checking to guard against errors.

Long term support depends on clear and complete documentation, and this is achieved by a top-down design approach with four levels of definition below the functional specification. Configuration and change control procedures ensure that documentation and firmware are identified and traceable.

## Maintainer facilities

The overall availability targets call for fast repair times, which must be achieved even though the system is more extensive, manning is reduced, and no increase in maintainer skill levels is assumed. However, with the diagnostic maintainer unit and self check software, defective modules can quickly be identified and replaced. Faults in external analogue sensors can be identified by validating input levels, which is performed automatically during input signal processing. The electronics, including memory, are constantly checked as a background task during normal operation and power up. Faults are indicated as VDU warnings and locally on each central station and outstation. When the portable processor-based maintainer unit is connected to the station, a range of facilities is available. While the station is operating normally, alarm and self check details can be shown and the current level of inputs or outputs displayed in engineering units.

If the station is taken out of service, authorised adjustment of settings, such as alarm levels or filter time constants, can be made without risk of changing control software. Higher levels of privileged access permit control schedules to be changed. Much of the testing can be made without opening the outstation or disturbing the electronics thus avoiding maintenance induced faults.

## CONCLUSIONS

The final design is more advanced than for some warship systems now being developed in terms of the extent of remote control, signal capacity and number of control positions. It has been made feasible and cost effective due to the advances in distributed microprocessor technology.

The major factors which have influenced the development of the control and surveillance equipment have been the unique combination of naval and merchant ship standards and the need to minimise cost. High levels of environmental protection require design and quality of engineering above normal classification society requirements, while duplication or multiple levels of backup control give assurance of operability after faults.

Tight cost constraints forced a design solution which minimises new development and includes flexibility for detailed requirements to be varied until well into the programme, including mimic displays and detailed control algorithms.

As the requirement for automation increases and the scope for complexity grows to meet it, the definition of control functions and monitoring requirements becomes more and more significant. In the early stages of design details of minor equipment, such as valves and sensors, may not be known, and the final definition of interfaces and interlocks requires considerable effort by experienced engineers from the shipyard and controls supplier. Ways to reduce this, including a limited range of proven methods for remote control of common items such as standby pumps, are being considered.

The modularity of hardware and software resulting from the development makes it usable for systems ranging from 500 – 5000 points, up to eight VDU control positions plus extra VDU monitors and hard-wired panels. Multi-function graphic displays can be combined with dedicated control panels according to ergonomic needs. Fault tolerance can be ensured by automatic changeover to standby equipment, stand alone operation of individual units and independent backup hardware. Control requirements from simple on-off switching to joystick manoeuvring with co-ordinated propulsion, steering and thrusters can be accommodated. These features enable the equipment to meet the needs of a wide range of ships, both naval and maritime.

## ACKNOWLEDGEMENTS

The author would like to thank colleagues at Shell Seatex and Hawker Siddeley Dynamics Engineering Limited for their help in preparing this paper, and to Harland and Wolff plc and the UK Ministry of Defence (PE) for permission to publish this paper.

Opinions expressed are those of the author.

## REFERENCES

1. C T Marwood and T Munk, 'Flexible controls for a flexible ship', Proceedings, 7th Ship Control Systems Symposium, Bath (1984).
2. C T Marwood, 'The growth of shipwide digital systems', Proceedings, 8th Ship Control Systems Symposium, The Hague (1987).
3. C T Marwood, 'Benefits of totally distributed control systems', Proceedings, Maritime Communications and Control, Institute of Marine Engineers, (October 1988).

# Discussion

**B S Rayfield (MoD(PE))** The MoD insist on using high grade electronic components, such as to BS9000, in such equipments for warships. Could Mr Marwood please comment, outlining the HSDE procedure for selection of components and how their contribution to reliability is assessed. It is noted that environmental conditions in the AOR are only slightly less onerous than those on a fully fledged warship.

**C T Marwood (Hawker Siddeley Dynamics Engineering Ltd)** HSDE component selection procedure is geared to the Quality Plan for each project, reflecting the reliability, availability and environmental requirements. Where the criticality of modules calls for maximum reliability, component specifications meet BS9000 or MIL Spec levels.

**Capt R Settle (Royal Fleet Auxiliary)** For such a shipwide system was it ever considered to incorporate condition monitoring/vibration monitoring with back analysis, in order to tie up with a PM system/performance control?

**C T Marwood (Hawker Siddeley Dynamics Engineering Ltd)** Machinery health monitoring, including vibration trend analysis, has been offered as a part of similar shipwide systems, as the data collection and display facilities are compatible. However, it has not been considered during our involvement with this project.

**J K Robinson (Lloyd's Register)** I would like to thank the author for his comprehensive paper on perhaps the most extensive and complex ship surveillance and control system installed to date. I am especially pleased to see his emphasis on configuration management and change control procedures.

1. *Hardware configuration.* It is presumed that availability targets were specified for various ship operations. Would the author give some typical figures and also clarify what other formal techniques were used to decide the degree of redundancy, segregation and diversity proposed in the final system?
2. *Software verification.* It is noted that the operating system and display software were propriety packages. Would the author illustrate some of the previous applications, length of in-service experience and performance statistics used to justify the choice of package(s)?

The large number of ship function applications multiplied by the number of individual commissioning engineers makes the task of software verification somewhat horrendous and the decision to use a software tool, in the form of automatic generation of PASCAL code, is very sensible. What confidence can we place on the 'tool' itself; was it in turn validated by analysis such as MALPAS?

3. *Software security.* What are the security arrangements limiting access to the various levels of authorisation corresponding to the different types of software modification?
4. *Fibre optic maintainability.* Whilst noting the high level of alternative routeing and segregation of the fibre optic network shown in Fig 6 was it considered prudent to have onboard repair capability? If so, what was the appropriate cost of the splicing and test equipment, and what degree of proven reliability of the joint was specified, especially in respect of vibration endurance?
5. *Environmental protection.* Would the author clarify what particular environmental criteria, other than shock and EMP aspects, were specified above classification society requirements?

**C T Marwood (Hawker Siddeley Dynamics Engineering Ltd)**

1. Availability targets for the system are classified, however the levels for operations of essential equipment in fault situations required multiple levels of backup, and segregation of vital systems. An availability analysis was used to validate the design.
2. Software for the display system has a history of 5000 applications over 9 years, ranging from control of oil rigs, hovercraft and steel mills to automated production lines. Many of these have safety-critical aspects.

The operating system has been in service since 1982 with hundreds of users in the UK and USA. Applications include railway signalling and real-time control of electrical generation and distribution.

The Kindra tool for automatic software generation has been exhaustively tested by British Telecom, the designers. In addition we have carried out our own validation of examples of code.

3. Maintainer onboard access to software is only permitted to predefined data areas where adjustment may be required, eg alarm levels, with password and/or key protection. At this level no changes to program code are possible. Authorised modifications can only be made by firmwave replacement. Display system software configuration changes require a special keyboard which is not part of the normal onboard equipment.
4. Fibre optic splicing equipment costs under £700, while detailed checks require a test kit at £2100. Reliability of a joint is specified as 757 000h and if supported by conventional ducting or ties will take account of normal shipborne vibration levels.
5. In addition to shock and EMP, ambient temperatures are specified up to 65°C and supply frequency transients to 15%.

**G S Penrose (MoD(PE))** I note that the main propulsion controls have connection with actuators by hard-wiring as well as through the digital control system, but it is not clear to me whether the controls of the main auxiliaries are activated by push buttons, or whether all controls have to be accessed via the keyboard.

I have two supplementary questions to add to Mr Robinson's regarding transducers and sensors:

1. Is the production testing of plant carried out with its own sensors, or is it in the ship that sensors and plant first meet?
2. I take it that plant subcontractors have no need to concern themselves over the control system that links their plant actuators and sensors other than to specify signal levels, ie the digital transmission system is 'transparent'.

**C T Marwood (Hawker Siddeley Dynamics Engineering Ltd)** Main auxiliaries are normally controlled from keyboards, however, push buttons are provided for emergency actions such as safety stops. Local control is also available for backup.

Sensors are not included in the MCAS Scope of Supply, but we would expect the majority of on-plant sensors to be checked during production testing of plant.

Plant subcontractors have an important role to ensure compatibility with MCAS. Signal types, ranges and earthing

must be agreed for monitoring, and interlocks, sequences, trips and local/remote switching for control. The functions of on-plant controls and trips must be clearly specified. Once this task is achieved – a major one for a large ship – the subcontractors need not be concerned with the way that the system functions.

**W F Cheung (Lloyd's Register)** Although, noticeably, an increased number of computer systems is being used onboard ships, the use of fully distributed computer controlled systems handling such high density of data are less common, compared with land based applications. With the advance in computer technology in recent years, and with much improved software coupled with a steadily reduced cost in hardware, it is almost certain the concept will have a far reaching impact in the marine industry as a whole in the forthcoming decade.

The paper presented by Mr Marwood not only provides a detailed yet comprehensive insight to the topic, but also helps, I believe, to remove some of the uncertainties about this type of system some operator may otherwise have, which should be congratulated. Following are questions which I would like the author to expand upon.

In the section on communication between the central station and the outstations, data flow is achieved by the polling method on serial lines. In view of the fact that there are 20 outstations comprising some 4000 points, which potentially could even be extended in future applications, it is not clear whether the target response time will always be guaranteed, particularly when functions which require attention may occur simultaneously? For most industrial applications, and Classification Rules, the update time is usually in the order of 1–2s for critical and alarm parameters. These figures are considered comparable to conventional alarm systems. If the number of data points is to be increased to such an extent that the update time falls outside the limit or the access time requires to be improved, could the signals be obtained via the two independent multidrop, fibre optic, links?

Information presented to the operator should be in a logical manner. In the case of the vessel being damaged in action, many alarms will occur at the same time. Could the author explain these situations by expanding upon the information as presented in Fig 7 of the paper, particularly in terms of alarm handling and the possibilities of overloading the system?

On software aspects, it is noted that both system and application softwares are mainly written in PASCAL, which is essentially a sequential language and not specifically designed for on-line real-time control applications. Traditionally, CORAL 66, with its proven track record, is mainly used in military related applications. Yet this computer language is not being selected in this instance. What would be the major factors in choosing PASCAL and not others?

**C T Marwood (Hawker Siddeley Dynamics Engineering Ltd)** The polling system is designed so that the update time for the data collection system does not deteriorate even under abnormally high alarm traffic caused by damage. Although performance could be further improved by increasing data and polling rates, the operator is now the limiting factor in handling alarms. To deal with large numbers of alarms, all the VDU terminals can be used for display of chronological alarm lists or mimics with highlighted alarms. Each operator can deal with a specific group of equipment. Further assistance is given by group alarm displays, identification of first-up alarms and by local indication at outstations.

PASCAL is a high level, block structured language which places particular emphasis on data typing, and is one of the most widely used languages for real-time systems. Alongside ADA and CORAL, PASCAL and FORTRAN have been used for many years in military circles, and support software and tools are less readily available, whereas PASCAL is one of the few compilers with a British Standard validation suite. We have experience of both for real-time use on similar hardware and found similar performance.

**G Tweed (Harland and Wolff (Technical Services) Ltd)** With reference to the system's flexibility, how easy is it to add or change signals with respect to cost and time?

**C T Marwood (Hawker Siddeley Dynamics Engineering Ltd)** Compared with hard-wired systems, it is cheaper and quicker to add an extra mimic page than to fit an extra control panel, and configure it with information from any channel in the system without adding wiring from one end of the ship to the other. The range of adjustments and additions which are possible is much wider, including complex control schedules, non-linear signal conditioning, interlocks and display techniques. Because of this, it is often assumed that any change is easy, but in practice because the system is more flexible, changes must be described in detail and checked thoroughly to ensure that no side effects have been introduced.

**J C A Crook (Harland and Wolff (Technical Services) Ltd)** I regret that I was unable to attend due to a prior engagement but wish to congratulate the author on a most interesting paper.

Engineers, like myself, who served their time before the introduction of the microprocessor, become confused by the concept of 'distributed' control and surveillance being described as a new concept. History has a way of repeating itself and at times going in circles.

A typical ship in the 1960s would have a number of local control panels, using pneumatic and hard-wired technology; important alarms, indications and grouped alarms would be cabled over multi-core to a central position. Alas, the air-conditioned central control room was not thought necessary at that time and of course manning levels were higher than today.

In the 1970s arguments raged about the relative merits of pneumatics versus electronics. Electronics finally won the day but the delicate nature of these systems dictated that a centralised, air-conditioned control centre became a necessity.

This brings me to my first point, which is the environmental protection of the local control units, which would seem to be a key issue but is not discussed in any detail. Could the author provide further information?

My particular worry centres on abnormal conditions such as protection of the electronics during maintenance, both of the electronics themselves and nearby machinery. For instance, on a ship in which I served in the 1970s, I recall one local control panel being ruined by water spray from a pipe flange which had been carelessly opened up, by shore-side workers, during maintenance. Panels were also damaged by impact by heavy items slung from cranes. In real life there can also be problems from 'finger trouble' and over keen painting. Centralised systems can be supervised more effectively.

I should be most interested in further details of comparative costings of the centralised versus decentralised arrangement. It would seem from the paper that each local control panel has four fibre optic cable terminations, two power supply cables and a dedicated alarm cable, whereas four 50 pair cables could be used to hard-wire signals from a termination box to a centralised control panel.

The paper mentions the fact that important backup controls are hard-wired to the control centre. This is good practice of course, and may be necessary to meet Lloyd's requirements.

But the authors will no doubt be aware of the HSE guidelines for microprocessor based systems which put things in a more general context and advocate analysis of the system. Were the HSE guidelines considered in the design; more particularly was a formal hazard analysis performed to identify the safety related systems? Is the author aware of any work being performed to put the HSE guidelines into a marine context?

The paper does not address the problem of software faults in any detail, but this is a major worry to the HSE and other industrial users.

A recent paper outlining proposed new HSE guidelines for ESD systems mentions a serious explosion and fire at an oil refinery due to concurrent failure of the control system, alarm system, shut-down system, along with inadequate relief, causing loss of life.

The paper says that hardware reliability does not protect against errors in the specification, misunderstandings or incorrect assumptions about the plant state, or failure to fully consider the effects of modifications on plant safety, all of which can totally invalidate the ESD system.

Whilst I appreciate this paper does not discuss ESD systems, the principle is the same in that hardware reliability is of no benefit if the system performs the wrong control action, due to an oversight. Has the author any comments on this point?

My personal view is that problems of this sort are best avoided if the control and surveillance system is understood in detail by the widest possible range of people. In fact, in my experience, many of the early problems of automation systems resulted from incomplete understanding by operators, and owners adopting a stand-off approach, treating the automation systems as another item on the shipping list. Training and education markedly improved the situation. Has the author any views on the subject?

Looking to the future, could the author give his views on the international initiatives to standardise communication protocol between computerised devices? OSI and Fieldbus seem appropriate to the marine world.

**C T Marwood (Hawker Siddeley Dynamics Engineering Ltd)**

1. Outstations are sealed to IP55, so would be unlikely to be damaged by accidental spray. The case will stand up to much heavier impacts than panels, and the two-part construction allows the electronics to be installed after cabling is complete and most of the heavy equipment has been secured. First-stage diagnostics is carried out without opening the case.
2. To compare costs, an equivalent centralised system to provide the same capability as an outstation would need to include:
   a. cables for up to 250 channels, each with three cores for potentiometers or RTD sensors, individually screened to reduce interference;
   b. duplicated cables to give the same redundancy as the dual fibre optic links – a further 750 cores;
   c. change-over switching for each channel between duplicated cables;
   d. thermocouple compensation and pre-amplification;
   e. local alarm annunciation.

Regarding safety, Mr Crook's concerns were considered in the initial stages before Dynamics became involved, and later during development. Lloyd's rules require that system design precludes a single failure affecting control, alarm and safety of essential plant. To ensure this, safety protection, such as machinery trips and fire detection, is independent of the control and surveillance system. HSE were consulted early in the design phase, and were satisfied that this policy was being implemented. Controls are designed to fail set, with backup reversion for critical functions. Software self-checks constantly monitor for discrepancies from normal operation, with hardware watchdogs in case the software 'goes to sleep'.

I strongly support the view that the risk of safety problems is increased by a stand-off approach and lack of information. While it would be impractical to explain the system in detail to 'the widest possible range of people', the present procurement system appears to preclude direct discussion between the user/operators and designers. The information gap can be alleviated by a good training programme, but this is not the time to find errors in specification.

Control and surveillance systems – sometimes referred to as Platform systems when their scope includes most non-weapons functions – will increasingly need standardised interfaces to other ships equipment.

Other computers should connect through gateways to ensure safety, using the appropriate levels of OSI, or the Fibre Distributed Data Interface FDDI II (ANSI X3T95). For connecting to on-plant controllers Fieldbus is one of the main industry standards under consideration, but according to a recent conference report fully compatible sensors are not expected to be generally available until 1993.