THROUGH LIFE SUPPORT OF D86 BASED CONTROL AND SURVEILLANCE SYSTEMS

BY

COMMANDER J. W. BAILEY AMIMarE R.N.
M. K. PADDOCK
(Director General Fleet Support (Equipment and Systems))

AND

J. P. MABEY BSc
(Vosper Thornycroft (U.K.) Ltd)

This article is the authors' modified version of the paper published at the tenth Ship Control Systems Symposium, held by the National Defence Headquarters, Ottawa, Canada on 25–29 October 1993.

ABSTRACT

Vosper Thornycroft Controls Division (VTC) has developed for the MoD, a digital control and surveillance system based on their D86 computer. This system has been installed in the Royal Navy's Type 23 frigate, single role minehunter, TRIDENT and Type 2400 submarines. From an early stage the MoD recognized that there was a requirement to provide an efficient, cost effective through life support programme for these systems. This activity would require the construction of a ship set of equipment on shore for each system to be supported; an expensive option to set-up and maintain. The D86 factor led the MoD to request VTC to set-up a D86 based reference facility at their site at Portsmouth. The system is due to be completed and fully operational by the end of 1994. The reference facility will give support to the MoD in two essential ways. Firstly, the ability to assess the effects of change to either the software or hardware and prove their correctness prior to release to the fleet. Secondly, reported faults in ships at sea can be replicated and investigated on the shore based facility. The article provides an insight into the requirements behind the setting-up of the through life support facility and the philosophy used in its design and application.

Introduction

The new generation of Royal Navy vessels currently in build all utilize microprocessor based control and/or surveillance equipment for their machinery fits. The transition from what was conventional analogue techniques was fairly rapid, but still resulted in a range of architectures that were set according to their particular applications. The introduction of digital technology and its attendant software which, although familiar within weapons projects for many years, had not yet been applied to the quite different demands of marine engineering. This made it necessary to carefully specify requirements to the software engineer during development and test phases and, in particular, the subject of this article, requirements for through life support.

By successful tendering, Vosper Thornycroft Controls Division (VTC) won contracts for the provision of seven digital Machinery Control and Surveillance systems (MCAS) in four different classes of vessel. These systems which utilize VTC's D86 microprocessor based equipment are:

Type 23 Frigate (T23)

(*a*) MCAS.
(*b*) Main Electrical Power System (MEPS).

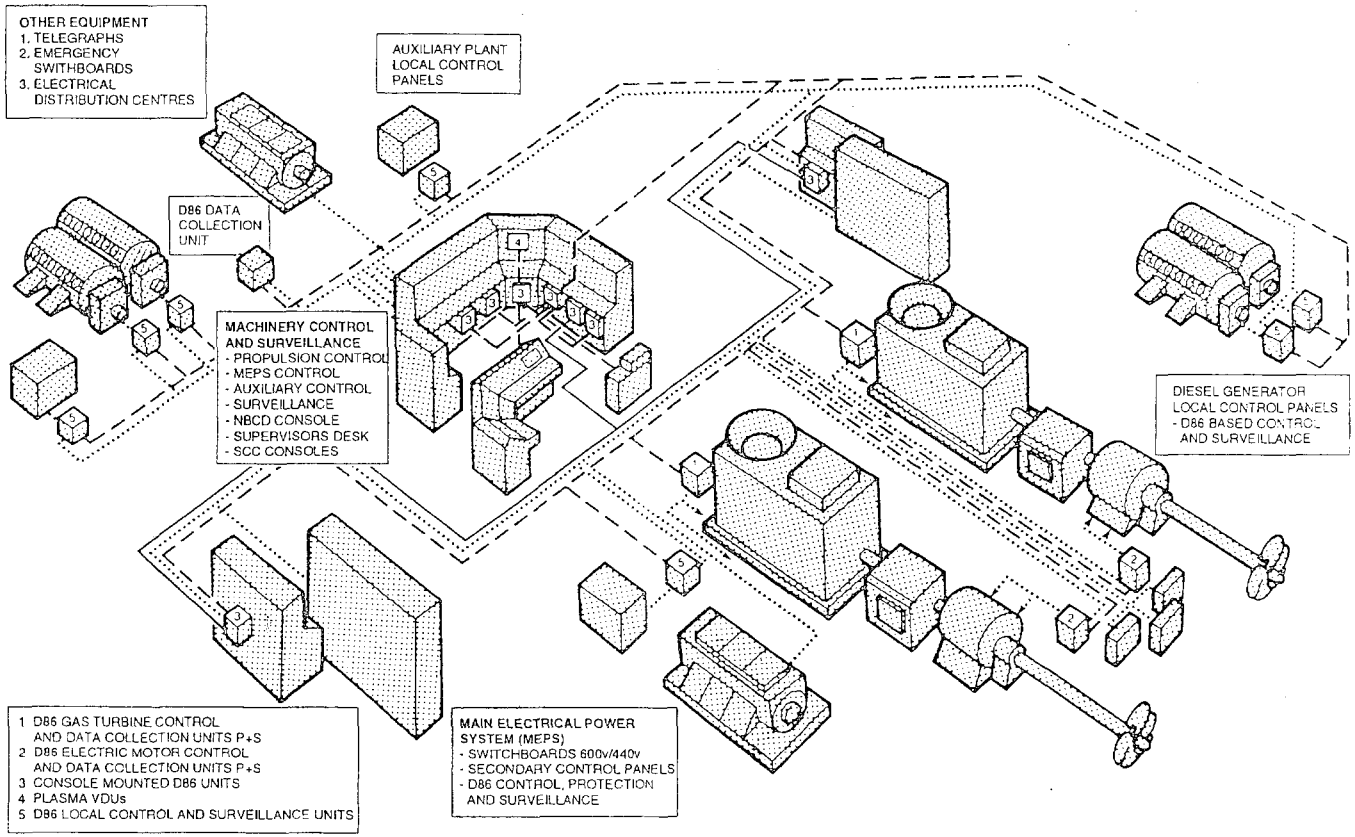

FIG. 1—TYPE 23 MCAS AND MEPS

(*c*) Diesel Generator Local Control Panels (DGLCP).
(*d*) Chilled Water Plant Local Control Panel (CWLCP).

Single Role Minehunter (SRMH)

(*a*) MCAS.
(*b*) Ship Positioning Control System (SPCS).

VANGUARD class submarine

(*a*) Machinery Surveillance System (MaSS).

UPHOLDER class submarine (T2400)

(*a*) MaSS.

This article will concentrate principally on the T23's MCAS system.

Type 23 Frigate—MCAS

The T23 is the Royal Navy's latest class of anti-submarine warship. It is equipped with a combined diesel electric and gas turbine propulsion system, which allows it to operate quietly at low power and achieve high speed at short notice. The T23 is the first British warship to make use of full digital control of its machinery and monitoring system. VTC was awarded the contract to design and build a completely integrated system (FIG. 1). The resultant system consists of D86 processors in the machinery control console with interfaces to the MCAS, MEPS, auxiliary machinery, chilled water and damage control system.

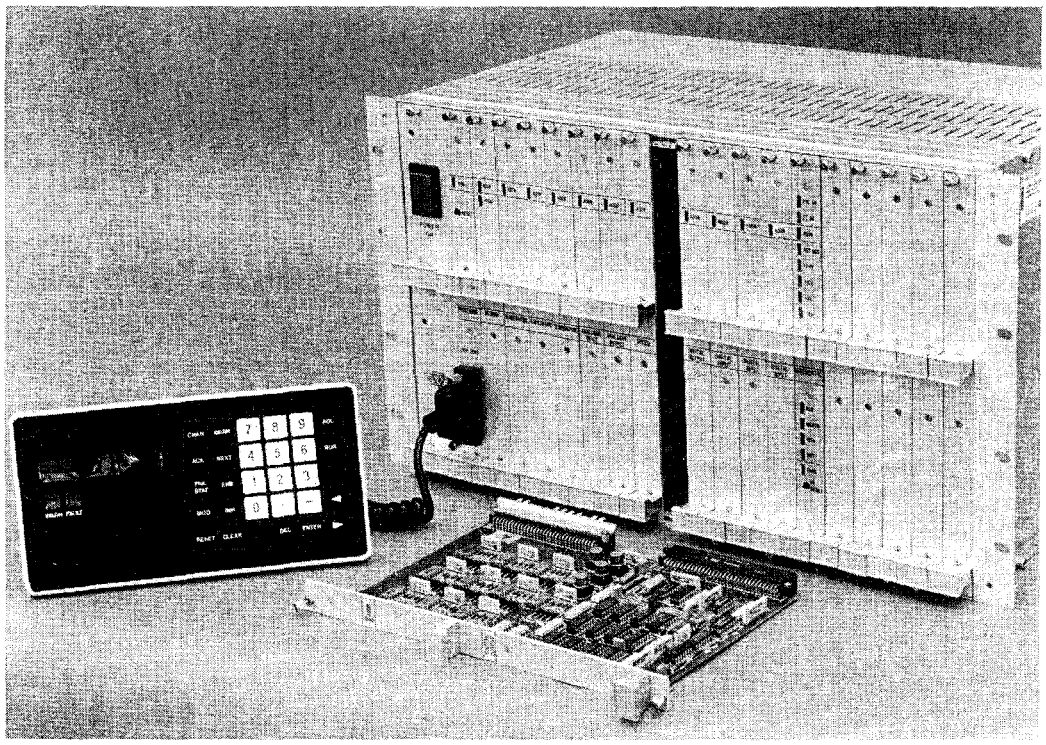

FIG. 2—D86 COMPUTER RACK ASSEMBLY

Each system comprises a central processor which communicates, via serial data links, with distributed Data Collection Units (DCUs) and Control and Data Collection Units (CDCUs). The DCUs and CDCUs, in turn, interface with the ship's plant providing control and monitoring. Each DCU/CDCU (FIG. 2) contains:

- D86 processor board.
- Memory board.
- Serial data communications board.
- Various digital and analogue Input/Output (I/O) boards.
- Diagnostics board.

Software contained on the processor and memory boards provides the control and monitoring functions associated with the attached plant.

The need for common support

D86 systems are based on a generic design developed by VTC. This means that, apart from a very limited amount of necessary development, the hardware for each of the systems is selected from an existing range. A similar situation exists with regard to foundation software, i.e. the software that carries out the low level functions associated with the control of the D86 hardware. The consequence of this is that there is a high degree of hardware commonality between the systems. Although there is more scope for the introduction of change into the foundation software, to suit the detailed system requirements, there should remain a good degree of commonality.

During the life of the Royal Navy's D86 systems it is to be expected that there will be modifications to hardware and foundation software, as well as to the high level user software and the Man Machine Interface (MMI). In order to minimise support costs and effort, it is necessary to ensure that the solutions to problems, that are common to more than one or all D86 systems, are only addressed once. This avoids the proliferation of differing standards for both hard and software within the supported systems.

The requirements can be met by the implementation of an effective system for configuration control. This will allow, before approval is given for the development of any modifications, for the:

- Identification of cases where commonality exists.
- Implications for all D86 systems where common hard or software is involved.

It is accepted for software driven machinery control systems, that the risk involved in using the platform as a proving ground for modifications is not acceptable due to:

- The potential for damage to machinery.
- Effects on the ship's operational programme.

For this reason, some form of shore based reference facility is required to allow development and proving of modifications to increase confidence before installation in a ship.

D86 systems are based on common hard and software, giving rise to the possibility of having a common reference facility with the consequential through life cost savings. It can be readily appreciated that the management of configuration control and the development, operation and support of a shore based reference facility, could best be controlled by the use of common facilities for developing and proving hard and software modifications and coordinating the approach to firmware control. This would also give rise to savings in staffing levels for support, by preventing the possibility of more than one group funding similar work on different projects.

REFERENCE FACILITY

Purpose

The reference facility is required to provide support to the D86 based systems in service with the Royal Navy, aboard the T23, SRMH and T2400 submarine. A separate facility for the TRIDENT MaSS is under investigation and collocation of these facilities has been proposed.

Primary purpose.

To provide an environment in which any element of D86 hardware, software or combination of these, under investigation, functions in the same manner as in its parent equipment and in real time.

Secondary purpose

To provide an environment in which the operation of any element of D86 hardware, software or combination of these, under investigation, can be studied to determine the detailed operating characteristics as an aid to fault finding. This need not necessarily occur in real time.

Requirements

In order that software faults might be investigated and modifications tested, the following major facility items are required:

(*a*) Target hardware.

(*b*) Test interfaces and equipments.

(*c*) Development and support computers.

The target hardware and associated test interfaces and equipments, must facilitate the exercise of system software (under investigation or modification), in a controlled and predictable manner. This enables the software in general, and modified modules in particular, to be tested in sufficient detail to ensure any software modification has been implemented correctly, without introducing adverse effect or error, detrimental to the system operation. The level of testing required and hence the sophistication of the test interface, depends upon the extent and complexity of the software changes being tested or fault investigated.

The hardware requirements are dependent upon the level of testing required and the complexity of the changes being tested. The facility requires a 'core' of target hardware and system test equipment, capable of testing the majority of perceived software changes and faults. Flexibility of design must be employed, so that if need be the facility may be enhanced at a future date.

The testing of certain software changes and in particular the investigation of specific faults, may necessitate the use of dynamic simulators if the required conditions are to be reproduced. As it is difficult to predict all potential fault scenarios, dynamic simulation may have to be provided for critical and complex areas of test interface. If fault conditions cannot be replicated on the reference facility, additional hardware and test equipment may be added, if deemed necessary, to replicate the required fault scenarios. Alternatively the fault might be investigated at source; i.e. on the ship itself. With respect to the ships, special data capture tools might be developed which would aid fault finding.

The reference facility is to be designed primarily as a software test tool. Fault finding being undertaken as a secondary role. By adopting this philosophy, the facility requirement for hardware test equipment may be targeted solely at the needs of software testing, rather than the subjective requirements of fault finding. The facility will then provide a technically competent, cost effective solution to software testing, whilst maintaining the ability to conduct limited fault finding investigations.

Options available

As a result of a study carried out by VTC, the following options, for the control and monitoring systems, were put forward for configuring a ship reference facility:

Hardware

(*a*) Option 1.
A complete set of equipment as supplied to the ship, including consoles and electronics racks.

(*b*) Option 2.
A complete set of equipment apparently as supplied to the ship, but constructed to commercial standards.

(*c*) Option 3.
A hybrid set of equipment which is functionally identical to the ship but has had the superficial equipment replaced. For example consoles would consist of a skeleton framework housing only the essential items.

(*d*) Option 4.
A complete set of ship's D86 racks with minimal packaging, suitable only for a test environment.

(*e*) Option 5.
A set of re-configurable racks that would allow all ship system scenarios to be tested adequately.

Test Interfaces

Similarly options were put forward simulating the items of plant to be controlled and monitored by the reference facility. These options were as follows:

(*a*) Static test interface (hardware driven):
Test interfaces consisting of sets of digital and analogue I/Os. In its simplest form this would be switches and potentiometers for inputs and lamps and meters for outputs. The test equipment driven by the facility operator to set up the required test scenario.

(*b*) Static test interface (software driven):
The test interface being computer driven. The operator would interface via a keyboard and pages on a screen. The pages showing a graphical representation of the real consoles and plant.

(*c*) Combined static test and computer driven interface:
Where signals are required to interact in real time, for instance during machinery changeover sequences, a computer simulation would be provided to respond to inputs and generate control outputs.

(*d*) Computer driven interface:
The entire I/O interface being controlled via a computer. Simulations of each item of plant being controlled and monitored, responding in real time to signals from the reference facility.

In order to assess the requirements further, two feasibility studies were carried out. The first looked in more detail at the option recommending re-configurable racks, by creating a prototype reference set for the T23 MCAS system. The second investigated the requirements for software testing during the through life support phase of a project. The levels of software testing required during this phase will influence the hardware requirements for the reference facility.

Software Development System (SDS)

Early in the design of the D86 T23 MCAS, a SDS was constructed by VTC to design and initially test software. Following this development phase, the software was fully system tested at VTC on ship sets, prior to their delivery to shipyards for installation. In the latter part of the MCAS build programme, the opportunity to system test software on ship sets before delivery diminished. In order to maintain continuity of system testing, it was decided that the SDS would be re-configured and enhanced to form what effectively became a prototype reference facility.

The SDS (FIG. 3), consists of a subset of the T23 MCAS hardware. Three permanently configured D86 racks replicate the central processing unit, with two more racks that can be configured as any of the remaining MCAS racks. The SDS also contains two plasma displays and printers. The I/Os are via D86 I/O test cards, which have been specifically designed to allow the static testing of the I/O on a specific D86 board. To help test the effects of loads on the serial data links another simulation has been created, known as the Bulk Loader. This provides the facility operator with the ability to load the serial data links, to various levels, connected to the central processing unit.

Software Testing

Software testing is generally regarded as a time-consuming and hence expensive exercise. Even the most detailed and prolonged testing cannot prove beyond all doubt that a system is error-free. The software user is therefore faced with deciding upon the degree of confidence which is acceptable for the application. The reference facility must provide sufficient flexibility to allow the normal software testing life cycle to be applied to a software modification. The software life cycle for new software under development is shown in (FIG. 4).

Unit and Integration Testing

There are two stages during testing which are dedicated to the task of testing software only. They are:

(*a*) Unit Testing:
Where the functionality and logic are checked.

(*b*) Integration Testing:
Where the interfaces between software modules are checked.

System Level Testing

After unit and integration testing of software is performed, systems level testing aimed at testing the software in conjunction with the hardware may be performed. Three specific types of systems level testing are:

(*a*) Load Testing:
Tests the software's ability to handle external stimuli.

(*b*) Regression Testing:
Provides sets of system level tests that exercise as much of the software as possible.

(*c*) Endurance Testing:
Tests the software over an extended period to ensure that there are no long term timing problems.

Whenever possible, tests should also be selected to demonstrate the defensive qualities of the software. This defensive testing ensures that the software does not adversely affect other areas of system operation. For instance the software must be able to handle corrupted input without crashing or failing to inform the operator.

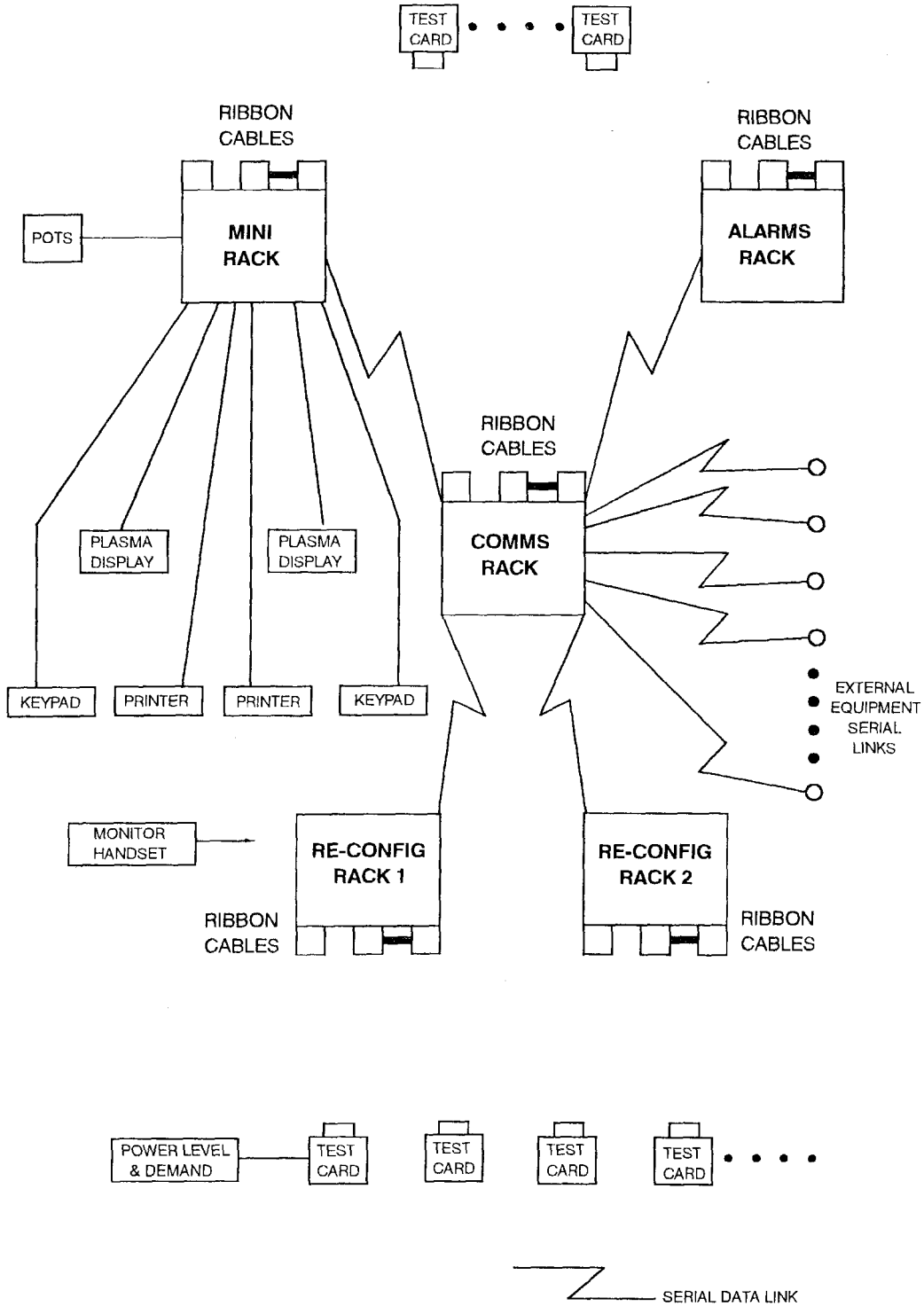

FIG. 3—SOFTWARE DEVELOPMENT SYSTEM BLOCK DIAGRAM

For post design support, it is often not necessary to test software changes at a unit/integration level. If a change can be fully tested at a higher level then there is no benefit to be gained in testing it at a lower level. If a change can be tested at a system level, less resource is required since it avoids the need to set up special software test harnesses for the test. If the test fails however, it can be more expensive to correct than if testing had automatically started at the lowest level required. Figures have been estimated for the level of confidence in the correctness of a software change, after differing levels of software testing have been carried out. Table I shows confidence levels for different levels of software testing on two types of software change:

- Simple data change, e.g. a warning level changes.
- Code change, e.g. the logic to an engine start sequence changes.

TABLE I—*Cumulative Testing Confidence Levels*

	Data			Code		
Software Test Level	**Minor** %	**Medium** %	**Major** %	**Minor** %	**Medium** %	**Major** %
Software rebuild only	66.0	30.0	10.0	50.0	30.0	10.0
Specific tests of change	90.0	65.0	50.0	90.0	65.0	50.0
Regression testing	95.0	90.0	70.0	95.0	90.0	65.0
Full system test	99.0	99.0	99.0	99.0	99.0	99.0
Full dynamic use at sea	99.5	99.5	99.5	99.5	99.5	99.5

Types of Software Testing

The different types of software testing are defined as follows:

(*a*) Software rebuild only.
The modified software is simply compiled and re-built into a system. The testing checks the modification has the correct syntax.

(*b*) Specific tests of change.
The module of software containing the change is tested.

(*c*) Relevant regression tests.
The regression tests pertinent to the software module containing the change are performed i.e. a subset of the full system test is carried out.

(*d*) Full system test.
A complete system test is carried out on the software system.

(*e*) Full dynamic use at sea.
The software system is exercised in its normal working environment.

Evaluation of options

A detailed evaluation of each option was made by the design authority and the following assessment made:

Option 1

Although providing the best system functionality and MMI with minimal design costs, the total cost of providing identical shore base ship sets for the seven systems and the space required to house them made this option prohibitive.

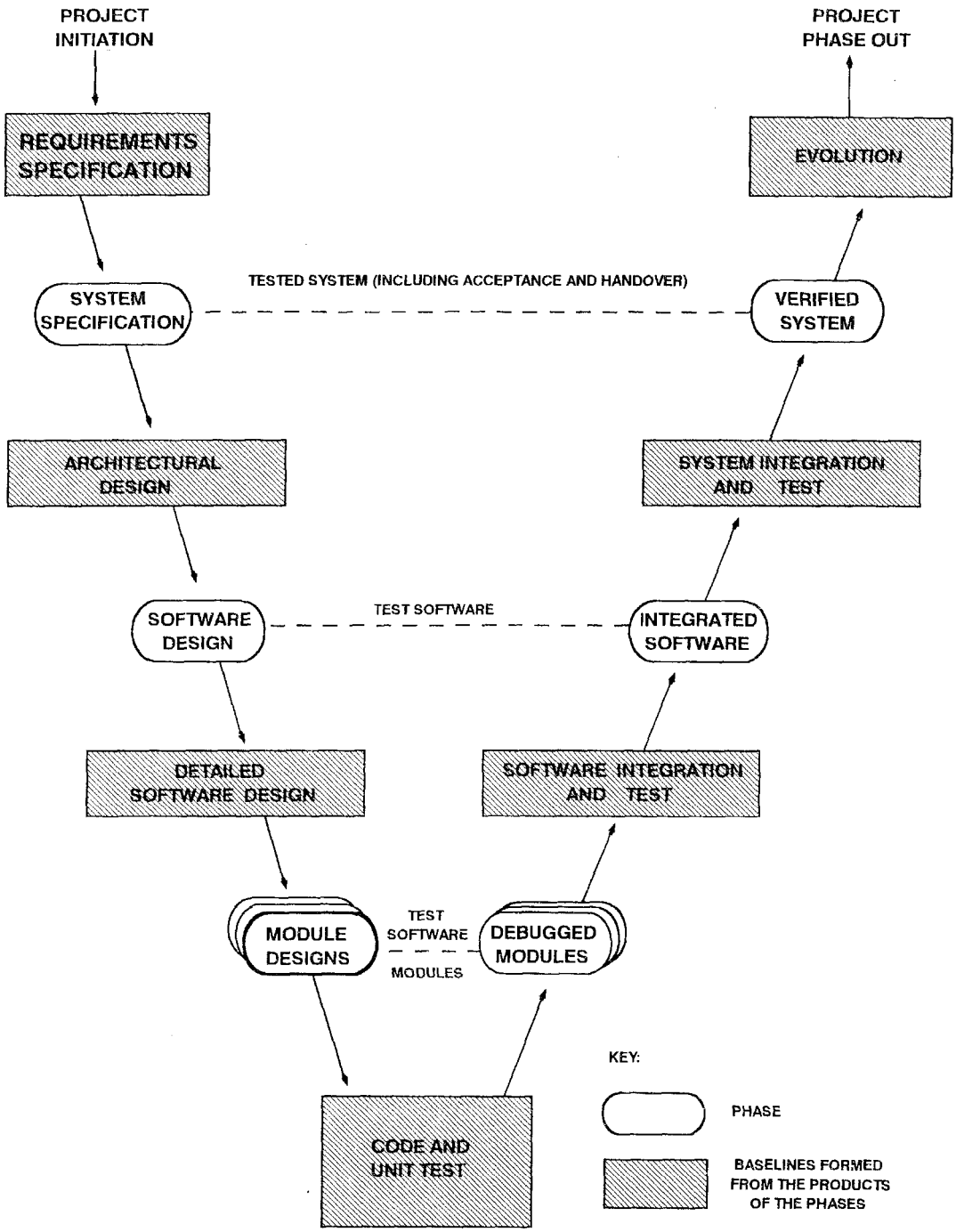

FIG. 4—THE SOFTWARE LIFE CYCLE

Option 2

Although a cheaper option, savings could be negated by the resulting design, drawing and document changes and the through life support of non-standard systems. It should be noted that near to the proposed site for the reference facility, is the Royal Navy's Marine Engineering Training School. Sited there are the MCAS training simulators, ergonomically identical to ship fitted systems. Proposed physical changes to MCAS MMI could be investigated on these

simulators, thus reducing the pain of not having ergonomically similar equipment available at the reference facility.

Option 3

As with option 1, racks for up to seven systems would be required and again the system would be expensive without sufficient flexibility.

Options 4 and 5

A combination of these two options, coupled with static and computer driven test interfaces and a plasma screen MMI similar to the ship fit, were eventually selected as a basis for further detailed design.

At this stage it became necessary to accurately define suitable facilities for a reference system by reviewing the:

- Requirements for each system.
- Likelihood of changes.
- Urgency for these changes.
- Possible risks from errors to those changes.

The result of this review, for the seven systems, is summarized in Table II

TABLE II—*Likelihood/Risk Analysis of Changes to D86 Systems*

	Likelihood of changes	**Urgency of Changes**	**Risk from Faulty Changes**
SRMH SPCS	High	Medium	High
SRMH MCAS	Low	Low	Medium
T2400	Medium	Low	Low
T23 CWLCP	Medium	Low	Medium
T23 DGLCP	Medium	Low	Medium
T23 MEPS	Medium	Low	High
T23 MCAS	High	High	High

It can be seen from Table II that the T23 MCAS and SRMH SPCS systems deserve greater attention than the T2400 and SRMH MCAS systems. It follows from this that the base configuration would provide a collection of racks dedicated to particular system elements where, major or ship critical software changes might be envisaged. A further set of re-configurable racks i.e. racks re-configured using common items, would be provided to accommodate 'less critical' systems such as the SRMH MCAS.

Whilst the SDS proved very useful in confirming the basic reference facility philosophy, it revealed that the time spent re-configuring racks and test cards and then proving them to function correctly could be considerable. Similarly by using the SDS, it was confirmed that static test equipment was suitable for most testing. However, for complex testing i.e. engine changeover sequences, a more dynamic approach is required.

The setting up time can be reduced by:

- Minimizing the number of re-configurations required to generate the most common hardware test scenarios.
- Providing the operator with checklists detailing tests to be carried out to prove the re-configuration.

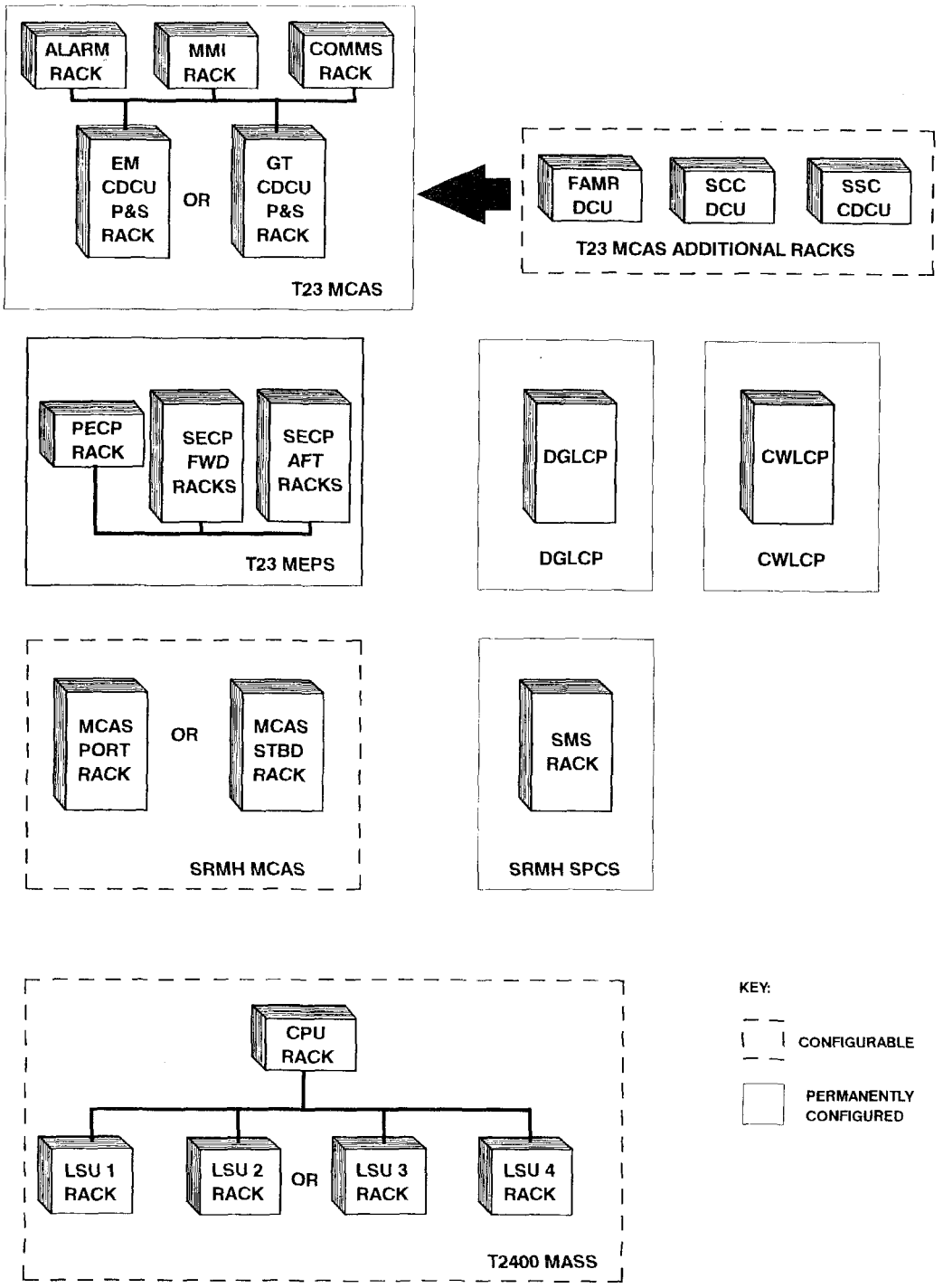

FIG. 5—D86 REFERENCE FACILITY HARDWARE—SELECTED SYSTEM
CDCU—CONTROL & DATA COLLECTION UNIT
DCU —DATA COLLECTION UNIT
LSU —LOCAL SCANNER UNIT

The more complex aspects of the testing are best achieved by the incorporation of a specific computer simulation of the dynamic aspects of the systems under test.

Finally, further cost savings would be made as options 4 and 5 would readily utilize hardware and test equipment originally used in the design proving stage

for ship fitted equipment and would make use of production items i.e. printed electronic circuits and racks identical to that installed on board.

(FIG. 5) shows the layout of the reference systems selected for detailed system definition. Further configurable racks have been added to the MCAS system to enable a complete system to be configured and tested if required. DGLCP and CWLCP are production standard panels identical to those fitted on board ship.

System Design

The reference facility will be set-up in a secure, air-conditioned environment at VTC's factory at Portsmouth. Definitions of each section of the whole facility follows.

Type 23 Reference Facility

This facility was considered to be the most important, requiring the fastest response time to reported faults and their correction. The experience gained from using the SDS suggested that the propulsion machinery control sub-system required special attention. Therefore the allocation of permanently configured racks is highest within the T23 section of the overall reference facility. The permanently configured D86 racks allow for the testing of the propulsion machinery change-over sequences.

To assist with the dynamic nature of the change-overs from electric to combined electric motor and gas turbine drive, a real time computer simulation of the signals generated during the sequence has been created. A full simulation of the ship's plant was not deemed necessary. The simulation simply provides the control signals in the correct order and time interval. The simulation also allows the facility operator to break into a change-over sequence and inject fault conditions e.g. the gas turbine fails to start when requested. In this way the defensive qualities of the software can be tested.

There are 18 serial data links on the full MCAS system for certain scenarios, such as recovery from a total electrical power failure and the loading on the serial links can become quite high. This is because the individual CDCU's need to unload their current status to the central control unit. Obviously this is a critical time for the software and is an area that needs to be very carefully tested. As with the SDS, the Bulk Loader will be used to apply varying loads to the serial data links.

The MEPS reference facility will contain a half ship set of permanently configured racks, with the option of creating a full ship set by using the reconfigurable racks. As stated previously the CWLCP and DGLCP will be full production standard units connected to dedicated test boxes. This method being chosen as it made maximum use of existing test equipment.

SRMH Reference Facility

The MCAS system will only be available via two re-configurable racks. The actual system is considered unlikely to change and has proved very reliable since it was installed.

The SPCS is different to the other systems being catered for by the reference facility. It provides the vessel with fully automatic modes of propulsion control by replacing the operator's manual inputs with computer generated values. The following modes of control are provided:

(*a*) Straight line track-keeping between designated waypoints.

(*b*) Hovering at a designated point over the sea bed.

(*c*) Autopilot.

(*d*) Ship manoeuvring via a joystick.

The control algorithms require data from various navigational aids, both directly and via the 1553B weapons system data bus, to automatically determine the demands to be output to the thrusters. A single permanently configured rack will be linked to a computer containing a simulation of the ship's hull and thrusters, the environment and the weapons system data bus. The computer simulation will be an updated version of the simulation used during the initial development and testing of the SPCS.

T2400 Reference Facility

As with the SRMH MCAS system, this section of the reference facility will only be available by utilizing the reconfigurable racks.

Future Enhancements

The following enhancements to the reference facility are already under consideration. However any attempts to increase the complexity of the reference facility must be balanced against the increased costs of supporting the support equipment.

(*a*) Computer MMI

The D86 I/O test cards could be replaced by a computer generated interface. A graphics representation of the real console layout would improve the operator's MMI and provide users familiar with the real equipment, but not the reference facility, with a means of communicating queries/faults to the facility operator.

(*b*) Video Link

The design authority is currently testing a photo video link, whereby images from the ship can be passed back to a shore based establishment and thus provide photographic evidence of faults/queries. This level of information is essential if a rapid response is required and/or the fault is to be replicated on the reference facility.

Summary and Conclusions

The microprocessor and its attendant software is now firmly established as the way ahead for marine control and surveillance. Its arrival however has brought a range of support problems not previously encountered with the more familiar analogue systems. With a digital system, it is essential that a comprehensive configuration control system is operated for the control of design changes to hardware and more importantly to software, including the development environment, compilers, application software and firmware.

The complexities of software also dictate the need for a specialised test environment. As discussed in this article, this can only be satisfactorily achieved by a representative reference facility capable of exhaustive testing of software modifications. It is also essential that the facility can effectively demonstrate the successful modification to the customer, to give the confidence required before commencing a shipborne trial.

The need may exist in the future for the design authority to fund a small hardware/software team to utilize the reference facility and to provide a rapid service to system enhancements or problem solving. Maintaining continuity of expertise, in both system soft and hardware, is vital to the provision of effective and timely support even when a system is well documented.

There is still much to be achieved before the through life support reference facility becomes fully operational. It will bring with it the confidence that D86 soft and hardware modifications have been fully tested and proved prior to issue; thus reducing testing and trials in operational and ship down time, to identify hardware defects and software shortcomings.