CONTROL SYSTEMS IN THE COMMERCIAL SECTOR

BY

ALAN BLIGHT, BSC (HONS), IENG
(*GE* FANUC AUTOMATION)

ABSTRACT

This article aims to aid naval engineers in their appraisal of commercially available systems. It is intended to give the reader an overview of the concepts and terminology found in contemporary industrial control solutions; to explore some of the configurations currently used in safety critical applications, and to outline some possible future trends in the commercial sector. Commercial standards for safety classification of control systems are also briefly discussed. A glossary is included at the end of the article.

Introduction

The last few years have seen an increasing pressure to purchase commercial off the shelf solutions to a variety of applications within the Navy. This is mainly driven by the need to reduce initial project procurement costs. There is also a recognition that the past has seen some expensive mistakes when the RN has opted out of the mainstream of customer-led technology and been left with an obsolete and difficult to support system on a relatively young platform.

The next generation of warships will probably use commercially available control systems for the marine engineering plant. Some of the potential advantages are:

- Use of widely accepted standards means greater choice of competitive manufacturers and ready availability of spares and upgrades.
- Procurement costs are less—R&D costs are spread over a larger customer base, and production runs are longer.
- Less risk—the system has already been independently proven.

Outside the marine engineering plant, automation gives the opportunity to reduce manning levels and improve reliability. Whilst the RN will probably not be subjected to the relentless drive seen in the commercial sector, the potential for savings in this area cannot be ignored.

The PLC—Mainstay of industrial control

The modern electronic control system can trace its ancestry back to the hard-wired relay racks of the 1950s. These systems were able to implement simple sequential logic but were difficult to install and maintain. Advances in solid state circuitry and computing techniques led to the introduction of the first Programmable Logic Controllers (PLCs) in the late 1960s, which were effectively just miniaturised versions of the relay racks. A PLC is a computer which runs the same sequential program continuously, monitoring the status of its input devices (sensors) and setting the state of its output devices (actuators and indicators) in accordance with the users logic program.

The first PLCs tended to be used primarily for rapid logical and sequencing operations, and were therefore ideally suited to the repetition found in mass production manufacturing. The variations found in continuous process control were better suited to analogue applications, and the scale of integration required on a large process site led to the development of Distributed Control Systems (DCS). These consisted of a number of separate control nodes, usually operating autonomously but perhaps sharing some data via a SCADA (Supervisory Control and Data Acquisition) interface.

The separate roots of DCS and PLC based systems resulted in two streams (manufacturing and process control) of control application which have only recently become integrated. The progress of the PLC has been driven by the demands of industry—in particular the number of Inputs and Outputs (I/O) required, and the size and complexity of the program and the technological advances made with the Personal Computer (PC). The mid 1970s saw the introduction of PLC functions such as PID controllers, as TTL was replaced with microprocessor technology, but this generation of PLC still lacked the processing power required to deal with large numbers of I/Os and complex continuous calculation. As processing power increased, there was a gradual merging of the two technologies of PLC and DCS, and the later additions of communications, motion control and floating point calculations have now made the modern PLC compatible with continuous process control. The term Process Control System (PCS) is sometimes used to describe a PLC based process controller.

Early PLCs were programmed using conventions similar to those used for representing relay diagrams, since this was a format familiar to contemporary electrical engineers. The programming language was called relay ladder logic—a term that still survives today, although the scope of modern programmes is far more complex than the simple logic of the original version. Initially, PLCs were programmed using a dedicated programmer, but now it is more common to write the program and configure the PLC using a Laptop PC (running a Windows or DOS based programming package), connected to

the PLC via its serial port. Ladder logic remains the predominant language, although packages are available using other methods, including Instruction Lists; C++ and Sequential Function Chart (SFC). It is worth pointing out that the Ladder Logic language is not a universal convention—although the general format is fairly consistent, each manufacturer has its own minor variations to suit the features available on its products.

On a large site, customer demands to reduce commissioning overheads, and advances in reliable communications, prompted the development of Distributed I/O where the aim was to reduce field wiring by installing remote stations for the connection of plant sensors and actuators. These could be fed back to the PLC on a suitable communications network (Fieldbus). Developments in computing and communications have allowed part of the control function to be integrated with the Distributed I/O, with some components of the plant running semi-autonomously with only limited communication with the main PLC. Modern systems are able to carry out diagnostic tasks in addition to data processing, and will automatically:

- Check the field wiring for sensor/actuator faults
- Monitor the integrity of the fieldbus
- Warn of overload and other potentially hazardous conditions.

Distributed I/O has allowed other developments, and although the PLC still remains a mainstay of industrial control, the 1990s have seen an alternative emerging in the form of PC based control systems (known as 'Soft PLC' or 'PC Control'). Here the functions of the PLC are implemented in PC software, and dedicated I/O stations are used to interface the PC with the plant. Although mini-computers were also available in the late 1960s, they failed to gain an effective market in industry. This may be partly attributed to the dominance of the electro-mechanical relay as the main control device of the time, but was probably also influenced by the image of computing as being an intellectual and expensive domain more suited to the university than the factory. Despite using the same basic technology, the PLC gained acceptance because of:

- Its simpler operating system (no peripherals to support)
- Familiar symbol based programming language
- Dedicated (I/O) interface—a customized interface designed to allow it to receive information from external sensors, and to output information to actuators and indicators.

However, PC control is now becoming more popular, as the demand for networked control systems grows, and technology allows real-time applications to run in a PC.

Another major area of advance has been the interface between the operator and the plant. Initially the only controls and indications available to the operator were lamps, dials, annunciators and switches, but the graphics abilities of modern computers have allowed the development of some sophisticated visual packages for representing the plant to the operator. Historically, the role of Supervisory Control and Data Acquisition (SCADA) was seen as separate from the actual control hardware, with various specialist manufacturers offering individual SCADA packages. The availability of modern PC networking tools have allowed much closer union between the SCADA and the shop floor, and the HMI (Human/Machine Interface) is now an integral part of the control solution.

ARCHITECTURE OF A MODERN PLC BASED CONTROL SYSTEM

A typical modern system consists of a PLC connected to localized field control stations by a fieldbus. The information held by the PLC is presented to the operator at one or more HMI stations, connected to the PLC by a high-level communications network (FIG.1).

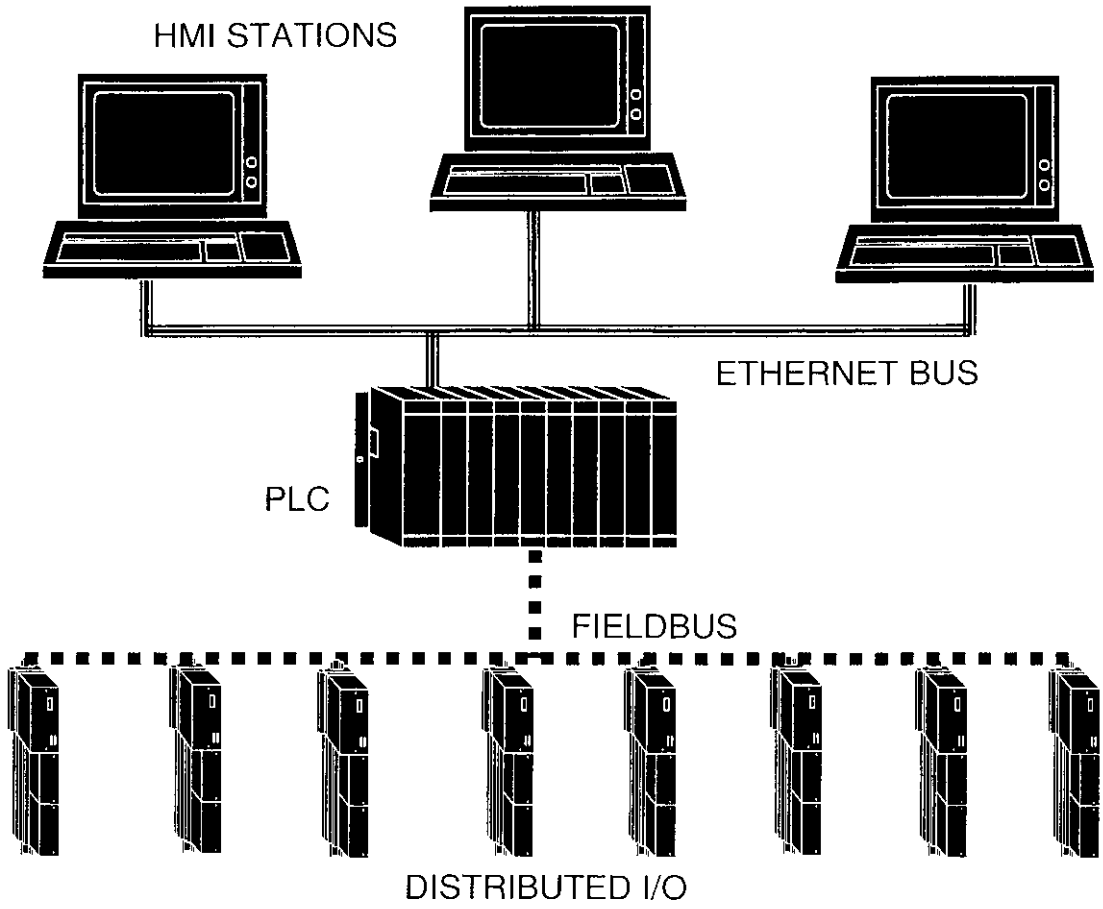

FIG.1 - ARCHITECTURE OF A TYPICAL MODERN PLC BASED CONTROL SYSTEM

The HMI

In most modern systems, the operator communicates with the plant via a visual display. This may be a custom designed Display Station (basically a unit incorporating a screen and industrial PC, usually in a splashproof case to withstand the harsh environment of the factory floor) or a remotely sited office PC and monitor. A large plant will have several HMI stations, each with different levels of access for control and monitoring. The HMI station will probably be running a proprietary software package to display the information; traditionally this SCADA software was a specialist product, but modern systems almost all use a common Microsoft Windows platform. This open standard has led to fierce competition, and the price of SCADA packages has plummeted in recent years, whilst the ability to integrate the manufacturing or process system into a corporate IT network has led to the development of a host of tools for importing and exporting data. A major advantage here is the ability to readily manipulate production data and produce trends and statistical analysis tools for management and Quality Assurance.

Modern HMI systems are far more than just displays, they can incorporate:

- Pagers to alert mobile staff of any alarms
- Drivers to data logging devices
- Wireless communications links to enable supervisors to view the current state of the plant from anywhere on the factory floor via a palmtop computer.

Proprietary software packages such as PC-Anywhere allow remote access to PCs, and it is possible for engineers to view the state of the plant, diagnose faults, and reprogram from almost anywhere in the world. Of course, as remote monitoring and control becomes available, it is necessary to ensure that appropriate precautions are in place to prevent unauthorised access, and again there is a range of proprietary security products available to achieve this.

With any SCADA package there is inevitably a trade-off. A monitor screen is of limited size and can only represent a limited amount of information, so it is important when designing the screen to use a layered architecture in order to filter out irrelevant material and to present important data clearly. The ability of the programmer to understand the needs of the operator is crucial in ensuring safe and effective operation of the plant, and the importance of carefully considered screen design cannot be overstressed.

The HMI / PLC communications bus

The choice here is usually between a continuation of the fieldbus system, or a dedicated bus for the HMI. Since the HMI is usually away from the hostile environment of the factory floor, it is possible to use similar networks to those found in most offices, and many large factory based systems will use Ethernet communications between the various HMI stations and the PLC. For most sites, a simple cable LAN is used, but more exotic communications systems such as fibre optics or microwave links allow the HMI to be remotely situated from the plant, so that a single control station may be responsible for several sites.

The PLC

The modern PLC is a highly sophisticated and compact computer, ruggedized to suit the industrial environment, and with its processing activity tailored to the individual application. Most PLCs have a modular design, consisting of a baseplate (or backplane), on which are mounted modules for:

- Power Supply
- Central Processing Unit
- Inputs
- Outputs
- Specialist functions.

The heart of the PLC is a Central Processing Unit (CPU) similar to that found in a desktop PC, which processes the data received from the plant. Each execution of the program is called a scan, and the program typically scans about 20 times per second. The actual scan time depends upon a number of factors, principally the:

- Amount of I/O
- Size of the user program
- Communications overhead required.

There are minor differences in the way PLCs from different manufacturers manage their scans, but broadly each scan consists of the following steps (in order of execution):

- Carry out pre-scan checks and calculations (such as resetting timers)
- Examine inputs from sensors and update input tables
- Perform program logic based on new input status and calculate new outputs
- Update Outputs to actuators or indicators
- Communicate with external devices
- Carry out diagnostic routines.

The PLCs themselves range from Micro models with less than 15 I/O, to models with CPUs supporting up to 20000 I/O with 32 bit processing and 6MB of user memory. Even the low-end Micro products are more than capable of controlling an item of plant such as an ACP or HPAC, and most have the ability to communicate with other devices. The range of I/O devices, which can be handled by the PLC, is constantly growing, as PLC manufacturers update their products to interface with the latest field devices.

The program resides within the PLC Central Processing Unit, typically stored in battery backed RAM or EEPROM. Although unlikely to be an issue for RN applications, commercial users frequently want to modify the PLC program without halting production, so on-line programming is a common feature. Once the program has been inserted into the PLC, multi-level password protection is used to limit access to various parts of the program and data registers.

In critical applications, where a failure of the PLC (FIG.2) could have disastrous consequences, various techniques are available to improve the integrity of the system, and these will be discussed later.

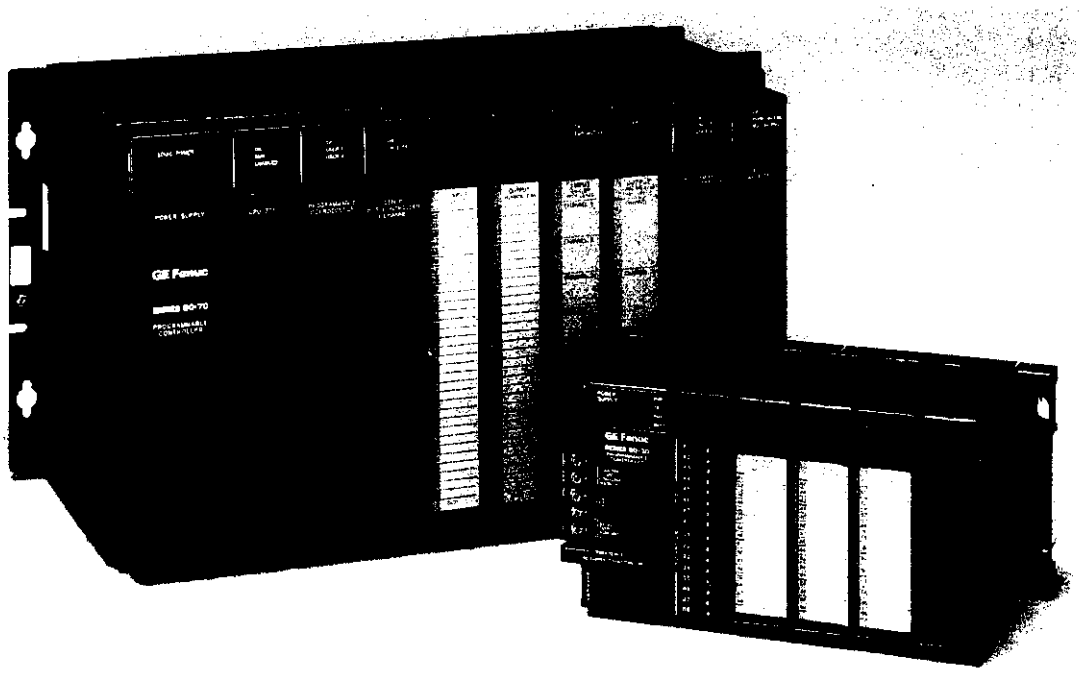

FIG.2 - TYPICAL MODULAR HIGH AND MID-RANGE PLCS

The fieldbus

At the time of writing, the choice of a fieldbus communications protocol remains one of the most hotly debated issues in specifying control applications. More than 20 years ago, the first moves were made to find a successor to the 4-20mA analogue signal lines then used in industrial control. From the start, however, there was division between the various controls manufacturers, and each major PLC manufacturer has developed its own proprietary protocol for communicating with their field devices. There are currently more than 50 fieldbus protocols to choose from. Unfortunately, each protocol has different strengths and weaknesses, so one, which is particularly well suited for use in electrically noisy environments, may not be the best choice if high-speed data transmission is the major requirement. Commercially, PLC manufacturers have a vested interest in protecting their fieldbuses since it ties end users to their hardware products, but customers have long been demanding a more open protocol which will give them a choice of hardware from different manufacturers. Not surprisingly, the member nations of the International Electrotechnical Commission were unable to agree a common standard and the game remains open with front runners including ProfiBus (derived from a Siemens proprietary protocol and strongly favoured by German influenced parts of Europe); Foundation Fieldbus (the USA's answer); and DeviceNet.

The situation is changing rapidly, and any information given here will be obsolete by the time of publication. However, there is little doubt that customers will demand a common fieldbus, and may well tend towards using Ethernet if the industry is unable to agree an open standard. Already there are some applications using Ethernet as a fieldbus, but for larger applications the relatively high power consumption of a large bus remains a barrier. Another argument against Ethernet in safety critical applications is that it is not really deterministic, but at very high data transfer rates (Gigabit Ethernet is available for those with deep pockets) this becomes less significant. The cost of the bus and interface cards is low, data integrity is good, and the popularity of Ethernet for high-level communications means that it is accepted and well understood. There is a strong possibility that as PC control becomes more popular, Ethernet will become more common on the factory floor for the I/O interface.

Incidentally, there is already an open communications standard specified for Marine applications—the Marine Information Technology Standard (MITS), used primarily on integrated control packages for commercial shipping, which has been agreed by a number of (mainly Scandinavian) manufacturers.

Physically, the construction of the fieldbus depends primarily on distance and data flow rates. At the low end (up to several thousand feet with a limited bandwidth), shielded twisted pair cabling may be sufficient, whereas a large fieldbus may use fibre-optic lines linked by microwave to different sites. Major considerations for any fieldbus used in the RN will be:

- Strong noise immunity
- High data integrity
- Ease of repair.

The I/O

The PLC interfaces with the plant by I/O modules (which may be mounted within the PLC rack, or situated remotely), and there is a huge range of PLC based I/O products available. Input modules start with basic discrete and analogue inputs ranging up to specialist modules for thermocouples or high-speed counters. Output modules include relay drivers, discrete and analogue

signals, and motion control products (e.g. servo amps) to drive motors and actuators. As I/O densities have increased, the physical size constraints of the PLC rack have led to versions where the field wiring terminal strip is connected to the I/O module by a flying lead with a high density plug and socket interface with the actual module. Even in versions where the field wiring is connected directly to the module, a detachable terminal block allows the I/O modules to be changed without disturbing the wiring.

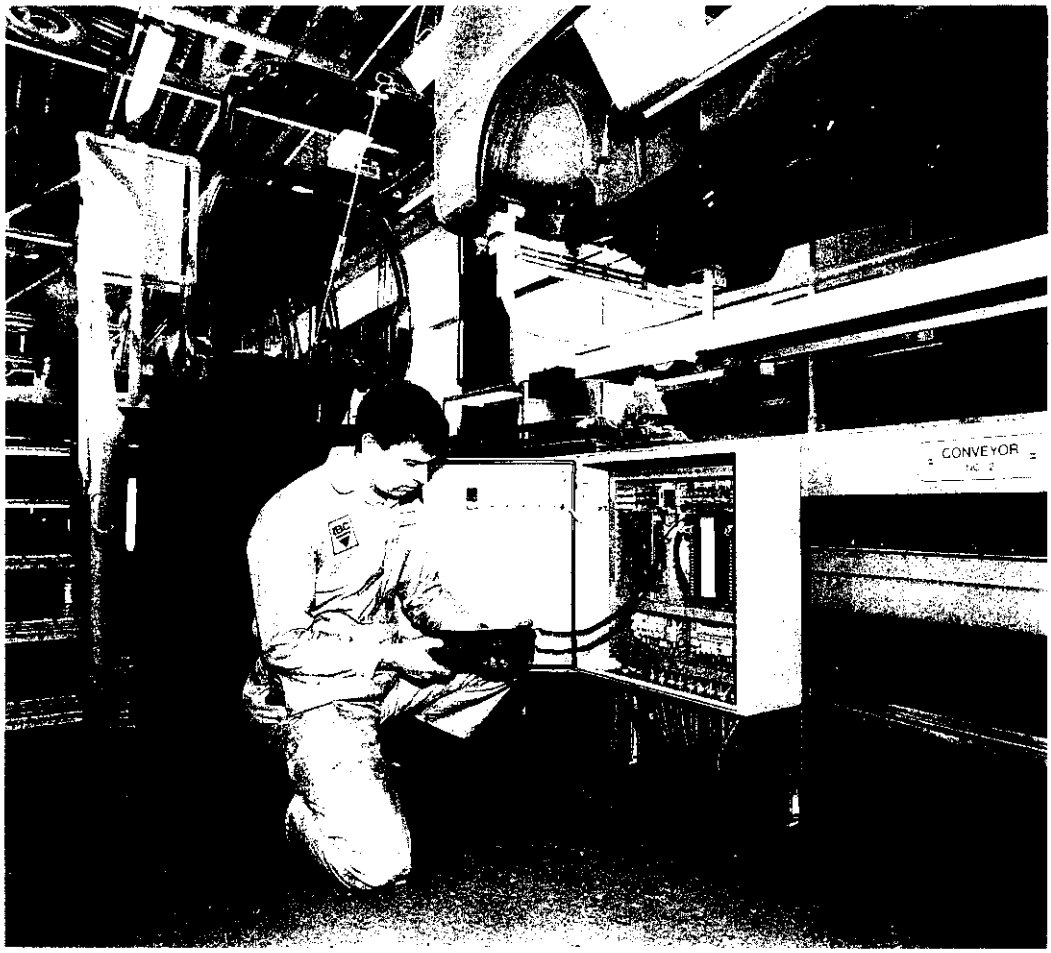

FIG.3 - FAULT FINDING AT A DISTRIBUTED I/O STATION USING A HAND-HELD PROGRAMMER

Distributed I/O stations (FIG.3) will include a communications interface with the fieldbus, and a number of I/O modules appropriate to the local application. Modern installations may use Intelligent I/O, where in addition to the I/O there can be some local processing and diagnostics to minimize the work carried out by the main PLC. Typical options include;

- Warnings for no-load or analogue values out of range
- Pulse testing to prove output circuit integrity before energisation
- Tri-state input levels to prove input circuit integrity
- Conversion of analogue values to engineering units
- Adjustable filters to customize input response to the ambient electrical environment.

If required, the actual state of the outputs can be fed back to the PLC as inputs to provide a confirmation of the state of the plant. Local electronic circuit protection can shut down a circuit within 5 microseconds of detecting a fault condition, providing far more effective protection than thermal fuses.

In any commercial system, production time must be maximized, so it is usual to have the facility to 'force' the state of I/O to overcome defective field devices. 'Hot insertion' (i.e. replacement with the PLC running) allows minimum disruption to the rest of the plant.

Strategies for dealing with safety critical systems.

Historically, the process industry has used different technology for control and safety systems. The safety systems were generally simple discrete logical functions, implemented using relays, and the process control system performed more complex tasks. The trend for integrated control solutions has merged these functions and led to the development of control strategies (notably in the oil and gas industry). These would survive a major incident and allow safe control of the plant to continue, at least for the duration of an Emergency Shut Down (ESD). Similarly, any application in the RN will need to consider a strategy for survivability in the event of catastrophic equipment failure or battle damage.

One common method of improving the reliability and integrity of a system (assuming good design and good quality processes have been used) is to employ multiple components to operate in a standby mode or to carry out a comparison vote. Although component redundancy increases the maintenance workload, and also the chance of failure occurring (more components to fail), the improvement in system reliability is illustrated below:

For a single system (voting 1oo1),

$$MTBF1oo1 = 1/(\text{sum of component MTBF's})$$

For a duplex system (voting 2oo2)

$$MTBF2oo2 = (MTBF1oo1)^2 / (2MTTR)$$

(assuming MTBF>>MTTR)

For a triplex system (voting 2oo3)

$$MTBF2oo3 = (MTBF1oo1)^3 / (3MTTR)^2$$

(assuming MTBF>>MTTR)

Note that the Mean Time to Repair (MTTR) starts when the failure occurs, not when it is detected. Redundant components can mask the occurrence of a fault, so diagnostic capability is an important factor in any control system. The MTTR is also critically dependent on the availability of a replacement component in the event of repair being impossible. For a warship on deployment, stores holdings play an important part in defining the availability of a system.

As an example of how multiple components can be used, some of the main safety critical configurations available from a particular manufacturer (GE Fanuc) are discussed below:

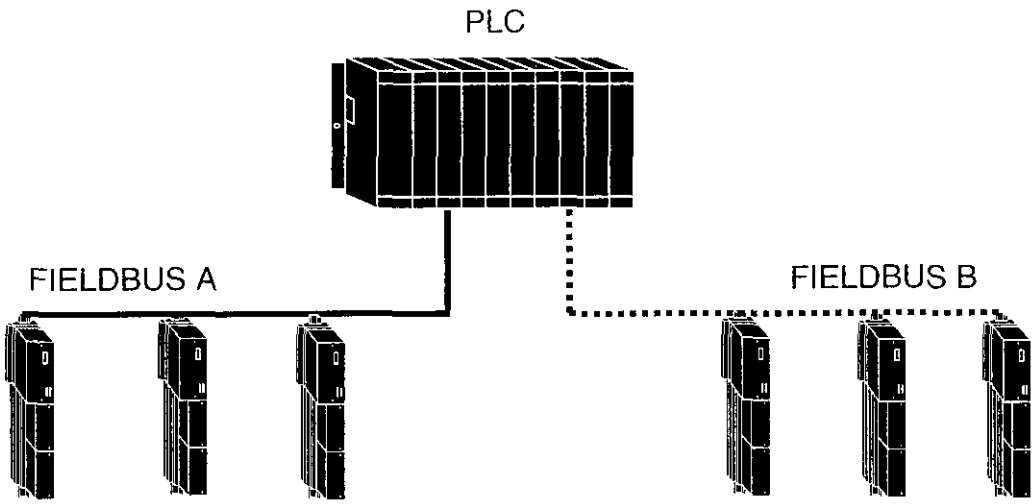

FIG.4 - FIELDBUS REDUNDANCY. SINGLE PLC WITH INDEPENDENT BUSES

Fieldbus redundancy

Because of its size the fieldbus is probably the most vulnerable component of the control system, so a first step in increasing system integrity is to have more than one fieldbus, preferably using a different route. There are two basic options available; the first is to have some field devices connected to one fieldbus, with the remaining ones connected to an independent bus (FIG.4).

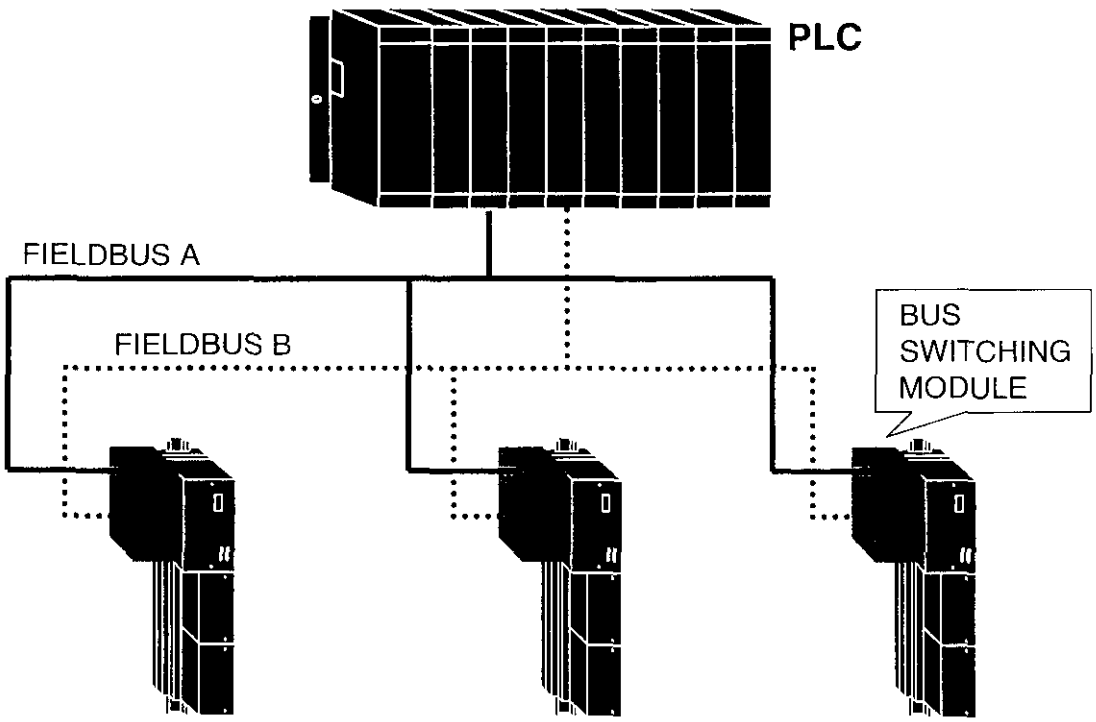

FIG.5 - FIELDBUS REDUNDANCY. SINGLE PLC WITH DUAL BUSES

The second option is to have two busses in parallel, connected to each device via a switching mechanism (FIG.5). The problem here is ensuring that all devices are talking on the same bus, and that all devices switch over to the same redundant bus in the event of damage or communications failure. Considerations include:

- Setting the initial configuration on power-up
- Defining the criteria for a communications failure (e.g. how long to wait before switching busses)
- Whether to switch back when the failed bus is restored.

Strategies for added integrity can be included in the fieldbus protocol—for example GE Fanuc's GENIUS bus transmits each packet of data three times, which is then subjected to a 2 out of 3 vote at the receiving station.

PLC redundancy

At the heart of the system, failure of the PLC can have catastrophic implications. Considerations to improve integrity here include the provision of multiple power supplies to the PLC, and installing a second PLC to take over in the event of failure of the primary controller—preferably in a different location. Internal diagnostics can also improve integrity at the PLC. Memory errors can be detected by parity or checksum tests (which can be compared by voting against the other PLCs running the same program), whilst internal bus faults can be detected by transmitting the data more than once and comparing the result.

The problem with multiple PLCs is that although they may both be running the same program, there is no guarantee that they will both be at the same point in the program at the moment of failure. This can lead to a 'bump' in the state of the I/O when the changeover occurs. This may not be a problem if the aim is to improve integrity of the I/O (because the voting system at the field device will decide whether to switch the I/O). It could be a problem if the aim was to improve the integrity at the CPU without a corresponding redundancy in the field. For a 'bumpless' changeover, it is necessary to synchronize the PLCs to ensure that they both contain the same internal data, and that they are both executing the same step of the program. This generally requires a dedicated communications link between the PLCs specifically for maintaining synchronization. In the event of a PLC failing to rendezvous at a synchronization point, the standby PLC will assume that a failure has occurred and take control.

If multiple PLCs are to be used in conjunction with multiple fieldbuses, a further consideration is whether to dedicate each PLC to a separate bus, or to have all busses connected to all PLCs. The latter gives higher integrity but requires more hardware, as multiple bus controllers are required in each PLC (FIG.6).

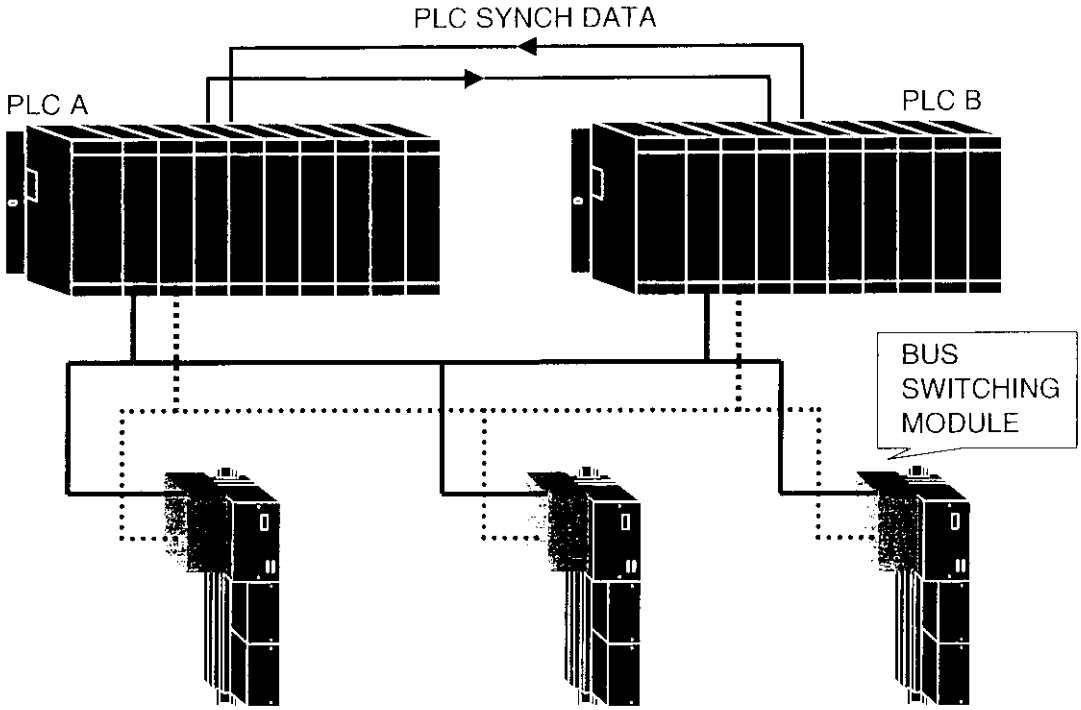

FIG.6 - PLC AND FIELDBUS REDUNDANCY. DUAL SYNCHRONIZED PLC WITH DUAL BUSES

I/O redundancy

The principles of integrity should continue right down to the plant, since applying several I/O channels to one field device increases complexity and maintenance overhead without eliminating the single point of failure. Connecting each bus to a different sensor can increase the benefits of using multiple fieldbuses. Even for a single fieldbus there may be a requirement to use redundant or co-located sensors if there is a high likelihood of failure, or a need for verification before any corrective action is taken (e.g. a sprinkler system). Although diagnostics may be able to detect a faulty sensor, it is possible that a failed sensor could give a feasible (but wrong) output. In this case, some kind of voting mechanism is required at the PLC, and a strategy for dealing with indeterminate results. (For example, if there are 3 sensors, a 2-out-of-3 logic could be used, but if there are only two sensors, we need to decide what default actions we want to take when they do not agree). As an example of how this works, consider three configurations for input sensors:

Simplex

The PLC receives the information from 1 sensor, connected to one field station. Loss of that input is interpreted as a need to bring the system to a safe state.

Duplex

The PLC receives data from two sensors connected to two separate field stations. The inputs are normally energized, and are voted 2oo2 in the PLC so that a change in state of either input is interpreted as a need to bring the system to a safe state.

Triplex

The PLC receives data from three sensors connected to three separate field stations (FIG.7). The inputs are voted 2oo3 in the PLC; loss of any two inputs is interpreted as a request to bring the system to a safe state.

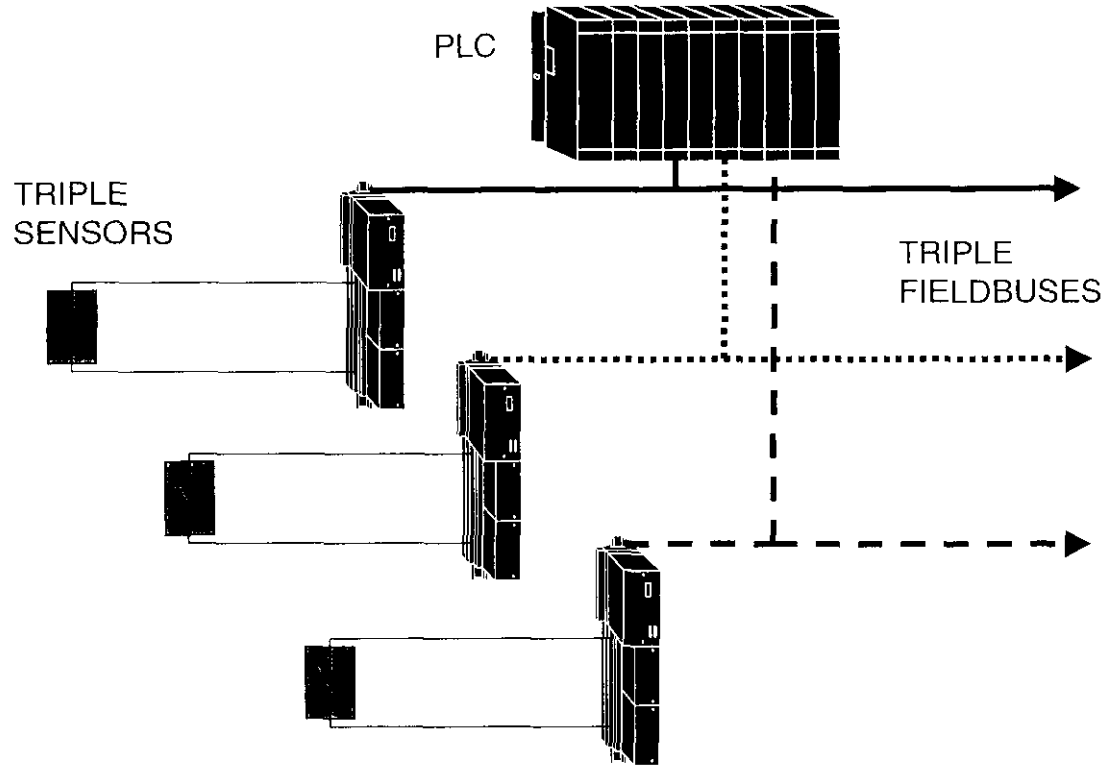

FIG.7 - I/O REDUNDANCY. TRIPLE INPUT CONFIGURATION

The situation is slightly more complicated for analogue signals; one way to improve integrity is to calculate average values for common parameter sensors, and reject a reading if it differs from the average by more than a selected percentage.

When driving an actuator similar considerations apply. A typical strategy is to implement voting by means of the 4-path 'H Configuration' (FIG.8). This consists of two output switches connected in parallel on the source side of the load (i.e. connected to the +ve side of the power supply) and two more connected in parallel on the sink side (i.e. connected to the -ve side of the power supply). The power supplies are derived locally. The major difference between the output subsystem and the input subsystem is that here the voting is done at the field station, rather than at the PLC. Each block receives the output from all PLCs (with each PLC having derived its output command from a separate vote on the inputs). Each of the four blocks then performs a simplex, duplex or triplex vote (depending on the number of PLC commands it is receiving) and outputs its vote to the load. In the event of a temporary or total loss of communication between the field station and a PLC, it is necessary to define a default status of the outputs (i.e. ON, OFF or HOLD LAST STATE) to resolve voting discrepancies. The default is chosen so as to bring the plant to a safe state. This configuration can withstand the loss of a PLC or fieldbus, or a fault in the field block itself, so no single failure will cause loss of control of the load. It also allows users to replace defective field modules with the system on-line, to minimize the knock-on effects of a failure.

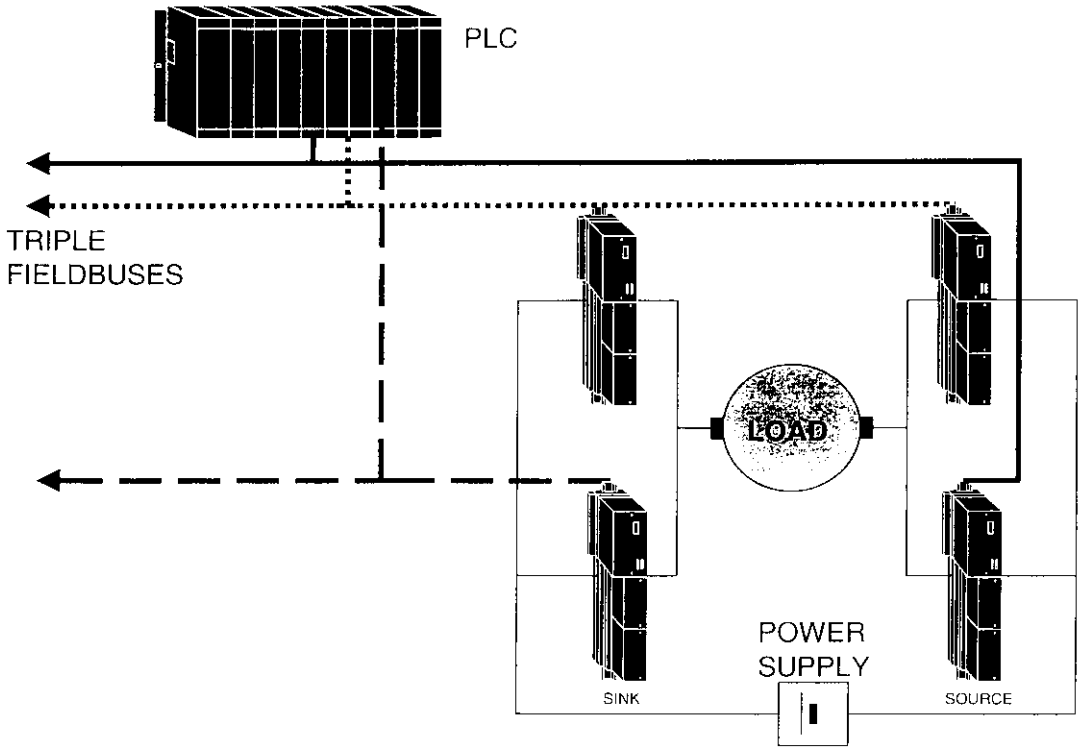

FIG.8 - I/O REDUNDANCY. 4 PATH 'H CONFIGURATION' FOR OUTPUTS

For maximum integrity, all of the above strategies may be implemented in a system (FIG.9). This philosophy is frequently found in Emergency Shut Down systems and is generally known as Triple Modular Redundancy. The best solution requires a truly scaleable system, where the individual redundant elements can be applied independently or as a combination to best match the control and performance criteria specified for a particular plant.

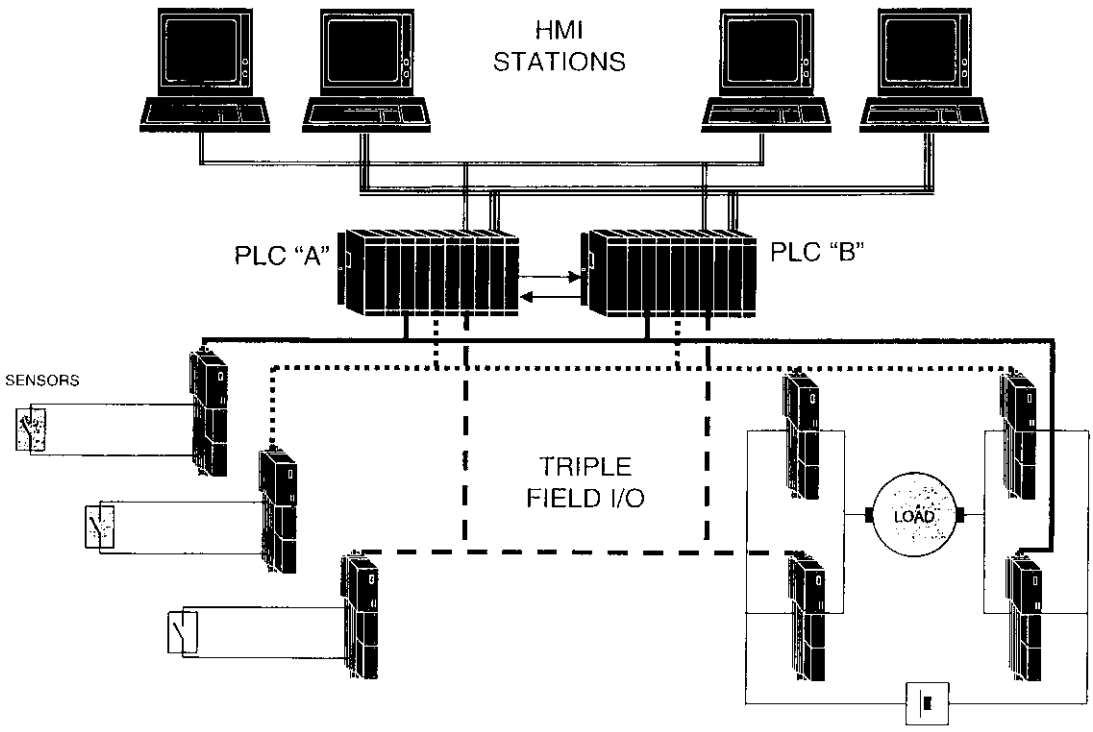

FIG.9 - TYPICAL SYSTEM FOR FULL REDFUNDANCY.
TRIPLE FIELBUS AND I/O; SYNCHRONIZED DUEL REDUNDANT PLC; DUAL ETHERNET AND HMI

The key players

Although some industrial control manufacturers will deliver a turnkey solution to a customer, most do not and the customer must employ a System Integrator to design build, and commission the plant. There is enormous choice here, ranging from one-man specialist engineers (Fred in a shed) to large multi-national corporations. Each integrator tends to build up specialist experience in certain applications, so it is important to choose a company with an appropriate background. The integrator may choose products from a number of different manufacturers for different aspects of the plant, and he will need to liaise with his chosen manufacturer's Applications Engineers to ensure compatibility, and to resolve any difficult technical issues. He may also sub-contract some of the work out to Panel Builders to build the control cabinets and physically wire up the components, and employ specialist programmers to write the software for the application program and HMI. Most engineers prefer to stick with products which they are familiar with, so the customer should be aware of what options are available (or employ an independent consultant to carry out this research) before accepting a heavy financial commitment to a particular solution.

Certification of systems

Commercial control systems in any safety-critical application need to be qualitatively assessed and certified, and one of the aspects that needs to be considered when specifying a commercial system is the comparison between Naval Engineering Standards and commercial classifications. At present there are a number of separately derived commercial standards used to classify the functional performance and integrity of critical control systems. Of these the most common in Europe is assessment and classification by TUV (Technischer Uberwachungs-Verein which loosely translates as Technical Supervisory Group)—an independent German Inspection Agency and Testing Laboratory. TUV tests against the DIN standards and awards certification accordingly.

The International Electrotechnical Commission (IEC) is in the process of formulating an International standard for assessing and classifying the *Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems* known as IEC 61508. Since it is likely that the text of the final document will also be adopted as a new European standard, and the principles behind it are already widely accepted, a short description is given below:

IEC 61508 sets out a generic approach for all safety lifecycle activities for Electrical/Electronic/Programmable Electronic Systems (E/E/PES). In this context the following refers:

Electrical

To systems where the logical functions are performed by electromechanical devices such as relays or motor-driven timers.

Electronic

To logical functions performed by solid state circuits.

Programmable electronic

To logical functions carried out by programmable devices such as PLCs.

The overall strategy is to ensure that any automation process is safe and that failures are detected and their effects managed.

The calculations classify a system in terms of a Safety Integrity Level (SIL). Broadly, the SIL for a low demand system (such as an ESD system that spends most of its time in a standby state) is determined by the probability

that a system will fail to carry out a control action when demanded. The SIL for a high demand system (such as a continuous process control) is determined by the likelihood of a dangerous failure occurring. The levels are as follows:

Safety Integrity Level (SIL)	Probability of 'Failure on Demand' (average range) Low Demand Mode	Probability of 'Dangerous Failure per Hour' High Demand Mode
1	$<10^{-1}$ to $> 10^{-2}$	$<10^{-5}$ to $> 10^{-6}$
2	$<10^{-2}$ to $> 10^{-3}$	$<10^{-6}$ to $> 10^{-7}$
3	$<10^{-3}$ to $> 10^{-4}$	$<10^{-7}$ to $> 10^{-8}$
4	$<10^{-4}$ to $> 10^{-5}$	$<10^{-8}$ to $> 10^{-9}$

IEC 61508 is divided into 7 parts as follows:

Part 1

General Requirements

The concepts of:

- Safety requirements
- Hazard and risk analysis
- Documentation
- Installation
- Commissioning
- Operation
- Maintenance
- Modification/retrofit
- Decommissioning and disposal of systems.

This part provides an overall framework to analyse risks, so that failures in Electrical/Electronic/Programmable Electronic Devices can be prevented or controlled.

Part 2

Specific requirements for Electrical / Electronic / Programmable Electronic Safety-Related Systems to be applied during the specification, design and modification of the hardware.

These include the prevention of random failures by specifying:

- Product quality (e.g. MTBF requirements)
- Management techniques such as preventative and predictive maintenance
- The control of failures by system architecture features such as redundancy and diagnostics.

Part 3

Specific requirements for Software, similar to above in concept.

The process requires the application of fault avoidance (quality assurance) and fault tolerance (software architecture) in both embedded and application software. A top-down, modular design approach is used, with systematic testing as proven modules are integrated into the final package.

Part 4

Definitions and abbreviations.

Part 5

Examples of methods used to calculate Safety Integrity Levels (SILs).

Part 6

Guidelines for the application of Parts 2 and 3.

Part 7

Overview of techniques and measures.

Meeting TUV and SIL standards are most common criteria specified by plant designers, but there are a number of other assessment and certification systems that may be required for specialist applications. Of these, Lloyds Register's Marine Type Approval certification (or its companion approval from the American Bureau of Shipping or DNV in Europe) is most likely to be relevant to RN applications. Other pertinent certification includes:

- CE marking (for conformity to European low voltage and EMC directives) and certification by UL (Underwriters Laboratories)
- FM (Factory Mutual); and CSA (Canadian Standards Association) for global applications.

The Crystal Ball becomes cloudy.....

Commercial systems are designed with a limited lifespan—manufacturers need to sell new products and cannot commit expensive resources to perpetuating obsolete designs. Having said that, every manufacturer has an eye on the past when introducing new products. They need to hang on to their existing customer base, and the best way to do that is to make updating older products as simple as possible—providing you buy from the same manufacturer of course! On the other side of the fence, end users want the latest technology but proven reliability, so there is always a degree of compromise.

Any commercial user making a substantial financial investment in a control system will require some insurance against obsolescence, and the oil and gas industry will frequently expect a guaranteed 10 year spares availability for a major application. Similarly, any system chosen by the RN will need to carry assurances on spares availability and upgradability, but providing the initial choice is wise this should provide a cost-effective and relatively simple way of maintaining platforms through their life.

The RN will need to specify a system, which will be safe, operable, and upgradeable. Commercial systems already exist which will meet these requirements, but they will need to be vetted against the special needs of a warship, and this will need careful work in specifying the design requirement. Experience of these systems within the RN is limited, and it will probably be necessary to buy in specialist advice. It is interesting to note that several traditional controls manufacturers and integrators are consolidating their knowledge base in the application of safety-critical control systems. For example, Vosper Thornycroft now own Brisco (an integrator specializing in the Oil and Gas Industry with particular interest in subsea systems) giving them an in-house capability in this field.

As far as future trends in control systems are concerned, this can only be a guess, but as a basis for discussion consider the following possibilities:

- Manufacturers will aim to provide a total system solution. Currently, several larger manufacturers are expanding their range of products by buying up smaller specialist companies.

- Manufacturing and process technologies which are currently disparate will become integrated—for example the design office will be linked to the HMI and control system. The Internet will be a key factor in global integration, and smart software will download its own updates.
- Artificial intelligence will start to appear in larger control systems—for example neural networks will be used in hardware, and software will be able to diagnose faults and repair itself.
- Processing will become more decentralized, with intelligent I/O and field processors.
- The HMI will improve. In the short term displays will be larger and clearer, and in the longer term the HMI will become more intuitive, along the lines of Virtual Reality.
- PC control will become more popular and replace PLC technology for some applications. The current barrier is the perceived unreliability of current operating systems (e.g. 'Illegal Operations' or the 'Blue Screen of Death') and the problems of safety calculations with a system that is not considered deterministic.
- The argument over fieldbus protocols will become irrelevant—possibly a tendency towards Ethernet over the next few years. In the longer term, new technologies will completely revolutionise the whole concept of communications.
- Miniaturization will continue allowing greater processing power and new applications for motion technologies.

Endpiece

Modern industrial control systems are fast, reliable, and relatively inexpensive. They offer the RN a sound alternative to the bespoke systems currently in service, and the option to automate many of the watchkeeping, husbandry, and damage control tasks currently undertaken manually. Research has consistently shown that human operators are expensive, inefficient, and perform badly under stress. Future project designers now have the opportunity to reduce manning levels, improve reliability, and reduce costs by introducing new technology.

Glossary of terms and acronyms

1oo1	One-out-of-One (voting).
2oo2	Two-out-of-Two (voting).
2oo3	Two-out-of-Three (voting).
Address	Location in memory where data is stored. PLCs usually define the type of data held in addresses so the %I0001 would be input data held in Input address 1, and %Q0001 would be output data held in Output address 1. The collection of addresses allocated to specific tasks is known as Tables, so that an Input Table would hold the information from the inputs, and a Fault Table would hold data on the status of various diagnostic tasks.
Analogue	Physical properties represented by a variable signal. In order to be processed in a digital controller, the signal must be digitized. Depending on the resolution, there is some loss of accuracy in this process.

Artificial Intelligence	The use of technology to devise machines which attempt to mimic human intelligence. In particular, such machines can learn to generalize and make inferences to generate new knowledge and predict possible outcomes. Although there are many applications of AI (such as pattern recognition for postcode reading, or search algorithms for critical path analysis) the human traits of curiosity and creativity have so far only been realised in a very limited sense.
Availability	Probability of a system working at a given time to the same functional standards achieved at installation. Specifications usually call for a required availability as a %, where it is calculated as either Uptime/(Uptime+Downtime) or MTTF/MTBF.
Bandwidth	Disregarding the technical definition, the term is also used to describe the amount of data that can be sent per unit time over a given medium. For example, if we equate 1 bit per sec to 1 Hz, then a bandwidth of 1 MHz allows us to send 1 million bits per sec.
Baud	Unit defining rate of data transmission, in bits per second.
Blackboard based system	Intelligent system having an area of working memory (called the blackboard) which is accessible to a number of independent agents (such as sensors; actuators and program modules). The agents can read from or write to the blackboard so that other agents may use their data. But this is their only external interface and they run autonomously in parallel (although with a single sequential processor this is virtual, since the processor must divide it's time between each agent).
Configuration Program	The part of the user's PLC program which is used to configure the module and system parameters. It defines which modules are used to make up the PLC and how those modules are to behave.
CPU	Central Processing Unit—the central processor that interprets user instructions; makes decisions; and executes functions.
Crisp Logic	See Fuzzy Logic.
DCS	Distributed Control System. Traditionally non PLC based, consisting of a number of nodes for continuous process control.
Determinism	The ability to calculate the response time of a system or fieldbus. Generally taken as the worst case scenario from an input change to an output change.
Discrete	I/O that can be represented by 1 bit (e.g. ON or OFF).
E/E/PES	Electrical/Electronic/Programmable Electronic Systems
Embedded software	Software that is part of the system supplied by the vendor, held in ROM and not accessible to the end user. Also known as firmware, or system software.
Energize to Trip	Circuits which are de-energized under normal operation. Note that they may still be fail-safe.
ESD	Emergency Shutdown System, comprised of sensors, logic solvers and control elements, for the purpose of taking the plant to a safe state when pre-determined conditions are violated. Usually Fail-Safe, employing duplex or triplex configurations. May also be known as Safety Instrumented system (SIS) or Safety Shutdown System (SSD).
F&G	Fire and Gas Detection System.
Fail-safe	The capability to assume a predetermined state in the event of a specified malfunction. Generally this means that equipment is normally energized, and a malfunction causes the equipment to de-energize.
Fault Tolerant	Capability of a system to continue to perform its required function in the presence of a limited number of hardware and/or software faults.

Field Devices	Refers to all devices connected to the controller I/O, such as wiring, sensors, actuators and operator interfaces. See I/O.
Fieldbus	Communications network between the controller and remotely situated field devices.
Firmware	See embedded software
Forcing	Instructing the controller to set one or more I/O to a given state, irrespective of the logic program. Frequently used as a temporary measure to overcome (fudge) faults with field devices.
Fuzzy Logic	Crisp (or Hard) logic has only two states. If we apply this to say a temperature alarm on a gearbox bearing, with the alarm set to 110C, then as far as the control system is concerned, everything is fine if the bearing temperature is 109, but we have a major problem if the temperature is 110. This is clearly not a realistic reflection, and fuzzy logic aims to address this by taking a band of temperatures (say 0 to 150 for our application) and splitting it into overlapping sets. In our case we could split the temperature band into 3 sets, say cool; warm and hot. Any given temperature is now classified in terms of the degree of membership of each set; at the low end of the band (say 20) the parameter has a high membership of the set 'cool', a low membership of the set 'warm' and no membership of the set 'hot'. At 75, it has a high membership of the set "warm" and a low membership of the sets 'cool' and 'hot'. As the temperature rises, the membership of the set 'hot' increases, and this allows a progressive response to the developing situation. (By the same token, membership of the set 'cool' could be used to trigger progressive heating of the lub oil). Fuzzy logic can be applied wherever the measured variable is an analogue, so it has particular application for process control.
Hard Logic	See Fuzzy Logic.
HMI	Human Machine Interface. The means by which the control system displays information to, and accepts commands from, its human operators. Typical information includes: • Machine status • Alarms • Messages • Diagnostics.
Hot Standby	Redundancy configuration using 2 CPUs connected to individual or shared I/O structures. One CPU is designated as 'active' and the other is designated 'standby'. Both CPUs receive input data, process the information, and set their outputs. The output device takes it's instructions from the active CPU if it is available, but if it fails the output device will switch to the standby CPU.
HVAC	Heating, Ventilation and Air Conditioning System.
I/O	The interface between the controller and the field devices such as sensors and actuators. Usually incorporates some form of internal isolation to separate the field wiring from the logic circuitry. The term I/O is also frequently used to refer to field devices as a whole.
IEC	International Electrotechnical Commission
IEC61131-3	European based standard for programming languages, setting out a uniform structured approach to program functions. The standard covers 5 languages: • Ladder Logic • SFC • Function Block • Structured Text • Instruction List.
IEC61158	Proposed international fieldbus standard. Currently hotly debated.

IEC61508	Proposed International Standard for functional safety of E/E/PES.
IEEE802.3	The standard that defines Ethernet.
Integrator	Specialist engineer who designs, builds and commissions a control system for a customer.
Intelligent I/O	/O module that provides on-board processing of input values to control output values, bypassing the controller for routine decision making.
ISA	Instrument Society of America (International Society for Measurement and Control).
MES	Manufacturing Execution System - tool allowing optimization of the total manufacturing process (from order to delivery) by delivering information for analysis and control of the plant.
Micro	Small (<approx 30 I/O) cheap PLC with limited features, aimed at the low end of the market (typically to replace timers and relays in a control panel).
MMI	Man Machine Interface. No longer politically correct. See HMI.
MTBF	Mean time between failures (= MTTF+MTTR).
MTTF	Mean time to fail (= MTBF-MTTR).
MTTR	Mean time to repair (= MTBF-MTTF).
Neural Network	A network of interconnected processing units which can be considered to mimic the behaviour of brain cells (neurons) in that they can learn to modify their response to a number of inputs by allocating 'weighting' factors to each one. In this way they can recognize incomplete or corrupted data because the weighted response closely resembles the response learned for known data. The main advantages are their cost, fault tolerance (graceful degradation) and speed. The main disadvantages are that they can give completely unpredictable responses for data outside their range of experience; and that there is no proven method for designing an optimal neural network. However, there is a high potential for their application in processing numerical data such as that obtained from Vibrational Analysis or visual recognition systems
OIU	Operator Interface Unit. May be a display with no control functions or a more complex control panel. See HMI.
OLE	Object Linking & Embedding - Microsoft convention (now called COM - Component Object Model) for 'external' features of objects allowing them to be connected together. Frequently used in PC driven SCADA systems.
OPC	OLE for Process Control - an extension to OLE which treats data as collections of objects which can be shared by applications supporting OLE. Provides a foundation for third party connectivity.
Open	Non proprietary, giving the option to purchase various components from a variety of manufacturers.
P & I D	Piping and Instrumentation Diagram. (Not to be confused with PID - Proportional, Integral and Derivative Control strategy).
PC Control	PC hardware and software based control package. Needs a separate I/O interface. Also known as Soft Logic, or Soft PLC.
PCS	Process Control System - term sometimes used to describe a PLC based process control system. See also DCS.
PFD	Probability of Failure on Demand. The probability that equipment will fail to perform a required action when demanded. Used in calculating SILs, where the term PFDavg is used for the average PFD.

PLC	Programmable Logic Controller - solid state controller with user programmable memory in which the user can store a dedicated set of instructions to implement control and automation functions. Usually a modular design incorporating customised I/O interface and communications facilities.
PLCOpen	Consortium of vendors, users, and institutes promoting the use of IEC1131-3.
Rack	Generic term for the PLC baseplate on which the modules are mounted, usually taken to mean the rack and it's mounted modules.
Redundancy	Use of multiple components to perform the same function.
Rule-based System	Strategy for solving problems by testing data (facts) against a series of rules held in the system's knowledge base. The system is able to use this information in order to make decisions and infer new information. Sometimes known as an Expert System, since a human expert frequently devises the rules (e.g. a Doctor may be employed to devise the strategy for a machine dealing with medical diagnosis).
Safety Life Cycle	Sequence of events involved in the implementation of a SIS from conception to decommissioning.
SCADA	Supervisory Control And Data Acquisition - describes the high level functions of a control system. Usually carried out by the HMI in a modern integrated system, but may be sold as a separate SCADA package.
SFC	Sequential Function Chart - programming convention, alternative to Ladder Logic.
SIL	Safety Integrity Level. Defined in terms of PFD, and frequently used when specifying systems.
SIS	Safety Instrumented System. See ESD.
Smart I/O	See Intelligent I/O
Soft Logic	See PC Control
SSD	Safety Shutdown System. See ESD.
Synchronzsed CPUs	Used to ensure a bumpless transfer between active and standby CPUs. The CPUs rendezvous at designated points in their scan to ensure that each is executing the same part of the program at the same time. Synchronization can involve program and data synchronization
TMR	Triple Modular Redundancy. Safety philosophy frequently used in ESD applications.
Volatile memory	Memory, which will lose the information stored in it in the event of a loss of power. A battery or capacitor may be provided to safeguard the memory.
Watchdog timer	A timer which will stop the PLC if the execution of a scan exceeds the preset time of the watchdog. Typically caused by entering an endless loop in a program.
Windows CE	Chip - based version of windows. The absence of a hard disk gives instant availability and robustness. The real-time version shows promise for industrial control applications, offering the determinism, speed. and ruggedness of a PLC with the familiar operating environment of Windows, and the flexibility and openness of a PC.
Windows NT	Desktop and server package frequently used in control applications to interface the manufacturing environment with the office environment. Control software may use the NT Kernel, or a real time subsystem to isolate the control application from Windows NT.