Fail-Safe Design Criteria for Computer-Based Reactor Protection Systems

by

A B KEATS - UKAEA, Winfrith

SUMMARY

The increasing size and complexity of nuclear power plants is accompanied by an increase in the quantity and complexity of the instrumentation required for their control and protection. This trend provides a strong incentive for using on line computers rather than individual dedicated instruments as the basis of the control and protection systems. In many industrial control and instrumentation applications, on-line computers, using multiplexed sampled data are already well established, but their application to nuclear reactor protection systems requires special measures to satisfy the very high reliability which is demanded in the interests of safety and availability. Some existing codes of practice, relating to segregation of replicated subsystems, continue to be applicable and will exert a strong influence upon the way in which the computer system is configured. Their application leads to division of the computer functions into two distinct parts. The first function is the implementation of trip algorithms, ie the equivalent of the function of the 'trip units' in a conventional instrumentation scheme. The first computer is therefore referred to as the Trip Algorithm Computer (TAC) which may incidentally, also control the multiplexer. The second function is voting, on each group of inputs, of the status (healthy or tripped) yielded by the trip algorithm computers. This function, equivalent to the protection system logic, is performed by the Vote Algorithm Computer (VAC). Whilst the configuration and partitioning of the computer-based protection system tend to be dictated by existing codes of practice, the conceptual disparaties between traditional hardwired reactor-protection systems and those employing computers give rise to a need for some new criteria. An important objective of these criteria is to eliminate, or at least to minimise, the need for a failure-mode-and-effect-analysis (FMEA) of the computer software. This demands some well-defined, but simple constraints upon the way in which data are stored in the computers but the objective is achieved almost entirely by "hardware" properties of the system. The first of these is the systematic use of hardwired test inputs which cause excursions of the trip algorithms into the tripped state in a uniquely ordered but easily recognisable sequence. The second is the use of hardwired "pattern recognition logic" which generates a dynamic "healthy" stimulus for the shutdown actuators only in response to the unique sequence generated by the hardwired input signal pattern. It therefore detects abnormal states of any of the system inputs, or software errors, wiring errors and hardware failures. This hardwired logic is conceptually simple, is fail-safe, and is amenable to simple FMEA. The adoption of the proposed design criteria ensure not only failure-to-safety in the hardware but the elimination, or at least minimisation, of the dependence on the correct functioning of the computer software for the safety of the system.

Fail-Safe Design Criteria for Computer-Based Reactor Protection Systems

by

A B KEATS

1. Introduction

The increasing size and complexity of nuclear power plants is accompanied by an increase in the quantity and complexity of the instrumentation required for their control and protection. This trend provides a strong incentive for using on-line computers rather than individual dedicated instruments as the basis of the control and protection systems. The potential advantages are four-fold. Firstly, the computer is capable of implementing more complex signal-processing algorithms. Secondly, because the time-shared computer hardware replaces many dedicated signal-processing instruments, less equipment will be used and therefore a lower failure rate can be expected. Thirdly, because less equipment will be required, the cost will be lower. Fourthly, a cost and reliability advantage may also be expected from the use of remote data-sampling and multiplexing which reduces the number of wires and connectors required between the plant measurement transducers and the centralised computer hardware. In many industrial control and instrumentation applications, on-line computers using multiplexed sampled-data are already well established, but their application to nuclear reactor protection systems requires special measures to satisfy the very high reliability which is demanded in the interests of safety and availability.

In conventional protection systems employing analogue trip units and hardwired logic, design criteria for satisfying performance requirements (speed, accuracy, spurious trip rate etc) are well established and the failure modes are well understood. The availability (spurious trip rate) and safety requirements (fractional dead-time) are satisfied by the use of redundancy; common-mode failures are avoided by segregation and diversity. Codes of practice already exist in this field (References 1, 2 and 3) and techniques for ensuring that practically all failures result in safe action (failure-to-safety) are well proven and are applied on a routine basis. Protection systems employing digital computers can also be designed to satisfy given performance requirements, but their failure modes are far more complex than in hardwired analogue and logic systems and, as demonstrated below, potentially unsafe conditions can occur unless adequate precautions are taken. Some of the requirements can be met by the above codes of practice, but some new techniques are required because of the conceptual disparities between hardwired and computer-based systems. The design criteria proposed in this paper are an extrapolation of the fail-safe mode of operation used in the UK in hardwired reactor-protection systems (References 4 and 5). This is achieved by making the "operational" condition of the reactor dependent upon an "energetic" state of the protection system components. In the shutdown state, the system components relax to a less-energetic state. As most component failures cause relaxation to a less-energetic state, the more probable (preferred) mode of failure is to the shutdown (safe) state. This objective can be achieved in a computer-based system by exploiting the inherently dynamic (ie, energetic) property of the data-sampling and multiplexing processes.

An important objective of the proposed design criteria is to eliminate, or at least to minimise, the need for a failure-mode-and-effect-analysis (FMEA) of the computer software. This demands some well-defined but simple constraints upon the way in which data are stored in the computers but the objective is achieved almost entirely by "hardware" properties of the system. The first of these is the systematic use of hardwired test inputs which cause transient excursions into the tripped state in a uniquely ordered but easily recognisable sequence. The second is the use of hardwired"pattern recognition logic" which generates a dynamic "healthy" stimulus for the shutdown actuators only in response to the unique sequence formed by the hardwired input signal pattern. It therefore detects abnormal states of any of the system inputs, or software errors, wiring errors and hardware failures. This hardwired logic is conceptually simple, is fail-safe, and is amenable to simple FMEA.

Whilst these techniques eliminate the safety-related connotations of software errors by ensuring that such errors lead to a safe state, the overall system availability can nevertheless be enhanced by some of the well-disciplined methods of software production which have been evolved in wider fields of applications of fault-tolerant computing (Reference 6).

2. The Computer-Based Protection System Configuration

Replication (or redundancy) coupled with majority voting, is necessary in computer-based protection systems for the same reasons as it is necessary in conventional hardwired protection systems, ie to achieve a specified overall system availability and fractional deadtime. The degree of redundancy will depend upon the expected system failure rates and repair times. Some existing codes of practice, relating to segregation of replicated subsystems, continue to be applicable and will exert a strong influence upon the way in which the computer system is configured. Their application leads to division of the computer functions into two distinct parts shown in Figure 1. The first function is the implementation of trip algorithms, ie the equivalent of the function of the 'trip units' to a conventional instrumentation scheme. The first computer is therefore referred to as the Trip Algorithm Computer (TAC) which may incidentally, also control the multiplexer. The second function is voting, on each group of inputs, of the status (healthy or tripped) yielded by the trip algorithm computers. This function, equivalent to the protection system logic, is performed by the Vote Algorithm Computer (VAC). This configuration and the modus operandi which follow are relevant to any type of digital computer. However, in most protection system applications, the TACs and VACs will be microprocessors dedicated to those specific tasks with their programs securely stored in read-only-memories (ROMs) and with strict control maintained over access to them.

To maintain segregation of the replicated safety channels up to the stage where they are combined by majority voting, each channel of a group monitoring any one reactor parameter, eg neutron flux, must be sampled by a separate multiplexer and processed by a separate trip algorithm computer. It follows from this that the degree of replication provided for the multiplexers must be at least the same as that provided for the sensors. Furthermore there must be at least one TAC to process the output of each multiplexer. A minimum redundant configuration of multiplexers and TACs is shown in Figure 1 for triple redundancy of the measurement sensors. This ensures that a failure of a single multiplexer or TAC affects only one measurement of any one parameter and does not constitute a common-mode failure.

Transmission of the status (healthy or tripped) outputs of the TACs to the Vote Algorithm Computer (VACs) must be via unidirectional, electrically isolated paths in order to prevent the possibility of a failure within a VAC being propagated to all the TACs and becoming a common-mode failure. This electrical isolation can be achieved by using optical coupler units or preferably, fibre optic cables.

As pointed out above, redundancy of hardware is normally essential to satisfy the reliability requirements. The degree of redundancy of the VACs is not necessarily the same as that provided for the earlier parts of the system. Figure 1 shows triple redundancy of the VACs by way of example although clearly higher degrees of redundancy may be required to satisfy given reliability criteria. The form of the final voting logic ($\equiv$ guard line voting) will in turn be influenced by the number and arrangement of the shutdown actuators. The final voting may, for example be implemented on contactors which precede the shutdown mechanisms or on multiple inputs to the shutdown actuators themselves.

3. Potential Failure Modes Peculiar to Multiplexed Computer-Based Systems

The fundamental difference between a traditional reactor protection system, comprising individual dedicated trip instruments combined by hardwired logic, and one using computers, is that the latter operates on sampled data using a common central processing unit (the CPU) in a time-sharing mode. This means that instead of each of the measurement transducers being continuously connected to a dedicated signal processing instrument, they are connected sequentially to the common processor by a multiplexer which samples each of them in turn. The time-division-multiplexed sampled-data is normally converted to digital form by an analogue-to-digital converter (ADC) before passing into the common processor. The common processor normally contains a store in which the current value of each input is memorised during the time interval between consecutive sampling instants. Multiplexed sampled-data systems of this type are widely used in process plant data acquisition and control systems. There are however certain potential modes of failure of the data acquisition hardware which, in the context of reactor protection systems must be rendered "safe" and self revealing. They are:-

(1) Failure of one or more of the multiplexer address bits to change state (ie stuck-at-1 or stuck-at-0 faults) which causes the multiplexer to repeatedly sample a limited subset of the full input address range.

(2) Complete stoppage of the multiplexer which causes the memory to retain the last set of values stored prior to the fault.

(3) Limited or complete failure of any part of the common, time-shared signal path (including the ADC) between the multiplexer and the processor, to accurately convey the sampled data (eg one or more data bits out of the ADC "stuck-at-1" or "stuck-at-0").

4. Methods of Protection Against Failures

4.1 The Use of Test Inputs to the Multiplexer

The first of the failure modes referred to in 3 above is made self-revealing by the introduction of "test inputs" to the multiplexer. The signals applied to the test inputs are chosen to be readily distinguishable from the signals originating from plant measurement transducers. The order in which the test inputs are interleaved between the plant signals is chosen so that a unique but easily recognisable pattern is generated (Figure 3) only when the multiplexer scans its full address range. The pattern cannot then be reproduced by repeated scanning

of a subset of the full address range. A preferred arrangement of the order of the test inputs is shown in Figure 2 for a 128-input multiplexer. This particular arrangement is chosen so that it is subsequently recognisable by simple logical shifting and comparison functions (see Paragraph 4.4 below). The properties of the test inputs (magnitude, rate of change, power spectral density, etc) are chosen to cause excursions of the trip algorithms into the tripped state. Differing properties may be ascribed to any or all of the test inputs so that all trip algorithms are exercised on every scan of the multiplexer inputs.

The response of the trip algorithms to the test and transducer signal inputs yields a sequential pattern of "status" bits in which a 1 represents the healthy status (not tripped) and a 0 represents the tripped status. Under normal conditions, the trip algorithms will yield a 1 status from transducer signal inputs and a 0 status from the test inputs (Figure 3). The unique status bit pattern thus generated is dictated by the order in which the test inputs are physically wired into the multiplexer.

The excursions caused by the test inputs, also provide a continuous dynamic check of the common signal path from the multiplexer through the ADC and into the processor, including the telemetry link where provided. The test input signal may be sufficiently accurately defined to provide a continuous calibration check of the ADC and any common amplification provided.

4.2 Polarity Reversal on Alternate Multiplexer Scans

In addition to ensuring that the input multiplexer is sampling all of the inputs, it is also necessary to check that the input data are being refreshed on each cycle of the multiplexer. It would otherwise be possible for the multiplexer to stop, leaving the last set of input data retained in the memory and the processor repeatedly reusing this obsolete data. This mode of failure may be prevented in one of two ways. The preferred solution is to force some property, such as polarity, of the input data to change on consecutive cycles of the multiplexer. A polarity reversing switch, following the multiplexer, which changes state on completion of every cycle of the multiplexer, causes the polarity of the input data stored in the processor's memory to reverse each time it is refreshed. The programs which process these data must be written to expect this regular polarity reversal and if it fails to occur, due to a failure of the multiplexer to refresh the memory, an incorrect status bit pattern will be generated and recognised. A further advantage of this technique is that it augments the continuous dynamic checking of the common data path which is provided by the test inputs. (A simpler but less comprehensive implementation of this principle is to reverse the polarity of the test inputs only on each multiplexer cycle.)

The use of polarity reversal to protect against the repeated re-use of obsolete data may also be applicable at later stages in the system.

4.3 Restriction of the Computer's Memory Capacity

An alternative to polarity reversal on alternate multiplexer scans, to ensure that the input data are being continuously refreshed, is to limit the capacity of the memory area available for storage of the input data to less than that required to store a complete set of values of all the inputs. This would ensure that on each complete scan of inputs, data acquired early in the scan were overwritten by those acquired later. Therefore, if the multiplexer stopped, it would be impossible to reproduce the complete sequence of data, with the test signals in their correct order, simply by repeated use of the stored subset of input data.

4.4 Hardwired Pattern Recognition Logic

The dynamically generated status word sequence is used throughout the subsequent functions of the TACs and VACs to represent the "healthy" state. It is ultimately used at the outputs of the VACs to generate a dynamic operational stimulus for the plant shutdown actuators. Recognition of the correct status pattern at the computer output is implemented in hardwired logic so that the overall self-monitoring and fail-safe properties are not dependent upon correct operation of computer software. The pattern recognition logic will remove the operational stimulus from the plant actuator, if it fails to recognise the correct pattern due to (a) deviation of any one of the system inputs beyond the prescribed limits or (b) a hardware fault, or (c) a software error or (d) a wiring error.

Pattern recognition logic suitable for the particular sequence of status words described above comprises a shift register and a comparator as shown in Figure 4. To initialise the logic elements, the first word, formed from the first 8 inputs to the multiplexer is loaded into the shift register at the same time as the corresponding status word is generated by the computer. Thereafter, the "reference pattern" held in the shift register, is shifted by one place each time a new status word is generated by the computer. The reference and output patterns should, therefore, shift in synchronism. To maintain fully dynamic operation and continuous monitoring of the comparator itself, the pattern match is tested before and after shifting the reference pattern, ie twice for each new status word generated by the computer. The output of the comparator should, therefore, be 0 before shifting (indicating a mismatch) and 1 after shifting (indicating a correct match). The alternating 1 and 0 outputs of the comparator provides the dynamic stimulus, after amplification, for the plant shutdown actuators. The shifting of the reference pattern is made conditional upon recognition of the correct match. The logic, therefore, becomes 'latched' if a mismatch is detected until manually reset.

A slight variation of this simple logical process is required to completely match the pattern generated by the arrangement of test inputs shown in Figure 2 for a 128-way multiplexer. It requires reversal of the direction of shifting the reference pattern to correspond with the reversal of the order of the test inputs over the two halves of the multiplexer.

5. Conclusions

5.1 The conceptual disparities between a traditional reactor protection system based on conventional instrumentation combined with hardwired logic and one based on the use of computers, give rise to some new design criteria and special requirements for their modus operandi. Some existing codes of practice for reactor protection systems are shown to be applicable to computer-based systems and strongly influence the computer configuration. However, additional failure modes, peculiar to computer-based systems have been identified and techniques to overcome them are put forward as design criteria. These should ensure not only failure-to-safety in the hardware, but the elimination, or at least minimisation, of the dependence upon the correct functioning of the computer software for the safety of the system.

5.2 The proposed modus operandi have evolved from the well-established practice, in reactor protection systems, of requiring the system components to maintain an energetic (or stimulated) state to enable them to sustain reactor operational conditions. The shutdown or tripped condition is achieved by relaxation to a less energetic (or de-energised) state. This results in a preferred mode of failure to the safe (ie less energetic) state. An example of this practice is the use of relays which are energised

to maintain operational conditions and de-energised to initiate a reactor trip or shutdown. In some later UK reactor protection systems, relays have been replaced by solid state logic devices such as Laddic or semiconductor logic elements. In these devices operational conditions are maintained by a dynamic or alternating state (eg of magnetic flux) and the shutdown state by a static condition; the dynamic condition being the more "energetic". Again, most failures result in relaxation to the static or less energetic condition giving a preferred mode of failure to the safe state. This fail-safe design criterion can be met in a computer-based reactor protection system by utilising the inherently dynamic property of the data sampling and multiplexing processes. The property is exploited by interleaving test inputs between the plant-sensor signals, which continuously exercise the common multiplexed data channel. The parameters of the test input signals are chosen to cause excursions of the trip algorithms into the tripped state. The unique order in which these excursions occur is detected dynamically by hardwired pattern-recognition-logic at the computer output. The reactor operational condition is maintained by continuous recognition of the dynamic status pattern. The pattern recognition logic will remove the operational stimulus if it fails to recognise the unique pattern due to (a) a deviation of any one of the plant-sensor inputs beyond the prescribed limits or (b) a hardware fault or (c) a software error, or (d) a wiring error. The computer itself has no knowledge of the unique operational status pattern; it can be generated only in response to correct operation of the input multiplexer and correct implementation of the trip algorithm. This results in a highly fail-safe diagnostic computer-based reactor-protection system.

REFERENCES

1. CEGB Specification US 76/10. "Instruments and Control Equipment General Technical Requirements".

2. CEGB Specification for Reactor Safety Systems, AGR Design Safety Requirements Annex VII.

3. IEEE Standards 279 - (1971).

4. A B KEATS. "Safety Circuits Based on Contemporary LSI Techniques". IAEA/NPPCI Specialists' Meeting, Cologne, 15-16 October 1973.

5. A B KEATS. "A Fail-Safe Computer-Based Reactor Protection System". IAEA/NPPCI Specialists' Meeting, Munich, 11-13 May 1976.

6. Proceedings of the 9th Annual International Symposium on Fault Tolerant Computing, (FTCS-9), Madison US, 20-22 June 1979.

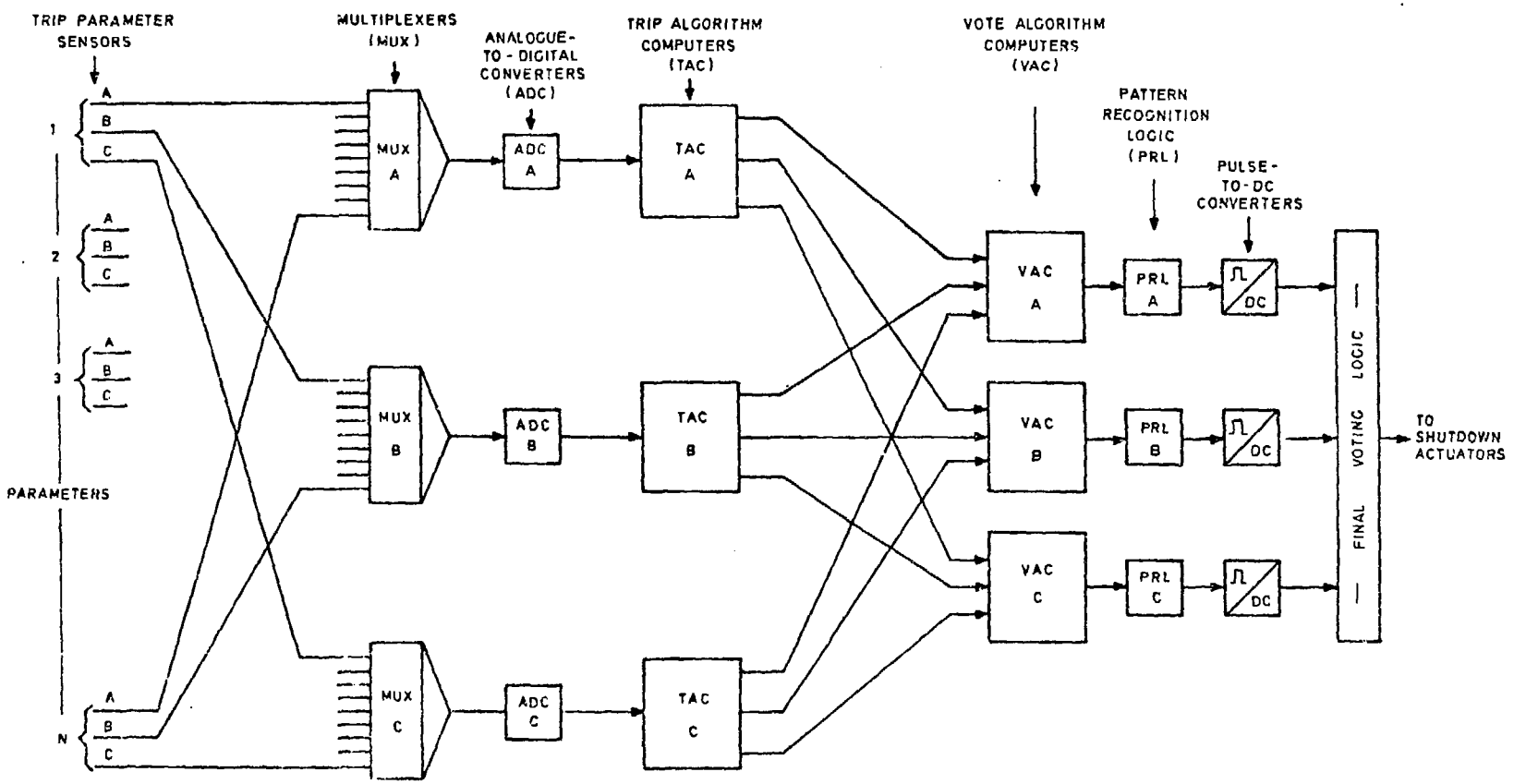

FIG. 1. COMPUTER-BASED REACTOR-PROTECTION SYSTEM

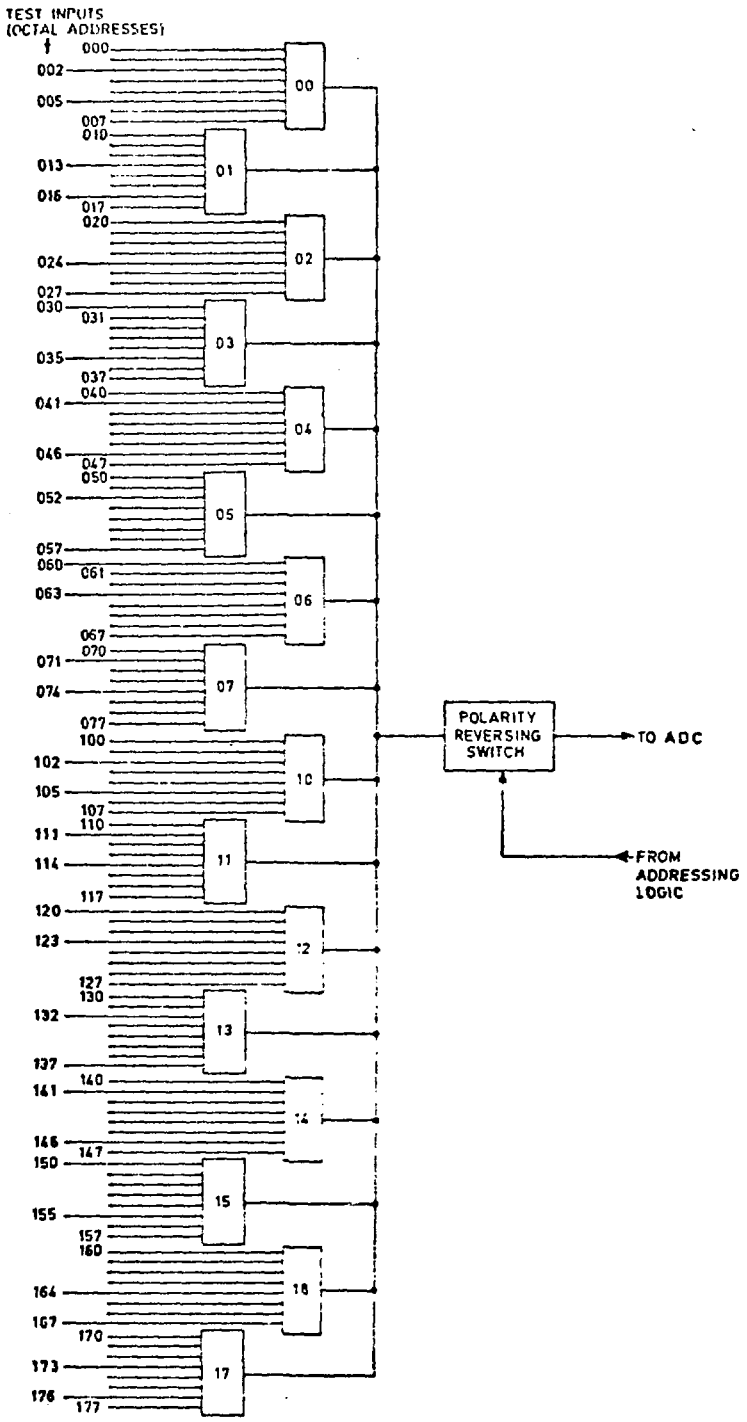

FIG 2. MULTIPLEXER INPUT WIRING PATTERN

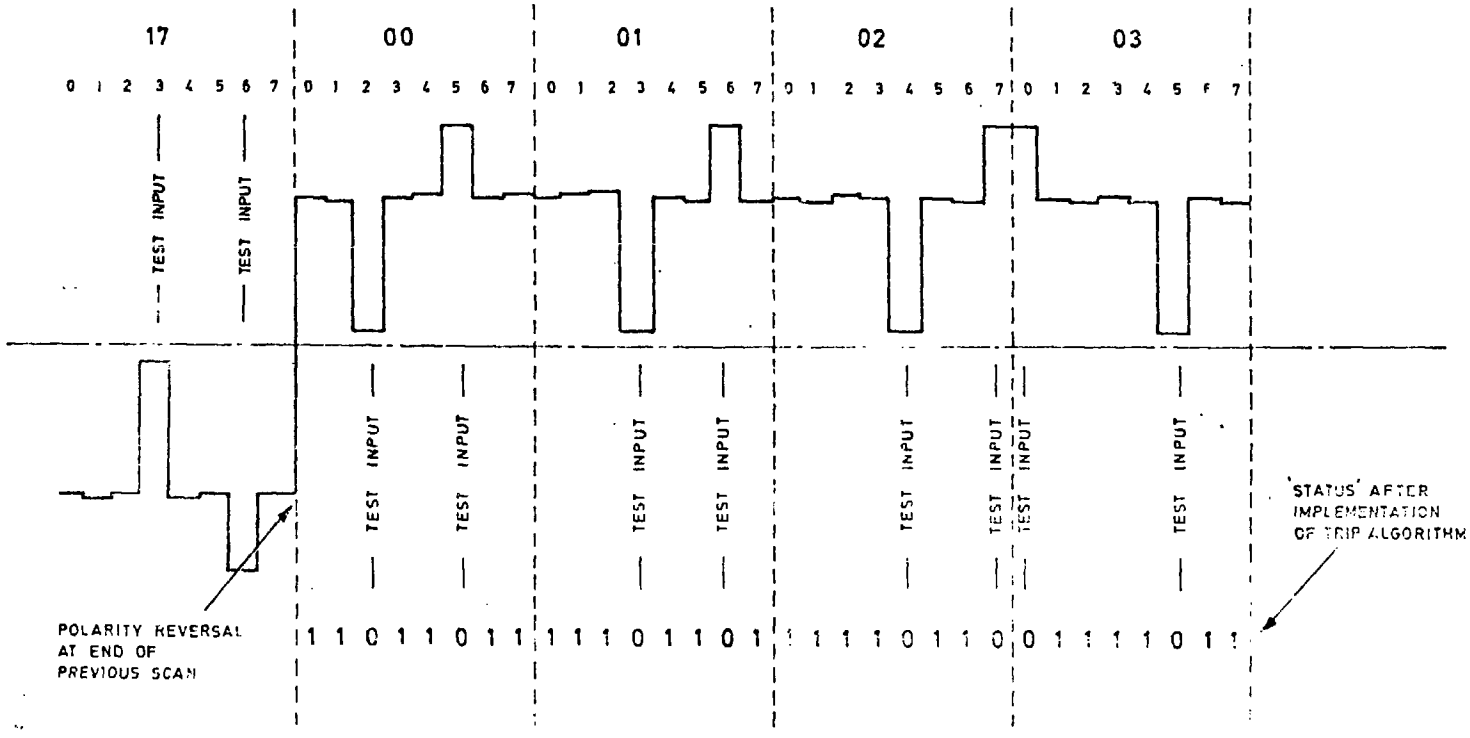

FIG. 3. SEQUENTIAL ANALOGUE SIGNALS AT MULTIPLEXER OUTPUT

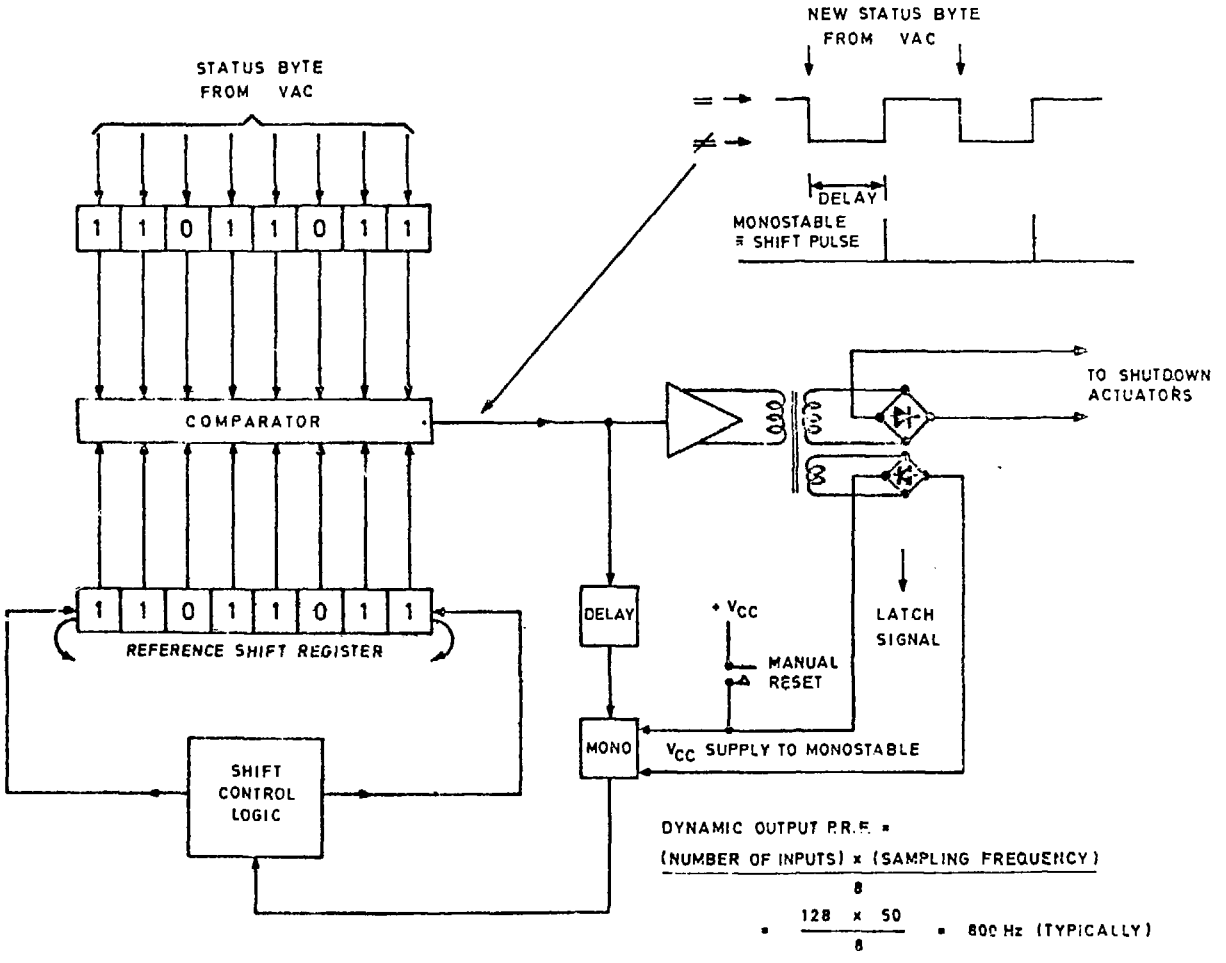

FIG. 4. PATTERN RECOGNITION LOGIC

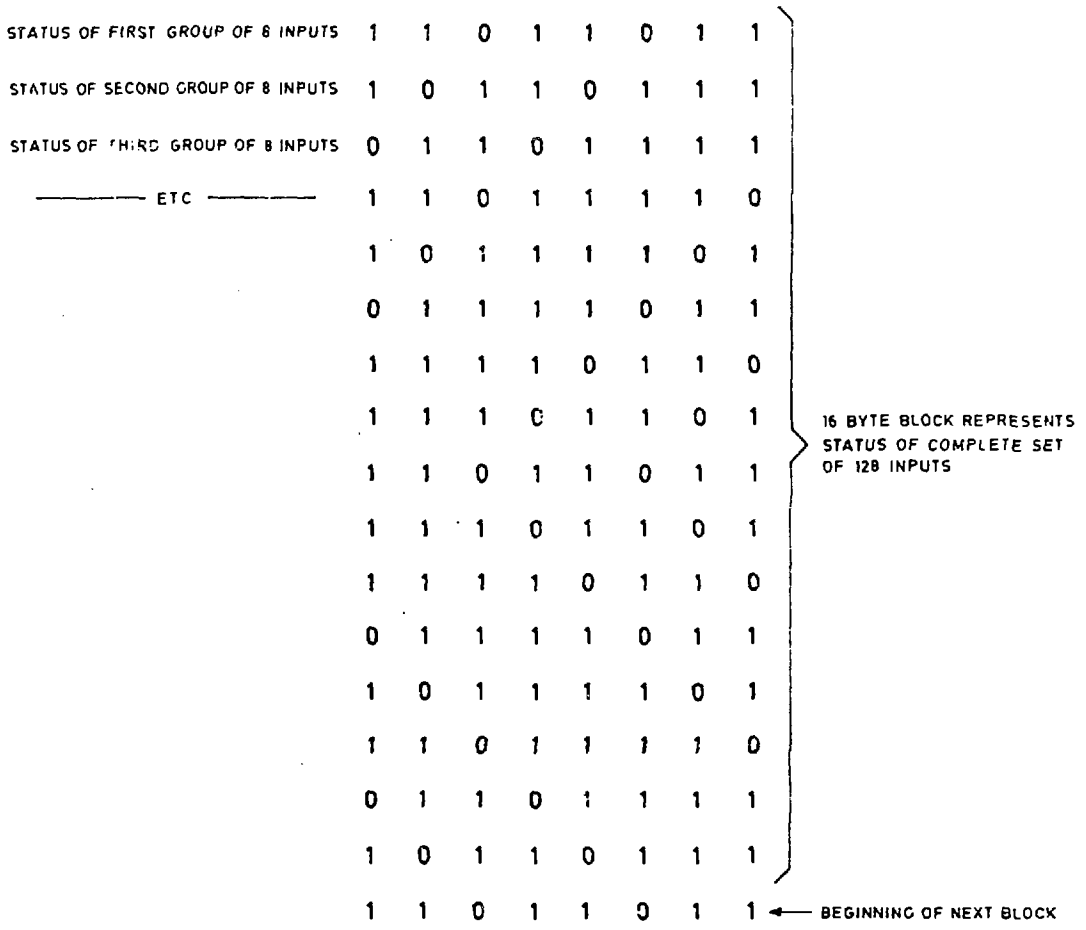

FIG. 5. FORMAT OF STATUS DATA AFTER IMPLEMENTATION OF TRIP ALGORITHMS