(12) UK Patent Application (19) GB (11) 2 200 476 (13) A

(43) Application published 3 Aug 1988

(21) Application No 8701964

(22) Date of filing 29 Jan 1987

(71) Applicant
British Gas plc

(Incorporated in United Kingdom)

Rivermill House, 152 Grosvenor Road,
London, SW1V 3JL

(72) Inventors
Barry Leonard Price
Christopher John Thomhill

(74) Agent and/or Address for Service
David J. Morgan
British Gas plc, Patents Dept, 326 High Holborn,
London, WC1V 7PT

(51) INT CL⁴
G05B 9/02

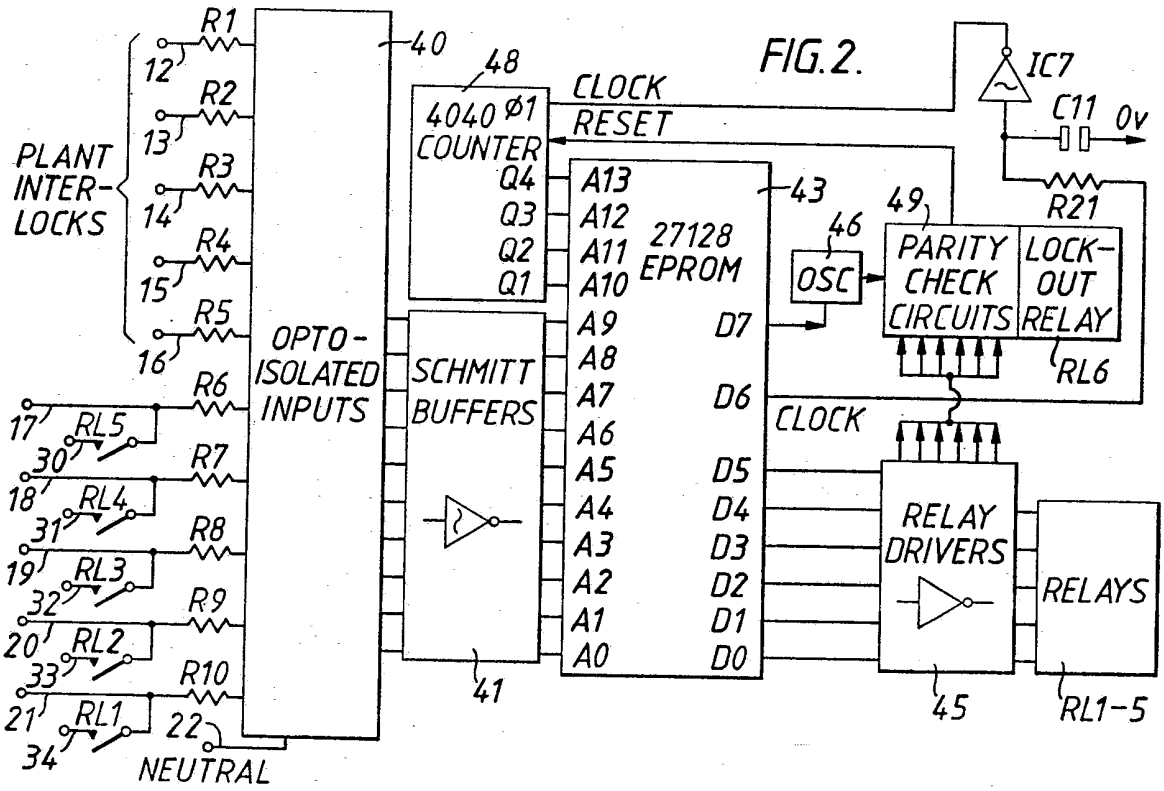
(52) Domestic classification (Edition J):
G3N 287 375 GK2A
U1S 1955 G3N

(56) Documents cited
GB A 2117122 GB A 2105492

(58) Field of search
G3N
Selected US specifications from IPC sub-classes
F02D G05B

(54) Monitor system

(57) A monitor system for safety critical situations such as burner control receives at inputs 17-21 control information from a programmable logic control and reference information at inputs 12-16 from plant interlocks. Failure of the PLC or monitor components will cause access to shutdown addresses of the EPROM and operation of the appropriate relays including lockout relay RL6.



GB 2 200 476 A

The drawing(s) originally filed was (were) informal and the print here reproduced is taken from a later filed formal copy.

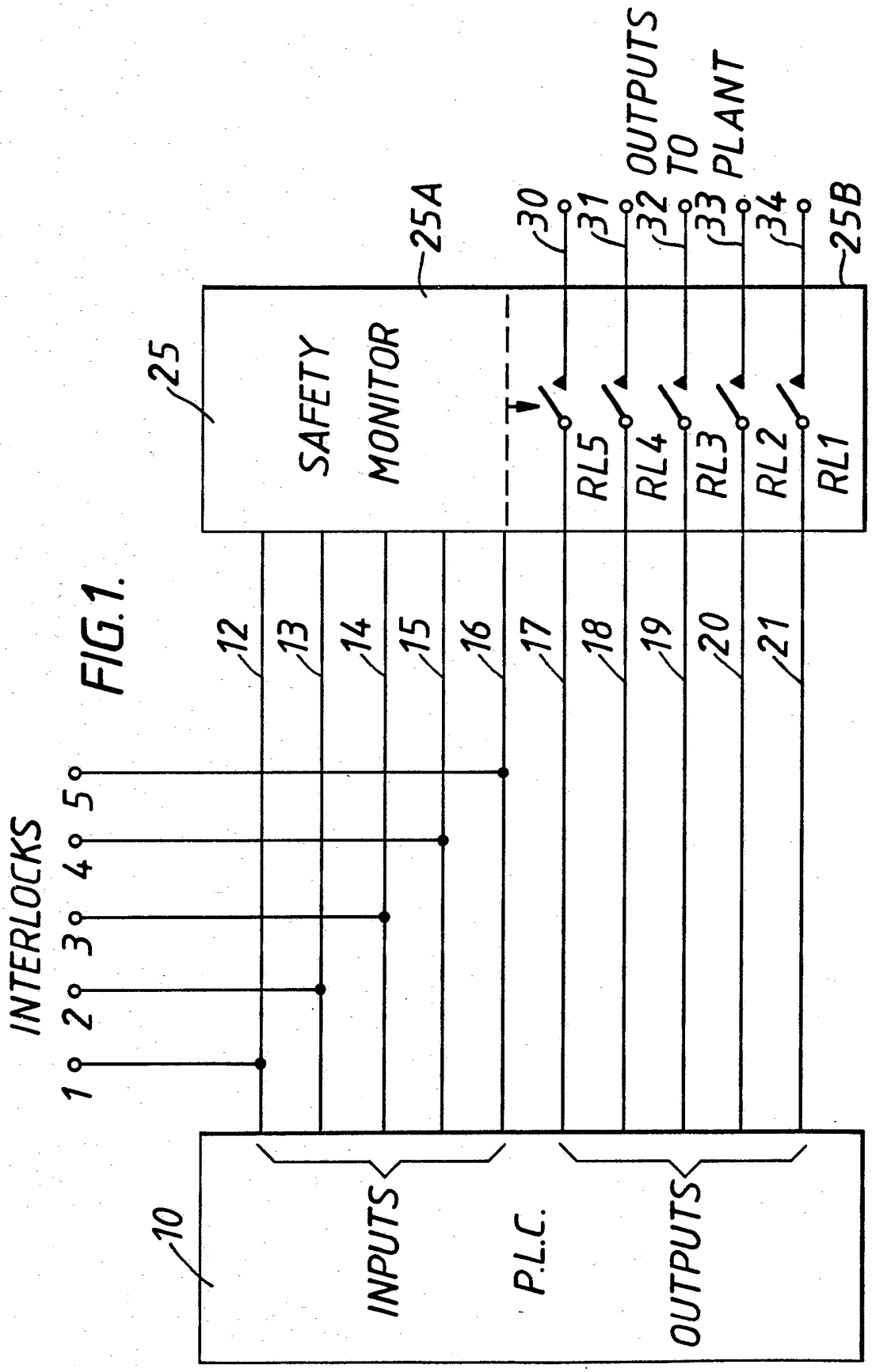

INTERLOCKS
1
2
3
4
5
10
P.L.C.
INPUTS
OUTPUTS
12
13
14
15
16
17
18
19
20
21
25
SAFETY MONITOR
25A
25B
30
31
32
33
34
RL5
RL4
RL3
RL2
RL1
OUTPUTS TO PLANT

FIG.1.

FIG.2.

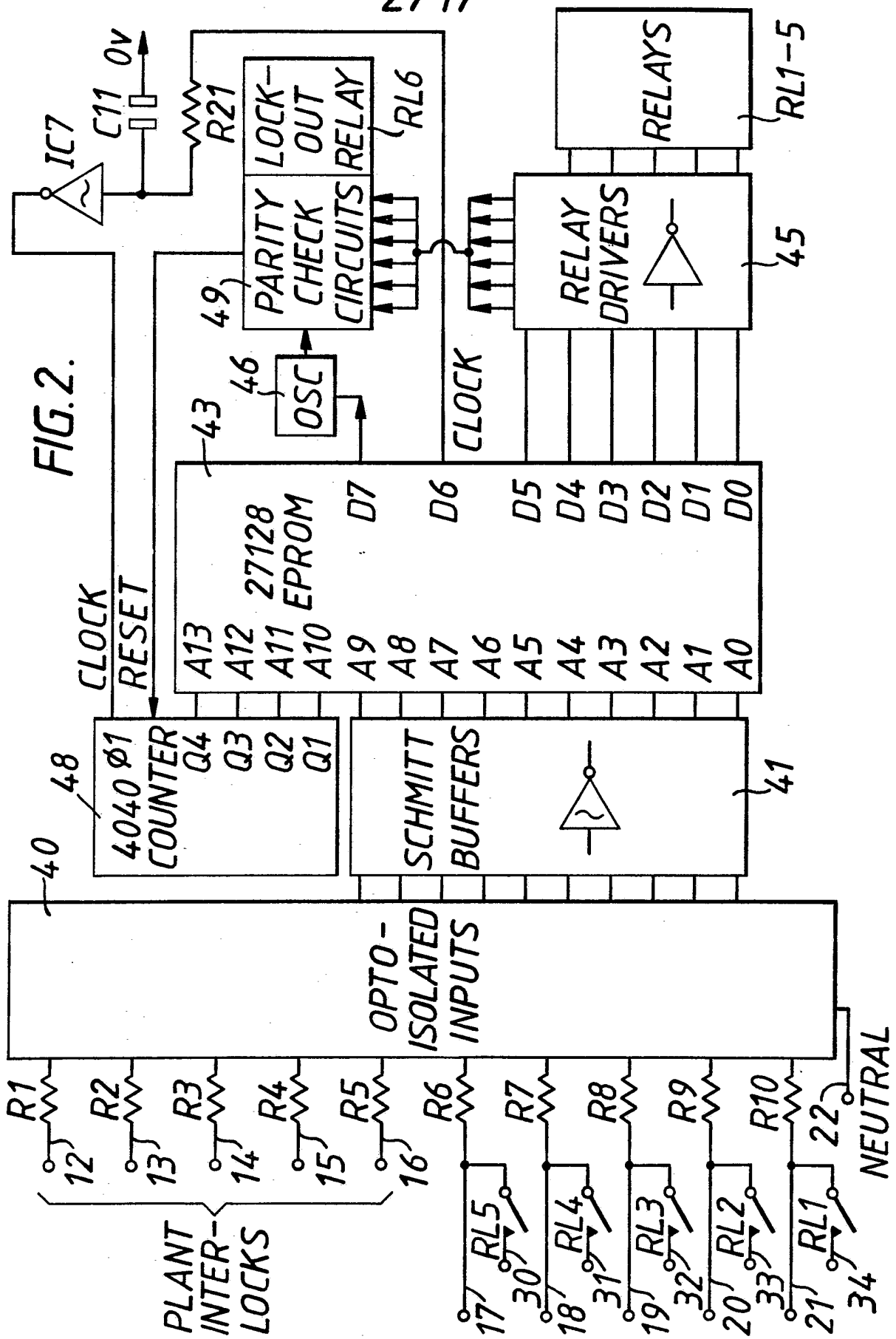

IC7
C11
0v
R21
LOCK-OUT RELAY
RL6
RELAYS
RL1-5
PARITY CHECK CIRCUITS
49
RELAY DRIVERS
45
46
OSC
43
CLOCK
27128 EPROM
A13 A12 A11 A10 A9 A8 A7 A6 A5 A4 A3 A2 A1 A0
D7 D6 D5 D4 D3 D2 D1 D0
CLOCK
RESET
48
4040 Ø1 COUNTER
Q4 Q3 Q2 Q1
SCHMITT BUFFERS
41
40
OPTO-ISOLATED INPUTS
R1 R2 R3 R4 R5 R6 R7 R8 R9 R10
12 13 14 15 16 17 18 19 20 21 22
RL5 RL4 RL3 RL2 RL1
30 31 32 33 34
PLANT INTER-LOCKS
NEUTRAL

FIG.3.

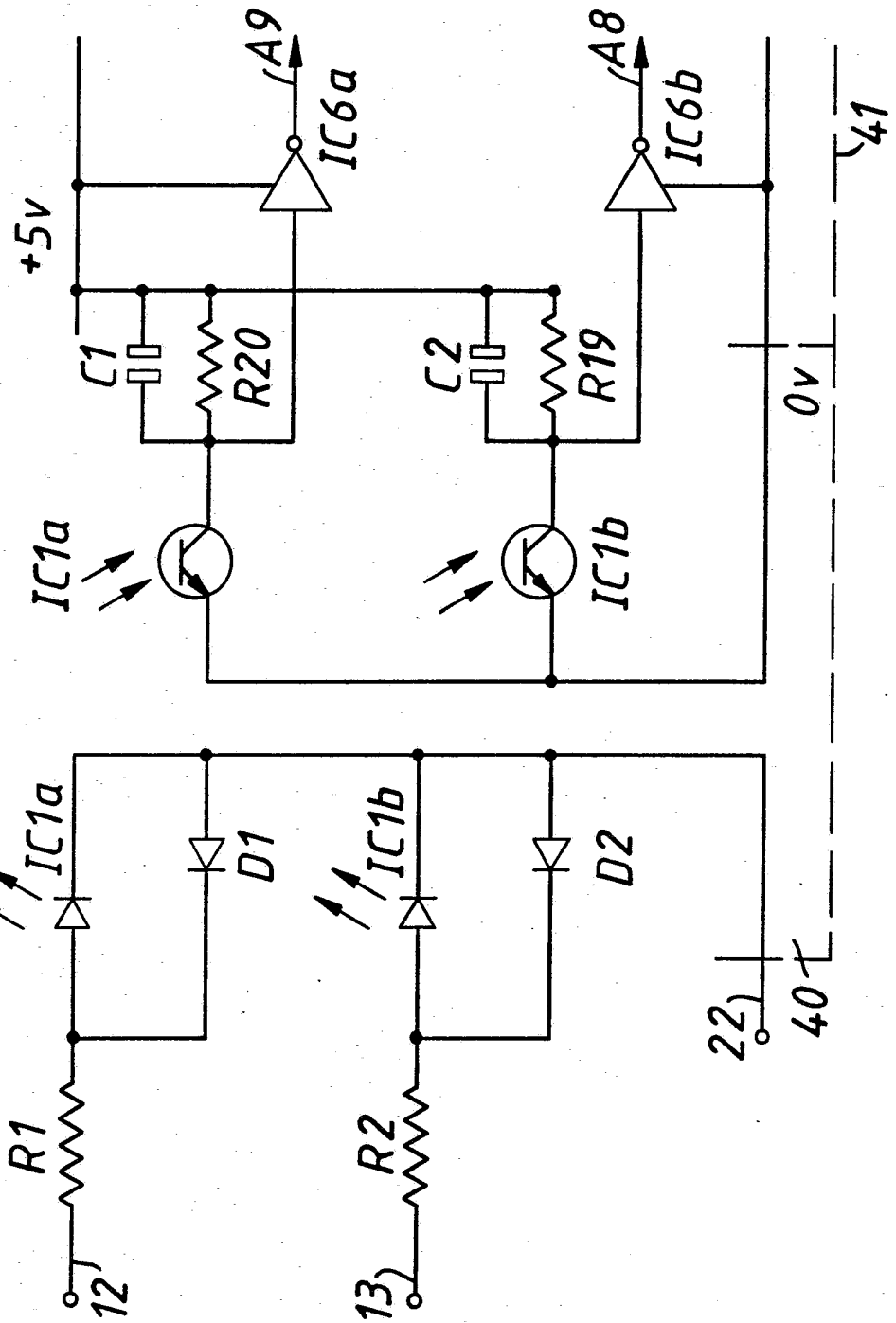

A9
IC6a
A8
IC6b
41
+5v
C1
R20
C2
R19
0v
IC1a
IC1b
IC1a
D1
IC1b
D2
R1
R2
12
13
22
40

FIG. 4.

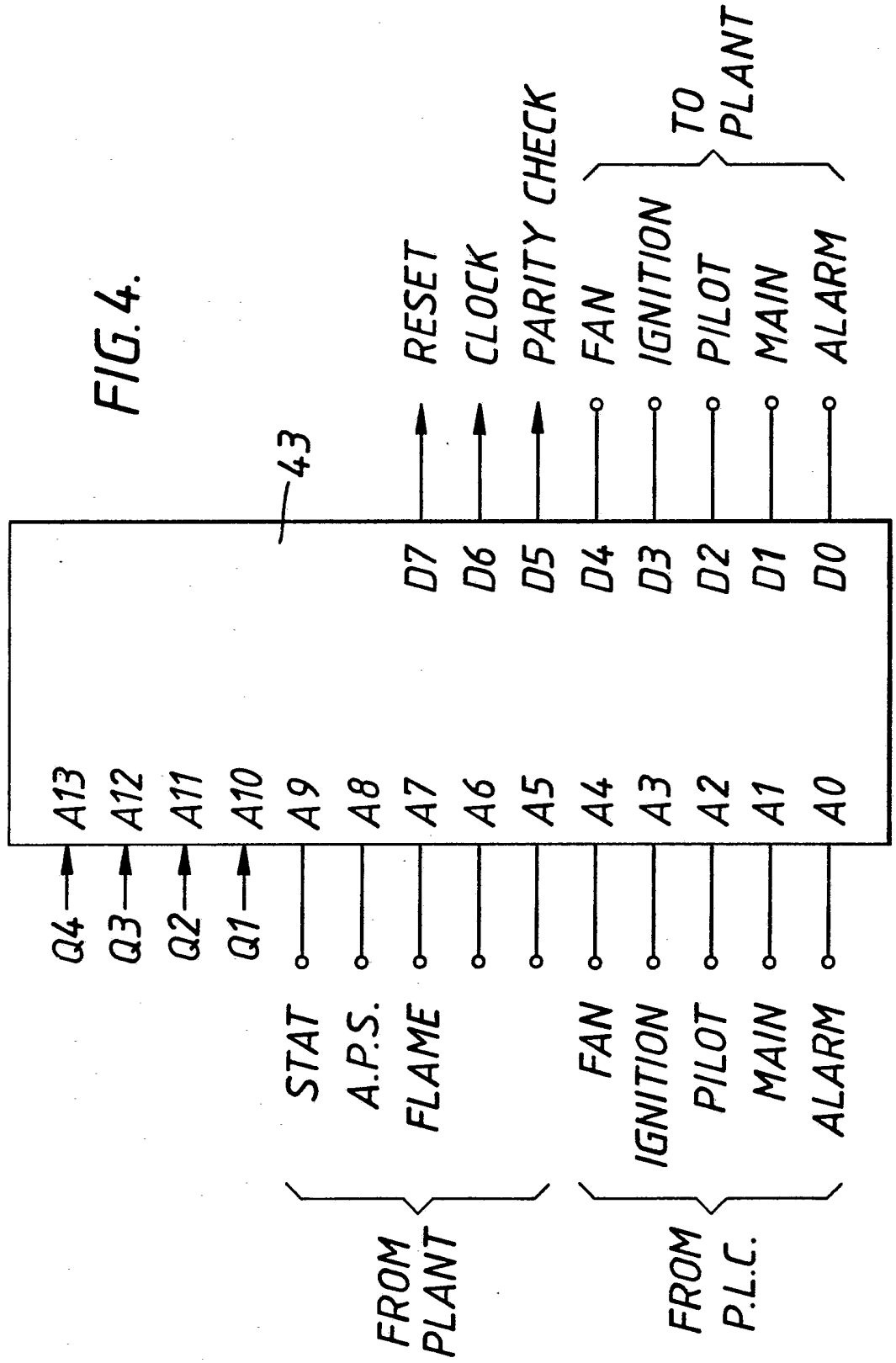

43
Q4
Q3
Q2
Q1
A13
A12
A11
A10
A9
A8
A7
A6
A5
A4
A3
A2
A1
A0
D7
D6
D5
D4
D3
D2
D1
D0
RESET
CLOCK
PARITY CHECK
FAN
IGNITION
PILOT
MAIN
ALARM
TO PLANT
FROM PLANT
STAT
A.P.S.
FLAME
FROM P.L.C.
FAN
IGNITION
PILOT
MAIN
ALARM

FIG. 5.

Stage	Period T	Main	Pilot	Ign	Fan	Flame	Alarm	APS	Stat
Shutdown	0	0	0	0	0	0	0	0	X
Start	1	0	0	0	X	0	0	0	1
Purge	2	0	0	0	1	0	0	X	1
Proven-Purge	3	0	0	X	1	0	0	1	1
Pilot-Ignition	4	0	X	1	1	X	0	1	1
Pilot-Proving	5	0	1	0	1	1	0	1	1
Main-Igninition	6	1	1	0	1	1	0	1	1
Main-Run	7	1	0	0	1	1	0	1	1
Post-Purge	8	0	0	0	1	X	0	X	0

0 = Output must be de-energised
1 = Output must be energised
X = Output - state is not critical (don't care)

2200476

FIG.6.

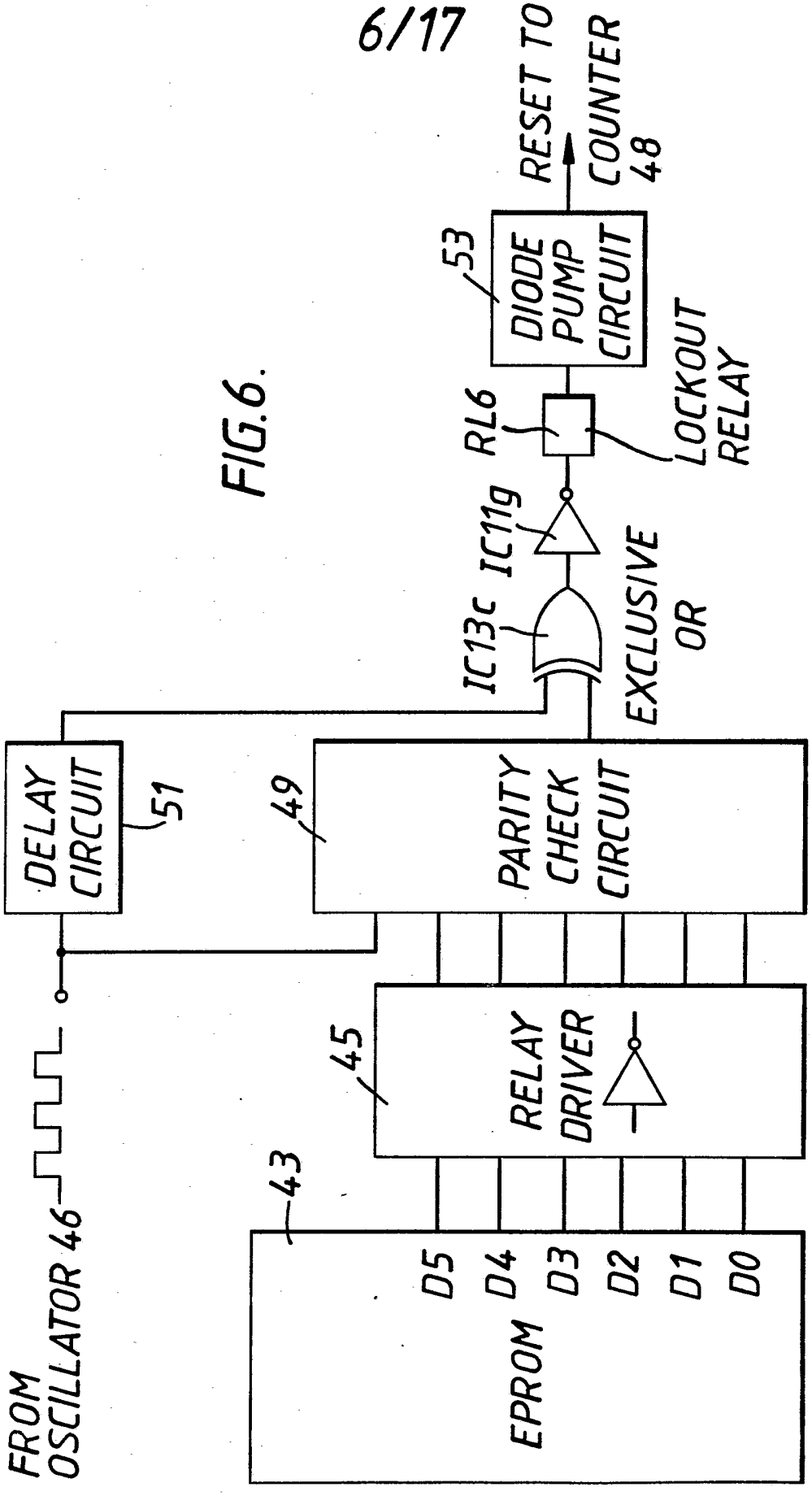

FROM OSCILLATOR 46
43
EPROM
D5
D4
D3
D2
D1
D0
45
RELAY DRIVER
49
PARITY CHECK CIRCUIT
DELAY CIRCUIT
51
IC13c
IC11g
EXCLUSIVE OR
RL6
LOCKOUT RELAY
53
DIODE PUMP CIRCUIT
RESET TO COUNTER 48

FIG. 7.

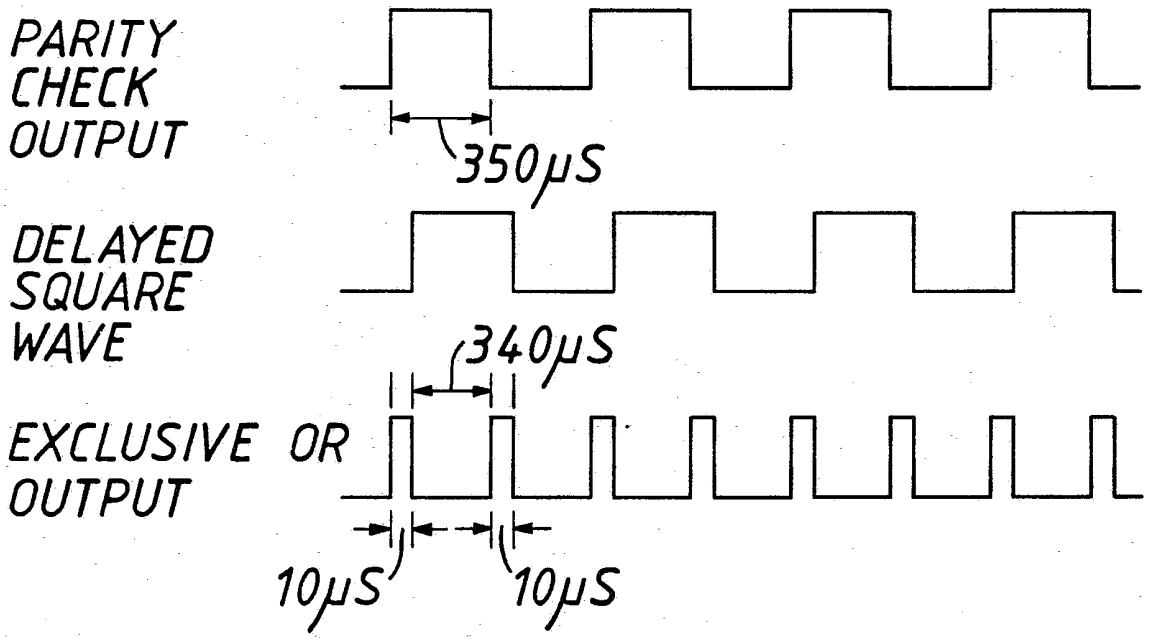


FIG. 8.

FIG. 9.

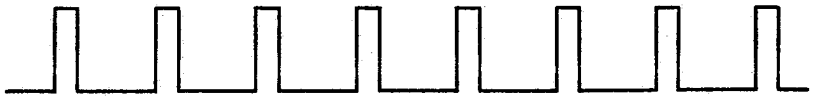


FIG.10.

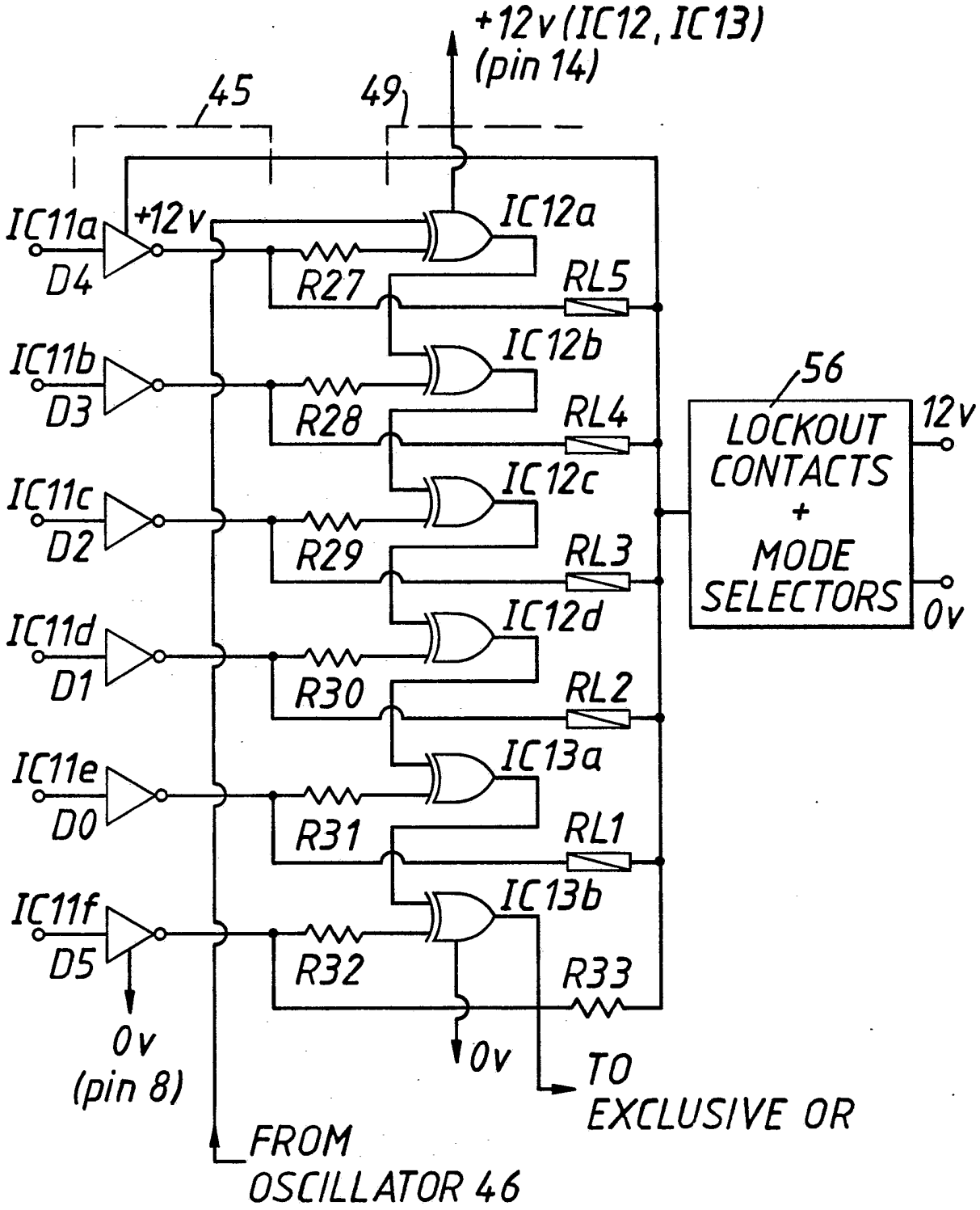

+12v (IC12, IC13)
(pin 14)
45
49
IC11a
D4
+12v
IC12a
R27
RL5
IC11b
D3
IC12b
R28
RL4
56
LOCKOUT
CONTACTS
+
MODE
SELECTORS
12v
0v
IC11c
D2
IC12c
R29
RL3
IC11d
D1
IC12d
R30
RL2
IC11e
D0
IC13a
R31
RL1
IC11f
D5
IC13b
R32
R33
0v
(pin 8)
0v
TO
EXCLUSIVE OR
FROM
OSCILLATOR 46

FIG.11.

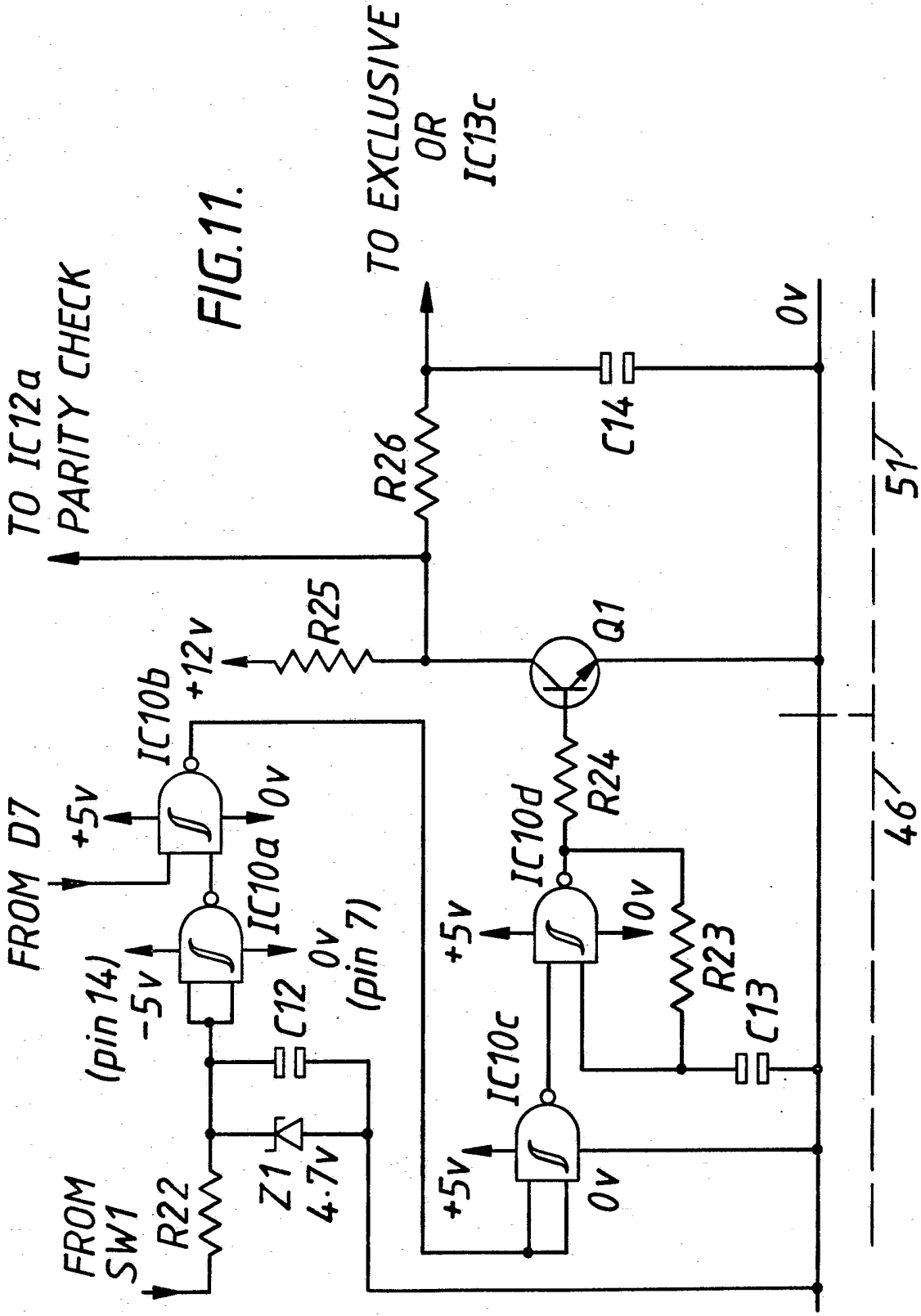

TO IC12a
PARITY CHECK
TO EXCLUSIVE
OR
IC13c
R26
C14
0v
51
R25
+12v
Q1
IC10b
+5v
0v
FROM D7
IC10a
(pin 14)
-5v
0v
(pin 7)
C12
IC10d
R24
+5v
0v
R23
C13
IC10c
+5v
0v
FROM
SW1
R22
Z1
4·7v
46

FIG.12.

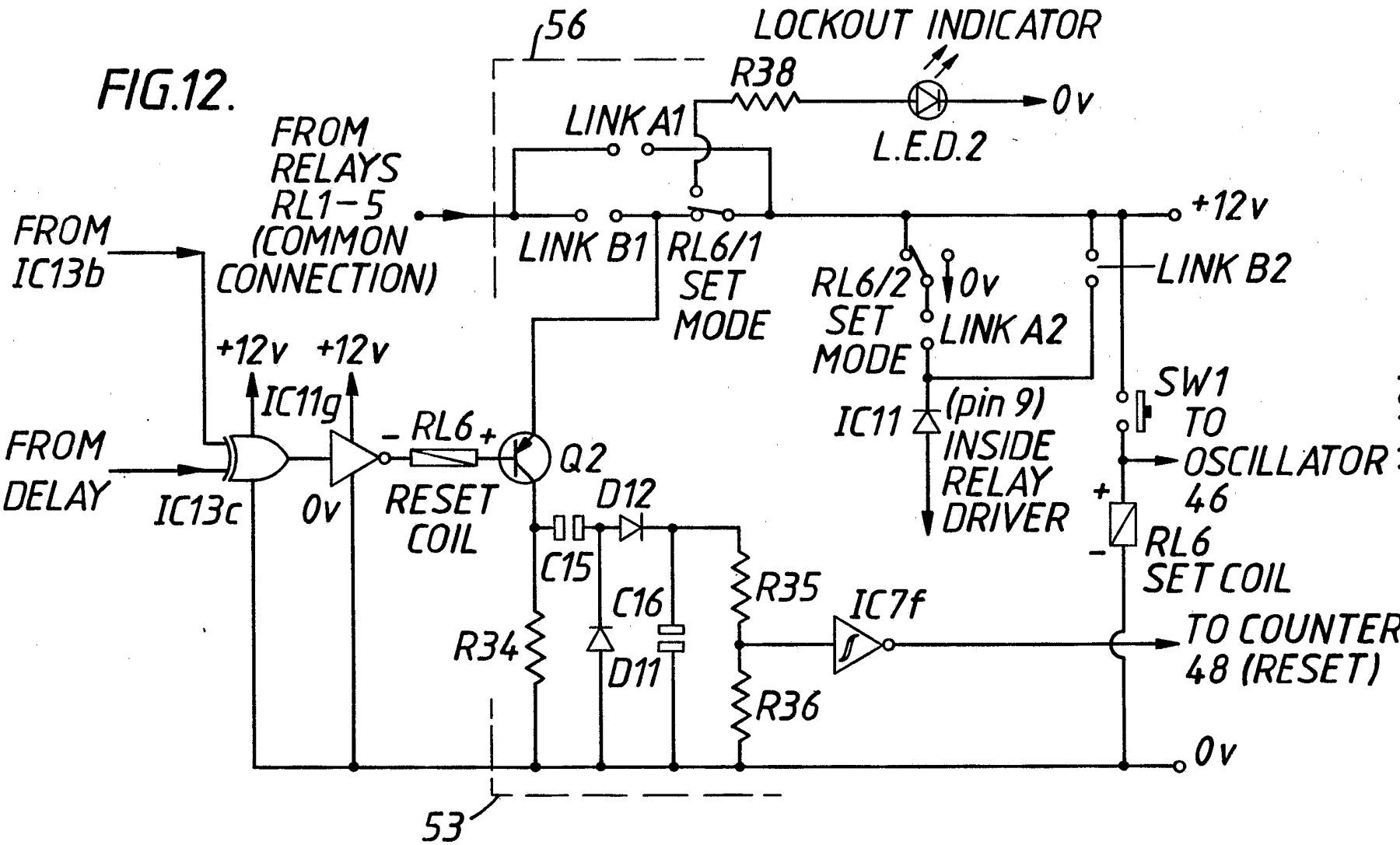

56
LOCKOUT INDICATOR
R38
0v
L.E.D.2
LINK A1
FROM RELAYS RL1-5 (COMMON CONNECTION)
FROM IC13b
LINK B1
RL6/1 SET MODE
+12v
LINK B2
RL6/2 SET MODE
0v
LINK A2
+12v
+12v
IC11g
IC11
(pin 9) INSIDE RELAY DRIVER
SW1 TO OSCILLATOR 46
FROM DELAY
IC13c
0v
RL6
RESET COIL
Q2
D12
C15
C16
D11
R34
R35
R36
IC7f
RL6 SET COIL
TO COUNTER 48 (RESET)
0v
53

FIG.13.

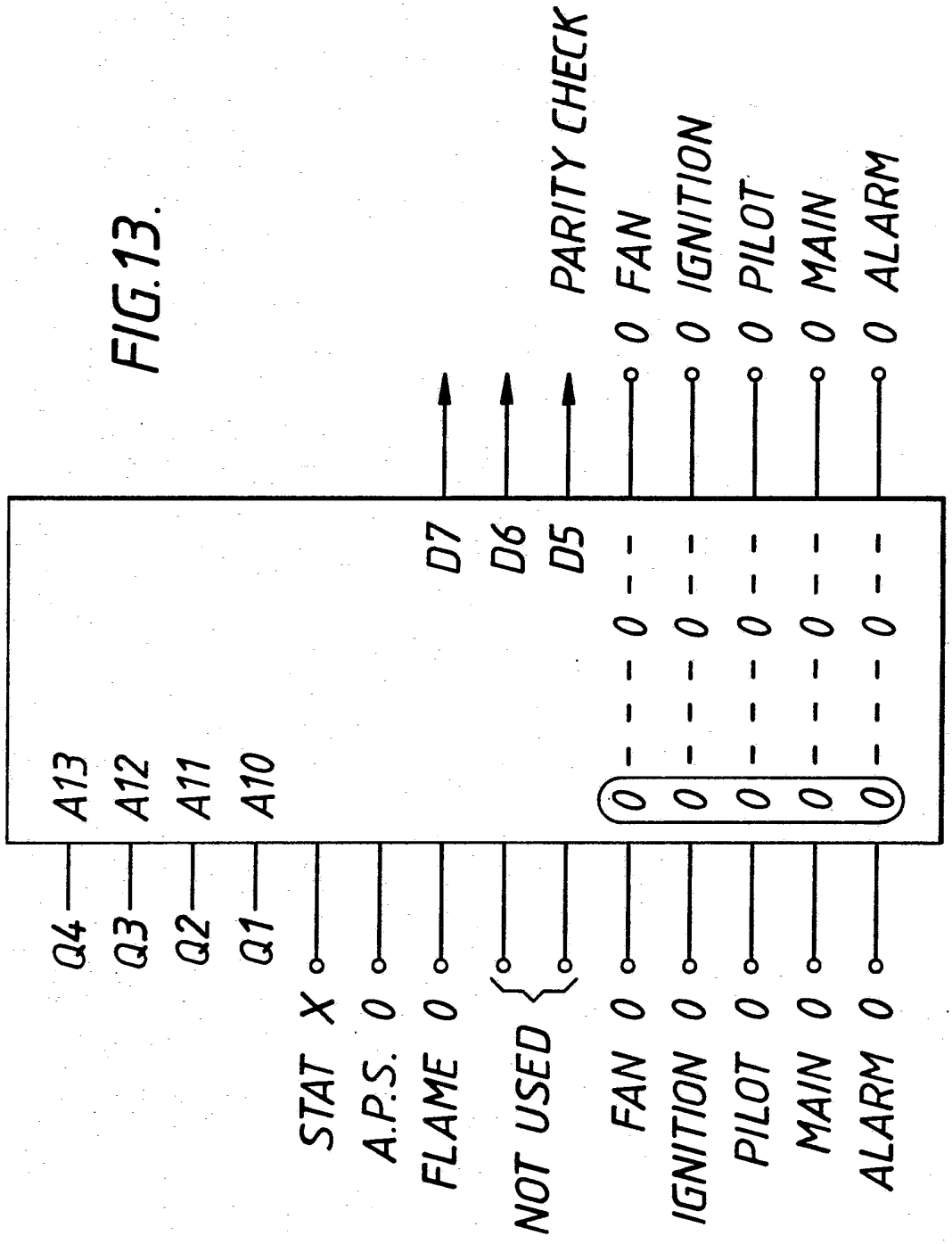

Q4
Q3
Q2
Q1
STAT X
A.P.S. 0
FLAME 0
NOT USED
FAN 0
IGNITION 0
PILOT 0
MAIN 0
ALARM 0
A13
A12
A11
A10
D7
D6
D5
PARITY CHECK
0 FAN
0 IGNITION
0 PILOT
0 MAIN
0 ALARM

FIG.14.

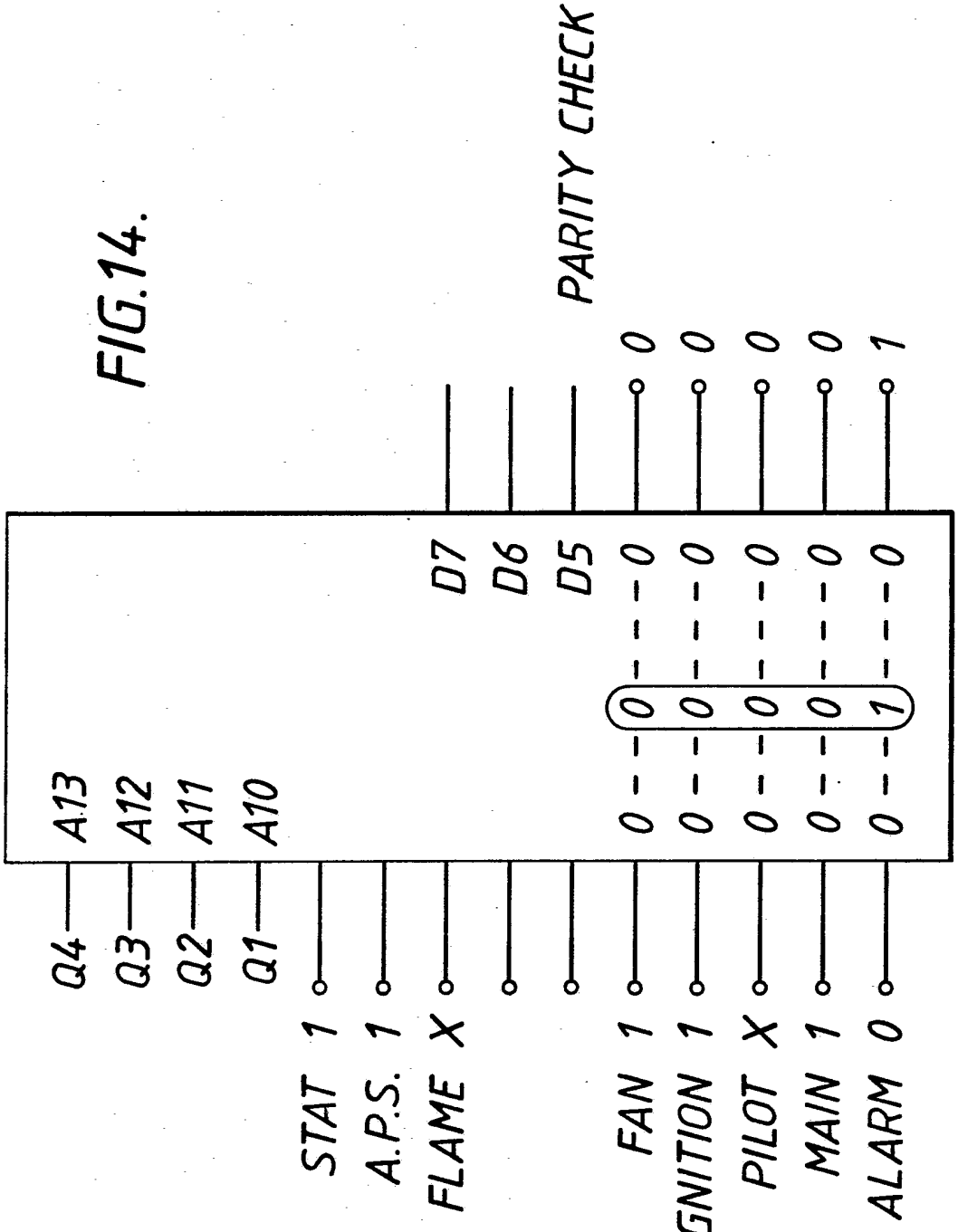

PARITY CHECK
D7
D6
D5
A13
A12
A11
A10
Q4
Q3
Q2
Q1
STAT 1
A.P.S. 1
FLAME X
FAN 1
IGNITION 1
PILOT X
MAIN 1
ALARM 0
0 0 0 0 1
0 0 0 0 0
0 0 0 0 0
0 0 0 0 1
0 0 0 0 0

FIG.15.

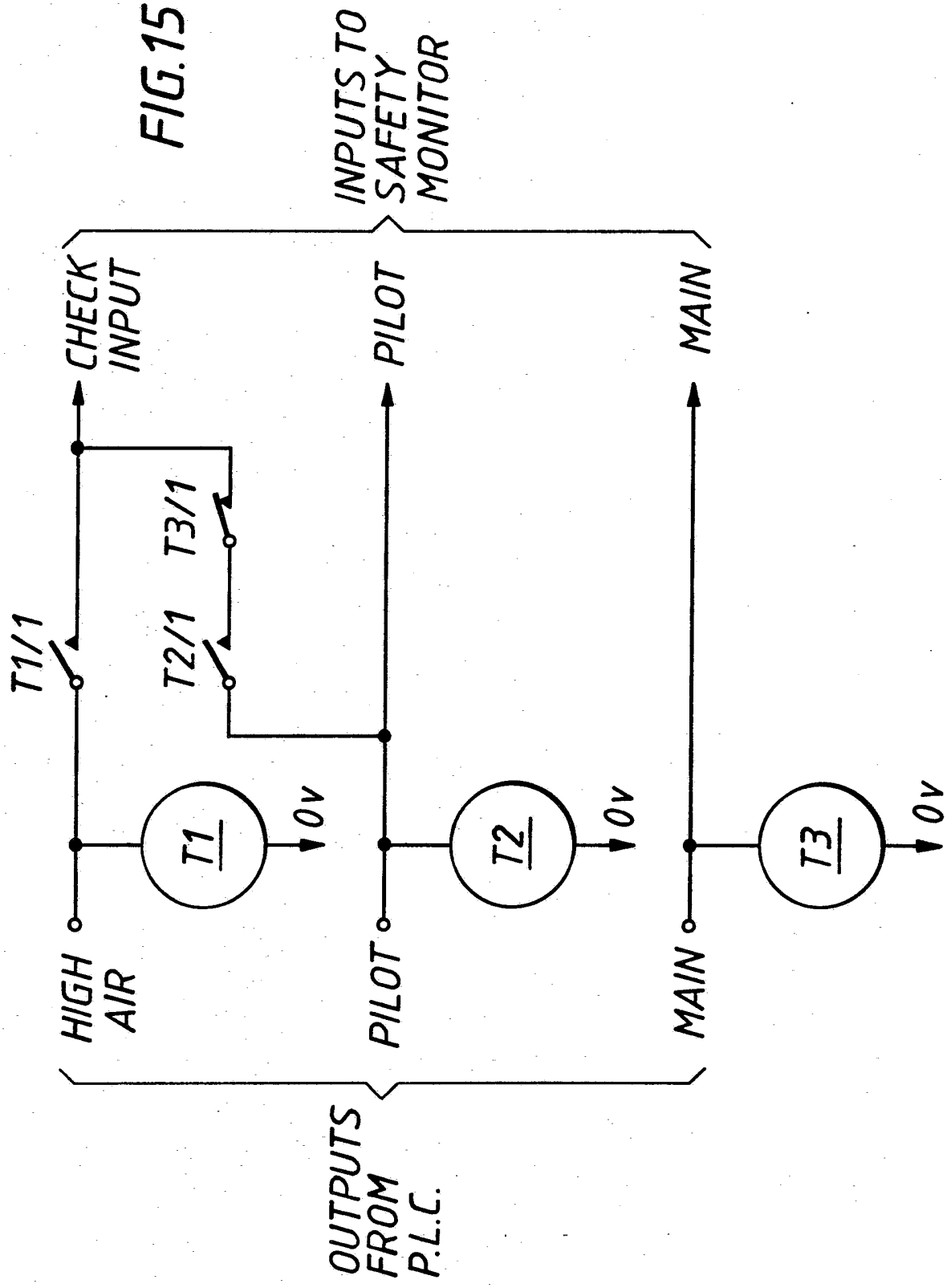

INPUTS TO SAFETY MONITOR
CHECK INPUT
PILOT
MAIN
T1/1
T2/1
T3/1
T1
T2
T3
0v
0v
0v
HIGH AIR
PILOT
MAIN
OUTPUTS FROM P.L.C.

FIG.16.

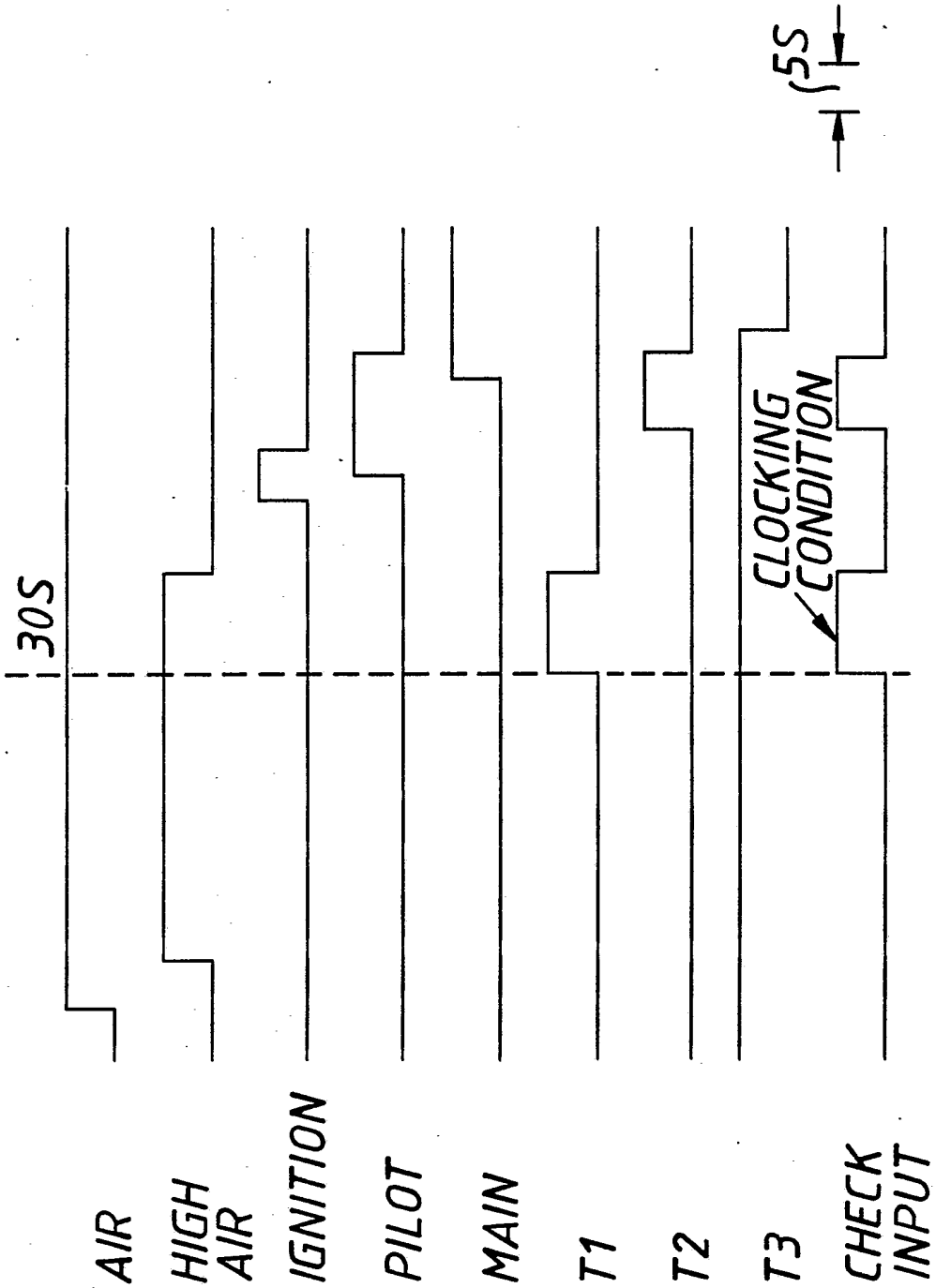

5S
30S
CLOCKING CONDITION
AIR
HIGH AIR
IGNITION
PILOT
MAIN
T1
T2
T3
CHECK INPUT

FIG.17.

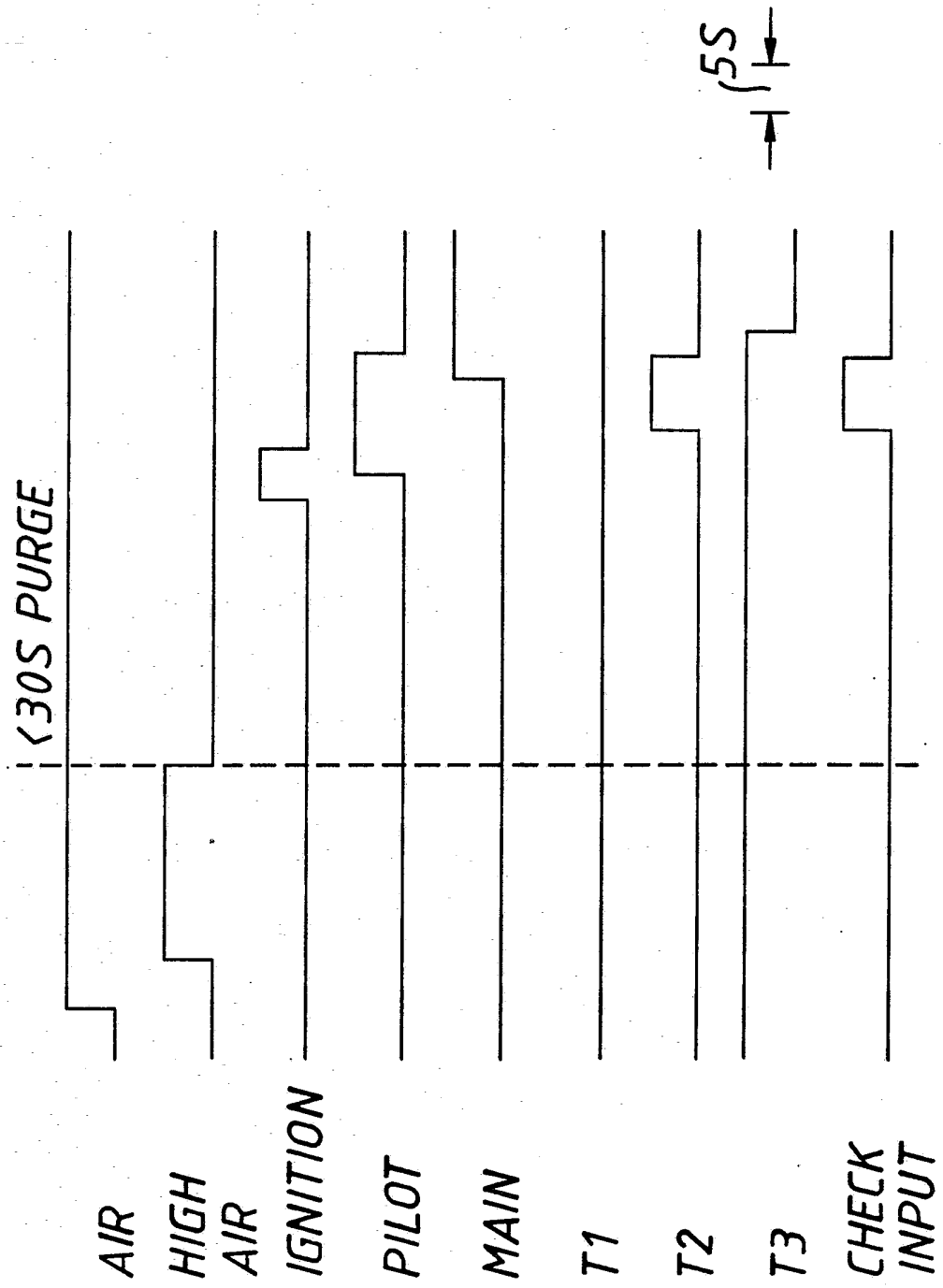

5S
<30S PURGE
AIR
HIGH AIR
IGNITION
PILOT
MAIN
T1
T2
T3
CHECK INPUT

FIG. 18.

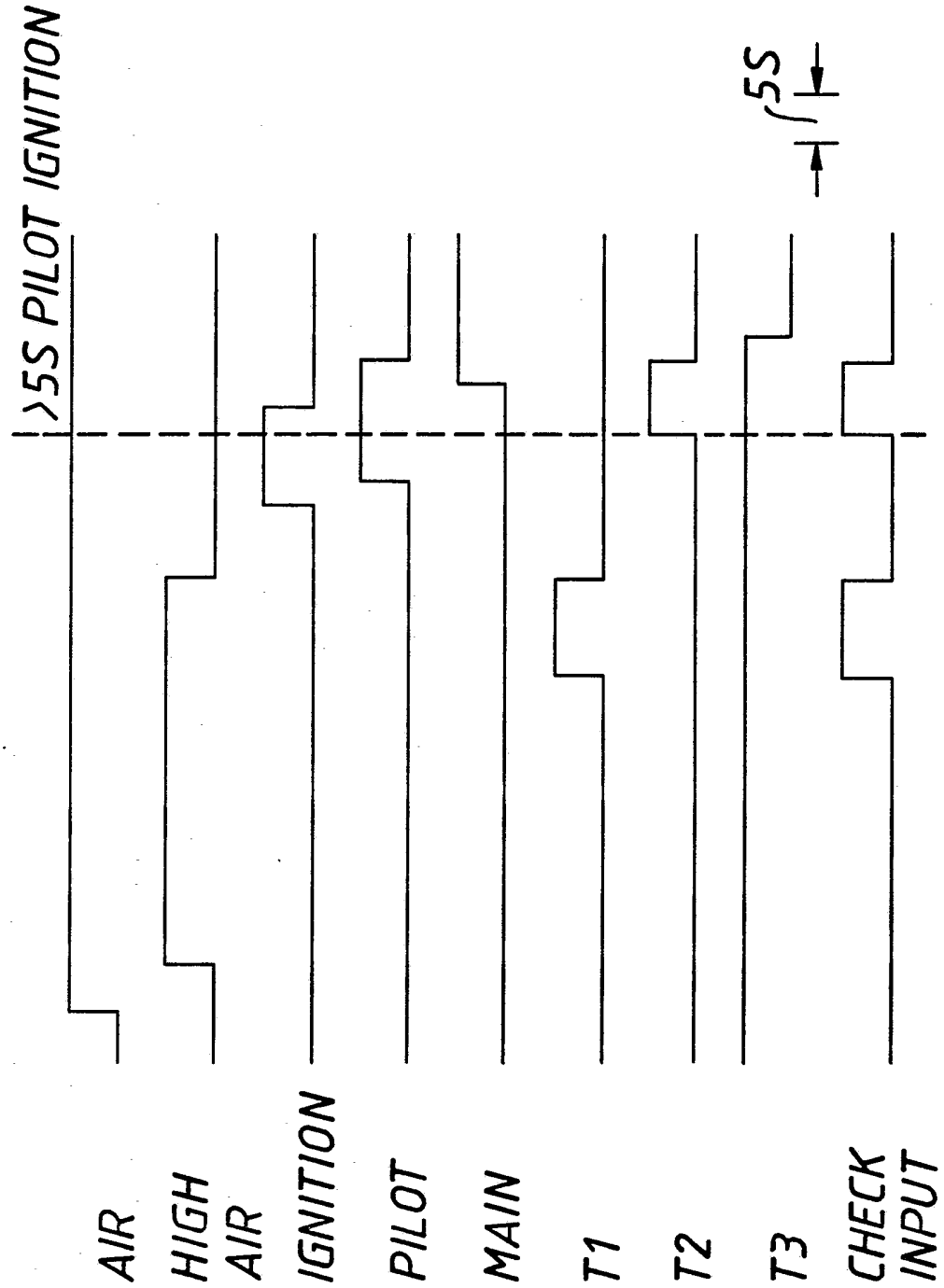
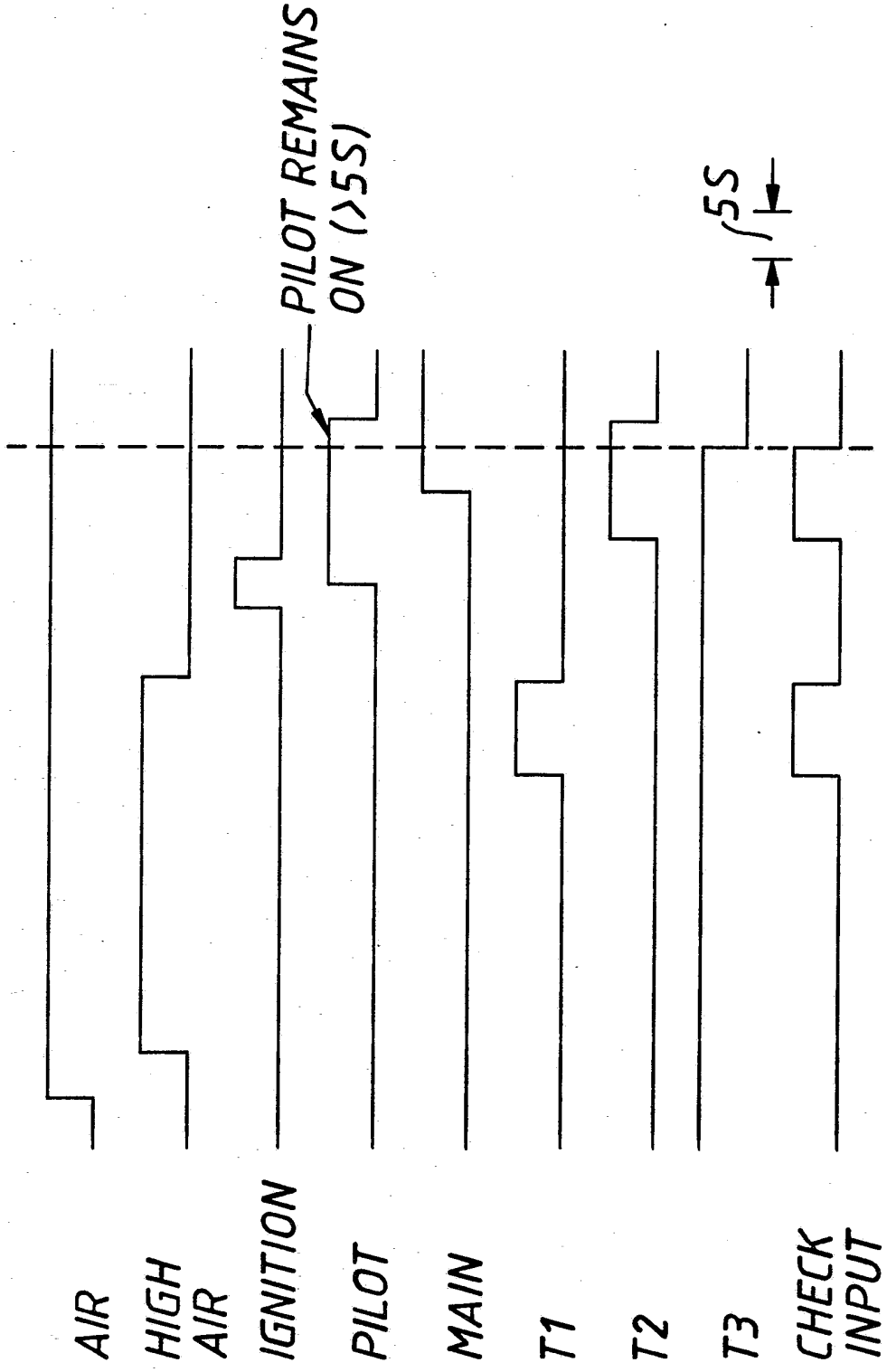

>5S PILOT IGNITION
5S
AIR
HIGH AIR
IGNITION
PILOT
MAIN
T1
T2
T3
CHECK INPUT

FIG.19.


PILOT REMAINS ON (>5S)
5S
AIR
HIGH AIR
IGNITION
PILOT
MAIN
T1
T2
T3
CHECK INPUT

2200476

MONITOR SYSTEM

MRS 2797

The invention relates to a monitor system.

In recent years microprocessor control systems have been used to control machines and systems because they are inexpensive and flexible.

When safety aspects have to be considered such as in burner control systems, inbuilt routines are used to help detect fault conditions in the systems they are controlling. Such a control system is disclosed in GB Patent Publication 2139782 for example. However, such systems can be subject to unpredictable failure modes because of the integral microprocessor control and so leave an element of doubt when used for safety critical applications.

The present invention is concerned with resolving such doubts to maintain safe operation even when unpredictable operational faults may occur.

According to the invention there is provided a monitoring system for monitoring a microprocessor based control device in safety critical situations, said system including: first input means for receiving control information from the microprocessor based control device; second input means for receiving reference information also received by said control device; means for determining whether the control information from said device corresponds to that expected in view of the reference information, and means for overriding the control information if any error in this control information is detected.

Preferably checking means are provided to ensure the integrity of the monitor system is maintained.

The system is preferably ROM based and received errors cause the memory to be addressed at a location containing overriding information.

The invention will now be described by way of example with reference to the accompanying drawings in which:

Figure 1 shows the monitor in conjunction with a microprocessor control;
Figure 2 shows an embodiment of the monitor in greater detail;
Figure 3 shows the input handling configuration;
Figure 4 shows the allocation of information with respect to the EPROM;
Figure 5 shows a table of operational conditions;
Figure 6 shows parity check aspects;
Figures 7 to 9 show signals associated with the monitor;
Figure 10 shows parity circuit aspects in greater detail;
Figure 11 shows oscillator and delay circuit details;
Figure 12 shows lockout circuit aspects;
Figure 13 shows input and EPROM output for shutdown;
Figure 14 shows a Main error from the PLC;
Figure 15 shows a timer configuration; and
Figures 16 to 19 show timing diagrams.

The Figure 1 configuration shows a PLC (programmable logic controller) 10 which is microprocessor based and would normally directly control the operation of burner plant in dependence on the input signals received from interlocks 1-5. In this new configuration however, the

control outputs from block 10 are not directly connected to the plant at terminals 30-34 but are connected in series with the safety monitor 25 using lines 17-21. The monitor also receives the interlock information via lines 12-16. The monitor can be broadly considered as having a first portion 25A which actually monitors the sequencing of the plant interlocks to check that the outputs from control 10 are as expected and if not then the monitor can itself initiate a control function to eliminate any potentially dangerous situation. The output control function is represented by the relay contacts RL1-RL5 of portion 25B. The monitor 25 is not provided to normally control the plant but to override control to initiate shutdown for example. Thus the monitor can be considered an 'active' monitor rather than merely being passive, as it can control the set of relay contacts RL1-5. This monitor contains the patterns for the PLC and expected plant outputs relating thereto at each stage of the sequence, e.g. pilot, ignition or fan operation dependent on thermostat and flame presence for example. If the monitor agrees with the status observed then it closes the appropriate relay contacts RL1-5 allowing the status of the outputs on lines 30-34 to mirror those received from the PLC. If the safety monitor dissagrees with the plant and PLC outputs then it will typically open all relay contacts initiating a plant shutdown in the event of PLC and plant interlock failures.

A more detailed embodiment of the monitor is shown in Figure 2. The plant interlocks 1-5 of Figure 1 and the PLC outputs are received as a.c. inputs on the lines 12-16 and 17-21 respectively and fed via resistors R1-R5 and R6-R10 to opto-isolator 40 (eg. 5 x dual opto-isolator type ILD 74). These resistors limit the current to a few milliamps which flows back through the common neutral 22. The isolated outputs are fed to buffers 41 prior to receipt by the EPROM 43 which is

at the heart of the monitor system. One pair of opto-isolators with associated buffers is shown in more detail in Figure 3.

Diodes D1 and D2 bypass the opto-isolator light emitting diodes (LEDS) forming part of the isolator chip IC1a on the non-conducting cycle of the a.c. input.

The collectors of each opto-isolator transistor forming the receiving part of chip IC1 feeds the input of the Schmitt inverted buffer (e.g. type 40106). When the input is active then the input to the Schmitt is pulled low by the conduction through the transistor. Also on the collector of each transistor is an RC network C1/R20 and C2/R19 connected up to +5v. This serves two purposes. The first is that it pulls the inputs of the Schmitt inverters up to supply rail (+5v) potential. Secondly, because the inputs are a.c. then when an input is active, the opto-isolator collector is switching between 0v and 5v at the a.c. input rate. This would cause the Schmitt to be flipping between logic states. The RC network has a decay time chosen to be long enough to sustain the input to the Schmitt at low during the off periods, thus keeping the input active.

Similar opto-isolation and buffering is provided for all lines 12-21. The Schmitt inverters IC6a,b have an inbuilt hysteresis to remove noise on the lines to prevent spurious input state changes.

Returning to Figure 2, the buffered inputs are received on address lines A0-A9 of the EPROM (e.g. type 27128 having 16k locations).

Each location in the EPROM is accessible by a unique binary address code on the fourteen address lines A0-A13 and when a particular

location is accessed the data at that location is placed in binary form onto the eight data lines D0-D7.

The EPROM is therefore essentially a large look-up table, into which can be stored the allowed operations of the PLC. The remainder of the EPROM can be stored with shutdown instructions. The use of the four remaining address lines A10-A13 is under the control of counter 48. The five plant loads can be controlled by data lines D0-D4 which are used via relay driver block 45 to energise the coils of relays RL1-RL5.

The data line D6 is used to clock counter 48 (e.g. type 4040). The clocking signal is fed via the RC network R21/C11 which filters out any spurious signals and the Schmitt inverter IC7 sharpens the signal and also helps to remove noise. The counter will only clock on a negative edge and so the clock data line has to change from a 0 to 1 in order to clock the counter on. The D7 reset line output is received via an oscillator 46 and this oscillator output is used by the parity check circuit 49 to ensure the EPROM 43 output and associated driver 45 output is not at fault as explained in more detail later. Any errors cause lockout relay RL6 to actuate.

The parity check circuit 49 operates dynamically as explained in more detail below, to ensure that all internal monitor circuits are correctly operating, hence the need to check signals from the EPROM via the relay drivers. A comparison bit D5 is provided for use in this check. Whether the counter 48 is incremented by a clock signal from D6 or a reset signal from D7 or merely is held at its present position will depend on the actual values stored in the EPROM for data positions D6 or D7 at any given time.

The lines Q1-Q4 of counter 48 are used to access the higher address lines of the EPROM 43 and these counter outputs give sixteen possible address states so effectively dividing the memory into 16 separate look-up tables, each table being accessed dependent on the address combination of A10 to A13 at any given time. Each table will have 1Kbyte allocated.

Each table will be accessed in sequence as each stage of the burner operation progresses. This sequencing is determined by a clock signal being available as stored data at location D6 at any given time. Using the EPROM as the source of clocking signals is a safety feature which prevents incorrect sequencing arising from the PLC or elsewhere. Within any one of the 16 tables, the actual locations accessed therein will be dependent on the address combination resulting from the signals on address lines A0-A9.

Hence the EPROM is accessed by a 14 bit word which is a combination derived from the counter, the plant interlocks and the PLC. If the combination is an 'allowed' one, i.e. not in error, then that accessed location will provide an 8 bit word on data lines D0-D7, which will have been prestored to correspond to the instructions received from the PLC.

An erroneous combination will define an address within the EPROM which will have prestored data which will be output to result in shutdown or other remedial action.

A typical combination used to define the EPROM address is shown in Figure 4.

The plant interlocks Flame, APS (air pressure switch) and thermostat (Stat) are available to address lines A7-A9 respectively (via the opto-isolators and buffers of Figure 2). Address inputs A5 and A6 are unused in this example. Control information from the PLC for alarm, main and pilot valves, ignition and fan operation is received at addresses A0-A4 respectively (via the Figure 2 isolators and buffers).

The start-up sequence and operation for such a burner configuration is shown in the truth table of Figure 5. This illustrates what states the PLC and plant outputs should be in at each stage of the burner sequence. The sequence commences from shutdown through start, purge, pilot ignition, main ignition to full running till a change in Stat condition resulting in post purge.

For normal operation, the EPROM will mirror the PLC outputs and changes of the various signals will cause different locations within a given area to be accessed. When a sequence step is due this will be carried out as a result of a clock signal being stored as data which is output to D6 for incrementing the counter.

The safety checks including parity check will now be described in more detail with reference to Figure 6. There are various potentially possible failure modes within the monitor which are attributable to component failure. These could potentially be a logic gate failure, open or short circuit, or a bit corruption within a location of the EPROM. It is necessary to have a sufficiently fail safe circuitry within the safety monitor and this is achieved by means which include parity checking the date lines of the EPROM and relay drivers. A check is done on the date lines D0-D4 plus the comparison bit D5 of the EPROM. The parity circuit also checks the relay drivers for

determination of failure, open or short circuit.

For an even number of bits in a data byte, even parity means that there are an even number of logic 1's and logic 0's in the byte. Odd parity refers to there being an odd number of logic 1's or 0's. This means that in all locations of the EPROM, a comparison bit D5 can be programmed to preserve one sense of parity, in the case of this monitor it is odd parity.

As already mentioned, the data lines D0 to D5 are fed into relay drivers 45. The outputs of these relay drivers then go into the parity check circuit 49 as seen earlier from Figure 2. The parity check circuit is dynamic which means in this embodiment that it is fed with a square wave signal from oscillator 46 which acts to check that all the gates of the parity check are continuing to work correctly.

Since the parity of the EPROM is constant, then the output of the parity check circuit will be constant. The output of the parity checking circuit will in fact be the same as the square wave input. The same square wave is also fed through a delay circuit 51 and the outputs of the delay circuit and parity check are combined in an exclusive OR gate IC13c.

The period of the square wave is approximately 350μS. The delay circuit has a time delay of approximately 10μS The function of the exclusive OR is that when both inputs are the same level then the output of this OR gate will be zero, otherwise it will be at logic 1.

The pulses emerging from this exclusive OR gate are shown in Figure 7. These short 10μS pulses seperated by approximately 340μS pass into a

relay driver IC11g which then drives the lockout relay coil RL6. The relay driver inverts the pulses from the exclusive OR gate. The mark to space ratio of the resulting signal makes it sufficiently positive to not allow the lockout relay to be energised. However, the signal keeps sufficient charge in the diode pump circuit 53 to keep the reset signal low, thus not resetting the EPROM. The signal is shown in Figure 8.

Suppose now a bit failure occurs in the location of the EPROM being accessed which results in a parity error at that location. This will cause the output of the parity check circuit 49 to be inverted, which will consequently invert the output of the relay driver driving the lockout relay coil RL6.

This signal, shown in Figure 9, has a mark to space ratio which makes it sufficiently low to power the lockout relay coil, putting the safety monitor into lockout mode. Neither is it possible for the signal in Figure 9 to be able to maintain sufficient charge in the diode pump circuit, and consequently the reset will go high. The counter 48 will be reset and therefore the EPROM will reset back to the start in the event of lockout.

It is possible that a fault could be caused due to the failure of a relay driver going open or short circuit.

Because the parity checking circuitry is dynamic, then any failure of any component will also result in lockout. So all the failsafe circuitry is itself integrally failsafe.

The relay driver and parity check configurations can be provided

using the components of Figure 10. The six buffer/drivers IC11a-f (e.g. type ULN 2003N) receive the EPROM outputs D5-D0 respectively and these are inverting so that any of the relays RL1-R15 will be driven when the output of the buffer goes low or the associated data line goes high. A lockout contact and mode selector block 56 is shown connected to the common connection for relays RL1-5 and provides the supply voltage selection to the relays as described shortly.

The parity check exclusive OR gates IC12a-d and IC13a-b (e.g. type 4070) are cascaded and have their respective other input connected via resistor R27-R32 to the relay drivers. The last exclusive OR IC13b has its output connected to the exclusive OR IC13c as just described with relation to Figure 6. The oscillator 46 output is received at one input of IC12a to give the dynamic safety check.

So it can be seen that if the parity input is even then the output of the parity check circuit will be 0, and if odd then logic 1. However, because of the square wave from the oscillator, the output changes continually at the oscillator rate and so exercises all gates to detect potential faults. The failure of any one gate will be detected by the loss of the square wave signal at the output of the parity check circuit. Thus the parity circuit is itself failsafe.

Figure 11 shows a suitable oscillator 46 and delay 51 already mentioned in respect of Figure 6.

The oscillator is formed by NAND gate IC10d (e.g. type 4093) and R23 and C13. The output is available via R24 and transistor Q1 having a collector resistor R25. The oscillator output passes both to the parity check circuit 49 and the delay circuit 51 formed by the RC

network of R26 and C14 giving a time constant of approximately 10μS. The oscillator can be enabled and disabled by the EPROM data output D7 which passes via NAND IC10b and IC10c (this latter connected as an inverter). The delayed oscillator output goes to exclusive OR IC13c as already described in Figure 6 and now shown in detail in Figure 12. This gate also receives the oscillator output that has passed through the gates of the parity check circuit. After inversion via driver IC11g the signal passes through the winding of reset coil RL6 and the diode pump via transistor Q2. The pump comprises R34, C15-16 and D11-12 and R35-36 acting as a potential divider. The output passes to reset the counter 48 via Schmitt inverter IC7f (e.g. type 40106).

During normal non-lockout operation of the circuit the transistor Q2 spends the majority of its time turned off, and a relatively very short time turned on. Both these periods are determined by the oscillator frequency and the delay circuit time constant. During the on period capacitors C15 and C16 will charge up through Q2.

Capacitor C15 is approximately half the capacitance of C16 and so C15 will charge up to approximately twice the voltage on C16. During the long off period C15 will discharge through R34 and D11. C16 will discharge slowly through R35 and R36. However, when Q2 turns back on again it will start to charge C15 and C16 back up again. This results in charge being dumped across from C15 to C16, therefore increasing the volts across C16. So, on each 'on' cycle of Q2 the charge on C16 is ramped up, therefore, increasing the volts on C16, to a level sufficient to keep the input voltage to IC7f high enough so as not to give a reset.

However, when the signal into the base of Q2 is inverted so as to give

a lockout condition, then Q2 spends the majority of its time turned on, and a relatively short time turned off. This means that C15 and C16 have very little time to discharge. When Q2 turns back on again, very little charge is transferred into C16, so the voltage on C16 remains low and hance the input to IC7f is low, instigating a reset signal to the counter. The same effect would occur if Q2 spent all its time off, or all its time on.

If Q2 was permanently off C15 and C16 would eventually fully discharge leaving zero volts on the input to IC7f, so instigating a reset. This is the case when the EPROM disables the oscillator via its data line D7. When Q2 is permanently on, i.e. when a lockout occurs, no charge is transferred to C16. The voltage on C16 remains low thus causing a reset.

In addition the EPROM output on data line D7 will reset the counter when the D7 output goes low. This is achieved by disabling the oscillator (see Figure 11) via the NAND gate IC10b (e.g. type 4093) and the gate IC10c (connected as an inverter). If the oscillator is disabled then the square wave is removed and this causes the output of IC7f again to go high and reset the counter. The capacitor C16 and the resistors R35-R36 provide filtering to prevent spurious reset signals due to noise. R35-36 also act as a potential divider.

A manual reset can be provided at switch SW1 of Figure 12 and this acts to disable the oscillator of Figure 11.

The zener diode Z1 clamps the voltage to inverter IC10a to 4.7v. This is inverted to logic 0 and this disables the oscillator, and this passes via the diode pump to cause the output of IC7f of Figure 12 to

go high so resetting the counter. The switch SW1 of Figure 12 can also be used to actuate the reset coil of RL6 after a lockout condition.

There are two possible lockout modes dependent on the selection of the links shown in Figure 12. As already discussed, the exclusive OR gate IC13c compares the output of the parity check circuit and the delay circuit. IC11g then inverts the signal and drives the latching lockout relay reset coil. There are two modes of lockout selectable by links A1-2 and B1-2. The diode associated with these links is contained within chip IC11.

If links A1 and A2 are selected (made) then in the event of a monitor fault, e.g. a bit corruption in an EPROM location, then the relays RL1 to RL5 are all energised and so their contacts are closed allowing total PLC CONTROL OF THE PLANT. The monitor is effectively bypassed due to its own internal fault, but the PLC continues to control the plant.

Alternatively, if links B1 and B2 are selected then a monitor fault, such as the one mentioned above, will give plant shutdown, preventing PLC control of the plant. This is because all the relays will drop out isolating the PLC and initiating shutdown.

The latching relay will remain in this lockout state until the set coil of RL6 is powered and so returning to normal operating mode by manually actuating switch SW1 once the fault has been removed. A lockout indicator LED2 with an associated current limiting resistor R38 provides visual indication of lockout.

PLC error will result in reset and hence plant shutdown but not

lockout, so the above modes do not affect the action of the monitor when a PLC fault occurs.

A standard regulated mains power supply can be used to provide the 5v and 12v d.c. supplies.

As already described with relation to Figures 4 and 5, the EPROM within the monitor system will mirror the PLC outputs normally associated with the burner status at any given time (except when the PLC is experiencing a fault condition).

Figure 13 shows this mirrored output in the EPROM. The 5 inputs from the PLC correspond to the shutdown status and are equivalent to all binary zeros. APS and Flame will be zero and STAT may or may not be closed (represented by X). This corresponds to the first line of the table shown in Figure 5.

As already discussed, counter 48 output Q1-Q4 will control which of the 16 possible areas of the EPROM is accessed.

Within the given area the specific location is determined by the 10 bit word (or more correctly by the 8 variable bits of this word - A5 and A6 do not change). These 8 bits are defined by A9-A7 and A4-A0, viz STAT, APS, Flame, Fan, IGN, Pilot, Main and Alarm.

The data prestored at the defined location will be all zeros for D0-D4 as shown in Figure 13 - to mirror the PLC. Figure 14 shows an example of a situation when the PLC output is in error. This illustrates a fault condition where the Main output is erroneously energised during the pilot ignition stage, which is obviously highly undesirable.

This energising is represented by the logic 1 at the Main output received from the PLC. It is shown that Alarm is 0 (illustrating that the PLC itself has failed to notice this fault). Other inputs correspond to those of line 5 of Figure 5.

The location within the EPROM will have prestored data as shown in Figure 14 where all zeros are present except in the D0 (alarm) location. These zeros will cause the relays RL1-5 to open so de-energising the plant for example, as represented in Figure 1. The monitor can thus be seen to have safely dealt with a potentially dangerous situation.

As discussed above, the A5 and A6 inputs to the EPROM have not been used. In an expanded version of the monitor system one or both of these can be employed to ensure that minimum or maximum timing of events within the burner sequences are within desired limits. To achieve this, external timers can be connected to the monitor system as shown in Figure 15.

Three timers T1,T2,T3 are incorporated and are powered from the high air proving switch, the pilot valve supply and the main valve supply respectively.

The timer T1 will check that the minimum purge time is satisfied, say 30 seconds. Timer T2 will check that the maximum time for pilot ignition is not exceeded. Timer T3 will check that the Main ignition time does not exceed the maximum allowed time.

When the high air limit switch on the modulating unit makes, the timer T1 is powered. After 30 seconds, the timer will time out and the

contact T1/1 will close. This will then set the check input to logic 1 (active). The check input going to a logic 1 can then be used as a check that the purge time was at least 30 seconds duration. This is illustrated in the Figure 16 waveforms. The EPROM can thus be pre-programmed with the correct state of the check input at each stage of the burner sequence. If there is a discrepancy, appropriate action can be initiated.

If the high air purge is less than the minimum time then power will be taken off T1 before it can time out, so the check input will not go high. The check input can be used as a clocking condition, so that if incorrect timing results, the EPROM is accessed at the wrong location, and shutdown will result.

This is illustrated in Figure 17. Here, because the check input has not gone high, the EPROM will not be stepped on. This has therefore checked the length of the purge.

The next time that can be checked is the pilot ignition time to confirm it does not exceed 5 seconds. Figure 18 shows the effect of an extended pilot ignition time. The ignition is on at the same time as the check input which means the pilot ignition period has exceeded 5 seconds.

This address can be pre-programmed as disallowed in the EPROM, and can contain a shutdown instruction. If the pilot ignition period is less than 5 seconds then the address word would be allowed, as shown in Figure 16.

The Main ignition time can be checked on timer T3 as seen from Figure

16. This timer is energised when the main valve output is energised and will then time out after 5 seconds, by which time the pilot should have been extinguished. However, if the pilot stays on for longer than 5 seconds, then when timer T3 times out, the pilot output will still be energised. This is shown in Figure 19. This can be pre-programmed as a disallowed address and so contain a shutdown instruction.

This configuration has thus checked the purge time, pilot ignition time and the Main ignition time.

The timers can be configured by standard preset solid state timers. If any timer should fail then any error will be picked up by the check input of the EPROM address line and appropriate action instigated.

The EPROM used in the monitor system can be pre-programmed with data at its various locations using standard techniques or by the use of a short program.

CLAIMS

1. A monitor system for monitoring a microprocessor based control device in safety critical situations, said system including :-

first input means for receiving control information from the microprocessor based control device;
second input means for receiving reference information also received by said control device;
means for determining whether the control information from said device corresponds to that expected in view of the reference information, and means for overriding the control information if any error in this control information is detected.

2. A system as claimed in claim, wherein the determining means includes a memory for storing binary data accessable in dependence on information received from the first and second input means.

3. A system as claimed in claim 2, wherein the memory comprises a ROM for receiving information derived from the control device and said reference information so as to address locations therein.

4. A system as claimed in claim 2 or 3, wherein the memory is configured to contain information mirroring the control device information and to contain overriding information, the information mirroring the control device information being located at addresses accessible during normal operation of the control device and the overriding information being located at addresses accessible during an error phase of the control device.

5. A system as claimed in claim 4, including selector means, and wherein the memory has sufficient capacity to store additional sequencing information for receipt by the selector means to cause different memory areas to be made available to the control device information and reference information.

6. A system as claimed in claim 5, wherein the selector means includes a counter, and wherein feedback means are provided from the data bus of said memory to reset or increment the counter in dependence on preprogrammable instructions within selected memory storage locations.

7. A system as claimed in any of one of claims 2 to 6, wherein the first and second input means include opto-isolators for electrically isolating the inputs and including buffers for converting the inputs to a level suitable for the address bus of the memory.

8. A system as claimed in any one of claims 2 to 7, wherein the second input means are configured to receive thermostat, air status input and flame presence information from a burner device.

9. A system as claimed in any one of claims 2 to 8, wherein the first input means is configured to receive fan, ignition, pilot, main, nd alarm information from the control device for burner control.

10. A system as claimed in any one of claims 1 to 9, including checking means provided to ensure the integrity of the monitor system is maintained.

11. A system as claimed in claim 10, wherein the checking means

include a dynamically operable check circuit for continually checking system integrity.

12. A system as claimed in claim 11, including a controllable oscillator for dynamically exercising the parity of the check circuit and a lockout device for initiating operational lockout in the event of a detected failure.

13. A system as claimed in claim 12, wherein the oscillator is controlled by an output provided by the determining means.

14. A system as claimed in claim 12 or 13, including at least one relay and a relay operating circuit under the control of a signal derived from the oscillator to establish the integrity of the at least one relay.

15. A system as claimed in claim 14, wherein the at least one relay includes a bistable lockout relay having a first coil operable to a lockout condition on receipt of an error detection signal from the parity check circuit, said relay being resettable by means of a second coil.

16. A system as claimed in any preceding claim, including relay means operable in dependence on an output derived from the determining means to interrupt the passage of control information from the control device to a remote location.

17. A system as claimed in claim 16, wherein the relay means are operable to by-pass the monitor in the event of monitor failure.

18. A system as claimed in any preceding claim, including timer means operable to provide reference sequencing information for use by the determining means.

19. A monitor system for monitoring a microprocessor based control device substantially as described herein with reference to the accompanying drawings.

Published 1988 at The Patent Office, State House, 66/71 High Holborn, London WC1R 4TP. Further copies may be obtained from The Patent Office, Sales Branch, St Mary Cray, Orpington, Kent BR5 3RD. Printed by Multiplex techniques ltd, St Mary Cray, Kent. Con. 1/87.