

[54] **COMPUTER BASED PLANT PROTECTION SYSTEM**

[75] Inventor: **Jack Ascher Schuss**, West Hartford, Conn.

[73] Assignee: **Combustion Engineering, Inc.**, Windsor, Conn.

[22] Filed: **Nov. 2, 1972**

[21] Appl. No.: **303,239**

[52] U.S. Cl. **431/24**

[51] Int. Cl. **F23n**

[58] Field of Search 431/24, 25, 26; 60/105

Primary Examiner—Carroll B. Dority, Jr.
Assistant Examiner—Harold Joyce

[57] **ABSTRACT**

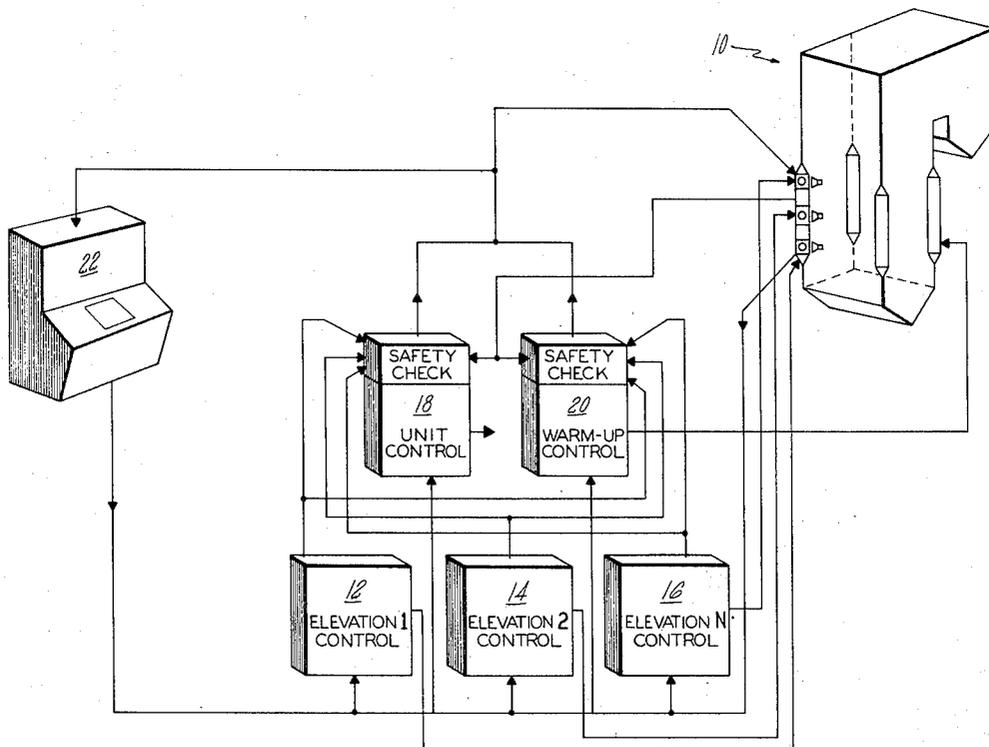
A plant protection system and technique utilizing a plurality of programmable controllers interconnected in a hierarchy arrangement is disclosed. A first plurality of "lower" level controllers receive signals commensurate with groups of sensed process parameters and employ these signals to generate safety-check signals indicative of the state of that portion of the plant with which each individual controller is associated. These safety-check signals are delivered to each of a pair of "higher" level programmable controllers which redundantly compute the need to terminate the entire process; the "higher" level controllers also checking the operability of the lower level controllers and the lower level controllers "voting" in the process termination computation.

4 Claims, 5 Drawing Figures

[56] **References Cited**

UNITED STATES PATENTS

3,258,053	6/1966	Schuss	431/29
3,324,927	6/1967	Staring	431/24 X
3,684,423	8/1972	Bryant	431/24
3,715,180	2/1973	Cordell	431/25
3,741,246	6/1973	Braytenbah	60/105



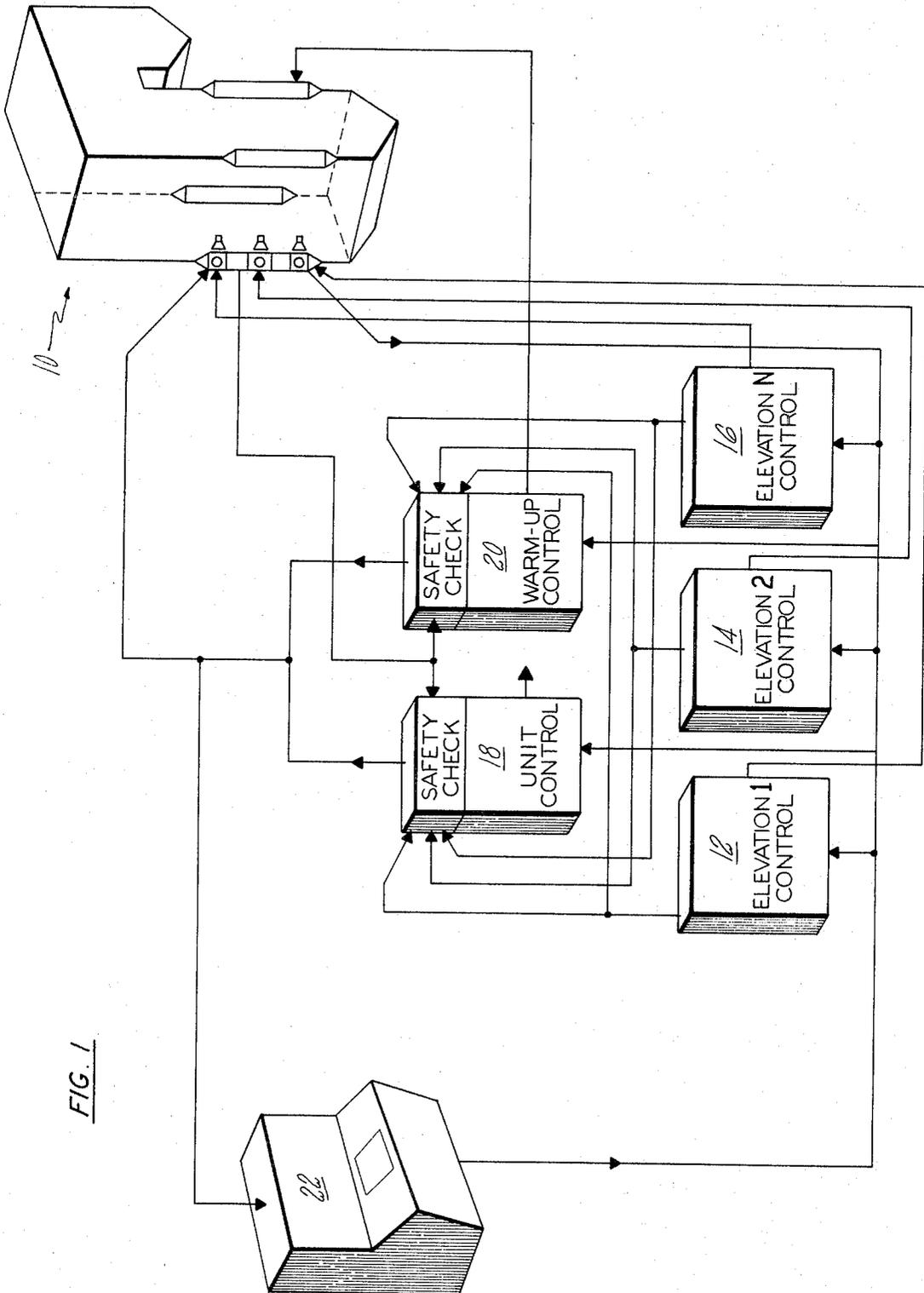
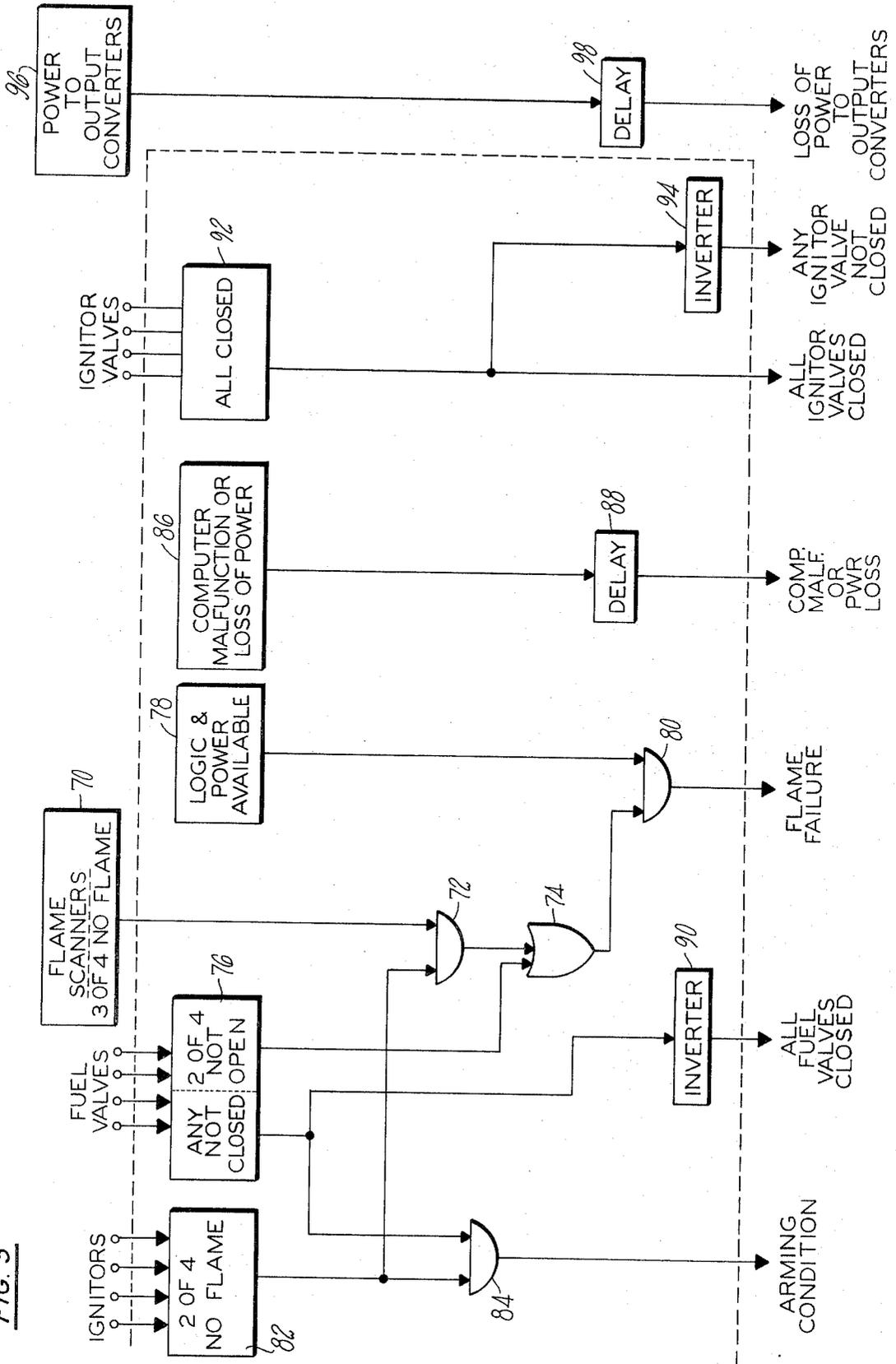


FIG. 1

FIG. 3



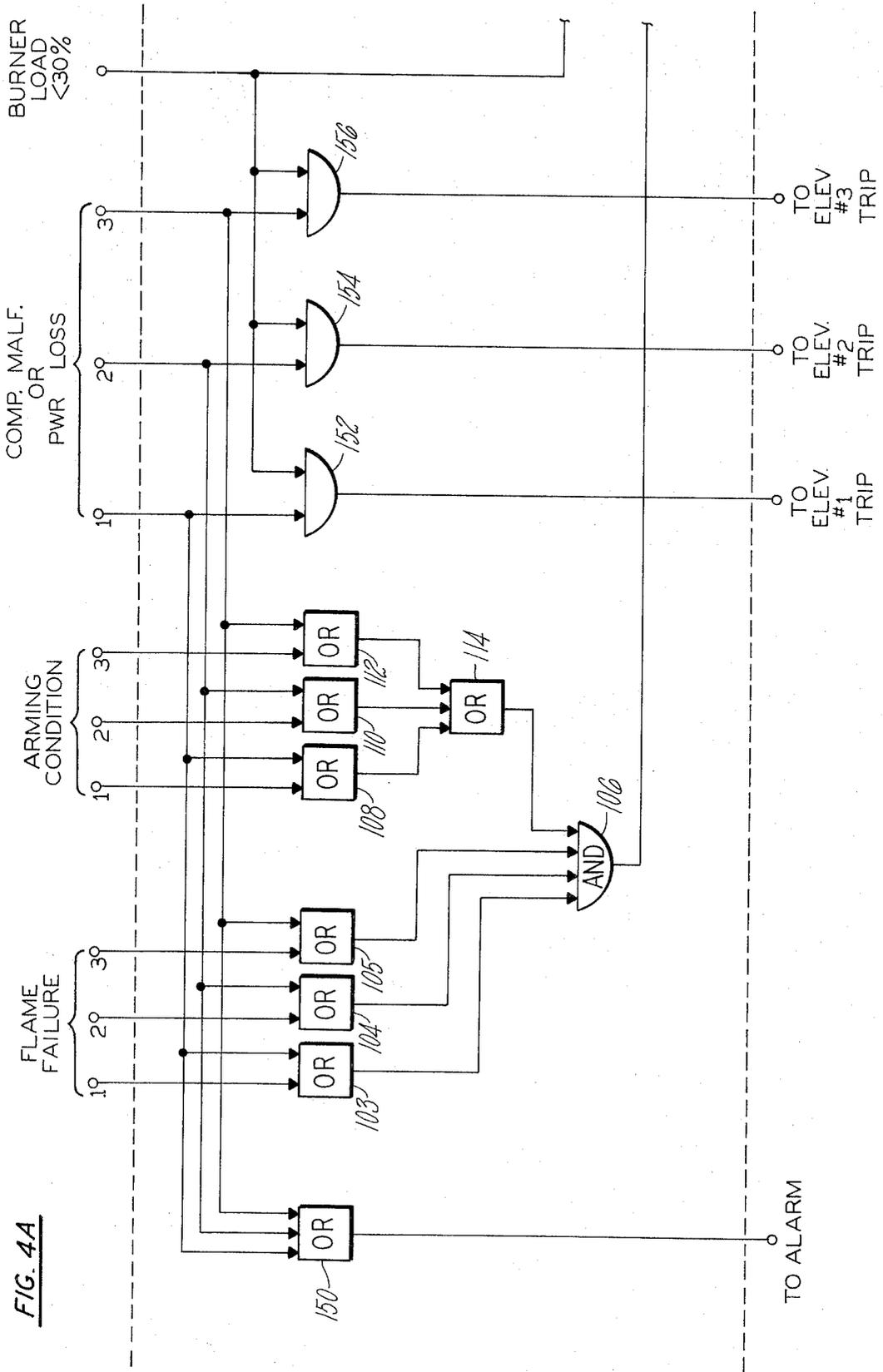
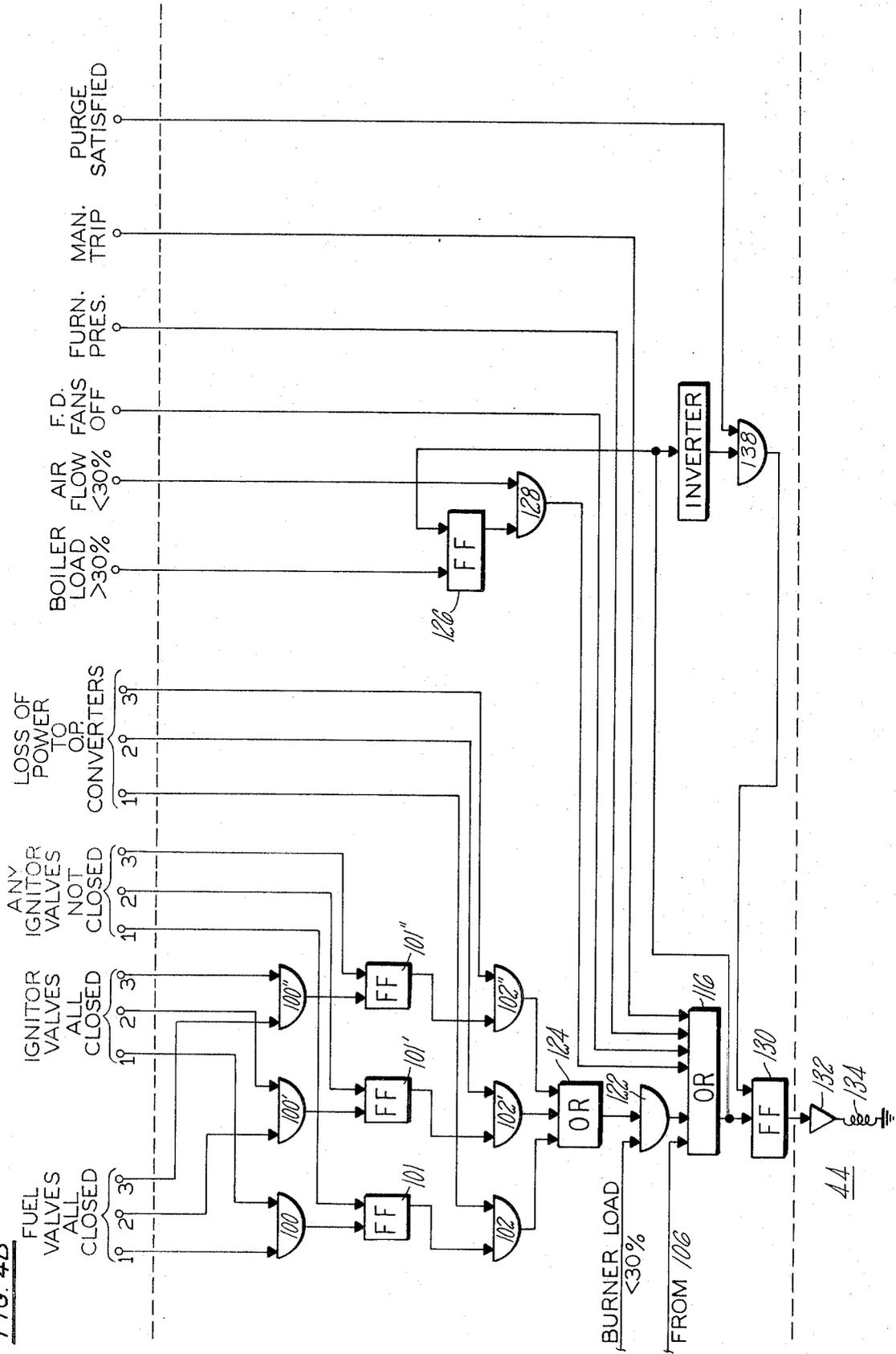


FIG. 4A

FIG. 4B



COMPUTER BASED PLANT PROTECTION SYSTEM

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to the control of vapor generators and other devices of similar character. More specifically, this invention is directed to a digital burner control system for enhancing the safety of operation of steam and other vapor generators. Accordingly, the general objects of the present invention are to provide novel and improved methods and apparatus of such character.

2. Description of the Prior Art

While not limited thereto in its utility, the present invention is particularly well suited for use in and as a burner control system for a fossil fueled furnace of the type employed by electrical utility companies to generate steam for driving turbines. Accordingly, solely for purposes of explanation, the invention will be described in the environment of a burner control system and will below be contrasted with prior art burner controls.

These safety requirements for operation of the furnace of a vapor generator are generally outlined in U.S. Pat. No. Re26,167 issued to Jack A. Schuss and Virginius Z. Caracristi. U.S. Pat. No. Re26,167 depicts a burner control system employing a "hard wired" approach of the type that has in recent years become standard in the industry. As an alternative to the "hard wired" type control, efforts have been made to assign the vapor generator safety supervision function to a suitably programmed, large general purpose computer already physically situated at an appropriate location and performing other plant operation associated functions. For the reasons to be discussed briefly below, both the "hard wired" and general purpose computer control system concepts have inherent disadvantages which have produced a desire in the art for an improved burner control system.

Considering further prior art "hard wired" controls, both electromechanical relays and solid state switching devices have been employed. While "hard wired" controls have the attribute of relatively low initial cost when compared to other previously available systems, with the exception that the requirements for filtering out noise and other transients have substantially increased the cost of solid state switching systems, such "hard wired" controls have imposed a number of undesirable limitations on the designer and user. Thus, by way of example, since all "hard wired" systems must be manually fabricated and installed, component damage resulting from wiring mistakes in the manufacturing and simulation stages has been unavoidable. Further, shop simulation of "hard wired" systems is inefficient and expensive due, in part, to the need to follow a substantial number of wiring diagrams which themselves are generated at a rather high cost. A closely allied problem is the need to update all of these wiring diagrams after each logic modification or correction found necessary during simulation or in the field during installation and checkout. Once installed, modification of a "hard wired" control system is exceedingly difficult and, of course, such controls are for all practical purposes inflexible. Also, the increases in reliability achievable through the use of redundant circuits can be

achieved in a "hard wired" control only at comparatively high cost and the incorporation of some means for self-checking the control system and its components is exceedingly difficult.

The use of a plant installed general purpose computer for specialized control sub-loops such as burner controls also possesses serious disadvantages. Bearing in mind that so-called "nuisance shutdowns" are extremely expensive to an electrical utility, use of a single large expensive general purpose computer, perhaps with an equally expensive back-up computer, poses obvious functional and economic disadvantages. Thus, by way of example, a failure in the computer or the power supply thereto totally unrelated to the equipment under control supervision would result in a "nuisance shutdown" in a system employing a single computer.

To summarize, the art has long needed a flexible and reliable method of exercising control over the furnace of a vapor generator or similar apparatus. The principal attribute and objective of such an improved control must be the virtual elimination of "nuisance shutdowns" and in achieving this objective it is desirable that the control system additionally be comparatively inexpensive, easy to install, include a self-checking feature, and directly interface with existing computer equipment to facilitate the monitoring of control system performance.

SUMMARY OF THE INVENTION

The above discussed and other desirable features of a control system are achieved by the present invention through the use of a plurality of small, general purpose, programmable digital computers which are interconnected in a unique manner so as to perform all of the logic functions required of the control system.

In accordance with the invention, groups of interrelated plant process parameters are sensed and signals commensurate with the sensed parameters of each group are supplied to separate controllers of a first plurality of programmable controllers. The controllers of the first plurality generate output signals indicative, from a safety standpoint, of the instantaneous state of that portion of the plant process being monitored by each controller as represented by the signals of each group. The "safety" signals provided by each programmable controller of the first plurality are delivered as inputs to second and third controllers; the second and third controllers being programmed such that the "safety" signals provided by the controllers of the first plurality have a "vote" in a computed decision as to whether the process should be terminated. Thus, the two "higher" level or second and third controllers redundantly solve safety-check equations based upon information provided by a first plurality of independent lower level programmable controllers and, in so doing, check on the operability of the lower level computation devices.

BRIEF DESCRIPTION OF THE DRAWING

The present invention may be better understood and its numerous objects and advantages will become apparent to those skilled in the art by reference to the accompanying drawing wherein like reference numerals refer to like elements in the several figures and in which:

FIG. 1 is a system block diagram depicting a preferred embodiment of the present invention;

FIG. 2 is an electrical block diagram depicting the means by which power for operation of the invention is delivered to the embodiment of FIG. 1;

FIG. 3 is a functional block diagram of one of the "elevation controls" of the embodiment of FIG. 1; and

FIGS. 4a and 4b comprise a functional block diagram of one of the redundant "safety check" controls of the FIG. 1 embodiment.

DESCRIPTION OF THE PREFERRED EMBODIMENT

With reference to FIG. 1, a block diagram of a preferred embodiment of a control system in accordance with the present invention is shown. FIG. 1 depicts the invention in the environment of a burner control system for the furnace of a vapor generator; the furnace or boiler being indicated generally at 10. For purposes of explanation, boiler 10 will be presumed to comprise three burner elevations each consisting of a plurality of burner nozzles; a typical elevation having a burner nozzle at each corner of the furnace. As is known, and as explained in referenced U.S. Pat. Re26,167, in the operation of a vapor generator steps must be taken to guard against the admission of fuel to the burners and thence into the furnace chamber when there is no flame for providing sufficient ignition energy to ignite and burn the fuel. The injection of unignited fuel into the furnace chamber would result in the creation of a highly explosive furnace atmosphere.

Conceptually, the present invention contemplates the functional separation of the burner system by firing elevations. In the normal operation of most vapor generators an entire elevation of burners is introduced into or removed from service as the load demand requires. Thus, by controlling the burner elevations separately, reduced capacity operation may be achieved if desired or if necessary as might be the case should there be a malfunction at one elevation; fuel to the burners at the elevation having the apparent malfunction being discontinued. Thus, in accordance with the invention, the requisite operational parameters at each burner elevation are sensed by means of suitable condition responsive devices and associated transducers and the informational signals thus generated are delivered to a plurality of "computers;" there being a separate "computer" corresponding to each burner elevation. In FIG. 1 these "computers" are indicated at 12, 13 and 16. For the purposes to be described below, a control system in accordance with the present invention employs additional "computers" 18 and 20. All five "computers" will usually be identical and will comprise small, general purpose, stored program digital computers comprising a memory, central processor, registers and signal conditioning circuitry. While the term "computer" has been employed in a generic sense, it will be understood that the devices 12, 14, 16, 18 and 20 are in fact programmable controllers having logic capability but without the complete arithmetic capability of a general purpose computer. Thus, the "computers" of the present invention are comparatively inexpensive devices capable of executing a control program to perform a variety of control functions.

The inputs to each of "computers" 12, 14 and 16 include, as noted, operational parameters associated with the corresponding furnace burner elevation. Thus, considering one elevation of a four burner furnace configuration, the corresponding "computer" will receive

input signals commensurate with a plurality of sensed conditions indicative of the operational state of each burner nozzle at that elevation. These input signals will be in the form of binary 1's and 0's and will be generated by limit switches, differential pressure type switch devices, optical flame scanners, etc. In the case of an oil fired burner, the various switches for providing the input signals commensurate with the operation of each burner are shown in FIG. 2 of U.S. Pat. No. 3,258,053 issued to J. A. Schuss. The optical flame scanner input associated with each burner is shown in FIG. 4 of referenced U.S. Pat. No. Re26,167. The normal operation of each of computers 12, 14 and 16 is commensurate with the functions performed by the prior art "hard wired" systems as exemplified by the combined teachings of U.S. Pat. Nos. 3,258,053 and Re26,167; U.S. Pat. No. 3,258,053 being directed to the logic associated with one "corner" of a four corner or four burner nozzle elevation. Thus, each of "computers" 12, 14 and 16 is programmed such that a portion of its capability supervises an elevation during normal start-up and shut-down. "Computers" 12, 14 and 16 provide output control signals for delivery, via appropriate signal conditioning equipment, to the various burner drive actuators and valves.

The "computers" 18 and 20 perform, as will be described in detail below, a redundant "safety check" operation on the entire burner control system and respectively exercise "unit" and "warm-up" control for the furnace. "Unit control" computer 18 supervises furnace purging, main fuel shut-off valve operation, air flow volume monitoring, boiler feed water supply monitoring, auxiliary air damper control, etc. The warm-up control function is exercised in the manner well known in the art, by "computer" 20 over a plurality of independent burners situated at the lowest elevation in furnace 10. Through temperature monitoring at the gas outlet of furnace 10, the "computers" 12, 14 and 16 will be "enabled" in the proper sequence only when the warm-up is completed. The "start-up" commands to computers 12, 14 and 16 may be generated manually from a control panel in a control console 22 or automatically under the command of "unit" control computer 18.

As noted, apparatus in accordance with the preferred embodiment of the invention also includes a master control console 22. The control or operating console 22 has the capability of monitoring the operation of the entire burner system and includes control switches for selectively initiating and/or discontinuing the firing of each burner elevation via "computers" 12, 14 and 16. This, of course, gives the system the ability to operate the furnace at less than full power output.

With reference now to FIG. 2, a partial block diagram depicting the embodiment of FIG. 1 in more detail is presented. FIG. 2 particularly shows the means by which power is delivered to the "computers;" only "computers" 18 and 20 being depicted in the interest of facilitating understanding of the drawing. FIG. 2 also depicts the routing of the input and output signals to and from the "computers." The power supply for the embodiment of FIGS. 1 and 2 includes two independent alternating current sources 24 and 26; the source 24 being the normal supply and source 26 being a stand-by supply. The power supply system also includes an automatic switching device 28, of a type well known in the art, which automatically switches to the stand-by

source on failure of the normal a.c. supply. Additionally, the system includes a direct current supply 30 for providing power to a total unit trip if a multiplicity of failures occur in the system.

Alternating current from the power source selected by switch 28 is delivered to ten fused conductors and a single unfused branch conductor. Of the fused branch conductors, branches 32, 34, 36, 38 and 40 supply power for respective individual "computers" 20, 18, 16, 14 and 12. The other five fused branch conductors supply power, through computer interface devices, to the output devices driven under control of the various "computers." Thus, by way of example, fused branch conductor 42 provides power, via a plurality of output signal converters 44 associated with "computer" 18, for driving the actuator of the main fuel shut-off valve of furnace 10 and various other devices; the actuators controlled by "computer" 18 being indicated generally at 46. The unfused a.c. branch conductor 48 provides power directly to the input signal converters, such as signal conditioning devices 50 of "computer" 18, of each of the five "computers." In the manner well known in the art, and not shown in FIG. 2 in the interest of clarity of the drawing, an under-voltage device such as a voltage sensitive relay is placed in parallel with the other output converters of each of the five "computers" and the loads on the converters. The output signals derived from such under-voltage devices are indicative of the availability of power to drive the actuators 46. Internal "watchdog" circuitry in the "computers" provides additional signals commensurate with the operational integrity of the "computers." These additional signals are routed through their associated "computer" thereby enabling monitoring of "computer" response through each "computers" output converter and permitting the checking of the performance of the "computer" as well as the state of its associated power supply and the input power thereto. Since all of the input signal converters are fed from a common unfused alternating current supply, selected input data may be delivered to duplicate input converters thereby facilitating selective redundancy of the system. The common power supply line to the input converters is unfused because it would be undesirable to immobilize the system and possibly trip the boiler in the unlikely case of an overload on one of the input devices; the input devices inherently not being susceptible to overload damage themselves. The direct current power supply 30 is delivered, via conductor 52, to the main safety trip for the boiler via the series connected contacts 54 and 56 of a pair of time delay relays; the time delay provided by these relays being needed to prevent unit trip when power is switched from a.c. source 24 to source 26. In the manner well known in the art, the main boiler trip may comprise an "energize-to-trip" master fuel relay which controls closing of a main fuel valve and the shut-down of the turbines associated with the furnace and other auxiliary equipment. Switches contacts 54 and 56 are normally opened and are controlled, in the manner to be described in detail below, via respective time delay relay solenoids 58 and 60 and associated driver amplifiers 62 and 64 from the outputs of "computers" 18 and 20.

Before describing the function and interconnection of the individual computers, as shown in the functional block diagrams comprising FIGS. 3 and 4, the control of a typical furnace burner elevation will be briefly de-

scribed. For a further and more detailed description reference may be had to copending Application Ser. No. 214,877 filed Jan. 3, 1972, now U.S. Pat. No. 3,781,161 issued Dec. 25, 1973, by J. A. Schuss and assigned to the same assignee as the present invention. Considering an oil fired furnace of the type depicted schematically at 10 in FIG. 1, a typical elevation may comprise four oil guns and associated ignitors. The oil guns are designed for mechanical atomization of fuel delivered to the furnace. The supply line to each individual oil gun is equipped with a manual shut-off valve, a power operated shut-off valve and a pressure switch. The pressure or gun proving switch indicates pressure loss downstream of the shut-off valve such as caused by leakage, a faulty coupling or a bad tip condition. Each oil supply line also includes a purging steam connection; the purging steam supply also being equipped with a power operated shut-off valve, a check valve, and a manual shut-off valve. Each of the oil guns further includes a gun retract mechanism, which is used to back the guns out of exposure to high furnace temperatures when not in use, and associated limit switches.

The oil guns and ignitors for a given elevation are controlled by the same functional subloop; that is by the same "computer." When operating condition prerequisites are satisfied by the "unit" and "warm-up" controls, a control signal may be generated which first starts the ignitors and thereafter the associated oil guns. It is a primary pre-requisite of the system that the ignitors go into service first and their operation be proven. No ignitor, however, is allowed to go into service unless its flame proving differential pressure switch is properly functioning and initially providing a "no flame present" signal. The "start-up" command also energizes the ignitor air booster fans and may be employed to cause the associated air dampers to be released to their analog controls for modulation. Once ignition is established, the individual oil guns will be placed in service in sequence with each oil gun being monitored to make sure that all "start-up" pre-requisites are satisfied. Thus, should the start-up pre-requisite be satisfied, the oil gun will be advanced into the furnace and, when advance is completed, the oil supply valve will be opened.

When sufficient time has elapsed to place all oil guns on the particular elevation in service, the number of apparently malfunctioning oil guns is counted and if the number exceeds tolerable limits, the entire elevation is shut-down. Oil gun shut-down for an individual elevation is accomplished in a manner similar to start-up and under the control of the associated "computer." However, if the decision to shut-down an individual elevation is predicated upon an apparent malfunction, as opposed to a desire to reduce power commensurate with boiler load as represented by an operator generated command at the control console, the undesired or "computer" controlled shut-down is "memorized" and an alarm triggered so that the plant operator will be alerted to take appropriate corrective action. When an elevation shut-down signal is generated, the ignitors are reenergized to support the scavenging cycle and the oil guns are removed from service in a sequential manner. The shut-down procedure includes complete purge of each oil gun. When purge is completed the oil gun is automatically retracted. At the end of the total elevation purge cycle, the ignitors are removed from service.

With reference now to FIG. 3, a functional block diagram of the flame failure logic of each of "computers" 12, 14 and 16 is shown. These "computers" as well as "computers" 18 and 20, are programmable controllers designed to perform sequencing, counting, logic and timing functions. Thus, by way of example, the "computers" of the present invention may comprise Type 084 controllers available from Modicon Corporation, Bedford, Mass.; these controllers including a random access memory, central processor, registers and signal conditioning equipment as shown schematically in the case of "computer" 18 in FIG. 2. Input and output signal conditioning equipment such as converters 50 and 44 associated with computer 18 provide the necessary isolation for each input signal level and adapt it to the requirements of the computer logic and provide the requisite power for driving output devices via the power supplies.

As previously noted, each of computers 12, 14 and 16 is identical and performs identical control and supervision functions with respect to a separate burner elevation in furnace 10. FIG. 3 is a functional block diagram of the safety logic portion of any one of the three elevation control computers presuming a furnace system which incorporates four burners at each elevation. The elevation control computers, in addition to normal control functions which do not comprise part of the present invention, provide flame failure protection and arming condition monitoring and generate output signals commensurate with achievement of arming, existence of flame failure, "computer" malfunction or power failure and loss of power to the actuators driven by "computer" generated control signals. Considering first the flame failure protection logic, whenever any three of four flame scanner associated switching devices indicates "no flame" and any two of four ignitor ignition energy monitoring switches indicates loss of ignition energy signals will be generated respectively by the scanner electronics 70, which includes a counter and associated logic as is well known in the art, and the computers internal counting logic 82. These signals are applied to an AND gate indicated schematically at 72. The output of AND gate 72 is OR'ed in an OR gate 74 with a deficient valve count signal. The deficient valve count signal is generated by computer internal counting circuitry 76 if, in the example being discussed, any two of the four burner fuel control valves is not indicated as open. The output of OR gate 74 and a signal indicative of the availability of power and computer logic operability from further computer internal circuitry 78 are applied to a further AND gate 80 to generate a signal commensurate with a flame failure condition. As will be described in more detail below, this "flame failure" signal is applied as one of the inputs to the safety check logic of computers 18 and 20.

Each of the "computers" 12, 14 and 16 also provides, via a voltage sensitive device 86 similar to and connected in the same manner as time delay relays 58 and 60, an output signal commensurate with either a computer malfunction or failure of power to the computer.

The elevation control "computers" also provide "arming condition" signals. Computer counting circuit 82 provides an output signal if two of the four ignitor monitor differential pressure responsive switches indicate that there is insufficient ignition energy. This signal is applied to an AND gate 84. Also applied to AND

gate 84 is a signal indicating that any fuel valve has started to open (any fuel valve not closed) as provided by counting circuitry 76. The output of AND gate 84 is a signal which enables the flame failure logic in "computers" 18 and 20; the output of gate 84 thus being a further input to the safety check logic of each of computers 18 and 20.

For the purposes to be explained below, the individual elevation "computers" may also provide signals to the safety check logic commensurate with the conditions of all fuel valves closed, all ignitor valves closed and any ignitor valve not closed. The signal indicative of all fuel valves closed is generated by inverting, in an inverter circuit 90, the "any not closed" signal provided by logic circuitry 76. A signal commensurate with the condition of all ignitor valves closed is provided by "computer" internal logic circuitry 92 and this signal is inverted in an inverter 94 to provide the signal commensurate with the condition of any ignitor valve not closed.

A signal indicative of a loss of power to the elevation "computer" output converters and thus also to the driven devices is provided by an undervoltage device 96 which does not form part of the elevation "computer" and this signal is delivered, via a time delay device 98, to the safety check logic. The undervoltage device 96 monitors the power to the output converters and driven devices. As noted above, the supply of power to the computer is monitored through self-checking circuitry 86 to provide a signal commensurate with the operative state of the computer itself and its internal power supply. Thus, in effect, circuitry 86 monitors the fused power lines to the "computers" while devices 98 monitor the fused power lines to the output converters.

Referring now to FIGS. 4a and 4b, a functional block diagram of the safety check logic portion of "computers" 18 and 20 is shown. The six output signals from the "elevation computers" 12, 14 and 16, as discussed above and indicated on FIG. 3, and the "loss of power to output converters" signal are applied to each of the safety check "computers" 18 and 20. As may be seen from FIG. 4, in addition to the input signals provided by or through each of the elevation "computers," each of "computers" 18 and 20 also receives signals commensurate with boiler and burner load, furnace air flow, the state of the furnace forced draft fans, violation of the furnace pressure limit and violation of the furnace purging requirements. In addition, the "trip" function signal provided by the safety check logic is fed back as a further input to "computers" 18 and 20.

In the safety check logic the signals commensurate with the condition of all ignitor valves closed at elevations 1, 2 and 3 are applied to respective AND gates 100, 100' and 100''. Also applied to gates 100 are the signals commensurate with the condition of all fuel valves closed. The output of AND gates 100 are employed to reset respective bistable circuits 101, 101' and 101''. Bistable circuits 101 are set by the signals commensurate with any of the ignitor valves not being closed. Upon being set, bistable circuits 101 provide a first input to respective further AND gates 102, 102' and 102''. The second input to each of gates 102 is the signal commensurate with the interruption of the supply of power to the "computer" output converters at the associated elevation. The output of AND gates 102 are thus signals commensurate with the loss of power

to the actuators operated under control of the associated elevation "computers" during a start-up. These signals are employed in the manner to be described below.

A signal commensurate with burner load, typically measured as a percent of maximum fuel pressure, is sensed by means which does not comprise part of the present invention. When this signal indicates that the burner load is less than 30 percent an enabling input is delivered to AND gate 122. A second input to gate 122 is derived from an OR gate 124 which has, as its inputs, the signals commensurate with loss of power to the driven devices at each elevation as provided by AND gates 102. Accordingly, AND gate 122 will provide an output signal to a trip function OR gate 116 when the load on the burners is less than 30 percent; i.e., when the total fuel pressure to the burner system is below 30 percent of rated value and there is loss of power to the actuators at any one of the three elevations. As will be obvious to those skilled in the art, when the burner load is less than 30 percent there may be insufficient energy to insure complete burning of fuel delivered to the furnace and thus a furnace trip will be commanded at low fuel pressure levels in the case of the loss of power to the actuators at any elevation in the interest of preventing the accumulation of unburned fuel.

The flame failure and "computer" malfunction or "computer" power loss signals from each elevation are applied to respective OR gates 103, 104 and 105. The signals passed by gates 103, 104 and 105 are applied to AND gate 106. The "computer" malfunction or power loss signals and the arming condition signal from each elevation are applied to respective OR gates 108, 110 and 112. The outputs of OR gates 108, 110 and 112 are applied to a further OR gate 114 and the output of gate 114 is applied as the fourth input to AND gate 106. The AND gate 106 will, accordingly, provide an output signal only when a total furnace flame failure has been confirmed or all "computers" at the firing elevations are malfunctioning. The output from AND gate 106 is applied as a second input to the trip function OR gate 116.

By means standard in the art, the boiler load is sensed and, if in excess of 30 percent of rated capacity, a boiler load signal is applied to the set input of a bistable circuit 126. The boiler or unit load is typically measured in terms of megawatts of power generated but may be measured in terms of steam flow or fuel flow. The second or reset input to bistable circuit 126 is the trip signal indicative of the shut-down of the furnace either on the operator's command or due to a malfunction. Bistable circuit 126 provides an output signal commensurate with boiler load being greater than 30 percent. This signal is applied as a first input to AND gate 128. The second input to gate 128 is a signal provided by air flow monitoring apparatus in the furnace and indicative of a furnace air flow rate of less than 30 percent of normal. The AND gate 128 thus provides an input to the trip function OR gate 116 only when the boiler load is greater than 30 percent of rated value and the air flow rate is less than 30 percent of normal. Bistable circuit 126 is reset when a "trip" occurs and attempts to restart the furnace with the air flow being less than 30 percent will result in AND gate 128 providing a trip signal to trip function OR gate 116. As the furnace load is raised bistable circuit 126 will be set and thereafter the operator can reduce load below 30 per-

cent without a "trip" automatically occurring; it being the intent of the system to insure an air rich mixture during start-up.

As noted above, an additional input to the safety check logic is provided by sensors which generate signals commensurate with the unsafe condition of the furnace forced draft fans all being in the off condition. A further input is provided by a sensor which generates a signal commensurate with furnace pressure in excess of a predetermined safe level. The furnace pressure will typically be measured, in inches of water, at the discharge of the forced draft fans or at the air heater inlet. These additional input signals are applied directly to the trip function OR gate 116.

The trip function OR gate 116 provides an output signal which is employed to set a bistable circuit 130. Upon being set, circuit 130 provides an output signal to a driver amplifier 132. The output of driver amplifier 132 is delivered to a trip solenoid 134; the contacts of solenoid 134 being connected in parallel with contacts 54 and 56 (see FIG. 2). Once set, bistable circuit 130 remembers and thus maintains the "trip" output signal until reset in the manner to be described below.

The output of trip function OR gate 116 is also applied as the input to an inverter 136 as well as being fed back to the reset input to bistable circuit 126. The output of inverter 136 is applied as a first input to AND gate 138. The second input to gate 138 is a "purge permissive satisfied" signal which will typically be provided by the unit control "computer" 18 logic. Before restarting of any large furnace can be attempted it is necessary that a purging cycle of predetermined duration be completed. The "purge permissive satisfied" signal is generated, by means known in the art, as a function of both timing and air flow subsequent to initiation of a purge cycle by a furnace restart command. Accordingly, if the "trip" condition or conditions sensed by the above described logic do not exist, and the purge cycle has been completed, AND gate 138 will provide a reset signal to bistable circuit 130 thereby removing the "trip" signal from the input to driver amplifier 132.

As noted, the "trip" contacts operated by solenoid 134 are connected in parallel with contacts 54 and 56 which provide a trip if there is a loss of power to or malfunction of both of safety check "computers" 18 and 20. Presuming that FIG. 4 depicts the safety check logic of "computer" 18 and bearing in mind that "computer" 20 has identical safety check logic in the interest of redundancy, the contacts of a further solenoid 134' (not shown) controlled by the output of "computer" 18 will be in parallel with the contacts of trip solenoid 134. Accordingly, safety is enhanced and nuisance shut-downs minimized by obtaining redundancy without the use of redundant circuitry or redundant general purpose computers. The avoidance of nuisance shut-downs is further enhanced by using a plurality of programmable controllers arranged in a hierarchy wherein the lower or elevation "computers" vote and are checked by the higher of safety check "computers."

Considering further FIG. 4, the malfunction or power loss signals from each elevation are also applied to a further OR gate 150. Gate 150 is employed to generate an alarm signal at control console 22; this alarm signal indicating to the operator that there has been a loss of power to or a malfunction in one of the elevation controls. In addition, the malfunction or power loss signals

from each elevation are applied as first inputs to respective AND gates 152, 154 and 156. The second input to each of gates 152, 154 and 156 is the signal commensurate with the burner load being less than 30 percent. Accordingly, each of gates 152, 154 and 156 will provide an output signal commensurate with the condition of a "computer" failure at the associated elevation at a time when burner load is at a level below 30 percent. The outputs of gates 152, 154 and 156 are utilized, through special a.c. operated relays which have not been shown on FIG. 4, to trip respective burner elevations singly. As previously noted, with the burner load less than 30 percent there may not be a sufficiently large flame envelope to insure ignition assist between elevations; i.e., the combustion at the various elevations will not be interdependent. It is, accordingly, deemed desirable to trip an elevation having a control malfunction or power failure at low levels of burner loading. The individual elevation trip relays will be provided with plural contacts so as to provide an alarm at the control console. With burner load above 30 percent, however, there will be sufficient ignition energy from other elevations to insure combustion of fuel delivered to the furnace at an elevation having a malfunctioning "computer" and thus the elevation will not be tripped. However, through the operation of gate 150, an alarm will be sounded so as to advise the operator that the elevation "computers" should be checked.

While a preferred embodiment has been shown and described, various modifications and substitutions may be made thereto without departing from the spirit and scope of the present invention. Accordingly, it is to be understood that the present invention has been described by way of illustration and not limitation.

I claim:

1. A protection system for a furnace, the furnace having a plurality of burners and associated ignitors situated at each of a plurality of vertically displaced elevations, condition responsive signal generators being associated with each furnace elevation for providing signals commensurate with the state of the burners and ignitors and the presence of flame, said protection system comprising:

a plurality of first programmable controllers, each of said controllers of said first plurality being associated with one of said furnace burner elevations and receiving signals commensurate with the state of the burners and ignitors at that elevation and the presence or absence of flame, each of said controllers of said first plurality providing output signals for controlling the ignitors and burners at the associated elevation in accordance with the received signals and a stored program, each of said controllers of said first plurality further generating an arming signal commensurate with the condition of flame desired and a flame failure signal;

a second programmable controller, said second controller being responsive to the arming and flame failure signals generated by each of said controllers

of said first plurality for generating a control signal for terminating furnace operation when the arming and flame failure signals from all of said first controllers indicate unsafe operating conditions;

a third programmable controller, said third programmable controller being responsive to the arming and flame failure signals generated by each of said controllers of said first plurality for generating a control signal for terminating furnace operation when the arming and flame failure signals from all of said first controllers indicate unsafe operating conditions;

means for delivering the arming and flame failure signals provided by each of said controllers of said first plurality to said second and third controllers; and

means connecting the outputs of said second and third controllers in parallel.

2. The apparatus of claim 1 wherein each of said controllers of said first plurality includes self-checking means for providing an output signal commensurate with a controller malfunction or power loss and wherein the signal commensurate with a preselected ratio of actual to rated plant operating capacity is generated and delivered to each of said second and third controllers, said apparatus further comprising:

means for delivering said malfunction or power loss signals from each of said controllers of said first plurality to each of said second and third controllers; and

wherein said second and third controllers each further comprise:

means responsive to said malfunction or power loss signals and to said signal commensurate with the preselected ratio for generating a disabling signal for an elevation having a controller malfunction or power loss when the plant is operating at a capacity less than that commensurate with said preselected ratio.

3. The apparatus of claim 2 further comprising: means for generating signals commensurate with the availability of power for driving the actuators associated with each controller of said first plurality; and

means for delivering said power availability signals as further inputs to each of said second and third controllers.

4. The apparatus of claim 3 wherein said second and third controllers each further comprise:

means responsive to said power availability signals and said signal commensurate with the preselected operating capacity ratio for generating process termination signals when power is unavailable for operating the actuators associated with each of said first controllers and the plant is operating at a level below that commensurate with said preselected ratio.

* * * * *