AUTOMATIC CONTROL AND INSTRUMENTATION FOR HAZARDOUS PROCESSES

By A. H. ISAAC, B.Sc, A.M.I.Chem.E.*

SUMMARY

The appropriate use of instrumentation can make a substantial contribution to the safe operation of processes. An analysis of some of the sources of hazardous conditions that can arise in plant indicates the nature of protection that instruments can provide. This can be achieved only by emphasis on safety throughout design and by attention to details. The use of automatic process control itself may introduce special hazards that must be anticipated and overcome. Safety and alarm systems can be used to provide warning of dangerous conditions and to shut down the plant automatically when this is essential.

Introduction

The most innocuous of chemical plants may give rise to accidents under exceptional operating conditions. The consequences of such occurrences are naturally more serious where the plant is handling flammable or toxic materials or where it is subject to excessive corrosion and extremes of pressure or temperature. The correct incorporation of instrumentation and automatic control in the plant design can avoid this danger and minimise the risks arising from such conditions. Such hazards may jeopardize the plant, the process, the product, and the personnel.

In any particular case one or other of these categories may be the most serious; in others several or all may be involved. It is convenient to consider some classification of this type to allocate the appropriate significance to precautions that must be taken. For example, overheating in a batch polymerisation process may not involve any hazard to operators or endanger the plant but may well result in a ruined batch of high-value product. In a similar way rupture of a bursting disc can adequately protect the plant but at the risk of releasing poisonous or flammable materials which may both endanger the operating staff and shut down the process.

Clearly, a large number of types of equipment may contribute to safety in plant operation and could be classified as instrumentation. It is proposed to exclude from this paper such devices as safety valves, non-return valves, bursting discs, safety seals, and torque shear pins which are essentially limiting devices. Consideration must also necessarily be extremely brief in respect of items that are strictly limited to " spot testing " or general laboratory supervision. If principal consideration is given to instruments on continuously operating plant, it should be understood that such items are used as complementary to the above. Some of the implications of abnormal conditions on automatically controlled plant are considered in relation to safety.

Sources of Hazard in Plant Operation—Protection by Instruments

A brief consideration of some of the sources of hazardous conditions that can arise serves to indicate the way in which instrumentation is applied to reduce or avoid the occurrence of serious dangers.

Breakdown or failure of plant items

The problem of breakdown or failure of plant items lies essentially in anticipating incipient failure of equipment. Instruments cannot indicate a potential breakdown of a pressure vessel under operating conditions: however, the examination and inspection of pressure equipment by various means of non-destructive testing is being increasingly used. Routine examination of condenser tube walls, pressure-vessel shells, and similar units as a check on corrosion is a valuable protection but these techniques are not applicable for continuous service.

In the protection of rotating machinery the measurement of bearing temperatures, lubricating-oil pressures, and the continuous monitoring of vibration conditions are widely applied and serve in their turn to indicate the development of bearing failure and similar conditions before this has produced any serious consequences. Direct measurements of shaft-torque using strain gauges and other techniques serve to protect large agitators and centrifugal machines against overloading.

In the case of heat transfer equipment protection lies in ensuring even heat distribution and the avoidance of " hot spots " which may give rise to breakdowns. The measurement of tube wall temperatures in water-tube boilers is a good example of this technique. In a similar way differential pressure measurements across a tube-still coil will indicate coking conditions which can result in a burn-out.

Breakdown due to corrosion is common and can be prevented in many cases by measurement and control of the environment giving rise to the attack. Examples of this include recording the flue-gas temperature of a boiler as a guide to prevent cooling to dewpoint causing deposition of acid liquors in a steel stack. A more elementary case is that of limiting the water-side temperature of gas coolers with galvanised tubes to prevent attack of the zinc. Serious hazards can arise in closed condensate-return systems for boiler feed. If the condensate is trapped from heaters handling corrosive liquids any leakage of process fluid into the heater steam space can result in corrosive feed being passed to the boiler with potentially very serious consequences. Adequate conductivity monitoring of condensate return lines

* Foxboro-Yoxall Ltd., Redhill. Surrey.

can avoid this by automatically diverting contaminated streams with a suitable alarm.

Interruption of services and supplies

Plants are designed to operate satisfactorily in the presence of certain services, *e.g.* steam at specified pressures, water at particular temperatures, electrical power supplies of certain characteristics, fuel supplies, etc. In the event of failure or interruption of such services plants are operating under seriously abnormal conditions and this may give rise to hazardous conditions. A suitable degree of instrumentation must be provided both to give warning of the failures and possibly to introduce standby supplies or alternative methods of operation. For example, a steam feed-pump can be started by the fall of pressure which a power failure will cause in the delivery of an electric pump.

Failure of feed flows to processes can be dangerous, particularly with heat exchange equipment. The differential temperatures across heat-exchange surfaces will be very different when there is no flow past these than under design operating conditions. Water boiling in the shells of condensers or liquors freezing in brine coolers at very low flows are typical cases.

In many problems of this type the consequences of failure are so serious that interlocked shut-down mechanisms must be included to safeguard the plant.

Departure from design operating conditions

No processes operated under design conditions are inherently hazardous. However, dependent upon the nature of the process or plant, even minor departures from these conditions may have serious results. Such departures may be caused by extraneous circumstances, by inadequate supervision of plant operation, or even by attempting to operate plants at conditions for which they have not been designed. One case of this in which instrumentation plays a very significant part is the use of flame failure devices on oil or gas burning furnaces. A trace of water in the fuel or some other momentary interruption of fuel supply may be sufficient to extinguish the flame. In the lack of any immediate action the furnace will rapidly fill with an explosive mixture constituting a very serious hazard. Flame failure devices properly applied can shut down the plant and provide suitable warning to the operator.

In a similar category lies a wide range of catalytic vapour phase reactions such as the oxidation of benzene, naphthalene, methyl alcohol, and ammonia which are carried out on a large scale. The explosive properties of the vapour-air mixtures limits operation to an extremely narrow band of compositions if the danger of explosion is to be avoided. Very precise control over the proportions must be maintained and a detailed knowledge of any departure from these conditions is of great significance. Not only may the plant and personnel be jeopardized by serious explosion hazards but, for example, in the case of nitric acid or formaldehyde oxidations even a minor departure from appropriate proportions is sufficient to destroy the high-value metallic catalyst bed. For this reason it is usual to provide warning devices both for the departure of the air vapour flow ratio from normal, either high or low, and for excessive temperatures in the catalyst bed.

Mal-operation of plant

Manually operated plant is inevitably subject to the vagaries and characteristics of the operating staff and consequently may be subjected to serious hazard due to their inadequate instruction, inattention or error. In fact, a large majority of accidents on chemical plant are ultimately accountable to human failure. The use of suitable measurement and alarm equipment serves to assist the operator in this respect and to enable him to take appropriate steps in any situation. Recording instruments provide a check of conditions which enable errors to be rectified and assist analysis of the situation by management. In the ultimate, the use of automatic process control removes much of the responsibility for detailed operation from the operator but it must be appreciated that the most hazardous period on such plants is during start up, when the automatic control may not be in full command of the situation.

In batch processes where a complex sequence of operations must be followed suitable interlocks and cycle operators serve to avoid the possibility of omitting a step or confusing the procedure. Mal-operation can extend to gross interference with the plant items as installed. For example, the screwing down of safety valves to prevent leakage, the wiring out of alarms and overload trips and disconnection of fire appliances. Suitable alarms and indicating lamps can avoid some of these but in the extreme they are essentially management problems. One common source of hazard arises in the filling of storage tanks with toxic or flammable liquids. Spillage due to overfilling of these can be avoided by reliable and accurate level-measuring equipment with automatic cut-off and alarms where appropriate.

Hazards inherent in the process

A large number of processes inherently possess potentially hazardous characteristics and the plant design accepts this. The instrumentation requirement is for adequate information on conditions to avoid the basically hazardous components creating a serious menace. Mention has already been made of the explosive or toxic properties of many chemical reactants. For adequate supervision of handling, processing, and disposal of such materials measurement and observation of their properties must be made at all stages.

For example, in the disposal of cyanide effluents by oxidation to cyanates the completion of reaction is observed and the process controlled by continuous measurements of the oxidation-reduction potential of the system. Other hazards arise from the physical conditions ruling in the plant and clearly where these involve excessive pressures and temperatures, there is a tendency to work closer to the limiting performance of the plant materials. Regulation of water to superheater control tubes, maintenance of feed to tube-still heaters, and protection of furnace linings from overheating by roof temperature measurements are some typical examples.

Plant Design for Hazardous Processes—Instrumentation Considerations

The above comments serve to indicate the type and origin of hazardous conditions that can arise in any plant and the contribution instrumentation can make in avoiding them. In the design of plant for processes known to exhibit hazardous characteristics, an analysis of this type must be combined with a review of the relevant instrumentation considerations. Some of these will be mentioned.

Measurement

To maintain the operation of plant in a safe state a continuous provision of information is required on the operating conditions at various points in the plant. Essentially this implies measurement at these locations and the adequate presentation of data on pressures, temperatures, flows, levels, analytical quality, and other properties. In this way the operator is in a position to assess precisely the conditions and circumstances not only of the significant operating regions of the plant but also at extraneous points and in ancillary units to ensure that hazardous conditions do not arise in these.

The choice of the significant factors for measurement on any particular plant must necessarily be an individual one. Such instrumentation may be primarily incorporated for protection against danger but may also have other functions which would support its application, *e.g.* costing, production, process operation, etc.

Instrument location

Modern instrumentation permits the transmission of information over relatively long distances and this removes the necessity for the operator's presence in the immediate vicinity of the plant units. In particular in the case of toxic reactants where there must always be the danger of slight leakages, such a precaution is obviously desirable and in the case of highly explosive or radio-active reactions it is essential. In an extensive plant it has the added advantage of centralising information to one locality so that the operator can rapidly assess the general operating conditions on the plant. The operation of the plant from a remote location places a great emphasis on the completeness and reliability of the instrument readings.

It should not necessarily be assumed however that a hazardous process is always best operated remotely. In particular where reactions are only partially instrumented or automatically controlled there is every reason for grouping the measuring equipment together but at a point immediately adjacent to the reaction equipment. This means that the operator is in a position to supervise visually and operate manually the reaction equipment whilst having the added advantage of specific measurements made available to him. Many batch operations are in this category. In certain cases visual examination may appear to be essential, *e.g.* condition of solids on conveyor belts, shape and characteristics of flames and sprays, discharge of solids from chutes, etc. Undoubtedly these present a challenge but in a number of cases they have been successfully solved by the use of closed-circuit television systems. These are, however, relatively costly and elaborate and their use is justified only where no other solution is available.

Instrument mounting

The display of information on a panel may be either conventional or graphic. In the former the basic critical measurements are grouped at one location on the panel with the incidental indications around these arranged generally in relation to the plant units they serve. The graphic display presents the information in the form of a flow sheet of the process with the various indications shown at the appropriate points in this. This arrangement is said by a number of users to overcome the problem of operational errors when hazardous situations arise by its inherent demonstration of the interrelation and interaction of the various units. The presentation of alarms is covered below.

Reliability of measurement

The value of protection derived from instrument readings depends on the attention given at the design stage to the performance of the measuring equipment and its characteristics. For example, due allowance must be made for the time of response of temperature measuring instruments when considering transient temperature peaks. What appears from a record to be a peak of 10° lasting 4 minutes may well have reached 15° or more but the full amplitude of the peak has been lost due to the attentuation of the thermometer and its associated pocket. This also applies to many types of analytical equipment since their time of response is slow and they may appear to show incorrect values when conditions are changing rapidly. Dangerous conditions can therefore develop without any indication of their occurrence, unless the measuring device performance is matched to that demanded under alarm conditions.

Another significant factor in the potential reliability of any measurement is the problem of location of the sensitive element or the sampling point for analytical equipment. Temperature measurements in catalyst beds, furnaces, or nuclear-reactor blocks can give widely differing values dependent upon location, and great care must be used in the original positioning to yield satisfactory results. The fuel-element failure in the Sellafield nuclear reactor was a good example of this because it happened to be in a fuel channel not incorporating a thermocouple so that the excessive temperature was not observed.

Control

In addition to information on the operation of the plant it is of course reasonable to provide some means for the operator to counteract the development of hazardous conditions when these are indicated. This may be achieved by the use of remotely operated valves or pumps, the actuation of fire sprinkler systems, dump-valves, etc. In the ultimate, automatic control clearly has much to offer in applications of this type. Not only does it permit the operation of the plant with minimum possibilities of human error but fundamentally makes corrective action more evenly and more gently and with less over-shoot than is possible with the human operator. In many hazardous processes, such as catalytic cracking, for example, this if of such great consequence that the processes are virtually uncontrollable by manual means. The use of automatic control, however, introduces itself a number of potential hazards that must be considered.

Safety Considerations in the Use of Automatic Process Control

As mentioned above, the purpose of automatic control on hazardous plants is to retain the variables at safe operating values. At the same time the use of automatic control on plant implies only a limited degree of routine supervision by the operator and therefore more serious consequences if for any reason the plant variables should deviate substantially from the desired values. Automatic control loops are usually established and designed for a normal range of operating conditions only. Their rangeability may well be considerable but will limit the flexibility to deal with exceptional operating conditions that may arise due to extraneous causes. The automatic controller is **a** blind device with no power of discretion in these circumstances if faults give rise to unusual operating conditions an automatic controller can aggravate the situation.

Since deviation from control may imply the development of hazardous conditions it is worth analysing some of the reasons which will cause variables to deviate substantially although they are under the general command of an automatic controller.

Excessive demands

The imposition of operating requirements beyond the limiting performance of the plant units means that control valves are completely opened, surge tanks overflow, distillation columns prime, etc. Needless to say, under such conditions the plant cannot continue to operate in a normal condition. The reasons for these limitations being achieved may be as mentioned above, be due to faulty operation, unusual operating demands, or limitations due to failure of some item in the plant equipment.

To avoid these problems the maximum flexibility must be provided in the basic-control system-design. This can be greatly increased by the use of sequenced control valves, cascade control systems, and other arrangements. Auto-selector control provides good protection in such cases as flow-controlled pumps where the level in the suction pump over-rides the flow control to protect the pump against the danger of running dry.

To take care of exceptional circumstances occurring on the plant, particularly during the start-up phase, most automatic controllers are provided with suitable automatic-to-manual transfer so that normal type remote/manual operation can be carried on when the process or the plant is not operating under anticipated design conditions and where the control systems provided might lead to dangerous situations.

Failure of controlled flow

Failure of controlled flow is a self-evident condition where for example failure of the cooling water to a heat exchanger or an inadequate steam pressure to a heater must result in deviation from control. To avoid dangerous conditions as a consequence of such deviations, suitable alarms must be used. One case is worth mentioning. In controlling the ratio of gas to air fed to burners it is usual to hold the gas in a fixed ratio to the independent air flow. This is because of the danger of losing air due to fan-power failure. With this system zero air flow will call for reduction of gas flow to zero under ratio control thus avoiding the production of a gas-rich explosive mixture.

Transient disturbances

The case of transient disturbances is an extension of the case of excessive demand and covers those cases where demands are made upon the plant that are in the long term no greater than the basic plant design is capable of handling, but which dynamically occur at faster rates, or give rise to transient disturbances through the system at such a rate, that it is temporarily overloaded and cannot respond in a stable manner. The limitation is the long time-constant of the plant.

Mechanical failure of plant

Obvious examples of mechanical failure of plant are those of burnt-out heater tubes and blocked lines. Control must suffer and may aggravate the failure once it has occurred. For example, a temperature-controlled gas-fired heater coil will open the gas valve wide if the coil ruptures and flow past the thermometer bulb ceases.

Saturation conditions or instabilities arising from the control equipment

Poor controller adjustment or inadequate and incorrect control loop design can give rise either to instabilities in loop behaviour or to saturation of some point of the loop. This means that a measurement reaches the extremes of its range or the control-valve travels to one of its limits. An example arises in the start-up of a batch reactor under temperature control. The temperature is bound to over-shoot because of saturation of the integral term which means that control does not start until the set-point is exceeded. It can be avoided by the use of an integral cut-out mechanism.

Failure of instrument power supplies

Pneumatic control valves normally have a fail-safe sense, since they are spring-opposed. In a number of cases it will not be possible to decide, however, whether a control valve should open or close on air failure and a safety lock or stay-put mechanism can be used. The gas collector main on a coke-oven battery is a good example. Even such devices are not entirely safe since clearly a safety-lock will only retain a control valve in the same position as it was at the moment of failure. Frequently such conditions as lead to failure are exceptional and the valve may well have been at an extreme position in the course of making correction for some disturbed conditions.

Where pneumatic transmission is used signal failure also may have a safe sense. Since air-failure may be a local situation only, it can fail at the transmitter but not at the valve. For example, if a temperature controller is used on a gas-fired furnace and is based on a normal type pneumatic transmitter where an air signal of 15 lb/in^2 corresponds to maximum temperature and 3 lb/in^2 to minimum temperature, air-failure at the transmitter will appear to the controller like a low-temperature condition. This will increase the supply to the burners to maximum in an attempt to correct this condition. This can cause irreparable damage to the heater and must be avoided by using reverse-signal transmitters.

Mechanical failure of the measurement or control equipment

Mechanical failure will generally occur only as a result of exceptional conditions such as over-range of the measurement, excessive corrosion, etc. It is apparent that a factor of safety in quality and design of equipment must be considered in setting up individual control loops, installation, and the selection of the mechanical components. An example of a safety feature is the " burn out" device used on potentiometric temperature controllers. This serves to simulate a high temperature condition when the thermocouple goes open circuit, as it will if the pocket burns through. This causes the control valve to shut to a safe condition.

Safety and Alarm Systems

General

An alarm system serves to draw attention to the presence of a fault or the development of a potentially dangerous value of any variable on the plant. It must also identify the nature and location of the hazardous condition. A complete safety system will, by means of an interlock circuit, automatically shut down all or part of a plant under any alarm condition or combination of such conditions.

These systems are based on measured process variables and should be distinguished from pilot lamps or tell-tale indicators, which are essentially running lights indicating the operation of motors, agitators, and the position of isolating valves. They are initiated by relays, starters, and limit switches associated with the equipment concerned.

A simple alarm system comprises, therefore, an initiation device, relay, presentation and display means. Complex systems will also include interlocks and shut-down devices. These are considered individually.

Initiation

The basic initiation of alarm systems utilises a sensitive detecting device which can be set to operate at some predetermined value of the measured variable. Since the presentation of the alarm is nearly always in the form of electric signal lamps, bells, etc., contacts are incorporated in the device. Very high reliability is essential and mercury switch type contacts are therefore preferred. In order to fail-safe in the event of power failure such units are usually arranged to open, not close, circuit on alarm conditions.

The actuation of the alarm device must be from some measurement of the variable concerned. This may be the same basic measuring device that serves to provide a signal for recording or control, *e.g.* mounted in a temperature recorder or connected to the output of a flow transmitter. It is possible to adjust the point at which the alarm trips. For the highest degree of safety the alarm should be based on an independent measuring device using a different method of measurement, a separate plant connection, and an isolated power system from that actuating the basic plant operation and control equipment. Only in the most critical duties will this be followed throughout since it implies duplication of most of the measurements on the plant.

The commonest form of initiation device used with pneumatic transmission systems is a high-quality pressure switch connected into the output of the pneumatic transmitter. Isolating valves in the transmission line permit servicing of the controller or recorder whilst retaining the alarm in service.

Relay system

In all but the very simplest alarm systems it is necessary to include an intermediate relay system between the initiation and the presentation. This permits the interpretation of initiation contact-action to a form suitable for the presentation and display equipment. At this point facilities for alarm testing, audible alarm actuation, and cancellation and the introduction of an intermittent power supply for " flashing " presentations is possible. The relay systems may be centralised serving all alarm points on a plant, or they may be in the form of self-contained individual units for each alarm system. In some cases they are combined with the signal lights and switches in a single housing.

Presentation and display

There is a wide variety of means by which the operator can be informed of the existence of hazardous conditions. The most immediate response is produced to an audible device such as a bell, siren, or buzzer. It is preferable that only one type should be used although several units may be located at different points of the plant to attract the operator's attention to the visual display. This serves to discriminate which of the particular alarm conditions has been exceeded. Consideration must be given to audibility particularly where much extraneous noise exists, for example in compressor houses and mixing rooms they must be immediately discriminated from any other audible systems used on the plant. In many cases the audible alarm may serve only as a warning of changing conditions that are not themselves immediately hazardous. For this reason corrective action may take some time and it is essential that a cancellation system is provided to permit the operator to silence the alarm during this period but which will keep the audible unit available for any other alarm condition. Such a system is illustrated in Fig. 1.

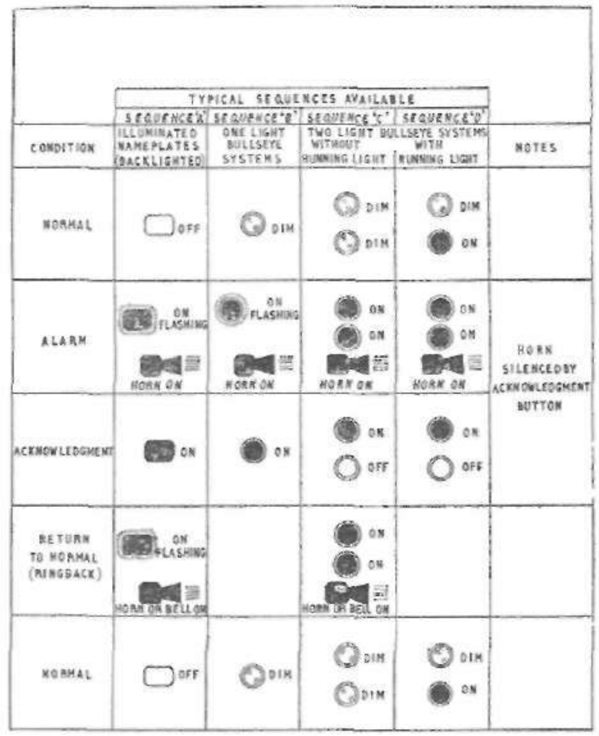

Fig. 1.—*Typical presentation sequences for alarm conditions*

The visual presentation of the alarm can either be in the form of individual signal lamps, colour identified where necessary for normal and abnormal conditions and titled by means of nameplates or an annunciator system where translucent nameplates are provided either individually or in banks, illuminated from the rear by the signal lamps. In either case they must be of adequate brightness in the face of normal illumination of the control room and preferably possess a wide angle of visibility. As an additional aid to attract attention flashing lights may be used and it is common for these to be arranged so that on first initiation the alarm light flashes and the audible warning sounds but on cancellation of the audible warning the flashing light reverts to a steady bright condition.

The use of multiple-light systems has many advantages. Two light systems are used for " normal and alarm " or for " high-low" while three light systems can give " high-normal-low " indications from one lamp at a time and two additional indications " below normal " and " above normal " with simultaneous illumination of two lights " normal and high " or " normal and low ". In some alarm sequences a " ring-back " system is provided which restores the audible alarm and the flashing when the alarm contacts revert to their normal condition. A further acknowledgment resets the system for further operation. In general, discharge lamps do not have a sufficient intensity for this duty and filament lamps must be used. These have a finite life for continuous burning (approximately 10 lamps per year at rated voltage will be necessary). This means that adequate provision must be made for indication of lamp failure. They may be continuously operated at low voltage showing a dim illumination level which can readily be discriminated from the bright alarm

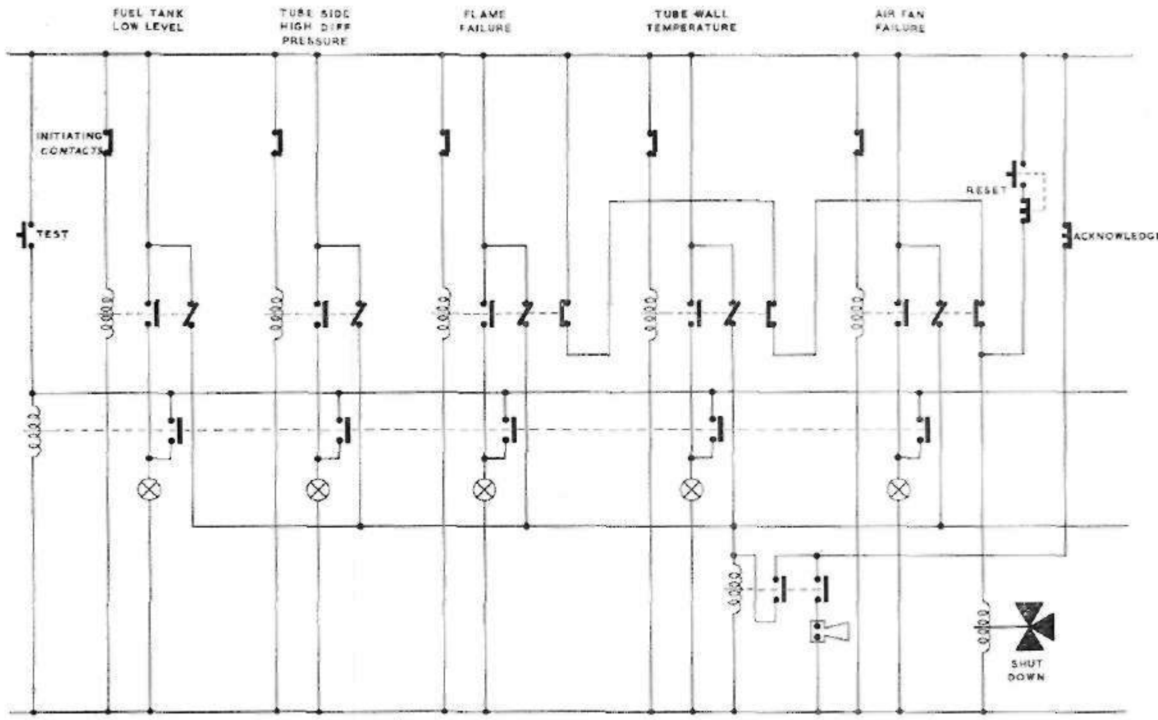

Fig. 2—*Typical wiring schematic for alarm system with shut-down circuit*

condition. Alternatively a test button may be installed, usually common to all alarms on the panel, which actuates all audible and visual alarms. This is checked once per shift and gives operators a desirable measure of confidence in the alarm system.

Complex alarm systems

By provision of appropriate contacts in the relay system several alarm points on a plant can be interlocked in such a way that any one of them by series connection will serve to shut down the plant. Such an arrangement is illustrated in Fig. 2. Such systems have an important part to play in the safe operation of the plant but very careful consideration should be given before a high degree of automatic shut-down is introduced. The cost or danger of a shut-down may well exceed the immediate hazards of continuing operation. In addition, after a plant is shut down automatically it is frequently difficult to identify which of the particular interlocked variables was responsible. In the safety systems applied to nuclear power reactors, for example, the consequences of shut-down are so serious that a " two out of three " safety system is used. This means that three independent installations are made at all alarm points. Before shut-down occurs two out of the three must indicate alarm conditions. This is a safeguard against failure of the alarm devices themselves. This technique will not normally be justified but it does emphasize the advantages of simplicity in design and reliability in operation required in alarm systems. Many automatic shut-down systems require manual restarting. In the simplest case, for example, flame-failure alarm will shut off the fuel and it cannot be restarted until some suitable interlock system has been actuated by the operator. This permits the necessary purging of the furnace chamber and ignition of pilot flames. The interlock and shut-down operation may be electric using solenoid valves or pneumatic using small air pilot valves.

Where complex shut-down systems are employed the reliability of power supply is most important and independent emergency electrical systems are often used. Low voltage d.c. supply with storage battery support has many advantages. The location of fuses and isolators in such systems is most important since a momentary overload in one of the safety circuits can blow a fuse and shut the whole plant down.

Conclusions

The large majority of instruments applied in process operation and control make a contribution to the safety of operation of the plant. Facilities for remote data transmission and automatic process control reduce even further the hazards of operating plants that would otherwise be substantially impossible to run in a safe condition. A range of safety and alarm systems has been developed which serve to limit the consequences of the inevitable failures and major disturbances that will occur on any plant and which, in the absence of adequate warning and perhaps automatic shut-down of the process, would cause very serious results.

Acknowledgment

Acknowledgment is due to L. S. Yoxall, Esq., Managing Director, Foxboro-Yoxall Limited, for permission to present this paper.

The manuscript of this paper was received on 8 *April,* 1960.