# Computer-Aided Safety Interlock Systems

J. ROBERTO RIVAS

*Instituto Tecnologico y de Estudios Superiores*
*de Monterrey, Monterrey, N.L. Mexico*

DALE F. RUDD

College of Engineering
and Mathematics Research Center
University of Wisconsin
Madison, Wisconsin 53706

and
LLOYD R. KELLY

Atlantic Richfield Company
Dallas, Texas

Since operation error is a major factor contributing to industrial disaster, it is necessary to develop safety interlock systems which prevent modes of operation that are known to be dangerous. It is not possible to foresee all the disruptions that might occur and, for this reason, an a priori analysis of safety problems is incomplete. At each step in operation the state of the process must be updated if hazardous conditions are to be avoided. To a large extent this is a problem in logic which can be handled rapidly by the computer using the methods developed here.

## SCOPE

Systems that handle chemically reactive, toxic, radioactive, and other dangerous materials must be designed and operated with special care to avoid loss of life and property. Provisions must be taken for the reduction of the frequency of equipment and human failure, for the containment or release to a safe area of materials during unintended excursions from normal operation, and for a multitude of other factors which determine the disaster tolerance of a system. Studies of loss prevention have been extensive and a large body of empirical information has evolved. However, major industrial disasters still occur, indicating a critical need for further study (Kletz, 1972; Browning, 1970).

An enormously large number of ways exist for manipulating most industrial processes, many of which are extremely dangerous and a few of which achieve useful processing objectives. In the sample process considered in this report seventeen valves can be opened or closed leading to $2^{17} = 131,072$ final valve positions. Considering that the sequence in which the valves are manipulated during transient operation forms an even larger combinatorial problem, it is hopeless to examine the safety of all possible operating problems that might arise. In practice only normal operation, start-up, shut-down and major emergency situations can be examined a priori, leading to the unfortunate possibility that an extremely hazardous mode of operation may be entered into unknown to the operators as they attempt to contend to other innocuous situations which might arise.

We expand on the conjecture that the violent and destructive events which are so prominent in industrial disaster to a large extent are the effects of an inability to anticipate the long-range effects of current actions. Sequences of seemingly innocuous events occur before the first major disruptions, which force the system into a mode of operation from which it cannot be extricated without disaster. Further, could the effects of these events be foreseen, actions could be taken to intercept and quench the impending disaster.

The process system is viewed as a network of connectors through which material flows, the routes taken being determined by the position of valves. Symbolic logic is used to model the system and to determine the long-range effects of valve operation policies. Proposed changes in operation can be assessed in matters of seconds by the computer providing an interface between the operator and the process to prevent the implementation of operations which in the long-run are hazardous. This leads to an Adaptive Safety Interlock System to provide a level of protection which cannot be obtained by the a priori assessment of operating policies.

## CONCLUSIONS AND SIGNIFICANCE

In this report attention focuses on those hazardous conditions which arise by the movement of material through a complex processing system. The difficulty to be overcome arises from an inability to keep track of the implications of operation changes. Even for simple industrial problems the systems would not allow themselves to be analyzed accurately and rapidly by intuitive and empirical means. The hazards which accompany an error in analysis prompt the development of rapid and accurate methods.

By limiting the model of the process to the major features which dominate the movement of material, the problem of operation procedure analysis was cast in a sequential logic form. This enabled the rapid and accurate computer analysis of operation procedures, handling typical industrial operation problems in fractions of seconds. This then led directly to the extension of the logic analysis to hazardous state analysis. The Adaptive Safety Interlock capability is a direct result of this problem formulation. It is important to realize that these developments are based on the conjecture that the opera-

Correspondence concerning this paper should be addressed to D. F. Rudd.

**tions problem is dominated by the overall movement of material from high pressure inlets to low pressure outlets through connectors which are controlled by valves that are either open or closed. It is the presence or absence of material in the system which is analyzed and not the relative amounts. This then leads to conservative controls.**

## EVENTS OF MAJOR CONCERN

To consider all events which can contribute to disaster leads to problems which will not allow themselves to be formulated or solved. On the other hand, a careless abstraction of the real situation may ignore critical factors. We seek an abstraction which both contains the essence of disaster tolerant operation and which is capable of ready solution. The usefulness of this work depends completely on the accuracy with which we recognize the events of major concern.

The system is viewed as an assembly of connectors which are joined at nodes. The connectors are the pipes, vessels, reactors, and other equipment through which material can flow from input sites to output sites. The flow through certain connectors can be stopped by the action of valves. The valves are thought to be either open or closed and serve merely to permit or prevent the passage of material, the amount of material not being a parameter entering this formulation.

Certain material species *A*, *B*, *C* may be driven through this system of connectors by the action of pumps, pressure differences, or other driving forces, the path taken being determined by the driving force and the positions of the valves.

We are not concerned with the amount of material present at a given point in the system, merely the presence and absence of material. Figure 1 shows the patterns of material flow with which we must be concerned. In pattern (a) species *A* flows through the system in its own private route, in (b) species *A* and *B* share a common route, in (c) species *A* is driven into the system to a point where it is held by a closed valve, in (d) species *A* is trapped within the system by two closed valves, in (e) *A* eventually is flushed from the system leaving the connector empty, and in (f) species *A* is held in a dead-end region of the system, not by closed valves as in (d), but, by the driving force which causes the flow of the second species *B*. We will be concerned with combinations of these basic patterns existing in the complex assembly of nodes and connectors.

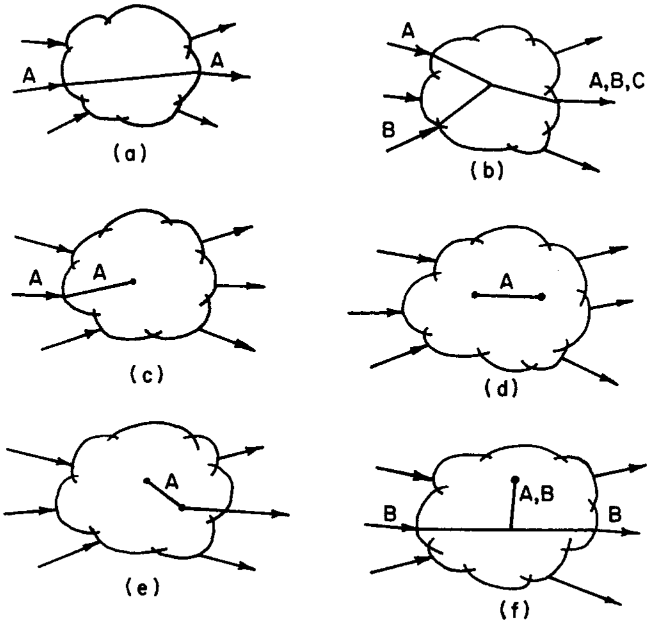

Fig. 1. Possible states of the chemical species.

Figure 2 is part of the flowsheet for a petroleum refinery. In this system hydrocarbons are reacted in several large spherical reactors by the action of a chloroplatinic acid on alumina catalyst. Periodically, individual reactors are drawn out of service for catalyst regeneration, involving the burning off of carbon deposits with dilute oxygen mixtures, hydrogen treatments, and rechlorination with the reaction products of carbon tetrachloride. This process illustrates the principles developed throughout this paper. Figure 3 shows the transition from the flowsheet to the network of connectors.

For example, connector 10 in Figure 3 is that region of Figure 2 including the left-most reactor and the associated piping to the points where streams join or split. Connector 4 begins at the inert gas generator, includes the inert gas cooling tower, the inert gas compressor, two heat exchangers and the heater, and terminates at the junction with the pipeline coming from the air compressor. Recall that a connector is defined as the region between nodes where connectors join and may include large amounts of equipment or merely a short section of pipe. Connectors which are capable of being closed have the valve symbol affixed. For example, the valve symbol on connector 17 represents the two motor driven valves below the first reactor, a pair which operates simultaneously with an intermediate nitrogen purge: the symbol merely represents the ability to stop flow and we are not concerned with the mechanical details.

Table 1 contains all of the essentials on the structure of this abstraction of the process system. Included are the connector number, the number of the nodes associated with each connector, and the connectors which are common to that node. The last entry, for example, states that the two ends of connector 27 have been denoted as 2 and 3 and that connectors 15 and 19 join connector 27 at node 2 and connectors 11 and 26 join connector 27 at node 3. The connectors which can be closed by valves are also noted.

To illustrate the kind of material movement with which we will be concerned, consider the small network of con-

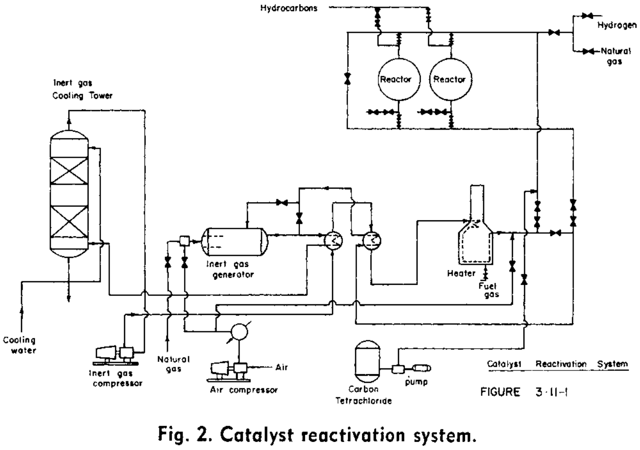

Fig. 2. Catalyst reactivation system.

nectors shown in Figure 4. This consists of two inlets where species *A* and *B* respectively can enter, an internal loop of three connectors, and one outlet connector. Six valves can be manipulated. Suppose that initially all six valves are closed and no material is trapped in the system. What are the consequences of the operation procedure shown in Table 2?

When the first operation procedure is performed (open valves on connectors 1, 3, 5, and 6), an open path from inlet 1 to outlet 3 originates and species *A* can flow through connectors 1, 3, and 5. It can also reach sides 2 and 3 of connector 6, side 2 of outlet 2, and sides 1 and 2 of connector 4. When the second operation procedure is executed (open valve of connector 2, close valves of connectors 1 and 5), an open path forms between inlet 2 and outlet 3 and species *B* can flow through connectors 2, 6, and 3 and can reach side 2 of connector 4 and side 3 of connector 5. Species *A* is trapped in side 1 of connectors 1, 4, and 5, in side 2 of connector 4, and in side 3 of connector 5. *A* is not in connector 6 any more because species *B* flushed it away, but it can be trapped in side 2 of connector 4 and side 3 of connector 5 because it is reached by an outlet but also by species coming from an inlet. After the third operation procedure is performed (open valve 4, closed valves 2 and 3), there are no more inlets or outlets open and the two species are trapped in all the connectors.

Table 1. Structure of the Catalyst Reactivation System

| Connector *i* | Node *j* | Node *l* | Connectors joined to node *j* | Connectors joined to node *l* | Species | Valves |
|---|---|---|---|---|---|---|
| 1 | 1 | | 14, 26 | | 1 | |
| 2 | 2 | | 3, 25 | | 2 | x |
| 3 | 2 | | 2, 25 | | 3 | x |
| 4 | 2 | | 5, 24 | | 4 | x |
| 5 | 2 | | 4, 24 | | 5 | x |
| 6 | 2 | | 20, 21 | | 6 | |
| 7 | | 1 | 10, 17 | | | x |
| 8 | | 2 | 11. 18 | | | x |
| 9 | | 2 | 22. 23 | | | |
| 10 | 1 | 2 | 7. 17 | 13, 14 | | |
| 11 | 2 | 3 | 8. 18 | 26, 27 | | |
| 12 | 1 | 2 | 13. 15 | 16, 17 | | x |
| 13 | 1 | 2 | 12, 15 | 10, 14 | | x |
| 14 | 1 | 2 | 1, 26 | 10, 13 | | x |
| 15 | 1 | 2 | 12, 13 | 19, 27 | | |
| 16 | 1 | 2 | 18, 22 | 12, 17 | | |
| 17 | 1 | 2 | 7, 10 | 12, 16 | | |
| 18 | 1 | 2 | 16, 22 | 8, 11 | | |
| 19 | 1 | 2 | 21, 25 | 15, 27 | | |
| 20 | 1 | 2 | 23, 24 | 6, 21 | | x |
| 21 | 1 | 2 | 19, 25 | 6, 20 | | |
| 22 | 1 | 2 | 16, 18 | 9, 23 | | x |
| 23 | 1 | 2 | 20, 24 | 9, 22 | | x |
| 24 | 1 | 2 | 20, 23 | 4, 5 | | |
| 25 | 1 | 2 | 19, 21 | 2, 3 | | x |
| 26 | 1 | 3 | 1, 14 | 11, 27 | | x |
| 27 | 2 | 3 | 15, 19 | 11, 26 | | x |

Note: There were no trapped species initially.

Table 2. Operation Procedure for Network of Figure 4

| Order of operation procedure | Open valves | Closed valves |
|---|---|---|
| 1 | 1, 3, 5, 6 | |
| 2 | 2 | 1, 5 |
| 3 | 4 | 2, 3 |

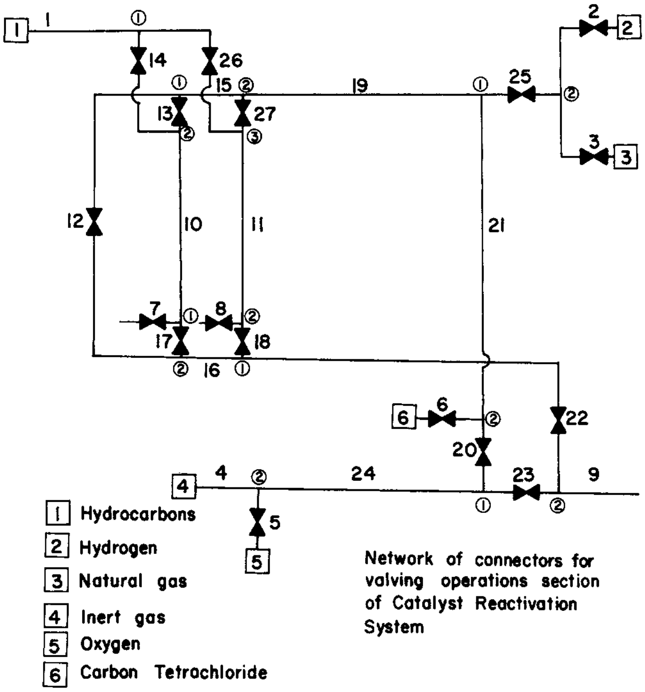

Fig. 3. Network of connectors for valving operations section of catalyst reactivation system.

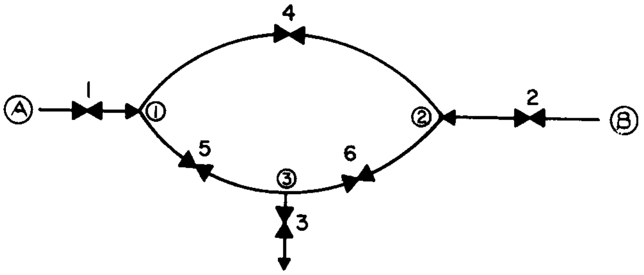

Fig. 4. A small network of connectors.

Such a study of the logical consequences of proposed valving operations is called analysis in this report. The analysis of operation procedures for any but the simplest systems is an enormous bookkeeping problem with a high likelihood of error unless special care is taken. This can be formulated as a problem in sequential logic to be solved on the computer, eliminating the possibility of a bookkeeping error.

Operation procedure synthesis is much more difficult than analysis. Synthesis starts with a general statement of an operation goal such as "Remove species *C* trapped in connector 6 without disrupting the normal flow of species *A* and avoid all hazardous conditions" and generates the detailed operation procedures such as shown in Table 2. Synthesis requires ability in analysis so that the consequences of proposed valve changes can be predicted, but it also requires ability to achieve an operation objective such as "synthesize operation procedures to reach the operation goal so that the maximum number of valving errors can be made before the known hazardous conditions are reached," or "so that the goal is reached in a minimum number of valve operations." Synthesis is orders of magnitude more difficult than analysis (see

Rivas and Rudd, 1974).

In summary, the major effects that must be understood if disaster interception ability is to be achieved at all involve the macro-movement of material through the system. This ability coupled with a knowledge of locally hazardous conditions leads to the problem of the synthesis of operation instructions to accomplish rather general operation goals. We have had to abstract the real problem into the idealized form to obtain the disaster interception capability discussed here. The results are accurate to the extent that such macro-movement of material dominates the disaster tolerance of the system.

## OPERATION PROCEDURE ANALYSIS

The computer ought to be able to handle the bookkeeping problems associated with the analysis of proposed operating procedures. Given the structure of the network of inputs, outputs, connectors and valves, and the proposed sequence of valve operations the computer should be able to determine the complete movement of species through the process system. All that is needed is a suitable theory of operation procedure analysis.

We approach this problem through symbolic logic. The operation procedure is described by a set of declarative and unambiguous statements that are either true or false, and these statements are related by the principles of symbolic logic forming a model of the system operation. The computer can form, manipulate, and solve this model in matters of seconds for industrially large problems, thereby providing a rapid assessment of proposed operation procedures.

Of the many algebras which could be developed to handle this problem, we have found a sequential logic to be suitable (Dietmeyer, 1971). With A and B as declarative statements which are either true or false, the following notation is used:

$$A = \begin{cases} 1 \text{ if true} \\ 0 \text{ if false} \end{cases}$$

$$A \cdot B \equiv A \text{ and } B$$

$$A + B \equiv A \text{ or } B$$

$$\bar{A} \equiv \text{not } A$$

$$\sum_{a_j} A(a_j) \equiv A(a_1) + A(a_2) + \ldots$$

$$\prod_{a_j} A(a_j) \equiv A(a_1) \cdot A(a_2) \ldots$$

and

$A \rightarrow B$ the next truth value of B equals the current truth value of A

The last operation implies that the truth value of a set of statements interlinked by symbolic logic operation changes with time, the next values being dependent on the current values. We are concerned only with the final values of such sequences of logic operations and find this sequential logic only useful as a tool in problem formulation. We are not concerned with the methods of convergence as long as the convergence occurs rapidly enough.

We now cast the ill-defined problem of operation procedure analysis into the rigorous sequential logic form. The skill with which these equations are formed determines the usefulness and accuracy of the operation procedure analysis computer program.

Figure 5 illustrates the nomenclature for the arbitrary connector $i$ which exists between node $l$ and node $j$. The position of the valve is defined by the statement $v(i)$

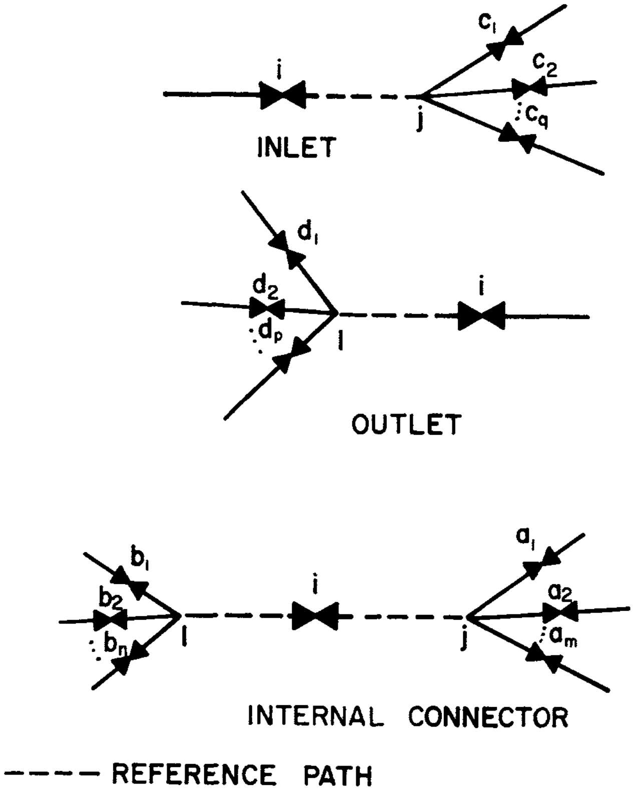

Fig. 5. Reference paths and nomenclature for the structure of process systems.

$v(i)$: The valve on connector $i$ is open (1)

This statement can either be true (1) or false (0). Depending on the conditions which exist in the network, these three statements can be true or false

IFT$(i, j, k)$: Species $k$ is flowing through side $j$ of connector $i$ (2)

IFI$(i, j, k)$: Species $k$ has reached side $j$ of connector $i$ from an inlet but there is no flow. (3)

IFS$(i, j, k)$: Species $k$ is trapped in side $j$ of connector $i$ (4)

To bridge the gap between information on the position of the valves, statements 1, and the state of the system, statements 2, 3, and 4, the logic equations which connect these statements must be formed. This involves the use of a variety of intermediate variables.

### Flow of Species Through the System

Species $k$ can be flowing through the system from an inlet to an outlet passing through side $j$ of connector $i$ only if both of the following statements are true simultaneously.

IAC$(i, j, k)$: Side $j$ of connector $i$ is reachable by species $k$ coming from an inlet (5)

and

IPT$(i, j)$: Side $j$ of connector $i$ is included in path which allows steady flow but is not in a loop (6)

or

ISRC$(i, j)$: Side $j$ of connector $i$ is included in a loop which allows steady flow (7)

That is,

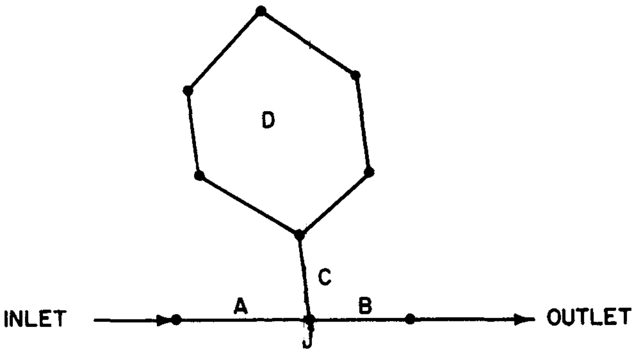

**Fig. 6. Loop joined by a single connector to an open path from an inlet to an outlet.**

$$\mathrm{IFT}(i,j,k) \leftarrow \mathrm{IAC}(i,j,k) \cdot [\mathrm{IPT}(i,j) + \mathrm{ISRC}(i,j)] \qquad \text{(a)}$$

Statement 5 is true if any of the half connectors joined to node $j$ has been reached by species $k$ from an inlet, or if side $l$ of connector $i$ has been reached by species $k$ at the same time valve $i$ is open.

$$\mathrm{IAC}(i,j,k) \leftarrow [\sum_{a_m} \mathrm{IAC}(a_m,j,k)] + \mathrm{IAC}(i,l,k) \cdot v(i) \qquad \text{(b)}$$

Statements 6 and 7 may seem redundant. Figure 6 shows a system in which steady flow is not possible involving loop D, such a flow requiring two-way flow through connector C. The remaining developments in subsection I deal with these possibilities. This requires the introduction of a variable describing the local possible direction of flow.

$\mathrm{IND}(i,j)$: Side $j$ of connector $i$ is the high pressure side (8)

Now statement 6 is true if valve $i$ is open and if (a) any of the half connectors joined to node $j$ is included in an open path with side $j$ as the low pressure side, or (b) if side $j$ is a high pressure side and side $l$ is included in an open path.

$$\mathrm{IPT}(i,j) \leftarrow v(i) \cdot [(\sum_{a_m} \mathrm{IPT}(a_m,j) \cdot \overline{\mathrm{IND}(i,j)} + \mathrm{IND}(i,j) \cdot \mathrm{IPT}(i,l)] \qquad \text{(c)}$$

Statement c takes this form because of the special way in which the high pressure side of connectors are determined.

Inlets are at high pressure, thus the connectedness to an inlet determines the high pressure side of internal connectors. The following intermediate variable is used:

$\mathrm{INI}(i,j)$: Side $j$ of connector $i$ is reached by an inlet (9)

Thus, side $j$ of connector $i$ is the high pressure side if any of the half connectors joined to node $j$ is reached by an inlet and at the same time side $l$ is not also a high pressure side.

$$\mathrm{IND}(i,j) \leftarrow [\sum_{a_m} \mathrm{INI}(a_m,j)] \cdot \overline{\mathrm{IND}(i,l)} \qquad \text{(d)}$$

The variable INI is true only if (a) any of the half connectors joined to node $j$ is reached by an inlet, or if (b) side $l$ is reached by an inlet with the valve open.

$$\mathrm{INI}(i,j) \leftarrow [\sum_{a_m} \mathrm{INI}(a_m,j)] + \mathrm{INI}(i,l) \cdot v(i) \qquad \text{(e)}$$

Finally we must deal with loops in the system with these variables.

$\mathrm{ISRC}(i,j)$: Side $j$ of connector $i$ is included in an open path and in a loop (10)

$\mathrm{IPRC}(i,j)$: Side $j$ of connector $i$ is part of a loop (11)

Side $j$ is part of a loop only if the valve is open, and any of the half connectors joined at node $j$ are part of a loop and the half connector at side $l$ is part of a loop.

$$\mathrm{IPRC}(i,j) \leftarrow v(i) \cdot \mathrm{IPRC}(i,l) \cdot [\sum_{a_m} \mathrm{IPRC}(a_m,j)] \qquad \text{(f)}$$

In a similar fashion

$$\mathrm{ISRC}(i,j) \leftarrow \mathrm{IPRC}(i,j) \cdot [\mathrm{IPT}(i,j) \cdot \mathrm{IPRC}(i,j) + \mathrm{ISRC}(i,l) + \sum_{a_m} \mathrm{ISRC}(a_m,i)] \qquad \text{(g)}$$

This completes the missing link in Equation (a), thereby accounting for all the circumstances under which species $k$ can be flowing through side $j$ of connector $i$.

#### Species Backed Up from an Inlet

Statement 3, "species $k$ has reached side $j$ of connector $i$ from an inlet but there is no flow" is true if side $j$ of connector $i$ can be reached by species $k$ coming from an inlet and if side $j$ of connector $i$ is not included in an open path.

$$\mathrm{IFI}(i,j,k) \leftarrow \mathrm{IAC}(i,j,k) \cdot \overline{[\mathrm{IPT}(i,j) + \mathrm{ISRC}(i,j)]} \qquad \text{(h)}$$

This is all that is needed to determine where species are backed up from an inlet by a closed valve somewhere.

#### Trapped Material

Species $k$ is trapped in side $j$ of connector $i$ only if the following statement is true.

$$\mathrm{IFS}(i,j,k) \leftarrow \left\{\begin{array}{l}\text{species } k \text{ is} \\ \text{present in side} \\ j \text{ of connector } i\end{array}\right\} \cdot \left\{\begin{array}{l}\text{side } j \text{ of connector} \\ i \text{ is not connected} \\ \text{to an open outlet} \\ \text{which is not} \\ \text{reached by species} \\ \text{coming from an} \\ \text{inlet}\end{array}\right\}$$
$$\cdot \left\{\begin{array}{l}\text{side } j \text{ of connec-} \\ \text{tor } i \text{ is not} \\ \text{connected to an} \\ \text{inlet where spe-} \\ \text{cies } k \text{ is present}\end{array}\right\} \cdot \left\{\begin{array}{l}\text{side } j \text{ of connector} \\ i \text{ is not included} \\ \text{in an open path}\end{array}\right\}$$

The last two propositions are the complements of the previously defined variables, $\mathrm{IAC}(i,j,k)$, $\mathrm{IPT}(i,j)$, and $\mathrm{ISRC}(i,j)$. The first and second propositions are new variables.

$\mathrm{ISAT}(i\,j,k)$: Species $k$ is present in side $j$ of connector $i$ (12)

$\mathrm{INACT}(i,j)$: Side $j$ of connector $i$ is not connected to an open outlet which is not reached by species coming from an inlet. (13)

Species $k$ is present in side $j$ of connector $i$ if (a) species $k$ is present at any of the half connectors joined to node $j$ or if (b) species $k$ is present at side $l$ and the valve is open, or (c) if species $k$ was present at side $j$ of connector $i$ at the previous operating increment.

$$\mathrm{ISAT}(i, j, k) \leftarrow [\sum_{a_m} \mathrm{ISAT}(a_m, j, k)]$$

$$+ \mathrm{ISAT}(i, l, k) \cdot v(i) + \mathrm{ISAT}^{*}(i, j, k) \qquad \text{(i)}$$

where (*) denotes the last operation time.

The variable INACT$(i, j, k)$ indicates when species cannot be trapped as they leave through open outlet paths. This is a deactivation condition.

$$\mathrm{INACT}(i, j) \leftarrow [\mathrm{INACT}(i, l) + \mathrm{INI}(i, l) + \overline{v(i)}]$$

$$\cdot \overline{[\sum_{a_m} \overline{\mathrm{INACT}}(a_m, j)} + \mathrm{INI}(i, j)] \qquad \text{(j)}$$

The term INACT$(i, l)$ + INI$(i, l)$ + $\overline{v(i)}$ states that if the valve of the connector is open, side $j$ of connector $i$ is deactivated if side $l$ is deactivated and is not reached by an inlet. If the valve is open and side $l$ is not deactivated or if the valve is closed, the state of side $j$ depends on the value of the terms in the second bracket. The terms in the second bracket mean that if side $j$ of connector $i$ has been reached by species coming from an inlet, the deactivation condition can not come from this side. But if that side is not reached by species coming from inlets, it is deactivated if any of the half connectors joined to it are deactivated.

Table 3. Initial State of the Catalyst Reactivation System Shown in Figures 1 and 2

| Connector | Node | Species | State |
|---|---|---|---|
| 1 | 1 | 1 | T |
| 2 | 2 | 2 | I |
| 3* | 2 | 2 | I |
| 4 | 2 | 4 | T |
| 5* | 2 | 4 | I |
| 6* | 2 | 2 | I |
| 7 | 1 | 1 | T |
| 9 | 2 | 4 | T |
| 10 | 2 | 1 | T |
| 10 | 1 | 1 | T |
| 12* | 1 | 2 | I |
| 13* | 2 | 1 | I |
| 13 | 1 | 2 | I |
| 14 | 2 | 1 | T |
| 14 | 1 | 1 | T |
| 15 | 2 | 2 | I |
| 15 | 1 | 2 | I |
| 17* | 1 | 1 | I |
| 19 | 2 | 2 | I |
| 19 | 1 | 2 | I |
| 20* | 2 | 2 | I |
| 20 | 1 | 4 | I |
| 21 | 2 | 2 | I |
| 21 | 1 | 2 | I |
| 22* | 2 | 4 | I |
| 23 | 2 | 4 | T |
| 23 | 1 | 4 | T |
| 24 | 2 | 4 | T |
| 24 | 1 | 4 | T |
| 25 | 2 | 2 | I |
| 25 | 1 | 2 | I |
| 26* | 1 | 1 | I |
| 27* | 2 | 2 | I |

Note: Only connectors with species are included in this table.
* Denotes closed valves, valves otherwise open
$T$ if IFT$(ijk)$ = 1
$I$ if IFI$(ijk)$ = 1
S if IFS$(ijk)$ = 1
$N$ if empty

This then completes the final expression for trapped species.

$$\mathrm{IFS}(i, j, k) \leftarrow \mathrm{ISAT}(i, j, k) \cdot \mathrm{INACT}(i, j)$$

$$\cdot \overline{\mathrm{IAC}(i, j, k)} \cdot \overline{\mathrm{IPT}(i, j)} \cdot \overline{\mathrm{ISRC}(i, j)} \qquad \text{(k)}$$

Equations (a) through (f) constitute the basic model of the system, representing a large number of individual sequential logic equations for industrial systems with reasonable numbers of connectors $i$ and species $k$. Special forms of the equations occur at inlet and outlet connectors, and these are not mentioned here (Rivas, 1973). The input data to this model of the system includes the system structure, the identification of input and output connectors, the previous location of species in the system and the proposed valve changes. The computer forms and solves the equations specific to the problem encountered and determines the consequences. We outline this in the following example.

### Catalyst Reactivation System

It is useful to illustrate the capability of the Operations Procedure Analysis Program on an industrial example. Our testing has been on the Catalyst Regeneration System mentioned previously and on a larger Hydrogen Drying System. The following operations are to be performed on the system shown in Figure 2 which initially is found in the state shown in Table 3.

1. Replace reactor in service and stop hydrocarbon flow in reactor to be reactivated.
2. Purge hydrocarbons from reactor with hydrogen.
3. Pressurize reactor with hydrogen.
4. Depressurize reactor and remove hydrogen.
5. Pressurize with inert gas.
6. Circulate inert gas.
7. Divert total flow of inert gas to reactor.
8. Chlorinate and rejuvenate catalyst.
9. Pressurize with inert gas, chlorine, and oxygen.
10. Depressurize and evacuate reactor.
11. Pressurize with natural gas.
12. Purge with natural gas.
13. Stop flow of natural gas.
14. Purge with hydrogen.
15. Pressurize with hydrogen.
16. Depressurize and evacuate hydrogen, start hydrocarbon flow, stop hydrocarbon flow in other reactor and leave hydrogen in the upper header. Each of these steps have several sequential valve operations (Tables 4 through 6).

Tables 4 through 6 show the material movement predicted by the Operation Procedure Analysis Program, showing only the connectors which experience a change at any given time. We have not included all of the regeneration operations here since the tables become very extensive especially for the later operations where a number of things occur simultaneously.

The generation of these tables by hand is particularly troublesome and subject to error, taking a day or so of careful study. The computer took less than 15 seconds of UNIVAC 1108 time, at an average time of 0.4 seconds per valve operation. Our tests indicate that the program is ready for industrial application. We recommend that the reader examine Tables 4 through 6 in detail in preparation for the next section on safety-interlock design.

## ADAPTIVE SAFETY INTERLOCK SYSTEMS

The operations analysis program developed in the previous section is the basic starting point for the development of interlock capability. Each valve change proposed

Table 4. Results of the Operations in Step 1 for Reactivating the Catalyst

| Operation | Connector | Node | Species | State |
|---|---|---|---|---|
| Open valve 26 | 8 | 2 | 1 | I |
| | 11 | 3 | 1 | I |
| | 11 | 2 | 1 | I |
| | 18 | 2 | 1 | I |
| | 26 | 3 | 1 | I |
| | 27 | 3 | 1 | I |
| Open valve 8 | 8 | 2 | 1 | T |
| | 11 | 3 | 1 | T |
| | 11 | 2 | 1 | T |
| | 26 | 3 | 1 | T |
| | 26 | 1 | 1 | T |
| Close valve 14 | 7 | 1 | 1 | N |
| | 10 | 2 | 1 | N |
| | 10 | 1 | 1 | N |
| | 13 | 2 | 1 | N |
| | 14 | 2 | 1 | N |
| | 14 | 1 | 1 | I |
| | 17 | 1 | 1 | N |

Table 5. Results of the Operations in Step 2 for Reactivating the Catalyst

| Operation | Connector | Node | Species | State |
|---|---|---|---|---|
| Open valve 13 | 2 | 2 | 2 | T |
| | 7 | 1 | 2 | T |
| | 10 | 2 | 2 | T |
| | 10 | 1 | 2 | T |
| | 13 | 2 | 2 | T |
| | 13 | 1 | 2 | T |
| | 14 | 2 | 2 | I |
| | 15 | 2 | 2 | T |
| | 15 | 1 | 2 | T |
| | 17 | 1 | 2 | I |
| | 19 | 2 | 2 | T |
| | 19 | 1 | 2 | T |
| | 25 | 2 | 2 | T |
| | 25 | 1 | 2 | T |

by the operator is monitored by the computer and only those operations are allowed which do not initiate operation sequences leading to disaster. The speed at which the computer can perform this service, in fractions of a second, allows the real time adaptation of the safety interlock system to the current condition of the process. In effect, the Adaptive Safety Interlock System is a filter which allows only safe operating instructions to pass through to the process, and it is only with an over-ride capability that the interlock ought to be bypassed.

The empirical and a priori development of interlock capability is a standard practice in process development [(see for example, Kletz, 1972; Browning, 1970)]. For normal operation, start-up, shut down, and certain emergency situations, well thought out procedures are established which prevent certain sequences of valve operations which are directly hazardous or which come too close to being hazardous. For example, the policy may be established that the system ought to be at the least one or two operation errors from a hazardous condition. Unfortunately, there are situations in which the predeveloped interlock procedures have been applied in unusual situations in which they were contributing factors in the propagation of a disaster. All possibilities cannot be anticipated, and we must be able to analyze situations as we are thrown into them in an emergency. We now show how this can be done by the computer once the logic of safety interlock systems is available.

We use the Catalyst Regeneration System to illustrate the features to be built into the interlock logic. The major safety considerations are: (a) the hydrocarbon inlet must not be connected by an open path to either the hydrogen or natural gas inlets. (b) The hydrogen inlet must not be connected by an open path to the natural gas inlet. (c) The hydrocarbons, hydrogen, and natural gas must not be mixed with inert gas, oxygen, or carbon tetrachloride. (d) The flow of hydrocarbons and inert gas must never be blocked. (e) Oxygen and carbon tetrachloride must never flow to the hydrocarbon outlets. (f) Hydrocarbons must never appear in the upper and lower reactor headers. (g) Hydrogen and natural gas must never go into the lower reactor headers. These constraints are shown in Table 7. This is the kind of information handling capability that must be built into the interlock logic.

Next we illustrate the empirical reasoning used to develop an a priori interlock procedure, prior to the general development. We wish to avoid reliance on this kind of analysis. Valve 2 in Figure 3 can only be opened if valve 3 is closed, or else the hydrogen and natural gas inlets will be connected. If valve 3 is closed, valve 2 can be opened if valve 25 is closed. If valve 25 is open, valve 2 can be opened only if valves 6 and 20 are closed, to avoid the connection of the inert gas and carbon tetrachloride inlets with the hydrogen inlet. If valves 6 and 20 are closed,

Table 6. Results of the Operations in Step 3 for Reactivating the Catalyst

| Operation | Connector | Node | Species | State |
|---|---|---|---|---|
| Close valve 7 | 2 | 2 | 2 | I |
| | 7 | 1 | 2 | I |
| | 10 | 2 | 2 | I |
| | 10 | 1 | 2 | I |
| | 13 | 2 | 2 | I |
| | 13 | 1 | 2 | I |
| | 15 | 2 | 2 | I |
| | 15 | 1 | 2 | I |
| | 19 | 2 | 2 | I |
| | 19 | 1 | 2 | I |
| | 25 | 2 | 2 | I |
| | 25 | 1 | 2 | I |
| Close valve 25 | 6 | 2 | 2 | S |
| | 7 | 1 | 2 | S |
| | 10 | 2 | 2 | S |
| | 10 | 1 | 2 | S |
| | 12 | 1 | 2 | S |
| | 13 | 2 | 2 | S |
| | 13 | 1 | 2 | S |
| | 14 | 2 | 2 | S |
| | 15 | 2 | 2 | S |
| | 15 | 1 | 2 | S |
| | 17 | 1 | 2 | S |
| | 19 | 2 | 2 | S |
| | 19 | 1 | 2 | S |
| | 20 | 2 | 2 | S |
| | 21 | 2 | 2 | S |
| | 21 | 1 | 2 | S |
| | 25 | 1 | 2 | S |
| | 27 | 2 | 2 | S |
| Close valve 2 | 2 | 2 | 2 | S |
| | 3 | 2 | 2 | S |
| | 25 | 2 | 2 | S |

Note: Sometimes it is desired to pressurize by trapping species and sometimes may be convenient to pressurize from an inlet.

Table 7. Safety Constraints for the Catalyst Regeneration System

| Must not mix | Must not connect inlets | Must not block flow | Must not flow at outlets 7 and 8 | Must not be at reactor headers |
|---|---|---|---|---|
| 1, 4 | 1, 2 | 1 | 4 | 1 (upper and lower headers) |
| 1, 5 | 1, 3 | 4 | 5 | |
| 1, 6 | 2, 3 | | 6 | |
| 2, 4 | | | | 2, 3 (lower header) |
| 2, 5 | | | | |
| 2, 6 | | | | |
| 3, 4 | | | | |
| 3, 5 | | | | |
| 3, 6 | | | | |

Note: The species nomenclature is from Figure 2.

Table 8. Meaning of the Combination of Values of the Variables PT($t$), PI($t$), PS($t$)

| PT($t$) | PI($t$) | PS($t$) | Meaning |
|---|---|---|---|
| 1 | 0 | 0 | Species $k(t)$ must always be flowing at side $j(t)$ of connector $i(t)$ |
| 0 | 1 | 0 | Must always be coming from inlet |
| 0 | 0 | 1 | Must always be trapped |
| 1 | 1 | 0 | Must always be flowing or coming from an inlet |
| 1 | 0 | 1 | Must always be flowing or trapped |
| 0 | 1 | 1 | Must always be coming from an inlet or trapped |
| 1 | 1 | 1 | Must always be present in any state |

valve 2 can be opened if valve 12 is closed and if valves 13, 14, 17, and 18 do not allow an open path between the reactor headers. The position of valve 22 is not critical because if 22 is open inert gas and oxygen cannot go into the upper reactor header, and if it is closed hydrogen cannot go into the lower header. The empirical interlock logic for the opening of valve 2 is thus

valve 2 can be opened if this statement is true :

$$\overline{v(3)}\ \overline{[v(25)} + \overline{v(6)} \cdot \overline{v(20)} \cdot \overline{v(12)} \cdot \overline{(v(13)} + \overline{v(17))} \cdot \overline{(v27)} + \overline{v(18))]}$$

This is one of the simplest interlock conditions for this process and, at that, is valid only if certain preconceived conditions exist. For example, if it were discovered that by some previous error oxygen had found its way into connector 19, the application of this interlock procedure would lead to disaster. We cannot rely on this slow and error prone analysis.

We now develop general logic statements of events to be avoided, so that the computer can handle these complicated problems.

### Connecting Inlets

For species $A_p$ and $B_p$ whose inlets are not to be connected by an open path the following variable is defined:

RSI($i$): The opening of valve $i$ does not create a hazard by connecting two inlets. (14)

along with statement 3 in the previous section

IFI($i, j, k$): species $k$ has reached side $j$ of connector $i$ from an inlet but there is no flow (3)

to develop

$$\mathrm{RSI}(i) \leftarrow \overline{[\mathrm{IFI}(i, j, A_p)} + \overline{\mathrm{IFI}(i, l, B_p)]} \cdot \overline{[\mathrm{IFI}(i, j, B_p)} + \overline{\mathrm{IFI}(i, l, A_p)]} \quad (1)$$

For the special case of the Catalyst Regeneration System, three pairs of inlets must not be connected, as shown in Table 11.

### Mixing of Species

The following variable is defined:

RSIS($i$): The opening of valve $i$ does not create a hazard by mixing (15)

A group of species which cannot be mixed is represented by the index $p$ and the hazard occurs only if there are $q_p$ species present in a subgroup which will be mixed with $r_p$ species present in another subgroup, where all species must be present to cause the hazard. Using the variables previously defined,

$$\mathrm{RSIS}(i) \leftarrow \left[\left\{\begin{matrix}\overline{(\mathrm{IFI}(i, j, C(p, 1)) + \mathrm{IFS}(i, j, C(p, 1)))\cdot\ldots} \\ (\mathrm{IFI}(i, j, C(p, q_p)) + \mathrm{IFS}(i, j, C(p, q_p)))\end{matrix}\right\} + \left\{\begin{matrix}\overline{(\mathrm{IFI}(\mathrm{i}, l, D(p, 1)) + \mathrm{IFS}(i, l, D(p, 1)))\cdot\ldots} \\ (\mathrm{IFI}(i, l, D(p, r_p)) + \mathrm{IFS}(i, l, D(p, r_p)))\end{matrix}\right\}\right] \cdot \left[\left\{\begin{matrix}\overline{(\mathrm{IFI}(i, j, D(p, 1)) + \mathrm{IFS}(i, j, D(p, 1)))\cdot\ldots} \\ (\mathrm{IFI}(i, j, D(p, r_p)) + \mathrm{IFS}(i, j, D(p, r_p)))\end{matrix}\right\} + \left\{\begin{matrix}\overline{(\mathrm{IFI}(i, l, C(p, 1)) + \mathrm{IFS}(i, l, C(p, 1)))\cdot\ldots} \\ (\mathrm{IFI}(i, l, C(p, q_p)) + \mathrm{IFS}(i, l, C(p, q_p)))\end{matrix}\right\}\right] \quad (\mathrm{m})$$

In the Catalyst Reactivation System, there are 9 different kinds of hazards that arise by the mixing of species with subgroup $q_p = r_p = 1$ (see Table 7).

### General Hazards

We now build up general hazards in terms of a series of elementary logic conditions.

PT($t$) species $k(t)$ must be always flowing at side $j(t)$ of connector $i(t)$ (16)

PI($t$) species $k(t)$ must be always coming from an inlet at side $j(t)$ of connector $i(t)$ (17)

PS($t$) species $k(t)$ must be always trapped at side $j(t)$ of connector $i(t)$ (18)

$\overline{\mathrm{QT}}(t)$ species $k(t)$ must never be flowing at side $j(t)$ of connector $i(t)$ (19)

$\overline{\mathrm{QI}}(t)$ species $k(t)$ must never be coming from an inlet at side $j(t)$ of connector $i(t)$ (20)

$\overline{\mathrm{QS}}(t)$ species $k(t)$ must never be trapped at side $j(t)$ of connector $i(t)$ (21)

Table 9. Meaning of the Combination of Values of the Variables QT($t$), QI($t$), QS($t$)

| $\overline{QT}(t)$ | $\overline{QI}(t)$ | $\overline{QS}(t)$ | Meaning |
|---|---|---|---|
| 0 | 1 | 1 | Species $k(t)$ must never be flowing at side $j(t)$ of connector $i(t)$ |
| 1 | 0 | 1 | Must never be coming from an inlet |
| 1 | 1 | 0 | Must never be trapped |
| 0 | 0 | 1 | Must never be flowing or coming from an inlet |
| 0 | 1 | 0 | Must never be flowing or trapped |
| 1 | 0 | 0 | Must never be coming from an inlet or trapped |
| 0 | 0 | 0 | Must never be present in any state |

Table 10. Positive After-Operation Restrictions for the Catalyst Regeneration System

| $t$ | $i(t)$ | $j(t)$ | $k(t)$ | PT($t$) | PI($t$) | PS($t$) |
|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 | 0 | 0 |
| 2 | 9 | 2 | 4 | 1 | 0 | 0 |

Table 11. Negative After-Operation Restrictions for the Catalyst Regeneration System

| $t$ | $i(t)$ | $j(t)$ | $k(t)$ | $\overline{QT}(t)$ | $\overline{QI}(t)$ | $\overline{QS}(t)$ |
|---|---|---|---|---|---|---|
| 1 | 15 | 1 | 1 | 0 | 0 | 0 |
| 2 | 16 | 2 | 1 | 0 | 0 | 0 |
| 3 | 16 | 2 | 2 | 0 | 0 | 0 |
| 4 | 16 | 2 | 3 | 0 | 0 | 0 |
| 5 | 7 | 1 | 4 | 0 | 1 | 1 |
| 6 | 7 | 1 | 5 | 0 | 1 | 1 |
| 7 | 7 | 1 | 6 | 0 | 1 | 1 |
| 8 | 8 | 2 | 4 | 0 | 1 | 1 |
| 9 | 8 | 2 | 5 | 0 | 1 | 1 |
| 10 | 8 | 2 | 6 | 0 | 1 | 1 |

where the index $t$ denotes the constraint number. Then if

IRZ: a general hazard exists other than those caused by connecting inlets or mixing species (22)

$$\mathrm{IRZ} \leftarrow \left[ \prod_{t=1}^{\mathrm{NAO}} (\mathrm{PT}\cdot\mathrm{IFT} + \mathrm{PI}\cdot\mathrm{IFI} + \mathrm{PS}\cdot\mathrm{IFS} \right] \cdot \left[ \prod_{t=1}^{\mathrm{NAN}} (\mathrm{QT}\cdot\mathrm{QI}\cdot\mathrm{QS}\cdot\overline{\mathrm{IFT}}\cdot\overline{\mathrm{IFI}}\cdot\overline{\mathrm{IFS}} + \mathrm{QT}\cdot\mathrm{QI}\cdot\overline{\mathrm{QS}}\cdot\overline{\mathrm{IFT}}\cdot\overline{\mathrm{IFI}} + \overline{\mathrm{QT}}\cdot\mathrm{QI}\cdot\mathrm{QS}\cdot\overline{\mathrm{IFI}}\cdot\overline{\mathrm{IFS}} + \mathrm{QT}\cdot\overline{\mathrm{QI}}\cdot\mathrm{QS}\cdot\overline{\mathrm{IFT}}\cdot\overline{\mathrm{IFS}} + \overline{\mathrm{QT}}\cdot\mathrm{QI}\cdot\overline{\mathrm{QS}}\cdot\overline{\mathrm{IFI}} + \mathrm{QT}\cdot\overline{\mathrm{QI}}\cdot\overline{\mathrm{QS}}\cdot\overline{\mathrm{IFT}} + \overline{\mathrm{QT}}\cdot\overline{\mathrm{QI}}\cdot\mathrm{QS}\cdot\overline{\mathrm{IFS}}) \right] \quad \text{(n)}$$

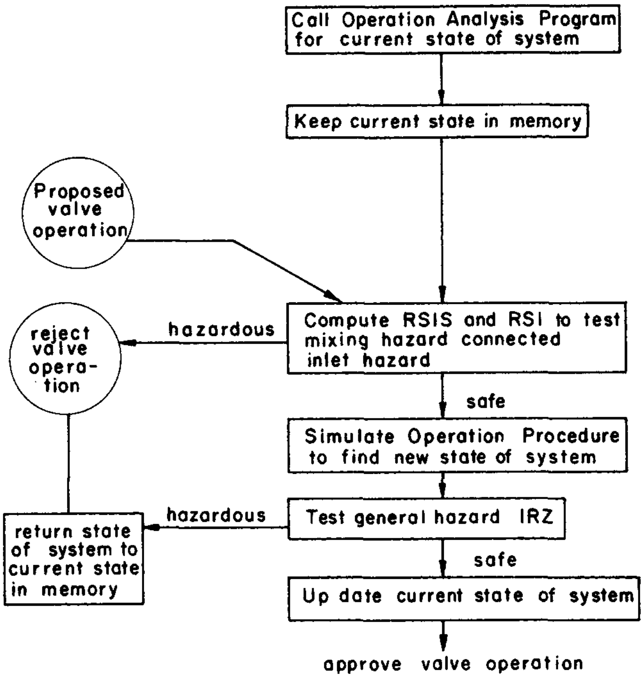
Call Operation Analysis Program for current state of system
Keep current state in memory
Proposed valve operation
Compute RSIS and RSI to test mixing hazard connected inlet hazard
hazardous
reject valve opera-tion
safe
Simulate Operation Procedure to find new state of system
Test general hazard IRZ
hazardous
return state of system to current state in memory
safe
Up date current state of system
approve valve operation

Fig. 7. Adaptive safety interlock system.

The desired or undesired state of species $k(t)$ in side $j(t)$ of connector $i(t)$ can be completely specified by the three values of PT($t$), PI($t$), and PS($t$) or the three values of QT($t$), QI($t$) and QS($t$). Tables 8 and 9 describe the meaning of all the possible combinations. Tables 10 and 11 describe the after-operation safety restrictions for the Catalyst Regeneration System, which together with the first two columns of Table 7 (before-operation restrictions) is all the necessary information for the Computer Interlock System.

All the general Boolean equations described for the Computer Interlock System can be programmed with a surprising small number of statements. Figure 7 illustrates the application of this interlock language. Our experience indicates that this Safety Interlock System does not permit us to force hazardous operations onto the industrial systems examined.

## ACKNOWLEDGMENT

Work performed at the University of Wisconsin with the support of the National Science Foundation, Shell Oil Foundation, and the United States Army.

## LITERATURE CITED

Browing, C. L., *Accident Prevention and Loss Control,* American Management Association, New York (1970).

Dietmeyer, D. L., *Logic Design of Digital Systems,* Allyn and Bacon, New York (1971).

Kletz, T. A., "Specifying and Designing Protective Systems," Loss Prevention No. 6 Chemical Engr. Prog. Tech. Man. (1972).

Rivas, J. R., Ph.D. thesis, Univ. Wisconsin, Madison (1973).

———., and D. F. Rudd, "Synthesis of Failure—Safe Operations," *AIChE J.*, **20**, 000 (1974).

*Manuscript received September 11, 1973; revision received December 19 and accepted December 20, 1973.*