The detection for the digital devices was programmed in the same form as shown in the constructs given in Appendix C, section C.1 . Word logic was used on the pumps and valves in groups and this proved affective in coding. The safety and indicator limit switches were dealt with separately, as most were critical condition indications.

Tne analogue signals were considered differently. In the same form as the analogue fault constructs of Appendix C, section C.1, the temperature measurements had a zero and full-range check of 3.0 and 95.0 degrees Centigrade. This was necessary to detect critical cooling or heating fault, ie. near freezing or boiling conditions.

Under control conditions, heating and cooling control limits were set which are controlled using Proportional, Intergral and Differential (PID) control.

5.1.2 Fault Recovery

If one considers the simple and complex fault recovery strategies as given in Table 3.1, section 3. , it can be seen that all strategies are used in this process.

Simple digital and analogue fault recovery can be viewed as normal control functions, eg. the three and four stage heater systems were controlled in a "bang-bang" mode, where the temperature low and high conditions would switch ON and OFF the heaters respectively.

The general control strategy for the analogue control loops, ie. bang-bang and PID loops are not catered for in a complex fault recovery strategy. However, if the temperatures measured are outside the general operating bandwidth, then all operation is aborted.

The complex fault recovery strategies used for this process involved both back-up or redundant systems and state restoration.

As given in Figure 5.1 , the plant has incorporated a number of back-up systems. These include for the following :-

- vacuum systems
- resin feed systems
- safety systems

In general, the construct g[illegible]n Appendix C, section C.2 for redundant control was used. If a certain item in the resin transfer system being operated is detected, (for both pumps and isolating valves), then switchover to standby is performed, and this reported on the printer. This is also true of the vacuum systems, of which there are two lines of vacuum pumps. For both the vacuum and the resin feed systems, if the standby devices also failed, then complete aborting of the process cycle would be performed.

The safety systems included duplicated impregnator tank full indicators, and differential pressure limit switches across the resin transfer filter for indicating a blocked filter.

If the resin transfer was being done and the first impregnator full indicator did not activate, the resin would be continually heated to impregnation temperature and pumped into the impregnator. This is protected by the second full indicator, and when activated, a fault message is printed, (see Appendix A, section A.3.3).

If the first differential pressure switch is activated, then the next process to be done is prohibited until the filter is cleaned, signalled by the maintenance mode being selected. If the filter is not cleaned, and the standby limit switch is activated, then an abort sequence is performed, protecting against burning the resin feeder pumps out while attempting to pump through a blocked filter.

One of the major concerns of the customer for this process was what conditions could be catered for when an " unplanned shutdown " occurred due to power failure, (see Appendix A for details of the following descriptions).

Unplanned shutdown fault action occurring during a process cycle was determined by the step in the sequence which was being performed just prior to the power failure. This can be viewed as the implementing of complete and conditional state restoration and backward and forward recovery, as shown in Figure 5.2 .

If the process had just been started, (step 01), or if the vacuum had just been started, (step 02), then the process is not affected, and is continued, ie. complete state restoration.

If the operating vacuum had been reached and maintained during the unplanned shutdown, (step 03), then a backward recovery is initiated and the cycle is restarted from the beginning of the vacuum step. If the vacuum had fallen after resin transfer had been started or during the 'wet' vacuum step, (step 04 or 05 respectively), then forward recovery is initiated and any resin which had been transferred to the impregnating vessel must be cooled and transferred back to the storage vessel and then the process is ended normally.

If the process had begun the pressurising sequence, (steps 06 - 08), then the temperature of the unit being impregnated must be kept within the impregnating bandwidth for efficient impregnation. If it was good,then continue the cycle, else the pressurising time was doubled to adapt to the change in impregnation properties of the resin on a too hot or cold stator or rotor. This can be seen as a conditional state restoration, where the operation is continued as if a complete state restoration, but the process parameter for pressure time has been conditionally doubled.

Once the return of the resin had been initiated, (from step 09 - 11), then the cycle would just continue as a complete state restoration.

Semi-automatic process cycles would have the same fault recovery procedure.

In the Rest, Refill, Sampling, Maintenance modes and under manual control, the process is not affected and a complete state restoration is done. No fault recovery is necessary except to restore the plant state for the particular mode.

Apart from the unplanned shutdown fault recovery strategies, certain additional faults had to be recognised during normal operating conditions and acted upon, (see Appendix A, section A.3.3).

Any valve malfunction causes the process to be stopped until the valve corrects itself. Combinations of valve statii are usually necessary for the process to continue smoothly.

Redundant systems, as stated above for the vacuum and resin feeder systems are also programmed to react when faults occur on the system in use. The state restoration intiated is such that the recovery to the backup sub-system ensures a state of vacuum control or continuation of resin transfer to or from the impregnator.

5.1.3 System Implementation

The system comprises of two basic hardware systems, viz. dedicated instumentation and a Programmable Logic Cotroller (PLC).

The analogue signals for the temperature , the vacuum and pressure sensors are all directed through transducer modules. Other dedicated instrumentation for level sensing and excess differential pressure detection were also used.

The control and fault recovery system was implemented using a GEM 80 130/12K Programmable Logic Controller, [30, 31]. The general modes of operation are automatic, semi-automatic and manual control, and fault recovery control, as given in Appendix A.

The automatic mode is selected by the operator through a keyboard interface. Different process parameters are used for differing voltage sizes of machines which are impregnated. If a special machine is to be impregnated, the unique process parameters can be set for semi-automatic control, and each step in the control sequence is initiated by the operator.

When no impregnation is being done, the system is considered to be in Rest mode. The resin used in the process is stored in conditions which do not cause the resin to react and cure naturally, ie. with low temperature and under vacuum. The resin condition can be tested in the Sampling mode, to determine if resin should be replaced. As more processes are done, the resin must be replenished, and this is done in the Refill mode. The maintenance and testing of all plant equipment can be done in the Maintenance mode.

In Figure 5.3 the level heirarchy of the control system for the VPI plant is given, as discussed in section 4.

The level 0 of this system comprises all the mechanical equipment. Design safety factors were included, eg. the impregnation vessel was designed to withstand vacuum much lower than all the vacuum pumps could produce if these all failed in a running condition. It was also designed to withstand pressures at least 300 to 500 kPa greater than producible from the pressurising system.

Level 1 systems would include plant safety interlocks and safe operating modes, eg. the impregnation vessel could not be opened without operating the lid closed limit switches, and even if the retaining and locking ring for the lid were opened under pressure conditions, the lifting of the lid had hardwired controls which causes the lid to pause at a position just open to allow venting without blowing the lid off.

Level 2 of the system includes for the manual controls available with the GEM 80 processor operational, and device controls affected in the Maintenance mode. This would overlap with the other semi-automatic modes (eg. Refill), as manual functions under software control.

Levels 3 and up to 6 would typically include the semi-automatic and the fully automatic process cycles, with all the parameter control functions, fault recovery systems and interlocks.

Above level 6 would be the alarm and event printing routines and the operator interfaces.

It can be seen that if and when the PLC fails, the manual controls provided allow the plant to be brought into a safe condition by the control of all critical devices and sub-systems, viz. the vacuum and resin transfer sub-systems, (pumps and control valves), and the heating and cooling sub-systems. Under extreme operating conditions, the process cycle can be performed using the manual controls, but this is prone to high error and wide control bandwidths for the heating, cooling, vacuum and pressure control. The level system as discussed above would degrade to a level 0 system, with some of level 1 systems operational. This means that the plant items were specified and designed to be capable of all loading which could possibly be brought to bear on the equipment.

Standby systems for sub-systems other than the vacuum, resin feed and critical indicator sub-systems of the plant were not deemed necessary. Any faults in these other systems would cause control to be lost, and complete aborting of the process cycle to be initiated, ie. shutdown to a safe state with all outputs OFF, and valves and pumps in rest positions.

General device malfunctions causes the fault to be reported first, and if the device is critical to the cycle sequence, the process may also be halted until it is corrected by manual interventtion or natural (slow) operation.

5.1.4 Case study Evaluation

No redundancy in the process control PLC was included in this project. The underlying reasons for standby computer hardware as detailed in section 4.3 are relevant, viz. the waste of the redundant PLC's waiting for a failure in the working PLC, the cost of the redundant PLC's, and the reluctance to accept complete computer control of a process plant.

The author feels that the fault detection system for the digital and analogue I/O was good enough for the size and complexity of the process. This could well have been extended with multiple redundant I/O and control devices, but the cost would have been significant. The complexity of voting and deciding on faulty inputs would have extended the program beyond the memory capacity of the GEM 80/130 (12K) processor.

The fault recovery implementation was carefully prepared to allow for the more common faults possible. All the faults detected were reported even if no fault recovery was implemented, so that the operator could decide if the fault was serious, and then possibly correct the fault without aborting the process.

The PLC control system was not configured with expansion in mind, and this could restrict future additions to control and fault recovery strategies.

It was found that the control program and fault recovery system with their complex message reporting principles have used up all the memory capacity for user program in the GEM 80/130 12K. This is most probably due to a number of factors :-

(1) The complexity of the control and fault recovery scheme was not fully realised, ie. underestimation of software effort. The requirements for memory size is easily understated to the detriment of the final implementation. It may have been possible to split the functions required of the controlling system and use a number of PLC's or similar systems in a heirarchical and distributed function computer control system.

(2) The restriction of memory capacity of the PLC used was repeatedly overcome by rehashing of the software and the operating procedures. This was to the detriment of special messages designed for all the faults detected, and detrimental to the ease of use by the operator.

(3) This plant was developed with trainee engineering time, which caused inefficient programming and utilisation of special features available in the PLC system software.

5.2 CASE II - A Distributed Conveyor Control System

This application involves the complex routing and control of conveyors in a coal mine stockyard, for Anglo-America's New Denmark Colliery and Tutuka Power Station stockyard. The strategy of the computer control implementation is to use dedicated Programmable Logic Controllers for each sub-system of the stockyard.

The stockyard topography is illustrated in Figure 5.4 . From the mine an underground conveyor loads into a 6 000 tonne transfer silo, and then across a 3 - 4 km conveyor from the mine itself to a large 12 000 tonne silo, from which feeder conveyors convey the coal to the crushing plant. The crushed material is then passed into the main routing system which comprises six transfer towers and numerous bi-directional flopper gates and conveyors. A Sampling plant is included in this main transfer system. The coal can then be routed to any of three stacker-reclaimers, a rail loadout facility, and to the power station. Phase I of the A stream system of this contract is completed, and Phase II or the B stream is currently being engineered. Phase II is basically a duplication of Phase I. Coal from the stockpiles can also be reclaimed and rerouted to either of the rail loadout facility or the power station.

Details of the control philosophy for this project are given in Appendix B, and in [38]. The control and supervisory system for the stockyard covers two main operational areas, as follows :-

Area 1 :- Control over logically grouped areas is done by individidual control PLC's performing such functions as sequencing, interlocking and continuous analogue control.

Area 2 :- The supervisory control and monitoring system in the central control building. The function of this system is to display the status of all plant unit operations and form the operator interface.

5.2.1 Fault Detectior

Fault detection of the control equipment is done in the control PLC's.

All conveyor manual start and stop pushbuttons, and the trip and contactor closed contacts and stop wires along each conveyor are monitored.The trip and contactor closed contact inputs are used to detect if a drive which is commanded to operate is working correctly. A stop wire along a conveyor is used by the controlling PLC to immediately stop the conveyor.

In the supervisory scheme, any conveyor operating in a manual manner, ie. started and stopped with the pushbuttons, is considered an alarm condition as this is not an automatic event.

The operation of all control equipment is monitored through the feedback signals, and detection of faults, eg. trips and stops unhealthy, is done by using logic as given in the constructs, Appendix C, section C.1.3 .

The analogue values, eg. belt weighers, feeder speeds, are not generally used in a fault detection scheme. All relevant parameter values are sent to the supervisory PLC for display. As given in Appendix B, section B.4, an alarm is generated from the belt weigher information when the supply of coal from the mine is insufficient according to the demand of the power station.

The route selection command causes all current alarm conditions for all conveyors of that route to be sent back to the supervisory PLC. This is necessary because of the large number of faults that can be present at any time especially if the route is non-operational or being repaired. The selection of a route can be a combination of conveyors in a number of the controlling PLC's. All operational alarm are detected using word constructs where possible. To find the relevant alarms for the routes selected, multiple mask word sets are used in each of the control PLC's. Then, by using pattern recognition and template matching as detailed in the software constructs for fault detection in Appendix C, section C.1.2, the faults detected are sent to the supervisory console for display, printing and annunciation.

A combination of routes may be running at any one time, for which the operator must be aware of all alarms at all times. Combinations of mask words are also necessary to complete the fault detection.

The stacker/reclaimers, (stackers), form an integral part of the conveyor system and these also incorporate fault detection systems. The most important information the stackers handle is the relative position of the stackers to each other because the stackers can travel such that two stackers could collide. The stacker travel and the boom position are used to detect if a collision is possible. Other faults detected on the stackers are trips, stops and contact not closed/open. All faults pertinent to the stackers are signalled to the supervisory and to the alarm annunciator in each stacker control cab.

5.2.2 Fault Recovery

The fault recovery system is split into three parts depending on faults occurring during the following different operations :-

- Route selection
- Route starting
- Route running
- Route stopping

As given in Appendix B, section B.5, the route is selected before starting to establish that all devices are functional and to position flopper gates. The fault recovery for the route selection operation is an operator dependent function. The faults detected in the selection of the route are to pre-empt the operator to not start the route if a fault is present.

If an alarm condition occurs during a startup sequence of conveyors, the starting is aborted by the controlling PLC's, ie. a complete shutdown of the route is done. This can be viewed as either state restoration in it's most primitive form, or as a complete forward recovery to a condition of route stopped, or backward recovery to the beginning of the startup sequence. This is the simplest manner in which the fault recovery is possible. The operator at the supervisory is displayed messages for the alarms occurring, and mimics of the conveyor statii are also displayable. Once manual correction of the fault for the route being started up is done, the startup can be re-attempted.

The concept of the state restoration, forward and backward recovery for this is shown in Figure 5.5 . The state is shown in the sequence of operations, and a fault occurring while starting conveyor x can be seen as backward or forward recovery backwards or forwards to a all conveyor stopped state.

Fault recovery while a route is running enforces the stopping of the conveyor in which the fault has occurred and all the conveyors upstream of the faulted conveyor. All downstream conveyors will then stop sequentially, allowing time for each conveyor to empty so no coal is left on the conveyors. This can be termed partial shutdown, and then forward recovery into the normal sequential stop of all conveyors for the route. The partial shutdown and forward recovery sequence is shown in Figure 5.6.

Fault recovery while the route is stopping is affected depending on whether the fault occurs in a conveyor upstream or downstream of the conveyor presently being stopped.

If the fault is upstream then no fault recovery is affected as this can be seen as a special case of the above fault recovery for a fault while the route is running. Forward recovery of the above fault recovery for running has been affected, and the sequential stopping of downstream conveyors is being done.

If the fault is downstream then a partial state restoration is done to stop all conveyors up to and including the faulted conveyor, and then sequential stopping is done.

The system is basically a digital controlling system, ie. the majority of the control is in terms of ON, OFF, RUNNING, STOPPED, etc. types of inputs and outputs.

As was stated in section 5.2.1, the analogue parameter values are not included in the fault detection scheme. All parameters are sent to the supervisory for display. A particular case is detected where the supply of coal from the mine is insufficient to satisfy the demand of the power station. This is handled by alarming the condition on the visual display units, and relying on the operator to change the routing to satisfy the needs of the power station. As detailed in Appendix B, section B.4, the operator must switch to supplying coal from the stacker/reclaimers (Case 2).

Analogue control in the system is basically simple bang-bang and proportional control, eg. for feed-rate control of the coal in tonnes per hour. Thus, the analogues can be seen to be satisfied by simple fault recovery schemes which are considered normal control operations.

As the stacker/reclaimers, (stackers), form an integral part of the conveyor system, faults in the stacking or reclaiming operations affect the conveyor route/s being served by the stackers. These faults cause stopping of routes as discussed above.

5.2.3 System Implementation

The system is comprised of all basic hardware systems, viz. dedicated instrumentation, Programmable Logic Controllers (PLC's) for control, and a large PLC with video graphics for supervisory and a BASIC language PLC above the supervisory.

The belt weighers, silo levels, feeder speeds, etc. all form part of the dedicated instrumentation. These all connect to the control PLC's for which they function.

The control strategy of the distributed functions incorporates the simple fault detection and diagnosis systems. A heirarchical distributed system is implemented, as illustrated in Figure 5.7 . Both A and B streams must be considered as two completely independent control systems, although there are conveyors linking the two streams together. The controlling PLC's are all GEM 80 130/12K Programmable Logic Controllers, (PLC) , [30, 31].

The supervisory control system is a GEM 80 235/48K PLC, and the management information system is a GEM 80 235 BASIC Language PLC.

For both A and B streams, functions are split into four basic sub-systems, ie. the transfer silos and conveyors from the mine and the crusher plant, the transfer routing, the stacker-reclaimers, and other smaller sub-systems. On the coal mine system there are three GEM 80 130/12K PLC's. These are situated at the central mine 6 000 tonne silo, the overland conveyor control sub-station at the 12 000 tonne silo, and the crusher plant. The transfer routing system comprises two GEM 80 130/12K PLC's, housed in the main control station. Each of the three stacker-reclaimers have two GEM 80 130/12K PLC's. The other systems comprise the rail loadout facility, the sampling plant, and the control of the conveyors to the power station, each with one GEM 80 130/12K PLC.

In Figure 5.8 the appropriate levels according to that detailed in section 4. are also given.

The level 0 of this application is the conveyor equipment and all mechanical systems, eg. flopper gates, stacker-reclaimers, etc. . The level 1 of this system are the hardwired safety interlocks and protection systems, eg. trip and stop interlocks inserted in drive control wiring, speed switches, and stop wires along all conveyors.

From level 2 to level 6, the distributed control PLC's are implemented. Each PLC has the trip and stop functions wired into the input/output (I/O) of the PLC, with interlocking performed in software. Manual control functions are also available, (level 3). Routing data and commands are sent via serial links to the control PLC's from the supervisory, and the start-up and stopping of conveyors in sequence for any route is controlled here, (level 4 to 6). In the transfer control PLC's, the flopper gates must first be positioned according to which route has been selected, and then the command for sequential starting of the conveyors from the last backwards up to the first can then be initiated and performed. Stopping of the