The fault recovery effectiveness is dependent on the fault detection, the actual fault recovery, and the complete system design and implementation. The constructs of Appendix C form the basis for effective fault detection and recovery. For system design and implementation, I believe that the future for fault recovery in process control is based on a level-based heirarchical control system design. Distributed Computer Control Systems and a distributed fault detection, diagnosis and recovery strategy will then form an integral part of this level-based heirarchical control system.

APPENDIX A. CASE STUDY I

A VACUUM PRESSURE IMPREGNATION PLANT

A simplified extract of the full functional specification for the VPI plant, [37].

The information contained in this Appendix contains confidential information, and may not be disclosed to any third party without the written consent of G.E.C. System Engineering Company.

A.1 PROGRAMMABLE CONTROLLER SPECIFICATION

A GEM 80 130/12K Programmable Controller is to be used for this application. The input and output (I/O) has been determined as follows :-

20 Analogue inputs

69 Digital inputs
73 Digital outputs

The digital inputs and outputs are interfaced to the GEM 80 processor through 8 way digital I/O modules. The analogue inputs are multiplexed through 8 way multiplexers, thus requiring only 3 analogue input modules, instead of 20.

The operator control desk incorporates the following equipment :-

1. An AUTO/MANUAL selector switch for switching to manual control when the programmable controller fails.

2. START/STOP pushbuttons and ON/OFF switches for manual control of critical devices, to effect manual recovery to safe states.

3. A mimic panel with indicator lights for pump,valve and limit switch states, and for mode indication.

4. A 12 channel chart recorder, for hard copy of temperature, vacuum and pressure values during process.

5. Vacuum, tank level and pressure displays.

6. Four LED digit displays for display of different plant temperatures, one of which incorporates a 12 position switch for multiple temperature display on one of the LED digit displays.

7. An horn and flashing lamp for alarm annunciation, and a second flashing lamp for end of step indication for the operator.

8. A printer for logging of events, alarms and report printing, and an operator membrane keyboard for control functions.

A.2 MODES OF OPERATION

A.2.1 Automatic

The Automatic process cycle consists of a timed control sequence of programmed operations. When the cycle is completed, the system automatically returns to the Rest mode.

The sequence of operations for each of the six process cycles is identical, except for changes in process parameters such as times, temperature, vacuum and pressure setpoints.

Preheated unit/s are placed into the impregnating vessel and the temperature sensors for the unit temperatures during process are attached to the unit/s. Then, the maximum level sensor switch is set at a level sufficient to submerge the unit/s, and the lid is closed and locked with the seperate hydraulic lid control system. The manual filling valves for the impregnating vessel are then set, and the process started from the keyboard.

The automatic mode lamp is lit to indicate a process is in progress, and the process is controlled and reported as described below :

AUTO 1 - On a new page, the printer prints the headings and the table for unit/s being treated to be completed by the operator after the process.

Then the printer prints :-

(-time-) ** PREHEAT TIME (-preheat time-) MINS

The system check is then performed.

The lid limit switches must indicate that the lid is closed and locked. The lid interlock is then asserted to inhibit the hydraulic lid control from being used until completion or aborting of the process cycle.

The impregnator pressure release valve, impregnator air admittance valve and the compressed air valve must be closed. Also, the cooling water and compressed air pressures must be sufficient.

The impregnator filling valves for top or bottom filling are checked such that only one of the two should be open for the process.

All of these above conditions are checked using limit switch inputs into the GEM 80 programmable controller.

The control of the storage temperature is stopped by closing the heating and cooling water valves to the storage tank, pipeline and heat exchanger water jackets.

Preheat is then performed for the time specified on activation of the process through the membrane keyboard by the operator. This allows the units being treated to be put into the impregnator without preheating in the main oven, and as the impregnator heating will affect the heating up of the units. This allows the units to be preheated from the end of the previous day. and for the cycle to start early in the morning, such that the process ends early afternoon during normal shift time. (A typical process cycle can take 10 to 15 hours).

The impregnator vessel water jacket is heated up to process setpoint, and if it reaches this setpoint before the preheat time is finished, the temperature is controlled to this setpoint through the use of the four-stage heater.

After the preheat time, the printer prints :-

(-time-) START VACUUM

AUTO 02 - The impregnator vacuum pumps are started and 'dry' vacuum is pulled. The impregnator heating is stopped to allow for cooling down to the next setpoint.

'Dry' vacuum is controlled between two limit setpoints, by switching the pumps on above the high limit, and off at or below the lower setpoint.

The temperature of the units are monitored, and when this drops to the setpoint, the impregnator heating is restarted.

From when the vacuum reaches the lower setpoint limit, the 'dry' vacuum time is initiated, and the printer prints :-

(-time-) START DRY VACUUM

The heating of the pipelines and the heat exchanger is started for preheating before resin is transferred to the impregnating vessel. These are controlled to new setpoints, and the motorised valves are controlled using PID control special functions, while the four stage heaters are controlled to a second setpoint.

This step ends when the unit temperature has dropped down to setpoint and when the hot water circulation has been started, and the printer prints :-

(-time-) START HEATING

AUTO 03 - 'Dry' vacuum is maintained between the two limits for the set time, or until the inner temperature sensor on the units reads in the range of the setpoint, whichever is longest, and then the printer prints :-

(-time-) START TRANSFER CHECK

AUTO 04 - At this point the unit temperatures must be within a set bandwidth, and if either is too low, the cycle is aborted, and the process goes into the Rest mode. On this fault, the printer would print :-

UNIT CORE TEMPERATURE TOO LOW AT (-time-)

(-time-) PLANT IN REST MODE

If the unit temperatures are within the set bandwidth, the printer prints :-

(-time-) START RESIN TRANSFER

AUTO 05 - The transfer of resin is started.

The resin feeder pumps are to be given equal duty. This is done by switching over to the standby resin feeder pump every day.

The heat exchanger and pipeline temperatures are controlled to a setpoint through PID controlled motorised valves and the four-stage heater system.

When the impregnator full limit switch is activated, allowing 10 secs for debounce and bubbling of the hot resin, the resin transfer is stopped, and the printer prints :-

(-time-) START WET VACUUM

If the back-up impregnator full limit switch is activated, then the resin transfer is stopped, and the above message is printed, along with the following :-

(-time-) 1.3 NOT CLOSED - MALFUNCTION

where 1.3 is the item number for the primary full limit switch as shown on the mimic diagram.

AUTO 06 - The pipelines and heat exchanger are now cooled by closing the hot water inlet and outlet valves, and by opening the cold water inlet and outlet valves, while simultaneously switching on the refrigeration unit. This will cool down to the minimum value of a setpoint.

The compressed air dryer is also started.

The 'wet' vacuum is maintained for a process dependent time, after which the vacuum pumps are switched off, and the printer prints :-

(-time-) START AIR ADMITTANCE

AUTO 07 - The impregnator air admittance valve is opened to allow the impregnator vessel to return to atmospheric pressure. When this happens, the printer prints :-

```
(-time-) START PRESSURISING
```

AUTO 08 - Pressurising is started by opening the compressed air valve.

If the pressure setpoint is not reached within 45 mins, then the printer prints :-

```
(-time-) PRESSURE (-P-) KPA NOT ATTAINED, COMPRESSED AIR
         FAULT
         PROCESS CONTINUING
```

When the pressure setpoint is reached, the compressed air valve is closed and the compressor is switched off, and then the printer prints :-

```
(-time-) START PRESSURE TIME
```

The vacuum on the storage vessel is applied.

AUTO 09 - After a process set time at pressure setpoint, the impregnator pressure release valve is opened, and the impregnator heating is stopped, and then the printer prints :-

```
(-time-) START VENTING
```

When the impregnator is back at atmospheric pressure, then the pressure release valve is closed, and the impregnator air admittance valve is opened, and then the printer prints :-

```
(-time-) START RESIN RETURN
```

AUTO 10 - The return of the resin to the storage vessel is done, while cooling is applied to the heat exchanger and pipelines to cool down the resin to storage temperature. When the impregnator empty switch is activated, the resin transfer is stopped, and the printer prints :-

(-time-) START DRAIN TIME

AUTO 11 - After the drain time, the cycle ends and the plant goes into the Rest mode.

Please note that reference to process setpoints indicate process dependent parameters, which are client confidential information.

A.2.2 Semi-Automatic

The semi-automatic operations involve the Rest, Refill, Sampling and Maintenance modes. Also, a semi-automatic process can be performed.

The Rest mode is the standby mode, and is the non-operational state of the plant. The resin is kept in the storage vessel under controlled vacuum and temperature.

The Refill mode is selected when new resin is to be added to the storage vessel.

The Sampling mode is selected to sample the resin and test the resin for quality and operational characteristics to ascertain the expected life of the resin and the time before renewal. Every process slowly cures the resin, and it's impregnating properties deteriorate.

The Maintenance mode is selected when a device is to be replaced and tested. The devices can be selected and switched on and off or opened and closed from selection keys on the operator membrane keyboard.

The Semi-Automatic process is selected when a unique non-preprogrammed process cycle is to be done. All the setpoints can be set through dedicated keys on the operator keyboard. and then a semi-automatic process initiated. Each step as detailed in section A.2.1 are done with the ma[illegible] set parameters, but each end of step must be ac[illegible] and the next step started from the operator k[illegible] Each end of step is indicated with the end of [illegible]shing lamp.

A.3 FAULT ACTION AND FAULT REPORTING

A.3.1 General fault messages

The general fault messages for the digital I/O are of the following form :-

```
(-item no-) NOT RUNNING
(-item no-) NOT STOPPED
(-item no-) NOT OPEN
(-item no-) NOT CLOSED
```

For the analogue I/O, only the temperatures are deemed to be critical, ie. limits for correct readings are required. For the temperature inputs, the limits for correct operation are set at 3.0 and 95.0 degrees centigrade. If any measure outside this range, then printing of the following message form is done :-

```
TEMPERATURE (-no.-) (-temp-) DEG.C
```

A.3.2 Unplanned Shutdown

This may occur at any time when the power fails. The time of the power failure is to be reported on the printer when the power is restored by printing the power failure report, viz. :-

```
(-date-)
(-time-) POWER FAILED, FAULT ACTION TAKEN
```

If the power fails during an AUTO or SEMI-AUTO process cycle, the fault action required when the power is restored depends on the duration of the power failure and on which step the process was performing immediately prior to the power failure. The following fault action must be taken for the following steps :-

AUTO 01/02 - Print power failure report and continue as before.

AUTO 03 - Print the power failure report and restart from step 02.

AUTO 04/05 - If the vacuum level is less than 1 mbar, then print power failure and status report and continue. Otherwise, print power failure report and continue in step 10, where the resin is returned to the storage vessel before going into Rest mode.

AUTO 06-08 - If the unit temperature is within double the set bandwidth, then print power failure and status report, and continue. If not, extend the pressure time by 100 %, print power failure and status report, and

```
PRESSURE TIME DOUBLED - CONTINUING
```

AUTO 09-11 - Print power failure report and continue.

If the power fails in either of the Rest, Refill, Sampling or Maintenance modes, then print power failure report and continue.

There is no fault action required for an unplanned shutdown in the Shutdown mode or when the system is in Manual control.

A.3.3 Automatic/Semi-Automatic Mode Fault Action

It is not practical to cater for every possible failure in detail at every step, but the following fault action is programmed.

Other faults will cause the whole process to be aborted, and the plant will go into Rest mode.

AUTO 01 - Any system check fault will cause the process to be aborted, and the system will go into Rest mode. The faulty device/s will be reported using the standard fault messages as in A.3.1 .

AUTO 02-04 - If a fault occurs on the storage system, sound alarm and switch to Maintenance mode.

If the fault occurs on the impregnator jacket heating, valves, vacuum measurement, the heat exchanger or pipeline jacket hot water systems, then the cycle is aborted to Rest mode.

If the fault is in the impregnator vacuum system, then automatic switchover to the standby vacuum line is effected, and print :-

(-time-) SWITCHED TO STANDBY

The process is then resumed.

If the standby system also fails, then abort to the Sampling mode.

Also, if the vacuum system valves fail, then abort to Sampling mde.

AUTO 05 - If the vacuum plant fails, automatic switchover to the standby unit is effected, and print :-

(-time-) SWITCHED TO STANDBY

The process cycle is then resumed.

If the standby unit also fails, then continue from AUTO 10, where the resin is returned to storage vessel, and then switch to the Sampling mode. If the vacuum system valves fail, then switch to the Sampling mode directly.

If the refrigeration system fails, then abort to the Maintenance mode.

If the excessive differential pressure switch is activated, indicating a blocked filter, report alarm, but continue. An interlock is enforced to inhibit the starting of the next process cycle unless the plant is put into Maintenance mode, assuming the intention is to clear the blocked filter. If the fault is not cleared, the excessive differential pressure switch will be continuely activated during resin transfer, until the second switch is activated.

If the second excessive differential pressure switch is activated, then abort to Maintenance mode.

If a valve malfunctions, stop resin transfer and heating systems until valve corrected and print :-

(-time-) PROCESS STOPPED

If there is a heat exchanger fault, then abort to Rest mode.

If the impregnator jacket heating fails, then the pressure time is doubled, and print :-

(-time-) PRESSURE TIME DOUBLED

If there is a storage system failure other than a refrigeration fault, then report fault but continue.

AUTO 06 - If the vacuum plant fails, switch to standby as before, and print :-

(-time-) SWITCHED TO STANDBY

If the standby vacuum plant fails, then report failure but continue.

If the impregnator jacket heating system fails, double the pressure time, and print :-

(-time-) PRESSURE TIME DOUBLED

If the refrigeration plant fails, report fault but continue.

AUTO 07-08 - If a valve malfunctions, stop the process until the valve is corrected, and print :-

(-time-) PROCESS STOPPED

If the storage system including the refrigeration plant fails, report fault but continue.

If the impregnator jacket heating system fails, report fault but continue.

AUTO 09-11 - If there is a valve malfunction, stop process until corrected, and print :-

(-time-) PROCESS STOPPED

If the heat exchanger or refrigeration plant fails, report but continue.

A.3.4 Semi-Automatic Modes Fault Action

In general, all faults are reported using the standard messages.

When a fault occurs in Rest, Refill or Sampling modes switch to Maintenance mode.

In Maintenance mode, the storage vessel temperature is monitored, and if it rises above 25 degrees Centigrade, then print :-

(-date-)
(-time-) RESIN OVER-TEMPERATURE

A compressed water or air fault is a serious fault and thus all modes and process cycles abort to Shutdown mode if this occurs.