The safe design of computer controlled pipeless batch plants

This item was submitted to Loughborough University’s Institutional Repository by the/an author.

Additional Information:

- A Doctoral Thesis. Submitted in partial fulfilment of the requirements for the award of Doctor of Philosophy of Loughborough University.

Metadata Record: https://dspace.lboro.ac.uk/2134/14553

Publisher: © Fesil Mushatq

Please cite the published version.
This item was submitted to Loughborough University as a PhD thesis by the author and is made available in the Institutional Repository (https://dspace.lboro.ac.uk/) under the following Creative Commons Licence conditions.

For the full text of this licence, please go to: http://creativecommons.org/licenses/by-nc-nd/2.5/
Pilkington Library

Author/Filing Title MUSHTAQ

Vol. No. Class Mark

Please note that fines are charged on ALL overdue items.

REFERENCE ONLY

040238647X
The Safe Design of Computer Controlled Pipeless Batch Plants

By

Fesil Mushtaq

A Doctoral Thesis

Submitted in partial fulfilment of the requirements for the award of

Doctor of Philosophy of Loughborough University

© by Fesil Mushatq 2000
Abstract

High profit (low volume) products are very attractive economically, and are influencing the direction of manufacture towards product based batch processes. One new system which has a great deal of potential is a "pipeless" plant, in which the reactor moves to different areas of the plant where heating, agitation etc. takes place. There are obvious advantages in its use in providing a means of quickly responding to fast market changes while maintaining high product quality with reduced waste. The basic concept has been successfully demonstrated with several production plants already in operation, mainly in Japan. Nevertheless the safety issues associated with pipeless plants have not been dealt with.

Three main areas of further work have been identified in the safe design of computer controlled pipeless batch plants: process, computer control, and scheduling safety. In essence it is a batch process that is carried out, and therefore entails all the safety issues associated with a batch process, such as the sharing of resources. As with all new processes, it is necessary to identify and eliminate as many hazards as possible at the design stage. Computers can introduce hazards as well as benefits. There is extensive use of computer control in automated pipeless plants, and the primary manner in which problems occur is through hardware and software failures. Possible hazards need to be identified and eliminated at the design stage, without losing the benefits of plant flexibility and speed of product changeover. Scheduling is usually concerned with optimum product output, and does not consider safety. One of the biggest problems with moving reactors is collisions. To overcome, or minimise the possibility of this problem, the plant layout and schedule require careful consideration. Simulation is a very useful tool for demonstrating the interaction between the two.

The aim of this research is to develop an integrated approach to hazard identification and safety requirement specification. The results of which should be a methodology that allows the user to produce a safe design for an economically attractive pipeless plant for batch processes.
Acknowledgements

I would like to express my deep gratitude to my supervisors Professor Paul Chung and Dr. Robin Wilcockson. Paul, for his constant supervision, encouragement, and assistance towards the completion of this thesis, and Robin, for his fresh ideas and assistance part way through the project. I would also like to thank all my friends and colleagues, both in the Department and in John Phillips Court for their support during the last three and a bit years.

I would also like to thank the Engineering and Physical Sciences Research Council for funding my project.

There are not enough words to thank my family, especially my parents, for all their love and support for the long duration of my studies. They are the reason I am the person I have grown up to be.
Section 3: Computer Control Safety

5. Computer Control of Batch Processes

5.1 The Benefits of and Problems with Computer Control

5.2 Concepts of Batch Control System Design

5.2.1 Differences between Batch and Continuous Control

5.2.2 Computer Control Functions

5.2.3 Computerised Sequence Control

5.2.4 System Co-ordination Tasks

5.2.5 Operator Interface

5.2.6 Instrumentation Design

5.2.7 Distributed Systems

5.2.8 System Check-out and Commissioning

5.3 Back-up Systems

5.3.1 Requirements of a Back-up System

5.3.2 Establishing a Back-up Philosophy

5.4 Application of Batch Computer Control to Pipeless Plants

5.4.1 Software and Hardware Considerations for Pipeless Plants

5.4.2 Backup Philosophy for Pipeless Plants

5.5 Conclusions

6. Hazop of Computer Systems

6.1 Chazop

6.2 Automatic Verification of Sequential Control Systems

6.3 HAZAPS Methodology

6.4 Hazard Analysis and Support Tool

6.4.1 Stage 1. Safety Requirements Identification

6.4.2 Stage 2. Process and Control Logic Representation

6.4.3 Stage 3. Verification of Control Logic

6.4.4 Stage 4. Safety Critical Events Identification

6.4.5 Stage 5. Application of Life Cycle Question Library
Section 4: Schedule Safety

7. Discrete Event Simulation
   7.1 Techniques
   7.2 Applications
   7.3 DES Tools
      7.3.1 ARENA
      7.3.2 WITNESS
   7.4 Conclusions

8. Simulation Case Study
   8.1 Description of the Process and Plant
      8.1.1 Plant Layout
   8.2 The Schedule
   8.3 Setting up the Simulation
   8.4 Running the Simulation
   8.5 Points for Discussion
      8.5.1 Starting Points for the Vessels
      8.5.2 Intersections
      8.5.3 Vessels returning to the start position
      8.5.4 Vessel breakdowns
      8.5.5 Number of vessels
   8.6 Discussion of Simulation Results
   8.7 Simulation Conclusions

Section 5: Integrated Methodology

9. Integrated Methodology
   9.1 Process Safety
   9.2 Computer Control Safety
   9.3 Schedule Safety
   9.4 Conclusions

Section 6: Case Study

10. Case Study: Production of Cakes in a Bakery Pipeless Plant
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1</td>
<td>Introduction to Baking</td>
<td>106</td>
</tr>
<tr>
<td>10.2</td>
<td>Process Description</td>
<td>107</td>
</tr>
<tr>
<td>10.3</td>
<td>Process Operation: Charging</td>
<td>112</td>
</tr>
<tr>
<td>10.3.1</td>
<td>Automatic Batching Systems</td>
<td>113</td>
</tr>
<tr>
<td>10.4</td>
<td>Process Operation: Mixing</td>
<td>114</td>
</tr>
<tr>
<td>10.4.1</td>
<td>Mixing Station</td>
<td>114</td>
</tr>
<tr>
<td>10.4.2</td>
<td>Vertical Mixers</td>
<td>115</td>
</tr>
<tr>
<td>10.4.3</td>
<td>Power Requirements For Dough Mixing</td>
<td>116</td>
</tr>
<tr>
<td>10.4.4</td>
<td>Temperature And Mixing</td>
<td>116</td>
</tr>
<tr>
<td>10.5</td>
<td>Process Operation: Separating (dividing)</td>
<td>117</td>
</tr>
<tr>
<td>10.5.1</td>
<td>Dough Dividing Station</td>
<td>117</td>
</tr>
<tr>
<td>10.5.2</td>
<td>Precautions to be Taken with Dough Dividers</td>
<td>119</td>
</tr>
<tr>
<td>10.5.3</td>
<td>Safety Features of Dough Dividers</td>
<td>120</td>
</tr>
<tr>
<td>10.5.4</td>
<td>Maintenance and Cleaning of Dough Dividers</td>
<td>121</td>
</tr>
<tr>
<td>10.6</td>
<td>Process Operation: Heating (baking)</td>
<td>122</td>
</tr>
<tr>
<td>10.6.1</td>
<td>Heating Station (Oven)</td>
<td>122</td>
</tr>
<tr>
<td>10.6.2</td>
<td>Ovens And Associated Equipment</td>
<td>123</td>
</tr>
<tr>
<td>10.6.3</td>
<td>Tray ovens</td>
<td>124</td>
</tr>
<tr>
<td>10.6.4</td>
<td>Auxiliary Equipment</td>
<td>126</td>
</tr>
<tr>
<td>10.6.5</td>
<td>Unloaders</td>
<td>127</td>
</tr>
<tr>
<td>10.7</td>
<td>Process Operation: Packaging</td>
<td>128</td>
</tr>
<tr>
<td>10.7.1</td>
<td>Depanners</td>
<td>128</td>
</tr>
<tr>
<td>10.7.2</td>
<td>Coolers</td>
<td>128</td>
</tr>
<tr>
<td>10.8</td>
<td>Process Operation: Cleaning</td>
<td>129</td>
</tr>
<tr>
<td>10.8.1</td>
<td>Cleaning Station</td>
<td>129</td>
</tr>
<tr>
<td>10.8.2</td>
<td>Spray Cleaning of the Processing Vessel</td>
<td>129</td>
</tr>
<tr>
<td>10.8.3</td>
<td>Spray Cleaning of the Pans</td>
<td>131</td>
</tr>
<tr>
<td>10.9</td>
<td>Maintenance</td>
<td>131</td>
</tr>
<tr>
<td>10.10</td>
<td>Potential hazards and operational issues associated with baking</td>
<td>132</td>
</tr>
<tr>
<td>10.11</td>
<td>Application of the Pipeless Plant Hazop Procedure to the Bakery</td>
<td>134</td>
</tr>
<tr>
<td>10.12</td>
<td>Application of the modified HAZAPS Methodology to the Bakery</td>
<td>135</td>
</tr>
<tr>
<td>10.13</td>
<td>Key Findings from the Pipeless Plant Hazop and modified HAZAPS</td>
<td>135</td>
</tr>
<tr>
<td>10.14</td>
<td>Modifications to the Original Design</td>
<td>136</td>
</tr>
</tbody>
</table>
List of Figures

Figure 1: Simple Example PCED.................................................................35
Figure 2: Flow Diagram showing the Hazop Procedure for a Pipeless Plant......40
Figure 3: Simple Example PCED...............................................................69
Figure 4: Plant Layout..............................................................................81
Figure 5: The Schedule............................................................................83
Figure 6: Alternative Plant Layout - External Loop..................................91
Figure 7: Alternative Plant Layout - Central Loop..................................92
Figure 8: Alternative Plant Layout – Loop from Cleaning Station.............92
Figure 9: Screen grab showing the plant running with the external loop from the cleaning station.................................................................93
Figure 10: Flow Diagram Showing the Integrated Methodology..............100
Figure 11: Simple flow diagram of the baking process, illustrating the different functional stations in a pipeless plant...........................................109
Figure 12: P&ID for a combined Charging Station for the bakery.............112
Figure 13: P&ID showing the Mixing Station........................................114
Figure 14: Schematic of dough divider, Matz (1972)..............................118
Figure 15: P&ID showing the Heating Station........................................122
Figure 16: Schematic of a Travel Tray Oven, taken from Matz (1972).........124
Figure 17: Diagram showing different cleaning devices for tanks, Sieberling (1997)...130
Figure 18: Screenshot of the Hazop Table in Excel..................................134
Figure 19: P&ID showing a Dry Charging Station....................................136
Figure 20: P&ID showing a Liquid Charging Station.............................137
Figure 21: Screenshot showing Simulation of Bakery Case Study in Arena....138
List of Tables

Table 1: Summary of Hazard Identification Techniques, their Applications and Appropriateness to Pipeless Plants ................................................................. 30
Table 2: Review Team ........................................................................................................... 33
Table 3: Guide Words and their Interpretation .................................................................... 34
Table 4: Hazop Procedure for a Batch Process ................................................................. 36
Table 5: Hazop Procedure for a Pipeless Plant ................................................................... 39
Table 6: Summary of Computer Hazard Identification Techniques, their Applications and Appropriateness to Pipeless Plants ......................................................... 72
Table 7: Values of Parameters as used in the Simulation .................................................... 84
Table 8: Ingredients to produce 100kg batches of different cakes, Matz (1972) ............ 110
Section 1:
Introduction to Pipeless Plants
1. Introduction

1.1 Motivation

High profit (low volume) products are very attractive economically, and are influencing the direction of manufacture towards product based batch processes. One new system which has a great deal of potential is a "pipeless" plant, in which the reactor moves to different areas of the plant where heating, agitation etc. takes place. There are obvious advantages in its use in providing a means of quickly responding to fast market changes while maintaining high product quality with reduced waste. The basic concept has been successfully demonstrated with several production plants already in operation, mainly in Japan. Nevertheless the safety issues associated with pipeless plants have not been dealt with.

Much work has been done on developing mathematical algorithms to overcome scheduling problems. However scheduling is only one part of the safety issues associated with pipeless plants. Plant layout has a very large influence on the scheduling and therefore needs to be considered simultaneously. With every new process, the first step is to identify and remove, or minimise the risk of, process-related hazards. Existing hazard identification techniques, such as HAZOP, have been developed for continuous processes, and have required modification before being applied to batch processes. For pipeless batch plants, either new identification methods are needed or it is necessary to further manipulate existing techniques to make them more applicable. In addition the operation of automated pipeless plants relies heavily on the computer control system. The security of this system is crucial to the safety of the whole plant, and therefore requires a great deal of consideration in the design.

In conclusion, more appropriate procedures need to be defined for identifying and controlling hazards in automated pipeless batch plants.
1.2 Project Overview

Three main areas of further research have been identified in the safe design of computer controlled pipeless plants:

- Process safety: in essence the process being carried out is a batch sequence of operations and therefore entails all the safety issues associated with a batch process, such as the sharing of resources. As with all new processes, it is necessary to identify and eliminate as many hazards as possible at the design stage.

- Computer control safety: computers can introduce hazards as well as benefits. There is extensive use of computer control in automated pipeless plants, and the primary manner in which problems occur is through hardware and software failures. Possible hazards need to be identified and eliminated at the design stage, without losing the benefits of plant flexibility and speed of product changeover.

- Schedule safety: scheduling is usually concerned with optimum product output, and does not consider safety. One of the biggest problems with moving reactors is collision. To overcome, or minimise the possibility of this problem, the plant layout and schedule require careful consideration. Simulation is a very useful tool for demonstrating the interaction between the two.

The aim of this research is to bring together the knowledge of the two independent disciplines of chemical engineering and systems engineering, to develop an integrated approach to hazard identification and safety requirement specification. The results of which should be a methodology that allows the user to produce a safe design for an economically attractive pipeless plant for batch processes.
1.3 Contribution of Thesis

The areas of safety that are particularly relevant to pipeless plants are identified in Section 1, i.e. process, computer control and schedule safety. The research carried out considers each of these three areas of safety individually in Sections 2, 3 and 4. The safety problem is described for each section and a possible solution to each problem is presented in Chapters 4, 6 and 8. An integrated methodology combining all three areas of safety is proposed in Section 5 (Chapter 9), and a case study to illustrate the methodology is presented in Section 6 (Chapter 10).

1.4 Structure of the Thesis

In greater depth the report has been divided into nine sections. Section 1 contains two chapters (1 and 2). The first is the introduction describing the motivation for carrying out the work, and a project overview summarising the basis of the work that needs to be done. The second chapter describes the concept of the pipeless plant and the technology used. It includes brief descriptions of existing plants, a summary of previous research, and an outline of the safety issues associated with pipeless plants. Section 2 covers process safety and contains two chapters (3 and 4). Chapter 3 describes existing hazard identification techniques and their present applications. Chapter 4 describes a new batch Hazop procedure, and its application to pipeless plants. Section 3 covers computer control safety and contains two chapters (5 and 6). Chapter 5 describes the computer control systems required by batch processes, and their particular application to pipeless plants. Chapter 6 describes different hazard identification techniques for computer control systems, presents a developed HAZAPs methodology, and shows its usefulness to pipeless plants. Section 4 covers schedule safety and contains two chapters (7 and 8). Chapter 7 is on discrete event simulation (DES) and includes a description of two tools, one of which Arena was purchased. Chapter 8 describes a case study, taken from a published paper, that is simulated on the Arena software to observe the performance of the proposed schedule for a given plant layout. The lessons learned are described, in particular the development of rules for improving plant layouts and schedules. Section 5 describes the influence of the
different areas of research on each other, and describes how the outputs from one section can be the inputs to another. An integrated methodology is presented that should produce a safe design for a computer controlled pipeless batch plant. Section 6 presents a case study to which the integrated methodology is applied, the results of which are in the appendices. Section 7 contains the conclusions of the research, and the direction towards which further research should be carried out. Section 8 contains the references and Section 9 the appendices: the results of the case study.
2. Pipeless Plants

In technical terms a pipeless batch plant is an arrangement of many units, such as movable reactors and other functional stations, which work co-operatively by avoiding collision or conflict (Kuroda and Ishida, 1993). To understand this it can be likened to a chemical laboratory (Niwa, 1993), where a beaker or flask could be a "mobile vessel", and the laboratory equipment such as the Bunsen burners are "processing stations". Usually all the operations required to formulate a product are carried out in a single flask which is moved around. Therefore the basic idea of a pipeless plant is to move the process vessel between fixed stations for mixing, separation and other activities.

2.1 Existing Plants

The idea of using mobile robots was introduced at Shell U.K. Oil's Shell Haven automated lubricant-blending plant in 1980 (Chowdhury, 1982). The idea was to use the robots to move vessels around during the filling, mixing and decanting process (Zanetti, 1992). The main aim being to eliminate the complex piping required. Since then the idea has been intensively developed in Japan, via the pipeless plant.

Asahi, Japan, has delivered 14 plants so far (Japan Supplement to the Chemical Engineer, 1997). Five plants are being used to produce paints and inks, two are being used to make water management chemicals, and another five for lubricants, photochemicals and other specialities. Asahi plans to export the concept to the U.S. and Europe.

Toyo Engineering Co. (Tokyo) has delivered 3 Milox plants using AGV technology for vessel transport (Shimatani and Okudo, 1992). The plants are being used to manufacture paints, adhesives and other products. A key element of Milox is the control system, which conducts the entire plant operation, including the connecting to and disconnecting from stations.
At Herberts GmbH (Wuppertal, Germany), a subsidiary of Hoechst AG’s Paints and Coatings, a 15,000 m.t./yr pipeless plant making automotive coatings has been running since 1995 (Kamiya and Fouhy, 1997). This is the first application of the concept in an explosive atmosphere. The closed mixing vessels used are mounted on hovercraft vehicles to move from station to station. There are 64 mixing vessels of varying capacities, ranging from 3 to 20 m\(^3\). Components are pumped from two separate metering stations into the vessels (each of which has an integrated stirrer), dependent on the paint recipe required. The vessels are then tested for quality control before the paint is metered into cans. The entire process is automated thereby reducing staffing requirements. Capital costs are said to be similar to those of conventional plants at around $64 million, and automation accounted for about 6%, or roughly $3.6 million of that total.

ICI plc (Rouen, France) started up a pipeless plant in 1995 to mix, blend and fill solvent-borne paints (Kamiya and Fouhy, 1997). According to manager, Martin Blythe, the pipeless concept is “significantly cheaper” than conventional plants in comparable applications.

The Inoue (USA) Pipeless System is the state-of-the-art process for material mixing, milling, dispersing and packaging. The Pipeless System, with its patented Automatic Guided Vehicles (AGVs) and moving tanks, meets industry demands for diversified production with smaller batches and shorter production times. It provides higher productivity while drastically reducing the number of manpower hours and storage space required with a fixed-tank system, and it reduces the level of environmental contamination (Inoue Products USA, 2000).

A planned move for Cheesebrough-Pond USA’s dentifrice products plant enabled designers to implement a new pipeless system consisting of AGVs moving totes of raw materials and tanks of toothpaste. A computer simulation model also helped company managers to verify the cost savings associated with the new "pipeless" processing strategy (Modern Materials Handling, 1997).
Other companies also active in developing pipeless plant technology are Japan Steel Works (Tokyo), JGC Corp. (Tokyo) and Sumitomo Heavy Industries (Tokyo).

2.2 Pipeless Plant Technology

A batch operation can be divided into its various stages, such as materials being charged, reacted, separated, sampled and discharged (Zanetti, 1992). In the final stage equipment is cleaned. In a pipeless plant the reactors move from stage to stage by means of a transport system. There are two existing types of automatic vessel transport systems:
- track or on-track
- non-track or off-track

Non-track is better from the point of view of flexibility, but it poses real challenges in terms of plant management, production scheduling and process control. Hiransoog et al (1997) describe the requirements of an autonomous mobile vessel, and propose an architecture for proactive (decision making) robotic reactors. However a great deal of work is still required before a robot can think and make decisions like a human. In industrial practice the track approach is a favoured because it yields more controllability (Liu and McGreavy, 1996).

Some of the different uses of the two options are described below (Kamiya and Fouhy, 1997). With the track system vessels up to 5 m$^3$ are driven by an explosion-proof motor along a rail-guided transport system. The non-track system uses a battery-powered, automated guided vehicle (AGV) suitable for use in non-flammable environments. The vessel volume in AGV transports is limited to up to 2 m$^3$, generally AGV facilities are more expensive than Suspension-type Tank Transportation System (STTS) units, which are on a par with conventional batch plants. Another type of non-track system uses hovercraft-like vehicles. This system makes it easier to clean floors, and can easily be made explosion proof. It also reduces transportation time and investment costs (by 20-40%). The technology, however, can only be used in vessels up to 3 m$^3$. 
Kuraray Engineering Co. (Osaka, Japan) and Japan Steel Works Co. (Tokyo) have developed a Suspension-type Tank Transportation System (STTS) to move a production vessel from one process step to another. A novel feature of STTS is that it is located above the plant floor, making floor space available for other uses, says Yoshio Ishibashi, manager of Japan Steel Works’ Environmental & Engineering Business Div (Parkinson, 1996).

The main advantage of the pipeless plant concept is that the removal of complicated pipework would enable multiproduct production to be more flexible and adaptable. This is achieved by having the intelligent units, such as the movable reactors and the functional stations, co-operating with each other to avoid collision or conflict. Centralised computer systems are currently being used to manage and operate such processes, but as plants become larger this centralised control will become more difficult to maintain safely.

The following unexpected problems may often appear in the operation of a pipeless batch plant (Kuroda and Ishida, 1993):

1. Fluctuations of operating time
2. The requirement for event-driven operations
3. Unforeseen accidents, requiring fault tolerance

These issues make centralised operation more difficult.

In decentralised operation the robot reactors can move by themselves and the functional stations can be in charge of their own unit operations. The way a batch is started is by the creation of a recipe by the process managers (intelligent computer units and man). The recipe describes only information about the process sequence, and does not assign tasks or time schedules to the stations. The reactor and the stations start the production in co-operation through a communication network, but they also have their own knowledge so they can carry out their own functions independently. Scheduling software can be used to determine which mobile vessel should visit which station for the most efficient operation. In order to change the product or the reaction conditions there is the option either to change the stations to be visited, or to re-
programme each station. Cleaning is usually only required for the mobile vessels, and is handled at a cleaning station independent of the process, and therefore does not interfere with production.

Companies are continuously trying to upgrade their technology. This includes improved routing, filling and other equipment, such as coupling devices and metering devices. Leakproof pipe connections, which combine pneumatically actuated valves with a lever lock system, are necessary when the material being handled is toxic or flammable (Niwa, 1993). There are also other types of connections dependent on the type of material being used. Connections are also required for the supplying of electrical power. Due to the number of moving parts, a scheduled maintenance program is needed to keep high reliability.

Communication technologies, so prominent in our personal lives, also are changing the plant-floor landscape. The trend to use short-haul wireless communications to/from sensors and control devices will increase to meet agile, flexible manufacturing demands. One example is the use of wireless communications to continuously monitor content integrity regardless of vessel location in a food production pipeless plant-facility using AGVs (Harrold, 2000).

Other important design considerations are (Lakhapate, 1998):

Civil & Structural: Movement of vessels/equipment from one place to another on the floor surface calls for desired quality of floor involving additional expenses. Since pipelines and valves are eliminated, piperack structure and supports are not required. Since the equipment will be moving, civil/structural design will change accordingly.

Electrical: Due to movement of equipment, remote control concepts need to be used. This leads to cable-less plant.

Systems: Computerised programme control is going to be a requirement of these plants.
Utilities & Piping: Probably all the utilities and piping are still required up to the battery limit. Because of pipeless concept, costly valves, pipes and their support can be eliminated.

The plants are also being made for easier cleaning. Asahi uses solvent-spraying and brush rotation to clean its pipeless-plant vessel walls. Toyo has developed a new type of ball-valve, based on a cube with rounded edges instead of a ball. The design should simplify cleaning, as there should be fewer recesses in the valve shell.

The external dimensions of the units and stations need to be standardised so that they can be freely rearranged to form new process connections. The internal dimensions also need to be standardised so that multipurpose operations can be carried out. There is usually a common utility network, where the headers, piping and communication wiring built into each unit are connected. In addition each station has its own computer and control software which has to be modularised.

2.3 Pipeless Plants versus Conventional Batch Plants

The emergence of pipeless plants and their potential advantages over more conventional batch plants have been discussed in a number of papers (Zanetti, 1992), (Niwa, 1993), (Fruci, 1993), (IMI Project Detailed Proposal February, 1997), and (Pantelides et al 1995).

These advantages claimed by the above authors can be described in terms of:
- increased speed of product and process development
- multi-product flexibility without complicated pipework
- ease of cleaning (due to less pipework)
- usefulness in larger production runs
- reduced labour costs
- savings on time (such as product changeover) and energy
- simplifying just-in-time processing
- reduced space requirements: reduced inventories – raw materials and products
- reduced raw material handling and costs
- reduced product loss
- reduced risk of product contamination
- reduced environmental damage (less waste produced)
- reduced cost of piping and valves flowmeters etc.

The disadvantages of pipeless plants seem to be:
- the initial capital cost is potentially higher, dependent on transport system - "track" or "non-track"
- the additional safety issues that arise such as:
  - identification of safety problems due to product and process changes
  - safety requirement specification and assessment of control systems
  - the problems associated with the movement of vessels.

There are also limitations to the use of pipeless plants:
- they are not suitable for processing large quantities of products
- there is an increased risk when dealing with harmful materials (such as toxic or flammable materials) because of the possibility of leakage or spillage
- there are potential problems for processes operating at high pressure or high temperature

The last two can be overcome by specially developed technology or employing thorough operating procedures.

In summary, the flexibility of the pipeless plant allows changes to be made easily and quickly. However these changes introduce new hazards, and therefore need to be considered carefully before being implemented.

2.4 Research into Pipeless Plants

There is a small number of papers written on the subject of pipeless plants. The majority however have not considered the safety issues. Of the ones that have they consider that a correctly working schedule would overcome many of the potential safety problems. This, however, is avoiding the issue. No schedule is a hundred per
cent safe, problems can occur with sensor failures, which allow the plant to continue running even though a hazardous situation has developed.

Pantelides et al (1995) present a mathematical approach for formulating and solving the short-term scheduling problem in pipeless plants. In their work the recipe for the various products to be manufactured in the plant is represented in the form of a State-Task Network. The different types of material and transferable vessels in different conditions are represented as states. Transformations from one state into another are represented as tasks. The scheduling problem is formulated as an MILP (Mixed Integer Linear Program) format. The problem of deriving detailed short-term schedules for a variety of plants implementing complex recipes is examined. The routing of transferable vessels is not considered. The rigorous mathematical formulation not only keeps track of processing station utilisation, but also the precise location of all transferable vessels. An assumption made in the paper is that the details of the routing of transferable vessels need not be considered by the scheduling algorithm, and will be dealt with once the schedule is decided. This assumption is not valid if the movements take place on track, as restrictions on certain movements such as vessels overtaking or passing each other on the same track need to be taken into account. This means that the schedule cannot be considered independently of the plant layout.

Realff et al (1996) argue that the design, plant layout and scheduling need to be considered simultaneously. They present a mathematical formulation for their combined problems, using the short-term scheduling formulation of Pantelides et al (1995). The formulation applies the constraints governing the design, layout and operation in terms of parameters and variables describing the existence, layout and utilisation of processing stations, and the number and utilisation of the transferable vessels. A decomposition procedure for the solution of the large mixed integer optimisation problem resulting from the formulation was proposed. The procedure employs an aggregate description of the plant operation to determine appropriate equipment selections and layouts at an outer level, while the inner level determines the number of transferable vessels and a detailed operating schedule. It is interesting
to note that when the procedure was applied to their example problem, the first three
designs proposed by the outer level were suboptimal.

Kuroda and Ishida (1993) proposed a system for multiple-criteria decentralised
decision-making in pipeless plants. Local scheduling is made possible through
communication between intelligent units. By integrating multiple local schedules, co­
operative operation and management of the whole plant may be achieved. This system
has been proposed to deal with the flexibility and adaptability of pipeless plants.
However the decision-making is function-based and duty-based i.e. which available
unit is appropriate for the task at the time required. This does not take into account the
location of the units in relation to each other and other units, and therefore layout is
not considered in the decision-making process.

Liu and McGreavy (1996) and Liu (1996) have proposed a framework for operation
strategies of pipeless batch plants. A support environment has been developed to
provide operators with a tool for planning production strategy and to carry out process
analysis. This combines the scheduling algorithm with production activity simulation,
its main use being to check whether the schedule is feasible. Therefore the usefulness
of the support environment is in terms of demonstrating an achievable and safe
schedule, for which there exists manufacturing engineering simulation software, such
as Witness and Arena.

2.5 The Safety Issues

First of all there are issues concerning process safety as in all chemical processes, such
as:

- the sharing of resources
- the problems associated with certain process operations, such as thermal
  runaways
- human involvement, therefore potential for human error.
Many of the references that were found on pipeless plants covered scheduling. This on its own, however, is not adequate from a safety perspective. One of the most prominent dangers associated with moving vessels is the possibility of collision. The way to overcome this problem is to analyse the course a vessel takes together with the time it is on each leg of its journey. If possible intersecting routes should be avoided. If this is not feasible then the timing of each vessel becomes very important. In other words scheduling should be considered alongside routing. One way that collisions are avoided is by the units all communicating with each other.

In the design of a process plant a number of systems are needed for safe and reliable operation. These are control systems, which enable reliable production and maintain plant operation within presented limits, and protection systems, which guard against the loss of production or product, damage to the equipment and environment and avoid harm to people. There is extensive use of computer control in a pipeless plant, without which it could not operate. Everything from the unit operations, to the connecting and disconnecting, and to monitoring the progress of the batches is automated. However computers can introduce hazards as well as benefits. The designers of the system have to take into account the impact the computer control system has on the safe operation of the plant. Some people seem to expect computers to behave like humans and cannot understand the mistakes that no human would make (Kletz, 1997). Computers can fail in two ways: hardware and software. These possible failures need to be detected and minimised at the design stage.

There are other important considerations specific to pipeless plants to ensure smooth operation. These can be summarised as follows:

- control structure
- connecting and disconnecting of vessels
- product switchover
- problems with cleaning

These points need to be properly addressed early on in the design to avoid problems later.
2.6 Conclusions

Pipeless plants are already in use in other countries, especially Japan, thereby proving their benefits. They have a number of advantages over conventional batch plants, especially in terms of multi-product flexibility, but also significant savings in terms of cleaning time and costs due to product loss and labour. However pipeless plants also introduce additional safety issues that require careful consideration. Three main areas of concern have already been identified: process safety, schedule safety, and control safety.

To ensure the safe manufacture of a product, it should be ensured, first of all, that the batch process to be carried out is safe. This means that the hazards in the process have to be identified and minimised or controlled. There are many existing techniques for doing this which are mainly applicable to continuous plants. Some of these techniques have been modified for batch plants, but they have not been applied to pipeless plants. Secondly, the idea of moving reactors also introduces safety problems, mainly due to the possibility of collision. Past research on pipeless plants has indicated the importance of scheduling and plant layout in overcoming this problem. Finally, a pipeless plant is heavily reliant on computer control since it is fully automated. Therefore the hazards associated with hardware and software failures need to be identified and minimised. There are also existing techniques for this but not an established generally accepted method of carrying it out. The work that needs to be done would have to consider all of the above problems simultaneously. Therefore an integrated methodology is required for the safe design of computer controlled pipeless batch plants.
Section 2:

Process Safety
3. **Hazard Identification**

A hazard has the potential to cause harm, and can take the form of damage to people, property, plant, products or the environment; production losses; business harm and increased liabilities (Wells, 1996). In the process industries such hazards fall into particular categories: chemical, thermodynamic, electrical and electromagnetic, and mechanical. A pipeless plant could potentially give rise to hazards in all these categories and more due to the movement of vessels. Any change to a system could potentially lead to a hazardous situation developing. The whole point of a pipeless plant is that it can quickly respond to market changes. Therefore it needs to be initially designed in such a way that changes in production do not lead to hazards.

For a long time it has been recognised that there is a need to check designs for errors. However, this has historically been done on an individual basis. Different experts have checked particular parts of the design, according to their experience. For example, a control engineer would check the control systems. Although this technique does improve the design, it will not detect a hazard caused by the interaction between a number of different elements. There are a number of hazard identification and hazard analysis methods available, which can either be qualitative or quantitative in nature.

Qualitative methods include:
- Checklists
- What-If Reviews
- HAZOP Reviews
- Preliminary Hazard Analysis
- Failure Modes Analysis (FMA)

Quantitative methods include:
- Event Trees
- Fault Trees
- Failure Modes and Effects Analysis (FMEA)
The most beneficial method would make use of the combined skills of a group of experts to study these interactions together within meetings, such as Hazop, with the backup of other complementary methods such as Fault Tree Analysis carried out outside the meetings. Some of these methods are describe below under three categories:

- Classical Techniques
- Hazop of Computer Systems
- Hazop of Batch Systems

Safety reviews are ultimately looking for the possibilities where human error may occur. This is usually in the operational phase, but could also be the cause of defects in the design or construction of a plant. In an automated pipeless plant, there would not normally be any operators, only someone overseeing the smooth running of the plant from a control room. This greatly reduces the human operational errors that may occur, and therefore emphasises the need for a safe design.

3.1 Classical Techniques

3.1.1 Checklists

Checklists can be used to identify hazards, and help to indicate appropriate action. They take the form of a list of questions or a trigger statements. They should be prepared by an experienced engineer familiar with the plant operation and the company's standard procedures, and are a particularly useful tool for conveying information to personnel who are not skilled in this field (Battelle Columbus Division, 1985). Although a checklist is useful for identifying faults, it does have a big disadvantage in that items that are not on the list are not checked. The list therefore may be extended until it is so long, and may contain so many irrelevant items, that it is discarded. A checklist should therefore be used as a memory aid and a source of ideas, and not in a rigid manner as described above. It should help identify problems that require further attention and to ensure that standard procedures are being followed.
Many organisations use checklists for controlling the development of a project from initial design to decommissioning. The checklist is passed through various staff and management functions for approval before a project can proceed from one stage to the next. In this way, it serves as both a means of communication and a form of control.

3.1.2 HAZOP

Hazop (hazard and operability studies) is a methodology developed by ICI in the 1960s for identifying hazards in (continuous) chemical plant design (Kletz, 1983). A Hazop team consists of a leader, and members from the production, technical and engineering departments. The examination procedure is the fundamental part of a Hazard and Operability Study. A full description of the process is made available at the Hazop meetings, such as a Piping and Instrumentation Diagram (P&ID) (or an Engineering Line Diagram (ELD)). Every part of it is examined systematically (normally line by line), using guide words as prompts to determine how deviations from the design intent could occur, and whether or not these deviations could lead to hazardous situations. The guide words are used to ensure that the integrity of each part of the design is questioned, and that every conceivable way that the design could deviate from the design intent is explored. Each deviation is considered to determine the causes and consequences. In the case where the deviation indicates a cause that is conceivable and the consequence is potentially hazardous, some kind of remedial action is required, and this has to be noted in the minutes of the Hazop.

Hazop is a difficult, time-consuming and labour-intensive activity. Research into automated Hazop (Venkatasubramanian and Vaidhyananath, 1994, Leone, 1996, Wakeman et al, 1997, Larkin et al, 1997) holds promise of greatly reducing the time and effort required in a Hazop study, making the study more thorough and detailed, and minimising or eliminating human errors.

A typical operation of batch plants consists of three operating processes: charge, reaction, and discharge. The charge and discharge steps can be considered in a similar way to a Hazop on a continuous process. However, in a pipeless plant the charge and
discharge steps involve the connecting and disconnecting of pipework and therefore require special attention. Normally in the Hazop of a batch plant particular attention is paid to the reaction step, particular to the possible deviations that could occur on the reactor support systems, such as agitator, heating and cooling units etc. as well as pipelines; this would also be true for pipeless plants.

There is no published work to be found on the Hazop of pipeless plants, so initially a Hazop methodology would have to be developed (which includes an appropriate list of guide words). This should be done with reference to existing work on the safety of batch plants, and take into account the important role played by the computer in the running of the plant.

3.1.3 Operability Study

An operability study is a systematic technique for identifying hazards or operability problems throughout an entire facility. The principle for operability study is the same as for HAZOP, using guide words to identify process deviations from the design intent. It has proved useful in identifying the most critical parts of the plant (Piccinini, 1984). Its effectiveness can be substantiated by subsequent fault tree analysis. Although fault tree analysis appears to be vastly superior to operability analysis, its reliability is dependent on the availability of good data. Therefore it is not so much the final result as the methodology adopted at the design stage that makes operability analysis important.

As with a HAZOP study an Operability Study is time-consuming, Shimada et al (1995) propose an approach using knowledge engineering for automating the Operability Study.

An expert system (i.e. a computer package that can simulate or model a human expert) for carrying out an operability study, requires two types of knowledge:

1. the generic knowledge - guide words, property words, components failures etc.
2. the plant specific knowledge - information about materials, reactions, the P&ID, etc.

The plant specific knowledge has to be provided by the user.

The inference engine, using both knowledge-bases together, studies each process variable of equipment in sequence, searching for deviations using the guide words. In this method causal relations between deviations and component failures are modelled by the use of decision tables.

Advantages:
1. Much quicker than carrying out a HAZOP with a full team of experts present.
2. Possibility of identifying potential problems that could be missed in a HAZOP meeting due to the thoroughness of the search methods.

Limitations:
1. Only as good as the knowledge-bases.
2. A human can notice that the solution of one deviation might create a problem somewhere else in the plant. How would the expert system know to what extent changing one variable would affect another? Would the expert system pick up a potential problem a possible solution could create in an earlier part of the system that has already been covered?

Shimada et al (1995) have further developed the methodology for batch plants.

3.1.4 Failure Modes and Effect Analysis (FMEA)

This is based on identifying the possible failure modes of each component of a system and predicting the consequences of the failure. For example, if a control valve fails it would result in too much flow, too much pressure, or change to an undesired chemical reaction etc. This requires a knowledge of each failure mode of the plant items. In general this method only examines certain elements of the plant such as pumps,
vessels and pipes. To carry out an analysis involves following the steps below (Wells, 1996):
- describe the system;
- list all system items;
- identify all faults for each item;
- determine the effects on other items for each fault and evaluate the resulting impact on overall performance or the integrity of the system;
- estimate the probability and seriousness for each fault: a criticality index may be assigned.

This technique is particularly useful for the analysis of very critical processes but is extremely time consuming if applied on too broad a scale.

3.1.5 Fault Tree and Event Tree Analysis

Fault Trees and Event Trees are widely used as communication aids to demonstrate system failures and their development to managers, designers and operators. Their use in qualitative analysis demonstrates the effect of system failure modes and design changes.

Fault Tree Analysis (FTA)

This works by using a top event, and then considering the combination of failures and conditions that could cause this event to occur (Lowe, 1983). This technique is widely used for quantitative risk analysis particularly where extremely tight process controls are needed to attain the required standards of safety. The fault tree itself is a graphic model that displays the various combinations of equipment faults and failures that can result in the accident event. The solution of the fault tree is a list of the sets of equipment failures that are sufficient to result in the accident event of interest. FTA can include contributing human/operator error as well as equipment failures.

In addition to identifying the root causes of the top events this process will also reveal other outcomes of the root causes. In this way the method can help to identify further top events.
Both FMEA and FTA are useful aids to hazard identification as they structure and document the analysis. However, as they involve very detailed analysis of components and operations, their use in the process industry is mainly limited to the identification of special hazards where they form the basis of quantification of risks.

**Event Tree Analysis (ETA)**

This is a technique for evaluating potential accident outcomes resulting from a specific equipment system failure or human error called the initiating event, and is a systematic representation of all the possible states of the system, conditional to the given initiating event and relevant for a given type of consequence. The results of the event tree analysis are accident sequences, i.e. a chronological set of failures or errors that define an accident. Event tree analysis is well suited for systems that have safety systems or emergency procedures in place to respond to specific initiating events.

Any given event may be the initiating event in an event tree, as well as the top event in a fault tree. The main problem is at which level an event has to be regarded as top event, e.g. initiating event. Too high will lead to extensive fault trees and small event trees; too low will lead to the reverse.

### 3.2 Safety Review of Batch Systems

The Hazop of a batch process cannot be carried out in the same way as it is with a continuous process. Apart from the increased importance of operator instructions, a different method of using the P&IDs to follow the progress of a batch is required. Since it is no longer a case of following lines etc. this leads to a different way of thinking and detecting potential hazards that are specific to batch processes. Kavianian et al (1992) present two hazard evaluation techniques, namely Preliminary Hazard Analysis (PHA) and ‘What If’ Analysis, and illustrate their application to a batch process. The paper using flowsheets and operating instructions demonstrates the importance of examining the operation intent in a batch process and not just following the lines and valves.
The following sections describe different procedures for reviewing the safety of batch processes, and highlights the issues that are particularly concerned with batch processes.

3.2.1 Sneak Analysis of Batch Processes

Whetton and Armstrong (1994) have given the definition of a sneak as a hazard arising from a design error or deficiency, i.e. a latent hazard. Although the word “sneak” is not altogether suitable, it has been retained as it is commonly used as a keyword in the existing literature.

Sneak analysis (SA) may be used to identify certain classes of systematic failure. Specific aspects of the technique pay special attention to states of the plant, which is of particular importance to batch operations, where such problems tend to be common.

Originating in the aerospace industries, current research into SA centres on two areas:
1. Identification of paths down which an unintended flow of material, energy, or information might occur.
2. Use of clue lists (type of checklist) to identify other categories of sneak.

The idea of assigning categories to sneaks is very important to the use of clue lists for their identification. For process applications the most useful categories are: Flow, Indication, Energy, Label, Procedure, and Reaction. The identification of sneak flows requires a combination of path tracing and constructing a state table for the system, whereas the other sneak categories use a method based upon a checklist, known as a sneak clue list. The clue list works in the style of HAZOP guide words and deviations, and as such could quite easily be integrated with a HAZOP analysis.

Whetton and Armstrong (1994) state that historical evidence suggests that sneaks are particularly common in batch plants, and this may be due to their multi-purpose nature. Any kind of refiguring would lead to possible sneak flows and sneak
procedures. By the same token a pipeless plant, which is more flexible than a conventional batch plant would be even more susceptible to the problems associated with sneaks.

Advantages of the method:

1. Identifies a class of problems which are unlikely to be identified by HAZOP alone, thereby justifying the extra effort involved.
2. Commercial version of the program, designed to work with HAZOP, is under development.

Limitations of the method:

1. Cannot be used as a complete means of hazard identification. Should be used as a supplement to existing methods such as HAZOP.
2. No formal methods established.
3. The quality of analysis is dependent on the skill of the analyst.

Restricted by the quality of clue lists.

3.2.2 Automated Hazop of Batch Processes

There has not been a great deal of research carried out in the Hazop of batch processes, however, there have been studies carried out in automating Hazop analysis for batch processes. The issues involved are significantly different to those for continuous processes, therefore existing methods cannot be easily adapted to batch operations. Two important points have to be considered in the Hazop of batch processes:
- the role of operating procedures and operator actions in plant operations
- the discrete-event character of batch processes.

Therefore the Hazop analysis of batch plants can be split into two distinct parts: the analysis of plant maloperation, and the analysis of process variable deviation.

**Plant Maloperation**
Multi-purpose units are commonly used in batch plants. Different tasks can be performed in the same unit during different campaigns. Each task comprises of various subtasks. The operator has to initiate or terminate the subtasks which is the basis of plant maloperation (Srinivasan and Venkatasubramanian, 1996). Hazardous situations can develop if the subtasks are carried out in the wrong sequence or at the wrong time, e.g. failing to terminate a heat subtask would lead to hazards due to high temperature.

**Process Variable Deviation**
The hazards due to process variable deviations in batch plants are similar to those that occur in continuous plants. The usual set of Hazop guide words can be applied to process variables like flow rate, temperature, and level in each subtask of the product recipe, to generate meaningful process variable deviations.

Knowledge of the plant P&ID is not sufficient to represent batch plant operation. A product recipe, a detailed description of how each elementary processing step is implemented, is also required. This describes the process rather than a specific plant. If a task based language is used for representing the operation of a batch plant, each subtask is an elementary processing step. A task is a list of subtasks to be carried out in a particular equipment, and the sequence of tasks used in processing a product constitutes a task network. The difficulty in modeling batch processes comes from the multiplicity in the scales of change.

Petri nets, used for modeling discrete-event systems, cannot adequately describe the continuous changes that occur in each subtask. Digraphs, used for modeling continuous processes, cannot account for discontinuities in batch operations. Task Petri nets (TPNs) contain all information available in the product recipe about each task. The product recipe does not however contain information about the cause and effect relationships between the process variables. This knowledge is required for an expert system performing Hazop analysis, and is provided using subtask digraphs which can represent the causal relationships between variables relevant to that subtask. Srinivasan and Venkatasubramanian (1996) present this framework and implement it in a model based system called Batch HAZOPExpert, in an object-
orientated architecture using Gensym's G2 expert system shell. Tested on a pharmaceutical batch process case study Batch HAZOPExpert was found to generate all the results of a conventional hazard review. However, it was limited in its use to simple process units and subtasks for which models have already been developed. Srinivasan and Venkatasubramanian (1998) further improve this framework and successfully apply it to an industrial case study.

Viswanathan et al (1999) present an architecture for integrating Batch HAZOPExpert, as described above, with iTOPS, an Intelligent Tool for Operating Procedure Synthesis – used for generating operator instructions for batch processes. The advantage of the integrated system is that using Batch HAZOPExpert’s process hazards analysis (PHA), the operator instructions synthesised by iTOPS can be modified to include the safety critical information and appropriate recommendations into them. The two systems individually save considerable time and effort, and their integration leads to the use of consistent process and plant information. Zhao et al (2000) use the integrated system to examine a large-scale pharmaceutical industrial case study, and the results are compared with OPS and PHA carried out manually. In both cases the automated systems not only saved considerable time and effort but also influenced an operationally better and safer design, e.g. for a particular section of the case study a Hazop team identified 12 potential hazards whereas the BHE identified 68 (including all 12 from the Hazop team).

Viswanathan et al (2000) also propose an integrated framework which incorporates BatchHAZOPExpert. The framework presented deals with the three main parts of process hazards analysis (PHA): hazard identification, hazard evaluation and hazard mitigation. BatchHAZOPExpert is used for the identification, and gPROMS and gOPT are used for the hazard evaluation and mitigation. Not all hazards identified need to be evaluated further, but there are some, especially ones with potentially very serious consequences, that do. For each of these hazards a process model incorporating the parts of the process relevant to the specific hazard is developed in gPROMS. Once this has been done, the optimisation problem to analyse and evaluate the hazard is developed in gOPT. The solution should be a better operating policy that eliminates the hazard, or lessens its effect if it happens. A case study is used to
highlight the efficiency of the integrated system: BatchHAZOPExpert is fast and its results comprehensive, after manual filtering, the process modelling in gPROMS is focused and is therefore smaller and quicker to implement, which then makes the optimisation problem in gOPT computationally faster and more efficient.

3.3 Conclusions

The application and appropriateness to pipeless plants of different methods of hazard identification is summarised in Table 1.

There are many different hazard identification techniques available, but none that have been developed specifically for pipeless plants. Each technique has its advantages and disadvantages, but not all are applicable. Remember that the processes to be carried out in a pipeless plant are batch processes, whereas most techniques have been developed for continuous processes. The most thorough seem to be ones which involve a systematic examination (i.e. a modified form of Hazop), and have some kind of computer support tool to enable the analysis to be carried out quickly.
<table>
<thead>
<tr>
<th>Hazard Identification Techniques</th>
<th>Application</th>
<th>Appropriateness to Pipeless Plants</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checklists</td>
<td>Mainly to ensure company standards are followed, and for information passing.</td>
<td>Good in terms of quickly identifying hazards that need to be addressed, but not specific enough. Since hazards are picked up by trigger statements drawn up by the engineer, the right questions need to be asked or problems will be missed.</td>
</tr>
<tr>
<td>HAZOP</td>
<td>Designed for continuous processes</td>
<td>Very thorough and systematic method for identifying hazards, but very time-consuming. Modifications already introduced for batch processes. Requires further work before useful to pipeless plants. Computer-aided (automated) HAZOP would be much quicker but also requires experience (for the knowledge-base of the expert system). Thoroughness of automated HAZOP questionable (will the system pick up that a solution has created a problem somewhere else).</td>
</tr>
<tr>
<td>Operability Study (automated)</td>
<td>Designed for continuous processes, but quicker than HAZOP</td>
<td>Again a very thorough and systematic method for identifying hazards, but not as time-consuming as HAZOP especially automated. Also requires experience for knowledge-base of the expert system (again thoroughness questionable). Modifications already introduced for batch processes. Requires further work before useful to pipeless plants.</td>
</tr>
<tr>
<td>Failure Mode and Effects Analysis (FMEA)</td>
<td>Usually examines specific plant equipment, such as pumps and vessels</td>
<td>Requires knowledge of every failure mode of every item. Extremely time-consuming if applied too broadly.</td>
</tr>
<tr>
<td>Fault Tree Analysis (FTA)</td>
<td>Continuous processes, and computer control</td>
<td>Quantitative and specific. Indicates more of the risk of particular failures, rather than identifying hazards. Again, extremely time-consuming if applied too broadly. Therefore used more as a support tool.</td>
</tr>
<tr>
<td>Event Tree Analysis (ETA)</td>
<td>Continuous processes, and computer control</td>
<td>Used more to evaluate the possible outcomes of specific failures. Again, extremely time-consuming if applied too broadly. Therefore used more as a support tool.</td>
</tr>
<tr>
<td>Sneak Analysis</td>
<td>Batch processes</td>
<td>Due to the very nature of pipeless plants modifications are made to the plant layout to implement different processes. These modifications lead to possible sneak flows and sneak procedures. Therefore very applicable. However cannot be used as a complete means of hazard identification. Should be used as a supplement to existing methods such as HAZOP. Since no formal methods have been established a great deal of work needs to be done before can be used industrially.</td>
</tr>
<tr>
<td>Petri Net-Digraph Models</td>
<td>Batch processes</td>
<td>This is an expert system carrying out Hazop analysis on batch processes. It requires modification before being used for pipeless plants. It seems to be very useful, however, it is presently limited in its use to simple process units and subtasks for which models have already been developed.</td>
</tr>
</tbody>
</table>

Table 1: Summary of Hazard Identification Techniques, their Applications and Appropriateness to Pipeless Plants
4. A New Hazop Procedure For Batch Processes

Although a great deal of information is available on the Hazop of continuous processes, there has been little work published on the development of a systematic methodology of Hazop analysis for batch processes. The papers that have been produced have concentrated on automated batch Hazop studies (Shimada et al, 1995, Srinivasan and Venkatasubramanian, 1996). The issues involved with batch processes are significantly different to those for continuous processes especially in two specific areas:

- the role of operating procedures and operator actions
- the discrete-event character of batch processes.

Houton et al (1996) have suggested a special approach to the analysis of the design of batch processes using hierarchical methods. This particular methodology was developed to address the problem of waste in batch processes, and therefore concentrates on waste minimisation. The design of a batch process can be very complex. Hierarchical methods can be used to break the design down into smaller sections (levels) for ease of analysis, from an overview of the whole process to the analysis of individual operations. Questions are used at each stage to determine if there is a problem. The approach of breaking the analysis down in smaller sections is sound, however, the success of the analysis is determined by whether the right questions are asked. The hierarchical design method will give an indication of the issues involved but will not identify problems as thoroughly as other studies such as Hazop.

The batch Hazop procedure can be further developed to apply to pipeless plants. The main areas that require modification are the charge and discharge steps. These require special attention as they involve the connecting and disconnecting of pipework.

Safety reviews are ultimately looking for the possibilities where human error may occur. This is usually in the operational phase, but could also be the cause of defects in the design or construction of a plant. In an automated pipeless plant, there would not normally be any operators, only someone overseeing the smooth running of the
plant from a control room. This greatly reduces the human operational errors that may occur, and therefore emphasises the need for a safe design.

4.1 Batch Hazop Procedure

The concept of having a review team using a systematic method for examining a system has been very successful. The method of using guide words as prompts has been advantageous in finding potential problems. However, for a batch process the guide words and deviations/parameters that would need to be applied is different from a continuous plant and the general method for applying them is also different. Instead of reviewing a plant line by line, a typical batch plant can be examined by dividing it into three operational phases: charge, reaction (or "process"), and discharge. The charge and discharge steps can be analysed in a similar way to a Hazop on a continuous process. The reaction step can be reviewed by separating it into its different operations such as mixing, heating etc. Each step changes the contents and conditions in the reactor. The reactor itself should also be examined, especially the possible deviations that could occur in its support systems, such as agitator, heating and cooling units etc. as well as pipelines.

4.1.1 Review team

The review team would be selected from the people who have carried out the design, people who have knowledge and experience of the process, plant operation and maintenance, and people who are independent of the design but have knowledge and experience of the hazard review procedure. This is similar to continuous processes. Table 2 shows a typical team and describes the contribution of each team member.
Design Engineer  Usually a mechanical engineer (wants to minimise costs and keep changes to a minimum, while at the same time finding out any potential problems at a relatively early stage).

Process Engineer  Usually a chemical engineer (draws up the flow sheet)

Commissioning Manager  Usually a chemical engineer (will have to start up and operate the plant, therefore will press for changes that will make his/her life easier).

Instrument Design Engineer  A knowledge of the control strategy and instrumentation is very useful in the reviews (in additional more instrumentation may be required, therefore it is useful to have the engineer in the meeting)

Research Chemist  Specialist in the chemistry of the process to be carried out (may also be required to carry out further research)

Team Leader  Expert in Hazard Review technique (independent of the design, he needs to ensure that the correct procedure is followed).

Secretary  To record the minutes of the meeting (could be done by Team Leader as well), using a computerised recording system

Table 2: Review Team

4.1.2 Information Requirements

The information requirements of a batch Hazop would be different from those of a continuous Hazop. Knowledge of the plant P&ID is not sufficient to represent batch plant operation. A product recipe, a detailed description of how each elementary processing step is implemented, is also required. This describes the process rather than a specific plant. Additional requirements include information on the process chemistry, process materials safety data sheets, and information on the plant control.

4.1.3 Guide Words

This section describes guide words for use in the hazard review of batch processes. There is a basic set of guide words which is applicable to most continuous systems, and includes words such as no, more and less (Wells, 1996, Kletz, 1999). The Ministry of Defence (1996) has produced a Defence Standard for carrying out a Hazop on systems containing programmable electronics. The guide words used and their interpretations are different from the basic set used in continuous processes. Timing is essential in the safety of these systems, as it is with batch processes due to their discrete event nature. Therefore the words 'early' and 'late' are used for actions or events relative to time, and the words 'before' and 'after' are used for considering the
order of actions or events (Kletz et al, 1995, Little, 1995). Shimada, et al (1995) gives an example of how to consider the charging of a catalyst in a batch process, and also places emphasis on the words 'early' and 'late'. Knowlton (1976) explains how the applicability of guide words is dependent on the aspects to which they are applied, and states that they can be applied to activities such as 'react' to generate intelligible deviations. In addition Knowlton introduces extra guide words, 'sooner' and 'later' to be used when dealing with sequence or absolute time. Table 3 gives a list of guide words and their interpretation. Some of the words are similar to those used for continuous processes, although their interpretation may not be the same.

<table>
<thead>
<tr>
<th>Word</th>
<th>Interpretation</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>This is the complete negation of the design intent. No part of the intention is achieved and nothing else happens.</td>
</tr>
<tr>
<td>More</td>
<td>This is a quantitative increase.</td>
</tr>
<tr>
<td>Less</td>
<td>This is a quantitative decrease.</td>
</tr>
<tr>
<td>As well as</td>
<td>All the design intent is achieved together with additions.</td>
</tr>
<tr>
<td>Part of</td>
<td>Only some of the design intent is achieved.</td>
</tr>
<tr>
<td>Reverse</td>
<td>The logical opposite of the design intent is achieved.</td>
</tr>
<tr>
<td>Other than</td>
<td>Complete substitution, where no part of the design intent is achieved but something different happens.</td>
</tr>
<tr>
<td>Early</td>
<td>Something happens earlier than expected relative to clock time.</td>
</tr>
<tr>
<td>Late</td>
<td>Something happens later than expected relative to clock time.</td>
</tr>
<tr>
<td>Before</td>
<td>Something happens before it is expected, relating to order or sequence.</td>
</tr>
<tr>
<td>After</td>
<td>Something happens after it is expected, relating to order or sequence.</td>
</tr>
<tr>
<td>Quickly</td>
<td>Something happens quicker than expected.</td>
</tr>
<tr>
<td>Slowly</td>
<td>Something happens slower than expected.</td>
</tr>
</tbody>
</table>

Table 3: Guide Words and their Interpretation

4.1.4. Deviations/Parameters

The set of deviation words to be used should be generated by the Chairperson and Secretary before the Hazop, with the option to add further relevant words to the list. An example of a standard set of deviation words is given below:

Standard Set: Flow, Temperature, Pressure, Level, Inspect, Maintenance, and Services
In addition, for a Hazop study on a batch process it is necessary to apply the guide words to the instructions (process operations). An example of an instruction set of deviation words is given below:

Instruction Set: Mix, React, Separate, Heat, and Clean
4.1.5 Review Procedure for Batch Processes

When the preparation for the study has been completed, and the relevant information is available the Hazop team must meet and go through the procedure shown in Table 4 in order to ensure the success of the study.

<table>
<thead>
<tr>
<th>STAGE</th>
<th>PROCEDURE</th>
</tr>
</thead>
</table>
| 1. Select Vessel and Discuss Product Changeover | 1.1 Select a vessel/reactor to use. Determine whether or not the vessel has been in use previously to make a different product. If it has, knowledge of the previous product is required in terms of its process chemistry (raw materials used etc.) to ascertain whether there are any compatibility problems.  
1.2 If there is a compatibility problem, its causes and consequences should be recorded in the minutes under the parameter of cleaning (from the Instruction Set), since cleaning is the last operation (instruction) of the previous batch. If an action is required it should be recorded and assigned to one of the review team. |
| 2. Select Process Recipe | 2.1 Select a process recipe for review (should include flow sheet, operating instructions and other relevant information) – must be an operation at a time going through the new process in order, starting from charging, then mixing, then heating etc. |
| 3. Charging | 3.1 This should be dealt with in the same way as in a continuous process. Problems should be picked up by selecting a line or node and applying the guide words to the Standard Set, e.g. no flow. Causes and consequences should be identified and recorded.  
3.2 Decide if there is a problem that requires action. If yes, take action to consider changes to reduce the risk of the hazard (or problem), and assign the action to one of the Hazop team. |
| 4. Review Operations | 4.1 Apply the guide words to the operations from the Instruction Set, e.g. no mixing. Identify the causes of the deviation, and the consequences and safeguards.  
4.2 Decide if there is a problem that requires action. If yes, take action to consider changes to reduce the risk of the hazard (or problem), and assign the action to one of the Hazop team.  
4.3 Once action has been taken (or no action is required), continue with the Hazop by returning to Step 4.1. Do this until all the guide words have been applied to all the relevant operations from the Instruction Set.  
4.4 Guide words should then be applied to parameters from the Standard Set such as temperature, pressure and level. Again, causes, consequences and actions should be recorded. |
| 5. Discharging | 5.1 The next step is to consider the discharge step in the same way as in a continuous process. Problems should be picked up by selecting a line or node and applying the guide words to the Standard Set, e.g. no flow. Causes and consequences should be identified and recorded.  
5.2 Decide if there is a problem that requires action. If yes, take action to consider changes to reduce the risk of the hazard (or problem), and assign the action to one of the Hazop team. |
| 6. Select Next Vessel/Reactor | 6.1 This section of the review on the particular vessel/reactor is now complete. Return to Stage 1 and select the next vessel in the process sequence. |
| 7. Follow-up Work | 7.1 Once the Hazop is complete, there must be a follow-up meeting to ensure that the actions have been carried out. |

Table 4: Hazop Procedure for a Batch Process
The procedure can be followed more effectively using a flow diagram (see Figure 1):

1. Select Vessel
   
   Discuss Product Changeover by applying guide words to the parameter "cleaning". Causes, consequences and any action required should be recorded.

2. Select Process Flowsheet for Review

3. Review the Charging Procedure
   
   Apply Guide Words to parameters from the Standard Set
   
   Record Causes, Consequences and Any Action Required.
   
   Have all the Guide Words been applied?

4. Review the Operations
   
   Apply Guide Words to parameters from the Instruction Set and the Standard Set
   
   Record Causes, Consequences and Any Action Required.
   
   Have all the Guide Words been applied?

5. Review the Discharging Procedure
   
   Apply Guide Words to parameters from the Standard Set
   
   Record Causes, Consequences and Any Action Required.
   
   Have all the Guide Words been applied?

Figure 1: Hazop Procedure for a Batch Process
4.2 Application of Batch Hazop Procedure to Pipeless Plants

A pipeless plant could potentially give rise to hazards in all the categories described for batch plants and more due to the movement of vessels. Any change to a system could potentially lead to a hazardous situation developing, and the whole point of a pipeless plant is that it can quickly respond to market changes (Zanetti, 1992). Therefore it needs to be initially designed in such a way that changes in production do not lead to hazards.

The review procedure for a pipeless plant is very similar to the procedure above. A batch process commences with the charging of a reactor with raw materials and concludes with the discharging of the product (before cleaning). The intermediary steps to produce the final product occur in the reactor, and can be reviewed simultaneously from a safety perspective.

With a pipeless plant, however, the charging process is an operation, as is the discharging process. Each operation, from charging, mixing and heating, to discharging occurs at a distinct station. Every operation commences with the reactor connecting up to a station, and concludes with the reactor disconnecting. Therefore, the way to review this is to analyse each station in three steps:
- Connect: apply guide words ...
- The Operation: review as for a batch Hazop
- Disconnect: apply guide words ...

The modified procedure for pipeless plants is shown in Table 5, and the corresponding flow diagram is shown in Figure 2.
4.2.1 Batch Hazop Procedure for Pipeless Plants

<table>
<thead>
<tr>
<th>STAGE</th>
<th>PROCEDURE</th>
</tr>
</thead>
</table>
| **1. Select Vessel and Discuss Product Changeover** | 1. Select a vessel/reactor to use. Determine whether or not the vessel has been in use previously to make a different product. If it has, knowledge of the previous product is required in terms of its process chemistry (raw materials used etc.) to ascertain whether there are any compatibility problems.  
1.2 If there is a compatibility problem, its causes and consequences should be recorded in the minutes under the parameter of cleaning (from the Instruction Set), since cleaning is the last operation (instruction) of the previous batch. If an action is required it should be recorded and assigned to one of the review team. |
| **2. Select Process Recipe** | 2.1 Select a process recipe for review (should include flow sheet, operating instructions and other relevant information) – must be an operation at a time going through the new process in order, starting from charging, then mixing, then heating etc. |
| **3. Connecting** | 3.1 The connecting operation should be considered by applying the guide words to the Connect parameter, e.g. no connect. Causes and consequences should be identified and recorded.  
3.2 Decide if there is a problem that requires action. If yes, this should be recorded and assigned to one of the Hazop team. |
| **4. Review Operation** | 4.1 Now apply the guide words (e.g. no) to an operation (e.g. mixing) from the Instruction Set to be carried out at the station under review, (e.g. no mixing). Identify the causes of the deviation, and the consequences and safeguards.  
4.2 Decide if there is a problem that requires action. If yes, take action to consider changes to reduce the risk of the hazard (or problem), and assign the action to one of the Hazop team.  
4.3 Once action has been taken (or no action is required), continue with the Hazop until all the guide words have been applied to the relevant operation from the Instruction Set.  
4.4 Guide words should then be applied to parameters from the Standard Set such as temperature, pressure and level. Again, causes, consequences and actions should be recorded. |
| **5. Disconnecting** | 5.1 Once all the lines have been reviewed the next step is to apply the guide words to the Disconnect parameter. Any potential problems associated with the vessel disconnecting from the station should be picked up here. Causes and consequences should be identified and recorded.  
5.2 Decide if there is a problem that requires action. If yes, take action to consider changes in terms of the disconnection between the vessel and the station. This should be recorded and assigned to one of the Hazop team. |
| **6. Select Next Vessel/Reactor** | 6.1 This section of the review on the particular station is now complete. Return to Stage 2 and select the next station in the process sequence. Repeat Stages 2-5 until all the process steps for the vessel have been examined. The Hazop is then complete for this process and vessel. |
| **7. Follow-up Work** | 7.1 There must be a follow-up meeting to ensure that the actions have been carried out to the satisfaction of the Hazop team. |

**Table 5:** Hazop Procedure for a Pipeless Plant
1. Select Vessel

Discuss Product Changeover by applying guide words to the parameter “cleaning”. Causes, consequences and any action required should be recorded.

2. Select Process Flowsheet for Review

3. Review the Connect Procedure
   - Apply Guide Words to parameters from the Standard Set
   - Record Causes, Consequences and Any Action Required.
   - Have all the Guide Words been applied?
     - No
     - Yes

4. Review the Operation
   - Apply Guide Words to parameters from the Instruction Set and the Standard Set
   - Record Causes, Consequences and Any Action Required.
   - Have all the Guide Words been applied?
     - No
     - Yes

5. Review the Disconnect Procedure
   - Apply Guide Words to parameters from the Standard Set
   - Record Causes, Consequences and Any Action Required.
   - Have all the Guide Words been applied?
     - No
     - Yes

Figure 2: Flow Diagram showing the Hazop Procedure for a Pipeless Plant
4.3 Conclusions

There is a lack of a formalised procedure for the Hazop of batch processes. Some case studies have been published which suggest how the procedure for continuous processes can be modified, or emphasise other approaches for reviewing the safety of batch processes. The issues concerned with batch process safety have been described, and a methodology developed which breaks a complex design down into smaller sections for analysis in a strict sequential manner. An extension of this methodology has also been developed for use in the safe design of processes in pipeless plants.

As would be expected in any systematic safety study, the methodology is time-consuming. A computer-support tool to guide and document the study would prove useful and is being considered.
Section 3:

Computer Control Safety
5. Computer Control of Batch Processes

5.1 The Benefits of and Problems with Computer Control

Manual control involves adjustment of valves, starting of pumps, checking the level in tanks etc. by operators moving around a plant. All important controls and signals can be brought to the computer in a control room, and the operator can work from there, leaving him/her to monitor the operation and solve problems pointed out by the computer. Spellman and Quinn (1997), Frade (1976), Gray (1976) and Steel (1980) point out a number of advantages afforded by computer control:

1. Flexibility: a computer can automatically adjust flowrates, react to changes in temperature, pressure etc., and change the process recipe.
2. Safety: enables continuous monitoring of all important controls, such as tank levels, temperatures, and valve positions, ensuring the integrity of the procedure.
3. Logging: a computer can prepare final logs for all batches leaving a clear written record of what happened.
4. Expandability: additional equipment/operations can be added to the computer algorithm.
5. More complex control strategies, e.g. checking desired versus actual.
6. More sophisticated alarm and interlock systems.
7. Increased efficiency: easier, faster startup and shutdown.
8. Decrease in personnel.

There is also the capability of the user to write and later modify his/her own control program. This allows greater flexibility than would the use of hard-wired relays, or electronic control logic, while at the same time the plant would run in a consistent and predictable manner until the program is altered.
However there is still apprehension in using computer control due to stories of long start-ups, computer problems, hardware and software failures, expensive training, operation interface nightmares, etc. All of these can result in the loss of production and money.

A wide range of electronic devices which may be used are available, and computer control is not always required. Computers are used for processes that are more complex or require some special flexibility, e.g. a multi-product plant needing a large number of process recipes to be stored and accessed automatically. Manufacturing flexibility is the aim of many industries aiming at high profitability, high productivity and competitiveness in world markets. Some situations in which computer control would be considered useful are:

- Multi-purpose plants: where plants have to produce a wide range of products in the same equipment, computer control can be very useful.
- Scarcity of personnel: larger and more complex plants, with fewer operators, e.g. offshore rigs.

Whitman (1976) states the following characteristics of batch processes are important from a control point of view:

1. Frequent reactor start-up.
2. A variety of similar processes run in different vessels at the same time or in the same vessels at different times.
3. A reactor operation may have different stages requiring different control strategies during an individual cycle.
4. Measurements may be difficult to obtain and accuracy may be a key consideration.

Frade (1976) states that special consideration should be given to the following when using computer control:

- backup: what must be done when the computer fails and/or sequence calls for manual intervention;
- remote transmission: an integral concept involved with computer installation and requiring cable runs, transducers, power supplies, etc.;
- explosion-proofing versus intrinsically safe devices;
Reduced manpower: Centralisation carries personnel reduction with it because the computer control concept means modern instrumentation, remote transmission and, hence, pulling away production personnel heretofore at the equipment and into a central control area.

According to a survey carried out by Drakulich (1998), the greatest challenges faced by control engineers working in batch control, are:

1. The need for consistency
2. Flexibility in product changeover
3. Budgets
4. Safety
5. Training

Due to the need to maintain product and operational consistency it is reported that a significant amount of operator intervention is still required. However, computer control is popular as it enables flexibility in changing products. The preferred practice of the majority of companies is to use a combination of system integrators and in-house engineers for system development. The system integrators are usually experienced in similar-sized projects, skilled at developing detailed specifications, provide implementation and testing, and are staffed to provide training, installation, and on-site post-project support.

Usability has become a keyword for the control engineer or system integrator faced with configuring a system using batch software (Johnson, 1997). By keeping batch system operation straightforward, batch control software has been made more user-friendly. This is especially clear at the start of the process where the computer asks the operator questions about the product to be made and the process conditions. The computer then takes over the production, keeping the operator up to date on the progress of the manufacture. Operator assistance may be requested at certain intervals, the control system holds the process until the operator makes a response. Therefore computer control removes the operator's routine work, allowing him/her to spend more time and effort in planning, maintenance, and overseeing the production.
5.2 Concepts of Batch Control System Design

5.2.1 Differences between Batch and Continuous Control

In terms of control the most visible way that a batch plant is different from a continuous one is by the many discrete state inputs and outputs compared to relatively few control loops. Discrete outputs allow the system to start and stop motors, open and close valves etc., which is very important to batch processes that rely on the timed sequences of such actions. Many batch processes require operator intervention, however even if there are no planned interventions the control system must allow manual access to the discrete control elements. Problems arise from multiple access to the control elements making it necessary to define different operating modes, such as manual or automatic.

A batch plant may consist of only one reactor with associated auxiliary equipment. However, it is more difficult to control than the corresponding continuous plant, and therefore needs a complex control system to operate efficiently. Batch process control systems have two different performance functions:

1. Those that require high level software language, complete with advanced mathematical capability for such operations as process scheduling, direct digital and supervisory control, operator interface formatting, etc.

2. Those that require simple logic typical of what has been performed by relay logic and step sequencers, except that this logic may easily be changed on-line to adhere to individual batch processing requirements. Typical functions would include liquid charging system valve line-up and verification, pump and agitator motor start/stops, reactor cleaning or sterilisation cycles.

The digital process computer is the only logical choice to handle 1 (specifically developed for this reason). To handle 2 either a digital computer designed for process control or programmable controllers with read/write memory can be used.

The multi-product (multi-purpose) batch plant is very popular in pharmaceuticals and similar industries producing a variety of products in relatively small quantities. It consists of multiple reactors with associated equipment such as metering devices,
heating/cooling systems etc. Equipment can be shared by several reactors simultaneously or used by one reactor at a time. However available reactors and equipment are signed to a particular product dynamically, i.e. at the time when the product will be made. The problem is further complicated by different products requiring different configurations. The control system for a multi-product plant will have to cope with the following:

1. Sequence control logic for the product has to be executed in parallel lines.
2. Within each lines, there are activities which must be carried out in parallel (e.g. metering and dissolving feed material, and reacting)
3. Shared equipment that may be used simultaneously by several lines must be protected from being turned off by any individual line while other lines are still running.
4. The sequence control system must provide a formal way to describe and reference plant equipment configuration needed to make a particular product.
5. The sequence control logic for making a product must be assignable to specific plant equipment at execution time.
6. Equipment assigned to produce one product should be protected from being allocated to another product.

In case of failure of the computer system of a batch plant, the backups developed for continuous processes are not directly applicable. An analogue back-up system capable of sustaining full plant operation would be very expensive. In a multi-product plant falling back to manual operation would be virtually impossible. Therefore the strategy often adopted is to halt the process in a safe state. This usually means interrupting all material flows, and positioning heating and cooling valves to predetermined safe levels. For the process to be continued, either manually or automatically, all information on the current status of the process has to be stored in an external device and constantly updated by the computer.

5.2.2 Computer Control Functions
The procedure for initiating a batch is quite simple. The particular reactor that is to be used is called up on the display screen, of which CRT (cathode ray tube) is one type, and the desired formula or recipe identification and procedure number for the batch is entered. The outside operator performs a manual check to ensure that there are no leaks, and returns a positive instruction for the computer to proceed. The computer then continues the batch cycle to the point of discharge, without the operators taking any action unless an alarm condition occurs. Should equipment failure occur, the computer places the reactor in "hold" status and issues an alarm. The operator is to decide which of the several pre-programmed alternate actions to request and inputs his selection via the display (CRT) keyboard.

Once a reactor has been assigned the computer control mode, operators cannot manually operate any device for that reactor or in the charge area. Conversely, if a batch is initiated in the manual mode there can be no computer intervention, nor can control be returned to the computer. One very important safety feature is that the computer monitors all of the critical reactor header valves, as long as one of the reactors is under computer control. The computer prevents any charging to the reactor under computer control if any of the reactor header valves has been opened manually.

This design philosophy essentially achieves the goal of maintaining desired separation between manual control and computer automatic control while maximising safety considerations.

5.2.3 Computerised Sequence Control

Sequence control is used to ensure orderly and efficient progression of a process operation. This is done by executing procedures whereby a series of events are correctly initiated, controlled and completed. Sequence control has been implemented effectively using industrial process computers. Before computer control, sequenced operations were initiated manually or through timers. However timers ignore any changing process condition, and are therefore set conservatively to allow time for the cycle to be completed. Therefore cycle times are prolonged, and productivity is
decreased. With computer control, sequenced operations can be event-initiated, and the overall efficiency of a plant is increased. Automatic sequence control has not responded well to analytical approaches and has resulted in one-of-a-kind systems. Therefore, only a small fraction of possible sequences have been automated. This, however, is changing since: in the future many more sequences will be automated (Kennedy, 1976):

- Payouts can be significantly higher than other advanced control algorithms;
- Automation of these sequences is easier with modern process computers;
- Payouts are easily obtainable and readily demonstrable;
- Safety, health, energy, manpower and capital costs, process changes and a fast-changing economy can all dictate automated sequences.

Sequencing control logic flow is generally expressed as a ladder diagram, a fixed pattern of steps keyed by time or external events. To accomplish many of the desirable features of automated sequence control, we must go beyond this fixed pattern of steps. Techniques described are (Kennedy, 1976):

1. Automatic sequence/recipe loading,
2. Communications with continuous control,
3. Backchecking/pattern checking,
4. Communication with the operator,
5. Parallel asynchronous procedures,
6. Relative unit addressing.

1. **Automatic sequence/recipe loading**

Automatic sequence or recipe loading is a key concept for automating manual procedures. In cases where the sequence is different (depending on the state of the unit or product type,) automation has been difficult with normal logic hardware. Examples of this are:

- Plants that can make several different products
- Emergency hold or shut-down procedures which depend on the state of the unit or other measured data
- Different control systems at different times for any reason
2. Communications with continuous control

Communication between the batch control or sequence control system and the continuous control system has always been a primary problem in automatic sequence operations. It is undesirable to have one console or panel for continuous control, a different one for sequence control and possibly a third for computer control. The computer can handle all three. When sequencing and continuous control are done in the same computer, one system must direct the operation of the other. If we have the sequencing control directing the continuous control then the sequencer can be continuously making changes in the control system. Examples are:

- Altering of setpoints by recipe optimisation
- Changing of control structure (as defined earlier)
- Altering of any number of parameters in the control system, i.e., alarm suppression, scan and control mode
- Structured design of units

3. Backchecking/pattern checking

It is often heard that we have progressed as far as possible without improved sensors. Although there will be better sensors available, there are other ways around this problem. It can be broken down into two areas - accuracy and reliability. Accuracy can be improved by on-line recalibration, a standard technique for paper machine control and instrumentation in the nuclear industry. The problem of reliability is not actually in the sensor itself, as it is the effect of a failed sensor. The backchecking ability of a computerised system - where one measurement is checked against another - improves not only reliability but also confidence in the measurement. Often a second measurement is available at no additional cost. For example, a flowmeter can be checked against a level change in the tank.

Pattern check is another method of improving confidence of the control system. The devices around a unit have an established pattern and any change should create an emergency procedure. These patterns can differ as the unit operations progress. For example, a dump valve and a charge valve should not be open simultaneously. By doing a pattern check every few seconds, the computer can detect that something is wrong - independent of production procedures.
4. Communication with the operator

In order to effectively run a plant, an operator needs information from the continuous control system, the sequence control system, and the process computer. Communication via three different channels or three different operator consoles is a situation to avoid. This is eliminated by generating console displays that give an operator all pertinent information about a plant, regardless of its origin (i.e. the operator interface). This requires a considerable amount of application software, such as:

- status displays of digital devices around a unit
- recipe displays
- displays of grouping of continuous control loops around a unit
- trend displays of process variables
- status displays of all plant units
- status displays of a particular unit
- displays of system timers and other recipe data
- control loop data displays
- measurements data displays.

The ability of the process computer to interface with an operator via CRT displays has helped the control system run a plant. By giving an operator complete access to the control system, he is used where he is most valuable, i.e. in response to abnormal conditions, and in work that cannot be handled economically by the computer.

5. Parallel asynchronous procedures

Nearly everything that can be automated by computer can be automated by relay logic, but generally it isn’t. One of the main stumbling blocks is the need for different time bases within the plant. These are needed to run units independently, to effectively time-share common equipment, to use different system timers in varying procedures for diverse devices, etc. In a plant with several units there can be as many as 100 to 200 separate procedures running simultaneously, each with their own time base. The ability to run parallel procedures allows for simpler control system designs. Each unit acts independently unless information about other units or shared equipment is needed. In these cases data is obtained from a common database. Shared use of
common equipment is handled by parameters such as “busy” flags.

6. Relative unit addressing
A common situation is to have similar units in a single plant producing multiple products. A technique used to greatly simplify the automatic sequencing is called relative unit addressing. A single procedure or process such as FILL can be generated and brought in for any unit without process recoding. All devices must be identified in a relative manner. In other words, the filling procedure must be programmed so that the fill valve operates, but the address and type of valve is determined when executed for a specific unit. This is done by assigning each device its own table and driver so that a single high level command such as CLOSE, can close any valve regardless of type. There is a different type for each device with varied characteristics such as the number of contacts it takes to operate the valve, the number of contacts available from the valve as feedback, the type of contact such as momentary or latching, the time-out for the individual valve, and anything else necessary to drive the device.

Relative unit addressing is particularly advantageous in modern philosophy of plants where the number of grades is intentionally limited to lower production cost. In these cases a series of large similar units are designed to only make a few specific products. Computerised plants make it possible to manufacture products considerably lower in cost than flexible manually controlled multi-product plants.

5.2.4 System Co-ordination Tasks
Good software should allow engineers to concentrate on process strategies rather than on programming techniques. The system not only has to support process-orientated functions, but also all communication and system co-ordination tasks. An important task in batch control is initialising a batch. Before a batch is started it is important to have all the valves in the plant in the correct position. This can be achieved by having an initial portion of the sequence program output desired states, such as valve positions, to the plant, thereby checking actual states with the required states. This approach works when a batch starts from the beginning, but not when a sequence was
interrupted and must be continued. It is an unsafe assumption that the computer outputs remain in the correct position, and therefore must be initialised before continuing a suspended batch. There are several ways to do this:

1. Insert initialisation segments at various points in the programme - not attractive as it is troublesome to the programmer, uses up memory space and/or limits plant operations.

2. Provide computer commands allowing operators to position individual outputs before switching back to computer mode - excessive time required initialising the many outputs of a large plant.

3. Provide a system program that automatically adjusts computer output to actual position of the field elements when the plant is on backup - therefore the operator would have to initialise only those outputs which need to change position before the sequence program is continued.

Other system co-ordination tasks include:

1. Keeping track of the operating mode of different plant groups or individual elements.

2. Keeping track of the assignment of equipment to programs.

3. Keeping track of the status of sequence programs.

In conclusion, computerised sequence control makes a significant impact; by taking routine work from an operator, we have not only increased the reliability of an operation, but have control of the most important parameter in a plant - the time base. Doing the same each time will often greatly reduce major product variations. A disturbance is not restricted to a setpoint deviation - it can be a pump failure or heat exchange leak. Response is not restricted to modulation of a valve - it can be initiating a shutdown sequence, suspension of a supervisory control system, or notification to an operator. Between these definitions is the control system action that devises an intelligent response to a detected disturbance. Clearly, the control system can no longer be considered a separate entity - it is as an integral part of the process as the operator.
5.2.5 Operator Interface

The success of a computer control system is partly due to the success with which it is able to provide an effective communication link between operator, process, and computer (Gray, 1976). In multi-product plants different product are produced in the same equipment by changing certain process variables, known as the batch recipe. Therefore at the start of each batch the operator needs to review the recipe, and make any necessary changes for the start of the next batch. Almost all the decisions could be made by the computer but this makes the program more complex and establishes certain barriers between operator and computer. This gives the operator a sense of involvement, a need for process knowledge, and the ability to think and control are combined to form an effective “interface” between operator, process, and computer. A combination of hardware and software are required for the operator interface. The hardware includes display screens, such as CRTs (cathode ray tubes), equipped with standard typewriter keyboards used by the operator to input information to the process via the computer. The display screens also output information to the operator, along with alarms and flashing lights (indicating problems). Printers document the alarm messages and generate reports. In addition the operator’s console provides for other functions, such as an alarm acknowledge button, or an emergency button. The main use for the operator interface software is to take information from around the plant such as the status of units, the status of the recipe, measurements etc., and display them to the operator. The operator uses this information to monitor the plant and make decisions about any changes that need to be made.

5.2.6 Instrumentation Design

Control systems have moved on from operators manually performing logic checks or sequencing actions by directly opening valves or pushing buttons on the control panel. Now a digital computer permits the ultimate batch control system design. Tsai and Lane (1976) discuss instrumentation design philosophy reflecting working experience with the Tenneco Chemicals system.

The overall instrumentation design concept is to:
- develop a system with the capability to maintain automatic control of the process operation at least 99% of the time
- involve minor operator intervention for a broad range of conditions

This concept dictates a significantly different instrumentation system from one designed for manually-controlled operation. The differences include:

a. On/off valves: can be operated either by computer or manually (with status monitoring), more complicated than the conventional design
b. Reactor charging system: materials are metered in automatically, using flow and level measurements
c. Reactor header valves: for increased safety all charge and discharge lines for each reactor are equipped with redundant valves. Each valve is independently controlled by the computer or panel push buttons when the panel is in manual mode. This design increases the probability that the system remains under computer control even in the event of valve failure.

5.2.7 Distributed Systems

A distributed system is attractive if it is cheaper, less vulnerable, easier to program, and easier to operate and maintain than a conventional system (or at least satisfies some of these criteria). The cost of cabling signal wires to one central computer in the control room can be reduced by decentralising the control function to field devices that communicate with the central computer via a digital data link, as long as there is no need to buy more expensive hardware. A distributed system may also be less vulnerable, as a failure in one reactor does not affect the other 29 reactors (true as long as they can operate independently of the central computer). This means that the peripheral devices must store and execute sequence programs. A challenge for the designers of the system is to protect these decentralised processors from adverse environmental conditions, and to avoid electrical safety hazards.
5.2.8 System Check-out and Commissioning

Normally there is a complicated interaction between the computer system, control panels and the process. Therefore this needs to be checked before installation on the plant site. The best way to do this is to obtain the total system from one vendor, and to perform the integrated system test at the manufacturing facilities. It is of great benefit if the majority of compatibility problems, wiring errors and component failures can be picked up and resolved before shipping, making installation at the plant site less problematic.

5.3 Back-up Systems

There are scores of examples where a process design worked as long as all conditions followed the design premise yet failed when subjected to unscheduled outages, i.e. electrical power, pump or valve failures, or piping plugs (Gore and Hayden, 1976). Process designs are pilot planted to define many of these surprises. However, we cannot afford to find these surprises by pilot planting. Batch reactions are particularly susceptible to hazy projections because we seldom set up the degree of integration of reactant charging facilities or product handling capacity that is typical of a battery of full-size reactors. Also notable is the increased complexity of the instrumentation job as plants are designed. A result of designing larger batch systems is the degree of automation in a batch process plant. The case for automation has been proven many times over. Reliability of digital devices has made advanced software programming an attractive option. The problem is hardware reliability; the control function can be so complex and the control system failures so infrequent that the process operator is incapable of handling a major system failure in a safe and economical way.

Prevalent in digital system designs have been extensive backup systems to provide the operator a means of action during system failure. For on-off devices these systems have been primarily push-button-based relay stations permitting the operator to be in parallel with the computer. For direct digital control, computer/manual or computer/automatic/manual stations offer requisite backup. We have seen the number
of such stations grow as new and better ways to run processes are found. This growth has spawned the operator's problem especially after the system has already been running on its own. The operator would have been trained what action to take in an emergency, but if the system has run successfully on its own for a long period of time and then one day several alarms are initiated would the operator remember what to do.

This situation leads to a re-examination of methods used to backup digital systems. We shall take a look at functions being handled by the digital computer to identify means of handling the backup situation without overburdening the operator and yet functioning at reasonable costs.

5.3.1 Requirements of a Back-up System

Requirements such as achieving a ratio of chemical reactants, or adhering to a temperature profile, should influence the choice of backup system. Digital systems have taken over many functions from operators including:

- taking over recall of operating procedure and figuring out a schedule to use process equipment in an optimum fashion – a job that once belonged to production control personnel;
- handling performance process control according to predefined profiles - done previously by cam programmers and analogue controllers;
- lining up charging valves to and from shared reactant headers, monitoring valve positions and starting pumps and motors in a safe manner - this is done effectively by sequence controllers and more recently by programmable controllers;
- batching reactants into premix tanks and reactors according to specified recipes - a job handled by pulse-driven batching systems and weigh-scale trip systems.

Each function had previously involved plant operators. The primary purpose of equipment being displaced by the digital system was to make the product safer, faster and more reproducible. The digital system has been able to integrate these jobs and yet improve its flexibility over those using individual items. Cost of this added capability has not been high because several devices previously used had been expensive. The back-up system whether manual or automatic needs to be able to keep the plant
running, but not necessarily sustain all the duties of the digital system.

5.3.2 Establishing a Back-up Philosophy

The nature of batch reaction control systems has been shown to require:

1. A high degree of flexibility to tolerate a variety of processing requirements;
2. Provisions to avoid contamination because of shared facilities;
3. Fast and accurate action timing to meet recipe requirements.

These characteristics lead to the conclusion that many reactions cannot be adequately handled by manual controls. Certainly use of direct digital stations with automatic/manual backup is common, as is supervisory control.

If the operator cannot handle all control functions of a digital system, what can be done?

1. It is not likely for batches involving even the slightest complex charging schemes to be successful when manually implemented. Therefore, a backup system need not support all capabilities of the digital system particularly when starting new batches.
2. The backup system must safely and economically handle failure of any part of the system at any time. In batch reactions, since many reactions are so path dependent, this conclusion generally means that the backup system must permit reaction continuation on reaching a stage where a change from the expected reaction course would ruin a significant amount of product or cause damage or extended equipment outage.

The most important design criterion for the computer system is to achieve maximum reliability at a reasonable cost. Systems sometimes include redundant central processing units (CPUs), with control automatically switching when failure is detected in the CPU in use. Some doubt the necessity of the second CPU as it is usually the most reliable part of the computer system; however, the consequences of computer failure for a batch process are more serious than for a continuous process. The second
CPU allows completely uninterrupted control of the process, without loss of data. Without the second CPU, all batches in operation at the time of computer failure would need to be manually completed or aborted. This would create not only a tedious situation, but also a potentially hazardous one. Controls such as reactor temperature and pressure should use direct digital control, but conventional analogue controllers should back up each one. The back-up philosophy must also include maintenance functions, which support debugging, and the testing of a system with a problem. It must also allow us to test field equipment during start-up and maintenance functions.

5.4 Application of Batch Computer Control to Pipeless Plants

The multi-product (multi-purpose) pipeless plant consists of multiple mobile reactors and functional stations where charging, mixing etc. occurs. The major concern throughout a batch process is temperature; adding or mixing chemicals changes the temperature for each step; maintaining a desired temperature may require heating and cooling in the same vessel. It is also important to control reactor pressure in all steps. This is also true for pipeless plants, but there are other points of concern that need to be monitored and controlled such as the position of the reactor, the progress of the batch, contamination from product changeovers etc. The following characteristics of pipeless plants are important from a control point of view:

1. Product change-over, leading to frequent reactor start-up and shut-down
2. Processes run in different mobile reactors at the same time
3. Different stages requiring different control strategies during an individual cycle

The overall design concept is the same as with a batch plant, to develop a system with the capability to maintain automatic control of the process operation at least 99% of the time, with minor operator intervention for a broad range of conditions. The design philosophy essentially maintains the desired separation between manual control and computer automatic control while maximising safety considerations.
Sequence control is necessary for the very concept of pipeless plants, where the process can be split into operations, and each operation split into smaller tasks which need to be completed in order to formulate a product. In computer controlled pipeless plants, sequenced operations can be event-initiated, and are therefore less wasteful of time. The reactor does not have to wait for operator intervention, as it completes tasks. The computer monitors the progress of each task/operation from initiation to completion, and eliminates delays due to the operator.

5.4.1 Software and Hardware Considerations for Pipeless Plants

The control system for a pipeless plant will have to cope with many of the same issues as multi-product batch plants. A pipeless plant will have many discrete state inputs and outputs and relatively few control loops. Discrete outputs are very important to processes carried out in pipeless plants that rely on the timed sequences of such actions. There should not be any planned operator intervention but manual access to the discrete control elements must be allowed, to deal with problems that could arise.

The computer carries out the batch cycle, with minimum participation by the operator. A batch is initiated by selecting an empty, clean vessel and assigning a product recipe to it. With confirmation required from the operator before proceeding at specified intervals the vessel would follow the recipe sequence and make a product. After discharging the product the vessel would go to the cleaning station, after which it would be empty, clean and available again. The hardware required for this control system would be very similar to multi-product batch plants, e.g. on/off valves with status monitoring, automatic charging system, redundant valves for safety etc. The operator interface would also be like that of a batch plant. A distributed control system could be used to operate a pipeless plant. Each functional station could be under its own control, with the ability to communicate with the central computer. This allows for a more secure system, i.e. failure in one station does not mean a plant shut-down. The software developed for pipeless plants should be similar to batch plants, but with attention focused on additional parameters such as the mobility of the vessels, status monitoring, equipment assignments etc. This is where computerised sequenced
control becomes very important, particularly automatic sequence/recipe loading, communications with continuous control, and communication with the operator.

5.4.2 Backup Philosophy for Pipeless Plants

In case of failure to the computer system of a pipeless plant, the backups developed would be comparable to a batch plant. An analogue back-up system capable of sustaining full plant operation would be very expensive. This makes a second CPU necessary in order to prevent a complete shut-down in case of CPU failure. The control strategy would be to halt the process in a safe state. This means stopping all material flows, and positioning heating and cooling valves to predetermined safe levels, but may also require the removal of the mobile reactors. Status monitoring is required in order to continue the processes from their interrupted states. Backups of temperature, pressure, level controllers etc., should also be provided.

5.5 Conclusions

With the degree of flexibility that a computer control system can effectively use comes potential confusion when we manually try to assume the computer’s role. With pipeless plants, we must learn to build systems so that we can preserve the plant’s economic value. Attractive computer control opportunities involve reactions that would require close supervision to prevent going out of product specification and doing it safely. With the high reliability of digital systems the emphasis of the operator’s training would stress recovery from critical process steps.

The digital portion of the system, as in a great many operating batch control systems, has a significant amount of redundancy. Dual CPUs and operator’s consoles offer considerable insurance against total unavailability of the digital system. However, should there be such a problem, safe back-up will be provided by the programmable controllers and analogue computer stations. To guard against a PC failure causing an unsafe situation, some inputs and outputs are shared with another PC.
To progress, we must be able to develop more analytical approaches to sequencing control, to develop a new generation of control systems which will respond as an operator would respond. One must be careful about operator use in a computerised plant. If there are manual operations to be done, it is desirable to allow an operator to ready the operation but let the computer actually control the time at which it happens. Absolute regulation of this time will allow us to commercialise many processes that cannot currently be commercialised because of normal operator variability along the time base. For the application engineer, this means that any procedure that can be easily computerised should be, and those that cannot be computerised must be engineered to interface with an operator.
6. Hazop of Computer Systems

Although the use of computer control provides many benefits to the running of a process plant, it also introduces problems due to faults. Most hardware faults occur in the measurement and control systems attached to the computer rather than the computer itself, but computer faults do occur and are more common than once thought (Kletz, 1994). Using experience of these failures it may be possible to prevent them from recurring or at least reduce their impact. Therefore hazard and operability studies should check that systems are designed so that the effects of predictable failures of power or equipment are minimised.

The hazard identification techniques described in the chapter 3 are useful for identifying process and component failures and their effects. However, they are not appropriate for computer controlled systems as they do not consider the control logic and are not suitable for identifying potential hazards due to computer system failures or inappropriate responses from the computer system. Therefore new or modified hazard identification techniques are required for studying computer control systems.

6.1 Chazop

There already exist modified versions of Hazop for computer-related systems (Andow (1991), Nimmo (1994)) called Chazop or PES (Programmable Electronics Systems) Hazop.

There should be a preliminary study as well as a full one. The preliminary study should identify factors that influence the overall architecture, and the safety-related functions of the system.

There are several different Chazop schemes available (Kletz et al, 1995):

1. The simplest scheme replaces existing process-related guide words and deviations with computer-related ones. Different sets of words could also be used, one set
considering the hardware and logic of the system, and the other for considering human factors. There is a draft guideline for Chazop requirements and general application guidance produced by the UK Ministry of Defence (1996). During a Chazop the team would go through a diagrammatic representation of the system by considering all the links between different components on the diagram. Possible deviations from the design intent being investigated systematically applying the guide words to attributes such as data flow and control flow. Not all guide words are applicable, therefore inappropriate ones should be removed from the study list during the planning stage, and new ones may be added during the study at the discretion of the leader.

2. Chazop methodology, according to Andow, need not stick rigidly to the format of the traditional Hazop, although the essential ingredients of a team, using questions to systematically investigate a system are essential. He suggests that there should be a preliminary and a full Chazop. The preliminary to identify critical factors that influence the overall architecture and functionality of the system, to be carried out early in the design, including:
   - the proposed architecture of the system
   - safety-related functions
   - system failure
   - failure of power and other services.

The full Chazop to be carried out in greater detail later in the design, taking into account three different aspects of the system:
   - computer system/environment
   - input/output (I/O) signals
   - complex control schemes.

3. Lear suggests an alternative to Andow's Chazop, specifically concerned with computer control. The top three concerns in this case are hardware, continuous control, and sequence control. Guide words used include short- and long-term power supply failure. In addition it advises using a checklist published by the Health and Safety Executive.
4. Another alternative Chazop framework by Nimmo, also highlights three main concerns, hardware, software interactions, and the effect software has on the process. In this scheme a conventional Hazop is first carried out, with the computer treated as a black box. The next stage is to retrace the route but this time concentrating on how the software will respond under different circumstances. The last stage considers how the software, divided into areas such as sequence control, continuous control and data links achieves its control actions. A list of topics is provided for discussion in a series of Chazop meetings, under the headings: the overall plant, the safety backup system, instrumentation and the PES.

Other schemes also exist which also use different lists and interpretations of guide words such as the one developed by Little (1995).

There is no specific right method for carrying out a Chazop, and there is little experience in applying the different methodologies. However the view is that software cannot be considered alone and the framework for any study should include hardware, software and the environment in which they operate (including human interaction). The main strength of conventional Hazop is that it facilitates systematic exploratory thinking, with the use of guide words and deviations. The problem of using the various Chazop schemes is that they are not only specific to a particular study, they are also influenced by their creators, and therefore the relevance of certain guide words/headings and questions is questioned. The suitability of the different schemes will only become evident through practical applications.

There is a general Chazop methodology being developed (Kletz et al, 1995) based on incident analysis, i.e. using information from past incidents involving safety-critical systems. This information is organised to provide a structured framework for considering future applications. The strategy behind the methodology was to derive a set of questions for a particular incident, asking why the incident occurred and what could have prevented it, and then to generalise these questions. An example is given in chapter 2 of Kletz et al (1995). It used Event Time Diagrams, task structures and the associated questions for analysing tasks.
6.2 Automatic Verification of Sequential Control Systems

The article by Moon et al (1992) addresses the use of an automatic verification method for process control systems that involve discrete event dynamics. The aim of the study is to determine whether a formal verification method would be able to identify effectively errors in a system that includes both the control system and the chemical process equipment. A search method using temporal logic is used to find errors in the control system.

This method consists of three components:

- **Assertions**: questions about the system
- **Process models**: describing the system
- **Model checker**: automatically determines whether the system operates as specified by the assertions

Errors are identified by comparing a question (an assertion) about system behaviour with a model of the system. The question, given as a series of temporal logic statements, is associated with safety and operability and is derived from industrial standard checklists, process design specifications, and/or other methods such as Hazop or Fault Tree Analysis. The model of the system is derived from the process flow diagram, control software, and the piping and instrumentation diagram (P&ID).

The model checker searches the state space of the system and determines the truth of the question (assertion), i.e. whether or not each of the logic statements is satisfied.

The main advantages of this method as applied to pipeless plants is:

1. The inclusion of process models means that the interactions between software and process hardware are tested.
2. The procedural search method (algorithmic) gives a very thorough inspection of the system.
3. Testing with the same set of assertions can compare alternate designs.
4. An automated search method means that there is potential for testing complex systems.
The current method does not automatically revise the system design. In addition the limitations of this procedure are:

1. Its use is restricted to discrete event systems.
2. Its success depends on the development (completeness) of process models.
3. Generation of appropriate assertions is dependent on the user's interpretation of the system.

Moon et al (1992) have suggested four points that need to be considered carefully before this method is applied to real industrial problems:

- A more extensive library of state transition models that include timers, delays, and counters.
- A more complete list of temporal logic assertions for the general testing of discrete chemical process control system safety and operability.
- A high-level language for stating assertions.
- A strategy for identifying the source of errors so that appropriate design changes could be proposed and evaluated.

Other points of importance:

1. This technique finds potentially hazardous states that can exist, and therefore would make the system safer. However it does not indicate operational problems, and it does not tell us how the modifications in terms of safety affect the operation. If certain conditions are not allowed how is the flexibility of the pipeless plant affected?

2. Who is going to analyse and develop a chemical processing system using this method?

The designer of the system may not be able to ask the right questions of his/her own design.

A consultant trained in the technique could be expensive, and may not know the business and operational strategies of the company he/she would be developing the system for.

A team made up similar to a Hazop team, where knowledge and experience is important, would have difficulty in applying the technique.
6.3 HAZAPS Methodology

The HAZAPS methodology has been proposed by Broomfield and Chung (1997) as a possible means of solving the problem of integration between hazard analysis and requirements engineering. Methods used include fault tree analysis, use of generic hazards list, structured design and object orientated analysis. The procedure for applying HAZAPS is developed further by Yang and Chung (1998). It is split into four stages. The objectives of the first stage is to subdivide the system and to identify the subsystems which are safety critical. The purpose of the next stage is to construct safety requirements for the subsystem based on the associated hazards. Each of the hazards are investigated using a fault tree. The objective of the third stage is to transform a safety requirement into operational requirement for the system. The purpose of the final stage is to analyse the critical events using a library of keywords/questions. The end result of applying the methodology is that safety critical subsystems have been identified with their associated safety requirements, hazards, components, task lists, Event Time Diagrams (ETDs) and recommendations.

6.4 Hazard Analysis and Support Tool

Chung et al (1999) have extended and modified the HAZAPS approach. A framework for identifying hazards in general computer controlled processes is proposed, and a computer support tool for this framework is described. The Process Control Event Diagram (PCED) representation proposed in the paper is described below. Not only the control logic is expressed but also the effect of each control action on the process. Unfortunately existing representations such as Piping and Instrumentation Diagrams (P&IDs) and Signed Directed Graphs (SDGs) do not represent precisely the structural and behavioural information of computer control systems. The Process Control Event Diagram (PCED) representation described in the paper complements P&IDs. It consists of seven functional levels: human, input device and display, communication 1, computer, communication 2, sensor and actuator, and process.
The PCED represents the system in terms of events, order of events, components, and control and data flow. It is made up of:

- labelled arcs: propagation of signal, or the causal action or effect
- nodes: objects, input/output variables, or computations

The PCED model is based on the sequential behaviour of a computer, and the order of events can be read from left to right. A simple example of a PCED is shown below.

![Simple Example PCED Diagram]

**Figure 3:** Simple Example PCED

The content of the computation node is simply:

If temperature < setpoint then goto N1

This representation can be understood by people from different disciplines, and can facilitate discussion and identification of errors and hazards. This takes the form of a computer Hazop. Possible deviations to the design intent are introduced using guide words, the same as conventional Hazops but with different definitions, as prompts for each action in the PCED. The computer support tool incorporates all these stages, and
includes a built-in safety related question library based on industrial incident reports as the final stage. The questions are organised in a structural framework so that only relevant questions are prompted, e.g. by components such as sensors, alarms and actuators.

This process of hazard identification is time-consuming especially for complex chemical plants. Computer-aided identification makes the process far more efficient. The support tool described in this paper (Chung et al, 1999) implements the hazard analysis framework, records all the information generated during the analysis and produces customised reports. Both discrete and continuous control systems are considered in the paper. There are five stages in the framework:

6.4.1 Stage 1. Safety Requirements Identification

The system is sub-divided and the safety-critical subsystems identified, e.g. a high temperature reactor. The safety requirements are constructed by examination of the environment and identification of potential hazards. A chemical process can be divided into smaller parts on the basis of operating units with a standard function. Safety requirements are expressed in terms of critical states that certain operating units should not reach. The control logic should prevent the system from reaching these critical states.

6.4.2 Stage 2. Process and Control Logic Representation

The control logic to achieve a required function is specified. It is expressed at a high level so that it can be examined by a review team made of experts in different fields. The Process Control Event Diagram (PCED) has been developed for this purpose.
6.4.3 Stage 3. Verification of Control Logic

The control logic has to be shown to satisfy the safety requirements of the system before being implemented. The PCED is used to determine the state transitions of the control logic. The final and all intermediate states have to be safe for the control logic to be acceptable. If this is not the case then the control logic needs to be modified and verified again.

6.4.4 Stage 4. Safety Critical Events Identification

By the introduction of deviations from normal behaviour for each control action, e.g. no signal, the causes and consequences (response of the control logic) of each deviation can be identified. If the deviation causes the system to move into a state that violates the safety requirements, then it may be necessary to modify the control logic, or to prevent the causes of the deviation from occurring.

6.4.5 Stage 5. Application of Life Cycle Question Library

Some safety critical events can be prevented from occurring by asking appropriate questions early in the design stage. A safety question library, based on experience from industrial incident reports, is part of the computer support tool. The library is structured so that relevant questions can be located easily.

6.4.6 Application of the framework

The first step of the framework is process representation. This involves the subdivision of the plant and identification of safety-critical subsystems. This fits very well with the pipeless plant concept as the plant is already divided into dedicated functional stations. In addition, for each station the pipeless plant HAZOP has already indicated the safety critical subsystems, and the safety requirements of those systems.
### 6.5 Summary of Computer Hazard Identification Techniques

<table>
<thead>
<tr>
<th>Hazard Identification Techniques</th>
<th>Application</th>
<th>Appropriateness to Pipeless Plants</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHAZOP</td>
<td>Computer control systems</td>
<td>Same philosophy as conventional Hazop, modified to specifically deal with computer control - hardware, software and interaction with the process. Problems with process and control representation.</td>
</tr>
<tr>
<td>Automatic Verification of Sequential Control Systems Using Temporal Logic</td>
<td>Computer control systems</td>
<td>Success dependent on the development (completeness) of process models, and the generation of appropriate assertions (questions), using checklists, Hazop etc. is dependent on the user’s interpretation of the system. No indication of affect of changes on operation or flexibility. Requires a great deal of work before can be applied industrially.</td>
</tr>
<tr>
<td>HAZAPS</td>
<td>Computer control systems</td>
<td>Systematic and thorough, but may be time-consuming due to the use of FTA for every hazard in every subsystem.</td>
</tr>
<tr>
<td>Hazard analysis and support tool for computer controlled processes</td>
<td>Computer control for both continuous and discrete systems</td>
<td>Systematic and thorough, and very similar to HAZAPS but developed further. The representation is much improved, using PCEDES which include not only the control logic, but also the effect of each control action on the process. A computer support tool is available to make the analysis less time-consuming, which includes Questions Library from past incidents.</td>
</tr>
<tr>
<td>Fault Tree Analysis (FTA)</td>
<td>Continuous processes, and computer control</td>
<td>Quantitative and specific. Indicates more of the risk of particular failures, rather than identifying hazards. Again, extremely time-consuming if applied too broadly. Therefore used more as a support tool.</td>
</tr>
<tr>
<td>Event Tree Analysis (ETA)</td>
<td>Continuous processes, and computer control</td>
<td>Used more to evaluate the possible outcomes of specific failures. Again, extremely time-consuming if applied too broadly. Therefore used more as a support tool.</td>
</tr>
</tbody>
</table>

Table 6: Summary of Computer Hazard Identification Techniques, their Applications and Appropriateness to Pipeless Plants
Section 4:

Schedule Safety
7. Discrete Event Simulation

A simulation is a model whose behaviour can, with some imagination, be interpreted in terms of the behaviour of the system being studied. From a different perspective, a simulation model can simply be a mathematical description of the system being studied. This type of model can then be manipulated using the laws of mathematics to generate useful information. Discrete event systems are dynamic systems that evolve in accordance with the abrupt occurrence of physical events. To ensure the orderly occurrence of events in such systems some degree of supervision and control is generally required. A batch process running in a pipeless plant is such a system. A vessel following a recipe to formulate a product visits stations in a predefined sequence. Each time the vessel visits a station a transformation occurs to the vessel contents. This transformation is a discrete event. After the product has been formulated it is discharged and the vessel is cleaned. It is then available to be assigned another product and starts production all over again. If there are a number of these vessels operating within a plant, the issue of optimal utilisation of available resources with regard to safety needs to be examined.

7.1 Techniques

A strategy for solving complex pipeless plant problems needs to be developed, through the use of computer-aided analysis. The production paths of products are determined not only by the production sequence (decided by scheduling) but also by the location of stations and the movement of vessels. In developing a plant layout a suitable structure for station and parking area positioning, and the layout of tracks for the movement of vessels needs to be developed. The main objectives of a plant layout are to make the movement of vessels easy, minimise the production lead times and facilitate quick changeovers. The best way to do this would be to simulate the production using different plant layouts and then deciding on the best, depending on performance. We therefore need to establish a strategy for simulation.

We require two types of data to describe the plant layout:
• the track segment and nodes
• the position of each station

The usual type of stations that will be used in a pipeless plant are: filling, mixing, reaction, separation, discharging and washing. There are various ways to arrange these stations such as: linear, herringbone, and star.

Liu (1996) uses simulation to develop an operational strategy for pipeless plants. Liu (1996) states that to carry out a simulation would require the input of the plant configuration, production requirements and schedules. The main duty of the simulation would be to examine the movement of the vessels that carry out the production tasks. The way to simulate movement is to divide each section of the plant layout into different steps, and at any instant in time, one vessel can only move one step. Certain assumptions have to be made about the movement, such as: only one vessel can use or occupy one station at a time; only one vessel can use the track at the entrance to a station at a time; vessels waiting for the next process step either remain in their present station if not required or go to a parking (waiting) station. Liu (1996) develops the simulation to evaluate a particular plant layout, however the results of the simulation are not included in the thesis.

Collision problems that have been identified are:
• Station conflict
• Head on collisions between vessels travelling in opposite directions on the same track
• Collisions between vessels travelling in the same direction on the same track at different speeds
• Vessels breaking down on a track blocking other vessels
• Vessels on the wrong tracks

The operation of a pipeless plant requires co-ordination of the production tasks, particularly when operating concurrently. Safety is a critical issue, and needs to be addressed in terms of the relationship between plant layout and smooth production.
A discrete event system is one in which a phenomenon of interest changes value or state at discrete moments of time rather than continuously with time. One example of this is a bus, a system in which the number of passengers can change only when the bus arrives at a stop. Another example is a pipeless plant, where the contents of a reactor undergo a change when they arrive at a fixed station.

In a computer simulation the investigator of necessity must explicitly specify the sources of variation and the degree of variation due to each source in order to make his simulation run. This enables the investigator to eliminate unwanted sources of variation simply by omitting them from his simulation.

Computer simulation also enables the replication of an experiment. This means rerunning an experiment with selected changes in parameters of operating conditions being made by the investigator.

### 7.2 Applications

A simulation program that will enable us to model the behaviour of a pipeless plant as close as possible to a real life situation.

- Require communication between vehicles and stations
- Need to enter as much detail as possible about the process recipe to make the model as accurate as possible
- Need to be able to do more than one process reaction at a time
- Need to have some kind of queuing for shared resources
- Need a priority system for station selection
- Need to be able to introduce interruptions/problems/breakdowns

The simulation should be able to help to demonstrate and hopefully help solve some of the following problems:

- Effects of safety precautions on multi-product flexibility
- Hazards associated with changing the plant layout
- Safety-related rules for producing plant layout
Combining of process hazard identification with layout/routing/scheduling hazard identification, e.g. combining HAZOP with simulation

How does plant control change with changing layout?

Other useful products of simulation:
- Output of unit operation analysis
- Enable us to produce production schedules
- Enable us to explore production policies in terms of plant layout
- Indication of bottlenecks, e.g. track usage, waiting times etc.

Other safety problems to be considered:
- Connection/disconnection at the stations
- Product switchover

7.3 DES Tools

There are many different software packages available which would allow the discrete event simulation of pipeless plants. Two of these, ARENA and WITNESS, are described below:

7.3.1 ARENA

SIMAN/Cinema (Banks, 1995), from Systems Modeling Corporation, is a general-purpose simulation language and animation system designed to model discrete event, continuous, and combined discrete/continuous systems.

SIMAN models are generally constructed in a graphical form, but can also be constructed in a statement form. Therefore not requiring programming it is not limited to experts.
The user's component, called Application Solution Template (AST), can be tailored to a specific industry, company, or project. Users can create their own ASTs to aid in developing focused simulation models, using Arena's Professional Edition. Template design is done graphically, without any programming.

Arena is easy to work with, using the SIMAN simulation language and Cinema animation system.

Built-in verification tools offer a wide range of capabilities to monitor the execution of the simulation and to explore new scenarios by immediately implementing changes to the executing simulations.

Data can be easily transferred from and delivered to popular software products like Lotus and Excel. Plus, Arena can interface with any ASCII data file and import AUTOCAD layouts.

Important aspects of SIMAN V:

1. Special features useful in modeling manufacturing systems include the ability to describe environments as workcentres (stations) and the ability to define a sequence for moving entities through the system.
2. Constructs that enable the modeling of transporters and guided vehicles.
3. An interactive run controller permits breakpoints, watches, and other execution control procedures.
5. Input and Output Analysers

7.3.2 WITNESS

Manufacturing Orientated Software: designed to quickly and accurately create a simulation. Greatly reduces the time required to build a model (Thompson, 1995).
Machines can be single, batch, multi-station or multi-cycle. Options exist for vehicles and tracks. Parts can be smart (having their routing attached), or dumb (elements of the processing decide the appropriate routing).

Track and vehicle logic allow requests for certain types of jobs, vehicle acceleration and deceleration, park when idle and change destinations dynamically. Many types of routing logic are possible in addition to the standard push and pull. If-Then-Else conditions may be specified.

Reporting capabilities include on-screen information about modeled elements. Reports may be exported to spreadsheet software.

Debugging or brainstorming can be accomplished by stopping the model, changing desired parameters, and continuing with the model from the same point in the simulation time. According to the instruction manual the running of the model cannot be stopped to introduce a breakdown. Breakdowns have to either be scheduled, or introduced before the model starts its run.

7.4 Conclusions

Simulation is a very useful visual aid for demonstrating the behaviour of pipeless plants. It can be used to identify safety and operational problems related to the movement of reactors between stations. One of the advantages of pipeless plants is to be able to implement new processes quickly. Simulation is very useful for this as it allows different plant layouts and schedules can be tested quickly and easily. It can also be used to illustrate how a change in the layout or schedule would affect the system.

After a demonstration of the capabilities of both software packages ARENA was believed to be the more applicable for the research that needed to be carried out.
8. Simulation Case Study

There are many useful lessons that can be learned from simulation. If it is used for modelling the behaviour of pipeless plants it becomes a hazard identification tool and can help to:

1. Show the importance of explicit behaviour specification, i.e. the simulation software will not allow you to proceed until every single item that is involved has been specified correctly. These items can be missed in real life, but the simulation software flags them as errors, and in this way becomes a safety tool.
2. Show the location of possible collisions between vessels.
3. Show the effects of failures to particular items, such as a station or a vessel, on the overall plant.

Simulation can also be used as a design tool. It enables the designer to propose alternatives, and explore them. This is much faster, cheaper and easier than building a plant and then finding problems that would be very expensive to put right.

Below is an example of a process which can be carried out in pipeless plants. This is taken from a published paper (Realff et al, 1996), where the primary aim was to produce a schedule to obtain the optimum yields of different products. Safety has not been considered in designing the plant layout for this process. This case study was carried out, firstly to observe how the schedule performed and to investigate what improvements could be made. Secondly to introduce problems and examine their effects on the plant. The problems encountered in setting up the simulation and running it are described below.

8.1 Description of the Process and Plant

The process has the following steps:
1. A clean vessel goes to a Charging Station, where it is charged with Feed A. Both Charging Stations have the same feed.
2. The charged vessel then goes to a Reaction Station where a product, ProdA, is formed. Both Reaction Stations can carry out the task, but Reaction Station A is faster (and more expensive).

3. The vessel can then be discharged to an external storage tank (ProdA), thereby leaving an empty (essentially clean) vessel, or go to a Mixing Station. Both the Mixing Stations are the same.

4. At the Mixing Station the vessel contents can be blended with additives A1 or A2. The corresponding products Prod1 and Prod2 are discharged to external storage tanks directly from the Mixing Station.

5. The empty, soiled vessels must then be cleaned before re-use.

8.1.1 Plant Layout

The plant layout considered has a “herringbone” structure, which can accommodate up to eight processing stations, up to four stations can be on either side of the centre track, which is bi-directional. No more than one vessel at a time can occupy a station. Realff et al (1996) conclude that the optimum plant to produce the maximum amounts of all three products on a daily basis, comprises 7 processing stations and 6 transferable vessels.

![Plant Layout Diagram]

Figure 4: Plant Layout
It is assumed that travelling time between stations opposite each other is zero, and between stations adjacent to each other is 15 minutes.

### 8.2 The Schedule

The suggested schedule for the first 12 hours of the case study is shown in Figure 4.

The initial progress of Vessel 2 can be followed on the schedule:

- **0:15-0:45** Charging at Charging Station B (Station 2 on schedule)
- **0:45-1:00** Travelling from Charging Station B to Reacting Station A
- **1:00-1:30** Reacting at Reacting Station A (Station 3)
- **1:30-2:00** Mixing with A2 at Mixing Station A (Station 2)
  \[\text{Assumes zero travelling time between station as they are opposite}\]
- **2:00-2:15** Travelling from Mixing Station A to Cleaning Station
- **2:15-2:45** Cleaning at Cleaning Station (Station 7)
- **2:45-3:15** Charging at Charging Station B (Station 2) and so on ...

For the simulation this series of steps can be translated into a sequence that Vessel 2 follows while travelling around the plant, including the duration it is stopped at each station.

Since the processing time for Reacting Station A is less than Reacting Station B, and it is a shorter distance from Charging Station B, it is primarily used for the reaction step. Both Mixing Stations are the same, however, Mixing Station A (Station Number 5) is used because it is directly opposite Reacting Station A so the travelling time is very small. Three operations are performed at the mixing stations: discharge of ProdA; addition of A1, and then discharge of Prod1; addition of A2, and then discharge of Prod2.

After the discharge of any product, a vessel is cleaned before being used for the next batch. The suggested plant layout has the Cleaning Station located opposite Charging Station B in order to reduce the time that the vessels are empty, clean and not in use.
Vessel 1 does not enter production until 10:45 hours. It is assumed to have travelled to Charging Station A (Station Number 1), and remained there until required. This would explain why Charging Station B (Station Number 2) is primarily used for the first 12 hours.

Key to Tasks:

<table>
<thead>
<tr>
<th>x:y</th>
<th>x: vessel</th>
<th>y: task</th>
</tr>
</thead>
<tbody>
<tr>
<td>1: Charge</td>
<td>4: Mixing 1</td>
<td></td>
</tr>
<tr>
<td>2: Reaction</td>
<td>5: Mixing 2</td>
<td></td>
</tr>
<tr>
<td>3: Discharge A</td>
<td>6: Cleaning</td>
<td></td>
</tr>
</tbody>
</table>

Figure 5: The Schedule
8.3 Setting up the Simulation

The plant described above was simulated using ARENA simulation software (Banks, 1995), to investigate the performance of the schedule proposed by Realff et al (1996) for the layout. The simulation was specified as close as possible to the case study as described. While trying to set up the simulation the importance of explicit behaviour specification became evident. This meant that vessel sizes, vessel speeds, network paths, track lengths, processing times in stations etc., see Table 6, could not be missed as they would be flagged as errors. This makes the simulation software very useful as a safety tool.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vessel size</td>
<td>1 unit</td>
</tr>
<tr>
<td>Vessel speed</td>
<td>1 unit/minute</td>
</tr>
<tr>
<td>Track length between adjacent stations</td>
<td>15 units</td>
</tr>
<tr>
<td>Track length between opposite stations</td>
<td>2 units</td>
</tr>
<tr>
<td>Charging time</td>
<td>28 minutes</td>
</tr>
<tr>
<td>Reaction Time</td>
<td>28 minutes</td>
</tr>
<tr>
<td>Mixing Time</td>
<td>28 minutes</td>
</tr>
<tr>
<td>Discharging Time of A</td>
<td>28 minutes</td>
</tr>
<tr>
<td>Cleaning time</td>
<td>28 minutes</td>
</tr>
</tbody>
</table>

Table 7: Values of Parameters as used in the Simulation

The travelling time between stations opposite each is specified in the paper as 0 minutes. However, in the simulation the vehicles have a definite size (of 1 unit), therefore the track length leading to the station cannot be 0 units (it has to be 1 or more) otherwise the vehicle cannot enter. This means that it takes the vehicle 1 minute to enter and 1 minute to leave each station. The processing time for every operation is specified in the paper as 30 minutes. Therefore by using 28 minutes for processing times in the simulation, with 1 minute to enter and 1 minute to leave each station, the time spent at each station is 30 minutes.
8.4 Running the Simulation

Once the plant and schedule had been specified Arena attempted to run the simulation. However, the simulation could not keep to the specified schedule, and eventually terminated, flagging up errors such as vessels moving in opposite directions on the same tracks. This happened as a result of delays forced upon vessels in the plant, due to having to wait at intersections or at stations. Consequently subsequent batches were introduced before the preceding ones had completely finished. As a result more vessels than specified in the schedule were moving around in the plant leading to traffic congestion. A number of problems were identified and these had to be solved before the simulation could run to completion.

8.5 Points for Discussion

Building and then running the simulation case study highlighted some important points, namely:
1. The starting points for the vessels – off plant, behind charging station etc.
2. Intersections – number and location, vessel priority
3. Vessels returning to the start after the completion – route: main track or alternative
4. Vessel breakdowns – removing and reinstating
5. Number of vessels used – congestion, utilisation

8.5.1 Starting Points for the Vessels

There was an immediate problem with the schedule, as it is not specified where each of the vessels starts. The first batch starts after 15 minutes at Charging Station B, therefore it appears from the schedule that the first vessel enters the plant at the right hand side. After charging is complete (30 minutes) the vessel goes to Reaction Station A, and after 30 minutes processing time it goes to Mixing Station A for another 30 minutes before going to the Cleaning Station (for 30 minutes). The subsequent batches carry out the same sequence. It is not possible for the vessels to enter the plant
from the right, follow the sequence and keep to the schedule published. The vessels are all using the same section of the main track, travelling in both directions. It is not specified as to whether or not the vessels can pass each other on the track, however, common sense would imply that the vessels cannot pass each other on the same length of track, otherwise plant layout and scheduling would not be an issue. One other possibility is for each track to have two lanes, but this is not stated in the paper. Therefore assuming a one-lane track where vessels cannot pass each other, the only way to enable the vessels to follow the sequences of actions in the production, is to introduce delays and therefore the schedule as published does not work.

Starting the vessels at the left-hand side of the plant would reduce some of the delays by reducing the traffic in that particularly busy section of track. To make the simulation as close as possible to the published schedule the first vessel started from the right hand side of the main track, and all the rest started from the left. One possible way of reducing delays in production is for a number of vessels to be able to be waiting at the intersection at Charging Station B, thereby reducing the time that the station is unoccupied (and idle). However, parking areas have not been specified in the paper, so the vessels would have to wait on the track before the station. As there is no production going on in the left side of the plant, and as long as the vessels arrived at the intersection to Charging Station B at the correct time then there is no need for them to wait on the main track, which would just lead to more congestion.

The starting points of each vessel must be specified and taken account of in the schedule. Ideally for simplicity and safety they should start from the same specified parking place, which should be as close as possible to one of the Charging Stations.

8.5.2. Intersections

The issue of vessels passing each other, at intersections, causes a real problem at the intersection between Mixing Station A and Reacting Station A. At time 1:45 hours, Vessel 4 has to go from Charging Station B to Reacting Station A, arriving at 2:00 hours. However it cannot enter the station as it is already occupied by Vessel 3.
Therefore Vessel 4 has to wait at the intersection. The next station in the sequence for Vessel 3 is Mixing Station A, which it cannot go to as it is already occupied by Vessel 2. The next station in Vessel 2’s sequence is the Cleaning Station. To do this it must pass Vessel 4, waiting at the intersection. It is not possible to do this and therefore all the vessels in the simulation stop, this is termed “shop locking”. The only way that Vessel 2 could continue would be if Vessel 4 had actually gone through the intersection and waited at the other side. This particular scenario occurs several times at the same intersection during the first 12 hours of the schedule, i.e. at times 2:30, 3:00, 4:45, 5:15, 5:45, 6:45 etc. Basically every time that Mixing Station A and Reacting Station A are occupied and the next vessel has been charged and sent to Reacting Station A. The rules of movement through intersections have not been specified in the original paper. At other points in the plant, such as at the charging stations, the vessel must wait before the intersection so there is no problem for the vessel being charged exiting the station, and moving in a particular direction. It would be difficult to program vessels to treat each intersection differently. The easiest and safest way to run the plant would be to specify the intersection rather than the vessel. Rules are required to specify where the vessels wait for all intersections. Therefore it does not matter which vessel it is, or what stage in the production schedule has been reached, the positioning of the vessel is always known.

8.5.3 Vessels returning to the start position

There is a problem with vessels returning to the start after they have completed their tasks and been cleaned, because of the next vessel coming into the plant. In the paper because the Cleaning Station is opposite Charging Station B, most of the time the schedule shows that as soon as the vessel has been cleaned it immediately starts the next batch, and does not leave the plant. However, at certain points all four stations (Charging Station B, Reacting Station A, Mixing Station A and Cleaning Station) are occupied. The only way for the vessels to proceed with their sequences is for the Cleaning Station to be made available, but the vessel cannot enter Charging Station B as it is occupied, so the options are either to wait on the track (increasing congestion) or for the vessel to leave the plant. In addition, at time 3:30 hours, Vessel 5 completes
its run, and then is not shown on the schedule until it starts its next batch at 4:00 hours. It cannot wait on the track as it would interfere with other vessels, therefore to maintain the schedule it must exit the plant to the right, and then re-enter from the right at the start of the next batch. When it re-enters it will encounter the same problems as described in the previous section on starting points. Due to delays being introduced to overcome the other problems in the simulation, it could not be guaranteed that immediately after cleaning the vessel could go to the charging station. In reality any delay at all from vessel breakdowns to erratic processing times would lead to the problem of a vessel that, after having being cleaned, could not immediately start the next batch. However, the vessel cannot remain in the station as it is needed for the next vessel, and can only wait on the track as long as it doesn’t interfere with movement of other vessels. Therefore the safest option again is for the vessel to leave the plant, and then re-enter when it is required for a subsequent batch. Leaving and re-entering to the right of the plant is the quickest way, but it also creates more problems. Leaving to the left of the plant is much safer, but takes longer as it is a greater distance from the Cleaning Station. Since the vessels enter from the left it is more logical for them to return to their starting point when not in use. The best option would be for the vessels to leave directly from the Cleaning Station.

8.5.4 Vessel breakdowns

The paper has not specified any parking stations or any way to remove vessels from the plant in the event of a breakdown. As the paper is concerned with the design, layout and schedule together some thought should be given to what would happen should a breakdown occur. The vessel needs to be removed, and maybe even re-introduced, with minimum interruption, if any, to the schedule. We should consider whether all vessels should be stopped, or just vessels in the nearby vicinity. What about vessels in stations? Should they continue with their processes or be stopped as well?
8.5.5 Number of vessels

Realff et al (1996) specified that the optimum number of vessels is six. However in the schedule for the first 10 hours 45 minutes only five vessels are used, with real problems of congestion. A sixth is introduced which just adds to the problems. By reducing the number of vessels the congestion can be eased and the plant can be run more smoothly, however the productivity will be down. On the other hand, it is a waste to have six vessels and use only five of them for nearly 11 hours out of 12. Therefore another layout is required, that will make better use of the vessels.

Overall it was found that the schedule could not be made to work precisely, as published, on the ARENA simulation software. It required modifications to the times to incorporate necessary delays for the production to proceed. The delays made the plant slower, and it is possible therefore that the design chosen was not the optimum.

8.6 Discussion of Simulation Results

The aim of the plant is to manufacture products as quickly and safely as possible. In business productivity will not be totally surrendered for safety. The best plant would be one in which the productivity is high and safety is acceptable, rather than one in which safety is exceptional and productivity is average. In the simulation it is necessary to introduce delays into the published schedule to make it work, but with reduced productivity. To overcome the problem at the intersection between Mixing Station A and Reacting Station A, as described above, the schedule has to incorporate a total delay time of 1 hour 45 minutes in the first 12 hours (since the problem occurs 7 times). There are other possible solutions, such as altering the plant layout, instead of introducing delays. However it is much simpler to alter a schedule than the layout, therefore altering the layout should be considered only if the new layout significantly improves productivity.

One way to alter the layout is in terms of the positioning of the stations, such as the Cleaning Station. Although this does save travelling time in some instances since
some of the stations are now closer together, it also adds time in others, and overall cannot be significantly improved from the layout as described in the paper. In addition to this it is not desirable to change the layout continually.

Another possible modification would be to include a loop into the layout whereby the vessels can return to the start after they have completed their tasks. This tackles some of the issues described previously in terms of:

- the starting points of the vessels
- the problems encountered at intersections
- vessels returning to the start after completion of batches
- vessels can be removed more easily in the event of problems such as breakdowns.

The problem of collisions between vessels travelling in opposite directions on the same track is greatly reduced, especially if the loop is uni-directional. In addition some of the delays introduced before the initiation of batches can be removed. Removing the delays will improve the productivity, however, the time taken to travel around the loop could be significant. This time would not matter as long as there were enough vessels to continue production (may require more than six). In the published schedule only five vessels are in use at any time.

Figure 6 shows the loop running from either end of the central track. This is the simplest positioning of the loop. The vessels may enter from the left side and leave the plant at the right side, following the loop back to the start. This reduces the traffic congestion on the main track. Vessels may also be removed from the loop for maintenance. The main drawback as described previously is the distance the vessel has to travel around the loop and therefore the increased travelling time (a minimum of one hour for the vessel to travel from the Cleaning Station back to the start).
A simulation of this layout was created. The vessel was given the destination and automatically chose the route that was the shortest distance and therefore never used the loop. The modifications to the original simulation to make it work with the introduction of the delays produced a better production schedule than by using the loop.

Another option could be to have a central loop, i.e. two tracks running parallel with each other, as in Figure 6. This option could however introduce additional safety problems as it proposes even more intersections (eight instead of four). Therefore although possibly solving some of the problems it supplements others.
As stated before, the best solution would involve the vessel leaving the plant directly from the Cleaning Station to the starting point. It solves the problem of congestion, vessels returning to the start after the completion of a batch, vessel breakdowns, and increases productivity.

Analysis using the simulation software of the different layouts clarified that the best choice in terms of productivity is the loop from the Cleaning Station. Other factors
that have to be considered before a loop is installed include available space, safety, and cost. Below is a screen grab showing the plant running with the external loop from the cleaning station.

Figure 9: Screenshot showing the plant running with the external loop from the cleaning station.
8.7 Simulation Conclusions

The discrete event simulation of the case study has given definite indications of the type of problem pipeless plant designs would encounter in terms of layouts and schedules. Rules are required before commencing the building of the simulation, and to complete a successful running model. The points highlighted in Chapter 8.5 have indicated that the designer of the system must consider the following before building the simulation model:

1. Before commencing the designer must consider:
   - The starting location of the vessels: off plant in one location, or all queued up behind the charging stations
   - The finishing location of the vessels: position of cleaning station(s) is important
   - The route the vessels take to return to their starting location at the end of a batch: back through the plant or externally from the cleaning station(s).

2. Intersections also require careful consideration. The number of approaches should be minimised. The vessels may need to wait at intersections, and if so they could wait on the track or parking spaces could be provided within the intersections themselves. There may be a need to prioritise, and therefore queuing systems would also be required.

3. Broken down vessels need to be removed from the plant for safety. Consideration needs to be given to how this is done, and whether all vessels should be stopped in the event of a breakdown or selected ones. Vessels could be re-introduced at the point at which they were removed depending on the product. Alternatively they may need to be cleaned of any product and introduced back at the start as empty clean vessels.

4. The need for discharging stations. It may be possible to discharge directly from the reacting stations or mixing stations. However a station dedicated to one particular task is safer than a station where multiple tasks have to be carried out. However,
due to the short shelf-life of some products, having an extra station to which a vessel has to travel to is not such a good idea, in terms of both time and the increased possibility of vessel breakdown.

5. The number and location of cleaning stations. It may be possible to function with only one cleaning station, however a problem at the cleaning station would lead to the predicament of running out of clean vessels. Therefore redundant vessels although not cost-effective may be a good idea. It is also a good idea to locate the cleaning station(s) in a position that causes the least congestion, that means close to the charging stations if the vessel starting points are behind them.

6. The number of vessels: there needs to be enough vessels to maintain production, and may be even some redundant ones in case of breakdowns. However the greater the number of vessels actually moving around the plant the greater the congestion and the possibility of collision.

7. Future Expansion: there may be a need to add (or remove) stations later on, due to different products being manufactured, or even alter the plant layout. Some designs would limit this option and there the original layout chosen needs to be as flexible as possible.

Although the mathematical formulation in the paper by Realff et al (1996) uses constraints such as the location of the stations, which station carries out which processing task, the number of vessels and their transfer times between stations it does not take into account the location or specific routing of the vessels. Two papers by Gonzalez and Realff (1998) go some way to improving this original formulation. In the first paper mixed integer linear programming (MILP) formulations use travel times and task durations that allow for conflicts to be resolved and for variations in plant operations. The output of the MILP is implemented in a discrete event simulator, which is event driven rather than time driven. The performance of two plant layouts is compared in the paper; the MILP is not able to distinguish them between but the simulator is. This is expected as the scheduling does not take into account the detailed
interaction of the vessels as they move around the plant. This again shows the necessity of discrete event simulation for examining the layout and scheduling problem for pipeless plants. Since flexible vessel transfer times are used to account for unexpected fluctuations the exact whereabouts of vessels or the exact duration of tasks is not known. If the model is built using Arena simulation software, it would be possible to observe at any moment the exact location of the vessels and the points that the stations carrying out operations have reached. In addition to the other benefits such as detecting bottlenecks and exploring alternative layouts and schedules. The second paper by Gonzalez and Realff (1998) uses local dispatch rules to control station operation and vessel movement. The dispatch rules work by deciding the routing of a vessel progressively, i.e. the next station is decided only when the current task is completed. The results obtained using unsophisticated dispatch rules measure up quite poorly when compared with the results of the MILP obtained in the first paper. However, Gonzalez and Realff (1998) found that the dispatch rules performed much better when information from the MILP schedule was incorporated into them. In fact the results were comparable to the MILP. Although it is much better to use simple dispatch rules, that are easily understood and communicated, to run the plant, the right information is required to integrate these rules, such as the results of a predictive scheduling algorithm. Although it may be quite complex to build a plant in Arena simulation software, it is based on following simple rules as described earlier.

Huang and Chung (2000) propose a general constraint model for generating production schedules for pipeless plants. The scheduling problem is treated as a constraint satisfaction problem (CSP) and is solved using constraint satisfaction techniques (CST). The CSP consists of a number of variables and a number of constraints on or among those variables. The solution of the CSP is the designation of values to the variables that satisfy all the constraints simultaneously. This is achieved through constraint propagation, i.e. using constraints to deduce other constraints, and detecting inconsistencies in possible solutions. The main constraints in this paper are to do with vessel allocation, station or resource allocation, precedence and time constraints – starting of first job, ending of last job, and a vessel waiting for a station to become available. A working computer system called batch processing scheduler (BPS), originally developed by Huang and Chung (1999) to solve the scheduling
problems of common batch plants, is extended based on this constraint model to solve the scheduling problems of pipeless batch plants. A simple case study, similar to the one described earlier in this chapter, is used to demonstrate the applicability of this approach. Huang and Chung (2000) recognise the limitations of their system in not considering specific plant layouts and the routing of the vessels, and research is already underway to further develop the system.

In any case, whichever way a schedule is produced whether using MILP formulations, vessel dispatch rules or constraint satisfaction techniques (CST), it is still necessary to test the schedule. Discrete event simulation has shown to be a very useful tool for doing this.

The usefulness of visual discrete event simulation has been successfully demonstrated. It has been shown that no matter how good a scheduling program is, there is always the possibility of error (or that something has been overlooked). Only by visual simulation of the plant, with the proposed schedule and layout can one be confident that the proposed design will work. Simulation gives the designer a much deeper understanding of what is involved with the project, which otherwise would be achieved by actually building the plant (or pilot plant) and realising your mistakes.
Section 5:

Integrated Methodology
9. Integrated Methodology

It is necessary to provide an integrated methodology, not only combining the work carried out in different areas of safety progressively, but also allowing inter-linking and the versatility to consider the whole picture. Previously three areas of safety had been identified for examination: process, computer control and schedule safety. Each of these areas considered has some influence on the others areas of safety therefore there should be some kind of contribution from one to the other, rather than using the different procedures independently. A flow diagram has been produced to show the integrated procedure, starting from the initial design, showing the inputs and outputs from each stage in the methodology and their influence on other stages, concluding in an improved design. There is not only a progression from one phase to another but also feedback to improve the original ideas.

Phase 0: The proposed Initial Design, produced probably by a chemical engineer with an understanding of both the process and the plant engineering requirements.

Phase 1: The first procedure to be carried out, by a Review Team, is the Pipeless Plant Hazop. The aim of which is to identify and minimise or control the hazards in the process. Parts of the outcome are an improved P&ID and Operating Instructions. In addition the Hazop gives an indication of the requirements of the control system.

Phase 2: Once the critical control systems have been identified they need to be assessed using the modified HAZAPs methodology, to check that the control system performs in the way its design intended. The same Review team can be used as for the Hazop study.

Phase 3: The outcomes of both the Pipeless Plant Hazop and HAZAPs influence the proposed layout of the plant. Discrete Event Simulation is then used to explore the plant layout and scheduling problem, to ascertain the optimum combination in terms of output and safety.

Phase 4: The overall result of the combined methodologies is an Improved Design.
Figure 10:  Flow Diagram Showing the Integrated Methodology
9.1 Process Safety

The process safety is investigated initially as it is an examination of the design and the design intent. In a similar way to a conventional Hazop, a team of experts using a systematic method for examining the system is the way to proceed. Using guide words as prompts leads to the right questions being asked, thereby indicating potential problems. This is like a conventional Hazop, however, for a pipeless plant (batch process) the guide words and deviations/parameters that are applied are different, and the method for applying them is also different. The way that a pipeless plant is naturally divided up into distinct stations aids the investigation by allowing the process (and plant) to be analysed station by station. This is an inherently safer design as there will never be a problem of overcharging say at a mixing station, since there is nothing being charged. It should, therefore, also be quicker to examine the system from the point of view of safety. Particular control problems are indicated for particular stations such as level for a charging station, which can be investigated further in the computer control safety (CHAZAPS section). In addition the reactor itself is examined, especially the possible deviations that could occur on its support systems, such as agitator, heating and cooling units etc. as well as pipelines. The end results of the review should be improvements to the P&IDs, operating instructions and other information, an indication of the safety critical subsystems for the computer control safety review (CHAZAPS), and a further input for the Discrete Event Simulation section.

9.2 Computer Control Safety

The main problem to be overcome in a pipeless plant is that different stages require different control strategies during an individual cycle. The control cannot then be hardwired with permanently fixed set points for different control systems. The set points must be product (recipe) specific. Other important considerations for computer control are product changeover (frequent reactor start-up and shut-down), processes run in different mobile reactors at the same time. The overall design objective is to develop a system with the capability to maintain automatic control of the process
operation for the majority of the time, with minor operator intervention for a broad range of conditions.

As stated, different stages or operations require different control strategies therefore the overall control philosophy should be a combination of control philosophies required for each operation (and station) in the design. For example, for the charging operation the emphasis is on the level control. If the level control does not operate correctly it could be either hardware faults such as sensor failure, or software errors i.e. software will perform functions in the way it has been instructed to, therefore the original programming must have been flawed. The output of the pipeless plant Hazop can be used as an input to the CHAZAPS software. A review on the process safety should automatically pick up any safety critical subsystem such as level control during the charging operation. The CHAZAPS software tool allows a team of experts to analyse a particular control system. Developing and using a Process Control Event Diagram (PCED) the team can understand not only how the control system performs, but also the effects of operator input to the system and the output effect the control has on the process. Deviations from normal behaviour are then considered for each action in the PCED using a kind of computer Hazop (part of the CHAZAPS software), which using guide words and deviations indicates potential hazards. The guide words and deviations apply to control software such as ‘no data flow’. The CHAZAPS software enables the recording of minutes in the form of causes, consequences, actions etc. Another part of the software is the Safety Related Questions Library, a section where relevant safety questions are asked due to lessons learnt from past incidents. The results of the CHAZAPS should be an improved control philosophy and safer control of the processes running in the plant. In addition the information produced can be used as an input to the Discrete Event Simulation section.

9.3 Schedule Safety

The main aim of Discrete Event Simulation (DES) is to examine the movement of the vessels that carry out the production tasks. Carrying out a simulation requires the input of the plant configuration, production requirements and schedules. Any assumptions
made about the movement have to be stated, such as: only one vessel can use or occupy one station at a time; only one vessel can use the track at the entrance to a station at a time etc. The DES software used, Arena, demonstrates the importance of explicit behaviour specification, i.e. the simulation software will not allow you to proceed until every single item that is involved has been specified correctly. These items can be missed in real life, but the simulation software flags them as errors, and in this way becomes a safety tool. Computer simulation also enables the replication of an experiment. This means rerunning an experiment with selected changes in parameters of operating conditions being made by the investigator, i.e. exploring improvements and alternatives.

The number of stations is dependent on the production requirements, and available space. When making decisions about the layout and schedule, the results of the reviews on the process safety and computer control safety should be made available for consultation. The number of stations and their location in the layout can be influenced by the review of the process safety of pipeless plants. If there are raw materials that are incompatible then not only will they be charged at different charging stations, but their respective charging stations should be located a safe distance from each other.

To model the behaviour of a pipeless plant as close as possible to a real life situation the following is required:

- Fine details about the process recipe to make the model as accurate as possible
- Queuing systems for shared resources and priority systems for station selection
- Ability to introduce interruptions/problems/breakdowns

Problems that are looked for when carrying out an analysis:

- Station conflict
- Vessels conflict
- Vessels breaking down on a track blocking other vessels
- Vessels not where they should be, wrong station or wrong track
Discrete event simulation should not only be able show how well a particular schedule works with a specific layout but should also be able to demonstrate and hopefully help solve some of the following problems:

1. Indication of bottlenecks, track usage, waiting times etc.
2. Effects of safety precautions on multi-product flexibility
3. Hazards associated with changing the plant layout
4. Safety-related rules for producing plant layout
5. Combining of process hazard identification with layout/routing/scheduling hazard identification, e.g. combining HAZOP with simulation
6. Output of unit operation analysis
7. Enables the analysis of the efficiency of production schedules
8. Enables the exploration of production policies in terms of plant layout

The results of the DES should be a safe, efficient and correctly working schedule and plant layout.

9.4 Conclusions

Three areas of safety had previously been identified for careful consideration in the examination of the proposed design of a pipeless plant. It has been demonstrated how each of these areas has to be investigated. It has also been shown how these three areas interact with each other; the outputs from one study influence the inputs to another study. The end result is an integrated methodology that will systematically analyse a proposed design and correct problems, to produce an improved and safer pipeless plant.
Section 6:

Case Study
10. Case Study: Production of Cakes in a Bakery Pipeless Plant

There are a number of pipeless plants already in operation. The types of product being made at these plants include lubricants (Shell U.K.), paints and inks, water management chemicals, lubricants, and photochemicals (Asahi, Japan), paints and adhesives (Toyo, Japan), paints (Herberts GmbH, Germany), and solvent-borne paints (France). It was decided to use a case study to illustrate the integrated methodology described in the previous chapter. A number of different batch processes were examined mainly with regard to their suitability to pipeless plants. As well as the products referred to above the manufacture of waxes, co-polymers, pharmaceuticals, brewing, milk and fruit juices, and minerals was also considered. However, there were problems with each of these with regard to the availability of information about real life processes without an industrial partner. The only other option was to design a process. After careful consideration it was decided that a food process such as the baking of cakes would not only be suitable due to its very nature of always having to be carried out as a batch process, but would illustrate very well the concept of pipeless plants to enable flexible, multi-product manufacture.

10.1 Introduction to Baking

There are a number of features about a bakery that makes it ideally suited to pipeless plant technology and vice versa. A bakery normally makes a range of similar products, where the ingredients and certain process information may be different but the equipment required is the same. Product changeover with the acquisition of new business introducing new products to the plant such as different types of cake, different flavours, and different baked goods could be implemented quickly and easily with the altering of set-points, addition or removal of stations etc. Baked products have a limited shelf life and therefore will be made to order (Just-In-Time processing). Typically a bakery already functions as a set of individual stations, dedicated to single tasks, such as mixing, heating etc., therefore it should fit the model of a pipeless plant without too many modifications.
A bakery to produce different types of cake is described here. In the simplest of terms the baking process can be split into a number of operations:

- Charging of dry and liquid ingredients
- Mixing the ingredients into a homogeneous dough
- Separating (dividing) the dough up into specific sizes and shapes
- Heating (baking) the dough pieces to produce cakes
- Packaging the cakes that are discharged from the oven
- Cleaning the vessel and the pans from the oven

Both chemistry and physics are important in baking. If the chemistry of baking is looked at in its simplest terms with regard to the ingredients, it is the type of flour and the amount of water that are the biggest influences on the class of product. After that it is other ingredients such as sugar, fats and raising agents that play an important role on the quality of the product. The action of mixing the ingredients into a dough is probably the most important of the operations that is carried out. If it is not done right it will be the source of most of the quality problems (Blanshard et al, 1986). The dry ingredients are charged first, followed by the liquid ingredients. Carrying out the task the other way around results in lumps forming in the mix. There are several different methods of mixing, but the simplest single-stage method of mixing is to be used. All the ingredients are charged into the mixer bowl (mobile vessel), after which they are beaten at two different speeds to achieve a homogeneous dough. The dough is passed through a dough divider which cuts it into the required size. The dough pieces are then baked in an oven at around 180-200°C for the required length of time. The cakes produced are discharged to the packaging area, where they are packed and ready to deliver.

10.2 Process Description

In more detail the process steps can be described as:

1. A clean vessel goes to a Dry Charging Station, where it is charged with the dry ingredients (flour, sugar etc.). Each of the different Dry Charging Stations has a different feed corresponding to a particular recipe.
2. The vessel then goes to a Liquid Charging Station, where it is charged with the liquid ingredients. There are three Liquid Charging Stations, one feeding water, another feeding whole milk or whole eggs (labelled milk for simplicity), and the third feeding an ingredient specific to the recipe (such as chocolate liquor for chocolate cake).

3. The charged vessel goes to a Mixing Station where the contents are mixed to a desired consistency of dough.

4. The charged vessel then goes to a Dough Dividing Station. The contents of the vessel, the dough, are fed into the dough divider to be cut in specific sizes (and shapes).

5. An empty vessel is left behind, which must then travel to the Cleaning Station, to be cleaned before re-use.

6. In the mean time the dough pieces go on pans via a conveyor to the Heating Station (oven). The dough pieces are cooked for a certain length of time to produce cakes that are discharged via a conveyor.

7. The cakes leave the oven and travel to the Packaging Station where they are packed.

8. The pans from the oven can be cleaned after they have been allowed to cool.
A flow diagram of the baking process is shown below:

Figure 11: Simple flow diagram of the baking process, illustrating the different functional stations in a pipeless plant.
To produce one batch (100kg) of each type of cake, the total ingredients are listed in the following table.

<table>
<thead>
<tr>
<th>Ingredients</th>
<th>A Yellow Layer Cake</th>
<th>B White Layer Cake</th>
<th>C Ginger面包</th>
<th>D Chocolate Cake</th>
<th>E Devils Food Cake</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dry</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flour</td>
<td>21.5</td>
<td>25.6</td>
<td>21.1</td>
<td>18.0</td>
<td>17.3</td>
</tr>
<tr>
<td>Sugar</td>
<td>30.0</td>
<td>25.6</td>
<td>8.4</td>
<td>27.5</td>
<td>26.8</td>
</tr>
<tr>
<td>Shortening</td>
<td>11.5</td>
<td>11.2</td>
<td>9.4</td>
<td>10.6</td>
<td>9.6</td>
</tr>
<tr>
<td>Baking powder</td>
<td>1.3</td>
<td>1.6</td>
<td>0.5</td>
<td>1.0</td>
<td>0.7</td>
</tr>
<tr>
<td>Salt</td>
<td>0.8</td>
<td>0.6</td>
<td>0.5</td>
<td>0.8</td>
<td>0.8</td>
</tr>
<tr>
<td>Evaporated milk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>10.2</td>
</tr>
<tr>
<td>MSNF (Milk-Solids-No-Fat)</td>
<td></td>
<td>2.1</td>
<td>2.5</td>
<td>3.8</td>
<td></td>
</tr>
<tr>
<td>Sodium Bicarbonate</td>
<td>0.2</td>
<td></td>
<td></td>
<td></td>
<td>0.5</td>
</tr>
<tr>
<td>Cinnamon</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.5</td>
</tr>
<tr>
<td>Ginger</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.5</td>
</tr>
<tr>
<td>Allspice</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.2</td>
</tr>
<tr>
<td>Cocoa</td>
<td>3.8</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Liquid</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Water</td>
<td>9.2</td>
<td>14.7</td>
<td>21.2</td>
<td>24.1</td>
<td></td>
</tr>
<tr>
<td>Whole milk/Whole eggs</td>
<td>34.9</td>
<td>16.0</td>
<td>8.4</td>
<td>15.0</td>
<td>9.7</td>
</tr>
<tr>
<td>Egg whites</td>
<td>16.0</td>
<td></td>
<td></td>
<td></td>
<td>2.9</td>
</tr>
<tr>
<td>Molasses</td>
<td></td>
<td>33.5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chocolate liquor</td>
<td></td>
<td></td>
<td></td>
<td>3.5</td>
<td></td>
</tr>
</tbody>
</table>

Table 8: Ingredients to produce 100kg batches of different cakes, Matz (1972)

For this case study a number of stations are required. In particular we have to consider the number of charging stations for both the dry and the liquid ingredients, which are going to be different. The mixing stations should be the same, carrying out the same tasks at the same speeds etc., as should the dough dividing station(s) and heating station(s).
Although overall the manufacture is run as a batch process, it actually occurs in two distinct phases. The initiation of the manufacture: the charging and mixing is carried out in mobile vessels following a recipe, moving around the plant to specific stations. The second phase utilises the dough diving, heating stations etc. involves trays moving along a conveyor, without any flexibility as to the destination.

- Dry Charging Station 1 - Cake Mix A
- Dry Charging Station 2 - Cake Mix B
- Dry Charging Station 3 - Cake Mix C
- Dry Charging Station 4 - Cake Mix D
- Dry Charging Station 5 - Cake Mix E

  Mobile Vessel

- Liquid Charging Station 1 - Water
- Liquid Charging Station 2 - Milk
- Liquid Charging Station 3 - Other

  Mixing Stations

- Dough Dividing Station
- Heating Station (Oven)
- Packaging Station

  Conveyor

- Cleaning Station

  Both

For simplicity it was decided to only produce four types of cake, as this would make the production schedule easier to work out if eight vessels were to be used. Therefore only Dry Charging Stations 1 to 4 were used.
10.3 Process Operation: Charging

The charging of all the ingredients would be carried out at the same time in one reactor should this be a batch plant.

The liquid ingredients are metered in, and the dry ingredients are fed gravimetrically though the feed hopper. The amounts of all ingredients charged is controlled by the computer.

The batch Hazop is carried out first and one of its outcomes is that there are potential problems of overcharging, if all the charging is done at the same time at one station. It would be inherently safer to charge the dry and liquid ingredients at separate charging stations.

Figure 12: P&ID for a combined Charging Station for the bakery
10.3.1 Automatic Batching Systems

Weighing operations for flour, sugar, and some other ingredients are integral parts of the bulk-handling systems (Matz, 1972). Other ingredients can be dumped into receiving hoppers daily or more frequently. Bag unloaders, sifters, and conveying systems (mechanical or pneumatic) will precede the receiving or surge hopper. Automatic conveying and metering or weighing devices eliminate manual transfer thereafter. Automated bakeries generally use a central control panel registering and controlling many remote scales. In one form of the automated weighing system, formula weights are set in advance of each day's schedule by a supervisor who adjusts the weight selector dials behind the console. When the mixer operator signals readiness, the central control operator starts the material by pressing a button. A further advance is the computerised system, in which recipes for several kinds of products are recorded on tape, on circuit boards, or on punched cards. After the mixer operator signals for his ingredients the computer takes over all other functions. Changes, to compensate for differing flour moisture contents, can be made at will by typing them on the input station which is part of the computer circuit.

The advantages claimed for automatic batching include (1) elimination of human errors, (2) more consistent weights, (3) better sanitation, (4) less labour, and (5) reduction in loss of costly ingredients.

The automatic scale or meter is a system, or part of a system, made up of material handling devices, the weighing or metering equipment, data handling read-outs, and the controls which program the entire series of functions for automatic operation. All automatic scales transfer materials from some type of storage to a scale and from the scale to some destination. From the scale comes information in the form of electrical signals which controls the weights of ingredients and which can also be used to print out weight data for quality control, inventory control, and other management requirements. The simultaneous co-ordination of all feeders can be achieved by powering each of the critical drives with an induction motor receiving its electrical power from a central adjustable frequency source.
A typical digital blending system will include:

1. A master unit with integral controls for setting system demand rate, batch size, valve ramp rates (up and down), and preshutdown point. Automatic shutdown will be initiated either by measured or demand total.

2. Ratio unit (one or more) for setting individual component ratios by manual thumb-switches. Multicomponent ratios are available, and 3 or 4 digit settings are optional.

3. Individual component controllers, either pacing or memory, to provide control of the addition rates of the separate ingredients. Standard features include integrated total flow indication, manual valve control, and a low flow alarm to warn the operator when the measuring device is functioning below the linear flow range.

10.4 Process Operation: Mixing

10.4.1 Mixing Station

Figure 13: P&ID showing the Mixing Station
Process Steps:
1. When the vessel is in position the agitator is lowered into it.
2. The contents of the vessel are mixed at low speed for a specified time (e.g. 1-3 mins).
3. The mixer is then turned to high speed for a specified time (e.g. 5-8 mins).
4. The vessel is transferred to the Dough Dividing Station.

Fortunately the mixing of cake doughs is not as problematic as the mixing of some other doughs such as bread, therefore the more simple vertical mixer can be used as opposed to the horizontal mixer. In addition the vertical mixer is more adaptable to the idea of a pipeless plant. Since the dough bowl can be changed, the vessel can be the dough bowl.

10.4.2 Vertical Mixers

A unifying feature of vertical mixers is the use of movable bowls or troughs. The other characteristics may be quite diverse; that is, there may be one or more beater shafts, the beater shafts may move in a planetary design or remain stationary, and the designs of the agitators can be varied over a wide range. The main types of interest to the baker are the planetary mixers capable of mixing batters and some doughs but most often used for adjuncts such as icings, and the spindle mixer used in the cookie and cracker industry primarily for mixing saltine and graham cracker doughs. The agitator movement is called planetary because it not only revolves around its own vertical axis at relatively high speed, but the axis also moves in circles as it is rotated around the bowl. These compound motions ensure that all of the mixer bowl volume receives beater action. Usually, a small part of the bowl at the bottom centre is raised so that this blind spot does not become a collecting point for unmixed material. Some mixers have a geared transmission to provide a choice of 3 or 4 speeds while others have variable speed drives permitting the selection of any desired speed within the limits of the equipment. The bowl is raised or lowered by an auxiliary motor in the larger units. A fairly extensive range of agitators is also available which makes this type of mixer the most versatile in this respect.
10.4.3 Power Requirements For Dough Mixing

During the mixing operation, the power requirement increases gradually until it reaches a peak after which it declines as the dough starts to break down. The power requirement is affected by mixer load, ingredients, temperature, and mixer efficiency. In a given mixer operating on a given weight of dough, the flour strength and amount of water are probably the most important factors affecting power consumption.

There have been many attempts to adapt recording wattmeters or other power-measuring instruments which would show objectively the dough development in the mixer, as replacements for the "art" of judging the status of the batch by the sounds the dough makes while moving around inside the mixer or by its appearance or "feel." None of the instruments has become very popular, perhaps because it has been difficult to equate the measurements with dough condition, especially if several different kinds of dough are being mixed.

10.4.4 Temperature And Mixing

One undesirable result of the intense shearing action of high speed mixers, is the generation of heat in the dough. Temperatures can affect the response of cookie doughs to machining, as well as the spread, texture, and surface appearance of the finished piece. This is more of a problem in horizontal mixers than vertical ones. The temperature of the dough leaving the mixture should be 20-25°C or slightly less. In some cases it may be necessary to cool the dough. An alternative way of maintaining the low temperature is to prechill the ingredients. This is quite difficult for solids, but works well with liquids especially water (and milk). Ingredient water chillers using vapour compression refrigeration equipment can be obtained from mixer manufacturers.
10.5 Process Operation: Separating (dividing)

10.5.1 Dough Dividing Station

Process Steps:
1. The dough is transferred from the vessel into the top of the divider after which the vessel can be sent to the Cleaning Station.
2. The dough is divided (cut) into appropriate sizes by volume.
3. The dough is then transferred onto trays on a conveyor belt.
4. The conveyor takes the trays to the Heating Station (the oven).

Dough dividers are measuring devices. The elastic, cohesive nature of the dough does not adapt it to gravimetric procedures. Also the constantly varying density that results from fermentation interferes with accurate volumetric measurements. Volumetric scaling has proven to be the most practical and economical.

The dough has to be transferred from the vessel to the dough divider where it is cut into lumps of the requisite weight by being forced into "pockets" of set volumetric capacity. The pieces of constant volume are then ejected onto a conveyor and back to the vessel.

A schematic of a dough divider is shown below:
The dough flows from the hopper into the underlying compression chamber. At the start of the cycle, a knife moves horizontally to cut off a piece of dough near the hopper bottom. Next, the ram or piston moves forward pressing the severed dough piece into a chamber contained in a rotatable cylinder. At the end of the ram stroke the cylinder turns, cutting off the excess dough and finally, the discharge lever ejects the measured dough piece.
Commercial models are available which have from 2 to 8 pockets, and can scale dough pieces at a speed of 2400 to 9600 per hour.

Requirements for our design are 200 cakes - at 2400 cakes/hour the time taken is 5 minutes.

10.5.2 Precautions to be Taken with Dough Dividers

1. Proper clearances between the knife and the ram, and between the dough box and the divider head need to be maintained for correct operation of the machine. Excessive clearance causes the dough to leak, and insufficient clearance will cause the machine to overheat with consequent bad effects on the dough and extra demands on the motor.

2. The ram and the knife control the amount of dough that enters the dough box, and they are adjustable. If an insufficient amount of dough is taken in, the weights of the pieces will usually be erratic, while an excessive amount of dough will receive unnecessary punishment which may cause poor performance of the dough in the later stages of processing. The former condition is frequently accompanied by a knocking sound in the divider as the partially empty pockets allow gas to be compressed in them. An up and down movement of the dough in the hopper is considered a symptom of poor adjustment, or of dough which is not pliable enough. The adjustments which will produce the best results for any particular dough must be determined empirically.

3. Breaking of the dough between the divider chamber and the dough hopper is a certain indication of improperly conditioned dough. It is important for the chute to have the proper pitch so the dough will be given an even pressure at the chamber at all times. Authorities indicate the chute should have an angle of at least 45° if possible, and under no circumstances should be less than 30°.
4. Accidents occur more frequently with dough dividers than with any other machinery in a bakery. The main risk is at the cutting section, where hand injuries have occurred due to operators reaching down the feed hopper, to push down the last piece of dough or during cleaning. There are also trapping risks in the drive mechanism and delivery conveyor.

5. The operator must not be able to reach the cutting section when the machine is running. Therefore the feed hopper should be designed to be of a shape and length to prevent this.

6. The feed hopper should be interlocked to the power supply if it is hinged or removable (interlock switch).

7. Edible oil (colourless, odourless and tasteless as possible) should be applied to the sides of the hopper to prevent dough sticking.

8. Removable panels and access doors opened for cleaning should interlock the power supply to the drive motor.

9. Time-delay interlocks or a braked motor may be needed if the machine does not stop immediately it is switched off.

10. So far as sanitary problems are concerned, divider oil will not support insect, rodent, or microbial life. Dusting flour is subject to the usual infestation problems if not carefully watched. Dirty or hardened dough pieces, if allowed to accumulate, can end up in the finished loaves as readily detectable contaminants.

10.5.3 Safety Features of Dough Dividers

Serious accidents can be caused if the hazardous nature of the divider is not fully recognised. The American Standard Safety Code for Bakery Equipment (Matz, 1972) lists the following desirable safety features for bakery equipment.
1. Pinch and Shear Points: All pinch points and shear points from rotating or reciprocating parts of the divider shall be enclosed or guarded, to protect the operator's hands and fingers from these hazards.

2. Front Guards: Guards at the front of a divider shall be so arranged that the weight of dough can be adjusted without removing the guard.

3. Rear of Divider: The back of the divider shall have a complete cover to enclose all of the moving parts, or each individual part shall be enclosed or guarded to remove the separate hazards. The rear cover shall be provided with a limit switch in order that the machine cannot operate when this cover is open. The guard on the back shall be hinged so that it cannot be completely removed and if a catch or brace is provided for holding the cover open, it shall be designed so that it will not release due to vibrations or minor bumping whereby the cover may drop on an employee.

4. Oil Holes in Knife: The oil holes in the knife at the back of the divider shall be of such size that an employee's finger cannot go through the hole.

5. Knife Actuating Arm: There shall be a saddle guard or other protective device on any elongate hole in the knife actuating arm at the back of the divider.

6. Shear Pin: Dividers shall be equipped with mechanical overload release devices such as shear pins.

10.5.4 Maintenance and Cleaning of Dough Dividers

Cleaning the divider is a rather difficult job which must be performed whenever the machine is shut down for more than an hour in order to prevent caking of the retained dough. Proper cleaning requires removal of the ram, knife, dough hopper, and pistons.

The following is a recommended sequence for cleaning (Matz, 1972):

1. Stop the divider with the knife and the ram all the way back.

2. Remove the housing covering the knife connecting links and release the knife.

   Draw the knife out of its guide slots and, if possible, remove it from the machine.

3. Disengage the ram from its connecting shaft, and draw it out of the dough chamber.
4. Remove nut holding plunger in cylinder and remove the plunger. Since the pistons are usually not interchangeable, they should be plainly marked if the manufacturer has not provided an identification symbol.

5. Remove the excess dough from the parts with a hardwood or plastic scraper and finish cleaning with water and soda or detergent. After rinsing and drying, cover the parts with a thin film of divider oil.

6. Place the oil catch pan under the divider head to protect the conveyor belt and vacuum or blow out all flour from the divider proper, the conveyor belts, motor, drives, and switch boxes.

7. Clean the inside and the outside of the divider housing.

8. Replace the plungers, ram, and knife.

10.6 Process Operation: Heating (baking)

10.6.1 Heating Station (Oven)

Figure 15: P&ID showing the Heating Station
Process steps:
1. Dough is transferred from the dough dividing station to the oven via a conveyor.
2. Dough heated for 30 mins at 200°C until cakes produced.
3. Cakes exit the oven via a conveyor on their way to the Packaging Station.

10.6.2 Ovens And Associated Equipment

The oven is the most conspicuous and characteristic piece of equipment in the bakery. With its associated loaders, unloaders, coolers, depanners, and conveyors, it dominates the layout and determines, in large part, the arrangement of the other pieces of equipment. Baking is also the operation which limits the output in most cake producing plants. For this reason, selecting an oven, maintaining it properly, and operating it at a maximum rate are key elements in the successful management of the bakery.

The oven has an important influence on product quality. It cannot compensate for errors committed earlier in the processing sequence, but a well-adjusted oven of the proper design can bring out the potential of a well-processed dough piece. The elements of oven design and operation which govern its effectiveness in optimising product quality are not completely accessible to scientific analysis. The mechanical details of oven construction are, of course, important in that they are related to labour requirements, efficiency of fuel utilisation, frequency of product damage, and sanitation. But of more fundamental importance and less well understood are the effects of heat transfer mechanisms on product quality. All ovens transfer heat by conduction, convection, and radiation. It is the differences in the percentage of heat transferred by each route that accounts for the variation in baking results in different ovens.
10.6.3 Tray ovens

Each tray holds several pans or straps and is permanently fixed to a conveying chain. The trays are pulled by the chain from front to back of the oven, then moved to a
lower track and continue baking on the return trip to the front, where they are unloaded.

Small sized travelling tray ovens may be operated as batch or multicycle equipment. After the oven is loaded, the pans are permitted to make two or more round trips before they are unloaded. In longer ovens, however, the travel time required for one complete cycle is sufficient to complete the baking so the oven can be operated continuously, and automatic loaders and unloaders can be used.

**Design Features of Travelling Tray Ovens**
The shell of the oven consists of a steel frame, resting on a level concrete foundation. The frame supports the steel lining sheets which form a rectangular baking chamber. Expansion joints allow the lining to expand and contract as the temperature changes without affecting the outer shell. A horizontal baffle divides the baking chamber into upper and lower compartments. The oven can also be divided in "zones" along its length, to allow application of a sequence of temperatures. The top, bottom, and sides of the oven are insulated. The insulation is covered and concealed by the exterior finish sheets which are usually enamelled white. Generally, the exterior sheeting is designed so as to be readily removable for inspection and servicing of the mechanical components located between the inner and outer walls. Rows of direct gas-fired burners extend into the oven cavity below and above the tray conveyor. The burners are arranged in groups to form control zones for regulating the temperatures in different parts of the oven. Every zone has a separate air and gas supply, a modulating temperature controller, and a group of burners. To permit adjustment of the heat balance across the oven, some or all of the burners are constructed so as to allow variation in flame intensity along their length. Each burner has a fuel mixing inspirator where gas at 0 psig and air are combined. Ignition is continuous in ovens made by this manufacturer. Indirect fired ovens have a more complex heating system. They will have one or more heating units located outside the chamber area. A heating unit will consist of a burner, combustion tunnel, heater body, radiator tubes, delivery and return ducts, circulating blower, exhaust stock with damper, controls, and safety devices. Ovens are one of the largest consumers of energy in a bakery (McKenna, 125).
1984), and there is a move towards using light fuel oil. There are some electric ovens in use and although gas ovens are in use they are becoming rarer.

Safety devices are of three types:
1. Controls regulating the mechanical functions of the loader, unloader, and tray conveyor
2. Controls regulating the heat in the baking chamber
3. Devices to protect against damage to the conveyor system, loader, and unloader and to prevent overheating of the oven and flues.

The conveyor drive is protected by three safety devices. If a pan or some other object jams the conveyor, it will either break a shear pin to disengage the main drive sprocket or activate an overload clutch which shuts off the motor. In the event these do not operate, the excessive current will cause the overload-protected magnetic starter to interrupt the electricity flowing to the motor.

There is ordinarily a safety bar mounted across the top of the oven loading door, and it will cause the conveyor to stop if it is contacted by a pan or lid overhanging the edge of the tray.

Pressure relief panels are held in place by thin strips or special bolts which release the panel when a sudden increase in pressure occurs. This arrangement may prevent serious damage to the oven as the result of an explosion.

Temperature limit controls shut down the fuel supply when the heat becomes excessive. Pressure switches also stop gas flow when the blowers fail. Gas pressure safety controls function when the pressure is too high or too low.

10.6.4 Auxiliary Equipment

Ovens can, of course, be hand loaded with pans or straps. This arduous task is accomplished by mechanical means in nearly all large volume shops, however. The principle of operation of loading devices is relatively simple. Pans move over roller
conveyors from the final steam proofer to a point in front of the oven loading door. Their momentum carries them onto a series of rollers at right angles to the previous conveyor and parallel to the oven door. When a series of pans the width of the tray or hearth has collected, they are pushed into the oven. A retractable metal bar prevents additional pans from coming onto the loading platform while the pusher bar is operating. The moving element in the loading device is synchronised with the travel of the oven trays (if it is a tray oven). Design variations are seen mostly in the actuating mechanism of the pusher bar and the way in which it is returned to its starting position. For example, it may go back and forth on the same level. In this arrangement, movement of pans onto the loading platform must be held up during the retraction cycle leading to some waste of time. Another version is designed to raise the pusher mechanism to a higher level as it is retracted, so that it passes over any pans which are coming onto the loading platform. In a third design, the pusher bar moves back under the loading platform, rising again as it passes the front end of the loading plate. This method of operation also clears the path of incoming trays during the return cycle.

In tunnel ovens, pans can be loaded as soon as a set comes into position, but the loader on a tray oven must wait until the tray is correctly situated inside the loading door. If a tray starts to pass out of the loading area before pans are available, a substantial amount of hearth space will be wasted. Loaders are customarily fed from the side of the oven. Side-feed loaders operate best at about four cycles per minute. Higher rates cause too much mechanical disturbance of the dough pieces as a result of the sudden acceleration. On the other hand, slower speeds do not confer any added benefits.

10.6.5 Unloaders

On some models of tray ovens, provision is made for tilting the trays carrying the baked bread just before they reach the loading position, so that the pans slide by gravity onto a cross conveyor at a lower level. This conveyor carries the pans through an opening in the side of the oven. High production rates and simplicity of operation
are features of this design. Level plane or horizontal unloaders use pusher bars to move the pans off the trays. Unloaders may also have a special fork lift that picks up a row of pans and transfers them to a take-away conveyor.

10.7 Process Operation: Packaging

10.7.1 Depanners

Depanners are of two major types, the gravity models in which the cake is dislodged by dropping the inverted pans a short distance and vacuum depanners which rely on a multitude of suction cups to lift the cakes out of the pans. Vacuum depanners will function properly only with certain types of pans. Cake-filled pans are placed on the pan infeed conveyor, which has a positive indexing finger to properly situate the pans in the depanning area. Empty pans are than returned to infeed area or storage. Vacuum is supplied from a 3 hp turbine pump. In addition, a compressed air supply at 50 lb pressure is required.

Pans coming from the depanner will usually be at a temperature between 120° and 150°C. They must be cooled to about 30°C before dough is placed in them.

10.7.2 Coolers

After the cakes have been removed from the pans, they must be cooled before being wrapped. The cakes may be stacked on racks and exposed to the cooling effect of the atmosphere, either aided by fans or not. Since racks occupy a great deal of floor space and require considerable manual labour to load, unload, and transfer, high volume bakeries make use of conveyorised coolers which are suspended from the ceiling, leaving space underneath for installation of other equipment. These coolers are equipped with a fan system which draws in air at the discharge end and moves it past the cakes, exhausting it at the top. More elaborate coolers make use of
air-conditioning units to refrigerate the air current and cut down on the time required for reducing the temperature to the desired level.

10.8 Process Operation: Cleaning

10.8.1 Cleaning Station

There are two items of equipment which need cleaning in this plant:
1. The processing vessel (where all the materials were charged and mixed)
2. The pans onto which the dough was loaded at the Dough Dividing Station.

10.8.2 Spray Cleaning of the Processing Vessel

Successful spray cleaning of processing vessels is dependent upon properly designed vessels and properly applied spray devices. The permanently installed fixed-ball spray has gained favour over rotating and oscillating spray devices. Its advantages include (Stewart and Seiberling, 1996):

1. There are no moving parts.
2. It can be made completely of stainless steel.
3. Its performance is not affected greatly by minor variations in supply pressure.
4. A properly established installation will continue to provide satisfactory service.
5. It sprays the entire surface all of the time.
**Figure 15.7** Fixed ball-type spray device locations are suggested in this photograph for cylindrical horizontal tanks and processing vessels. Silt type tanks are generally cleaned with disk or disk distributors of nonclogging design to permit the CIP supply line to be used as a re-vent line as part of the tank overflow protection system.

**Figure 17:** Diagram showing different cleaning devices for tanks, Sieberling (1997).
Fixed-ball sprays are available with a variety of characteristics in terms of flow rate, discharge pressure, and pattern of coverage. Experience has indicated that cylindrical and rectangular tanks can be adequately cleaned if sprayed at 0.2 to 0.3 gal/min/ft² of internal surface, with patterns designed to spray the upper one third of the tank. If considerable appurtenances exist in the tank, such as heating or cooling coils and complex agitators, some special patterns may be required to cover these surfaces with resultant increases in the total flow rate required.

10.8.3 Spray Cleaning of the Pans

The pans can also be cleaned using the fixed-ball sprays, but may require to be done in a separate cleaning station to avoid traffic congestion.

10.9 Maintenance

It should be noted that flour dust is detrimental to moving parts since it absorbs the lubricant and chokes oil ducts, with resulting dry running conditions and consequent danger of seizure (Ministry of Labour (1962). For this reason there is extensive use of guards to protect certain types of machinery. The more intricate the machinery the more important the guard, and the greater the degree of maintenance required to ensure that the guard performs its duty. Therefore an effective maintenance regime would not only consider the machinery but also the guards, and would be in two parts:
- thorough examination of the machine and its protective devices at regular intervals
- a periodic check under service conditions to see that faults are not developing.

There are no rules to say how long the 'regular intervals' should be. It will normally be left to an experienced engineer with knowledge of the plant.
10.10 Potential hazards and operational issues associated with baking

Although baking cakes is not a hazardous process in the conventional sense there are a number of safety and operational issues that can be picked up in the Hazop. There are five main categories of hazards associated with foods. These are described below (Potter and Hotchkiss, 1995):

1. Biological Hazards – these include bacterial, fungal, viral, and parasitic organisms and/or their toxins. These lead to food borne diseases from which most recover, but some die every year. Care needs to be taken in the handling, storage and preparation foods to prevent this.

2. Nutrition-Related Diseases – there is a relationship between health and diet. It has been proven that some diets increase the risk of heart disease and cancer, whereas others reduce it. Obesity is also a problem for people who overeat. Governments and health organisations promote changes in diet that contribute to better health.

3. Trace Chemicals – these can be naturally occurring, indirectly added, and directly added. They can occur at high levels which cause acute food poisoning, or at lower levels which may represent chronic or long term risks.

4. Direct Food Additives – intentional addition of chemicals such as preservatives to maintain shelf-life or improve taste. These need to be thoroughly tested before use.

5. Physical Hazards – foods may contain stones, glass fragments or bits of metal. These may be part of foods from their natural environment or come loose from processing machinery. For this reason many processing operations have electronic metal detectors.

Quality is very important when dealing with food and there are a number of factors that determine quality (Potter and Hotchkiss, 1995). The three main ones are described below:

- appearance: size, shape, colour, consistency, wholeness and pattern are all important
- texture: indication of freshness (also consistency important here)
- flavour: taste and odour, associated with colour and texture (subjective)

In addition to these there are other factors such as nutritional quality, sanitary quality and keeping quality.
Operational problems can occur at each stage of the baking process: during charging, mixing, separating, and heating. Some of them are described below.

Problems with not charging the right amounts of ingredients:
- batters not being formed correctly
- incorrect texture in the final product
- defects in crust appearance
- coarse or irregular grain in the final product.

Problems with undermixing or overmixing:
- defects in batter texture
- defects in product texture
- coarse or irregular grain in the final product.

Problems with separating (dough dividing):
- defects in batter lead to wrong size or shape of dough pieces

There are also problems associated with the oven:
- overbaking leading to tough texture in final product
- bursting of crust at high temperature
- pale crust colour at too low a temperature
- coarse grain caused by too cold an oven
- wet streaks caused by underbaking.
10.11 Application of the Pipeless Plant Hazop Procedure to the Bakery

Using the information available on this plant about the ingredients, the processes and stations the safety aspects can be examined. The Hazop procedure described in Chapter 4.2 is applied to the baking process, (but without a proper review team). The guide words and deviations/parameters chosen to be used are shown below. A simple spreadsheet program is developed to record the minutes and guide the review, prompting the guide words etc.

Guide Words: No, More, Less, As well as, Part of, Reverse, Other than, Early, Late, Before, After, Quickly, Slowly

Deviations/Parameters:
Standard Set: Flow, Temperature, Pressure, Level, Inspect, Maintenance, and Services
Instruction Set: Connect, Disconnect, Mix, React, Cut, Heat, and Clean

![Figure 18: Screenshot of the Hazop Table in Excel](image.png)
The Hazop is carried out station by station. Only the ingredients are different, therefore the charging stations might be different, but any actions applied to the stations for one of the recipes should apply to all the recipes. A table showing the results of the Hazop has been produced. It is a simple excel word sheet that prompts for the guide words and deviations. An additional database of causes can also be added, to aid the users in detecting potential hazards. The minutes in this particular case can be found in Appendix 1.

10.12 Application of the modified HAZAPS Methodology to the Bakery

The detailed results of using this support tool for the case study are in Appendix 2. The critical subsystems for the charging, mixing and heating stations are examined. The other stations such as dough dividers and packaging machines are specialist equipment, and would be purchased ready to use. The results using the methodology show that the very nature of pipeless plants makes them easy to control as only one control system is usually critical at a station. This makes the control simple and easy to implement.

10.13 Key Findings from the Pipeless Plant Hazop and modified HAZAPS

The key findings of the pipeless plant Hazop are:

1. The importance of verification of connections and disconnections made at each station, including interlocks to prevent hazardous situations developing.

2. The problems with stations carrying out multiple tasks, e.g. having one charging station for charging all the ingredients can lead to problems: time taken at station, charging the wrong ingredients to the wrong vessel, charging incorrect amounts (overcharging) etc.

3. The importance of alarms to notify the operator of conditions developing, and continuous updating on the status/progress of the batches.

The key findings from applying the modified HAZAPS methodology are:
1. The control of the stations is less problematic if their control systems are less complicated (and the control logic has a smaller number of steps) e.g. it is inherently safer to monitor and direct one control valve than three for the charging station.

2. There is usually only one critical control system at each station such as level for the charging station and temperature for the heating station. This is beneficial from the control point of view as each system can be considered in isolation.

3. The Hazop analysis of control actions enables the review team to identify critical control equipment such as sensors, actuators etc. and indicate a need for strict inspection / maintenance regimes, or redundancy.

The majority of the problems with the original design were found to be in the set-up of the charging station. The multiple tasks that were carried out there made its operation and its control difficult. Therefore from an operational and control point of view it was better to split the charging station up into solids charging (dry ingredients) and liquid charging (milk, water etc.)

10.14 Modifications to the Original Design

10.14.1 Dry Charging Station

![Dry Charging Station P&ID](image)

Figure 19: P&ID showing a Dry Charging Station
Process Steps:

1. An empty, clean vessel receives the recipe order.

2. The vessel travels to the Dry Charging Station (dry ingredients must be charged first to prevent lumps forming in the dough).

3. The required ingredients, amounts shown in the ingredients list, are charged to the vessel.

4. When the charging is complete, the vessel then leaves the station, travelling to the Liquid Charging Station(s) depending on whether water, eggs, milk or other liquid ingredients are required are required.

10.14.2 Liquid Charging Station

![Diagram of the Liquid Charging Station]

Figure 20: P&ID showing a Liquid Charging Station

Process Steps:

1. The vessel arrives at the Liquid Charging Station.

2. The required ingredients, amounts shown in the ingredients list, are charged to the vessel.

3. When the charging is complete, the vessel leaves the station, travelling to the Mixing Station.
The remaining stations required minor changes. The Dough Dividing Station should be purchased satisfying all necessary safety requirements, as should the Oven.

10.15 Results of the Discrete Event Simulation Using the Arena Software

Using the information from the two studies on process and computer control safety, a plant layout and schedule is proposed. After examination and from experience of the previous case study, a herringbone structure is to be used for the main track, with an external loop to remove the vessels from the plant at the Dough Dividing Station. The Vessel Cleaning Station will be situated in the loop, where the vessels will be cleaned and inspected before being reintroduced to the plant.

The results of building the simulation model and implementing a schedule are shown in Appendix 3. A screenshot of the model is shown below:
10.16 Key Findings from the Simulation of the Bakery

The key findings and benefits of carrying out the simulation are:

1. The herringbone structure appears to function particularly well for the charging stage of this pipeless plant, and could well be favourable to most pipeless plants.

2. The layout of the stations also works well, the vessels all move from left to right in the plant. There is only movement in both directions when entering/exiting stations, therefore the central track could be uni-directional.

3. The vessels are removed from the plant and return to their starting position by way of the external loop.

4. There is only one station for Cleaning, Dough Dividing, Heating, and Packaging. These are potential bottlenecks, and it may be required to have two to maintain production (especially the Cleaning Station for the vessels).

5. The major problem of the layout is that a breakdown on the central track would halt all production until the vessel could be removed, since the vessels follow the same route.

The case study shows an ideal situation with unlimited space, and an unlimited number of vessels etc. However in real life there would be limits, and the number of stations, vessels etc. may well be smaller. It may be a possibility to incorporate somewhere within the proposed plant layout the actual size of the plant, and take into account the cost of the vessels etc. Using this information would give a more realistic simulation model, however in the case study there are no such limits.
Section 7: Conclusions and Further Work
11. Conclusions

11.1 Summary

The usefulness of the basic concept of pipeless plants in multi-product batch processing has been described, and there are already production plants in operation demonstrating that they are effective. The main advantage pipeless plants have over conventional batch plants is in terms of multi-product flexibility, in addition to savings in terms of cleaning time and costs due to product loss and labour. However, pipeless plants also introduce additional safety issues that require careful consideration due to this flexibility. The safety aspects of this type of plant had not been examined in any great detail in the past, which is the motivation for the research carried out. What has become apparent during this investigation is, that there are not only the problems that exist with all new batch processes, but also problems due to the manner in which pipeless plants are different from fixed batch plants due to the mobile reactors.

This report has outlined three main areas for study in the safe design of computer controlled pipeless batch plants. These three areas can be categorised as follows:

- process plant safety: hazard identification and analysis of batch processes
- computer control safety: hazard identification and analysis of control systems
- schedule safety: examination of schedules and layouts using discrete event simulation.

All of these areas influence each other in some way, and therefore have to be considered simultaneously.

11.2 Contribution and Limitations

11.2.1 Process Safety

It is a batch process that is carried out. The number of methods of examination of
batch process safety is not as extensive as with continuous processes. The most thorough technique for the examination of continuous processes is the Hazop procedure. However there is no formal procedure for the Hazop of batch processes; it is done in an improvised fashion for specific cases. It is difficult to break down a batch process into lines and nodes, the way a Hazop is carried out on a continuous process. However the way in which a pipeless plant operates with its dedicated functional stations leads to the development of a Batch Hazop methodology, which separates the process into smaller sections (individual operations) for analysis. An extension of this methodology has then been developed for use in the safe design of batch processes in pipeless plants. A simple spreadsheet has been produced to record the minutes of such a study. The outputs (actions) of the which can be used as inputs to the computer-control and scheduling safety sections.

As with all studies of this kind, it is only as good as the information available and the team which carries it out. The necessary requirements of such a team would be a chairperson, trained in the technique, and experts with knowledge of the plant. The experts may have the necessary information for the design but they would have to apply it differently. This should come from experience.

11.2.2 Computer Control Safety

The extensive use of computer control in automated pipeless plant computers can introduce hazards through hardware and software failures. There are a number of methods for checking the integrity of a computer control system, such as Chazop and Hazaps. Another methodology, which is an extension of Hazaps, introduces an alternative method of representing an event and the response of the control system called a Process Control Event Diagram (PCED). This representation can be understood by people from different disciplines, and can facilitate discussion using the same team as the Pipeless Plant Hazop, by introducing deviations in the same way as a Hazop to identify errors and hazards in the computer control system. The computer support tool includes a safety question library, based on experience from industrial incident reports. The technique has been shown to particularly suit the analysis of
control systems for individual stations in a pipeless plant.

The support tool is fairly easy to use and understand, and allows a review team to examine the control system. The framework does rely on the developer of the system to identify the top level hazards. This leads to the question as to who would initiate this analysis. A chemical engineer is most likely to be the developer of the system, whereas a control engineer is most likely to know how the control system would operate including the control logic and actions.

11.2.3 Schedule Safety

The plant layout and schedule need to be considered simultaneously. Moving vessels quite obviously present a problem. The most prominent danger would be a collision between two moving charged reactors, but there are other safety and operational issues such as mischarging, double-charging, vessels breaking down on tracks etc. The usefulness of visual Discrete Event Simulation (DES) has been successfully demonstrated for showing the interaction between the plant layout and schedule. A major contribution of the DES is that it enables the designer to generate safety-related rules for producing plant layout. The designer can then investigate the effects of these safety precautions on multi-product flexibility.

The plant layout is produced using the outputs from the process and computer control hazard identification procedures as influences. A schedule is then produced for the particular layout. DES is used to simulate the plant and schedule and allows us to better understand the plant operation and visually detect problems, such as bottlenecks. Different plant layouts and schedules can be explored using DES to find the optimum in terms of both safety and production. The Arena software used for DES offers a number of tools and facilities, from creating a picture on a screen to exporting information to other software applications such as spreadsheets. Training is required by anyone planning to use this software, and even then it can be time consuming to figure out how to carry out simple functions, although it becomes easier with experience.
11.3 Integrated Methodology

The research carried out in each of the three areas above should give the designer a number of similar safely designed processes, with a correctly operating computer control system, set in a plant layout and schedule that is both safe and high in productivity. This research should be applicable to any pipeless batch plant. Therefore the above procedures can be combined to develop of an integrated methodology for the safe design of computer controlled pipeless batch plants.

11.4 Future Work

11.4.1 Process Safety

As would be expected in any systematic safety study, the methodology is time-consuming. A record of the proceedings has been produced for the Bakery Case Study using a simple Excel spreadsheet. This could be extended further using database software such as Microsoft Access to not only generate minutes and action sheets, but also guide the review making it quicker and more complete. The training given to the chairperson of the review on batch processes should not be that different from the training for conventional Hazops. Since many engineers and other employees in the chemical industry already have some experience of Hazop the new methodology should not too difficult to understand and adopt. A preliminary process Hazop analysis could also be introduced as the first step to any kind of safety review. The outputs of this, especially the actions concerned with computer control, could be very useful in developing a strategy for the control system. This could be developed further, even automated. The outputs of a Hazop could be classified, such as checking or changing equipment, modifications to operating instructions, introduction of or verification of control system equipment or actions etc. Therefore every action that is classified as part of the control system could automatically be carried through to the computer control review.
11.4.2 Computer Control Safety

As described in the previous section the starting point of the computer control safety review, the Safety Requirements Specification could be linked to the outputs of a preliminary process Hazop analysis, possibly connected directly to the control actions. This would be a big help to either the control engineer (in charge of computer control) or the chemical engineer (designer). Either one of them could then produce the PCEDs and initiate the analysis. Another aid to any future development of the system could be to include any proposed changes in the reporting of the analysis. Currently only the actual changes to the control system are documented, considered changes that are decided to be unsuitable are not reported and therefore may still be introduced at a later date. The questions library although useful is very time consuming. There are a large number of questions, some of which may not be appropriate to pipeless plant control systems. This tool is helpful but needs to be constantly updated especially with questions specific to pipeless plants. Within a particular study the team could identify a problem which has not been thought of before, which then should be included as a question in future analyses.

11.4.3 Schedule Safety

The schedule for the Bakery Case Study has been produced manually for a specific plant layout. Further work is already being done to develop a schedule generating program (Huang and Chung, 1999). It takes into account constraints such as location and availability of resources, positions of vessels, and safety constraints. However it does not take into account the routing of vessels. The schedule may satisfy all the constraints it has been provided but that does not mean that it works correctly, or it may work but not be the best in terms of safety or productivity. A scheduling program would be very useful for generating schedules quickly for specific plant layouts. It would still be required to visually simulate the production to check if the schedule worked, to evaluate different schedules for the same plant layout or to explore different schedules for different plant layouts. The software employed although useful took time to get used to. In some ways it had too many features, and a simpler
program may have given the same results in a smaller amount of time. There are a
number of manufacturing simulation software programs available, and there may be
some that specialise in transporters (vehicles) and routing which would be more
suitable for pipeless plants.

11.4.4. Equipment

Other areas where further work is required for pipeless plant technology to become
more generally accepted is in terms of the mechanical design of equipment, especially
the connectors between the vessels and stations. This is an area that of concern for
engineers that there is the possibility that either the right connections are not made or
that vessels might leave the stations with some of the connections still existing. Also
this research has focused on track systems, and there is the scope for further
development for off track systems. Many of the same problems in terms of process,
and computer control safety apply to off track systems. However the scheduling and
plant layout problem become even more important with vehicles which could
potentially be anywhere in the plant.

11.4.5 Scope of Applicability

The basic concept of pipeless plants for charging and mixing operations has been
successfully demonstrated. So far this concept has been applied to non-reactive
processes; the plants currently in operation are mainly for blending. The extension of
this concept to other unit operations is required in order to expand the range of the
approach. The more widespread and flexible the approach is the more likely it is that
it will be adopted for future production plants. Currently the approach is new and
requires innovative engineers to guide, encourage, and develop the use of pipeless
plant technology. The research carried out here contributes to this, and hopefully,
promotes the use of pipeless plants as a practical alternative to using conventional
batch plants.
Section 8:

References
12. References


IMI Project Detailed Proposal February (1997). ‘BRITEST’
Internet location: http://www.britest.co.uk/Public/Documents/VerProp/VersPr03.asp

Internet location: http://www.inoueusa.com/inoue, Products4.htm

Japan Supplement to Chemical Engineer (1997). ‘Equipment Makers Showcase Technology’.
Internet location: http://www.che.com/ce-9705/html/05jp4.htm


Kamiya, T. and Fouhy, K. (1997). ‘Pipeless plants - Non-reactive processes are still the focus’, Chemical Engineering, ACHHEMA 97,
Internet location: http://www.che.com/achema/html/ad1p1s3.htm


Internet location:  http://www.exicom.org/cew/ Feature - Article from February 1998 issue of Chemical Engineering World A monthly trade publication from Exicom, India.htm


Little, A.D. (1995). 'A Guideline for HAZOP Studies on Systems which include a PES', Presentation to HAIG.


Internet location: http://www.manufacturing.net/AGVs provide manufacturing flexibility at Chesebrough-Pond.htm


Section 9:

Appendices
13. Appendices

Appendix 1: The Pipeless Plant Hazop results


<table>
<thead>
<tr>
<th>Stage</th>
<th>Guide Word</th>
<th>Deviation</th>
<th>Cause</th>
<th>Consequence</th>
<th>Symptoms/Protection</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Less</td>
<td>Clean</td>
<td>Vessel not cleaned properly after last production.</td>
<td>Possibility of contamination from previous product.</td>
<td>No previous product.</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Charing Station</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>No</td>
<td>Connect</td>
<td>Connections to feed hopper and liquid inlet lines not made.</td>
<td>Raw materials not charged and maybe lost to plant floor.</td>
<td>[1] Require confirmation of exactly which connections are made before any material is charged to the vessel.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Less</td>
<td>Connect</td>
<td>No all connections to feed hopper and liquid inlet lines made.</td>
<td>Raw materials not charged and maybe lost to plant floor.</td>
<td>Already covered in Action [1].</td>
<td></td>
</tr>
<tr>
<td></td>
<td>More</td>
<td>Connect</td>
<td>More connections to feed hopper and liquid inlet lines made than required.</td>
<td>Additional raw materials charged. Also when vessel leaves the station these connections may not be picked up and disconnected.</td>
<td>[2] Require confirmation of disconnections being made before vessel is allowed to move.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Late</td>
<td>Connect</td>
<td>Connections are made after material have started charging.</td>
<td>Loss of material to plant floor.</td>
<td>Already covered in Action [1].</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>No</td>
<td>Charge</td>
<td>Lines blocked, or pumps not working correctly.</td>
<td>Inappropriate mix of ingredients, leading to loss of product.</td>
<td>[3] Regular maintenance and inspection required on the inlet lines and</td>
<td></td>
</tr>
</tbody>
</table>
Charging Station - ingredients are charged via an Automatic Batching System.

<table>
<thead>
<tr>
<th>Stage</th>
<th>Guide Word</th>
<th>Deviation</th>
<th>Cause</th>
<th>Consequence</th>
<th>Symptoms/Protection</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Feed hopper malfunctioning.</td>
<td></td>
<td></td>
<td>feed hopper.</td>
</tr>
<tr>
<td>Less Charge</td>
<td></td>
<td>Lines</td>
<td>Malfunction of lines partially blocked, or pumps not working correctly. Feed hopper malfunctioning.</td>
<td>Inappropriate mix of ingredients, leading to loss of product.</td>
<td>Already covered in Action [3].</td>
<td></td>
</tr>
<tr>
<td>As well as</td>
<td></td>
<td>Additional</td>
<td>Additional materials charged due to error with automatic batching system.</td>
<td>Inappropriate mix of ingredients, leading to loss of product.</td>
<td>Covered partially by Action [1].</td>
<td>[5] Require check of feed hopper weight to compare with recipe. Ensures that the correct amounts of each ingredient have been added.</td>
</tr>
<tr>
<td>Other than</td>
<td></td>
<td>Charge</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Late Charge</td>
<td></td>
<td>Metering</td>
<td>Devices not functioning correctly.</td>
<td>Raw materials to plant floor. Inappropriate mix of</td>
<td>Covered in Action [6].</td>
<td></td>
</tr>
<tr>
<td>Stage</td>
<td>Guide Word</td>
<td>Deviation</td>
<td>Cause</td>
<td>Consequence</td>
<td>Symptoms/Protection</td>
<td>Action</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>-----------</td>
<td>-------</td>
<td>-------------</td>
<td>----------------------</td>
<td>--------</td>
</tr>
<tr>
<td>5</td>
<td>No</td>
<td>Flow</td>
<td>Lines blocked etc.</td>
<td>Inappropriate mix of ingredients, leading to loss of product.</td>
<td>Should be covered in the actions on the metering devices and feed hopper.</td>
<td></td>
</tr>
<tr>
<td>More</td>
<td>Temperatu re</td>
<td>Material heated up before or during charging.</td>
<td>Temperature of materials in vessel higher than wanted before the mixing stage.</td>
<td>[7] Consider chilling of the liquid ingredients such as milk and water before charging.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>More</td>
<td>Level</td>
<td>Level in vessel different to what it should be, due to error in charging.</td>
<td>Inappropriate mix of ingredients, leading to loss of product.</td>
<td>Should be covered in the actions on the metering devices and feed hopper.</td>
<td>[8] Consider using level in the vessel as an additional control to the metering devices and feed hopper.</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>No</td>
<td>Disconnect</td>
<td>Disconnections from feed hopper and liquid inlet lines not made, and vessel leaves the station.</td>
<td>Material lost to plant floor.</td>
<td>Covered in Action [2].</td>
<td></td>
</tr>
<tr>
<td>Early</td>
<td>Disconnect</td>
<td>Disconnections are made while material is being charging.</td>
<td>Loss of material to plant floor.</td>
<td>Covered in Action [6].</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Mixing Station - the vessel itself is used as the bowl for a Vertical Mixer.

<table>
<thead>
<tr>
<th>Stage</th>
<th>Guide Word</th>
<th>Deviation</th>
<th>Cause</th>
<th>Consequence</th>
<th>Symptoms/Protection</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>No</td>
<td>Connect</td>
<td>Connections to station not made.</td>
<td>No mixing takes place.</td>
<td>[9] Require confirmation that vessel has connected up to the mixing station, and that mixing is taking place (indication on the control panel).</td>
<td></td>
</tr>
<tr>
<td>Late</td>
<td>Connect</td>
<td>Connections are made late.</td>
<td>Less mixing time, therefore low quality of dough produced.</td>
<td>Already covered in Action [9].</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>No</td>
<td>Mix</td>
<td>Agitator not working. No power to the agitator.</td>
<td>Dough not produced.</td>
<td>[10] Alarm on the agitator to show agitator not working, power failure etc.</td>
<td></td>
</tr>
<tr>
<td>Less</td>
<td>Mix</td>
<td>Agitator not working correctly. Wrong amounts of each ingredient added (i.e. too much flour).</td>
<td>Inadequate mixing of ingredients, leading to low quality dough being produced.</td>
<td>Should be partially covered in the actions on charging.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Late</td>
<td>Mix</td>
<td>Agitator starts late.</td>
<td>Mixing is not done for an adequate amount of time.</td>
<td>[12] Interlock agitator start/stop to the connection/disconnection of the vessel to the station.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Slowly</td>
<td>Mix</td>
<td>Agitator is working at the wrong speed.</td>
<td>Inadequate mixing of ingredients,</td>
<td>[13] Ensure that the agitator</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Station | Mixing Station - the vessel itself is used as the bowl for a Vertical Mixer.
--- | ---
<table>
<thead>
<tr>
<th>Stage</th>
<th>Guide Word</th>
<th>Deviation</th>
<th>Cause</th>
<th>Consequence</th>
<th>Symptoms/Protection</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>More</td>
<td>Temperatur e</td>
<td>Intense shearing action generates heat in the dough.</td>
<td>Temperature can affect the dough and alter the texture and finish of the final product.</td>
<td>Covered in Action [7].</td>
<td>changes speed after the required amount of time. Either to change automatically, or make the speed of the agitator a required as input into the control panel.</td>
</tr>
</tbody>
</table>

5 | More | Temperatur e | Intense shearing action generates heat in the dough. | Temperature can affect the dough and alter the texture and finish of the final product. | Covered in Action [7]. | changes speed after the required amount of time. Either to change automatically, or make the speed of the agitator a required as input into the control panel. |

6 | No | Disconnect | Vessel not disconnected properly and leaves the station. | Damage to vessel and connectors. | [14] Require confirmation of disconnections being made before vessel is allowed to move. |

| 6 | No | Disconnect | Vessel not disconnected properly and leaves the station. | Damage to vessel and connectors. | [14] Require confirmation of disconnections being made before vessel is allowed to move. |

<p>| Early | Disconnect | Disconnection s are made while material is being mixing. | Inadequate mixing of ingredients, leading to low quality dough being produced. | [15] Need to ensure that the vessel remains at the mixing station for the right amount of time. | [15] Need to ensure that the vessel remains at the mixing station for the right amount of time. |</p>
<table>
<thead>
<tr>
<th>Stage</th>
<th>Guide Word</th>
<th>Deviation</th>
<th>Cause</th>
<th>Consequence</th>
<th>Symptoms/Protection</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>No</td>
<td>Connect</td>
<td>Connections to station not made.</td>
<td>Dough not delivered to the dough divider, and therefore not cut to the requisite weight.</td>
<td>[16] Require confirmation that vessel has connected up to the dough dividing station, and that operation is taking place (indication on the control panel).</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>No</td>
<td>Cut</td>
<td>No power to the dough divider.</td>
<td>Dough of requisite weight not produced.</td>
<td>[17] Alarm on the dough divider to show it not working, power failure etc.</td>
<td></td>
</tr>
<tr>
<td>More</td>
<td>Cut</td>
<td></td>
<td>Dough divider not working correctly.</td>
<td>Dough of requisite weight not produced.</td>
<td>[18] Need to ensure that the correct weight of dough is produced, e.g. by weighing a sample of the cut pieces.</td>
<td></td>
</tr>
<tr>
<td>Less</td>
<td>Cut</td>
<td></td>
<td>Dough divider not working correctly. Wrong amounts of each ingredient added (i.e. too much flour).</td>
<td>Dough of requisite weight not produced.</td>
<td>Should be partially covered in the actions on charging.</td>
<td></td>
</tr>
<tr>
<td>Late</td>
<td>Cut</td>
<td></td>
<td>Dough divider starts late.</td>
<td>Dough of requisite weight not produced.</td>
<td>[19] Regular maintenance of dough divider (knife etc.) required.</td>
<td></td>
</tr>
</tbody>
</table>

Dough Dividing Station - dough is cut into lumps of the requisite weight.
### Dough Dividing Station - dough is cut into lumps of the requisite weight.

<table>
<thead>
<tr>
<th>Stage</th>
<th>Guide Word</th>
<th>Deviation</th>
<th>Cause</th>
<th>Consequence</th>
<th>Symptoms/Protection</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>More</td>
<td>Flow</td>
<td>Conveyor between vessel and station set at too high a speed.</td>
<td>Transfer of dough to the dividing station is too quick.</td>
<td>[21] Conveyor speed to be set to the throughput of the dough divider.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Only part of the dough is transferred to the dough divider.</td>
<td>Product loss.</td>
<td>[22] Check vessel weight after transfer of dough to the dough divider, before it is released to go to the cleaning station.</td>
<td></td>
</tr>
<tr>
<td>Other than</td>
<td>Flow</td>
<td>Dough is not transferred from the dough dividing station to the pan vessel.</td>
<td>Product loss.</td>
<td>[23] Interlock dough divider start/stop to the connection/disc connection of both of the vessels to the station.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Part of</td>
<td>Flow</td>
<td>Only part of the dough is transferred to the pan vessel.</td>
<td>Product loss.</td>
<td>[24] Check vessel weight after transfer of dough from the dough divider.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>No</td>
<td>Disconnect</td>
<td>Vessel not disconnected properly and leaves the station.</td>
<td>Damage to vessel and connectors.</td>
<td>[25] Require confirmation of disconnections being made before vessel is allowed to move.</td>
<td></td>
</tr>
</tbody>
</table>
Dough Dividing Station - dough is cut into lumps of the requisite weight.

<table>
<thead>
<tr>
<th>Stage</th>
<th>Guide Word</th>
<th>Deviation</th>
<th>Cause</th>
<th>Consequence</th>
<th>Symptoms/ Protection</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Early</td>
<td>Disconnect</td>
<td>Disconnections are made while material is being transferred to the pan vessel.</td>
<td>Product loss to floor.</td>
<td>Already covered in Action [23].</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stage</td>
<td>Guide Word</td>
<td>Deviation</td>
<td>Cause</td>
<td>Consequence</td>
<td>Symptoms/ Protection</td>
<td>Action</td>
</tr>
<tr>
<td>-------</td>
<td>------------</td>
<td>-----------</td>
<td>-------</td>
<td>-------------</td>
<td>----------------------</td>
<td>--------</td>
</tr>
<tr>
<td>3</td>
<td>No</td>
<td>Connect</td>
<td>Connections to station not made.</td>
<td>No heating takes place.</td>
<td></td>
<td>[26] Require confirmation that vessel has connected up to the heating station, and that heating is taking place (indication on the control panel).</td>
</tr>
<tr>
<td></td>
<td>Late</td>
<td>Connect</td>
<td>Connections to station made late.</td>
<td>Heating process begins late.</td>
<td>Heating time set by travel time through oven, therefore does not matter when heating starts.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>More</td>
<td>Heat</td>
<td>Temperature of oven too high.</td>
<td>Product loss due to burning.</td>
<td></td>
<td>[27] Require temperature control on oven. Setting to be entered for each product.</td>
</tr>
<tr>
<td>5</td>
<td>No</td>
<td>Flow</td>
<td>Conveyor</td>
<td>Product loss</td>
<td></td>
<td>[29] Alarm on</td>
</tr>
<tr>
<td>Stage</td>
<td>Guide Word</td>
<td>Deviation</td>
<td>Cause</td>
<td>Consequence</td>
<td>Symptoms/ Protection</td>
<td>Action</td>
</tr>
<tr>
<td>-------------</td>
<td>------------</td>
<td>-----------</td>
<td>---------------------------------------------------</td>
<td>--------------------------------------------------</td>
<td>-----------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>through oven broken.</td>
<td>due to burning.</td>
<td></td>
<td>oven conveyor to indicate breakdown.</td>
</tr>
<tr>
<td>More</td>
<td>Flow</td>
<td></td>
<td>Conveyor between vessel and station set at too high a speed.</td>
<td>Transfer of dough to the heating station is too quick.</td>
<td></td>
<td>{30} Conveyor speed to be set to the throughput of the dough divider.</td>
</tr>
<tr>
<td>Part of</td>
<td>Flow</td>
<td></td>
<td>Only part of the dough is transferred to the oven.</td>
<td>Product loss.</td>
<td></td>
<td>{31} Check vessel weight after transfer of pans to the oven.</td>
</tr>
<tr>
<td>Other than</td>
<td>Flow</td>
<td></td>
<td>The pans are not transferred from the heating station back to the pan vessel.</td>
<td>Product loss.</td>
<td></td>
<td>{32} Interlock oven conveyor start/stop to the connection/disc connection of the pan vessel to the station.</td>
</tr>
<tr>
<td>Other than</td>
<td>Temperature</td>
<td></td>
<td>Temperature of oven too high or too low.</td>
<td>Product loss.</td>
<td>Covered in Action</td>
<td>[27].</td>
</tr>
<tr>
<td>6</td>
<td>No</td>
<td>Disconnect</td>
<td>Vessel not disconnected properly and leaves the station.</td>
<td>Damage to vessel and connectors, conveyors etc.</td>
<td></td>
<td>{33} Require confirmation of disconnections being made before vessel is allowed to move.</td>
</tr>
<tr>
<td>Early</td>
<td>Disconnect</td>
<td></td>
<td>Disconnections are made while material is being transferred.</td>
<td>Product loss to floor.</td>
<td></td>
<td>Covered in Action [32].</td>
</tr>
<tr>
<td>Stage</td>
<td>Guide Word</td>
<td>Deviation</td>
<td>Cause</td>
<td>Consequence</td>
<td>Symptoms/Action</td>
<td>Action</td>
</tr>
<tr>
<td>-------</td>
<td>------------</td>
<td>-----------</td>
<td>-------</td>
<td>-------------</td>
<td>-----------------</td>
<td>--------</td>
</tr>
<tr>
<td>3</td>
<td>No</td>
<td>Connect</td>
<td>Connections to station not made.</td>
<td>Product is not discharged.</td>
<td>[34] Require confirmation that vessel has connected up to the discharging station, and that discharging is taking place (indication on the control panel).</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>[35] Require interlock between conveyor and connections/disc connections.</td>
<td></td>
</tr>
<tr>
<td>Late</td>
<td>Connect</td>
<td>Connections to station made late.</td>
<td>Pans left on vehicle.</td>
<td></td>
<td>[36] Ensure that pans are empty before being returned to the vehicle.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>No</td>
<td>Discharge</td>
<td>Vacuum depanners not functioning properly.</td>
<td>Product remains in the pans.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>No</td>
<td>Flow</td>
<td>Conveyor through vacuum depanners broken.</td>
<td>Product remains in the pans.</td>
<td>[37] Alarm on depanner conveyor to indicate breakdown.</td>
<td></td>
</tr>
<tr>
<td>More</td>
<td>Flow</td>
<td></td>
<td>Conveyor between vehicle and station set at too high a speed.</td>
<td>Transfer of product to the discharging station is too quick.</td>
<td>[38] Conveyor speed to be set to the throughput of the vacuum depanner.</td>
<td></td>
</tr>
<tr>
<td>Other than Flow</td>
<td>The pans are not transferred from the discharging station back to the pan vessel.</td>
<td>Require pans to be cooled and returned to the dough dividing station.</td>
<td></td>
<td>[39] Interlock depanner conveyor start/stop to the connection/division of the pan vessel to the station.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Discharging Station

<table>
<thead>
<tr>
<th>Stage</th>
<th>Guide Word</th>
<th>Deviation</th>
<th>Cause</th>
<th>Consequence</th>
<th>Symptoms/Protection</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>More</td>
<td>Temperature</td>
<td>Temperature of pans high when returned to the dough dividing station.</td>
<td>Dough pieces will burn and stick when transferred.</td>
<td></td>
<td>[40] Require cooling of pans to 30°C before being used again.</td>
<td></td>
</tr>
<tr>
<td>More</td>
<td>Temperature</td>
<td>Temperature of product high when discharged to the packaging area.</td>
<td>Product requires cooling.</td>
<td></td>
<td>[41] Require cooling of product before being wrapped.</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>No</td>
<td>Disconnect</td>
<td>Vessel not disconnected properly and leaves the station.</td>
<td>Damage to vessel and connectors, conveyors etc.</td>
<td>[42] Require confirmation of disconnections being made before vessel is allowed to move.</td>
<td></td>
</tr>
<tr>
<td>Early</td>
<td>Disconnect</td>
<td>Disconnections are made while pans are being transferred.</td>
<td>Pans dropped on floor.</td>
<td></td>
<td>Action [42].</td>
<td></td>
</tr>
</tbody>
</table>

### Cleaning Station

<table>
<thead>
<tr>
<th>Stage</th>
<th>Guide Word</th>
<th>Deviation</th>
<th>Cause</th>
<th>Consequence</th>
<th>Symptoms/Protection</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>No</td>
<td>Connect</td>
<td>Connections to station not made.</td>
<td>No cleaning takes place.</td>
<td>[43] Require confirmation that vessel has connected up to the cleaning station, and that cleaning is taking place (indication on the control panel). [44] Interlock cleaning start/stop with</td>
<td></td>
</tr>
<tr>
<td>Stage</td>
<td>Guide Word</td>
<td>Deviation</td>
<td>Cause</td>
<td>Consequence</td>
<td>Symptoms/Protection</td>
<td>Action</td>
</tr>
<tr>
<td>-------</td>
<td>------------</td>
<td>-----------</td>
<td>-------</td>
<td>-------------</td>
<td>---------------------</td>
<td>--------</td>
</tr>
<tr>
<td>4</td>
<td>Less</td>
<td>Clean</td>
<td>Vessel insufficiently cleaned.</td>
<td>Product contamination</td>
<td>[45] Require check on vessel cleanliness before being used again. If necessary to go through two cleaning cycles.</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>No</td>
<td>Flow</td>
<td>Pans are not cleaned after each use.</td>
<td>Very low possibility of product contamination</td>
<td>[46] Pans to be cleaned regularly, but not required after every batch.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>More</td>
<td>Temperature</td>
<td>Pans are still hot after exiting the oven.</td>
<td>If there is hot oil present and the pans are sprayed with cold water, then there is a problem with slopover.</td>
<td>[47] Ensure that the pans are cooled down before going to the Cleaning Station.</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>No</td>
<td>Disconnect</td>
<td>Vessel not disconnected properly and leaves the station.</td>
<td>Damage to vessel and connectors, spray balls etc.</td>
<td>[48] Require confirmation of disconnections being made before vessel is allowed to move.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Early</td>
<td>Disconnect</td>
<td>Disconnect ions are made during cleaning.</td>
<td>Insufficient cleaning therefore product contamination</td>
<td>Covered in Actions [44] and [47].</td>
<td></td>
</tr>
</tbody>
</table>
Appendix 2: The HAZAPS Methodology and Computer Support Tool
Results from the HAZAPS computer support tool

Using the proposed framework by Yang & Chung (1998) for identifying hazards related to computer controlled processes, and utilising the computer support tool developed for this framework, the computer control of different stations in the bakery case study was examined. Control actions were developed for the safety requirements highlighted in the pipeless plant Hazop. From these control actions Process Control Event Diagrams (PCEDs) were produced, which were examined to ensure that the actions performed the function they were supposed to, and did not result in a hazardous situation themselves. The Hazop is not in great detail as a team is still required to examine the design in depth. What is delivered is more an example of what is possible.

Results of the HAZAPS: Charging the Reactor

System Description: Computer controlled batch reactor (mobile vessel)

An automated charging system is to be used to feed the dry and liquid ingredients. The computer monitors the reactor level via the level control, and ensures that the correct amount of each ingredient is charged. This is achieved by the computer controlling three control valves: the milk inlet valve, the water inlet valve, and the hopper feed valve. There is an alarm to indicate a low/high level in the reactor, to signal that operator intervention is required, as well as the automatic response from the control system. There is also temperature indication on the reactor, as some of the ingredients are temperature sensitive. This feeds back to control cooling on the liquid holdup tanks.

First of all, a P&ID of the process can be viewed using the Graphic Viewer item in the TOOLS menu. The graphic file is PiplCh1.bmp.
Safety Requirements

The safety requirements of the process are:
1. To prevent the overcharging of the vessel.
2. To ensure that the right amounts of raw materials are charged.
3. To keep the temperature in the reactor in a permitted range.

Safety Requirement 1

It is necessary to prevent overcharging of the vessel. Although the raw materials are not hazardous, discharging them into the plant would cause problems. As well as having to clean the plant there would also be cost implications due to delays in production and product loss.

Control Logic 1:

When a high level is registered by the LIC in the reactor, an alarm sounds and all inlets are closed until the operator responds to the alarm. The operator's response being dependent on the cause of the overcharging.
The control logic is inputted into the analysis software as shown below:

![Control Logic Diagram](image1)

From the control logic the PCED is produced as shown below:

![Process Controlled Event Diagram](image2)
PCED-No.1: Control actions to prevent overcharging

State Transitions under this Control Logic

<table>
<thead>
<tr>
<th>State</th>
<th>Vessel Level</th>
<th>Alarm</th>
<th>Water IN (WATV)</th>
<th>Milk IN (MILKV)</th>
<th>Hopper IN (HOPPERV)</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1</td>
<td>normal</td>
<td>silent</td>
<td>high</td>
<td>high</td>
<td>high</td>
</tr>
<tr>
<td>S2</td>
<td>high</td>
<td>silent</td>
<td>high</td>
<td>high</td>
<td>high</td>
</tr>
<tr>
<td>S3</td>
<td>high</td>
<td>sound</td>
<td>high</td>
<td>high</td>
<td>high</td>
</tr>
<tr>
<td>S4</td>
<td>high</td>
<td>sound</td>
<td>closed</td>
<td>closed</td>
<td>closed</td>
</tr>
</tbody>
</table>

The final (and all intermediate) states are safe therefore the control logic is safe. The requirement examined in this section is a safety constraint, and it deals with an abnormal condition. The control algorithm for operation under normal conditions should also be examined and this is done in Requirement 2.

Safety Requirement 2

This is actually more of an operability requirement than a safety one. If the right blend of raw materials is not charged it results in product loss and therefore cost.

Control Logic 2:

When a low level is registered by the LIC in the reactor, an alarm sounds to alert the operator to request information form the computer. The operator uses the information to input a set-point for the ingredients. This is then relayed to the control valves for all the feeds to the vessel.

This control logic to ensure that the correct blend of ingredients is charged is inputted into the software as shown below:
From this control logic the PCED is produced as shown below:

PCED-No.2: Control actions to charge the correct amount of raw materials
State Transitions under this Control Logic

<table>
<thead>
<tr>
<th>State</th>
<th>Vessel Level</th>
<th>Alarm</th>
<th>Operator</th>
<th>Water IN (WATV)</th>
<th>Milk IN (MILKV)</th>
<th>Hopper IN (HOPPERV)</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1</td>
<td>normal</td>
<td>silent</td>
<td>inactive</td>
<td>high</td>
<td>high</td>
<td>high</td>
</tr>
<tr>
<td>N1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S2</td>
<td>low/high</td>
<td>silent</td>
<td>inactive</td>
<td>low/high</td>
<td>low/high</td>
<td>low/high</td>
</tr>
<tr>
<td>N2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S3</td>
<td>low/high</td>
<td>sound</td>
<td>inactive</td>
<td>low/high</td>
<td>low/high</td>
<td>low/high</td>
</tr>
<tr>
<td>N3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S4</td>
<td>high</td>
<td>sound</td>
<td>active</td>
<td>low/high</td>
<td>low/high</td>
<td>low/high</td>
</tr>
<tr>
<td>N4, N5, N6, N7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S5</td>
<td>high</td>
<td>sound</td>
<td>active</td>
<td>regulated</td>
<td>regulated</td>
<td>regulated</td>
</tr>
</tbody>
</table>

The final (and all intermediate) states are safe therefore the control logic is safe.

Safety Requirement 3

Certain raw materials (ingredients) degrade unless maintained within a particular temperature range. The liquid ingredients are pre-chilled before being charged into the vessel, and therefore there should be feedback to the cooling systems on the liquid hold-up tanks to maintain the temperature of the vessel contents.

Control Logic 3:
When a high temperature is registered by the TIC in the reactor the alarm sounds. The inlet valves are closed, and cooling is turned on fully on the liquid hold-up tanks.

The control logic to maintain the temperature of the vessel is shown below:
From this control logic the PCED is produced as shown below:
PCED-No.3: Control actions to prevent the temperature of the reactor going outside the permitted range

State Transitions under this Control Logic

<table>
<thead>
<tr>
<th>State</th>
<th>Vessel Temp</th>
<th>Alarm</th>
<th>Water IN (WATV)</th>
<th>Milk IN (MILKV)</th>
<th>WHold-up Cooling (COOW)</th>
<th>MHold-up Cooling (COOW)</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1</td>
<td>normal</td>
<td>silent</td>
<td>high</td>
<td>high</td>
<td>low</td>
<td>low</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>N1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S2</td>
<td>high</td>
<td>silent</td>
<td>high</td>
<td>high</td>
<td>low</td>
<td>low</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>N2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S3</td>
<td>high</td>
<td>sound</td>
<td>high</td>
<td>high</td>
<td>low</td>
<td>low</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>N3, N4, N5, N6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S4</td>
<td>high</td>
<td>sound</td>
<td>closed</td>
<td>closed</td>
<td>high</td>
<td>high</td>
</tr>
</tbody>
</table>

The final (and all intermediate) states are safe therefore the control logic is safe.
Output of HAZOP analysis on the control actions, produced by the HAZAPS computer support tool

Requirements 1 and 2 essentially deal with the same control system: the level control. The Hazop is carried out on Requirement 2, and as Requirement 1 is an extension of Requirement 2 all the actions should apply to both.

HAZOP Analysis of Control Actions for Requirements 1 and 2

The results of the analysis are generated as a text file, which is then imported into word. They are shown below without any formatting.

=====HAZOP Item: N1=======
GUIDE WORD: NO
DEVIATION: No signal from liquid level sensor.
CAUSES: Liquid level sensor is out of order.
CONSEQUENCES: Overflow of reactor is not identified, and may not be prevented.
ACTIONS: Install duplicate sensor, require rigorous maintenance schedule.

GUIDE WORD: MORE
DEVIATION: Reactor liquid level outside normal limit.
CAUSES: Liquid level sensor has not been calibrated for a long time.
CONSEQUENCES: Batch is out of spec.
ACTIONS: Double check reactor level, with input of raw materials.
Recalibrate the reactor level sensor regularly.

GUIDE WORD: LESS
DEVIATION: Setpoint is incorrect.
CAUSES: The operator made an error inputting the setpoint.
CONSEQUENCES: The input of raw materials does not tally with the level sensor.
ACTIONS: In the event of the two figures not being the same operator to recheck setpoint.
HAZOP Item: N2
GUIDE WORD: NO
DEVIATION: No signal from HID.
CAUSES: Communication between alarm and computer is broken.
CONSEQUENCES: Alarm does not sound, and potential for overflow. Has to occur along with several other conditions such as water inlet, milk inlet, and hopper feed valves remaining open.
ACTIONS:

HAZOP Item: N3
GUIDE WORD: NO
DEVIATION: No signal to the water inlet valve.
CAUSES: The communication between the computer and water inlet valve is broken.
CONSEQUENCES: The water inlet valve is left uncontrollable.
ACTIONS: Operator to monitor the position of the water inlet valve, especially in the event of a high level alarm. Manual control provided.

HAZOP Item: N4
GUIDE WORD: NO
DEVIATION: No signal to the milk inlet valve.
CAUSES: The communication between the computer and milk inlet valve is broken.
CONSEQUENCES: Milk inlet valve is left uncontrollable.
ACTIONS: Operator to monitor the position of the milk inlet valve, especially in the event of a high level alarm. Manual control of valve provided.

HAZOP Item: N5
GUIDE WORD: NO
DEVIATION: No signal to the hopper feed valve.
CAUSES: The communication between the computer and the hopper feed valve is broken.
CONSEQUENCES: Hopper feed valve left uncontrollable.
ACTIONS: Operator to monitor the position of the hopper feed valve, especially in the event of a high level alarm. Manual control provided.

HAZOP Analysis of Control Actions for Requirement 3

=====HAZOP Item: N1=====

GUIDE WORD: NO

DEVIATION: No signal from temperature sensor.
CAUSES: Temperature sensor is out of order.
CONSEQUENCES: Ingredients, especially milk, spoiled if temperature is too high.
ACTIONS: Duplicate sensor required.

GUIDE WORD: MORE

DEVIATION: Reactor temperature outside normal limit.
CAUSES: Sensor has not been calibrated for a long time.
CONSEQUENCES: Batch spoiled.
ACTIONS: Maintain and recalibrate temperature sensor at regular intervals.

=====HAZOP Item: N2=====

GUIDE WORD: NO

DEVIATION: No signal from HID.
CAUSES: Communication between alarm and computer is broken.
CONSEQUENCES: Spoilt batch not picked up, potentially sent to customer.
ACTIONS: Operator to monitor temperature during charging.

These results are an example of what is possible. Since the HAZOP is based on the knowledge of a group of experts it would be done more thoroughly than the one carried out here individually.
Safety Related Questions

The next step in the analysis is the Safety Related Questions. A library of questions based on analysis of incident reports is available. Safety questions are asked relevant to the identified safety critical events. The questions can be put into three categories: specification, implementation, and protection. For example the type of questions to be asked about the sensor of the level control system:

**Specification**
- What state is to be monitored?
- Why is this state to be monitored?
- When is this state to be monitored?
- How is this state to be monitored?

**Implementation**
- What sensor is to be used?
- How will it be installed?
- How will it be tested and maintained?

**Protection**
- What alarms and/or trips are associated with this task?
- Why are these alarms/trips required?
- What is the setting of the alarms/trips?

This is just a small sample of the type of questions to be asked about one sensor. This shows the thoroughness of the procedure. There are over 170 questions available, and therefore it would be time consuming to go through in this case study especially without the expert knowledge required. A screenshot of this section of the support tool is shown below:
<table>
<thead>
<tr>
<th>Task Description</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receive high signal from LIC in the reactor</td>
<td>Require level detection for the vessel, which will be able to deal with a mixture of liquid and solids.</td>
</tr>
</tbody>
</table>

Response

The level inside the vessel during charging.

Screenshot: Safety Related Questions for the level sensor in the vessel
Amended Design for the Charging Stations

It was decided to divide the charging station into separate stations for liquid and dry charging ingredients. It was further decided to split the liquid charging station into separate milk charging and water charging stations. By having dedicated stations charging independently many of the problems identified were dealt with, and the control is much simpler from an operational point of view. Also as the computer only has regulate the charging of one material (one control valve) at a time it is better from a safety point of view as well.

New P&ID for dry charging station:
Also the new P&ID for the liquid charging station:

Separated into separate stations like this makes the design much safer and easier to control, although the charging time will be increased (due to travelling between stations). The Mixing Station does not introduce many hazards therefore its design and control strategy is quite simple, and does not require any major changes as a result of the HAZAPS analysis.

The computer support tool is also used to implement the HAZAPS methodology on the Mixing Station and the Heating Station (oven). The Dough Dividing Station is a special machine that can only be repaired by the manufacturer, therefore it is not possible to examine properly. It could however be a bottleneck in the production and the best solution to any problem might be to have a redundant dough divider (cost permitting). The usefulness of the methodology and support tool has been demonstrated in its application to the charging station and, therefore its application to the Mixing and Heating Stations has been carried out in less detail. The results of which are shown below.
Results of the HAZAPS: Mixing Station

System Description: Mixing Station

Mixing of the dough generates heat into the dough mixture. The ingredients in the dough mixture are temperature sensitive, and the temperature in the vessel is an indicator of mixing performance and therefore should be monitored. An increase in temperature could be due to the mixing or even incorrect charging of ingredients. If the temperature in the vessel exceeds an acceptable level then there is also the possibility of spoiling the batch. Therefore if there is an increase in temperature the agitation should be stopped while the operator inspects the vessel and contents.

First of all, the P&ID of the Mixing Station is viewed in the Graphic Viewer item in the TOOLS menu. The graphic file is PiplMix1.bmp.
Safety Requirement

Really an operational requirement: to ensure correct mixing of the cake dough, using the temperature of the cake mixture as a symptom of a problem with mixing performance.

Control Logic:
If the TIC on the reactor registers a high temperature outside the acceptable limit, then an alarm should sound to warn the operator and the agitator should be stopped until the operator has inspected the vessel and contents.

The control logic is inputted into the analysis software as shown below:

The corresponding PCED produced by the software is shown below:
PCED-No.: Control actions to prevent overheating of vessel contents

State Transitions under this Control Logic

<table>
<thead>
<tr>
<th>State</th>
<th>Vessel Temp</th>
<th>Alarm</th>
<th>Agitator Motor</th>
<th>Operator (INSPECTION)</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1</td>
<td>normal</td>
<td>silent</td>
<td>on</td>
<td>inactive</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S2</td>
<td>high</td>
<td>silent</td>
<td>on</td>
<td>inactive</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S3</td>
<td>high</td>
<td>sound</td>
<td>on</td>
<td>inactive</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S4</td>
<td>high</td>
<td>sound</td>
<td>off</td>
<td>inactive</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S5</td>
<td>high</td>
<td>sound</td>
<td>off</td>
<td>active</td>
</tr>
</tbody>
</table>

The final (and all intermediate) states are safe therefore the control logic is safe.
Example Output of HAZOP Analysis of Control Actions

=====HAZOP Item: N1=====  
GUIDE WORD: NO  
DEVIATION: No signal from temperature sensor.  
CAUSES: Temperature sensor is out of order.  
CONSEQUENCES: Problem with mixing not identified, leads to product loss.  
ACTIONS: Regular maintenance and testing of temperature to guard against failure.

The Mixing Station does not introduce many hazards therefore its design and control strategy is quite simple, and does not require any major changes as a result of the HAZOPS analysis.
Results of the HAZAPS: Heating Station

System Description: Heating Station

The oven is preheated and then maintained at the required temperature while the dough travels along conveyors through the tray oven. The cooking time is therefore controlled by the speed of the conveyors. The temperature is monitored at points throughout the oven. A high temperature should trigger an alarm stopping the incoming conveyor, but continuing the operation of the outgoing conveyor, and requiring operator intervention.

First of all, the P&ID of the process is viewed in the Graphic Viewer item in the TOOLS menu. The graphic file is HeatSt1.bmp.
Safety Requirements:

1. To ensure that the dough pieces are cooked at the correct temperature.
2. To ensure that the dough pieces are cooked for the right length of time.

Safety Requirement 1

Higher temperature in certain parts of the oven may burn the external surface of the cakes and lead to unacceptable product quality and product loss. Therefore it is important to maintain the correct temperature throughout the oven.

Control Logic 1:
If the Temperature Control system receives a high temperature signal then the heating is to be switched off. The outlet conveyor transporting the baked cakes is run as normal, but the inlet conveyor is stopped until the operator has dealt with the problem and re-initiates it.

This can be inputted into the analysis software as shown below:
The corresponding PCED produced by the software is shown below:

PCED-No.: Control actions in response to high temperature detection in the oven

State Transitions under this Control Logic

<table>
<thead>
<tr>
<th>State</th>
<th>Oven Temp</th>
<th>Alarm</th>
<th>Heating</th>
<th>In Convey (INCONV)</th>
<th>Out Convey (OUTCONV)</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1</td>
<td>normal</td>
<td>silent</td>
<td>on</td>
<td>on</td>
<td>on</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>N1</td>
<td></td>
</tr>
<tr>
<td>S2</td>
<td>high</td>
<td>silent</td>
<td>on</td>
<td>on</td>
<td>on</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>N2</td>
<td></td>
</tr>
<tr>
<td>S3</td>
<td>high</td>
<td>sound</td>
<td>on</td>
<td>on</td>
<td>on</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>N3, N4, N5</td>
<td></td>
</tr>
<tr>
<td>S4</td>
<td>high</td>
<td>sound</td>
<td>off</td>
<td>off</td>
<td>on</td>
</tr>
</tbody>
</table>

The final (and all intermediate) states are safe therefore the control logic is safe.
Safety Requirement 2

The cooking time of the cakes is determined by the length of the conveyor through the oven and the speed at which the trays move along the conveyor. The main problem then would be a delay in the movement of the tray, such as the conveyor breaking down, leading to overcooking, and therefore product loss.

Control Logic 2:
The movement of the conveyor is to be monitored. If the conveyor stops an alarm sounds to alert the operator. The outlet conveyor transporting the baked cakes is run as normal, but the inlet conveyor is stopped until the operator has dealt with the problem and re-initiates it. The status of the output of the dough dividing station is also checked to ensure that the right size and number of pieces of dough are being cut and sent to the oven.

This control logic is inputted into the analysis software as shown below:
The corresponding PCED produced by the software is shown below:

PCED-No.: Control actions in response to conveyor breakdown in the oven

State Transitions under this Control Logic

<table>
<thead>
<tr>
<th>State</th>
<th>Oven Temp</th>
<th>Alarm</th>
<th>Heating</th>
<th>In Convey (INCONV)</th>
<th>Operator (CHECKSTAT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1</td>
<td>normal</td>
<td>silent</td>
<td>on</td>
<td>on</td>
<td>inactive</td>
</tr>
<tr>
<td>S2</td>
<td>high</td>
<td>silent</td>
<td>on</td>
<td>on</td>
<td>inactive</td>
</tr>
<tr>
<td>S3</td>
<td>high</td>
<td>sound</td>
<td>on</td>
<td>on</td>
<td>inactive</td>
</tr>
<tr>
<td>S4</td>
<td>high</td>
<td>sound</td>
<td>off</td>
<td>off</td>
<td>active</td>
</tr>
</tbody>
</table>

The final (and all intermediate) states are safe therefore the control logic is safe.

196
Example Output of HAZOP Analysis of Control Actions

======HAZOP Item: N2======
GUIDE WORD: NO
DEVIATION: Alarm does not sound even though the conveyor has stopped.
CAUSES: Alarm out of order, or no connection between sensor and alarm
CONSEQUENCES: Operator unaware of problem.
ACTIONS: Install second alarm, plus strict maintenance and testing schedule.

The Heating Station (oven) is a standard design, and should not produce any additional hazards with its use in a pipeless plant. Many safety constraints will be built into the design by the manufacturer, therefore the heating station (oven) design and control strategy is quite simple, and does not require any major changes as a result of the HAZAPS analysis.
Appendix 3: Discrete Event Simulation using the Arena Software
Results of the Simulation using the Arena software

The stations to be used in the manufacture are listed below. As well as individual charging stations for each of the dry cake mixtures, four liquid charging stations (two for water, and two for milk), two mixing stations and a cleaning station are to be used as fixed stations on the track network. The Dough Dividing Station, Heating Station (Oven), Packaging Station and Pan Cleaning Station are all stations on a conveyor network.

- Charging Cake Mix A
- Charging Cake Mix B
- Charging Cake Mix C
- Charging Cake Mix D
- Charging Water A
- Charging Water B
- Charging Milk A
- Charging Milk B
- Mixing Station A
- Mixing Station B
- Dough Dividing Station
- Heating Station (Oven)
- Packaging Station
- Vessel Cleaning Station
- Pan Cleaning Station

Each station has to be specified i.e. a name has to be given. If a name is not given it is flagged as an error when attempting to run the simulation. Other fields such as number, Intersection I.D., and Recipe I.D. are optional. A screenshot of the station entry is shown below:
It is the same for every other item in the simulation. Everything has to be specified, especially the name, other fields are optional, e.g. the entity creation (screenshot show below).
Similarly all Links and Intersections have to be specified:
A schedule is produced in Excel based on the herringbone structure. The first 8 batches have been scheduled, using all 8 vessels.

This is translated into Transporter and Sequence information:
Also the conveyor between the Dough Dividing Station and the Packaging Station:
Another feature of the simulation software is the ability to export and import data from spreadsheet software such as Excel. However, it has to be exported first to create a spreadsheet file. The relevant data can then be changed and imported back into the simulation. The way this is carried out does not allow a great deal of control over the format of the file, so it cannot produce a schedule like the one shown above. Instead, it produces a number of sheets each containing different information, such as batch initiation times, processing times, transporter initiation, and the sequences to be followed. The cells can be connected so that changing the schedule changes the vessel sequences and initiation times etc. It may also be possible to use a scheduling program such as the one being developed by Huang and Chung (2000) to output to Excel and then link this with the import/export from the Arena simulation software. Screenshot of Module Data Transfer Wizard shown below.
The complete plant simulated in Arena is shown below:

Vessel and Product Route
It was decided to initiate the vessels at the left side of the plant. The dry charging station is visited first, followed by the liquid charging station, then the mixing station. The vessel delivers the dough to the dough divider, after which it is released to return to the start via the external loop and the Vessel Cleaning Station. The dough is cut up into pieces at the dough divider and transferred to pans which are then transported on a conveyor through an oven to the packaging station. The pans are then cleaned and returned to the dough divider.

Intersections
There are a number of intersections where the vessels may collide. The layout and schedule are such that the vessels are moving towards the right of the plant (the conveyor section). Therefore they do not cross-over moving in opposite directions. The schedule as it is written does not have any vessels waiting on the track for a station to become free, therefore a queueing (priority) system is not required.
Vessel Removal
If there is a breakdown or any problem on the main track then all the vessels would have to be stopped to remove the broken down vessel. If the breakdown occurs in a station then only the vessels (batches) using that station would have to be stopped (or not initiated). The broken down vessel may be removed either directly or via the external loop.

Cleaning Stations
It was decided that two cleaning stations would be required, each dedicated to a particular task. The Vessel Cleaning Station is located on the external loop close to the vessel starting position for convenience. If a large number of vessels is used in the plant it may be required to have more than one of these. The Pan Cleaning Station is located after the Packaging Station (or near the Dough Dividing Station).

Number of Vessels
Since the charging and mixing operations do not take a great deal of time it appears that there may be quite a high production rate. The time taken from when the vessel is freed and then cleaned before being re-introduced is comparable. Therefore to maintain production vessels are required in the plant, waiting to be introduced and waiting to be cleaned.

Future Expansion
There may be a need to add (or remove) stations later on, due to different products being manufactured. The herringbone structure does allow for this as long as space is available. The dough divider, oven and packaging equipment may also need to be purchased with future expansion in mind.
The charging and mixing operations:
The conveyor from the Dough Dividing Station to the Packing Station:

The schedule worked for the layout but required a very large number of vessels. Since the first vessel is cleaned and ready for re-use at time 01:50 hours, and two batches can be initiated every 00:10 hours (and completed every 00:10 hours). Then a total of 24 vessels are required to maintain production, with 8 vessels moving around the charging and mixing stations at any time. The Dough Dividing Station is the link between the mobile vessels and the conveyor. It is to be purchased dependent on production requirements. From the screenshot of the conveyor section it can be seen that the Dough Dividing Station is a potential bottleneck. As it is specialist equipment, it may be required to have a redundant dough divider.

The plant layout and schedule as proposed would be an ideal situation with no limit on space, cost or resources. However in real life, there would be restrictions. If space and cost were an issue then the number of milk and water charging stations and mixing stations can be reduced. This also reduces the production rate and therefore the requirements (space and cost) on the dough divider, oven and packaging equipment.