The development of an interlock and control system for a clinical proton therapy system.

T.J. Fulcher

Thesis presented in partial fulfilment of the requirements of a Masters Diploma in Technology in Electronics Engineering at the Cape Technikon.

Promotors: Mr D.L. Martin and Dr D.T.L. Jones

Acknowledgements

I would like to express my gratitude to Rudi Fisch, Sarel Burger, Charlie Wikner, Niek Schreuder and Johan van Niekerk for their patience with my relentless questioning.

This work is dedicated to my wife Lynn, my new son Daniel and my late father Harold "John" who would have been very pleased to see me finish.

Table of Contents

Abstract

The development of a 200 MeV clinical proton therapy facility at the National Accelerator Centre required an interlock and control system to supervise the delivery of radiation to a patient.

The interlock and control system is responsible for ensuring that nobody enters the treatment vault during an irradiation, the extraction of the beam-stop devices from the beam-line to allow the irradiation of the patient and the insertion of those beam-stop devices when an error condition is detected.

Because of its nature, the interlock and control system should be designed so that in the event of an error condition being detected, it should fail to a safe state. This is achieved by modelling the interlock and control system with an appropriate modeling method.

This thesis describes a graphical modelling method called Petri-nets, which was used to model the system, and the software developed from the model.

Objectives

1. To duplicate the existing neutron therapy interlock and control system on a personal computer.
2. To develop a software oriented system.
3. To evaluate a suitable modelling tool and become familiar with that modelling tool.
4. To divide the systems into subsystems and to model each subsystem.
5. To translate these models into source code and to test them.
6. To establish the period within which the system should terminate an irradiation on detection of an error.

Chapter 1

Introduction

1.1 The National Accelerator Centre.

The National Accelerator Centre (NAC) at Faure near Cape Town is a nuclear accelerator designed as a multidisciplinary facility to satisfy the often conflicting requirements of nuclear physics, isotope production and radiotherapy [Re88]. Its major components include a solid pole light ion injector cyclotron and a separated sector cyclotron capable of accelerating protons up to energies of 200 MeV. A heavy ion injector cyclotron has recently been constructed.

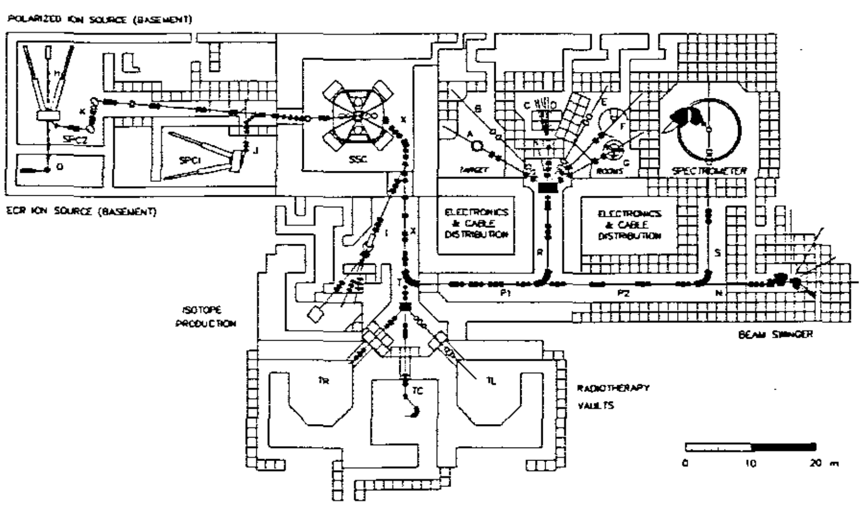


Figure 1.1 Layout of the N.A.C. facilities.

The National Accelerator Centre has developed 200 MeV clinical proton therapy facility.

1.2 Description of the NAC radiotherapy facilities.

X-rays were the first radiation source used for the treatment of cancer. Until 1970 most sources were either gamma rays from isotopes such as ^{60}Co or megavoltage x-rays from betatrons. Most contemporary sources are bremsstrahlung photons produced when high energy electrons from an electron linear accelerator strike a target material, or are themselves used for patient treatment. These sources are known as *conventional radiation* [Ra80].

The radiotherapy facilities at NAC include three radiotherapy treatment vaults, laboratories, offices, patient service areas, operating theatres and a thirty-bed hospital. The three radiotherapy vaults are to be used for an isocentric neutron therapy, fixed horizontal beam proton therapy facility and either a vertical or isocentric proton therapy facility respectively.

1.3 The NAC neutron therapy facility.

The NAC neutron therapy facility consists of a 50 tonne gantry, which can rotate about the patient so as to treat the patient from different angles. This gantry contains 70° and 160° bending magnets as well as beam steering and focussing devices. The neutrons are produced by the reaction of 66 MeV protons impinging on a beryllium target in which the proton beam dissipates 40 MeV. This reaction is referred to as p(66)/Be(40). Immediately upstream (towards the cyclotron) of the target assembly is a quadrant electrode system which provides information on the beam position and symmetry. Downstream of the target assembly are the hardening and flattening filters and the transmission ionisation chambers [Jo89].

Conventional radiotherapy is implemented using photons or electrons. Unlike photons, which interact with orbiting electrons and transfer their energy by photo-electric, Compton and pair production processes, neutrons interact with nuclei and transfer their energy to heavy charged particles. Hydrogen-rich materials such as soft tissue contain large amounts of water and absorb more energy from neutron beams than harder tissues such as bone. This is in contrast to photons which deposit more energy in harder tissues [Jo89].

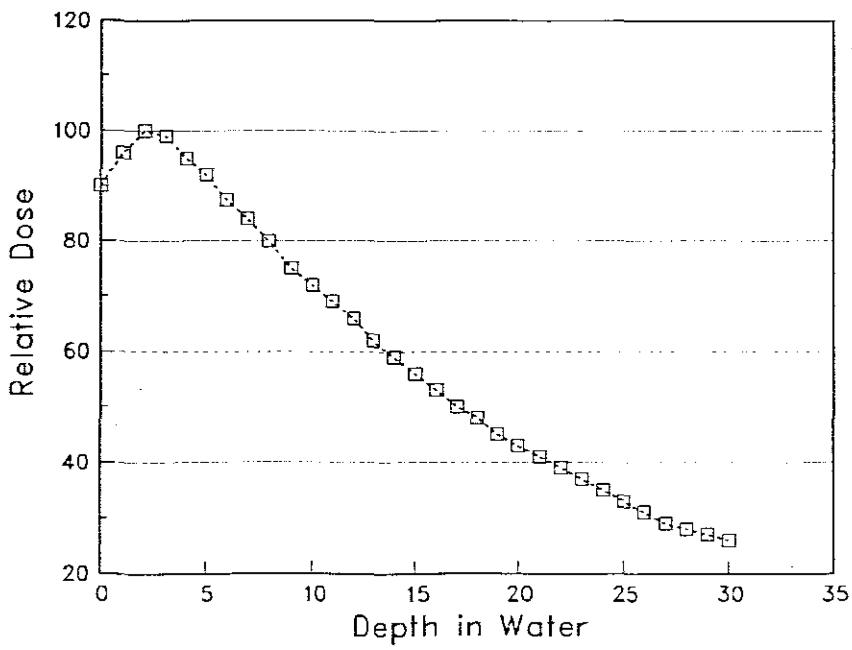


Figure 1.2 The depth dose curve of p(66)/Be(40) neutrons in water.

Tumours are frequently found deep inside the body. To treat these deep seated tumours the radiation has to pass through healthy tissue. One of the difficulties of radiotherapy is to limit the damage to healthy tissue [Ra80]. One method of limiting this damage is to irradiate the the tumour from different directions, concentrating the dose on the tumour site. This requires an isocentric beam delivery system, that is one that can rotate about the patient (fig 1.3).

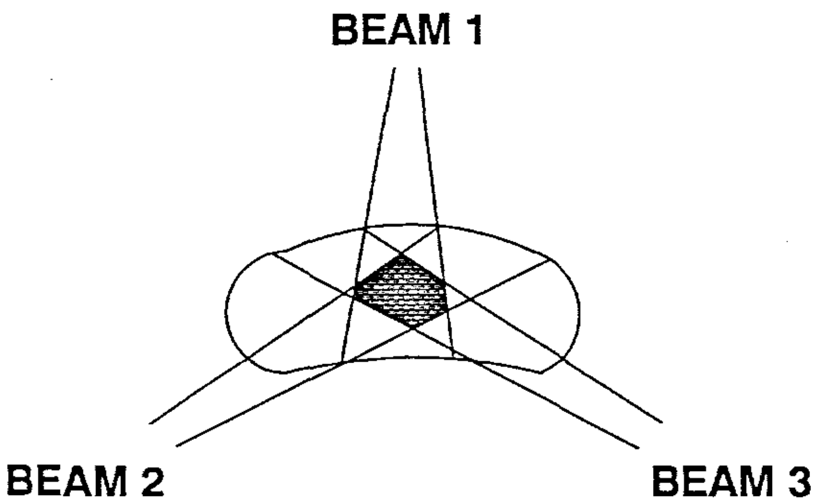


Figure 1.3 An illustration of the principle of isocentric treatment showing the beam irradiating the tumour from 3 directions and the shaded portion representing the target volume. The dose is concentrated in the target volume.

1.4 Proton therapy

1.4.1 History and overview.

Another method of limiting the dose delivered to the healthy tissue proximal to the tumour is by using protons. Proton therapy holds various advantages over other forms of radiotherapy by virtue of its delivering a relatively low dose of radiation to healthy tissue preceding the tumour, maximum dose to the tumour and no dose to the tissue distal to the tumour [Fo81]. This effect, which is reflected in Bragg ionisation curve was first noted by Bragg and Kleeman in 1904 [Br04] (fig 1.4). Protons with an energy of 200 MeV have a range of approximately 26 cm in tissue, which is suitable for treating most sites in the human body.

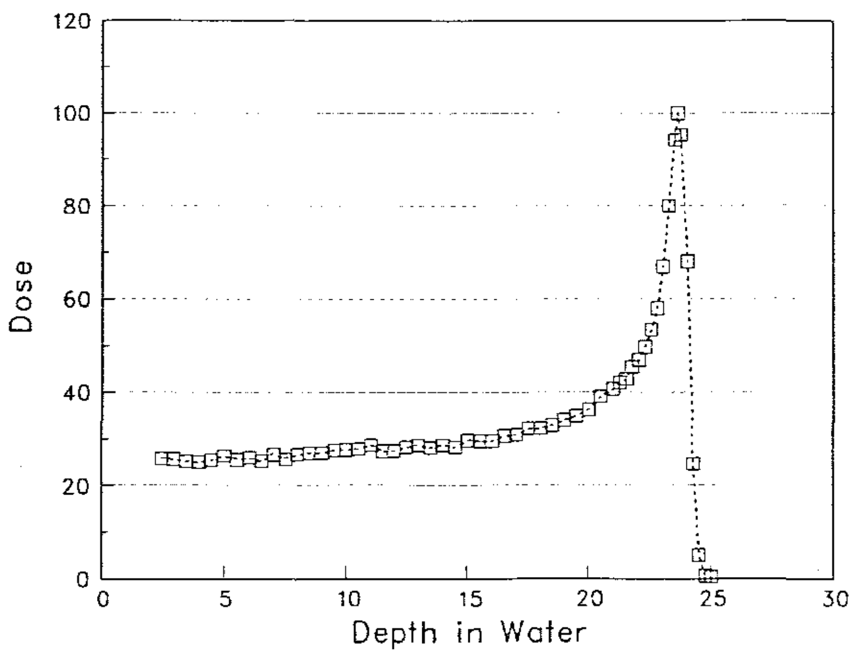


Figure 1.4 The 182 MeV Bragg curve measured in water.

Protons penetrate tissue in almost straight lines. As the proton proceeds through the tissue, tissue atoms are ionised at the expense of proton energy. The dose delivered to the tissue (energy deposited per unit mass) is proportional to the specific ionisation which varies almost inversely with the energy of the proton. Thus the specific ionisation is much less where the proton enters the tissue at high energy than it is in the last portion of its path [Ro89].

In 1946 Wilson [Wi46] proposed the potential application of protons and heavy charged particles in radiation therapy One year later biological investigations using high energy nuclei were begun by Tobias, Lawrence et al at the new Berkeley 184-inch synchrocyclotron [To52]. This led to the treatment of human diseases associated with the pituitary gland in December 1954. From 1957 to 1976 185 MeV protons from the 230 cm synchrocyclotron at the Gustav Werner Institute in Uppsala, Sweden were used for radiotherapeutic applications. The 184-inch Synchrocyclotron at Lawrence Berkeley Laboratory was also used for other precision high dose charged particle radiotherapy. Protons have also been used extensively at the Harvard Cyclotron Laboratory to treat more than 4000 patients [Ra80]. Proton therapy facilities which are operational are listed in Table 1.1.

1.4.2 NAC proton therapy facilities.

To take full advantage of the characteristics of a proton beam it is necessary that the patient be positioned extremely accurately during their treatment (to within 2 mm of the desired position). The University of Cape Town Departments of Mechanical Engineering and Surveying co-operated to develop a Patient Positioning System (PPS) that, by means of TV cameras, positions the patient and monitors the patient's position during treatment. If the patient's position changes during treatment the PPS should inform a supervisory system which should terminate the treatment. This is achieved by determining the position of the tumour relative to reflective markers on the patient's skin. These reflective markers are then monitored by the TV cameras (whose position has been determined) and if these markers move by more than a preset amount (usually 0,5 mm) the signal to terminate the treatment must be given [Va91].

The proton therapy facility would require an interlock and control system for the interlocking of the treatment vault and other associated devices and a system for the control of the delivery of the proton beam to a patient. By virtue of the nature of the controlled system it must be a **critical system** (ie a system upon which human life would depend). Accordingly this system must be designed to specific standards.

Table 1.1 Operational proton therapy facilities.

PLACE	ENERGY (MeV)	RANGE (cm) in water
Clatterbridge, UK	62	3,3
Chiba, Japan	70	4,1
Villigen, Switzerland	72	4,4
Cambridge, USA	160	18,0
Uppsala, Sweden	200	26,3
Dubna, Russia	200	26,3
Moscow, Russia	200	26,3
Tsukuba, Japan	25	38,5
St Petersburg, Russia	1000	330,3
Orsay, France	73	4, 5
Nice, France	65	3,6
Louvain-la-Neuve, Belgium	90	6,5
Bloomington, USA	200	26,3
Faure, RSA	200	26,3
Orsay, France	200	26,3
Loma Linda, USA	250	38,5

Chapter 2

Critical systems

2.1 An overview of critical systems.

A critical system may be defined as any system where the consequences of failure are serious and may involve grave danger to human life and property [Le87], for example an airliner flight control system, a process control system for a chemical plant or in the present case a control system for a radio-therapy facility.

Although electronics have been used in critical systems for many years the advent of cheap and fast computers has led to their adoption for the same tasks [Th89]. However recent events have illustrated the possible shortcomings of the computer-based critical system, especially the computer-controlled radiotherapy machine [Jo87]. Critical systems may be divided into three forms [Le87]:

1) Fault-tolerant systems - A system which continues to provide full performance and functional capabilities in the presence of operational faults.
2) Fail-soft systems - continues operation, but provides only degraded performance or reduced functional capabilities until the fault is removed.

3) Fail-safe systems - attempts to limit the damage caused by failure. No attempt is made to satisfy the functional specifications except where necessary to ensure safety.

In the case of an airliner control system it is obvious that either the fault-tolerant or fail-soft approach must be taken. In the event of a failure the airliner cannot fail-safe unless it is on the ground. However, in the case of a proton therapy control system a fail-safe option is imperative. In the event of a failure the system returns to a safe condition by removing the dangerous condition (the beam of radiation).

Hardware-based critical systems can be considered very reliable. Because software doesn't fail arbitarily, but fails systematically, it can be regarded as completely reliable [Th89]. Thus any software failures can be attributed to poor design or specification. Software cannot be regarded as overtly dangerous [Le87]. However, systematic or random failures of either software or hardware can lead to a set of circumstances that are life-threatening. The most likely causes of a failure in a critical system are a failure of specification or a design error. These cannot be quantified and therefore pragmatic non-numerical techniques must be employed to ensure adequate safety [Th89].

2.2 Design criteria for a critical system.

The first and most important step of designing a critical system is a formal hazard analysis of the entire system. The next step is the assesment of the identified hazards: how likely are they to occur and what effect will they have if they do occur? The final step is the design of the system to reduce, control or eliminate these risks [Th89, Le91].

2.2.1 Hazard analysis.

The earliest stage of the development of a critical system is the identification of hazards. A hazard may be defined as "a set of conditions (ie a state) that can lead to an accident, given certain enviromental conditions." [Le91]. This stage of the development of a safety critical system is the simplest as the hazards are frequently so obvious that it is difficult to overlook. Take, for instance, the example of an access door placed over high voltage equipment - a hazard exists when the access door is opened and the high voltage equipment is live. In this case the solution is simple - switch off the high voltage automatically when the access door is opened.

2.2.2 Hazard assesment.

After identifying the hazards it is necessary to quantify those hazards and then divide the quantified hazards into different classes of hazard eg negligable, marginal, serious and critical. The next step is the evaluation of the likelihood of a hazard [Le91]. This is usually very difficult to determine in the early stages of the design because this information is rarely available at the outset of the project and must usually be determined experimentally. Hence continuous re-evaluation of the likelihood of the occurrence of a hazard is frequently required through the life cycle of the development of a critical system.

2.2.3 Hazard control.

The control of hazards in a safety critical system involves employing various design techniques. If all hazards could be eliminated from a system that system is regarded as *intrinsically safe.* If it is not possible to completely eliminate all hazards then the hazards must be minimised in respect of their severity and likelihood. This is achieved by including devices that attempt to reduce the occurrence of a hazard, examples of such devices include speed governors, pressure release valves, lock-out devices, lock-in devices or interlocks.

A lock-out device prevents a hazardous event from occurring, a lock-in device maintains safe conditions and an interlock ensures that events occur in a strict sequence thus ensuring that hazards do not occur.

2.3 Formal approaches.

Once the design criteria have been established for a critical system the system must be modelled with consideration of those design criteria using a language or notation which is mathematically well defined. Numerous formal modelling techniques have been developed, these include N-version and recovery block programming. Both N-version and recovery block programming are fault-tolerant software, that is a redundancy technique that can be regarded as analogous to hardware redundancy techniques. Model based notations are well suited to formal specifications in notations based on typed set theory and are employed to model the internal state of a system. An example of a model based notation, which possesses an appealing graphic representation, is the Petri-net. Petri-nets are an abstract, formal model of information flow similar to flowcharts but are particularly suitable for modelling asynchronous concurrent systems [Ja90].

2.4 Hardware considerations.

If, after a formal hazard analysis, the developers of the critical system elect to pursue either the fail-soft or fault-tolerant options they are faced with two hardware design philosophy options [Th89]:

1) Redundancy - generally used to reduce the impact of hardware failures (remembering that software does not fail randomly). Redundancy is implemented by having two or more parallel systems with common inputs and outputs where the majority vote from the two or more systems determines the output (Fig 2.1). Redundancy is usually employed with diverse development (see overleaf).

2) Diverse development - when multiple versions of a system run in parallel with logic that requires multiple channels agreeing on the output for a specific input, each channel may be developed by different teams using different system models thus reducing the chance of a failure. The justification for diverse development is that different teams are unlikely to make identical or related mistakes (assuming that the formal specification is correct). Another example of diverse development is a critical system being developed by one team and tested by another.

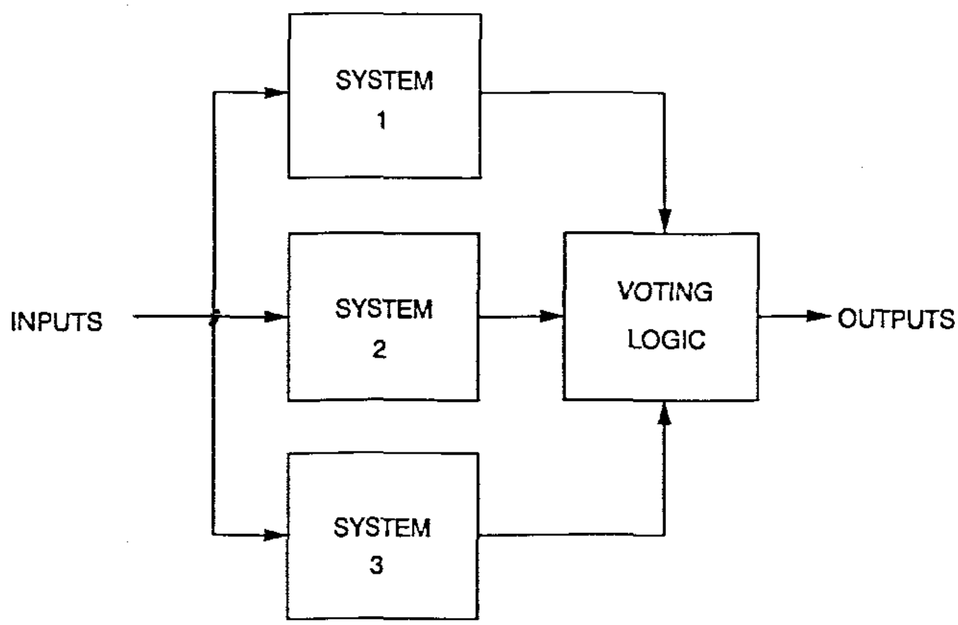


Figure 2.1 An example of a redundant system.

To construct a critical system which relies solely on the proper functioning of software could be considered foolhardy [Le91], hence it is usual to build in hardware checks on the software. One manner in which this can be achieved is by employing watchdog timers. A watchdog is a device which if not addressed within a preset period ensures that the device fails to a safe condition.

2.5 Testing of safety critical systems.

Once the system has been designed and built, the final step is the testing of that system. The testing of a safety critical system is a highly contentious issue because testing only interrogates a very small percentage of possible system behaviours, thus it is extremely difficult to say how safe a system is. This is not a justification for avoiding testing a system merely for avoiding quantifying system safety. Test rigs, which have the advantages of being fast and providing reproducible possibilities, can be used for testing [Th89].

Chapter 3

Functional specifications

3.1 Description of requirements.

The proposed proton therapy control system forms one part of a very complex main cyclotron interlock system.

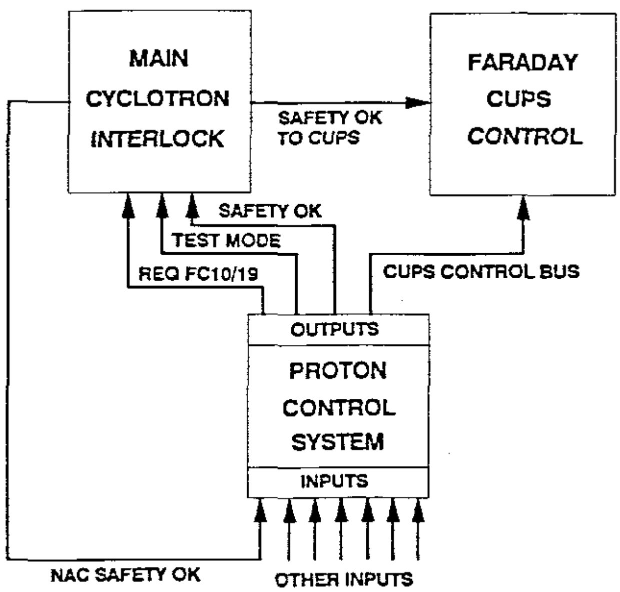


Figure 3.1 A schematic overview of the proton therapy control system showing its relationship with the other major components.

The proton therapy control system must confirm to the main cyclotron interlock whether a safe condition is detected, to request the beam and to inform the main cyclotron interlock which mode of treatment has been selected (fig 3.1). In addition the proton therapy control system is responsible for the extraction of various beam stopping devices, namely two Faraday cups and a neutron shutter.

The proton therapy control system is similar to the neutron therapy control system and was to be subdivided into three subsystems:

1) A room clearance subsystem - an interlock responsible for the safe evacuation of the treatment vault, and the maintenance of the integrity of that vault during treatment.
2) The safety interlock subsystem - responsible for terminating treatment or disallowing treatment should any safety requirements fail to be satisfied at any point before or during a treatment of a patient.
3) The cups control subsystem - switches the particle beam on and off by extracting or inserting the Faraday cups and neutron shutter.

The inputs and outputs relevant to each of the above-mentioned subsystems will be discussed in detail.

3.2 Description of inputs and outputs.

All the inputs and outputs to the proton therapy control system are binary, that is either on or off, the on or logic '1' (True) condition being represented by a short circuit and the off or logic '0' (False) condition being represented by an open circuit. The rationale behind this is that a safe condition is represented by a logic '0' or open circuit so that in the event of an equipment failure (ie a micro-switch failing, a power failure or a cable being cut) the input should fail from an *unsafe* (logic '1') to a *safe* (logic '0') condition. Similarly the outputs from the proton control system are binary outputs, that is a closed circuit representing a true or logic '1' condition and an open circuit representing a false or logic '0' condition.

3.2.1 Description and input and output listing of room clearance subsystem.

3.2.1.1 Inputs.

In Chapter 2 the description of an interlock was given as "a device that ensures that a sequence of events occurs in the correct order." The sequence of events for ensuring the proton therapy vault is *armed* or correct for patient treatment is:

1) eight panic buttons are distributed around the treatment vault. All eight panic buttons must be normal (a normal condition is a short circuit). If at any time any of these buttons is depressed the room must resort to *safe* condition (that is neither *armed* nor *primed*).

2) a gate is placed across the entrance to the basement of the treatment vault. This gate must be closed.

3) the door to the annex off the maze must be closed.

4) both access doors in the partition on either side of the beam-line must have been *primed* and closed within 10 seconds.

5) if all of the above conditions are satisfied then the room may be *primed* (a button at the exit of the treatment vault) for evacuation.

6) once the room has been *primed* for evacuation, the operators have 40 seconds in which to leave the room and close the boom at the maze exit.

7) if the boom is closed within the allocated 40 seconds the room is ready for *arming*. The room may be *armed* at any time after the closing of the boom. If the boom is not closed within the allocated 40 seconds, the room must resort to a *safe* condition, after which the room may be *primed* once again.

Once in the *armed* state it must be very easy for the room clearance subsystem to return to the state in which it is ready to be primed, thus removing the *Safety OK* signal to the main cyclotron interlock. This can be achieved in a number of ways :

1) either of two infra-red detectors in the maze is tripped.

2) the room is disarmed by depressing that button.

3) the boom is opened.

4) either of the access doors in the room partition either side of the beam-line is opened.

5) the gate across the entrance to the basement is opened.

6) any of the eight panic buttons is depressed.

To summarise, the inputs for the room clearance subsystem are :

1) Left Door Prime	2) Left Door Closed
3) Right Door Prime	4) Right Door Closed
5) Room Primed	6) Boom Closed
7) Room Armed	8) Room Disarm
9) Panic 0	10) Panic 1
11) Panic 2	12) Panic 3
13) Panic 4	14) Panic 5
15) Panic 6	16) Panic 7
17) Infra-Red Detector 0	18) Infra-Red Detector 1
19) Door to Basement Closed	20) Door in Maze Closed

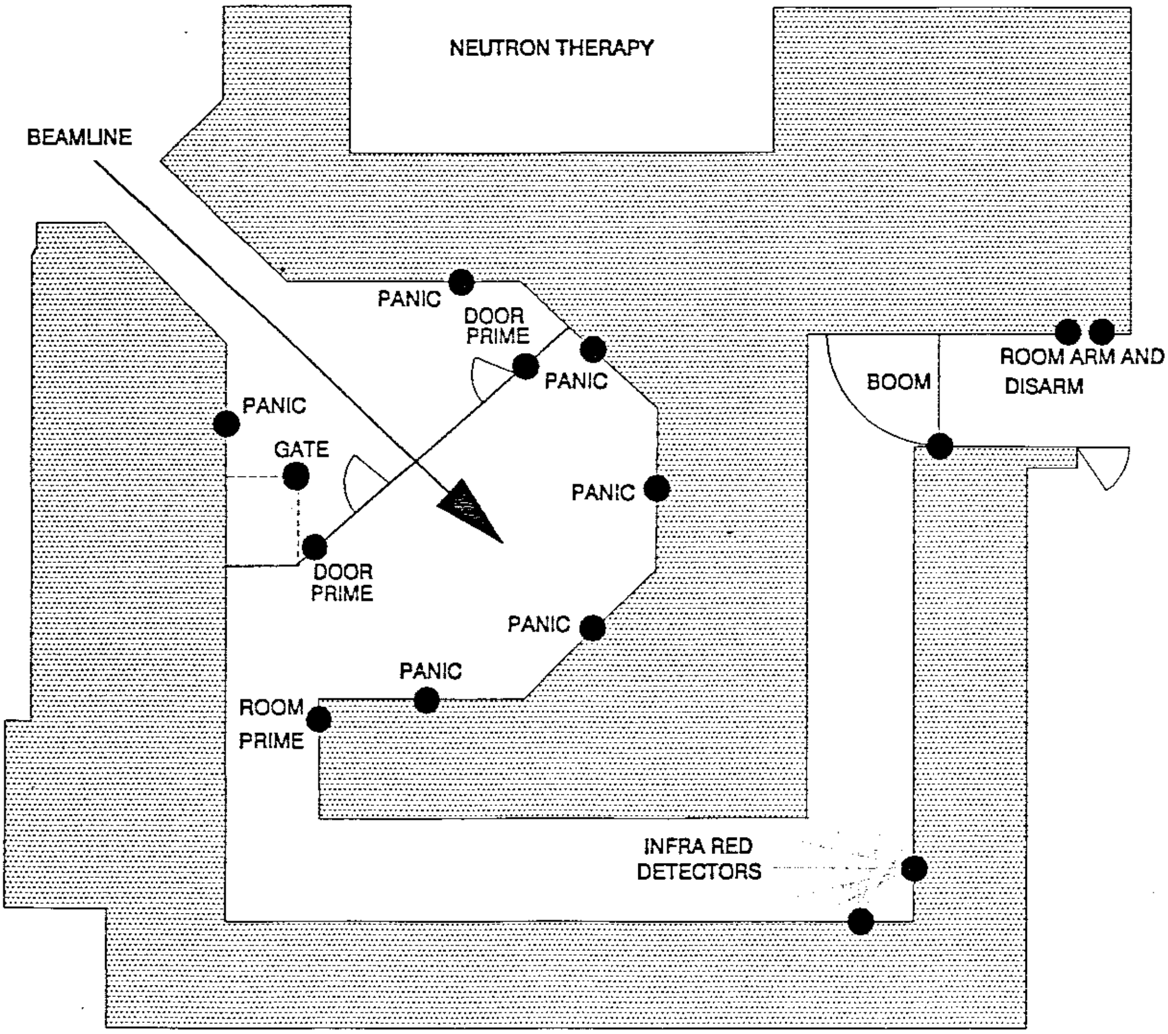


Figure 3.2 Diagram showing the layout of the treatment vault and entrance maze and the postitions of the relevant inputs.

3.2.1.2 Outputs.

Most of the outputs from the Room Clearance are informative (they have no effect on the system but act to inform the operating personnel of the status of the room clearance subsystem). The two outputs which are not informative are a global software flag (Room Armed) and a "Proton Therapy OK" output to the main cyclotron interlock. The Room Armed flag informs the remainder of the Proton Therapy System of the room status. If it is armed then the flag is true and vice versa. The "Proton Therapy OK" output informs the main cyclotron interlock that the proton therapy system is ready for treatment. If the main cyclotron interlock is satisfied it will then reply with a "NAC Safety OK" signal to the interlock subsystem.

The other outputs from the Room Clearance Subsystem are:

1) Room Primed Light - A light above the Room Prime button indicating the room has been primed.
2) Room Primed Bleep - A bleep giving an audio indication that the room has been primed.
3) Room Disarmed Light - A light in the maze which is illuminated when the room is disarmed.
4) Room Armed Light - A light in the maze which is illuminated when the room is armed.

3.2.2 Description and input and output listing for the safety interlock subsystem.

This is the simplest subsection of the Proton Control System consisting of a number of binary inputs and one output (again a global software flag). If any one or more of the input conditions is not satisfied then the Proton Control System must not be allowed to proceed any further than Room Clearance (thus implying the Interlock need not be satisfied for the room to be cleared). If all the inputs are satisfied then a composite signal (in effect a logical *AND* signal) must be generated.

3.2.2.1 Inputs.

The relevant input signals are :

1) NAC Safety OK - This is a composite signal from the Main Cyclotron Interlock indicating to the Proton Control System that it can proceed.
2) Console On - The Proton Control System must be switched on with a key that it shares with the Patient Positioning System.
3) Dose Failure - When the dosimetry system (the system for measuring the radiation or 'dose') determines that the patient has received less than a preset amount of radiation then this input must be true.
4) Ratios OK - The dosimetry system is responsible for measuring the symmetry of the proton beam. If the

asymmetry of the beam exceeds certain preset limits, then the output must go false. If, however, the beam current is less than a preset limit then the output must be true, otherwise the output would always be false.

5) High Voltage Failure - The ionisation chambers transducers for the measurement of the accumulated dose require a polarising voltage. If that voltage should not be correct the dose measurement may be incorrect, therefore in the event of failure the input must change to a false.

6) Chair OK - In section 1.2.2 it was mentioned that the University of Cape Town Departments of Mechanical Engineering and Surveying co-operated to design and manufacture a patient positioning system (P.P.S). This system automatically positions the patient and monitors that position during an irradiation. If the patient should move more than a preset amount (usually about 0,5 mm) then the output to the proton therapy control system should fail.

7) Emergency Stop - The system has an emergency stop button on the operating console, so in the event of an emergency the treatment can be stopped manually. This button has two contacts. Both are normally closed. The one contact provides the signal into the interlock. Should the button be depressed the interlock will be broken. The

Proton Therapy OK signal to the Main Cyclotron Interlock passes through the other contact in this button, if this button is depressed the Safety OK to the main cyclotron interlock will be removed resulting in a complete shutdown.

8) Neutrons OK - It must be impossible for both the neutron therapy unit and the proton therapy unit to be selected simultaneously (this is because elements of the neutron therapy unit are used in the proton therapy control system). If the neutron therapy unit is selected the neutron therapy interlock will break the proton therapy interlock. Note that the converse does not apply, rendering the neutron unit the master unit and the proton unit the slave.

9) Scatterer - This is one of several beam devices that have to be interlocked, the scatterer is a thin piece of lead that spreads the beam laterally. The scatterer **must** be in the beam for treatment to commence.

10) Rings - The natural intensity profile of the beam is Gaussian. For the profile to be clinically acceptable it must be flat. This is achieved by placing occluding rings in the beam. These rings must be in the beam for treatment to commence.

11) Laser - used for aligning the patient (it simulates the beam), It must be removed from the beam-line for treatment to commence.

12) Beam Defining Lamp - Used to illuminate the area to be irradiated when aligning the patient. It must be removed from the beam-line for treatment to commence.

13) Ionisation chamber - The transducer used to measure the radiation the patient receives. It must be in the beam-line for treatment to commence.

14) Collimator - Shapes the beam before it strikes the patient. It must be in the beam-line before treatment commences.

15) Barcoding system - Each patient has several unique components (these include collimators and masks) which must be in the beamline for treatment to commence. To ensure that the correct components are in the beamline each component is assigned a unique number and a barcoding sticker with that number is fixed to that component. Before treating that patient a file containing those unique components is created on a p.c. and those components are downloaded to a barcoding scanner. The components are then scanned by the barcoding scanner and downloaded to the p.c. If the components are correct the p.c. will inform the interlock that it may continue.

16) Treatment mode - Two types of treatment are possible Bragg peak and shoot-through. The barcoding system detects which type of treatment and informs the interlock.

17) Propeller - A modulator wheel used to spread out the Bragg peak. If Bragg peak treatment is selected the propeller must be in the beam. if shoot-through treatment is selected the propeller must not be in the beam.

18) Rotation - if Bragg peak treatment is selected the propeller must be rotating.

The relative postions of items 9) - 14) are shown in figure 3.3

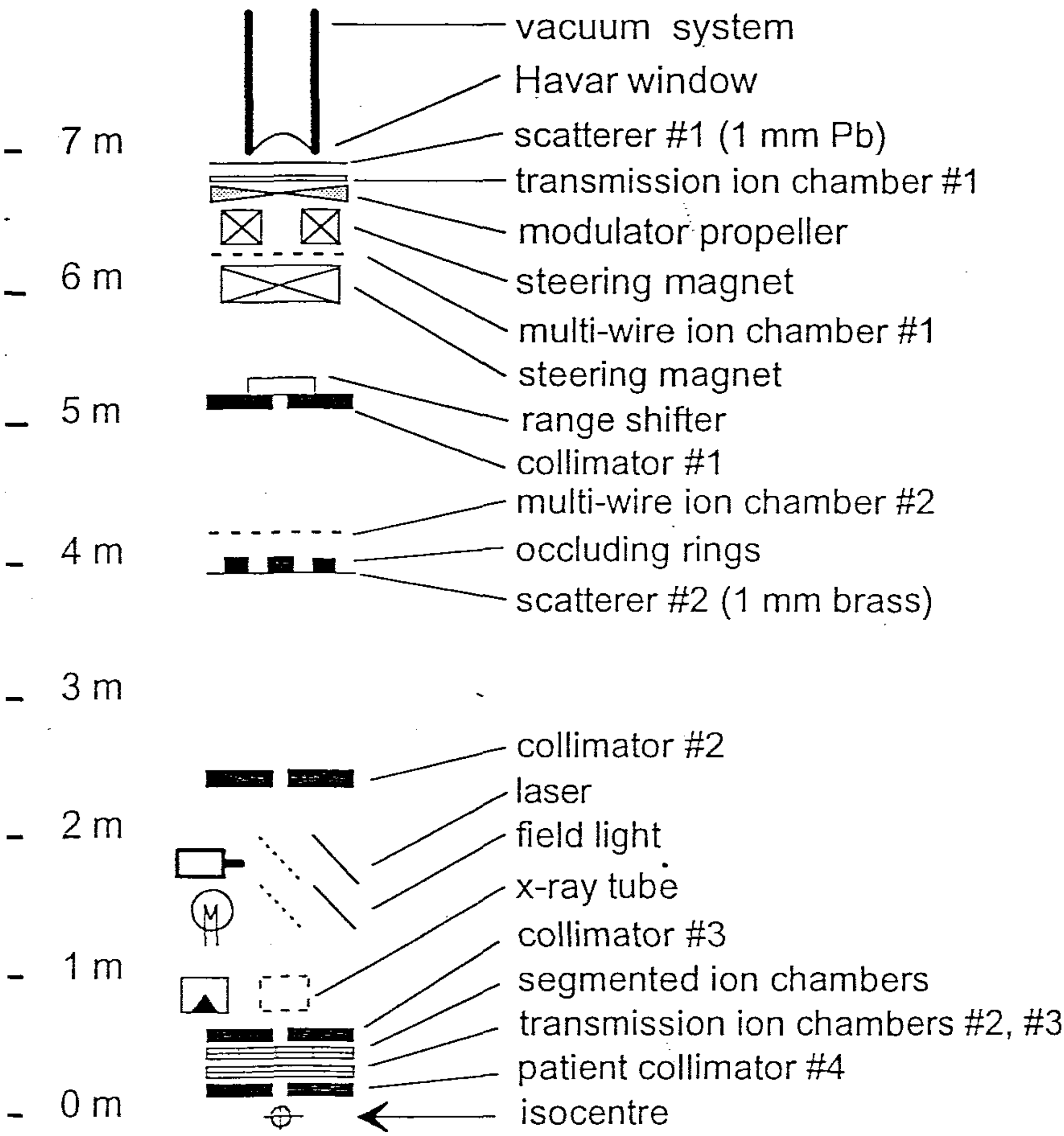


Figure 3.3 Illustration of the interlocked beamline devices downstream from Faraday cup 1.

3.2.2.2 Outputs.

The safety interlock subsystem has no physical outputs. If it is satisfied it sets a global software flag. Although it has no physical outputs and cannot extract any devices it is responsible for the insertion of two beam-line devices. The extraction of these beam-line devices (whose purpose will be discussed in section 3.2.3) is requested by the Cups Control Subsystem. It must be emphasised that the Cups Control Subsystem **requests** the extraction of those devices as opposed to **ordering** the other beam-line devices. If the Main Cyclotron Interlock considers it safe to extract those devices then it will do so.

Because timing is not critical in the delivery of the beam the low priority Cups Control Subsystem is responsible for requesting the extraction of those beam-line devices. However the termination of the beam is a high priority task and hence the high priority Interlock Subsystem removes the request for those beam-line devices.

3.2.3 Description and input and output listing for the cups control subsystem.

The Cups Control System Subsystem is responsible for activating the irradiation by extracting Faraday cups 1 and 2 and the neutron shutter and requesting the extraction of Faraday cups 10 and 19. It is also responsible for the insertion of Faraday cups 1 and 2 and the neutron shutter but it is not responsible for the insertion of Faraday cups 10 and 19 as discussed in section 3.2.2.2.

3.2.3.1 Inputs.

There are two types of beam stop devices - a Faraday Cup which is a cup shaped piece of copper (usually water cooled to dissipate the energy deposited when it is in the beam) and a neutron shutter which is a 1 m long steel cylinder used for radiation shielding.

The beam stop devices each have two micro-switches associated with each extreme of the movement of the device - in the beam or out out of the beam. Both positions were assigned an input. The four beam-stop devices are :

1) Faraday Cup 1 in/out - Located at the end of the beam line (last beam stop device before the patient.)
2) Faraday Cup 2 in/out - Located between the cyclotron and Neutron shutter.
3) Neutron Shutter in/out - Located in the wall of the treatment vault.
4) Faraday Cup 10/19 in/out - actually two cups between the injector cyclotron (SPC 1) and the main cyclotron (SSC). These two cups are used for the final delivery of the beam. The "in" and "out" signals are actually composite signals - "out" representing both FC10 *AND* FC19 out and "in" representing either FC10 *OR* FC19 in.

The convention that "in" represents *"In the beam"* (a safe condition) and "out" represents *"Out of the beam"* (an unsafe condition) has been adopted.

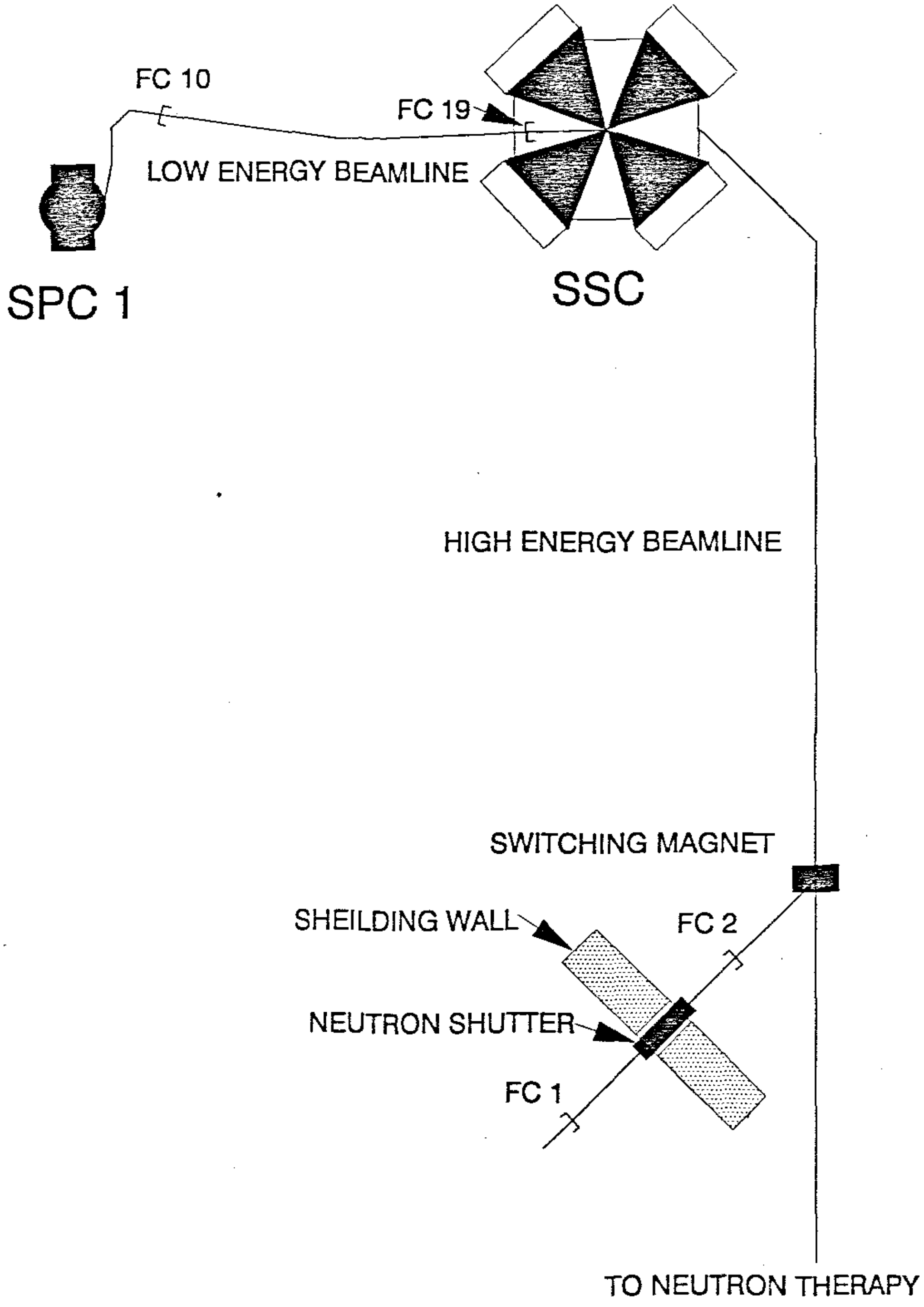


Figure 3.4 Illustration of the Beamline devices showing their positions relative to the cyclotrons.

In addition to the previously mentioned inputs there are also :

1) Treatment Start - A button which must be depressed to start an irradiation.
2) Test Mode Selected - A key-switch on the treatment console, Test Mode is similar to a normal mode treatment the only difference is that Faraday Cup 1 is left in the beam resulting in an intrusive measurement of the beam current at that point.

3.2.3.2 Outputs.

The control of Faraday Cups 1 and 2 and the Neutron Shutter is achieved through a control crate. This crate is shared with the Neutron Therapy system. The crate operates on a bus system with two three-bit addresses and two command lines. The two address busses are a crate address bus (if more than one crate is to be used) and a device address bus (to address the device on the bus).

The two command lines are a beam-device open command and a beam device insert command. In addition there is a request Faraday Cup 10/19 line. These devices have been discussed in a previous section and the Cups Control Subsystem only requests the extraction of these devices and is not responsible for their insertion. Summarising, the outputs from the Control Subsystem are :

1) Crate Control Address 3

2) Crate Control Address 2

3) Crate Control Address 1

4) Crate Address 3

5) Crate Address 2

6) Crate Address 1

7) Beam Device Open Command

8) Beam Device Close Command

9) Request Faraday Cup 10 and 19

When a treatment is started the sequence of events should be : firstly Faraday cup 1 must be extracted followed by the neutron shutter which is followed by the extraction of Faraday cup 2 and finally the extraction of Faraday cups 10 and 19 must be requested from the Main Cyclotron Interlock. If any of the devices fail to extract within ten seconds of the issuing of the command then the control subsystem should indicate a failure. The exception to this is the extraction of Faraday Cups 10 and 19 which may be extracted at random after the request to the Main Cyclotron Interlock. If a failure of either the Room Clearance Subsystem or the Safety Interlock Subsystem or the Control Subsystem is detected at any time during a treatment or after commencement of a treatment the system must close-down by initially removing the request for Faraday cups 10 and 19 and then inserting Faraday cup 2, followed by the neutron shutter and finally Faraday cup 1.

3.3 Design philosophy.

It is necessary for the designer of a system to adopt a design philosophy before embarking on the construction of that system. A software orientated approach was regarded as prudent both for reasons of economy and professional challenge. By software orientation it is meant that instead of using hardware to latch the state of an input and perform combinational logic operations, the system would use a personal computer to sample signals through an elementary input card, process and draw a conclusion from those inputs and use an elementary output card to provide the appropriate output signals. This approach has several advantages over the combinational logic approach, namely:-

1) The design and complexity of the hardware is reduced considerably. This design and manufacturing is both time consuming and costly.
2) Any modifications that need to be made (which are many in the life cycle of a system like this) can be made cheaply and neatly, assuming that both the software and hardware are well documented.
3) Information that has to be presented to the operator in the event of an error or during normal operation, can be presented in a manner that is unlikely to confuse even the most inexperienced operator.

Because of the decision to implement a system of this nature (a critical system) in a software orientated environment it was obvious from the literature that modelling techniques would have to be employed to ensure some degree of confidence in the system.

3.4 Timing requirements.

In Section 3.2.2.2 it was mentioned that the termination of an irradiation had a high priority. These timing requirements were to be determined by experimentation. It must be noted that it is only the safety interlock subsystem that requires this high priority. This is best illustrated by the example of somebody attempting to violate the integrity of the room. That person is going to take considerably in excess of initially estimated response time of 50 ms to enter the treatment vault and expose themselves to radiation. Thus it is not critical that the room clearance subsystem terminate the beam within that period. In the case of the cups control subsystem, this system is concerned only with the preparation of the vault for the delivery of the beam and ensuring that the vault has returned to a safe state after treatment. As a result any errors that occur in this subsystem are not of sufficient importance to require a high priority response. This does not imply that errors detected in either subsystem can be ignored but are of considerably less importance than errors detected in the interlock subsystem.

3.5 Miscellaneous.

The final specification was that the software was to be written in 'C' in keeping with other systems employed in the Proton Therapy treatment system.

Chapter 4

Hardware

4.1 Hardware overview.

In the previous chapter (section 3.3) it was mentioned that the design philosophy adopted by the author was software orientated. In view of this the hardware was designed to be as simple as possible. The hardware can be subdivided into 7 subsections :-

1) the personal computer.
2) The input line driver.
3) The personal computer input interface.
4) The output line driver.
5) The personal computer output interface.
6) The interrupt clock card.
7) The simulator/test-jig

In addition to this hardware a card crate was constructed in which to house the line driver cards and a modular power supply unit to supply that line driver crate. Any standard personal computer (P.C.) employing the Intel 80286 or a more recent chip-set would be considered sufficient for the processing tasks. This personal computer should be housed in a 19" rack housing.

4.2 The input line driver.

The specification for the inputs is that they consist of switches with a closed contact constituting a good or safe condition (logic "1") and an open contact constituting a bad or unsafe condition (logic "0"). Because of the damage that radiation can incur on solid state devices the P.C. is situated away from radiation and outside the vault. For this reason the switches were placed some 100 meters away from the P.C. and hence TTL logic levels were unsuitable for supplying the switches. It was decided to supply the switches with 24 volts to overcome these distance problems. To convert from the 24 volt line voltage to TTL levels whilst isolating the P.C. from any spurious voltages the signals are passed through opto-couplers. Each board consists of 8 input lines so that one card correlates with an 8 bit input channel on the P.C. input interface.

4.3 The p.c. input interface.

These two cards (each consisting of 3 x 8 line input channels) are proprietary cards available "off the shelf". Each card uses an Intel 8255 parallel peripheral interface chip and both are configured in their default state of all 8 bit channels in the input mode.

4.4 The output line driver.

Consists of 8 AND gates where the outputs from the P.C. interface card are logically multiplied with the watchdog signal. The outputs from these AND gates are then buffered by transistors which in turn switch reed relays to provide the open contact/closed contact outputs.

4.5 The p.c. output interface.

It was considered advantageous that the outputs be bit-addressable as opposed to byte-addressable. This implies that any relevant output line can be addressed individually by the software as opposed to addressing a byte of eight output lines, changing the state of one and maintaining the previous state of the other seven. Another requirement of the output line driver was that it have a watchdog timer on board. The purpose of the watchdog timer is to ensure that if the P.C. fails to address the outputs within a pre-defined period that those outputs should be forced to a safe state. This is achieved by the software addressing a monostable multivibrator whose period is set to slightly exceed the time required to complete a loop of the main subroutine once every loop of that subroutine. The output from this monostable is passed to the output line driver where it is logically multiplied with the outputs.

4.6 The interrupt clock card.

This card is a prototype card modified to house a 32,768 kHz "tuning fork" oscillator circuit which is then divided into periods of 15.6 ms. This signal is then supplied to the IRQ5 input on the P.C.

4.7 The simulator/test-jig.

Initially it was thought that a bypass facility would be required for certain inputs. An example of which would be the bypassing of the dosimetry system during quality control checks routinely performed by the physicists. It would also be necessary to simulate the interlock and control system during development and provide a test jig with which the system could be tested. A bypass/simulator/test-jig was designed and constructed for these purposes. It consists of 48 switches. When a switch is operated it provides a 5 volt signal representing a safe condition on an input into the personal computer input interface. After some use it was decided to remove the bypass/simulator/test-jig from the system for safety reasons. However the simulator test jig was employed extensively during development.

Chapter 5

Petri-nets

5.1 Introduction and overview.

A Petri-net is an abstract formal model of information flow, particularly suited to the modelling of asynchronous concurrent systems, that is any system in which it is possible for some of the events to occur concurrently but constraints exist on the concurrence, precedence and frequency of these occurrences†.

A Petri-net is comprised of a collection of places 'P' and of transitions 't'. A Petri-net also consists of an input function 'I', an output function 'O' and an initial marking μ_0. The input function I is a mapping from the transition t_i to a set of places I(t_i). Similarly the output function 'O' maps a transition t_i to a set of places O(t_i). The initial marking μ_i is the initial placement of tokens in the Petri-net.

The places are represented by circles and the transitions by bars, these nodes are joined by arcs (Fig 5.1). The Petri-net is executed by placing dots or 'tokens' in the place or places representing initial conditions. Those transitions whose preceding places are all marked with tokens are 'enabled'. An enabled transition may 'fire'.

† Extensive quotations from [Pe77] are used in this chapter.

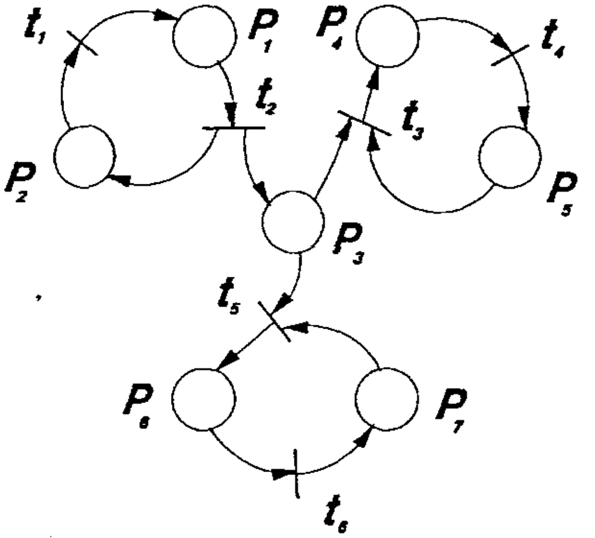


Figure 5.1 An example of an unmarked Petri-net.

A Petri-net with tokens present in places is a marked Petri-net. In Figure 5.2 t_2 is enabled since it has a token present at its input, but transition t_5 is not enabled since one of its inputs (P_3) does not have a token present. If a transition fires it passes the token to all of its subsequent places, thus if a transition is enabled by one token, several tokens may result after the firing of one transition (Fig 5.3 (a) and (b)).

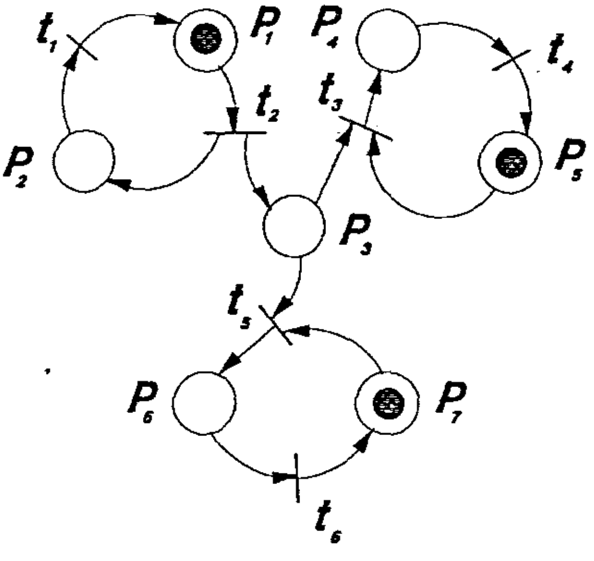


Figure 5.2 An example of a marked Petri-net.

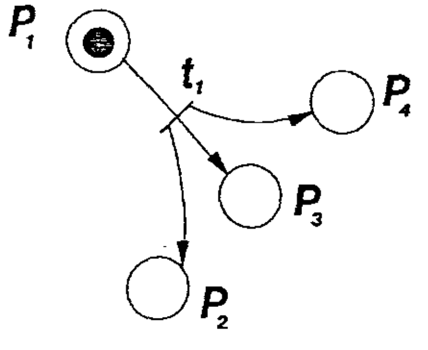


Figure 5.3(a) A marked Petri-net before firing transition t_1.

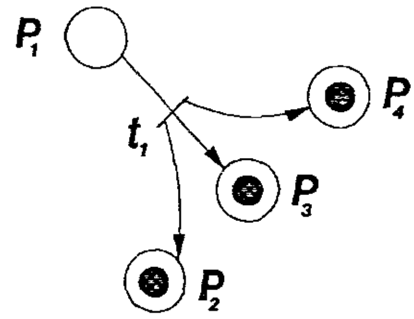


Figure 5.3(b) after firing transition t_1 (an example of non-deterministic firing of transition t_1).

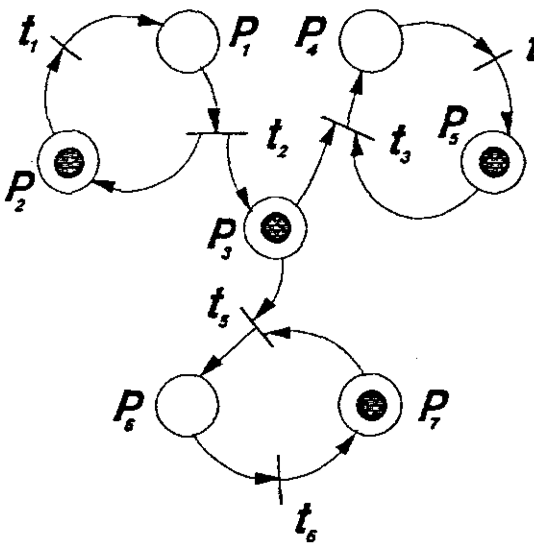


Figure 5.4 The marking that results from firing transition t_2 in figure 5.2.

The marking of a Petri-net changes with the firing of a transition. In different markings other transitions may be enabled. For example in figure 5.4 three transitions are enabled : t_1, t_3 and t_5 none of which were enabled in the previous marking (figure 5.2). In this situation we have a choice of which transition will fire next. From each of these choices other markings may reached, since firing of transitions may continue as long as a transition is enabled.

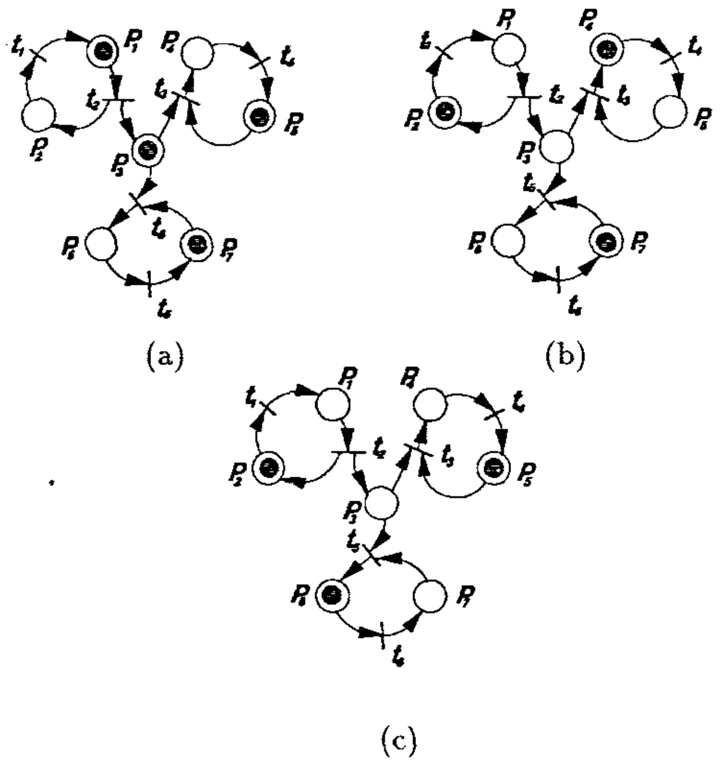


Figure 5.5 Markings that result from the firing of transition t_1 (a), t_3 (b), t_5 (c) in figure 5.4.

5.2 The structure of Petri-nets.

It was mentioned in section 5.1 that Petri-nets consist of two basic components, places representing conditions and transitions representing events. To elaborate it is necessary to define the relationship between places and transitions. This is achieved by specifying two functions, the input function which connects transitions to places I, and the output function O which connects places to transitions. The input function I defines the set of input places for the transition $I(t_j)$ for each transition t_j. The output function O defines the set of output places $O(t_j)$ for each transition t_j.

The structure of the Petri-net is defined by these four items : transitions, places, inputs and outputs. Formally a Petri-net 'C' is defined as the quadruple C = (P, T, I, O).

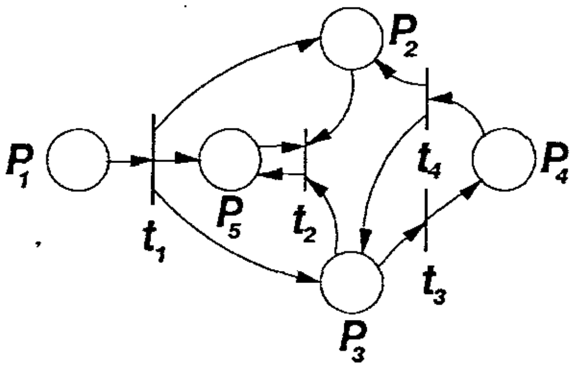


Figure 5.6 A Petri-net graph whose structure is described underneath.

This Petri-net (Fig 5.6) can be represented by the Petri-net structure :-

$$C = (P, T, I, O)$$

$$P = \{p_1, p_2, p_3, p_4, p_5\}$$

$$T = \{t_1, t_2, t_3, t_4\}$$

$I(t_1) = \{p_1\}$	$O(t_1) = \{p_2, p_3, p_5\}$
$I(t_2) = \{p_2, p_3, p_5\}$	$O(t_2) = \{p_5\}$
$I(t_3) = \{p_5\}$	$O(t_3) = \{p_4\}$
$I(t_4) = \{p_5\}$	$O(t_4) = \{p_2, p_3\}$

5.3 Marking.

The marking 'μ' of a Petri-net is the assignment of tokens in a Petri-net. The position and number of the tokens present in a Petri-net varies during its execution. A vector $\mu = (\mu_1, \mu_2, \mu_3, ..., \mu_n)$ gives, for each place in a Petri-net the number of tokens in that place. The number of tokens in a place p_i is μ_i, i = 1, 2 , . . . , n. The marking function $\mu : P \rightarrow N$ may be defined from the set of places to the natural numbers $N = \{0, 1, 2, . . .\}$, we can now use the notation $\mu\ (p_i)$ to specify the number of tokens in place p_i. Thus for a marking μ, $\mu\ (p_i) = \mu_i$.

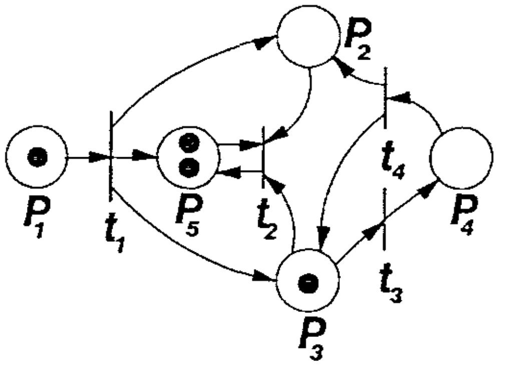


Figure 5.7 A marked Petri-net.

Figure 5.7 has a marking of μ = (1, 0, 1, 0, 2). A marked Petri-net C = (P, T, I, O) with a marking μ becomes the marked Petri-net M = (P, T, I, O, μ).

5.4 State space.

The marking of a Petri-net defines its *state*. The firing of a transition represents a change in the state. The *state-space* of a Petri-net with n places is the set of all markings i.e. N^n. The change in state caused by the firing of a transition is defined by a partial function δ, called the *next-state function*. Applying this function to a marking μ and a transition t_j gives us the value of the marking that results from the firing of the transition t_j in a marking μ. t_j can only fire if it is enabled, hence $\delta\ (\mu,\ t_j)$ is undefined if t_j is not enabled in marking μ.

A Petri-net with initial marking μ_0 can be executed by successively firing transitions. Firing a transition t_j in an initial marking μ_0 results in a new marking $\mu_1 = \delta\ (\mu_0,\ t_j)$, any enabled transition in this new marking, say t_k can be fired resulting in yet another new marking $\mu_2 = \delta\ (\mu_1,\ t_k)$. This can continue as long as a transition is enabled.

5.5 Reachability sets.

If, as a result of firing a transition t_k, a marking μ' is reached from a marking μ then μ' is said to be *immediately reachable* from μ. A marking μ' is reachable from μ if it is immediately reachable from μ or is reachable from a marking which is immediately reachable from μ. The reachability set *R(M)* for a Petri-net M = (P, T, I, O, μ) is defined as *"The set of all markings which can be reached from μ."*

Consider figure 5.2, the initial marking is $\mu = \{1, 0, 0, 0, 1, 0, 1\}$. If transition t_2 fires a marking $\mu' = \{0, 1, 1, 0, 1, 0, 1\}$ results. We say that μ' is immediately reachable from μ. From marking μ' several markings are reachable. By firing t_1 a marking $\mu'' = \{1, 0, 1, 0, 1, 0, 1\}$ results, or by firing t_3 marking $\{0, 1, 0, 1, 0, 0, 1\}$ is reached or by t_5 marking $\{0, 1, 0, 0, 1, 1, 0\}$ results.

This reachability tree is partially illustrated in Fig 5.8 below.

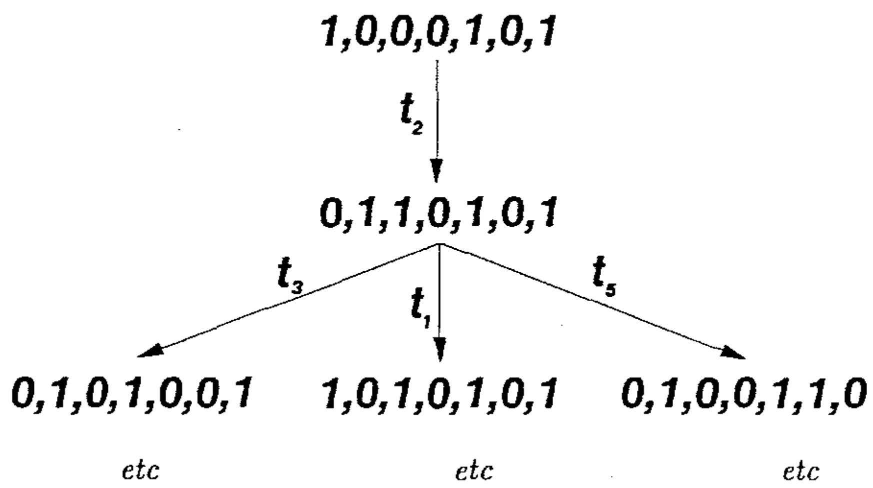


Figure 5.8 The partial reachability tree for Figure 5.2.

By evaluating the criticality of states (markings) the likelihood of those states being reached and the route by which they were reached can be identified. For example in fig 5.8 (above) if the marking $\mu' = \{0, 1, 0, 1, 0, 0, 1\}$ has been evaluated as critical we can see from the Reachability graph that state (marking) can be reached from its preceding state μ only if t_3 fires.

5.6 Modelling with Petri-nets.

In science the studying of phenomena is frequently difficult so instead a mathematical representation of the phenomena called a model is often studied. The model usually incorporates what are considered important properties of the physical phenomena. Petri-nets are a tool used for modelling systems and in particular events and conditions and the relationships that exist between them. It is thus important to know and understand the properties of Petri-nets.

5.7 Properties of Petri-nets.

5.7.1 Asynchronism.

In a Petri-net there is no inherent measure of time but merely the ordering of events. Because of this property Petri-nets are considered *asynchronous.*

5.7.2 Non-determinism.

A Petri-net can be seen as a sequence of discreet events whose order is one of many possibilities allowed by the structure of the Petri-net. This leads to *non-determinism.* If at any time more than one transition is enabled the choice of which transition will fire next is completely arbitrary insofar as the model is concerned.

To simplify further it is important to regard the firing of a transition as a *primitive event,* that is the firing of a transition can be regarded as instantaneous. Since time is a continuous variable the probability of two events occurring simultaneously is zero, ie two or more transitions cannot fire simultaneously. Put simply non-determinism means that more than one token can be present in a Petri-net at any instant.

A place can be regarded as a *non-primitive* event or an event that occurs in non zero time.

5.7.3 Hierarchism.

Either transitions or places may be modeled by sub-nets that are at a more abstract level to provide more detailed modeling. This can be understood by considering the example of a place being represented by a more complex sub-net consisting of more places and transitions.

5.7.4 Concurrency or parallelism.

Any transition (if enabled) may fire arbitrarily and there is no need to synchronize the firing of transitions. Because the firing of a transition is a primitive event (requiring infinitesimal time) two or more unrelated transitions may fire practically simultaneously.

Chapter 6

Software description

6.1 Software overview

The specifications of the Proton Therapy Interlock system were discussed in chapter 3 and included dividing the system into 3 subsystems viz :-

1) The room clearance subsystem,
2) the safety interlock subsystem and
3) the cups control subsystem.

In section 3.3 the priorities and duties of the above subsections were discussed and the need for a fast interlock subsection was emphasised while the other two subsections were of less importance than the interlock. Burger [Bu92] suggested employing a high priority synchronous sampling and interlock routine and a low priority asynchronous main loop whose duties would include all other tasks such as the operator interface. In addition to the above subsections there are also three other subsections namely :-

1) The Input Sampling Routine - Responsible for sampling the inputs.
2) The Error Handler - updates the screen when an error occurs.

3) The Operator Interface - Displays the input statuses. Is also responsible for changing the bypass matrix and for updating that matrix.

It was mentioned above that the system should consist of a synchronous sampling routine and an asynchronous main loop but this would mean that the main loop would have to be infinite. By virtue of this fact it would be impossible for any single Petri-net or subroutine to consist of a smaller loop that, while active, would deny the processor to other parts (sub-routines) of the main loop. Because of this the Petri-nets must be written in such a way as to be considered ***re-entrant***. Hence the software must make use of non-volatile flags (that is flags whose values remain unchanged even when the thread of the programme is outside the appropriate sub-routine). These flags are used to record the progress of the token within a particular Petri-net. Because of the re-entrant nature of the software it is important to note that as a rule a flag is associated with a place in a Petri-net (thus indicating whether a token is present in a particular place or not).

6.2 The interrupt routine.

In section 3.4 the need for a maximum error response time of 20 ms was discussed. In order to achieve this the inputs must be sampled with a period not exceeding 20 ms. This can be achieved by constructing external interrupt hardware and enabling the appropriate interrupt in the software. It was also mentioned that the request for the extraction of Faraday cups 10 and 19 is dealt with by the Cups Control Subsystem, but the insertion of those cups is done from the Interlock Subsystem. Because of the demanding timing requirements the Interlock Subsystem is included in the Interrupt routine. Each system input has associated with it three flags, namely the status of that input, and whether the input has changed state from a logic low to a logic high (set) or vice versa (reset). It must be noted that the Interrupt routine is only responsible for setting the flag and not evaluating the consequences of that flag being set or reset nor is it responsible for clearing those flags. Thus the Interrupt routine is responsible for the sampling of the inputs, the enabling of set and reset flags, the evaluation of the Interlock inputs and the insertion of Faraday cups 10 and 19.

In order to deduce the reset flag the present sample must be compared to the previous sample and if the samples are different (essentially an *XOR* function) and the new sample is a low then that flag must be set. In the case of the set flag the present sample must be compared to the previous sample and if the samples are different and the new sample is high then that flag must be set.

6.3 The error handler.

In the event of an error occurring, the system must first return a safe state and then pass an appropriate error message to an array storing the last 100 errors detected by the system. This routine receives a string from the routine by which it is called. Before loading the string into the array, the messages in the array are shifted up one position and the uppermost string is discarded. The new string is then inserted in the bottom of the array. In addition the Error Handler must also print the most recent error to a line printer to provide a real time hard-copy record of any treatment. The actual display of the array of errors is not the responsibility of the Error Handler but of the operator interface.

6.4 The operator interface.

This subroutine is responsible for the presentation of information to the operator and the processing of keyboard commands. The information presented to the operator on the screen can be divided into 5 windows viz :-

1) Room Clearance Inputs - displays statuses of the inputs of the Room Clearance Subsystem. A *good* condition is represented by green, a *bad* condition by red and a bypassed condition by yellow.
2) Interlock Inputs - displays statuses of the inputs of the Interlock Subsystem. The input conditions are represented as above.
3) Cup Inputs - displays statuses of the inputs of the Cups Control Subsystem. When a beamline device is in the beamline it is represented by green, out of the beamline by red, neither in nor out by white and faulty by flashing red.
4) Error Messages - A scroll window is used to display the error messages received by the system. Although the scroll window can only display 18 messages, all 100 error

messages in the buffer allocated for that purpose can be viewed by scrolling through the buffer by means of the up-cursor and down-cursor keys.

5) Bypass Utility - Used to display and modify the the bypass matrix which is used to bypass any inputs. Those inputs, which may be modified, are displayed in this section in white, those which may be changed are displayed in black. To be able to modify this window (which could have serious consequênces) a particular key sequence must be entered. Once entry into this window has been gained those inputs which may be modified may be reached by using the left, right, up and down cursor keys. The input which is now selected will flash and the bypass input may now be toggled by using the spacekey. To leave the Bypass utility the 'q' key is pressed.

6.5 The room clearance subsystem.

By employing the Petri-net property of hierarchism it is possible to break the Room Clearance subroutine down into smaller and less complex components. The first of these components which will be examined is that which is concerned with the priming and closing of the side doors.

6.5.1 The side doors.

Figure 6.1 is the Petri-net for the two access doors on either side of the beam line (see Figure 6.1). It was mentioned in section 3.2.1.1 that both doors have to be primed and closed within 10 seconds for the Room Clearance Subsystem to be primed for evacuation. Because this component of the Room Clearance Subsystem sets a flag indicating that the doors have been successfully primed and closed it can be represented as an independent component whose relationship with the larger subsection (Room Clearance subroutine) is binary and through that flag.

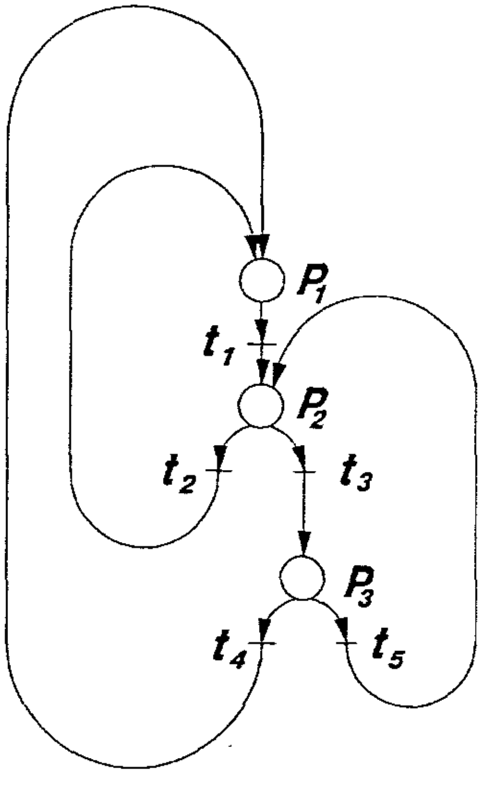


Figure 6.1 The Petri-net for the side doors routine.

Expressed as a Petri-net structure Figure 6.1 becomes :-

$$C = (P, T, I, O)$$

$$P = \{p_1, p_2, p_3\} \qquad T = \{t_1, t_2, t_3, t_4, t_5\}$$

and

$$I(t_1) = \{p_1\} \qquad O(t_1) = \{p_2\}$$

$$I(t_2) = \{p_2\} \qquad O(t_2) = \{p_1\}$$

$$I(t_3) = \{p_2\} \qquad O(t_3) = \{p_3\}$$

$$I(t_4) = \{p_3\} \qquad O(t_4) = \{p_1\}$$

$$I(t_5) = \{p_3\} \qquad O(t_5) = \{p_2\}$$

where :-

p_1="*Door Open*" t_1= "*Door Primed*"

p_2 ="*Waiting*" t_2= "*10 seconds elapsed*"

p_3 ="*Door Closed*" t_3= "*Door Closed, Flag = True*"

t_4= "*Door Opened, Flag = False*"

t_5 = "*Door Primed, Flag = False*"

If the description of the Petri-net begins with the door open and awaiting a prime signal the appropriate marking will be μ_0 = *{1, 0, 0}*. In this case the transition T_1 is enabled. The door is then primed, firing T_1 and the token is passed to the following place P_2 resulting in a marking μ_1 = *{0, 1, 0}*. In this marking transitions T_2 and T_3 are enabled, because this is a deterministic Petri-net (only one token is present). Which transition fires next is not arbitrary but determined by an event. If that event is the 10 second period (during which the door must be closed) elapsing, then the transition T_2 fires and the token will be returned to P_1 and marking μ_0

results. However if the side door was closed within the 10 second period then T_3 fires and the token moves to P_3, enabling transitions T_4 and T_5 and leading to a marking μ_2 = *{0, 0, 1}*. If the door is opened, transition T_4 fires and the token is passed to P_1 and again marking μ_0 results. If the door is primed whilst closed then transition T_5 fires and the token is passed to P_2 and the appropriate marking results.

6.5.2 The room clearance subsystem.

The Petri-net for the remaining Room Clearance System is illustrated in figure 6.2. In this Petri-net there is reference to a known place called *composite*. Composite is exactly as its name describes, a composite of several signals that have been *'anded'* together, for example the two side doors described in section 6.5.1 as well as any other conditions that may have to be satisfied before the room can be primed and cleared.

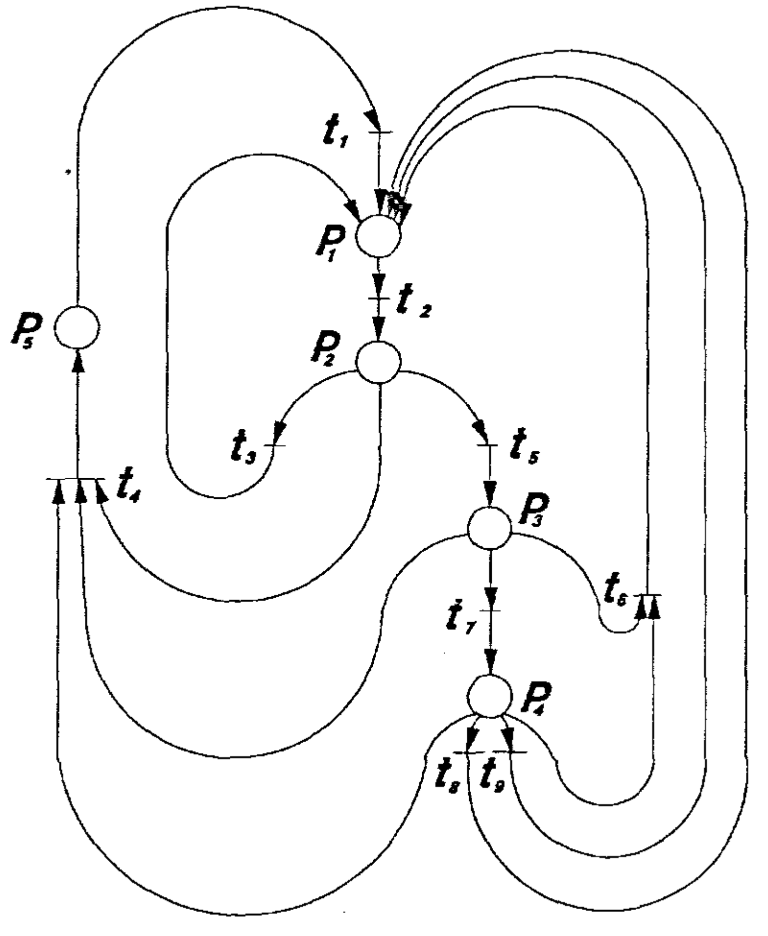


Figure 6.2 The Petri-net for the Room Clearance Subsystem.

The structure of figure 6.2 is :-

$$C = (P, T, I, O)$$

$$\text{where } P = \{p_1, p_2, p_3, p_4, p_5\}$$

$$\text{and } T = \{t_1, t_2, t_3, t_4, t_5, t_6, t_7, t_8, t_9\}$$

where :-

p_1= *"Composite = True"*	t_1= *"Composite passes"*
p_2= *"Room Timing"*	t_2= *"Room is primed"*
p_3= *"Boom' Closed"*	t_3= *"Preset time elapsed"*
p_4= *"Room Cleared"*	t_4= *"Composite fails"*
p_5= *"Composite = False"*	t_5= *"Boom is closed"*
	t_6= *"Boom is opened"*
	t_7= *"Room is armed"*
	t_8= *"Room is disarmed"*
	t_9= *"Light Barriers Failed"*

and the input and output functions are given by :-

$I(t_1) = \{p_5\}$	$O(t_1) = \{p_1\}$
$I(t_2) = \{p_1\}$	$O(t_2) = \{p_2\}$
$I(t_3) = \{p_2\}$	$O(t_3) = \{p_1\}$
$I(t_4) = \{p_2, p_3, p_4\}$	$O(t_4) = \{p_5\}$
$I(t_5) = \{p_2\}$	$O(t_5) = \{p_3\}$
$I(t_6) = \{p_3, p_4\}$	$O(t_6) = \{p_1\}$
$I(t_7) = \{p_3\}$	$O(t_7) = \{p_4\}$
$I(t_8) = \{p_4\}$	$O(t_8) = \{p_1\}$
$I(t_9) = \{p_4\}$	$O(t_9) = \{p_1\}$

The specifications for the room clearance system have been listed previously. We will begin the description of the room clearance subsystem with the composite true and the token in the place p_1 and with a corresponding marking $\mu_0 = \{1, 0, 0, 0, 0\}$. If the room is primed transition t_2 fires. Once this transition has fired the token is passed to the place p_2 and the marking $\mu_1 = \{0, 1, 0, 0, 0\}$ results. When the token is in this place it must remain there until either a preset period has elapsed (in which case transition t_3 fires, returning the token to place p_1 and the marking μ_0) or the composite signal fails (t_4 fires, token to p_5, $\mu_2 = \{0, 0, 0, 0, 1\}$). If t_4 fires, it will remain in the place p_5 until the composite signal becomes true (t_1 fires, returning the token to place p_2 and marking μ_0) or the boom is closed (t_5 fires, passing the token to p_3, $\mu_3 = \{0, 0, 1, 0, 0\}$). When the token is in this place it will remain there until either the composite fails (transition t_4 fires) which passes the token to p_5 (μ_2) or the *Room is Armed* (transition t_7 fires) passing the token to p_4 ($\mu_4 = \{0, 0, 0, 1, 0\}$) or the boom is opened in which case transition t_6 fires passing the token to place p_1 (μ_0). If the token is in place p_4 it will remain so until either the composite fails (t_4 fires) which passes the token to place p_5 (μ_2) or the boom is opened (t_6 fires) or the room is disarmed (t_8 fires) or either of the light barriers fail (t_9 fires) in each case the token is passed to place p_1 (μ_0).

6.6 The cups control subsystem.

This part of the system software is responsible for the extraction of the neutron shutter and Faraday cups 1 and 2 and for requesting the extraction of Faraday cups 10 and 19. It is also responsible for the insertion of Faraday cups 1 and 2 and the neutron shutter (Fig 6.4).

The shutter and Faraday cups can be extracted in one of two modes :- normal mode and test mode. In normal mode the neutron shutter and then Faraday cups 1 and 2 are extracted and finally the extraction of Faraday cups 10 and 19 is requested by the system. In test mode the neutron shutter is extracted then Faraday cup 2 is extracted and finally the extraction of Faraday cups 10 and 19 is requested by the system. Obviously the difference is that Faraday cup 1 is not extracted - this so that an invasive measurement of the beam intensity may be made on Faraday cup 1.

The extraction of the neutron shutter and the Faraday cups can only proceed if all those beam line components are in the beam and the room is cleared and the safety interlock is satisfied. If these conditions are satisfied the system will extract the neutron shutter, thereafter it will check to see if it is in test or normal mode. If the treatment start button is depressed and the system is in test mode then a signal must be sent to the Main Cyclotron Interlock indicating that test mode has been selected. If during the extraction of any of the beam line components either the Room Clearance Subsystem or the Interlock Subsystem should fail then the Cups Control Subsystem should immediately stop extracting the beamline components and begin inserting them. If an irradiation (either normal or test mode) is proceeding then if either of the two abovementioned subsystems should fail then it is the responsibility of the Cups Control Subsystem to begin to insert the beam line components. In this case it must be remembered that it is not the responsibility of the Cups Control Subsystem to remove the request for Faraday cups 10 and 19 this lies with the Interlock Subsystem.

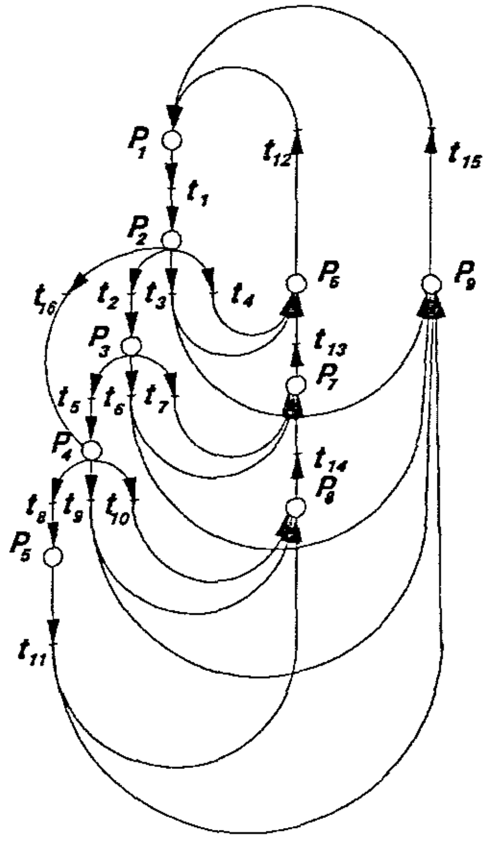


Figure 6.4 The Petri-net for the Cups Control Subsystem.

The structure of Fig 6.4 is :

$$C = (P, T, I, O)$$

$$P = \{p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8, p_9\}$$

$$T = \{t_1, t_2, t_3, t_4, t_5, t_6, t_7, t_8, t_9, t_{10}, t_{11}, t_{12}. t_{13}, t_{14}, t_{15}\}$$

where :-

p_1 = *waiting to start*

p_2 = *extracting neutron shutter*

p_3 = *extracting Faraday cup 1*

p_4 = *extracting Faraday cup 2*

p_5 = *treating*

p_6 = *inserting neutron shutter*

p_7 = *inserting Faraday cup 1*

p_8 = *inserting Faraday cup 2*

p_9 = *room clearance/safety interlock failed*

and :-

t_1 = *start treatment*

t_2 = *neutron shutter extracted in normal mode*

t_3 = *room clearance and/or interlock failure*

t_4 = *neutron shutter failed to extract within window period*

t_5 = *Faraday cup 1 extracted*

t_6 = *room clearance and/or interlock failure*

t_7 = *Faraday cup 1 failed to extract within window period*

t_8 = *Faraday cup 2 extracted/request extraction of faraday cups 10 and 19*

t_9 = *room clearance and/or interlock failure*

t_{10} = *Faraday cup 2 failed to extract within window period*

t_{11} = *room clearance and/or interlock failure/remove request for Faraday cups 10 and 19*

t_{12} = *neutron shutter inserted*

t_{13} = *Faraday cup 1 inserted*

t_{14} = *Faraday cup 2 inserted*

t_{15} = *room clearance and/or interlock failure*

t_{16} = *Neutron shutter extracted in test mode*

and the input and output functions are given by :

$$
\begin{array}{ll}
I(t_1) = \{p_1\} & O(t_1) = \{p_2\} \\
I(t_2) = \{p_2\} & O(t_2) = \{p_3\} \\
I(t_3) = \{p_2\} & O(t_3) = \{p_6,\ p_9\} \\
I(t_4) = \{p_2\} & O(t_4) = \{p_6\} \\
I(t_5) = \{p_3\} & O(t_5) = \{p_4\} \\
I(t_6) = \{p_3\} & O(t_6) = \{p_7,\ p_9\} \\
I(t_7) = \{p_3\} & O(t_7) = \{p_7\} \\
I(t_8) = \{p_4\} & O(t_8) = \{p_5\} \\
I(t_9) = \{p_4\} & O(t_9) = \{p_8,\ p_9\} \\
I(t_{10}) = \{p_4\} & O(t_{10}) = \{p_8\} \\
I(t_{11}) = \{p_5\} & O(t_{11}) = \{p_8,\ p_9\} \\
I(t_{12}) = \{p_6\} & O(t_{12}) = \{p_1\} \\
I(t_{13}) = \{p_7\} & O(t_{13}) = \{p_6\} \\
I(t_{14}) = \{p_8\} & O(t_{14}) = \{p_7\} \\
I(t_{15}) = \{p_9\} & O(t_{15}) = \{p_1\}
\end{array}
$$

The description of this Petri-net begins with the token present in the place p_1 and with an initial marking μ_0 = *{1, 0, 0, 0, 0, 0, 0, 0, 0}*. If the start button is depressed whilst in this marking transition t_1 fires and the token is passed to place p_2 and a marking μ_1 = *{0, 1, 0, 0, 0, 0, 0, 0, 0}* results.

When transition t_1 fires a command is sent to the Cups Control Subsystem ordering the extraction of the neutron shutter. The token will reside in place p_2 until either the shutter has successfully extracted or a predefined period has elapsed or either the Interlock or the Room Clearance subsystems fails. In the event of the shutter extracting one of two transitions may fire. If test mode has been selected transition t_{16} will fire passing the token directly to place p_4 and marking μ_5 = *{0, 0, 0, 1, 0, 0, 0, 0, 0}* (bypassing place p_3 and the request to extract Faraday cup 1, thereby leaving that Faraday cup in the beam for invasive beam current measurements. If normal mode is selected then transition t_2 fires passing the token to place p_3 and marking μ_2 = *{0, 0, 1, 0, 0, 0, 0, 0, 0}* results. If transition t_3 fires, two tokens are passed, one to p_6 where it will remain until the shutter has been inserted and one to p_9 where that token will remain until either the room has been cleared or the interlock has been satisfied. This is marking μ_3 = *{0, 0, 0, 0, 0, 1, 0, 0, 1}*. If either the room clearance fails or the interlock fails then transition t_4 fires and a single token will be passed to p_9 with the marking μ_4 = *{0, 0, 0, 0, 0, 0, 0, 0, 1}*. In the event of either transitions t_3 or t_4 firing a signal is sent to the cups control system inserting the neutron shutter.

When transition t_2 fires a signal is sent to the cups control system ordering the extraction of Faraday cup 1. The token is now in place p_4 and awaiting either the successful extraction of Faraday cup 1 (t_5 fires passing the token to p_4 and resulting in marking μ_5 = *{0, 0, 0, 1, 0, 0, 0, 0, 0}*) or the failure of either the room clearance system or the safety interlock system (t_6 fires, two tokens are passed, one to p_7 and one to p_9 and marking μ_6 = *{0, 0, 0, 0, 0, 0, 1, 0, 1}*) or the predefined window period to elapse (t_7 fires passing the token to p_7 and marking μ_7 = *{0, 0, 0, 0, 0, 0, 1, 0, 0}*). When either transition t_6 or t_7 fires a signal is sent to the cups control system inserting Faraday cup 1.

When transition t_5 fires the order of things is very similar to the preceding paragraph, a signal is sent to the cups control system ordering the extraction of Faraday cup 2. With the successful extraction of this Faraday cup transition t_8 fires passing the token to place p_5 and μ_8 = *{0, 0, 0, 0, 0, 0, 0, 1, 0}* results. If however either the room clearance or safety interlock fails then transition t_9 fires, passing two tokens, one to p_8 and one to p_9 in which case marking μ_9 = *{0, 0, 0, 0, 0, 0, 0, 1, 1}* results. The final option is if the timeout window of this Faraday cup is exceeded in which case transition t_{10} fires passing the token to place p_8 with marking μ_{10} = *{0, 0, 0, 0, 0, 0, 0, 1, 0}*.

If transition t_8 fires then a signal is sent to the main cyclotron interlock requesting the extraction of Faraday cups 10 and 19 after which the token is passed to place p_5 and the system is considered to be *treating*. The token will reside in this place until either the safety interlock or the room clearance fails or the treatment stop button is depressed in which case the transition t_{11} fires passing the token to two places p_8 and p_9 with the resultant marking μ_{11} = *{0, 0, 0, 0, 0, 0, 0, 1, 1}*. In addition the request to the main cyclotron interlock for the extraction of Faraday cups 10 and 19 is removed resulting in their insertion and the termination of the beam delivery.

When two tokens are present (always in place p_9 and either place p_8 or p_7 or p_6) these two tokens will remain until they are in places p_9 and p_6 similtaneously (marking μ_3 = *{0, 0, 0, 0, 0, 1, 0, 0, 1}*). When both t_{12} and t_{15} fire and the two tokens will recombine and be passed to p_1 where we began. In order to reach the marking μ_3 from marking μ_{11} (or for that matter from markings μ_3 or μ_6) transition t_{14} must fire (Faraday cup 2 must have inserted successfully) and a signal is sent to the Cups Control Subsystem inserting Faraday cup 1 and the token is passed to p_7 where it will remain until Faraday cup 1 has inserted. When Faraday cup 1 has inserted transition t_{13} fires passing the token to place p_6 and sending a signal to the Cups Control Subsystem ordering the insertion of the neutron shutter. Upon the successful insertion of the neutron shutter transition t_{12} fires passing the token to p_1. When both the safety interlock and room clearance systems are satisfied transition t_{15} fires passing the token to place p_1. When both tokens are present in place p_1 then the system is ready to treat again.

Chapter 7

Discussion

7.1 General.

In chapter 2 methods such as diverse development were discussed. In a project of this nature with limited financial resources, time and labour, these methods could be discounted. The option of several teams each developing software and hardware to identical specifications is a luxury only afforded larger companies.

7.2 Implementation of software.

Figure 7.1 is a printout of the operator interface screen which was captured without hardware connected to the system. It can be seen from this printout that the operator interface screen is divided into 4 major subsections.

7.2.1 Composite signals.

The first of these subsections shows the status of the composite signals inputs and is intended to assist faultfinding. The **RMCLR** input will be green if the room has been cleared and red if the room is not cleared. Likewise the **ILOCK** input will be green if the interlock is satisfied and red if the interlock is not satisfied. The inputs **SHTTR**, **FCUP1**, **FCUP2** and **FCP19** show the statuses of the beamline components. A red indicates that the device is out of the beam, a green indicates that the device is in the beam and a white indicates that the device is neither in the beam nor out of the beam (that is the device is moving).

7.2.2 Treatment mode

Because each patient requires several unique beamline components, a system was required that ensured that the correct components were being used for that particular patient. For this reason a patient database system was developed. After editing and verifying (to ensure that the correct components were specified) the database transmits codes for those unique components to a barcoding system. The associated barcode decals (which are fixed to the components) are then scanned, and if correct , confirm to the patient database that this is so. After confirmation, the patient database informs the interlock and control system that treatment may commence.

There are two modes of treatment, *Bragg peak* and *crossfire*. The patient database is capable of discriminating between these modes and informs the interlock which mode is selected. If the combination is correct, treatment may commence. However if the combination is incorrect the operator must be informed.

7.2.3 Alarms and information.

This is the region in which all the error messages are displayed as discussed in section 6.3. The error message displayed in figure 7.1 informs the operator that the system has been started. This region can display up to 18 messages with the most recent error display in yellow at the bottom and all other

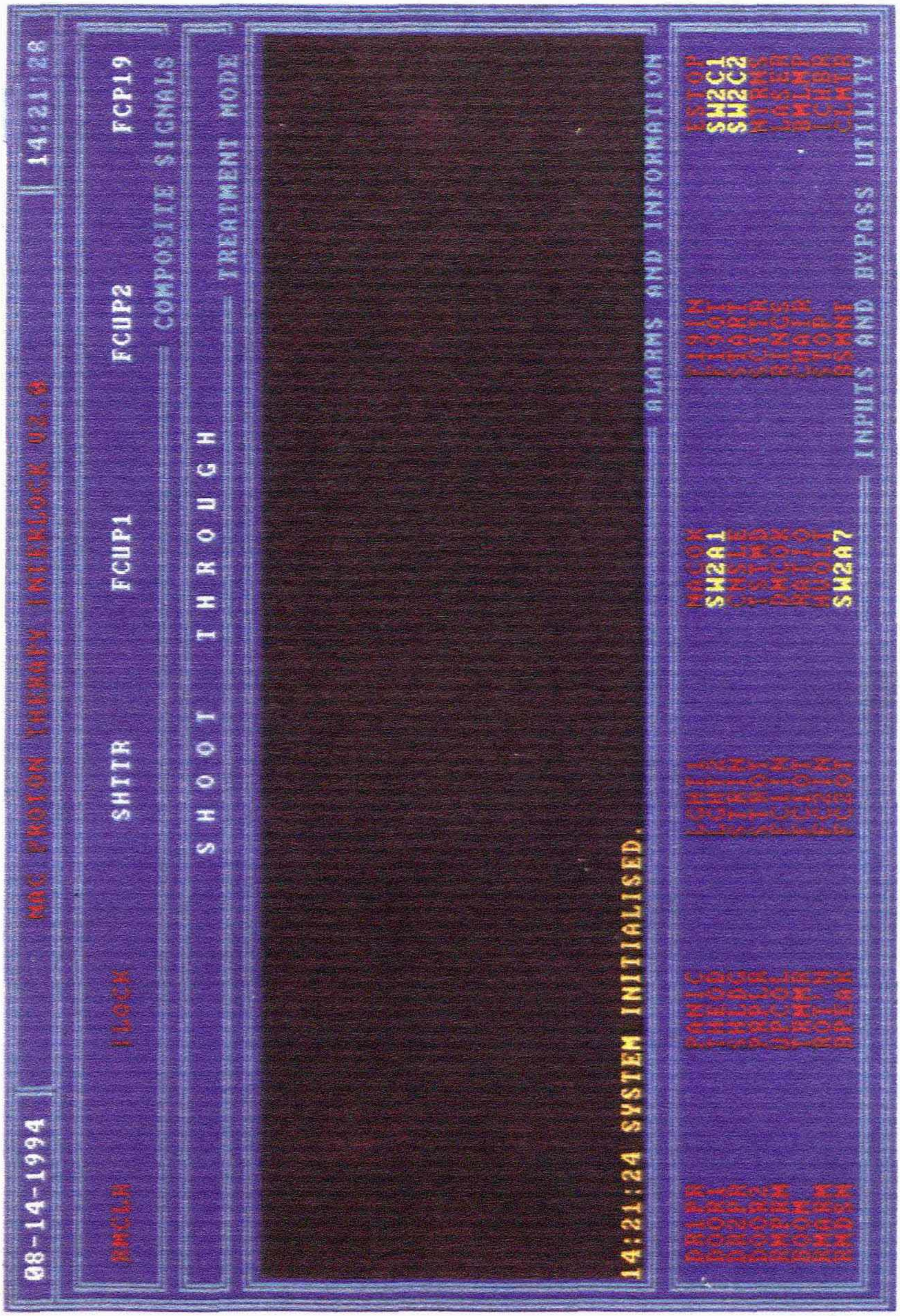


Figure 7.1 Printout of the operator interface screen.

messages displayed chronologically from top to bottom in white. The operator may scroll through these messages using the up arrow key to go backwards in time and the down arrow key to go forward in time.

7.2.4 Inputs and bypass utility.

The *'raw'* inputs are displayed in this region. It serves to isolate any errors indicated by either the composite signals region or the alarms and information region. Correct conditions are displayed in green and bad in red.

If an input is to be overridden then the operator must enter a key sequence and a cursor will appear indicating which input is selected. The selection may be changed using the up, down, left and right arrow keys. An input may be overridden by depressing the space bar on the selected input. When an input is overridden it will appear in flashing green. To exit the bypass utility the 'Q' button must be depressed.

Chapter 8

Conclusions

1. The neutron therapy system was successfully duplicated on a personal computer.
2. The decision to pursue a software orientated solution was amply justified by the continuously changing requirements of the operators.
3. The decision to use Petri-nets was questioned at times during the development · (a deterministic Petri-net exhibits very similar characteristics to a conventional flowchart) and it was only when the cups control subsystem model (the only non-deterministic Petri-net) was being developed that the benefits of Petri-nets became apparent. Because several tokens can exist simultaneously in a non-deterministic Petri-net it becomes evident that each token can be considered representative of a thread (process) in a multi-tasking operating system [Fr94].
4. The subdivision of the system was not as simple as it initially appeared. The low energy beamline Faraday cups (Faraday cups 10 and 19) control was split between the cups control and interlock subsections. During operation it was noticed that it was desirable to include some of the interlock components in the room clearance subsystem to avoid arming the room and then noticing that the interlock subsystem was not satisfied. These examples resulted in the distinction between the subsections being blurred.

5. Once familiar with 'C' the translation from Petri-nets to source code presented no problems.

6. In section 3.4 the timing requirements of the system were discussed. At the outset of the design the interrupt routine was driven by the clock tick interrupt. This interrupt occurs with a period of 50.4 ms. However, when testing, a dose overrun was experienced. In a single irradiation this overrun could be deemed negligible, but in the case of a patient receiving several irradiations the cumulative overrun might become significant. Thus it was necessary that this overrun be decreased to as small a value as possible. The R.F. division at N.A.C. developed an electrostatic beam deflector (situated in the low energy beam-line) that was to be activated by a command sent from the Main Cyclotron Interlock System. The Main Cyclotron Interlock System has a sampling period of 20 ms and requires a signal to terminate an irradiation from the Proton Therapy Interlock and Control System within that period. A prototype card, generating pulses with a 15.6 ms period was constructed and the software modified to accommodate this interrupt signal.

References

Br04 **Bragg, W.H. and Kleeman, R.** On the Ionisation Curves of Radiation. Phil Mag, 8, 726-738, 1904

Bu93 **Burger, S.J.** Private communication. 1993.

Fo81 **Fowler, J.F.** Nuclear Particles in Cancer Treatment. Adam Hilger (1981)

Fr94 **Franklin, E.J.S.** Private communication. 1994.

Ja90 **Jacky, J.** Proceedings of the ACM SIGSOFT InternationalWorkshop on Formal.Methods in Software Development. Napa, California, May 1990, 9-11.

Jo87 **Joyce, E.** Software bugs: A Matter of Life and Liability. Datamation. pages 88-92 May 15 (1987).

Jo89 **Jones, D.T.L.** Particles for Patients. Nuclear Active. 40, 30-36 (1989).

Le87 **Leveson, Nancy G. and Stolzy, Janice L.** Safety Analysis Using Petri Nets. IEEE Transactions on Software Engineering, Vol SE-13, No. 3, March 1987.

Le91 **Leveson, Nancy G.** Software Safety in Embedded Systems. Communications of the A.C.M., February 1991.

Pe77 **Peterson, J.L.** Petri Nets. Computing Surveys. Vol 9, No 3, September 1977.

Ra80 **Raju, M.R.** Heavy Particle Radiotherapy. Academic Press (1980).

Re88 **Reitmann, D.** From Promise to Proof. Nuclear Active. 39, 13-16, (1988).

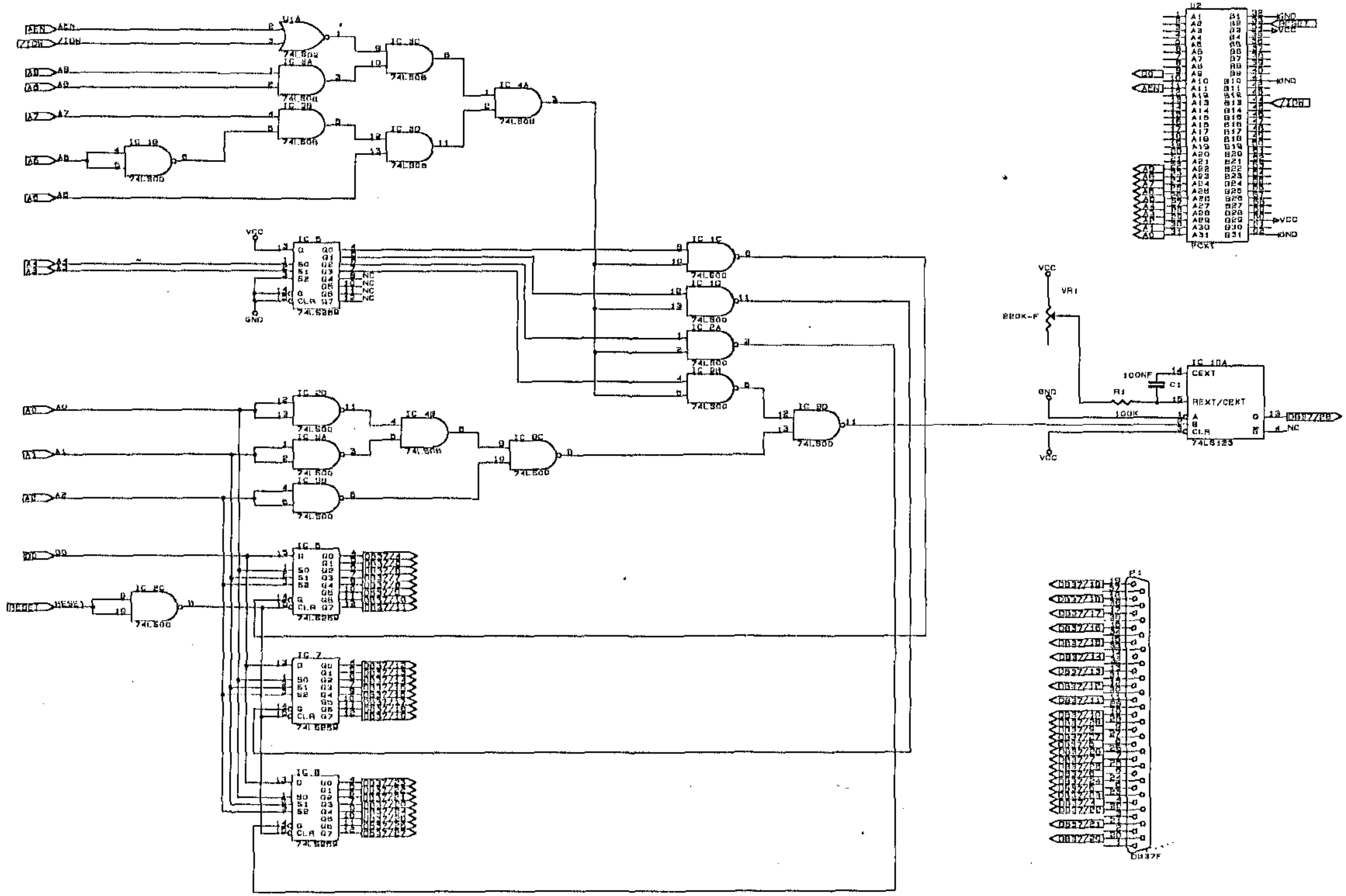
Ro89 **Robinson, L.P.G.** Preliminary Investigation of a Possible Dose-Rate Effect on Survival of Cells Irradiated With Low Energy Protons. M.Sc Thesis. University of Cape Town (1989).

Th89 **Thomas, M.** Can Software be Trusted? Physics World. 30-33, October 1989.

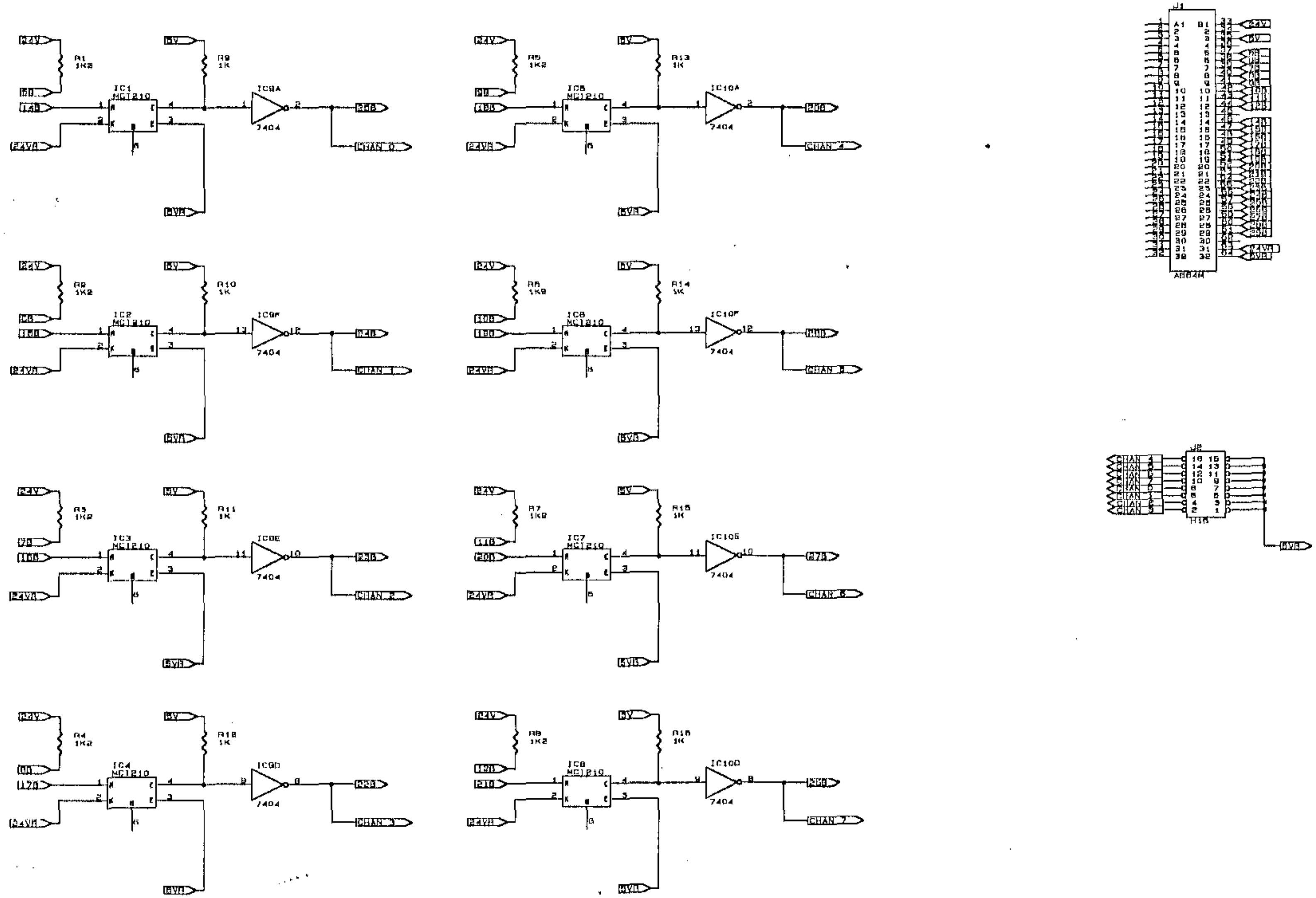
To52 **Tobias, C.A. Anger, H.O. and Lawrence, J.H.** Radiological use of High Energy Deuterons and Alpha Particles. Am. J. Roentgenol. Radiati Ther Nucl. Med. 67, 1-27, 1952

V91 **van der Vlugt. G.** The Development of a Real Time Photogrammetric System for Patient Positioning in Proton Therapy. M.Sc. Thesis. University of Cape Town (1991).

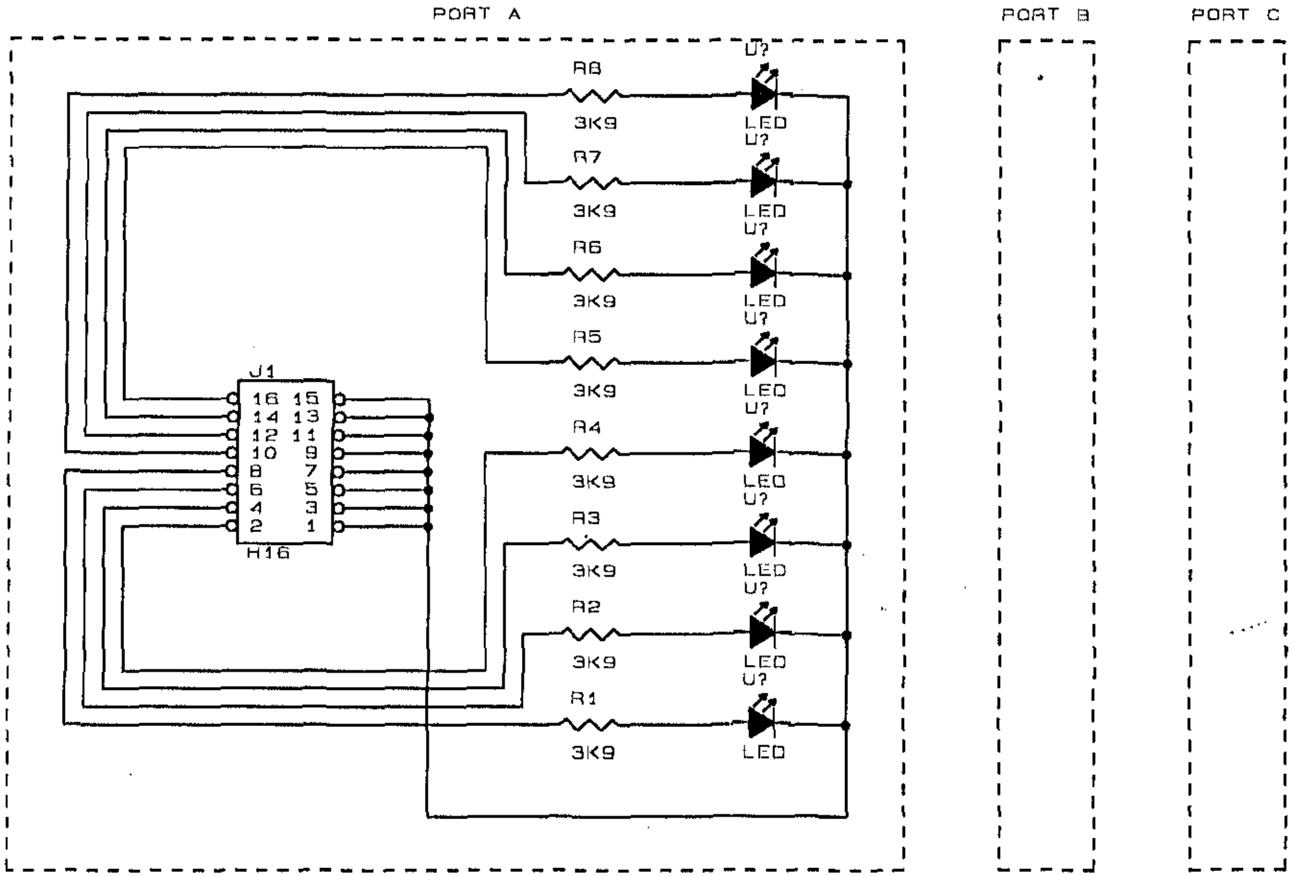
Wi46 **Wilson, R.R.** Radiological use of Fast Protons. Radiology, 47, 487-491, 1946.



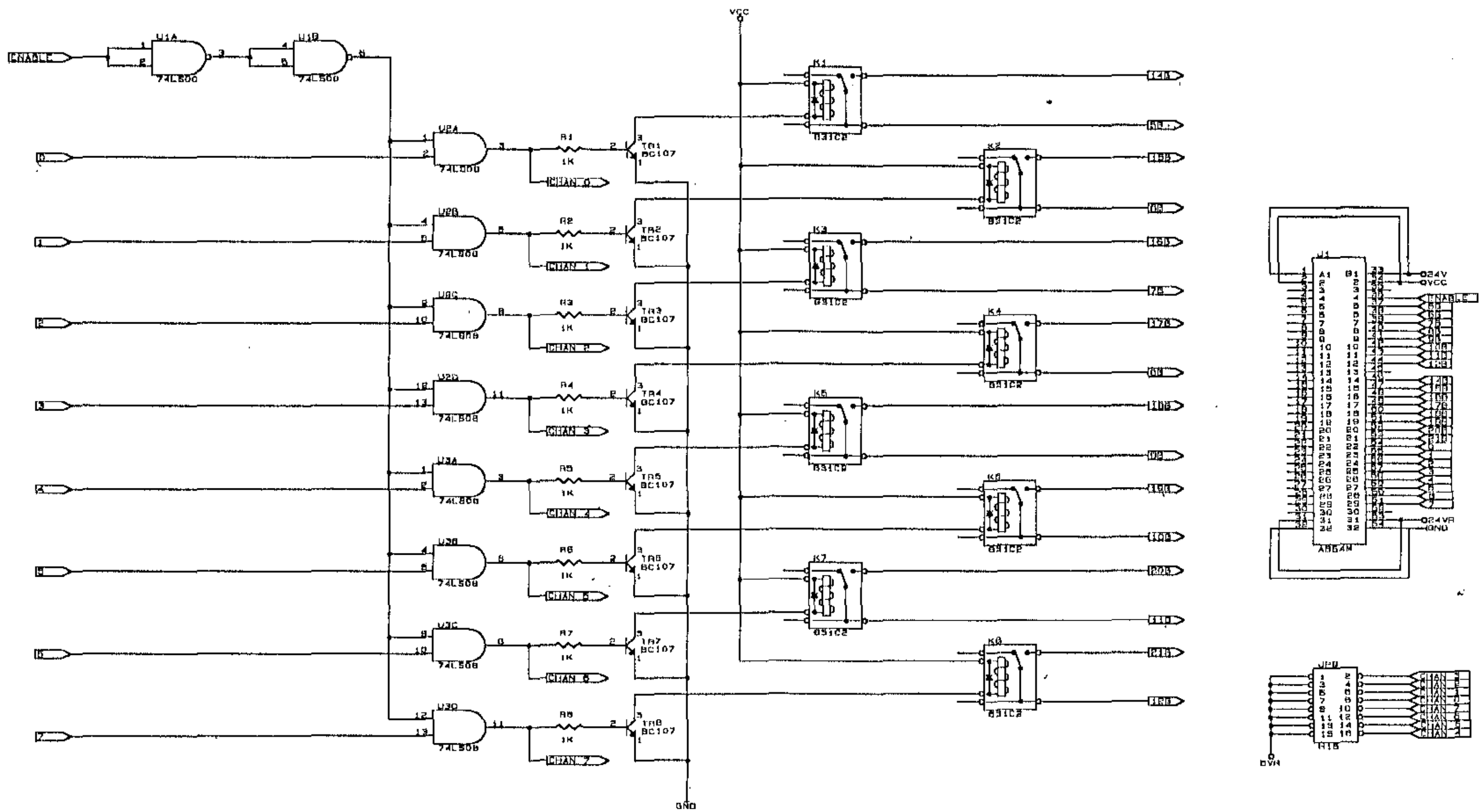
Title	INTERLOCK OUTPUT CARD FOR PC	
Size C	Document Number: T.J. FULCHER	REV



Title		
INPUT BUFFER FOR PROTON INTERLOCK		
Size: C	Document Number: TJF 1991	REV: 01
Date: January 20, 1994	Sheet	of

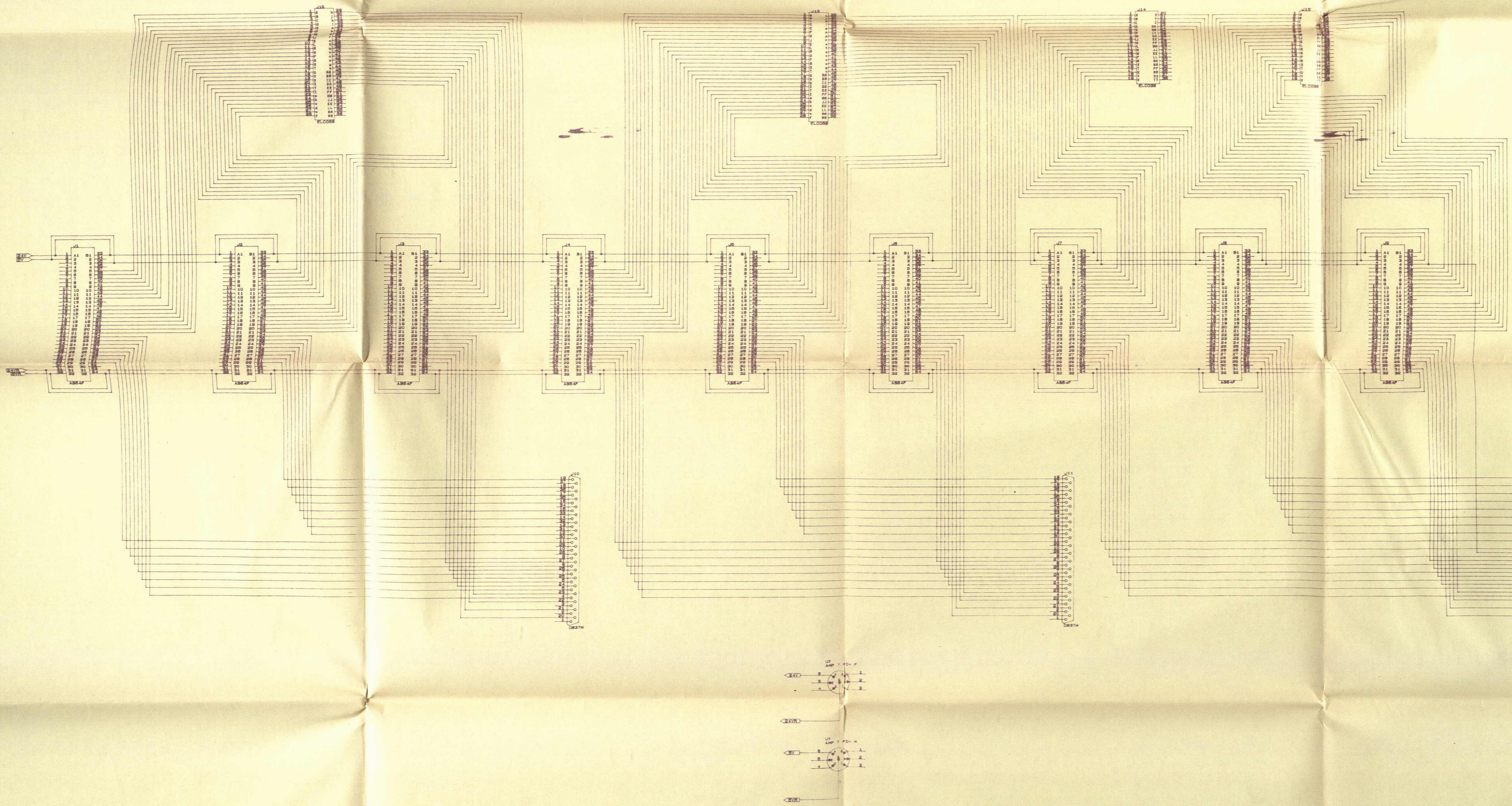


Title INPUT PANEL FOR INTERLOCK INTERFACE		
Size A	Document Number TIM FULCHER	REV
Date: January 28, 1994	Sheet of	



Size	Document Number	REV
C		

Date: January 20, 1994 Sheet of



Title		
PROTON THERAPY INTERLOCK INTERFACE BACKPLANE		
Size	Document Number	REV
E	TIM FULCHER	
Date: January 27, 1994	Sheet	of