Solution Monitoring As A Nuclear Materials Safeguards Tool

By

Stephen John Scothern

B.Sc., M.Sc.

A thesis presented to the University of Glasgow, in fulfilment of the requirements of the degree of Doctor of Philosophy

Centre for Systems and Control
Department of Mechanical Engineering
University of Glasgow

September 1998

Research Supervisor : Dr. J. Howell

ACKNOWLEDGEMENTS

The work presented in this thesis has progressed over more than 5 years with contributions from many individuals.

I would like to express my great appreciation to my supervisor, Dr. John Howell, who has continually provided advice, guidance and encouragement during the course of this research.

I am grateful to many members of the International Atomic Energy Agency for their helpful insight during the development of the system, in particular, Dr. Dieter Sellinschegg (SGPSA) for making numerous suggestions about the direction of the work, Mr. Freddy Franssen (now retired, formerly of SGCP) for supplying our first set of data and providing patient descriptions of what goes on in tanks, and Dr. Tom Shea (SGOA) for actively and enthusiastically supporting the concept, especially the use of G2.

I would also like to thank several members of the Los Alamos National Laboratory who have supplied valuable knowledge and input during the research; Dr. Tom Burr and Dr. Larry Wangen for numerous discussions about the role and structure of solution monitoring, and Dr. Alton Coulter for the use of his simulations.

Many thanks also go to the UK R&D Support Programme To The IAEA, for supporting the work and to the United Kingdom Atomic Energy Agency, in particular to Dr. Maurice Ward for enabling the finances, and to Dr. Bryan Patrick for supplying useful data.

Thanks also to Dr. Brian Hunt at JRC, Ispra, for access to his tank data.

I would also like to thank the staff of the Department of Mechanical Engineering for all of the help and assistance they have provided during my time at Glasgow University.

Special thanks to Tracey Black, my parents, and other members of my family, for the endless support, motivation and encouragement they have given me.

For Tracey

ABSTRACT

The work presented in this thesis describes a solution monitoring system that has been developed to assist United Nations' inspectors performing nuclear materials safeguards, primarily pertaining to plutonium storage and nuclear fuel reprocessing facilities. Based on the concept of the 'event', which is essentially any process that occurs on the plant, it aims to construct a hypothesis of which events have actually occurred, and to decide if any of these have safeguards implications. The package developed is robust, portable, and easy to use.

The system has been implemented in G2 with extensive call-outs to FORTRAN and C routines. Sensor data from the plant is first analysed, and salient features (sub-events) are extracted. A model based diagnostic algorithm is then used to determine all possible causes of these sub-events; based on topographical knowledge of the plant, this makes extensive use of a simulation model. A rule based system then examines permutations of these sub-events and diagnoses, to find all possible events which could explain the data. From the possibilities generated, the most likely events are chosen on the basis of user specified subjective probabilities and on supporting evidence; these probabilities reflect the view that some events are more likely to be acceptable to the operator than others. Bayesian evidential updating methods are used to achieve this.

An automatic model generator is presented, which extends the portability and applicability of the diagnostic aid, and makes implementation a great deal easier. Amongst other things, this enables simulations to be constructed automatically using a library of unit process models. The nature and forms of the various user interfaces are discussed. In particular facilities are available for creating and maintaining databases of rules which are used to identify, classify and rank the events.

The system has been tested using data from a number of plants, both hypothetical and real. The primary test facilities have pertained to plutonium nitrate solution storage areas. A hypothetical solvent-extraction and concentration facility has also been considered, to extend the range of applicability of the system. These studies have demonstrated that solution monitoring has the potential to be a valuable aid for inspectors responsible for nuclear materials safeguards.

The diagnostic algorithm has been revised to accommodate gross non-linearities in the simulation. The original regression algorithm has been supplemented by three additional options, namely Powells method, the Downhill Simplex method, and repeated iteration of the regression algorithm. Existing facilities for the reduction of large search spaces, which make use of aligned vectors, have been improved.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

NOMENCLATURE

Variables and symbols:

A	Event
C	Concentration
c	Pipe or common header
Cp	Specific heat capacity
D	Diagnosis
E	Set of events, event, evidence, rate of mass reduction due to evaporation
f_d	Desired plutonium flow rate
H+	Molarity
h	Specific enthalpy, hidden inventory
i	Inlet
J	Jacobian matrix
K	Proportional gain
k_l	Full load inventory
L	Level, load
l	Diptube reading
M	Mass
n	Node or tank
o	Outlet
p	Sample pot
P_k	Subjective covariance matrix
Pu	Plutonium
Q	Mass flowrate
R_k	Measurement vector covariance
S	Set of all possible explanations of all movements through the plant
SE	Set of sub-events, or sub-event
T	Temperature
t	Time
tol	Tolerance value
V	Volume, perturbation multiplier
V_i	Set of variables pertaining to all possible diagnoses of sub-event SE_i
x	State, mass fraction
y	Measurement
λ	Distance
ρ	Density
θ	Re-distribution variable
σ	Standard deviation
ψ	Heat input from delivery system
τ	Integral time constant

Subscripts:

d	Density
f	Finish
fg	Evaporation
ho	Heater out
hi	Heater in
l	Level
liq	Liquor
m	Measured
p	Pipe
Pu	Plutonium
r	Reference
s	Start, tank
t	Dip tube
w	Water

Superscripts:

~	Estimated
$\wedge$	Measured
*	Compound, corrected

CHAPTER 1

1. INTRODUCTION

1.1 Overview

The problems of safeguarding nuclear material in the chemical processing areas of a large nuclear fuel reprocessing plant are well-documented (LASCAR, 1992). Burr and Wangen (1996b) have pointed out that, in the case of the planned Rokkasho Reprocessing Plant (RRP), the annual material balance standard deviation based on traditional monthly accounting will be too large to meet the protracted loss detection goal specified by the International Atomic Energy Agency (IAEA). Thus there is a need for systems that enhance the conventional accountancy approach and one possible enhancement is to monitor solutions containing fissile material as they progress through the plant. To be more specific, because of the quantities involved, this means the monitoring of plutonium nitrate largely in tanks, and, to a lesser extent, in process units.

This thesis describes most of the key features of a data analysis system that has been developed to achieve this. The system is based on the premise that a computer simulation can be constructed to represent the nuclear materials inspector's understanding of what is actually happening on the plant; from an inspector's point of view, residuals, generated by comparing simulation predictions with plant data, then represent anomalies which might signal potential difficulties from a nuclear materials perspective. The anomalies can then be diagnosed on the basis of the model and on other knowledge that might be available. Thus the emphasis is on modelling and on the analysis of residuals. This is not simple; there are issues of modelling, of detection and diagnosis, a complete set of boundary conditions is needed to solve a computer model of the plant and it is not clear how to specify 'potential difficulties' *apriori*. To ameliorate the last two issues it is proposed to add an additional conceptual strand, that of the *event list*. Essentially the event list is the inspector's

understanding of plant activity and therefore is the primary source of information when constructing boundary conditions for the simulation. To elaborate on these ideas a little, consider the user interface shown in Figure 1.1.

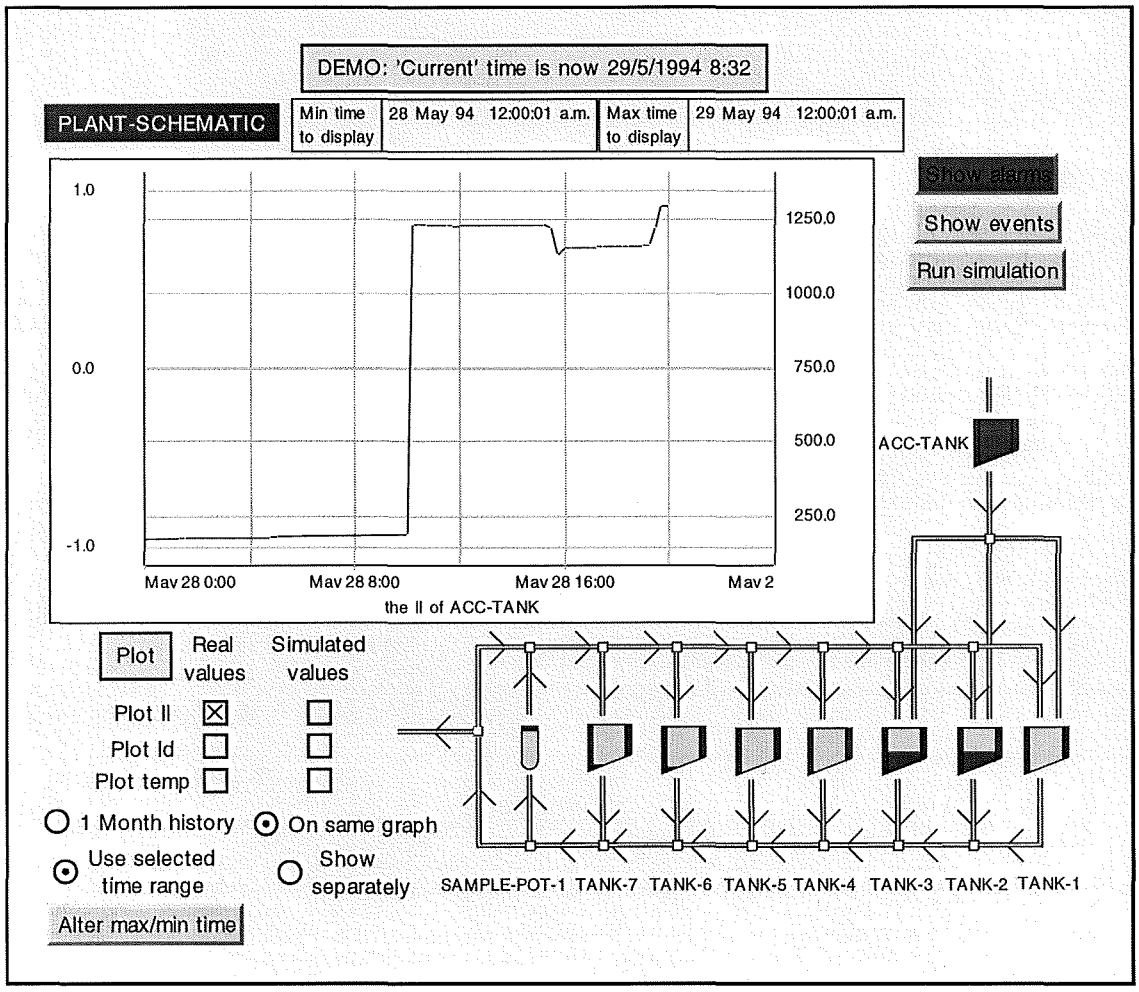


Figure 1.1: Main window showing plant schematic

This shows the main window of the G2 (Gensym) implemented user interface that has been developed as part of a solution monitoring system for a product storage facility. The idea is that the inspector would access the system on a daily basis; there are a number of key features:

- an animated schematic (bottom right) showing the solution levels present in each tank;
- a graphical window to display measurements obtained during a given period of time; measurements pertaining to any process unit can be displayed by clicking on the appropriate part of the schematic and on the graph buttons (bottom left); observe that simulation predictions can be superimposed on request;
- the ability to perform a simulation on request; residuals are generated and tested automatically, the background of the simulation button (denoted by MATCHED) will turn red if there is a mismatch, green if not;
- buttons to 'Show events' (i.e. the event list) and to 'Show alarms' i.e. those activities or events in need of further investigation. An example of an event list is shown in Figure 1.2;
- this leads to other windows that enable the inspector to interact with the system so that it can be updated with the inspector's understanding of what has happened.

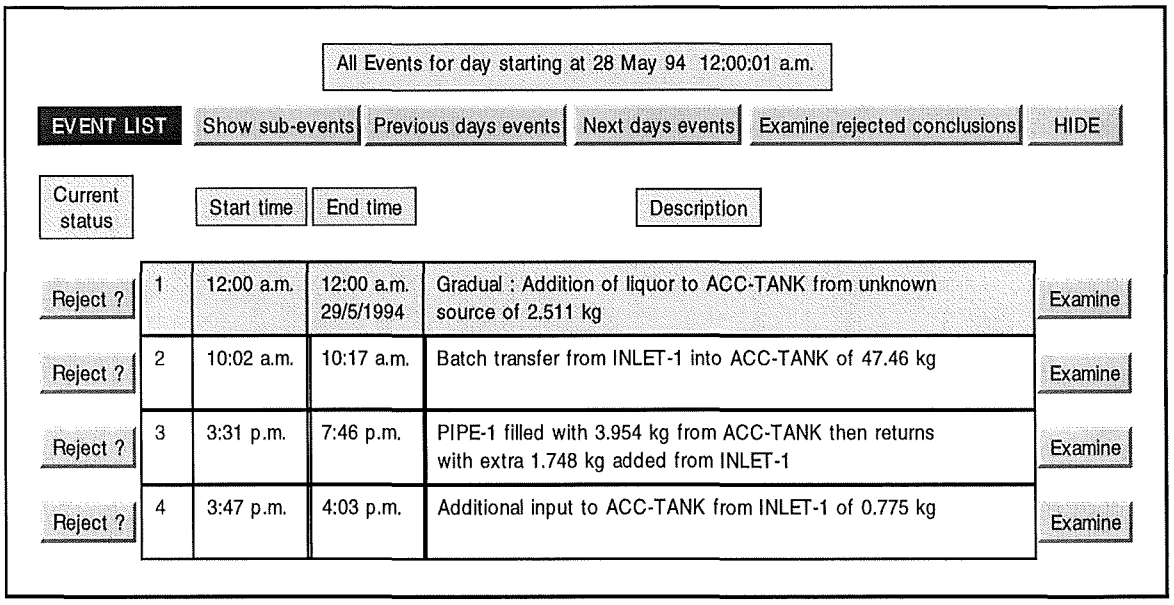


Figure 1.2: An event list

To summarise, the system has a number of conceptual strands: simulation, the generation of events and alarms, and user interaction. In addition, for the system to be practical, it must be transparent, robust, portable and easy to use. As far as possible the diagnostic methods should also be lateral rather than procedural, since if the procedure used is known, methods of avoiding detection can be devised.

Although this thesis describes the data analysis system that now exisits, it is worth noting that its development was somewhat evolutionary in nature. By analysing plant data, initial work focused on the model-based detection and diagnosis of anomalies that pertained to the product storage area where concentrated plutonium nitrate solution is stored. The work described in this thesis mostly pertains to this application although an update pertaining to chemical processing areas, more generally, is given in the penultimate chapter, Chapter 5. The rest of this chapter is given over to expanding on the above: the need for the system is addressed more fully in Section 1.2; a description of the different types of events that need to be examined by the system is given in Section 1.3; by referring to a simple example, the most important features of the system are summarised in Section 1.4 and, wherever possible, the role of subsequent chapters is explained; the need for the available data to be pre-filtered is discussed in Section 1.5; the original work needed to realise this system is then itemised in Section 1.6.

1.2 Need For The System

1.2.1 Nuclear Safeguards

Considerable effort is expended by the nuclear community to ensure the security of nuclear materials (IAEA, 1987, Dekens et al, 1995). The managers of plants handling nuclear material, national bodies overseeing the activities of such plants, and international agencies who are charged with implementing various international treaties all have an interest in safeguarding the nuclear materials. A primary focus of nuclear safeguards involves the timely detection of an attempt to divert a 'significant' quantity of fissile material from a civil nuclear facility (The Treaty on the Non-Proliferation of Nuclear Weapons, IAEA, 1992). The exact definitions of timely and significant are determined by various government policies, (see, for example, Islam et al, 1993), but by 'timely' we mean of the order of a week, and a 'significant' quantity is the same amount of material irrespective of whether the plant in question is large or small, and is an extremely small proportion of the inventory on a large facility (like THORP; see, for example, The Health and Safety Executive, 1995).

1.2.2 Practical Considerations

Most of the countries of the world have agreed to allow inspections of their nuclear facilities by the International Atomic Energy Authority (IAEA), which is a branch of the United Nations. The inspectors visit plants to assure themselves that material has not been diverted.

Although the countries have agreed in principle, there is sometimes conflict between the operators and the inspectors caused by this imposition. The inspectors might be forced to deal with what we might call information poor plants: for reasons of confidentiality and of cost, plant operators may be unwilling to disclose certain plant data or plant design information and plants are often lacking in certain instrumentation that would be desirable in an ideal case, for instance it might be desirable for all storage tanks to be equipped with density measurement devices.

1.2.3 Near Real Time Materials Accountancy (NRTA)

Many methods are employed by the inspectors to ensure that nuclear material is not diverted, see for example, Shipley, (1978), Ikawa et al, (1983), and IAEA, (1987). One of the major methods is known as 'materials accountancy' and in conventional systems this involves dividing the plant into a number of regions. The net transfers through each region are then measured to obtain book inventories of the material that should be present within the region, which can then be compared with actual physical inventory measurements at the end of a balance period, to determine values for the material unaccounted for (MUF). These MUF values can then be examined, (see, for example, Jaech, 1974, or Annibal and Roberts, 1989), to test if the values are significant. One of the main improvements to conventional materials accountancy is to keep an accurate and *frequently* updated account of the material contained in the plant. The balance obtained by adding the net flows into the plant can be *frequently* compared with the total obtained by actually measuring the plant inventory, and various statistical methods can be applied to detect diversions of material (Burr et al, 1995). Known as near real time accountancy (commonly abbreviated to NRTA), this process is limited by the rate at which it is practicable to form an account; the term 'near' relates to the fact that there is often a delay getting samples back from laboratories, to establish chemical composition for example.

1.2.4 Plant Monitoring And Alarm Analysis

For various reasons, accounts formed using NRTA are likely to be often in error (Speed and Chulpin, 1986), generating alarms which will need analysing. There might also be other anomalies in plant data, which, although they do not trigger the alarm conditions, they are nevertheless worth investigating, as they can help to determine what processes are actually being carried out by the plant operators, and give insight into the plant conditions and operations.

1.2.5 Solution Monitoring

Solution monitoring is defined for safeguards purposes in Burr and Wangen (1996b) as *'the essentially continuous monitoring of solution in all tanks in the process which contain, or could contain safeguards significant quantities of nuclear material'*. The role that solution monitoring could play in assisting the safeguarding of nuclear material is also discussed by Burr and Wangen, (1996a), and suggestions where such monitoring may be used include :

1. the provision of data for verification of operator declarations of plant operation;
2. design verification assurance;
3. consistency checks on transfers between monitored tanks;
4. continuously updated inventories of nuclear material;
5. identification of all normal process events;
6. identification of abnormal events;
7. estimation of unmeasured hold-ups in pipes connecting tanks.

Although the system described here might be adapted to meet all these aims, the focus is largely on item 5, other items e.g. 3 and 7 are covered incidentally. Thus the emphasis is on events: what is an event, how does one re-construct all events from plant data and so on.

1.3 Events And Their Effects In General

The term 'event' encompasses anything which can be occurring within the plant, from ordinary occurrences such as transfers between tanks and sampling, to measurement sensor drift and even deliberate diversion of nuclear material by any method. Most physical events on the plant can be categorised as either abrupt or gradual. Abrupt events can be decomposed in to one or more sub-events: a single sub-event can represent a transfer from a tank out of the plant, whereas multiple sub-events are needed to represent a recirculation where material temporarily leaves a tank and returns some time later. Figure 1.3 shows examples of typical abrupt events. They can be classified as 'abrupt' because the individual sub-events have a relatively short duration, and the majority of this thesis focuses upon this type of event. Gradual events are classified as long term trends in the data, that are in a single direction, such as calibration errors, or leaking valves, an example of which is shown in Figure 1.4. Specific details regarding the diagnosis of gradual events are given in Section 2.12. Other events may have features that pertain to one or more abrupt or gradual events, for instance an event may be long term but may vary in direction over time, any such events are called 'hybrid' events, an example of which is shown in Figure 1.5. Section 2.13 details the process by which hybrid events can be diagnosed, and an example of such an event and the methods of its diagnosis are given in Section 2.14.

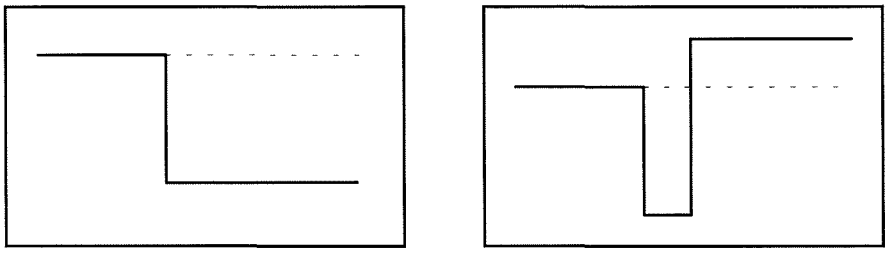


Figure 1.3: Examples of abrupt events, with single and multiple sub-events

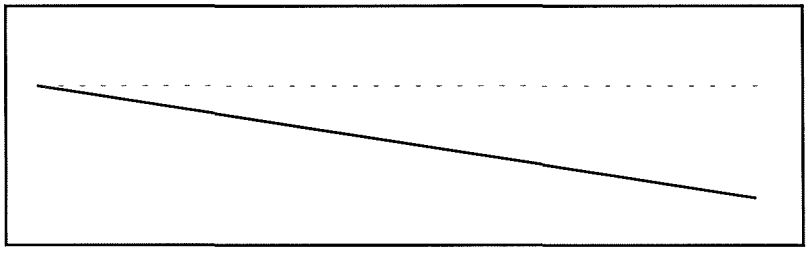


Figure 1.4: Example of a gradual event

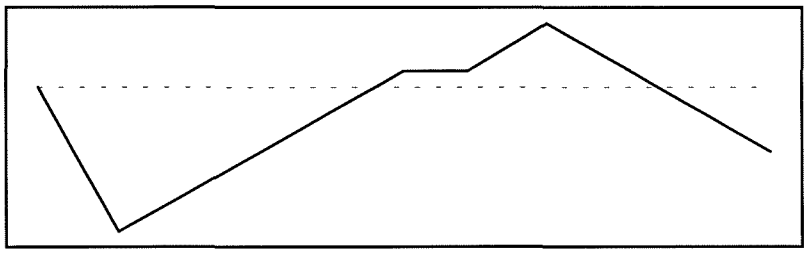


Figure 1.5: Example of a hybrid event

Events can only be detected and diagnosed if they have a noticeable effect on one or more of the sensor readings, so for example, a very small removal of material from a plant over a very long period of time may not be detected, if the size of the removals falls below tolerances necessary to accommodate measurement noise. An issue then arises as to the specification of the most appropriate tolerances: there is a balance between power to detect and the generation of a large number of false alarms.

The different event types are each diagnosed during different stages in the diagnostic procedure.

1. Abrupt anomalies: this step must be performed first, as any gradual trends in the data may be obscured by any abrupt anomalies that have not been diagnosed.
2. Gradual anomalies: after all abrupt events have been diagnosed, the model-based analysis is repeated but this time focusing on gradual anomalies.
3. Hybrid anomalies: if significant differences between the simulated and plant data still remain, this final step attempts to resolve them using a variety of methods.

The above procedure is explained in greater detail in Section 2.4. The next sub-section focuses on the abrupt case, to highlight the main functions of the diagnostic process.

1.4 Key Features Of The System

1.4.1 The Problem And Its Context

As an introduction, consider the following example; a very simple plutonium liquor storage facility consisting of only two tanks, of significantly different volumes, plus a single transfer device (Figure 1.6). Liquor is first fed into the smaller tank, Tank 1, where it is accounted prior to transfer to the larger tank, Tank 2. Extensive pipework is provided to enable recirculation, sampling, import and export. The facility can be represented by the connectivity diagram (Howell and Scothern, 1995b) shown in Figure 1.7, where n1, n2 denote the two tanks, c1 the transfer device and pipework that is *common* to both recirculation loops and c2, c3 those parts of the recirculation loops that are not common i.e. c1 is bounded by valves B, C, D, F and I whilst c2 is bounded by valve B and Tank 1 (via valve A) whilst c3 is bounded by Tank 2 and valve F where it is assumed that valve C is close to Tank 1 and valve D is close to Tank 2. In addition to the elements present in Figure 1.7, un-monitored nodes are added to both tanks, denoted by h1 and h2, which are added to accommodate unexplained gains/losses; in safeguards jargon, flow to and from hidden inventory. Level, density and temperature might be measured in both tanks.

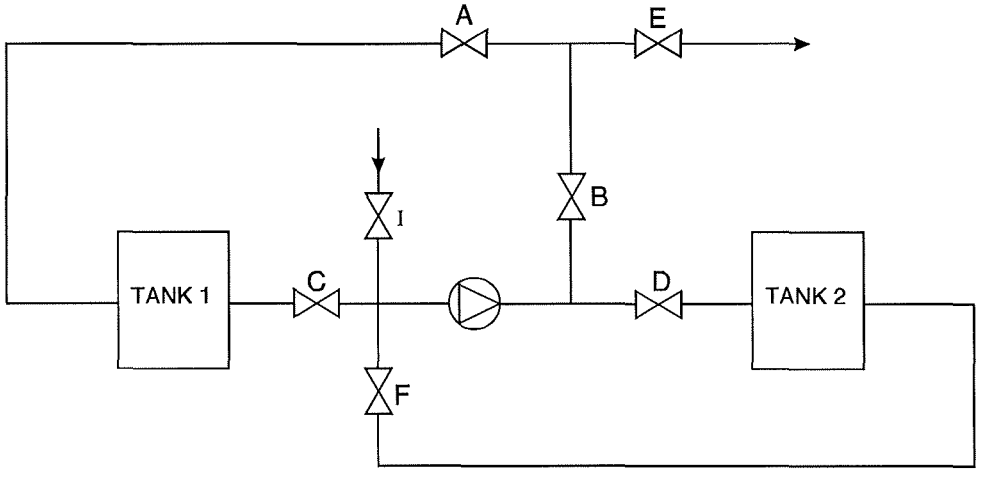


Figure 1.6: A simple plutonium liquor storage facility

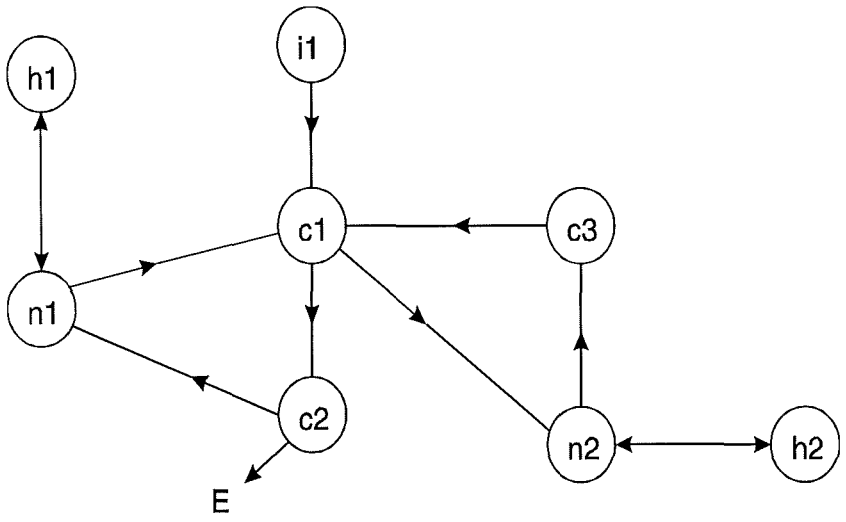


Figure 1.7: Its associated connectivity diagram

Imagine that the level in Tank 1, recorded over a period of time t: $t_A \leq t \leq t_F$, is as shown in Figure 1.8 whilst the level in Tank 2 is constant and the export valve, valve E, is kept closed. This transient might have been caused by the activities itemised in Table 1.1.

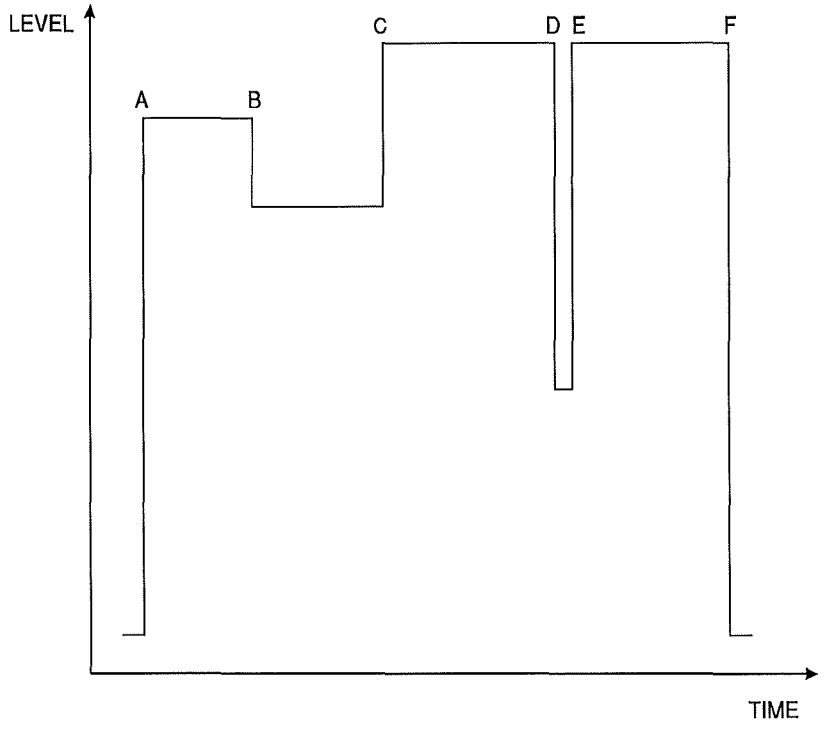


Figure 1.8: Tank 1 level

Activity	Time	Description
1	t_A	Tank 1 filled
2	t_B	Tank 1 partly emptied into recirculating pipework
3	t_C	Inlet re-opened and additional liquor introduced 'pushing' the pipe contents back into Tank 1
4	$t_D \rightarrow t_E$	Recirculation/sampling
5	t_F	Contents of tank 1 transferred to Tank 2

Table 1.1: List of activities

The main aim of the system is then to re-construct Table 1.1 from the various measurement histories available. This is achieved by performing the following (Howell and Scothern, 1995a): generate hypotheses, diagnose abrupt sub-events and interpret sub-events. To elaborate on these actions, consider how they might be applied to the simple example.

1.4.2 Sub-Event Hypothesis

A boundary condition generator, named SCAN, (Howell and Scothern, 1995a) is applied to the data to identify all activities observed in each of the level measurement records. Every notable change in level is deemed to signify that something (a *sub-event*) has occurred and, on the assumption that every change has resulted from a transfer of material, a hypothesis for the source and sink of each transfer is produced. Where either a source or sink are not readily identifiable, material is deemed to transfer to and from hidden inventory. Thus, for example, Activity 5 can be marked as a sub-event because the level in Tank 2 rose when that in Tank 1 fell and by an equivalent amount. It is extremely likely that Activity 1 represents another sub-event, in fact an input, by virtue of its size and by the fact that nothing happened, at that time, in Tank 2. Activities at t_B, t_C, t_D and t_E would then be marked as separate sub-events.

1.4.3 Sub-Event Diagnosis

Each of the sub-events is first assessed to determine whether or not the application of model-based diagnosis would provide additional information of value. This is accomplished by applying a set of simple rules: for instance, diagnosis would be required if any of the sub-events include any flows to or from a hidden inventory, but not if the sub-event is readily identifiable as a batch transfer either between tanks or in or out. A model-based diagnostic procedure (Howell, 1994) is then applied to those sub-events identified as being in need of further diagnosis. In essence, parameters pertaining to a simulation of the facility are adjusted so that simulation predictions *match* the various measurement histories pertaining to a particular sub-event. Figure 1.9 shows the more credible corrections that would result in the example. For instance, the sub-event at time t_B could be explained by either a transfer of material to pipe c1, a transfer of material to hidden inventory h1 or by the occurrence of measurement errors, simultaneously, in both level and density (e.g. as a common mode fault).

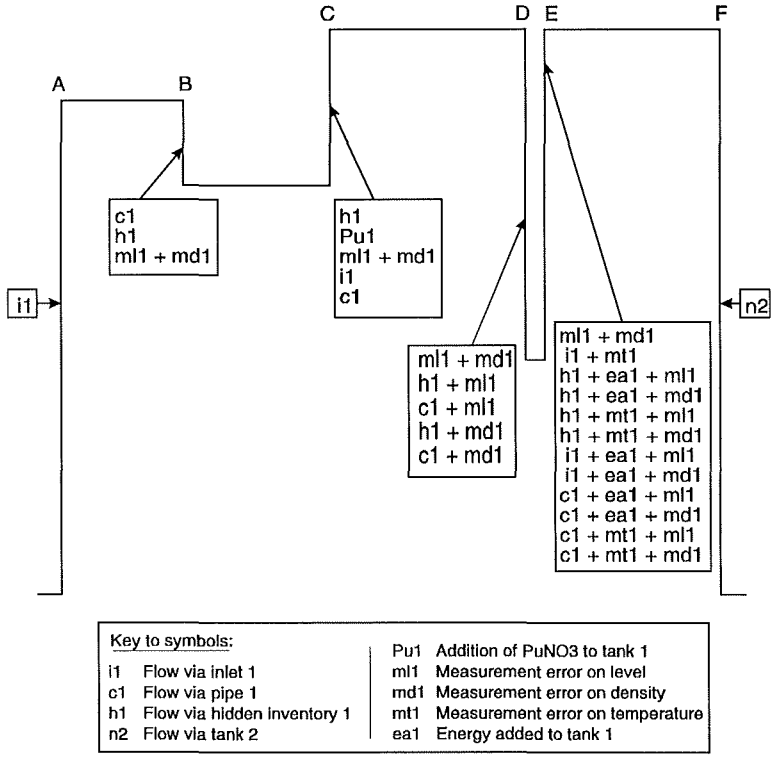


Figure 1.9: Individual diagnoses

Chapter 3 outlines the model-based diagnostic approach and then details some additions and refinements: specifically, the facility to make use of alternative methods to regression when searching for solutions and the improvement of the handling of aligned vectors in the solution space. Chapter 4 is concerned with the simulation of the plant, and describes the modelling issues that were addressed, along with the facility for automatic model generation for increased portability of the software.

1.4.4 Sub-Event Interpretation

This combines sub-events into events; that is it tries to establish which, if any, of the sub-events represent separate activities (i.e. events) and which combinations of sub-events can be identified as arising from a particular physical event. Of importance here is the fact that the diagnosis is unlikely to be unique; for instance, there is always a possibility, however ridiculous it might appear, that all transients can be explained as a set of measurement errors. Thus the interpreter must choose the most 'likely'. The diagnoses required for the example are given in Table 1.2. Chapter 2 of this thesis discusses the sub-event interpretation step in greater detail, building on the basic diagnosis to produce a time history of events occurring on the plant, encompassing both abrupt and gradual features present in the data. This chapter also covers the most important features of the user interface.

Event	Sub-event Diagnosis	Description
1	i1 → n1	Tank 1 filled
2	n1 → c1	Tank 1 partially emptied into pipework
	c1 → n1	Pipework emptied back into Tank 1
	i1 → n1	Additional input into Tank 1
3	n1 → c1	Recirculation - pipe filled
	c1 → n1	Recirculation - pipe emptied
4	n1 → n2	Tank 1 emptied

Table 1.2: Event diagnoses

1.5 Data Acquisition And Pre-Filtering

Finally it is worth pointing out that modern sensor equipment is capable of taking many readings per second, which can mean that the amount of data potentially available for a large plant, with many sensors, over an extended period of time is extremely large. Such large amounts of data only serve to slow down the diagnostic procedures, and as far as nuclear material safeguards is concerned, much of this data will be of little or no importance. If a tank is not involved in any transfers over several days, and the level is remaining steady, then there is no need to store a huge amount of data to show the activity in the tank, a small number of points will suffice, e.g. one at the start and end of each day perhaps, to show any minor level changes caused by evaporation.

For this reason it is assumed in this thesis that the raw sensor data is pre-filtered to strip out superfluous data points. One algorithm for this purpose could be to store a data point if one of the following conditions hold :

- the rate of change of the measured value changes by a significant amount, to store the start and ends of transfers, or

- the rate of change of the measured value is small, and the measured value is significantly different to the last measured value stored, to update the value when non-transfer changes such has evaporation have had a significant effect.

In both the above the meaning of the word 'significant' would have to be determined for the particular quantity measured.

1.6 Outline of Work

A number of different activities were needed to obtain a practical system for solution monitoring based on the approach described here:

1. physical models for the reprocessing plant elements had to be developed;
2. sub-events had to be generated from plant data;

3. possible causes of each sub-event had to be diagnosed;
4. possible events had to be generated from sub-events and diagnoses;
5. an expert system had to be developed to choose the most likely event history from all possibilities;
6. user interfaces had to be investigated;
7. the system had to be tested on realistic data;
8. models had to be automatically generated to aid portability.

Although sub-event diagnosis is performed using the technique first proposed by Howell (1994), the original technique was largely developed for the diagnosis of single abrupt anomalies, and had limited application. The technique has therefore been extended to the diagnosis of gradual and hybrid anomalies, to be more robust, and to be applicable to many different plants.

Each step listed above involved much original work, but the major original contributions presented in this thesis are entries 4 and 5, the generation and ranking of possible events, which are detailed in Chapter 2.

CHAPTER 2

2. IDENTIFICATION OF EVENTS

2.1 Introduction

The implementation of solution monitoring as a nuclear materials safeguards tool faces many obstacles, one of which is the fact that the operational history of the facility may not be available. This could be due to many factors, e.g. the plant operators may be unwilling to disclose operational procedures, or may not keep sufficiently accurate records of procedures which are carried out. Without such a history, the inspectors have only the data collected from the sensors installed on the plant on which to make their assessment of plant operation. Approaches for qualitatively understanding how a system is behaving from raw numerical data have been investigated by Forbus (1987), who stated that *'automation of this critical step is necessary for the next generation of expert systems'*.

The problem is also recognised in the application of artificial intelligence to control and supervision systems, see for example, Chen (1995). Within this field, the problem is called a 'Situation Assessment' (SA) task. Kirillov (1994) describes an SA-task as a general decision about what is happening, where and when, based on raw evidence concerning the observed object or the whole environment, including temporal dependencies, which must be taken into account in the situation assessment process. Shoham (1993) discusses the problems inherent in attempting to formally predict the future from current conditions, and states that *'The general problem is how to reason efficiently about what is true over extended periods of time, and it has to do with certain trade-offs between risk avoidance and economy in the process of prediction'*. This has obvious similarities with attempting to determine what has occurred in the past from incomplete, limited, or poor quality data.

The notion of an 'event' has many different interpretations, e.g. automata or Petri nets are given as examples of discrete event models in Lichtenberg and Lunze (1996), Gertler and

Anderson (1992) define an event as '*the occurrence of a fault in connection with a particular variable*' while Finch et al. (1990) define an event as '*a transition between process states, having no temporal extent*'. Within the field of artificial intelligence, the notion of an event is broader, and an 'event' can refer to any physically observable occurrence; Boutilier (1996) details a framework for the incorporation of observations into a set of plausible events that might have caused them. Throughout this thesis, references to 'events' are assumed to belong to the definition given in Section 2.3; this Section also provides descriptions of the commonly used terms in this thesis.

This Chapter describes an automatic method for examining plant data and for forming a hypothesis of the events which have occurred within the facility; such a method would be of significant interest to the inspector, particularly for those events which are not part of standard operating procedures for the plant under investigation. A summary of the entire procedure is given in Section 2.4, Sections 2.6 to 2.9 give details of the many steps involved in producing the final list of events, focusing on the diagnosis of abrupt sub-events. Gradual events are covered in Section 2.12, and the correction of any remaining errors is explained in Sections 2.13 and 2.14. Important features of the user interface are presented in sections 2.10 and 2.11, including the modification of the rules used to identify events and rank them according to supporting evidence. Finally, Section 2.15 discusses some of the situations in which the diagnostic procedure is not applicable, and explains how such situations can be dealt with.

2.2 Related Work

Finch et al, (1990) have produced a program for diagnosing abnormal transient conditions in various process plants. Named MIDAS (Model-Integrated Diagnostic Analysis System), the central concept of the program is the use of an 'event model' which contains all of the causal links between all of the various events which can occur as part of the process, and conditions for the violation of process constraint equations. Within MIDAS, the term 'event' is used to mean any significant observable change in process behaviour or condition, and the time evolution of the process state is viewed as a series of events, which

has close parallels with the concept of an 'event list' used throughout this thesis. The basic structure of MIDAS diagnostics is shown in Figure 2.1. For a detailed explanation of the diagram, see Finch et al, (1990). A brief comparison with the solution monitoring system is given here.

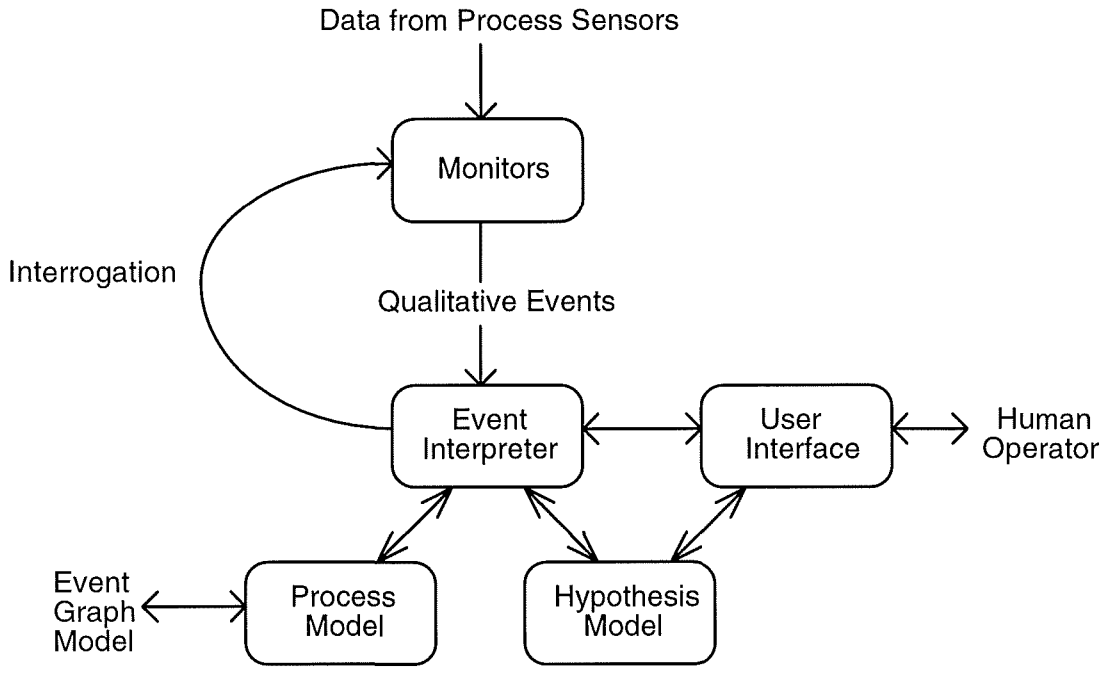


Figure 2.1: The basic structure of MIDAS diagnostics

The term 'Monitor' represents a method of generating events from process data, in much the same way as the SCAN data acquisition algorithm does in Section 1.4.2; however Monitors are designed to return qualitative data relating to a single sensor only, e.g. state change occurring or change in trend occurring, whilst SCAN produces a quantitative description of the activities occurring on the plant as a whole.

The MIDAS formulation has certain features in common with the diagnostic approach presented in this thesis, but since it is primarily designed as a fault diagnosis system, it has a number of features which make it unsuitable for solution monitoring, such as :

- the requirement that the process has a nominal steady state limits its application, and as stated in the paper, would require a dynamic process model running in parallel with the plant;

- the use of qualitative models, which saves computational time and reduces complexity when dealing with fault detection, is not sufficient for use in nuclear materials safeguards, which by its nature requires quantitative models to be used;

- the restriction that multiple simultaneous malfunctions can be diagnosed, but only if the malfunctions have non-overlapping symptoms, i.e. each malfunction affects a different group of sensors. This is not acceptable for a solution monitoring system, where some diversion strategies may be devised to make use of this restriction to fool the system.

Another model-based fault diagnosis system that has certain features in common with the diagnostic system presented in this thesis is that produced by Leitch et al, (1993). A schematic of its central components is given in Figure 2.2.

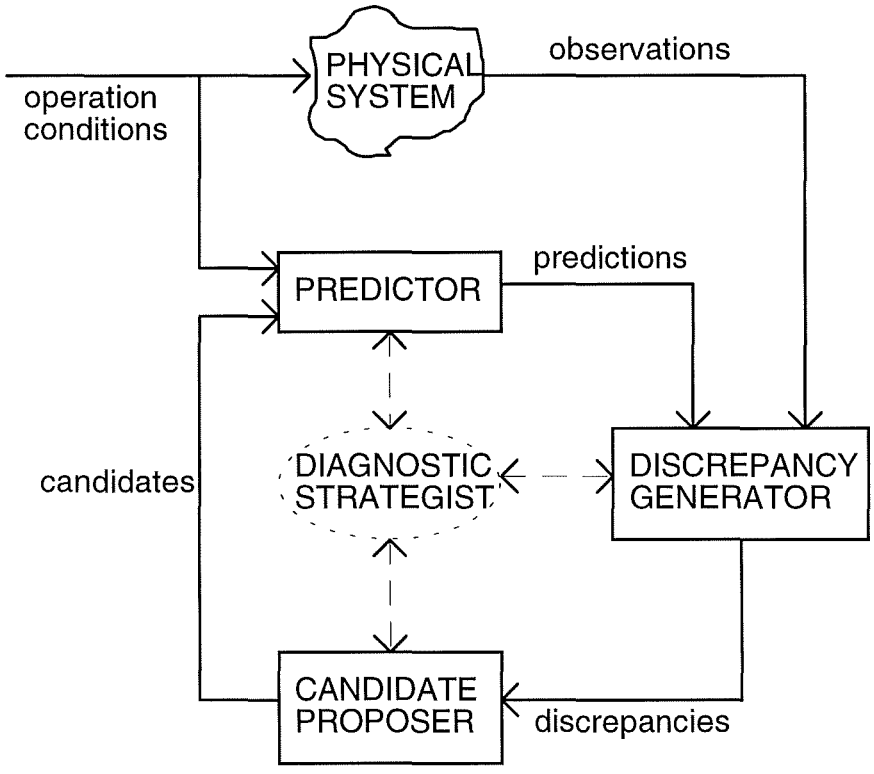


Figure 2.2: Leitch's model-based diagnostic system

This diagram summarises the basic components in the diagnostic system and their relationship to each other; the system makes use of a behaviour predictor, or simulation

model, which predicts the expected behaviour of the system; discrepancies between predictions and observations are then identified by the discrepancy generator; based on these discrepancies, fault candidates are produced by the candidate proposer; and the diagnostic strategist controls and co-ordinates the complete diagnostic process.

The system makes use of a simulation which synchronously tracks the real system, and searches for faults based on a characterisation of the modelling space. This has some parallels with the model based diagnostic method in the solution monitoring system here; in particular both systems adopt an iterative search approach in which the model is modified, this is then followed by the ranking of candidates. However the method of Leitch et al. examines changes in qualitative states only and as with the previous system, qualitative simulation is not suitable for use in nuclear materials safeguards. In addition to this, several shortcomings with the qualitative dynamic modelling approach used (Dynamo/FuSim) are highlighted in the ARTIST final report, Stefanini et al, (1993).

2.3 Definition Of Terms

Before describing how events are identified in the solution monitoring system, it is worthwhile clarifying the meaning of various terms.

2.3.1 Event

This is a matter of semantics. As far as solution monitoring is concerned, an event is a set of one or more actions that are viewed by the operator or inspector as representing a single entity. More often than not, the operator or inspector would have a name for that single entity. For instance, referring to activity 4 in Table 1.1: the term 'recirculation' might be used to denote the sequence of opening various valves, starting a pump, recirculating the liquor around a loop, eventually stopping the pump and finally closing the valves; the observed 'symptoms' of recirculation are two virtually identical sub-events but in opposite directions. Of key importance here is that a human has chosen to name a particular sequence of actions, the name has not been derived from the physics. Thus even in so called model-based diagnosis, there is still a central role for the human operator, in event classification. From a symptoms viewpoint, an event can be viewed as a sequence of

sub-events; in practice events comprising of one or two sub-events are the norm. In turn of sub-events, can be described by a particular choice of diagnoses. It is assumed that events can in general be categorised as either abrupt, gradual or as a 'hybrid' of these two (see Section 1.3). The majority of this chapter does not distinguish between these, as the theory for abrupt, gradual and hybrid events is conceptually very similar. Section 2.4 details the approach used for all three, and gives the overall strategy for diagnosis.

2.3.2 Sub-Event

Refers to a single rise or fall in the measured value of a sensor attached to a plant element. The most common sub-events are rises and falls in the level of a tank, as detected by the boundary condition generator (Howell and Scothern, 1995a).

2.3.3 Sub-Event Diagnosis

Is a possible explanation of the cause of a particular sub-event, generated by the diagnostic procedure. A diagnosis is deemed to be admissible if a computer simulation, executed over the same time span as that of the sub-event, predicts available measurements to within specified tolerances. The diagnosis may be specified in terms of one or more variables; these variables need not be unique, each such variable might have many other variables that cause similar effects.

2.3.4 Aligned Variable

If two or more variables have a similar effect on the output of the simulation, they are said to be aligned, and any one of these variables may be replaced with any one of its aligned variables. The degree of similarity required, for two variables to be declared aligned, can be varied, and is discussed in detail in Chapter 3.

2.3.5 Abrupt

An event, or sub-event is described as 'abrupt' if it is of relatively short duration, such as a transfer of material from tank to tank. An abrupt event may consist of one or more abrupt sub-events. They are usually easy to detect by visual inspection of the data.

2.3.6 Gradual

Gradual events or sub-events are classified as long term trends in the data, that are in a single direction, such as calibration errors, or leaking valves. These events may be much more difficult to detect by visual inspection alone.

2.3.7 Hybrid

An event may have features that pertain to one or more abrupt or gradual events, for instance an event may be long term but may vary in direction over time, any such events are called 'hybrid' events. An example of this is material gradually building up within a section of pipe, which later returns in a single transfer.

2.4 The Entire Procedure Summarised

The majority of this thesis deals with the identification of events in general, irrespective of whether they are abrupt or gradual in nature. In the complete system, the distinction between these types of event is obviously important. The procedure shown in Figure 2.3 and described below is proposed to isolate the various types of event (Scothern and Howell, 1997). This will be referred to throughout this Chapter.

1. By looking at the plant data, the hypothesis generator attempts to produce an initial description of plant activity by identifying, then attempting to explain, all individual mass transfers. Those transfers that cannot be explained on the basis of a few rules are then termed *abrupt anomalies*. Alternative diagnoses are now generated for each of these anomalies, by first performing model-based analysis on individual sub-events, and then by using the sub-event combiner to interpret one or more sub-events as events. The most 'desirable' are then hypothesised as having occurred. This stage is described in greater detail in Sections 2.5 to 2.10.

2. Based on these hypotheses, a plant simulation is now produced the output of which is compared with plant data; if any significant differences still remain, the model-based analysis is repeated but this time focusing on *gradual anomalies* and additional

hypotheses are generated to explain them. Section 2.12 gives more details on the gradual analysis stage.

3. If significant differences still remain between the simulation predictions and the plant data, then the error time history is examined to try to determine the cause of each error, using a variety of methods, detailed in Section 2.13. These errors may be due to abrupt, gradual or hybrid features of the data. The earliest error is tackled first, on the basis that the correction of an error earlier in the time history may have the effect of also correcting some of the later errors.

4. If, after all of the above procedures have been carried out, and the simulation and plant data still do not match to the required level, then the events hypothesised and the remaining errors can be examined by the user to try to determine the cause of the discrepancies manually. The methods of performing manual diagnosis and other methods of interacting with the diagnostic procedure are highlighted in Section 2.11.

The final goal of the procedure is to produce a table of events that represent the hypothesis of what is actually occurring upon the plant. The simulation of the plant is frequently used to check if the simulation predictions 'match' the real data, to within a specified tolerance, during both the formation of diagnoses and in the testing of the effects of the final hypotheses at each stage. Further details of the tolerance used for detecting a mismatch between the simulation and the plant measurements are given in Chapter 3. Although not specifically represented in the diagram, the user has the final say in rejecting or accepting any of the hypotheses generated by any stage of the diagnostic procedures.

2.5 Event Classification

Given that it is unlikely that an inspector would be able to construct a full list of possible events apriori and given the undesirability of believing that this is possible anyway, it is important that a human-computer interface is constructed to enable the inspector to describe observed events and to specify new ones. (This is discussed further in Section 2.10).

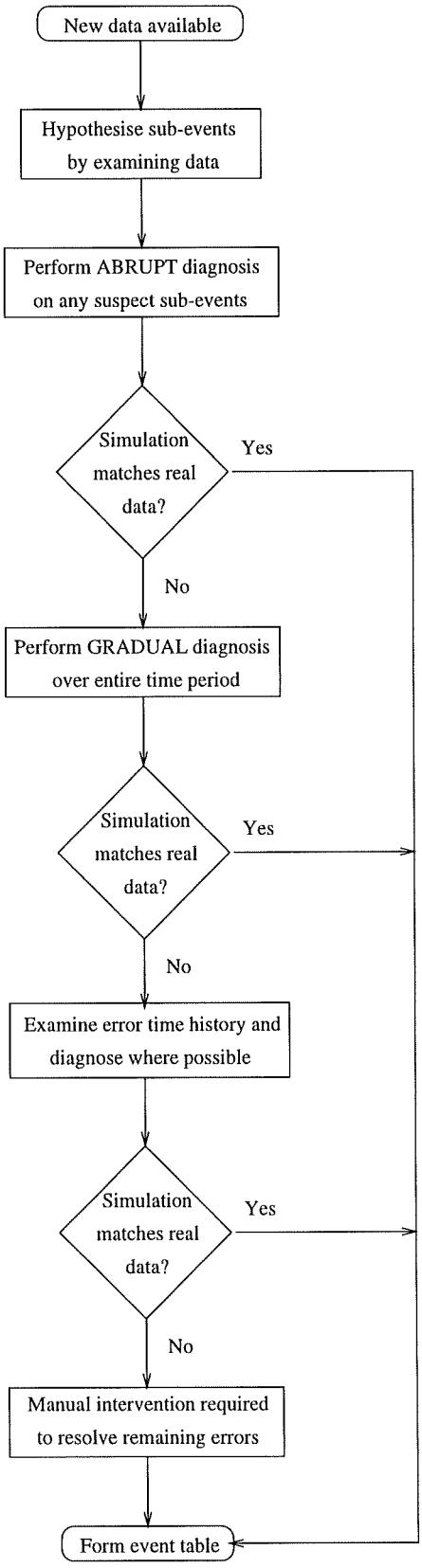


Figure 2.3: Flow chart overview of entire procedure

In addition, when confronted with a set of symptoms it is equally clear that the inspector would not view all events, that correlate with the symptoms, to be equally likely. Thus he would wish to categorise the events in some form of hierarchical structure. This is in agreement with Peng and Regia (1987b) who have stated that '*An important issue in diagnostic problem solving is how to generate and rank plausible hypotheses for a given set of manifestations*'. Within the field of nuclear materials safeguards and as far as the inspector is concerned, the occurrence of certain events is preferable to certain others. For instance, the nuclear materials inspector would prefer to explain what is observed, as a sequence of normal operational activities, rather than as a loss or gain. For this reason, it is proposed that events are classified by the perceived desirability of a particular result. This is achieved in 2 ways,

1. each type of event is placed in one of the following desirability categories : operator acceptable, needs follow up and diversion/alarm;
2. the likelihood of the event actually occurring is attached to each event description.

Operator Acceptable: These events are part of standard operating procedures, transfers between tanks, recirculations, sample taking and so on, and will generally not be of safeguards interest.

Needs Follow up: These events should occur less frequently. Although events in this category may be unusual enough to warrant further action by the inspector, they would not cause immediate concern as far as safeguards are concerned. Events in this category may be material gradually leaking from one tank to another, or material spending an unusual amount of time within pipework.

Diversion / Alarm: Events flagged as diversion/alarm are events that would certainly need investigation by the inspector, if only to verify that the alarm is false. Such events would include material leaving tanks and not reappearing elsewhere or unscheduled transfers out of the system.

The events are then organised according to the desirability category and by how many sub-events are present. Some events that might be implemented are listed in Table 2.1.

	1 Sub-event	2 Sub-events
Operator Acceptable	Batch transfer into tank from inlet Batch transfer out of tank to outlet	Recirculation (i.e. material leaves then returns) Tank to tank transfer (via pipe, hence two sub-events)
Needs Follow up	Additional input into tank from inlet Pipe filled Pipe unfilled	Pipe filled, then unfilled. (Similar to recirculation, but can allow greater time to pass before material returns) Pipe filled, then unfilled + additional input (i.e. a compound event).
Diversion / Alarm	Flow to hidden inventory Flow from hidden inventory	Diversion with addition (i.e. material replaced)

Table 2.1: Some typical events

Note the introduction of a *compound* event; this is needed because two single sub-events, flow from pipe and flow from input, might both be occurring at the same time. It is desirable that the initial list is made sufficiently comprehensive to ensure that all sub-events can be assigned to at least one event as otherwise there might be an excessive burden on the inspector at the time of commissioning. Finally it is worth pointing out that the process can be evolutionary, events can be customised on a plant by plant basis so that unusual occurrences can be accommodated.

2.6 Event Identification: An Overview

The goal of the event identification procedure is to produce a list of events such as the one shown in Figure 1.2, automatically, from the sensor data histories retrieved from the plant under investigation. Thus the aim is to identify a set of events E that describe all n activities (E_1, E_2, E_3, ..., E_n) during a specified time period $t: t_s \leq t \leq t_f$.

With the exception of noise, any variation in a sensor reading must be attributable to some physical effect, a movement of material, a movement of energy or whatever. Sometimes the effect of these variations will be visible elsewhere on a plant, sometimes they will only be local (Howell, 1994). The approach adopted here is to represent each variation as a sub-event and then to generate all possible explanations of why this sub-event could have arisen. The need for all possible explanations immediately rules out the possibility of forming, then comparing with a list of possible process events (Howell, 1994), the emphasis must be on structure and function (Davis, 1984). Individual sub-events must then be assigned to events. In other words each sub-event $SE_i \subset SE$ must be described solely in terms of a movement of material or whatever. Although at first sight this might imply the generation of a large number of alternatives, in practice the list of all possible explanations of all movements throughout the plant would be relatively small. Let this list be defined as a set ***S***. It is likely that a particular sub-event can be diagnosed by more than one set of movements or whatever. (See aligned variables in Section 2.3).

Let the set of variables pertaining to all possible diagnoses of a particular sub-event SE_i be $V_i : V_i \subseteq S$. Then methods exist (Howell, 1994) to enable the quantification of sub-sets of V_i, $D_{i_j} : D_{i_j} \subseteq V_i$ to obtain a diagnosis, i.e.

$$\left| \underline{\hat{y}}(t_{f_i}) - \underline{f}(t_{s_i}, t_{f_i}, D_{ij}) \right| < \text{tol} \qquad (2.1)$$

where $\underline{\hat{y}}(t_{f_i})$ is the vector of all plant measurements pertaining to time t_{f_i} and $\underline{f}$ is the output from the simulation executed from time t_{s_i}, with diagnosis D_{ij} included. These methods will be discussed in detail in Chapter 3.

Then an event $E_i \subseteq E$ is composed of one or more sub-events SE_{i1}, SE_{i2}, ... :

$$E_i = \{SE_{i1}, SE_{i2}, SE_{i3}, \ldots.\} \qquad (2.2)$$

and the conditions that are needed are :

$$(E_1 \cap E_2) \cup (E_1 \cap E_3) \cup \ldots. \cup (E_2 \cap E_3) \ldots. \cup (E_{n-1} \cap E_n) = \varnothing \qquad (2.3)$$

and

$$\overline{SE \cap (E_1 \cup E_2 \cup E_3 \cup ..... \cup E_n)} = \varnothing \qquad (2.4)$$

This leads to the general methodology for achieving this goal listed below:

1. extract salient features from the raw numerical data which need explaining such as obvious rises and falls in a level measurement. A single such feature is referred to as a *sub-event* (SE) throughout this thesis;
2. determine all possible causes for each such sub-event. Each possible cause is a *diagnosis* (D);
3. examine permutations of sub-events over time to find all possible *events* which could explain the data (E);
4. choose the most likely set of events from the set of possible events found above.

The extraction of the sub-events from the raw sensor data and the determination of possible causes for each sub-event is performed using the techniques mentioned in the previous chapter, and described in full by Howell and Scothern (1995a, 1997). The focus of this Chapter is the interpretation of sub-events and the formation of the event histories, in addition to some information on the form of the user interface. Details of how the sub-events and diagnoses are actually generated can be found in Howell and Scothern (1995a, 1997)

2.7 The Sub-Event Combiner

The sub-event combiner determines which permutations of sub-events and their associated diagnoses, can be combined to form specific events. Peng and Reggia (1987b), stated that *'The space of possible hypotheses can be astronomically large if multiple disorders can be present simultaneously and some method is needed to focus an expert systems attention on those hypotheses most likely to be valid'*. Checking every possible permutation becomes computationally intensive as the number of sub-events and the number of diagnoses increase, and is not practical for a large facility with many sub-events

occurring. For this reason, the combinations permitted are restricted in time and space by using the following conditions :

1. a maximum duration for an event is specified so that sub-events need only be combined with other sub-events within this time range;
2. sub-events are only checked for combination with other sub-events whose diagnoses relate to the same part of the plant. It is counter-productive to examine every sub-event with every other, since certain sub-events will obviously be unconnected, i.e. transfer tank-2 pipe-1 will be examined in conjunction with transfer pipe-1 tank-7, but not with transfer tank-4 tank-5. Hidden inventories (Section 1.4) are not viewed as local to a specific part of the plant since, by definition, they represent unknown paths: a sub-event involving any hidden inventory will be examined in conjunction with any other sub-events involving any hidden inventory;
3. one desirability category is searched at a time. If a suitable event $E_k \supset \{SE_{K1}, SE_{K2}, \ldots\}$ is identified in this category, then ignore associated sub-events $SE_{K1}, SE_{K2}, \ldots$ when searching other desirability categories.

When narrowing the search in this way, considerable emphasis must be placed on the user interface to enable the user to override the search algorithm and to input alternative event hypotheses. The sub-event combiner then performs the following procedure:

1. initially set the desirability category to that which is most politically acceptable, 'Operator Acceptable';
2. in turn, try all permutations of one, two and then three sub-events (within the restrictions described above), invoking the corresponding rule sets for the current desirability level; at present no event is described by more than three sub-events;
3. as soon as a sub-event is matched to an event in one category, it is removed from consideration in further categories to reduce processing overload.

If after trying all permutations, for the current desirability category, some sub-events have still not been associated to an event, then the next desirability category is activated and the procedure is repeated from step 2, as shown in Figure 2.4.

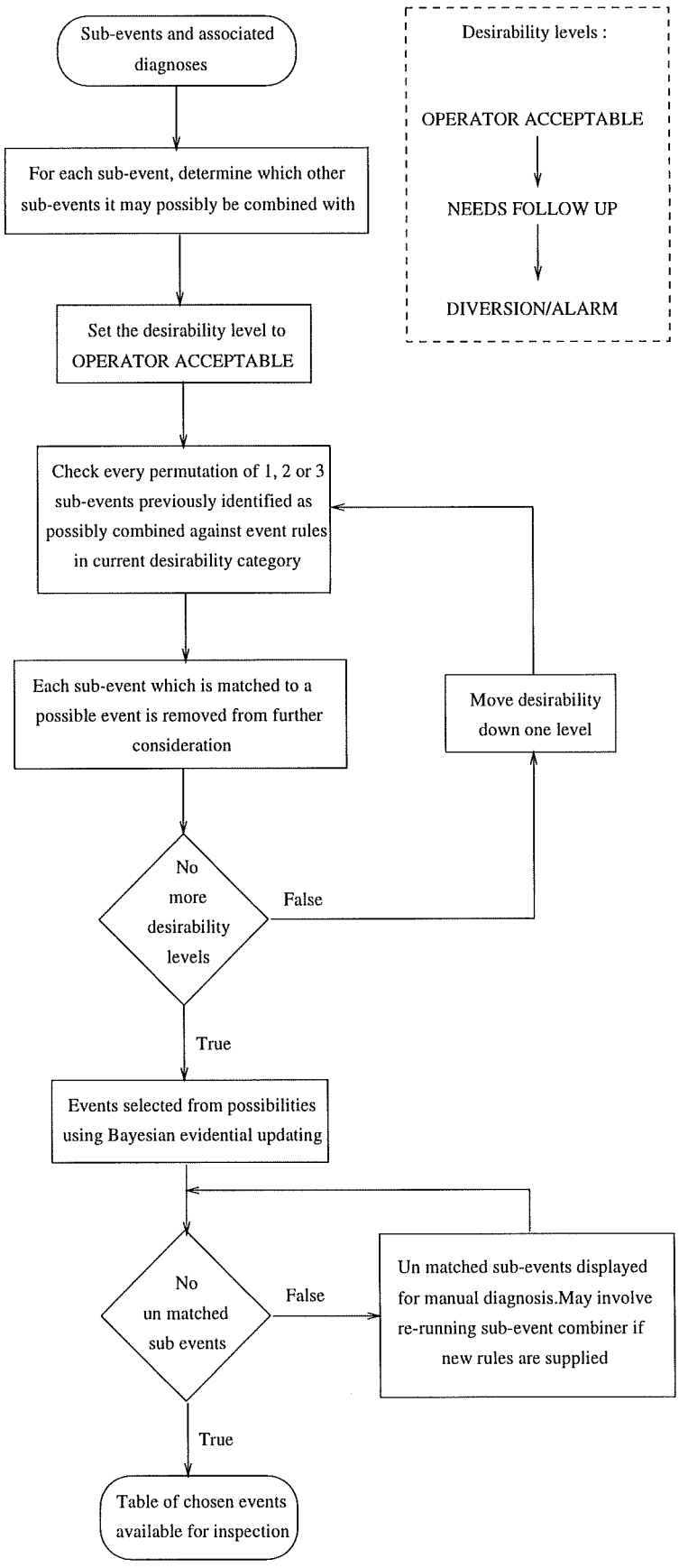


Figure 2.4: The sub-event combiner procedure

The result of this procedure is a list of many possible events, which must then be reduced so that no sub-event is present in more than one event. This reduction is done on the basis of the subjective probabilities assigned to each event, which may be modified by any supporting or conflicting evidence. The methods used to acomplish this are described in Section 2.9.

If any results are tied, even after comparing the subjective probabilities derived from supporting evidence, then one event is essentially taken at random on the basis that the actual choice between them must be of minor importance. Whichever result is automatically chosen, all of the other results would still be available for selection, should the user decide to reject the automatic choice.

2.7.1 Unmatched Sub-Events

If, after trying all rules in all categories of desirability for all combinations of one, two and three sub-events, some sub-events are still not matched successfully, then this will need to be investigated by the user. The emphasis, once more, is on the user interface. The user has a choice of either manually selecting sub-events that can be combined together, or of writing new rules to classify the sub-events on the basis of information provided, and of then re-running the sub-event combiner. The choice depends on whether the sub-events in question form a commonly occurring feature or a one off occurrence. In this way, the basic rule set can gradually be expanded to tailor it to a particular plant.

2.8 Other Factors: Continuity And Hidden Events

It is important to remember that a Solution Monitoring System would be accessed by the inspector on a day by day basis. At any particular instant of time it is quite likely that certain events would be happening on the plant and would not have been completed when the sub-event combiner is invoked.

Thus it is quite possible for an event to start during the period of time under examination, but finish sometime during the next period. For instance, the partial emptying phase of a recirculation could occur during one period, and its filling phase could occur during the next; failure to accommodate this possibility would result in incorrect diagnoses with both

parts incorrectly classified as transfers to or from the pipework. To resolve this problem, the sub-event combiner must consider any sub-events, that occurred during the previous period, and that could be combined successfully with current sub-events to produce a more desirable result.

Thus the combiner must first identify how far back in time it need look; this time interval, Δt_{max} minutes, corresponds to the largest possible event duration, already specified. Any sub-events that occurred during the last Δt_{max} minutes of the previous period, are then be considered as well. Taking these sub-events into account, the most desirable event is now selected and compared with the earlier hypotheses; the most desirable events are then selected.

Another factor worthy of discussion is the delayed or 'hidden' event. For instance, material might be transferred directly into a pipe; on such occasions the material would only be detected when it was 'washed out' into a tank. Again this requires some form of input from the user.

2.9 Event Description

The decision as to which sub-events (and their associated diagnoses) can be sensibly combined to form particular events must be made by consideration of the particular attributes of the sub-events themselves. This is accomplished by representing the defining characteristics of each event in a 'rule'. These 'rules' are used to decide if the sub-events under examination match the criteria specified as defining a particular specific event. In the current implementation using G2 (Gensym), rules can be of a standard format, which is in an easy to understand pseudo-English. For instance the rule for detecting a batch input looks like :

for any sub-event E

for any diagnosis D that is a-diagnosis-of E

if the type of D is transfer

and

the source of D is a member of inlets

and

the magnitude of D>= min-size-for-batch

then

start batch-in(E,D)

Details of how the user may create or modify these rules are given in section 2.10. Within the rules, the criteria tested for usually pertain to transfers of material, as this information is usually sufficient to identify an event as being of a particular type, e.g. a recirculation must consist of a transfer out of the tank in to the pipework, followed later by a similar sized transfer back into the tank from the same pipework. This information is the primary factor in identifying possible events, and these *primary* features are usually identified during sub-event hypothesis, although additional possibilities can be added during diagnosis. *Secondary* features normally pertain to changes in density, temperature and so on, and are only identified at the diagnosis stage.

In addition to the primary features of the event, quite often adjustments in other parameters are required to make the simulation match the plant measurements. For instance, in recirculation the observed changes in level are often accompanied by excursions in temperature and density caused by pump heating and by agitation; although it might be possible to model these effects in the simulation, for various reasons, they are unlikely to be modelled accurately. It is then quite often the case that these secondary effects can be explained by other activities, as well, so that many slightly different possible permutations can be generated which give a very similar effect overall. For example recirculation induced temperature and density excursions, might be explained by measurement errors, or by the presence of a solution in the pipe loop prior to the recirculation being at a different temperature and concentration to the solution in the tank. In the current implementation, corrections are permitted in up to three parameters per diagnosis, although each of these three parameters may be aligned with a number of others which are deemed to have a sufficiently similar effect. The number three was chosen as a

compromise between computation demands, the need for the simulation to match observations and the need to provide sufficient discrimination between events.

The problem of choosing which of the slightly different permutations should be chosen can be resolved by a large number of methods, including conventional probability distributions, fuzzy sets, confidence factors and so on. Various schemes have been proposed for the ranking of multiple behaviours predicted by a simulation, and for the use of these in establishing the most likely event, e.g. Leitch et al. (1993) and Peng and Regia (1987b). The MYCIN project discussed by Buchanan and Shortliffe (1985) makes use of weighted evidence both for and against each hypothesis.

Here the method of ranking used is based on Bayesian evidential updating, chosen since the theory is well established, (numerous treatments of Bayes Theorem are published, see for example Berger, 1985, or Bernado and Smith, 1993). The well known Prospector system also makes use of subjective probabilities and Bayesian decision theory, see for example, Gaschnig (1982). The Bayesian approach involves the updating of a base subjective probability (the value which would be used to rank the event should no other evidence be available) by the application of the following formula (Berger, 1985):

$$P(A_j \mid E) = \frac{P(A_j)P(E \mid A_j)}{\sum_{i=1}^{k} P(A_i)P(E \mid A_i)}, j = 1,2,\ldots,k \qquad (2.5)$$

where each A_j refers to a possible event, $P(A_j|E)$ is the revised probability of event A_j occurring given the evidence E, $P(A_j)$ is the base probability of event A_j occurring, which is assigned subjectively *a priori*, $P(E|A_j)$ is the conditional probability of the evidence occurring given that event A_j occurs, and k is the total number of possible events.

This is valid for the case where all possible events are known, along with base probabilities, and all possible evidence types are known, and probabilities for each type of evidence given each event are also known. For our purposes, the number of possible events and types of evidence would not be known, and so a simpler version is used instead:

$$\mathrm{P(A \mid E)} = \frac{\mathrm{P(A)P(E \mid A)}}{\mathrm{P(A)P(E \mid A) + (1 - P(A))P(E \mid \overline{A})}} \qquad (2.6)$$

$P(E|\overline{A})$ is simply the probability that the evidence has been caused by other events. For events which have multiple evidence present, the above formula is used to update the probability of the event sequentially, for each piece of evidence in turn. This approach may cause a problem because of what is known as the requirement for successively conditioned likelihoods (Bernardo et al, 1994, Quinlan, 1993), which is explained in the next paragraph.

The Bayesian approach above can be re-formulated into a simpler form for manipulation using the prior odds for event A, $O(A) = \frac{P(A)}{1-P(A)}$, giving

$$O(A|E) = \left[\frac{P(E|A)}{P(E|\overline{A}}\right] O(A) \tag{2.7}$$

Updating the prior odds for A using evidence E_1 gives

$$O(A|E_1) = \left[\frac{P(E_1|A)}{P(E_1|\overline{A}}\right] O(A) \tag{2.8}$$

and subsequent updating of this using evidence E_2 then leads to

$$O(A|E_1 \cap E_2) = \left[\frac{P(E_2|A \cap E_1)}{P(E_2|\overline{A} \cap E_1}\right] O(A|E_1) \tag{2.9}$$

There is then a need to specify the so called *measure of sufficiency* $\left[\frac{P(E_2|A \cap E_1)}{P(E_2|\overline{A} \cap E_1}\right]$. If the amount of possible evidence for a given event is large, then very many such measures of sufficiency would need to be specified, one for each possible combination of evidence. Although some systems do require such information (Szolovits and Pauker, 1978), the normal approach, used in systems such as Prospector, is to assume conditional independence:

$$P(E_2|A \cap E_1) = P(E_2|A) \tag{2.10}$$

$$P(E_2|\overline{A} \cap E_1) = P(E_2|\overline{A}) \tag{2.11}$$

The question as to whether conditional independence is true for a particular case needs to be ascertained, and if this does not hold, then the conditional probability distribution needs to be derived. How this is achieved in practice is detailed in Section 2.10.

The specification of apriori probabilities $P(E|A)$ and $P(E|\overline{A})$ is not only subjective, it is also dependent on the values of any variables describing the evidence. For instance a temperature excursion will have a magnitude. For simplicity, the template shown in Figure 2.5 is used to 'shape' $P(E|A)$.

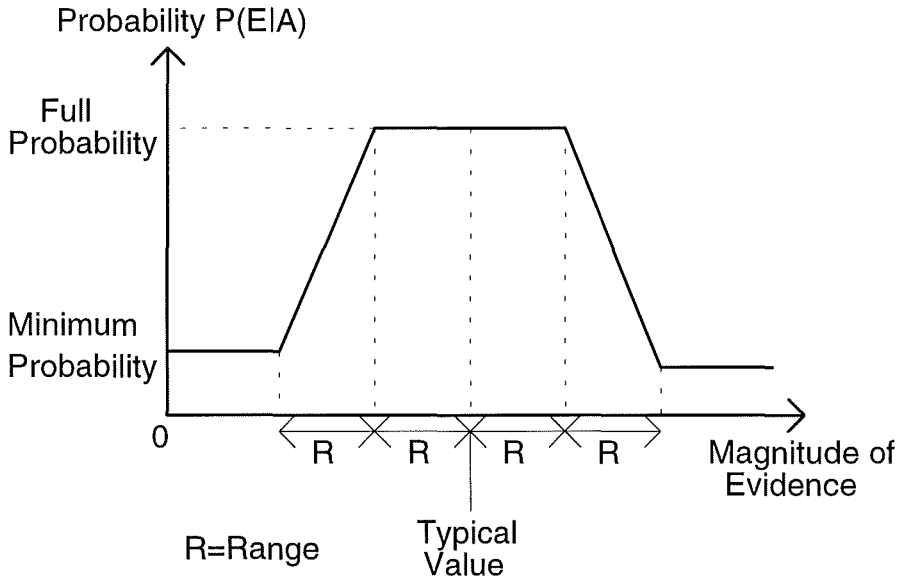


Figure 2.5: Subjective probability for the occurrence of evidence

Any occurrences of the evidence with a value within the specified range of the typical value are fully accepted, and so use the specified full probability. Occurrences of the evidence with values more than twice the specified range from the typical value use the minimum probability. Linear interpolation of the probability is used between the two extremes. For instance, in the case of recirculation, the variable associated with the addition of energy due to pump heating might have a typical value of 10kJ, with R=4kJ, this would indicate the amount of energy added by the pump may fluctuate considerably without ruling it out as evidence, while a value of R=1kJ would indicate that the amount of pump heating during recirculation usually falls within a small range of values. This

template was used for its simplicity and ease of manipulation, but any other desired shape could be used in its place, such as Normal or Gaussian distributions. The base value of the subjective probability of the event, in the absence of any other evidence, P(A), is also assigned by the user. This subjective assignment of probability is based on what the user would prefer to see. Quinlan (1983) has called the use of subjective probabilities *'the most straightforward approach'* of the common methods of representing uncertain information, and the requirement that both $P(E|A)$ and $P(E|\overline{A})$ be specified is not unreasonable; Duda et al. (1976) has stated that both of these probabilities are *'intuitively meaningful measures'*, and that *'such probabilities can readily be obtained from experts'*

2.10 Generation Of Rules For Identifying And Ranking Events

One of the main aims of the diagnostic system is that it should be user-friendly and easy to use. With this in mind, a system has been developed to guide the user through the process of supplying all the required information for the production of event identification rules, and of the supporting evidence necessary to rank the events.

2.10.1 Event Identification

Rather than creating an entire database from scratch, rules for identifying many typical events are provided in the system. These can then be tailored by the user to match the requirements of the plant. A simple menu system is provided to allow the user to view events currently present within the system, as shown in Figure 2.6. To allow simpler management of a large number of events, the types of event listed can be restricted to show only those events that match the chosen display criteria, such as the number of sub-events which make up the event, or the desirability category of the event. Choosing to add a new event will prompt the user to supply the required number of sub-events which make up the event, and suitable templates will be generated for all of the required rules and procedures, which can be easily modified to reflect the new event. Selection of any event brings up a display allowing the user to alter various characteristics of the event, as shown in Figure 2.7. Changes to characteristics such as desirability category or the name of the

event are automatically applied throughout all rules and procedures associated with the event, to ensure consistency.

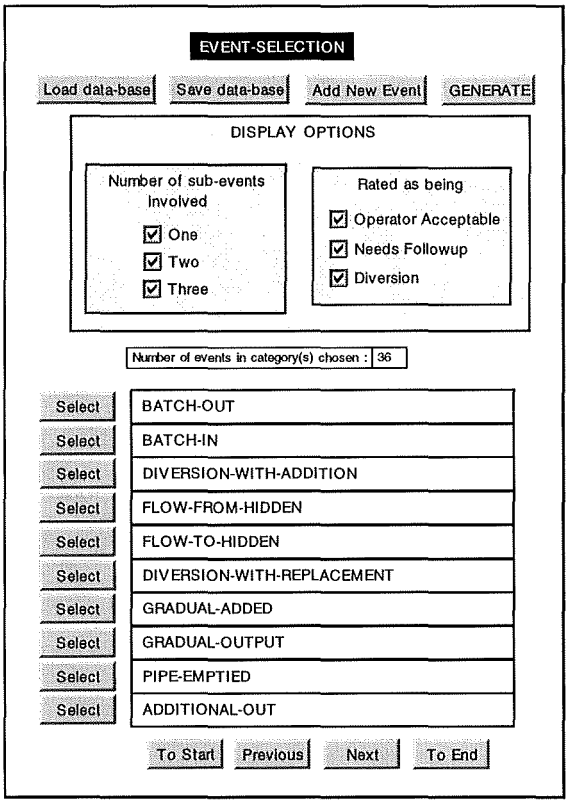


Figure 2.6: Event selection menu

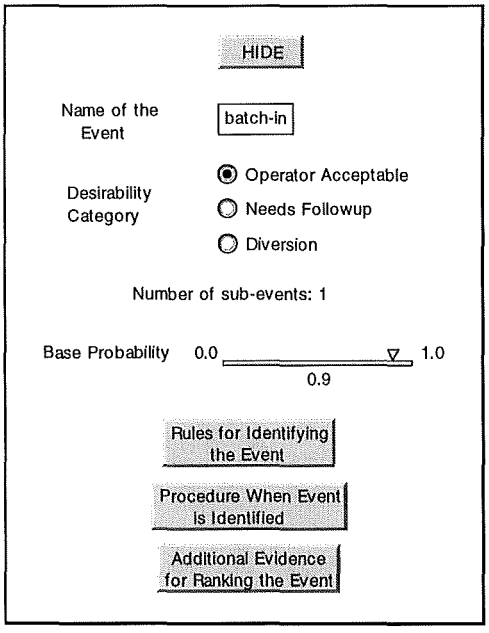


Figure 2.7: Examination of an event

The rules for an existing event can be viewed and modified using the workspace shown in Figure 2.8.

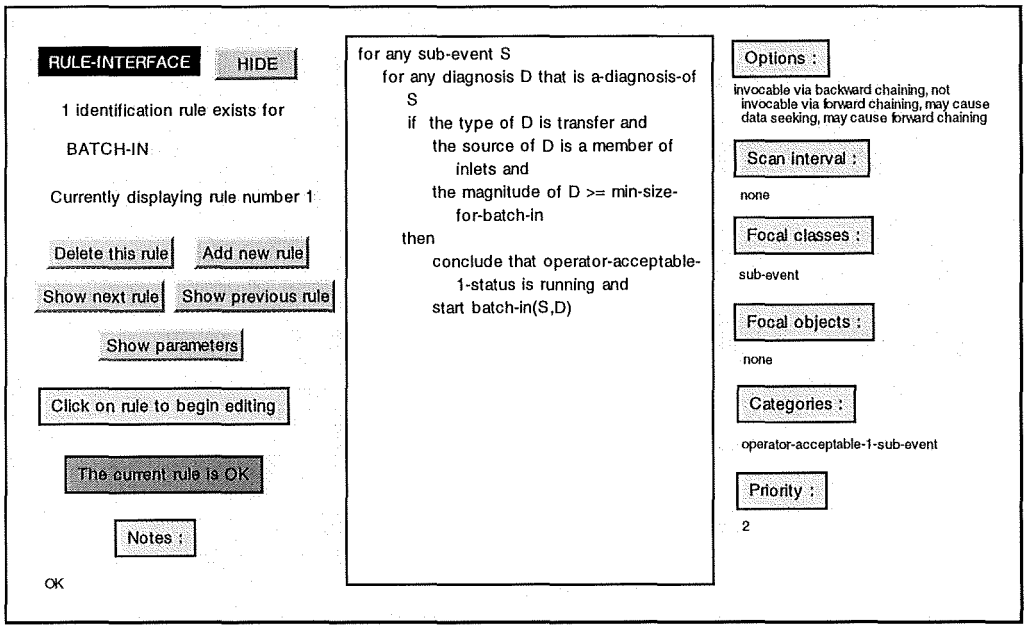


Figure 2.8: Interface for the modification of rules

Changes made to the rule are checked for correctness, and if errors are made, the user is informed of the nature of the error, and warned that the rule is not acceptable in its current form.

2.10.2 Specification Of Supporting Evidence

The current system groups the type of secondary evidence into two categories, density effects and temperature effects, and the user can select which specific entries from each category are required for the event in question, as shown in Figure 2.9. The categories were chosen to reflect the typical supporting evidence found in case studies so far, but these could obviously be extended should the need arise.

When considering the types of evidence, it is important to bear in mind that that the diagnoses generated are based on differences between simulation predictions and the actual plant measurements. This means that evidence such as 'temperature measurement error' does not necessarily mean 'a failure in a temperature sensor', but simply indicates that it is possible that the temperature estimated by the simulation is likely to be different

to the actual measured temperature. For example, if a recirculation is modelled within the simulation as simple movement of material, without modelling the effects of heating of the material by the pump, then there will be a difference in the simulated and measured temperatures after the recirculation, which the diagnostic procedure will always be able to correct by hypothesising a temperature measurement error. This difference is likely to be present for every recirculation, and so this 'evidence' can be added to the evidence used to rank recirculation events.

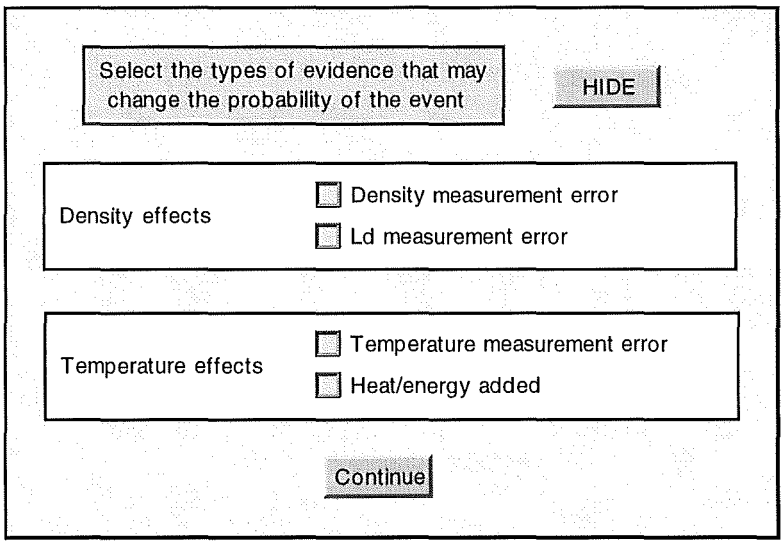


Figure 2.9: Selection of relevant evidence

After selection of the relevant categories, the user is guided through a series of windows designed to extract the relevant information required to produce the ranking rules. Figure 2.10 shows a typical window in which information is requested on the effect that the presence of a temperature measurement error may have.

The typical value and the range fields are straightforward, as are the values for P(E|A), the probability that such evidence will occur given that the event has occurred. Values of P(E|A) are entered using sliders: both normal values of the evidence, within the specified range of the typical value, and unusual values of the evidence, defined as being more than twice the range away from the typical value. These values allow the construction of the P(E|A) graph shown in Figure 2.5.

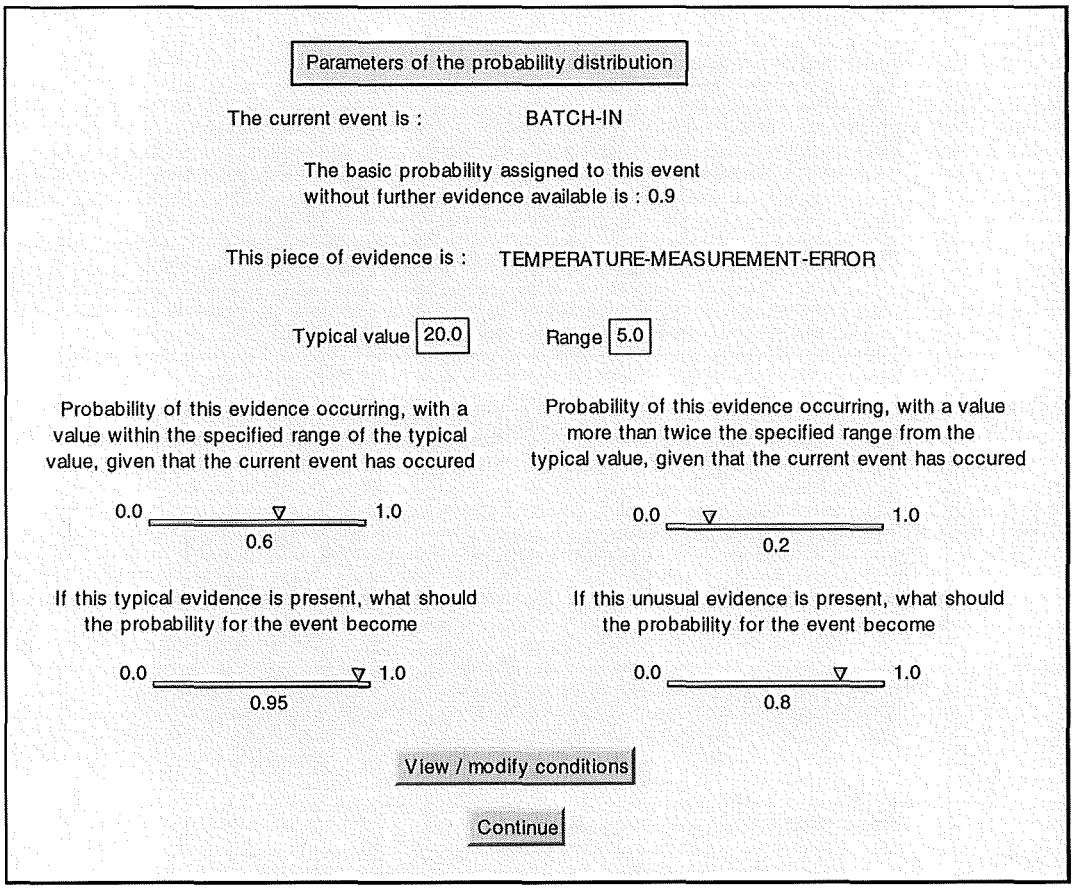


Figure 2.10: Specification of details for evidence

Values for $P(E|\overline{A})$, the probability that the evidence would occur given that the specified event has *not* occurred are less intuitively meaningful, and rather than ask this directly, the user is prompted to specify what the base probability of the event should be modified to if the indicated evidence is present, i.e. the value of P(A|E), for both normal and unusual values of the evidence. These values allow the required values for $P(E|\overline{A})$ to be calculated, using a re-arrangement of the Bayesian formula (2.6):

$$P(E|\overline{A}) = \frac{P(A)P(E|A)(1-P(A|E))}{P(A|E)(1-P(A)} \tag{2.12}$$

Also present on this workspace is a button which allows the user to specify additional conditions which must hold for the evidence to be relevant, as shown in Figure 2.11. For

example, in a recirculation event (e.g. transfer tank-1 pipe-1 followed by transfer pipe-1 tank-1), a temperature error in tank-1 may only be expected during the 'return' section of the event, and so the temperature error evidence should only be considered if it is associated with a diagnosis whose 'target' field matches the location of the evidence.

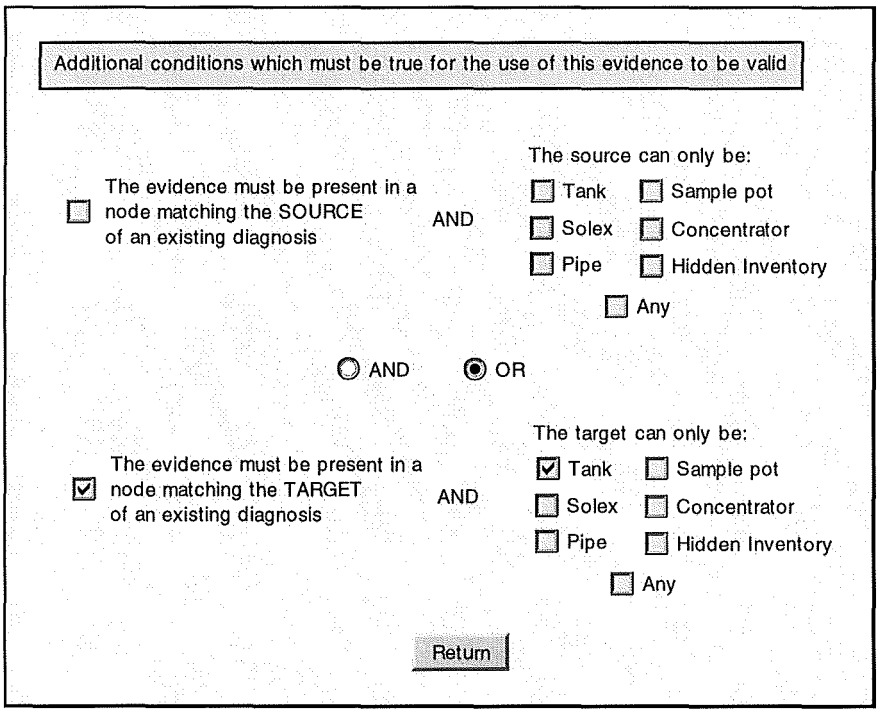


Figure 2.11: Additional conditions for the application of evidence

After the user has specified information on each of the relevant types of evidence, he will be asked to specify if the evidence is mutually independent or not, as shown in Figure 2.12. If conditional independence is not assumed, information on how each possible combination of evidence should be handled needs to be provided. In the current implementation, each particular sub-event can have no more than three (non-aligned) diagnoses elements associated with it, one of which will represent the movement of material, previously called the *primary* diagnosis, while the remainder will be made up of *secondary* diagnoses, which are effects such as temperature and density changes. For this reason, the system will only have to accommodate pairs of evidence when examining combinations.

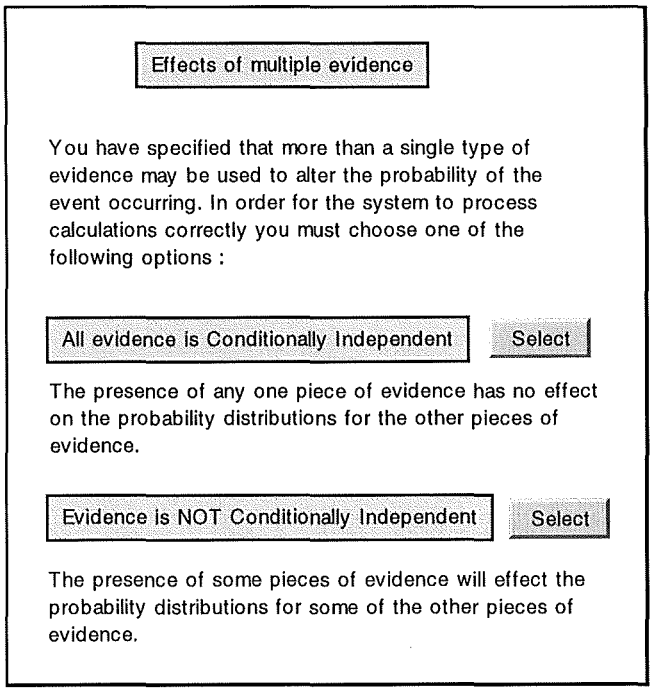


Figure 2.12: Conditional independence decision

The user is then presented with a series of windows, detailing the particular combination of evidence under consideration, and the effect that the assumption of conditional independence will have should both types of evidence be present. An example is given in Figure 2.13, the user can then decide whether these are reasonable for this particular pairing of evidence. If the user decides that the values are not acceptable, he must then specify how the presence of the first type of evidence affects the probability distribution of the second.

In reality, the conditional probability distribution could take any shape, since the interaction between types of evidence could be very complex. For simplicity it is here assumed that the cross-section of the distribution that represents $P(E_2|A \cap E_1)$ for a particular value of the occurrence of E_1 will take the same basic shape as shown in Figure 2.5. However, the characteristics of this shape can be specified to vary with the value of the first piece of evidence. All of the characteristics of the graph can be varied, not just the probabilities, since it is conceivable that, for example, a particularly large temperature error may indicate that the magnitude of any associated density errors that may occur

would be different than the magnitude of any density errors expected for a particularly small temperature error.

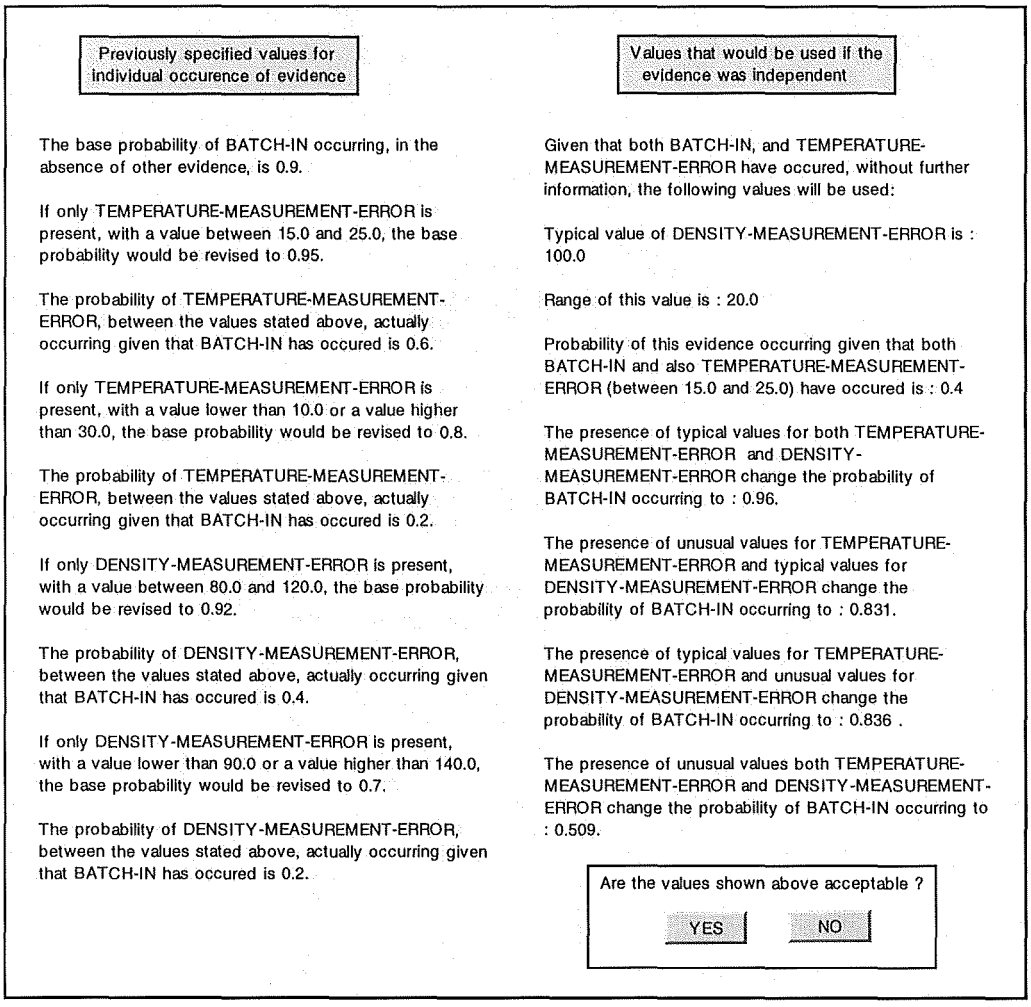


Figure 2.13: Details on one possible combination of evidence

Again, in reality, this variation could take many forms, but for simplicity, here it is assumed that specifying the distribution at four key points will be sufficient, with the probability distribution at intervening points linearly interpolated. Since it is unlikely that the end-user would be willing (or able) to specify more complex relations, this simplification is justified. The four key points used are the value of the first piece of evidence at the -2, -1, +1, and +2 ranges from its typical value, which are the vertices on the graph shown in Figure 2.5. At each of these points, the user is able to adjust all of the

values pertaining to the conditional probability distribution of the second piece of evidence, as shown in Figure 2.14.

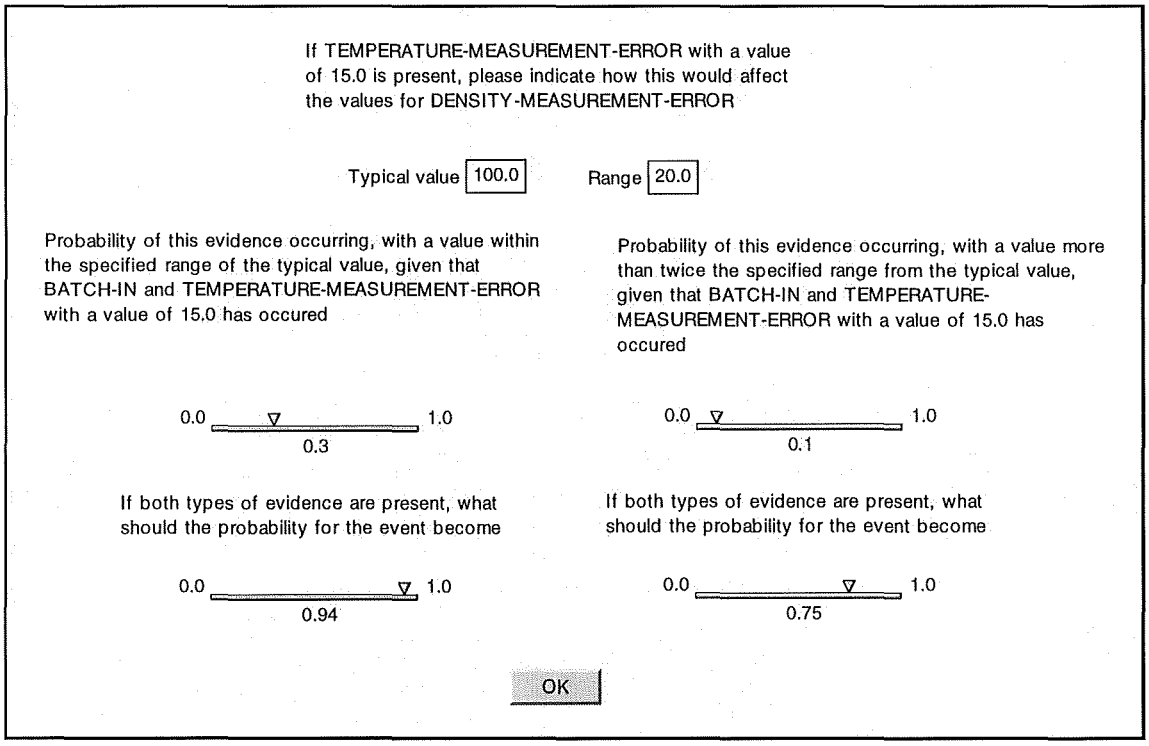


Figure 2.14: Specification of conditional probability in the presence of other evidence

After the specification process is complete, suitable rules and structures are automatically generated in a module which can be loaded into the main diagnostic package. The method used allows a single rule to be present for each type of evidence for a particular event, combinations of evidence are detected and allowed for in the updating procedure used. During the evaluation of an event, each evidence rule that matches the diagnoses associated with the event will call a procedure which updates the probability of the event. These rules execute in parallel, but all call the same procedure, which will finish processing the effects of one before moving on the next. The procedure used is summarised in Figure 2.15. This method has the added advantage that it mimics one's intuitive feelings that a number of events should be first be ordered on the basis that they have similar primary effects, followed by refinement of this order on the basis of the secondary evidence available.

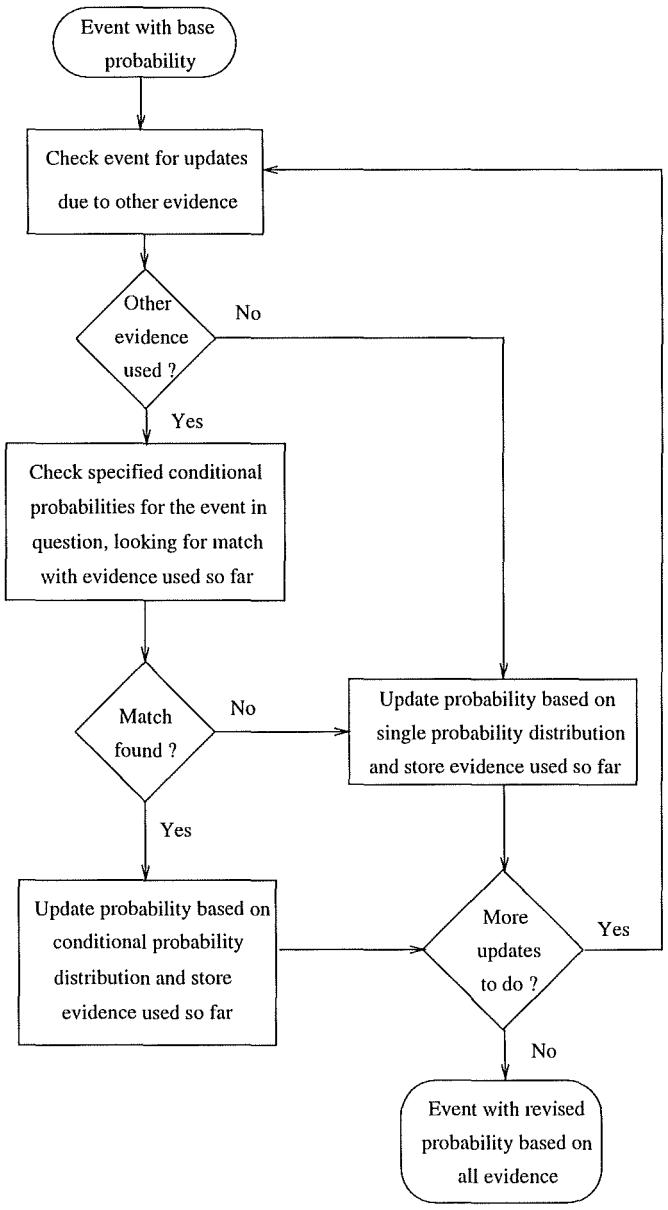


Figure 2.15: The procedure for updating the probability of an event based on supporting evidence

2.11 User Interaction

One of the primary requirements of a diagnostic system is that it should be easy to use, and so the form of the user interface is very important. Kramer (1981) makes the following comments '*The interpretation of large amounts of data is often difficult on a timely basis. This analysis problem is often present in nuclear safeguards and security systems .... The problem arises of how to quickly interpret the almost infinite amount of data available from computer systems. Computer graphics have proven to be a very*

useful tool in this endeavour'. With this in mind, the system has been designed to be graphically based, and user interaction to be 'point and click' as much as possible, so that the user can be led down an easy to follow hierarchy of windows. User options are controlled by only displaying buttons when appropriate. There is provision to look at measurement records pertaining to individual plant items, to examine events, sub-events and alarms, and to perform simulations and animation.

An important feature of the system is that particular classes of event can be selectively displayed, so events which need following up are not hidden by the potentially large number of operator acceptable events which could be generated. The importance of such a feature is highlighted in Vale and Machado e Mura (1993), where they cite cases where serious alarms were obscured due to the arrival of thousands of other, less serious alarms. On entering the system the user can display a list of events spanning the past one or more days (Figure 1.2) and a similar list of alarms; the justification for hypothesising each event can also be displayed by clicking on the appropriate button. As identified previously in this Chapter the user might want to perform one or more of the following actions :

1. select one or more alternative events to describe one or more sub-events;
2. hypothesise new events from unmatched sub-events;
3. specify a hidden event.

In taking these actions, the user must:

1. be presented with all appropriate available information,
2. be given the facilities to perform the actions, and
3. be given a means of assessing their effects.

2.11.1 Information Display And Effects Assessment

2.11.1.1 Measurement Record Display

The user can examine any of the plant data available for any tank in the system, just by clicking on its icon representation in the plant schematic. Plots can be made of records pertaining to any measurement source, for instance of level dip-tube pressure (ll), of density dip-tube pressure (ld) and of temperature. Either all measurements can be

superimposed on a single graph, or the user can choose to cycle through the various measurements in turn. (An action button, to move on to the next graph, will automatically appear if the *separate graphs* option is chosen). By default, the time scale of the graph is set for the current day, but any time period can be specified by using the '*Alter max/min time*' and '*1 month history*' buttons. The former opens the window shown in Figure 2.16.

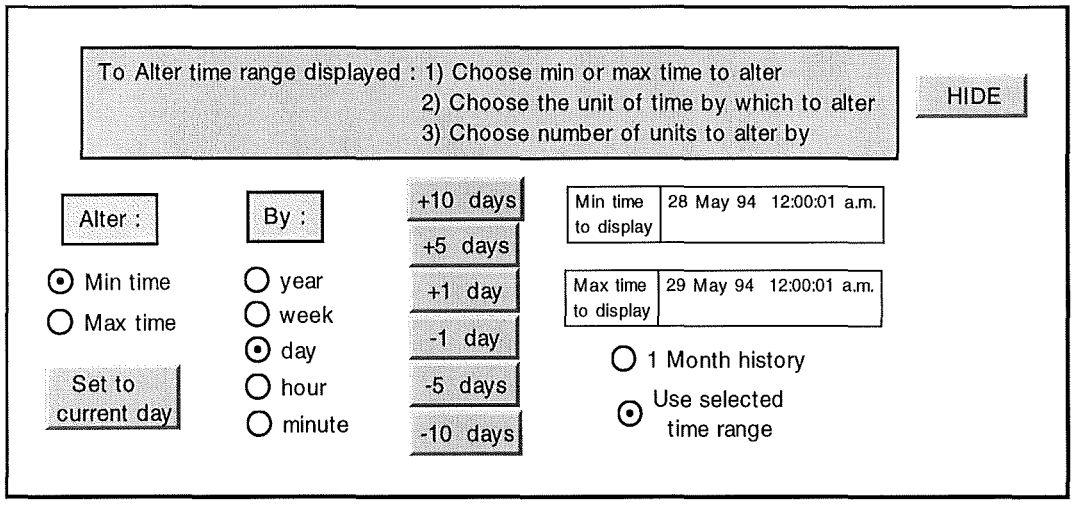


Figure 2.16: Specification of time range to plot

2.11.1.2 Running The Simulation

The simulation can be run over any chosen time range and for any set of hypothesised events. When the simulation is complete, the trend chart is modified so that it plots both real and simulated values, superimposed, on a single graph, and animation of the trend chart and plant schematic is automatically initiated from the start time of the simulation.

2.11.1.3 Viewing Hold Up In Pipe Headers

After running a simulation the user can view the hold up in any of the common headers in the system by clicking on the desired pipe representation in the plant schematic. Since the model makes use of common headers rather than modelling each pipe section separately, many of the pipe sections present in the plant schematic will cause the same common header state to be displayed. For instance, all pipes leading from the accountancy tank to tanks 1, 2 and 3 are designated as header-1.

2.11.1.4 Inspecting Individual Events

Diagnostic information pertaining to individual events, including their associated sub-events, can be displayed in separate windows (e.g. Figure 2.17), as can their alternative diagnoses (e.g. Figure 2.18). The alternative diagnoses are arranged as rows, with each row pertaining to a separate diagnosis: each disc represents an individual variable, discs coloured green relate to the first variable, those coloured blue relate to the second and those coloured yellow relate to the third. Aligned variables are displayed in the same colour, and therefore it is quite common for more than one disc, of the same colour, to be displayed on the same row.

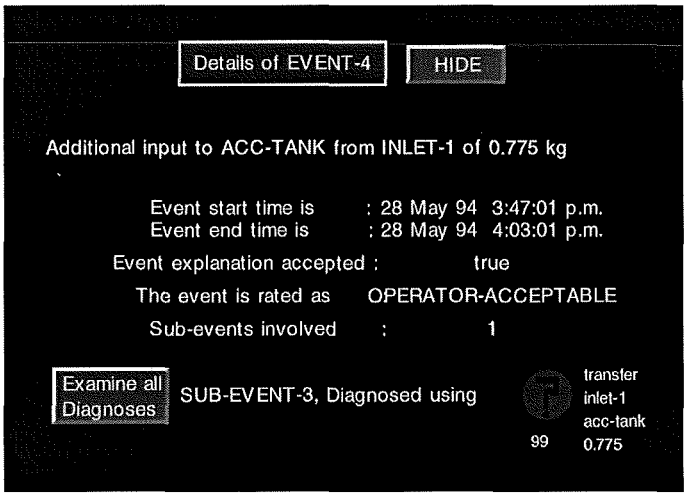


Figure 2.17: Details of an event

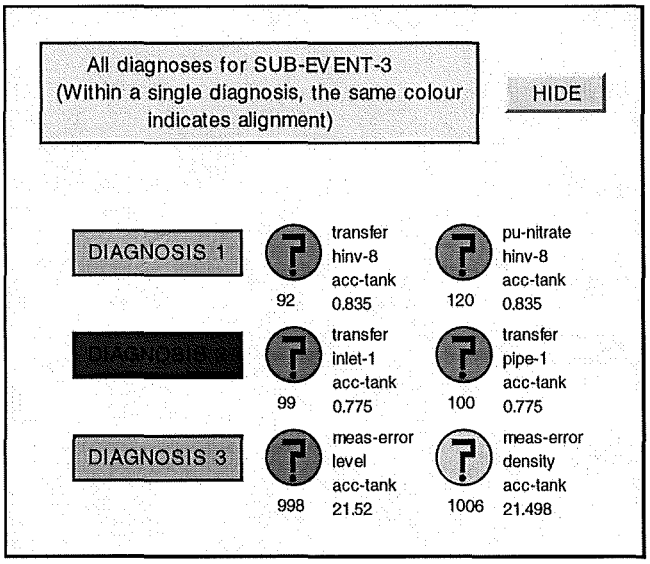


Figure 2.18: All diagnoses pertaining to a sub-event

2.11.2 Making Changes

If the user is unhappy about any of the hypotheses generated, for instance because the user knows something that is not available to the system, then any of the events presented can be rejected. If any of the events are rejected, then the user can re-run the sub-event combiner, with the rejected conclusions prohibited, to produce a new event list. This process can be repeated until the user is happy with all of the events generated.

Suppose the user believes that Event 3 (in Figure 1.2) has been diagnosed incorrectly, or that the user simply wishes to investigate the effects of alternative diagnoses for this event. The user would reject this event by clicking on the '*reject?*' button; this causes the cell, containing the event number, to turn red and triggers the appearance of two buttons: '*Re-diagnose with rejected conclusions prohibited*' and '*Manually diagnose*' This is shown in Figure 2.19.

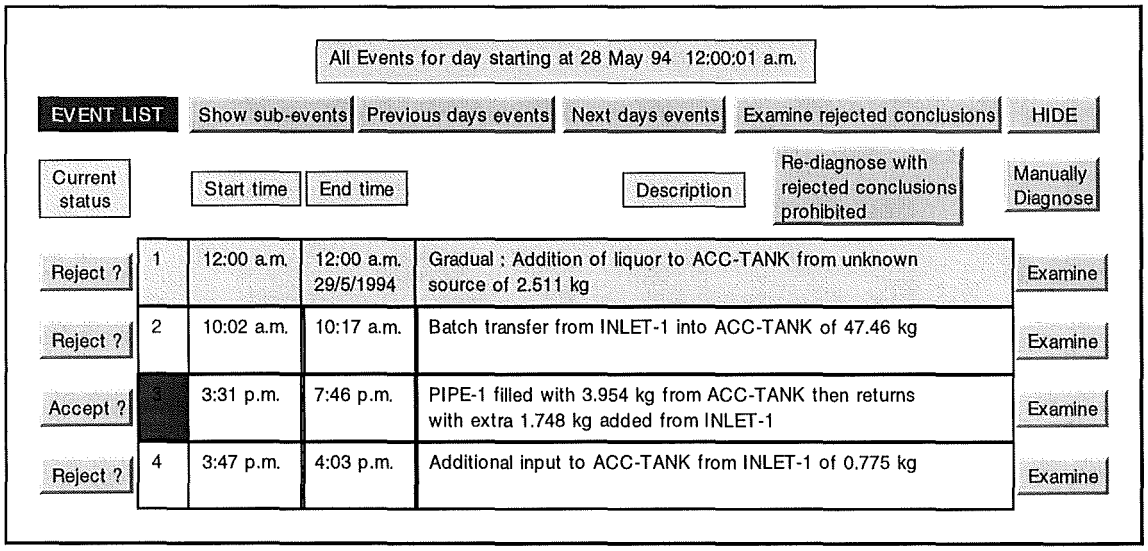


Figure 2.19: Event list with rejected event

Clicking on the '*Show sub-events*' button now opens a window displaying all the sub-events pertaining to the events of that day. In the example shown in Figure 2.20, the purpose of the highlighting (in red) is to indicate those sub-events that still need to be resolved.

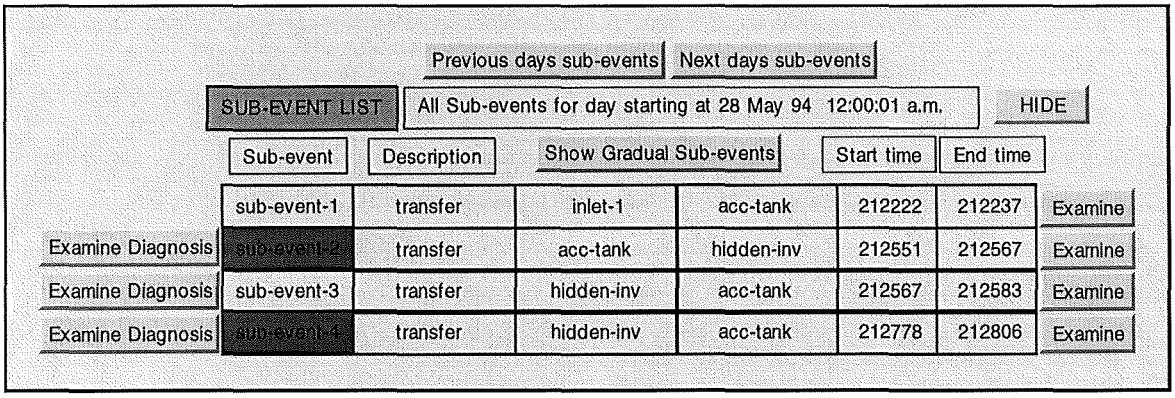


Figure 2.20: The sub-event list

Clicking on the '*Re-diagnose*' button first causes the rejected event descriptions (i.e. diagnoses) to be moved to a *rejected conclusions* list, and then causes the sub-event combiner to be re-invoked, but this time rejecting any diagnosis already entered on the *rejected conclusions* list. Thus a revised event list is generated like that shown in Figure 2.21.

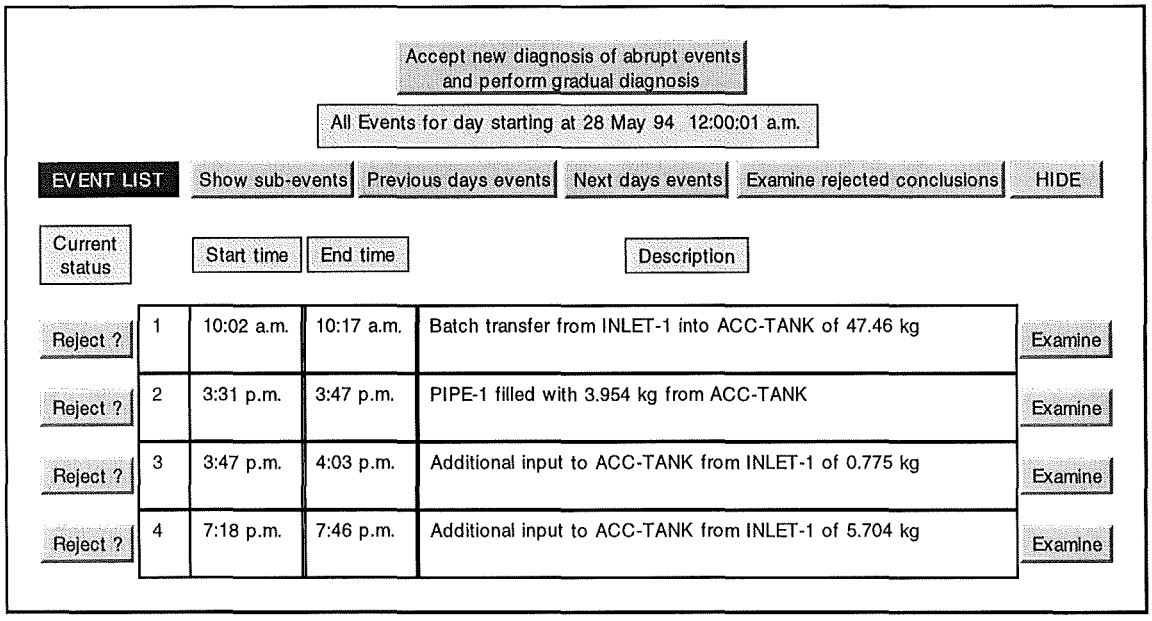


Figure 2.21: Revised event list after re-running the sub-event combiner

The *rejected conclusions* list can be inspected (e.g. as in Figure 2.22) by clicking on the '*Examine rejected conclusions*' button.

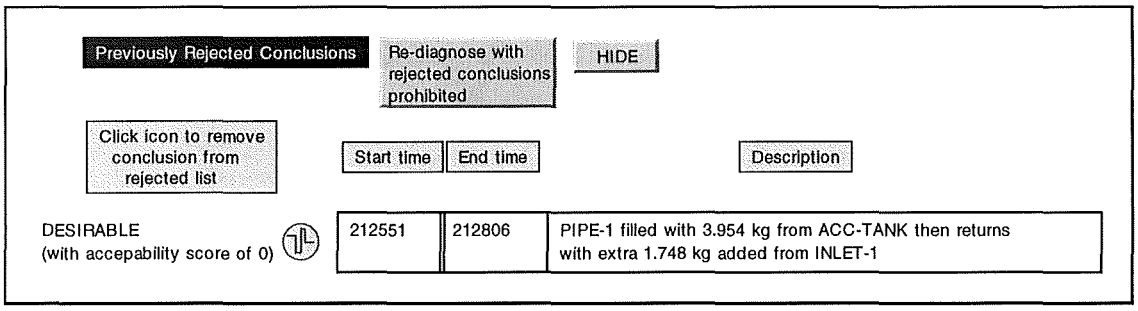


Figure 2.22: Rejected conclusions list

The user can continue to reject event hypotheses until all alternatives have been exhausted. At this point, the user would be asked to manually intervene to input a preferred diagnosis.

2.11.3 Manual Intervention

At any time the user might wish, to either manually overwrite an event description, or to modify, or add to, the rules applied by the sub-event combiner. Manual intervention is initiated by clicking on the button provided, labelled '*manually diagnose*'. This then opens a window giving two new options (Figure 2.23): '*Combine and explain sub-events*' and '*Output a diagnostic file*' to help the systems developer edit the rule base. Also displayed on this window is a list of all sub-events which are still to be resolved.

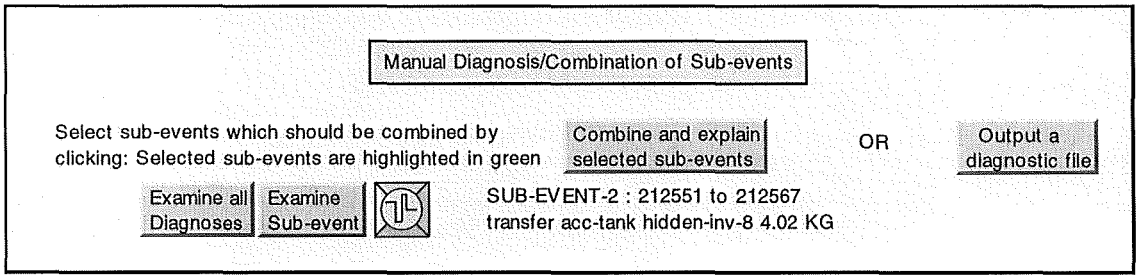


Figure 2.23: Initial window for manual diagnosis of events

Clicking on the '*Examine all Diagnoses*' button, for any sub-event, displays those diagnoses that would explain the sub-event (Figure 2.24) and clicking on '*Examine sub-event*' displays the original hypothesis of the sub-event (Figure 2.25).

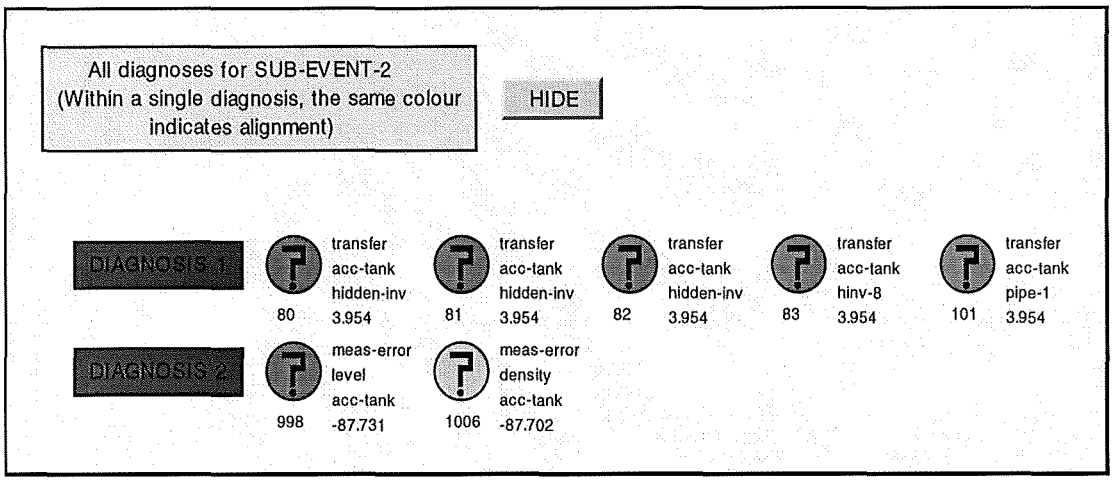


Figure 2.24: All diagnoses pertaining to sub-event 2

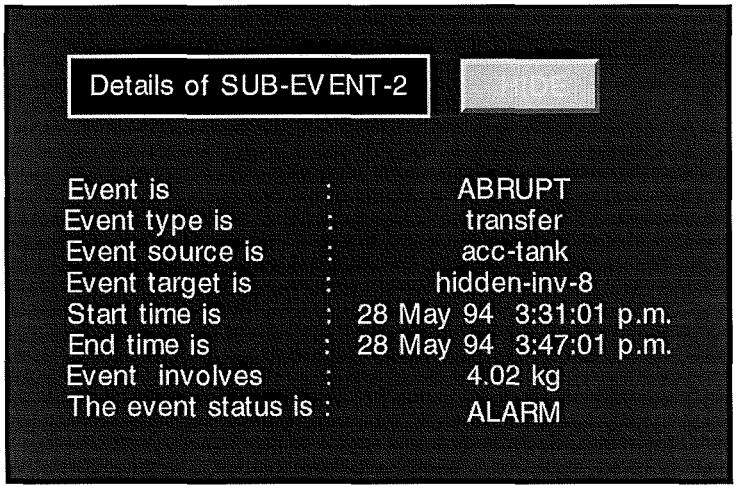


Figure 2.25: Details of original hypothesis of sub-event 2

The user can then select groups of one or more sub-events, which are to be combined into a single event, by simply clicking on the desired icons, and then initiating combination by clicking on the '*Combine and explain selected sub-events*' button. A new window is then

displayed, an example of which is shown in Figure 2.26, allowing the user to provide a description of the combined event, and to choose a diagnosis from all those available.

After selecting diagnoses, the system automatically checks the rule base, and displays any events which match the diagnoses chosen. Any of the suggestions shown can be chosen to provide the description of the event, or the user may choose to input a description manually.

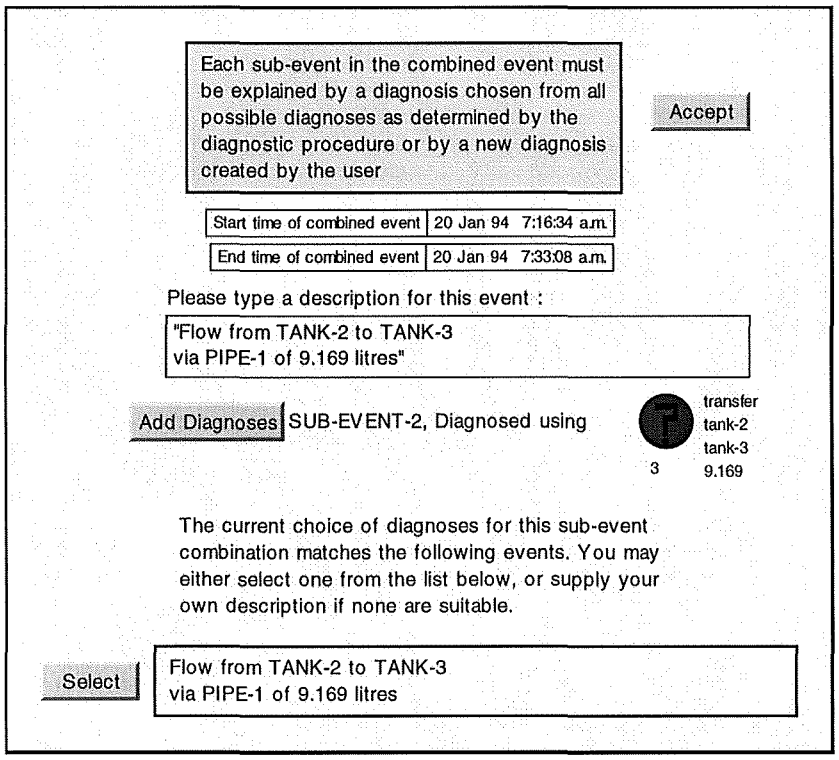


Figure 2.26: Details of manually combined event

If no diagnoses are available, or none of the supplied diagnoses are acceptable, then the user is free to create a new diagnosis using any of the existing flow paths of the system. This is done by specifying magnitude and flow path desired, as shown in Figure 2.27, and if relevant for the path chosen, how the flow interacts with the pipework (Figure 2.28).

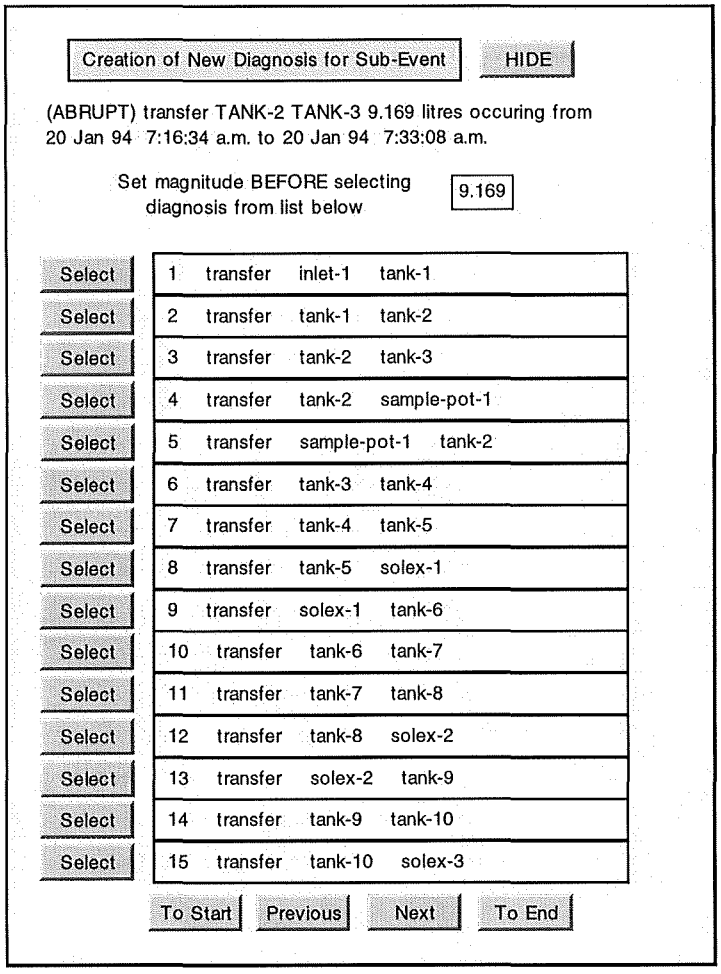


Figure 2.27: Choosing magnitude and material transfer path during manual diagnosis

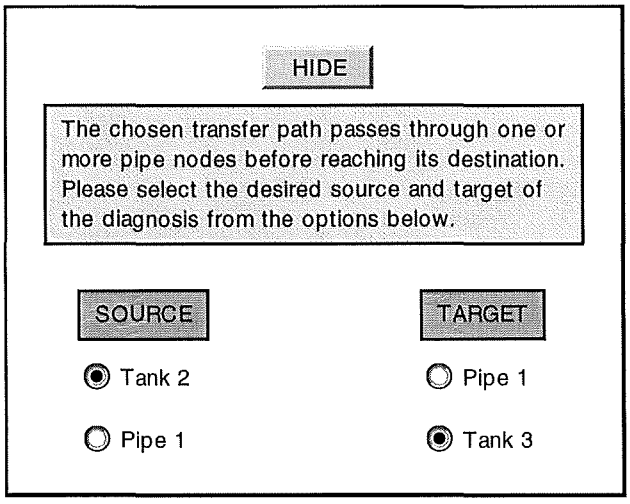


Figure 2.28: Specifying material transfer path through pipework

2.11.4 Choosing Proportions Of Aligned Parameters

Whenever a combination of two or more aligned parameters are chosen to explain a single feature, the relative proportions of each parameter need to be specified. By definition, each of these parameters is capable of explaining the feature completely, and so components must be scaled in such a way as to ensure that the overall magnitude is the same. The most common occurrence of this is in the addition of liquor from a hidden inventory: different proportions of two flows, of acid and of $Pu(NO_3)_4.6H_2O$, might be added whilst continuing to predict measurements *accurately*. Thus, for instance, a diagnosis of the addition of 5 Kg of material to a tank might be found to be composed of: either "transfer hidden-inv acc-tank 5.0 Kg" or "PuNO3 hinv8 acc-tank 5.0 Kg" or some combination. The addition to the tank could then be interpreted as either 100% acid, 100% plutonium nitrate, or some combination of the two, e.g. 70% acid + 30% plutonium nitrate.

The proportion can either be imposed automatically or manually: within the rule-sets of the sub-event combiner, any rule that involves aligned parameters should specify the proportions of each parameter by default, as part of the consequent of the rule, whereas when aligned parameters are chosen by the user as part of a manual diagnosis, the relative proportions of each aligned parameter can be adjusted by means of a set of sliders, one for each of the selected parameters, as shown in Figure 2.29.

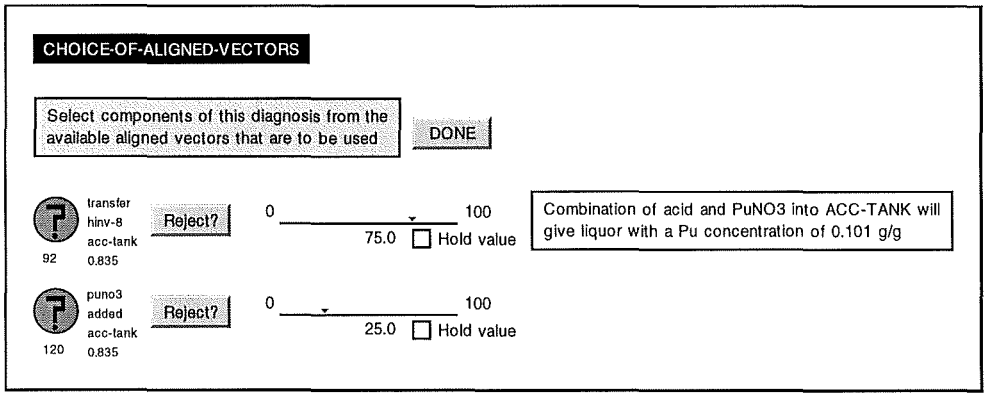


Figure 2.29: Choice of proportions for aligned vectors

In the manual case, the interface automatically ensures that the total of the proportions will equal 100% for each set of aligned vectors. The proportions chosen are then used to scale

the magnitude of the aligned parameters for use when running simulations. Additional features can be provided to make these proportions more meaningful. For instance, the plutonium concentration can be re-calculated and displayed as different proportions are selected.

2.11.5 Adding Hidden Events

This is to accommodate the unlikely event of the direct transfer of material into a pipe; on such occasions the material would only be detected when it was 'washed out' into a tank. If available, knowledge of such transfers can therefore be entered manually, via the interface shown in Figure 2.30.

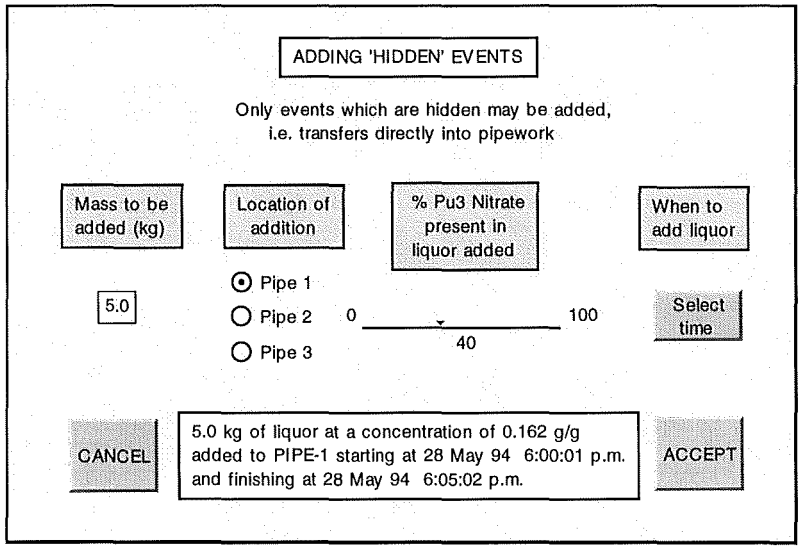


Figure 2.30: Addition of material from hidden inventory into pipe

2.12 Gradual Analysis

The purpose of performing a gradual analysis is to identify any of three main types of gradual event:

- the gradual transfer of material, where a small amount of material is transferred over a long period of time;

- the modification of a sequence of abrupt transfers pertaining to a particular unit; for instance, all transfers into Tank 1 from the inlet might be scaled by a small amount to compensate for incorrect estimation of the amounts transferred;

- calibration errors that can only be detected by analysing a sequence of measurements (Howell and Scothern, 1995a).

The approach is very similar to that for abrupt anomalies but with a few important differences (Howell and Scothern, 1995a): the simulation is performed over a much longer period of time; measurement models are now included explicitly because there are likely to be sufficient measurements with which to perform a correlation; and higher level gradual searches are only performed when lower level searches fail, due to the large amount of processing time needed to perform a gradual diagnostic search. Any gradual events thus identified are added to the list of events.

It is important to note that the diagnostic process here is largely an 'averaging' process, because correlation is performed over a significant period of time; the anomaly is assumed to be constant in time. This then prompts the question: 'what about a composite gradual/abrupt event?' e.g. one that starts out as a gradual event and then suddenly turns into an abrupt one. Stage 3 of the diagnostic process (Section 2.4), discussed in Section 2.13 below, is intended to search for these 'hybrid' events, amongst its other functions.

2.13 Diagnosing Remaining Errors

After the diagnostic procedure has completed its analysis for both abrupt and gradual anomalies, the simulation predictions are checked against the real data, to check for any remaining 'significant' errors that will require diagnosis. Which errors are deemed to be 'significant' can be altered by changing the number of standard deviations by which a simulated measurement is permitted to deviate from the real data. This list of errors is put into chronological order, and the earliest error is tackled first, on the basis that the correction of an error earlier in the time history, may have the effect of also correcting errors detected after it. After each error has been diagnosed, a new error time history is

generated, and the process repeated until all errors that can be diagnosed have been resolved. The automatic process used to correct the remaining errors is detailed below.

i) **Identifying The Original Source Of The Error:** The time at which the error may appear as significant is not always the time at which the error actually occurs, as it may be made up of several, individually insignificant errors. The first step is therefore to determine the time at which the error actually began. This is performed by working back in time from the point at which the error became significant, and examining the error at each measurement data point. If at some point the error changes direction, or the magnitude of the error falls below a certain level (e.g. 10% of the significant value), then this point is taken as the original source of the error.

ii) **Is The Error Due To Incorrect Initial Conditions ? :** If the original measurement in error is the first one of the day for the tank in question, then it is possible that the error is due to incorrect initial conditions, and so the state in question will be corrected, and no further action taken. Ideally, this will happen infrequently, since the goal of the diagnostic procedure is to ensure that the data matches successfully at the end of one day before moving onto the next.

iii) **Occurrence Of Error In Relation To Events:** The event list is checked to see if the original error is within an event occurring in the tank involved, or whether the error occurs during a period of tank inactivity, since this obviously has a significant bearing on the methods required to diagnose the error.

- **Error During Event:** If the error occurs within an existing event then the position of the error within the event is checked to see if a modification to the event will correct the error. This check is needed because under certain circumstances, a modification to the event will not correct the error, i.e. if the error occurs at the very start of the event, or the event is not a material transfer, or if the error occurs part way through, and the error at the end of the event is of a smaller magnitude. If this check deems the event suitable for modification, then the usual problem is that the flowrate has been estimated badly by the boundary condition generator. Based

on the size of the error, a new flowrate is calculated, and the simulation performed again. If the modification improves the simulation, it is left in, if not it is removed. If the simple approach of modifying the flowrate failed, a full diagnostic run is performed on the event under examination, to search for alternative diagnoses that may correct the error.

- **Error During Steady Period:** This type of error occurs when the boundary condition generator fails to detect a sub-event that should be present. This could be due to badly chosen parameters specified for the boundary condition generator, or simply that the amount of material transferred falls outside of the specified thresholds for detection. To correct the error, a new sub event is created, spanning from the time of the onset of the error to the time at which it was detected. This sub-event is examined by the diagnostic algorithm to generate hypotheses as to what occurred.

iv) **Measurement Errors:** It is possible that even after the application of all of the measures above, a suitable diagnosis for the correction of a specific error will not have been found. In this case, in order for the automatic system to be able to continue to investigate other errors, the error is deemed to be a measurement error. This is used as the last resort case, since this diagnosis could be used to explain any features present in the data.

v) **Manual Diagnosis:** After the automatic process has completed its analysis of the error time history, the user is able to view the diagnoses produced. If the user feels that any of the diagnoses are incorrect, features are available to allow the user to manually examine and diagnose any of the errors, using suggestions from the automatic system as a guide. Figure 2.31 shows an example of the information presented to the user to assist with such diagnoses.

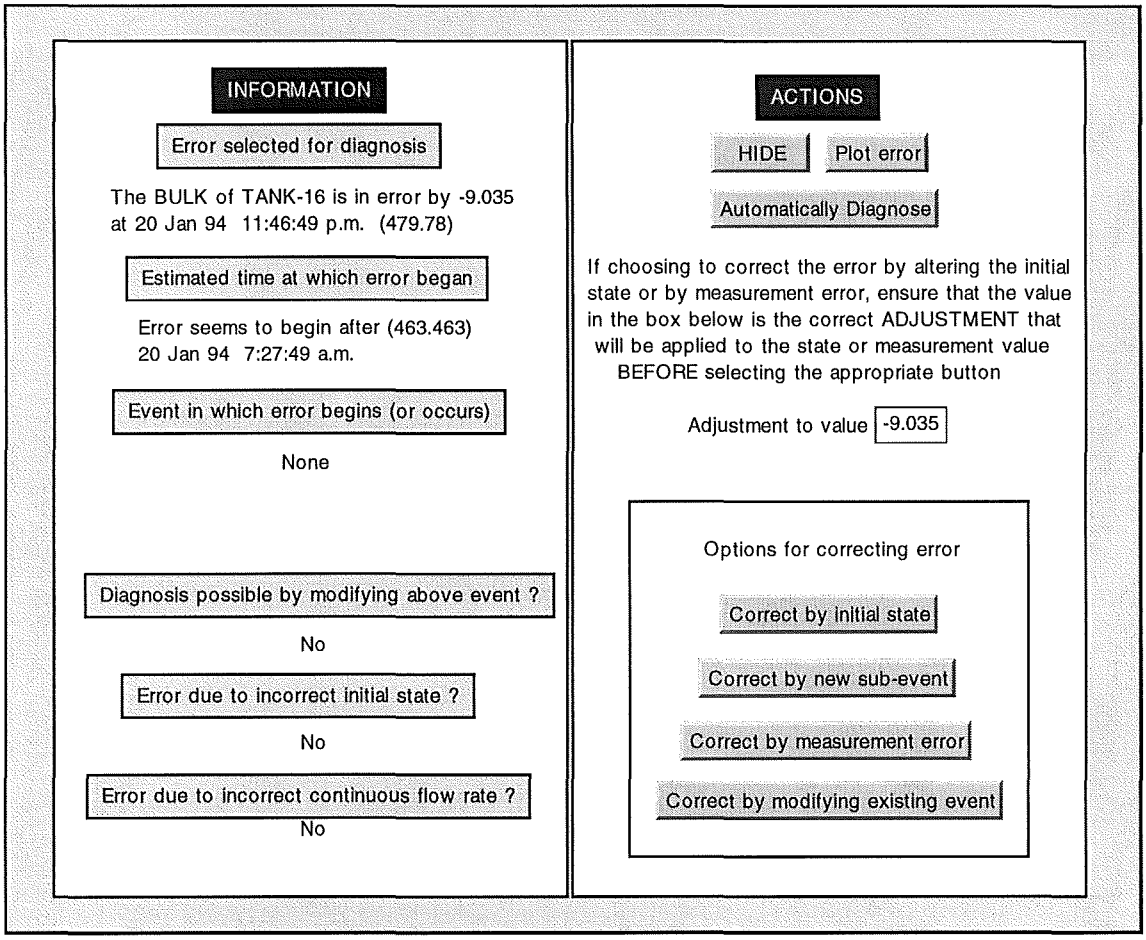


Figure 2.31: Manual diagnosis of an error

2.14 Example Of A Hybrid Gradual/Abrupt Event

Suppose that, during a sequence of three transfers from Tank 1 to Tank 2, a small amount is left behind each time in the pipework. Thus a gradual event would be observed. However suppose that all this material is washed out during the next transfer. The actual and simulated Tank 2 levels might then look like those shown in Figure 2.32. Depending on the magnitudes involved, it is possible that these activities would not be observed during Stage 1 of the diagnostic process presented in Section 2.4, and that, although detecting discrepancies, the 'averaging' process of the gradual analysis (Stage 2) would fail to produce any realistic solutions also. The diagnosis of such a sequence of activities would be performed during Stage 3, described in Section 2.13 above. The next sub-section examines how this procedure would be applied to diagnose the sequence of events.

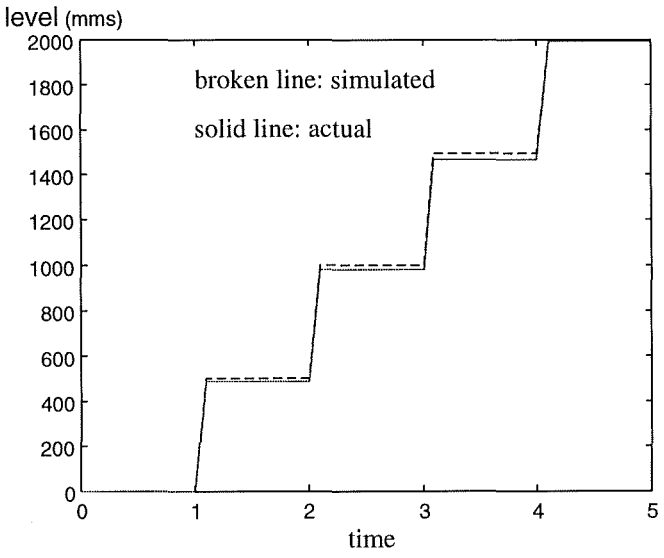


Figure 2.32: Effect of pipe hold-up on tank 2 level

2.14.1 Analysis Of The Error Time History

The error time history might, depending on the settings chosen for the 'significance' of errors, only show errors occurring after the third transfer into the tank, as this is where the cumulative effect of the hold up in the pipe is the most pronounced. The diagnostic process carried out for this example would then be as follows:

i) the source of the error would be traced back through the simulation history, which would determine that the error originated during the first transfer, since prior to this, the tank was empty, and the error zero;

ii) since the error is not at or before the start of the day, an incorrect initial condition would be ruled out;

iii) the error would be found to be present within the first transfer event into the tank. A simple alteration in the flowrate to this tank would not be successful (since fixing the error in this tank by altering the flowrate in would cause a similar size error in the tank from which the transfer originated). The diagnostic procedure would then be applied,

and alternative diagnoses generated. In this case, the error would be attributed to an increase in the residual pipe hold-up, which would be superimposed upon the existing event.

Since the error in the event under examination was diagnosed successfully, a new event history would be generated, and the process repeated. The next iteration would find the source of the error to be the second transfer, and so on. The end result of the repeated applications of the process would find that the first three transfers increased the hold up in the pipework, while the final transfer returned the hold up to normal levels by returning all of the 'missing' solution.

2.15 Failings Of The System

The system described above has been successfully applied to many test scenarios, and to many different sets of data. However, there have been some cases in which the process has failed to produce the desired results using the automatic procedures alone. These cases are detailed below.

2.15.1 Continuous Flowrates

Due to the nature of the scanning process, one of the most frequent source of errors is incorrectly specified flow rates to or from continuous plant elements, e.g. solvent extraction areas or concentrators. Since these elements are continuous, even small errors in the flow rates build up over time, until they eventually become significantly in error. Ideally, the system should be able to adjust the estimated flowrate slightly so that the simulation does not drift into error over time. Automatically determining if such a drift is present is frequently not straightforward, due to the difficulty in deciding what part of the error is due to this gradual drift, and what is due to as yet unresolved abrupt modifications that may need to be made. Unfortunately, diagnosis of these abrupt errors will often not be possible until the drift in the continuous elements is corrected, leading to a circular problem.

2.15.2 Multiple Simultaneous Errors

An additional problem area is the (rare) case in which multiple errors are present in many measurements during a short period of time. The diagnostic procedure is theoretically capable of resolving many simultaneous errors, but the cost of computation is very high, as all possible permutations of the many perturbations are examined. To limit this combinatorial problem, the diagnostic procedure was restricted to resolving three simultaneous errors at once. As the size of the plants under investigation increases, the chance of such a multiple error occurring increases. The problem of multiple simultaneous errors, or common mode faults, is a well known one, and many diagnostic systems have a maximum number of simultaneous faults which can be accommodated, for example the MIDAS system produced by Finch et al, (1990), can only diagnose multiple malfunctions if each malfunction has a 'non-overlapping' set of symptoms.

It should be noted that many of the problems encountered are due to either the unusual nature of some of the simulated plant data that the diagnostic procedures were tested on, or to the filtering algorithm used on noisy data, and as such, the problems encountered may be reduced when the techniques are applied to real data.

2.15.3 Resolving The Difficulties

In order to provide a workable system, a compromise was reached between automatic and manual diagnosis, in which the system would ignore all errors associated with continuously fed plant elements, and set any multiple simultaneous errors to be measurement errors during the automatic diagnosis phases. Following this, the user would be asked to manually diagnose each of the remaining errors, using information and guidance from the automatic system.

CHAPTER 3

3. REFINEMENTS TO THE DETERMINATION OF SUB-EVENT DIAGNOSES

3.1 Introduction

Considerable research has been carried out into the detection and diagnosis of faults, see for instance, Willsky (1976), Himmelblau (1978), Isermann (1984), Milne (1987), Patton et al (1989) and Frank (1990). However, the approaches have largely concentrated on plants or systems which are information rich, which may not always be the case for nuclear materials safeguards. The diagnostic technique referred to throughout this thesis is based upon an approach to model-based fault detection described by Howell (1994), which is particularly well suited to solution monitoring since it is capable of dealing with non-linear plants which are information poor. However the original algorithm was somewhat limited, and this chapter details some of the modifications and additions made. Specifically, it covers the adaptation of the way it handles aligned vectors to reduce computational overheads and explores various alternatives to the simple regression techniques used when searching for an acceptable solution. The alternatives discussed are repeated iteration of the diagnostic algorithm, re-using the initial solution as the starting point for further regression, Powells method (Powell, 1968) and the downhill simplex method (Nelder and Mead, 1965).

3.2 The Diagnostic Technique

3.2.1 Introduction To The Diagnostic Algorithm

The aim of the diagnostic algorithm proposed by Howell (1994) is to perturb a model of the plant in various ways until it produces reasonable predictions, that is all the *residues*

(differences between the plant measurements and the model predicted measurements) are reduced to lie within acceptable tolerances. The *diagnosis* is then the model adaptations needed to obtain agreement. Figure 3.1 shows the relationship between the plant, the model and the diagnostic system.

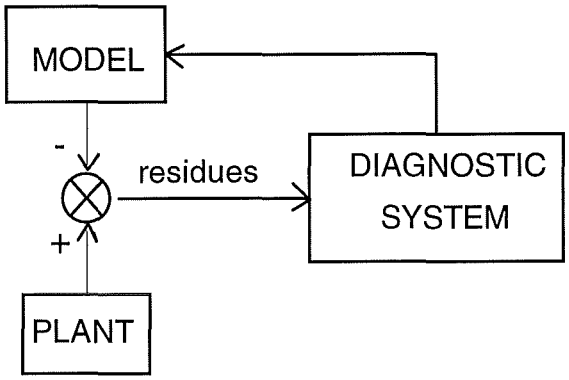


Figure 3.1: Model based diagnosis

The strategy followed is topographic rather than symptomatic since it has the potential to identify any fault, even those not previously anticipated. It is also lateral rather than procedural, which is important in safeguards because if the procedure became known then means could be devised to avoid detection and fool the procedure. It should be noted that the models used need not be accurate in general; accurate model predictions are only required for a set of specified plant measurement records. This is important since model complexity is likely to increase with both the number of sensors installed and with the accuracy required.

The approach is to view the plant as an inter-connection of process units (*nodes*) connected by paths along which energy and material can travel, since safeguards is primarily concerned with the movement of material, i.e. it is concerned with material flows. The Principle of Redistribution (Howell, 1994) states that anomalies will either cause a re-distribution of material or energy around the plant or they will cause something more localised like a measurement error. If a plant incident causes un-modelled perturbations in one or more of the path flows, such as a transfer between two tanks which is not listed in the boundary conditions of the simulation, the model will fail to predict the

plant measurements. However the estimate of the total mass in the plant will be correct unless one or more of the flows across the plant boundary are also in error. The diagnostic approach identifies those perturbations in flows along identifiable paths that would explain the re-distributions observed or put another way, identifies those flows that would result in the model predictions aligning with the plant measurements. At the same time, however, the approach also accommodates the more local effects like measurement errors. The perturbations that cause the re-distributions are known as path errors whilst the local effects are known as non-path errors. The goal of the diagnostic procedure is to find *all* of the possible diagnoses that can explain the differences between the plant data and the simulation predictions.

Section 3.2.2 below focuses on how the diagnostic algorithm and the model simulation interact to create a picture of how perturbations in the model affect the measurements produced. Section 3.2.3 introduces the search algorithm used to determine which combinations of perturbations are suitable candidates for correcting the simulation.

3.2.2 How The Diagnostic Program Views The Computer Simulation

The **function** of the simulation is to estimate the measurements recorded at specified times on the basis of a particular hypothesis. Thus the interfaces between the simulation and the other components are relatively straightforward: the initial/boundary conditions are **input** into the simulation and the measurement estimates are **output**. Measurements can be recorded at any time after the specified start time resulting in a list of measurement times, $t_k, t_{k+1}, t_{k+2} \ldots, t_{k+n-1}$ where n is the number of times when measurements have been recorded. Only a limited number of measurements might be recorded at any one time: let $\tilde{y}_k^*$ denote an estimated (~), compound (*) output vector formed by appending measurement estimates obtained at time t_k to those collected at time t_{k-1} and so on. Let $\hat{y}_{k-1}^*$ denote the corresponding compound measurement (^) vector at the start of the specified time period i.e.

$$\hat{y}_{k-1}^* = (\hat{y}_{k-1}^T \hat{y}_{k-1}^T \ldots \hat{y}_{k-1}^T)^T \tag{3.1}$$

(Note that if an abrupt anomaly were hypothesised, n = 1, $\tilde{y}^*_k = \tilde{y}_k$ and $\hat{y}^*_{k-1} = \hat{y}_{k-1}$, since during the diagnosis of abrupt events, only the final measurements are used).

Then the simulation can be viewed as a *black box* of the form

$$\tilde{y}^*_k = \hat{y}^*_{k-1} + f^*(\hat{x}_{k-1}, \hat{\theta}_k, k, k+n-1) \tag{3.2}$$

That is $\mathbf{f}^*$ is simply a mapping of a (compound) vector of measurements at the start of the simulation onto a (compound) vector of measurement estimates. The residuals are then $\hat{y}^*_k - \tilde{y}^*_k$. Vector $\hat{\theta}_k$ represents those boundary conditions whose manipulation might eliminate (i.e. zero) the residuals; thus it relates to the re-distribution variables, corresponding to paths that material may take to move around the plant, and non-path parameters that are needed to specify the model. Vector $\hat{\theta}_k$ is constrained by the assumption that it must remain constant during the entire period of time of interest (i.e. $\hat{\theta}_k = \hat{\theta}_{k+i-1}\ \forall i \le n$). Thus for instance an element of $\hat{\theta}_k$, $\{\hat{\theta}_k\}_i$ might represent a multiplier of a particular re-distribution variable, such as transfers between tank 2 and tank 3, or a time a pump is switched on or a tank calibration parameter and so on. As far as the diagnostic algorithm is concerned, the exact methods by which $\mathbf{f}^*$ accomplishes its mapping function are unimportant; all that is required is knowledge about how the measurements are affected by altering values of the boundary conditions. Details of the simulation model itself are given in Chapter 4.

The original formulation was only suitable for diagnosis of abrupt events, since it simulated only the net changes in the nodes, and only concentrated on how the final measurements were affected by perturbations to the system. To facilitate the genericity requirements of automatic model generation, which must also include gradual events, an additional constraint was imposed: those elements affecting paths are constrained to be multipliers, so, for instance, the true mass transfer history along a particular path would be represented as $[1+\{\hat{\theta}_k\}_i]$*default_history and the time a particular pump is switched on would be represented by $[1+\{\hat{\theta}_k\}_i]$*default_time. The vector is then initialised as a vector

of zeros. This approach obviously means that defaults need to be specified, and suggestions for doing so are given in Howell and Scothern (1995a).

The diagnostic program uses the above simulation interface to calculate the effect that changes in any boundary condition would have on all measurements. It performs this function by using a numerical perturbation technique to examine the effect that any **multiplicatively induced** path error would have on the residuals. Each path variable is perturbed by scaling its history and the resultant effect on the model obtained by repeating the simulation. In this way a global Jacobian-like matrix **J** is produced, such that:

$$J = \left[\frac{\Delta y_k^*\big|_1}{\{\Delta\theta_k\}_1} \quad \frac{\Delta y_k^*\big|_2}{\{\Delta\theta_k\}_2} \quad \ldots\ldots\ldots \right] \tag{3.3}$$

where $\Delta y_k^*\big|_j = \hat{y}_{k-1}^* + f^*(\hat{x}_{k-1}, \hat{\theta}_k + \{\Delta\theta_k\}_j . e_j, k, k+n-1) - \tilde{y}_k^*$.

In other words, the form of each entry J_{ij} in the matrix is:

Change in measurement j / change in variable i

The technique presented in Howell (1994) also incorporated the effect of local perturbations, which is neglected here because of the abnormally high number of re-distribution variables that are notionally zero.

As a refinement to the published technique, all flows are constrained to be positive in value (a negative flow would be represented by another path variable defined in the other direction): should the perturbation algorithm attempt to apply a negative value as a multiplier, this value will be converted to a positive small number, the larger the negative value, the closer to zero the actual value will be. This ensures that the perturbation algorithms are still driven in the correct direction, without producing unsuitable values for the simulation. Not permitting negative flows also allows information on plant construction to be more effectively utilised, for example, if two tanks are connected in

such a way so that it is physically impossible for material to flow from tank 2 to tank 1, then a diagnosis which implied that such a flow had taken place by including a negative flow from tank 1 to tank 2 will not be suitable.

3.2.3 The Diagnostic Algorithm Search Strategy

The preceding section detailed the methods use to determine how perturbations in the boundary conditions affected the measurements produced by the simulation. Once all of this information is known, the diagnostic algorithm must attempt to find all possible combinations of these perturbations which are successful in explaining the differences between the simulation predictions and the actual plant measurements. The algorithm is based on a parsimonious search strategy which is justified on the grounds that differences that result from a major anomaly are likely to be significantly larger than those caused by model inaccuracies. All combinations of first 1, then 2 and finally 3 elements of $\hat{\theta}_k$ are hypothesised as anomalous, one combination at a time, and their true values are estimated by performing a regression with all available measurements. Each set of estimates are then tested by re-running the simulation to determine whether its output now *matches* the measurements. The regression takes the form

$$E\{\theta_k^+ \left| (\hat{y}_k^* - \tilde{y}_k^*) \right.\} = \hat{\theta}_k^+ + P_k J'(R_{k-1} + R_k + JP_k J')^{-1}[\hat{y}_k^* - \tilde{y}_k^*] \tag{3.4}$$

where $\hat{\theta}_k^+$ is the particular vector of 1,2 or 3 variables, $\mathbf{P}_k$ is their associated **subjective** covariance, $\mathbf{J}$ is the global Jacobian-like matrix defined previously, and $\mathbf{R}_k$ is the measurement vector covariance. For details on the specification of the various covariance matrices, see Howell and Scothern (1995a).

Differences between the simulation predictions and the plant measurements only require the diagnostic procedure to be applied if the magnitude of the differences is deemed to be significant. The threshold test used to determine if the residual from an individual prediction is significant is:

$$\left| \{\hat{y}_k - \tilde{y}_k\}_i \right| \leq n_i \sqrt{\{\sigma_{k-1}^2 + \sigma_k^2\}_i} \tag{3.5}$$

where n_i is a user specified parameter, and the two standard deviations pertain to the measurement recorded at the current time and the time from which the simulation was executed. The choice of parameter n_i is subjective, and the intention is that it should be specified to reflect model uncertainty; if the model was perfect and the standard deviations were known accurately, then n_i would probably be set to 3 to avoid the detection of a purely noise generated mismatch. The value of n_i can also be used to emphasise the perceived importance of, for example, level measurements over density measurements. In previous studies, n_i has been set to 4, for volumes and for samples, to reflect some caution in model accuracy, and set to 16, for densities, partly to focus on level measurements and partly to reflect a lack of confidence in the standard deviations that were available at the time.

3.3 Reduction Of The Search Space Through The Use Of Aligned Vectors

When dealing with the diagnosis of a realistically sized plant, it is often the case that the number of parameters available for perturbation can be quite large, since all possible flow paths have to be included. For instance, for one particular case of a product storage area comprising of eight tanks and a sample pot, the number of parameters representing possible flow paths was 101, and added to this number were other, non path parameters such as initial states in the tanks, rate of pump heating etc. which raised the number of parameters available for perturbation to 137. Also included are potential measurement errors for each tanks sensors, and so the final total was 164.

When using the diagnostic procedure to solve for a particular problem, only the subset of this number that directly or indirectly affects the measurements in error are considered, but in many cases this can still be a sizeable number, particularly in cases where there is significant interconnection and interdependence between various elements. The diagnostic procedure needs to examine all possible permutations of combinations of these remaining parameters when looking for acceptable solutions, and when dealing with such combinatorial sets of parameters the time taken for computation can be quite large.

A method of reducing the number of combinations considered would have a significant effect in reducing the time needed to perform a diagnostic. Rai and Weinroth (1990) point out that, '*The reduction in the search space for the solution to the problem must occur as soon as possible in the solution process*', and Siklósy and Tulp (1991) add to this '*When searching, it often pays to first reduce the size of the search space, and then to search. The pay-off is increased if several searches are performed*', and also highlight one of the dangers of reducing the search space, namely '*When cutting the search space, we must be careful not to eliminate the optimal or interesting solutions to the problem*'. Many different methods for reducing search spaces for a variety of different problems exist, for example Raj and Weinroth (1990) suggest an expert system approach to the problem, posing various questions to the user to determine which areas of the search space are feasible in the current context. However, due to the particular nature of the diagnostic algorithm, the use of aligned vectors was chosen as the most suitable method, since it does not lose any significant information, the method can be 'tuned' to allow varying degrees of alignment, and the underlying concept is straightforward, which is important from the inspectors point of view.

The basic principles of the use of aligned vectors within the diagnostic algorithm are presented by Howell (1994). However, this paper makes no recommendations for the choice of tolerances that are required when determining if two vectors are aligned, and the method provided for selecting a primary vector from a particular group of aligned vectors was found to need refinement in certain circumstances. This Chapter addresses both of these issues.

3.3.1 Description Of Aligned Vectors

To try to reduce the large number of parameters which may be present for a particular problem, use is made of 'aligned' vectors. In this context these are defined as parameters which have roughly the same effect as others. In the ideal case, where the effects of multiple parameters on the measurement vector are identical, then any one of the multiple parameters can be replaced with any one of the others. In the diagnostic algorithm, this

means that a group of aligned parameters are included in the list of parameters to be examined as a single parameter, which can reduce the search space significantly.

For example, when diagnosing a sudden drop in the level of a tank, it may be the case that several locations are available for receiving material from the tank. Should more than one of these locations be unmeasured for any reason, i.e. faulty sensors, no sensors installed etc., then a transfer to any of these unmeasured locations will have exactly the same effect on the measurement vector, i.e. all will affect only the level in the tank which is the source of the transfer. In such a case all the unmeasured locations can be represented by a single parameter. In practice, the effect of one parameter is usually never identical to another, since small secondary effects are usually present. However, a method of specifying the amount of deviation from the ideal can be used, allowing vectors to be said to be aligned, should they be sufficiently 'close' to alignment.

3.3.2 Alignment Criteria

The vectors in question are the columns of the main Jacobian-like matrix used by the diagnostic procedure, described in Section 3.2.2; each column represents the effect of a different parameter on the entire measurement vector.

The form of each entry J_{ij} in the matrix is:

Change in measurement j / change in parameter i

When comparing columns for the purpose of determining alignment, the entries are scaled by the standard deviations of each measurement, so the relative importance of each change is taken into account, rather than just the magnitude of the change.

The criteria for perfect alignment of two vectors $\underline{\mathbf{a}}$ and $\underline{\mathbf{b}}$ is :

$$\frac{(\underline{a}.\underline{b})^2}{(\underline{a}.\underline{a})(\underline{b}.\underline{b})} = 1 \qquad (3.6)$$

If this condition holds exactly then the vectors in question are in parallel, and may differ only by a scaling factor. The test applied to the scaled column vectors of the Jacobian matrix allows less than perfect alignment to be accepted, and is of the form:

$$\left|1-\frac{(\underline{a}.\underline{b})^2}{(\underline{a}.\underline{a})(\underline{b}.\underline{b})}\right| \leq \text{tol} \tag{3.7}$$

Where *tol* is a small parameter, 0<=*tol*<1 (A *tol* of 1.0 would allow any, even perpendicular, vectors to be selected as aligned, while a *tol* of 0.0 would allow no deviation from exactly the same direction).

3.3.3 Choosing A Suitable Value Of Tol

The choice of *tol* should be made with care; too small a value will result in very few successful alignment matches, with the consequent cost in computational overhead, while too large a value may cause undesirable vectors to be dealt with as aligned, which may hide important secondary effects present in one of the vectors.

Without any loss of generality, since scaling factors will cancel and dot products are position independent, assume $\underline{a}$ and $\underline{b}$ are vectors of the form :

$$\underline{a}=[1\ 1\ 1\ 1\ 1\ .....\varepsilon\ \varepsilon\ \varepsilon\ \varepsilon\ \varepsilon\ \varepsilon\ \varepsilon\ ] \tag{3.8a}$$

$$\underline{b}=[1\ 1\ 1\ 1\ 1\ .....\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ ] \tag{3.8b}$$

i.e. both vectors are of length **n,** with the first **p** entries set to 1 and the remaining (**n-p**) entries set to ε or 0. These vectors are very similar, but whether they are taken to be aligned or not depends on the value chosen for ε and the number of 1's to 0's or ε's. Calculation of the various products gives :

$$(\underline{a}.\underline{a})=\mathbf{p}+(\mathbf{n}-\mathbf{p})\varepsilon^2 \tag{3.9}$$

$$(\underline{b}.\underline{b})=\mathbf{p} \tag{3.10}$$

$$(\underline{a}.\underline{b})=\mathbf{p} \tag{3.11}$$

So the criteria for alignment becomes :

$$\left|1-\frac{p^2}{p(p+(n-p)\varepsilon^2)}\right|<tol \tag{3.12}$$

Now,

$$\frac{p^2}{p(p+(n-p)\varepsilon^2)}=\left[1+\left(\frac{(n-p)\varepsilon^2}{p}\right)\right]^{-1} \tag{3.13}$$

And expanding as a power series :

$$\frac{p^2}{p(p+(n-p)\varepsilon^2)}=1-\left(\frac{(n-p)\varepsilon^2}{p}\right)+\left(\frac{(n-p)\varepsilon^2}{p}\right)^2-\left(\frac{(n-p)\varepsilon^2}{p}\right)^3+.... \tag{3.14}$$

For convergence of this series,

$$\left(\frac{(n-p)\varepsilon^2}{p}\right)<1 \tag{3.15}$$

and for acceptance as aligned,

$$\left|\left(\frac{(n-p)\varepsilon^2}{p}\right)-\left(\frac{(n-p)\varepsilon^2}{p}\right)^2+\left(\frac{(n-p)\varepsilon^2}{p}\right)^3-....\right|<tol \tag{3.16}$$

(n-p)/p is just the ratio of number of **0**'s or **ε**'s to number of **1**'s present in the vector, and is independent of the actual length of the vector itself, as shown in Table 3.1. Table 3.2 illustrates the variability of the value of *tol* required depending on the particular characteristics of the vectors under examination. This table shows various values of **(n-p)/p** and **ε**, and gives the minimum value of *tol* that would be required to allow the vectors to be taken to be aligned.

Any arbitrary choice of *tol* will be less than optimum, since there will always exist the potential that two undesirable vectors will be aligned, or that other vectors, which should be aligned, will not be. This depends to a large extent on the nature of the vectors under

investigation, of the relative number of zero to non-zero components, and the value of ε, which is itself subjective.

n	p	(n-p)/p
10	10	0
10	8	0.25
10	5	1
10	1	9
100	100	0
100	80	0.25
100	50	1
100	10	9
100	5	719
100	1	99
1000	1	999

Table 3.1: Values of (n-p)/p

In practice, a value of *tol* needs to be chosen which will give good behaviour in the majority of cases. Bearing this in mind, a value of 0.001 was recommended. To examine the consequences of choosing this value, two cases are considered, firstly vectors with a high proportion of 1's, and secondly vectors with a low proportion of 1's. For vectors which comprise 80% 1's, (corresponding to **(n-p)/p** of 0.25) the maximum value of ε found is 0.06. For vectors which comprise 10% 1's, (corresponding to **(n-p)/p** of 9.0) the maximum value of ε found is 0.01. So the first case would allow values of ε up to 0.06 to be classed as aligned with a similar vector where the ε's were all zero, while the second case, only vectors with ε values up to 0.01 would be classed as aligned with the similar vector. This actually seems to be a desirable property, since a vector with a large proportion of 1's will be less affected by deviations in ε than a vector in which the ε's far outnumber the 1's.

(n-p)/p	**ε**	***tol* required to allow as aligned**
0.0	Any	Automatically aligned *
0.25	0.00001	2.500e-11
0.25	0.0001	2.500e-9
0.25	0.001	2.500e-7
0.25	0.01	2.500e-5
0.25	0.1	2.494e-3
1.5	0.00001	1.500e-10
1.5	0.0001	1.500e-8
1.5	0.001	1.500e-6
1.5	0.01	1.500e-4
1.5	0.1	1.477e-2
4.0	0.00001	4.000e-10
4.0	0.0001	4.000e-8
4.0	0.001	4.000e-6
4.0	0.01	3.998e-4
4.0	0.1	3.846e-2
9.0	0.00001	9.000e-10
9.0	0.0001	9.000e-8
9.0	0.001	9.000e-6
9.0	0.01	8.992e-4
9.0	0.1	8.257e-2
99.0	0.00001	9.900e-9
99.0	0.0001	9.900e-7
99.0	0.001	9.899e-5
99.0	0.01	9.803e-3
99.0	0.1	2.911e-2
999.0	0.00001	9.990e-8
999.0	0.0001	9.990e-6
999.0	0.001	9.980e-4
999.0	0.01	9.803e-2
999.0	0.1	**

Table 3.2: Value of *tol* required for different vector characteristics

* If **(n-p)/p** = 0 then **n=p,** so both vectors consist just of **1**'s, and so are exactly aligned, regardless of the value of *tol*

** Fails, since for convergence of power series, each term must be below 1.0, and here power series is 9.99-(9.99)^2+ etc. which diverges.

The diagnostic procedure itself has several optional features relating to aligned vectors, such as the ability to automatically alter the value of *tol* used until at least some aligned vectors are found. It should also be noted that although the search algorithm within the diagnostic procedure will group all aligned variables together, these groupings will be automatically expanded when used to match sub-events to events, so the information will not be hidden or lost.

3.3.4 Choice Of Primary Vector

If several columns are flagged as aligned, then one has to be chosen as the 'primary' vector, i.e. the most suitable vector to choose for the purposes of the diagnostic procedure. The decision is made by choosing that column which contains the highest magnitude entry, again scaled by the appropriate standard deviation to give the most significant change rather than just the largest. There is one exception to this: if any of the columns under investigation were successful in solving the most important measurement error, (i.e. the measurement error which is the most standard deviations from its correct value), then the column chosen will be the column which contains the highest magnitude scaled entry of these only, since the other aligned parameters have their primary effect on less serious measurement errors.

3.4 Improving The Candidate Solution Generation Approach To Accommodate Grossly Non-Linear Models

The current diagnostic algorithm performs regression based on a global Jacobian-like matrix, as described previously in Section 3.2. This matrix is formed by solving, for each variable in turn, the most significant residual. Each column in this matrix represents the effect of a different parameter on the entire measurement vector, so that each element J_{ij} is given by :

Change in measurement j / change in parameter i

Thus, although the regression approach will be appropriate when predicting the most significant residual, it might be inappropriate for predicting other residuals. This is

particularly so when the model is very non-linear. After generating the Jacobian matrix J, (equation 3.3), the regression method tries to minimise the sum of the squared errors in the measurement vector, after which the remaining errors are examined to determine if any of them are 'significant', using the tolerance check described in Section 3.2.3. This is decided using the standard deviations of each measurement, which are themselves based on a supplied subjective probability (for details, see Howell and Scothern, 1995a). The advantages of this regression based approach are that it is fast, and in general successful for finding acceptable solutions. The disadvantage is that it can occasionally fail to find solutions which the minimisation approaches presented below will find, if they are possible, although much more computation is required.

The following sections detail three extensions to the regression process that have been examined, each of which takes the result of the regression analysis as its starting point, and attempts to find a better solution. The methods for dealing with this problem that have been examined are:

1. further iteration,
2. Powells method, and
3. the downhill simplex method.

3.4.1 Further Iteration

As a method of improving upon the initial solution generated by the regression process within the diagnostic algorithm, this initial solution can be input to the diagnostic program as a new starting point, and the diagnostic procedure repeated. In this way the solution produced can be refined and improved with each iteration.

3.4.2 Non-Linear Optimisation

The second approach is to attempt to find an acceptable solution by trying to minimise a function of the residuals, using standard minimisation routines, such as those found in Press et al (1992). These avoid the evaluation of residual derivatives which either might be difficult to obtain or are only correct locally for a highly non-linear model. Popular

algorithms include the Downhill Simplex Method (Nelder and Mead, 1965) or *direction-set* methods, of which Powells Method is the well known prototype (Powell, 1968).

For both of the methods considered here, the problem can be stated as follows :

Minimise a function ***F(P),*** where *P* is a point in N-dimensional space.

The function of the residuals chosen for minimisation is :

$$F(P) = \sum_i \left(\frac{\hat{y}_i - \bar{y}_i}{\sigma_i} \right)^2 \tag{3.17}$$

where *P* in this case is a vector made up of the values used by the diagnostic algorithm for the perturbation of up to 3 parameters, i.e. the dimensions of the solution space depend on the number of parameters perturbed simultaneously.

Ratio $(\hat{y}_i - \bar{y}_i)/\sigma_i$ gives the number of standard deviations a measurement is in error by, and minimising the sum of the squares of this over all measurements should give an answer which is the minimum number of standard deviations away from the result required.

3.4.3 Powells Method

An obvious method of minimising a function in N-dimensional space is by taking the unit vectors $e_1 \ldots . e_N$ as the *set of directions* and then using a linear minimisation algorithm (such as Brents method, 1973) to move along each unit vector in turn, to find the point with the minimum of the function in that direction, and using this point as the starting point for linear minimisation along the next unit vector. The unit vectors are repeatedly cycled through in this way until the function stops decreasing to within a chosen tolerance.

This simple method can be improved by choosing an improved set of directions, such as conjugate directions, with the property that minimising along any one direction does not adversely affect the minimising along the other directions. Such a choice of improved directions should help prevent excessive cycling through the chosen set of directions.

Powells method is a direction set method that produces a set of N mutually conjugate directions, and can be stated by the list of steps below.

1. Define, the set of N directions $\boldsymbol{u_1}.....\boldsymbol{u_N}$ as the simple unit vectors $\boldsymbol{e_1}.....\boldsymbol{e_N}$, and specify the starting point (i.e. the initial guess), $\boldsymbol{P_0}$.
2. For each value of i in turn, from 1 to N, move from point $\boldsymbol{P_{i-1}}$ along direction $\boldsymbol{u_i}$ to the point with the minimum value of F along this direction and name this new point $\boldsymbol{P_i}$.
3. For each value of i in turn, from 1 to N-1, set $\boldsymbol{u_i} = \boldsymbol{u_{i+1}}$ and set the final direction in the set to $\boldsymbol{u_N} = \boldsymbol{P_N} - \boldsymbol{P_0}$, i.e. the new direction is the direct route from the start point to the final point reached after minimising F along all N possible directions.
4. Minimise F along direction $\boldsymbol{u_N}$ and rename this point $\boldsymbol{P_0}$.

Each point $\boldsymbol{P_i}$ moved to will have improved the value of $\boldsymbol{F(P)}$, which is the function being minimised. Steps 2 to 4 are repeated until convergence occurs, i.e. until $\boldsymbol{F(P)}$ stops decreasing to within a specified tolerance.

The actual method used was a modified version of Powells method, where the modifications are made to avoid a build-up of linear dependence within the set of directions, see Acton (1970) and Press et al (1992) for details. Powells method requires an initial estimate for the values involved, and since the regression algorithm has already made one pass and produced an initial estimate of the parameters, these values can be used as the starting point.

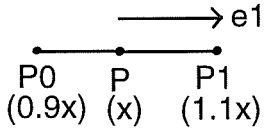
3.4.4 The Downhill Simplex Method

A simplex in N dimensions is just a geometrical figure consisting of N + 1 points and all of the lines that join these points, e.g. a two dimension simplex consists of 3 points, and their connecting lines, and so is obviously a triangle. Similarly a 3 dimensional simplex is a tetrahedron, and so on. The following section assumes that any simplexes used are non-degenerate, i.e. they enclose a finite, N dimensional volume within the simplex.

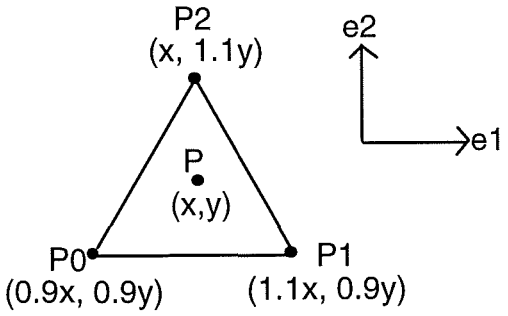
3.4.4.1 Initial Conditions

The Downhill Simplex method requires more than a single starting point, it requires an initial simplex, consisting of N + 1 points. In the diagnostic algorithm , the initial simplexes chosen were straightforward shapes surrounding the initial estimate as generated from the diagnostic algorithm, labelled *P*, as shown below :

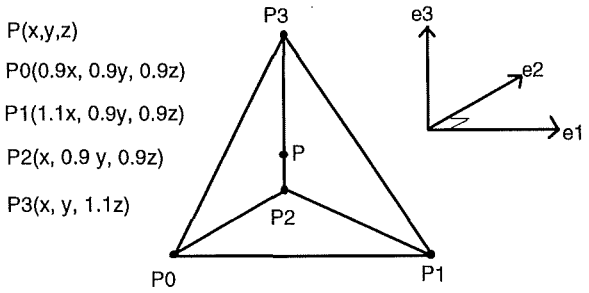
N = 1, Simplex formed from points P0 and P1.



N = 2, Simplex formed from points P0, P1 and P2



N = 3, Simplex formed from points P0, P1, P2 and P3



3.4.4.2 The Method

The simplex method itself consists of repeatedly applying a series of steps which adjust the points of the simplex in various ways, each of which is designed to search for improved values of F at the points of the simplex. In this way, the simplex moves through the solution space, searching for the minimum value.

The various possible steps are listed below :

- Contraction

  The simplex is contracted along one dimension, by moving the point of the simplex which currently is at the worst, or highest value of the function to be minimised.

- Multiple contraction

  The lowest point of the simplex remains fixed, while all the other points in the simplex are moved towards the low point.

- Reflection

  The high point of the simplex is reflected through the opposite face of the simplex, to a point with a lower value of F, conserving the volume of the simplex to as to ensure that it remains non-degenerate.

- Reflection and expansion

  The high point of the simplex is reflected through the opposite face of the simplex as above, but the final volume of the simplex is increased, (again, implying non-degeneracy).

The selection as to which of these steps will be performed depends on the nature of the function to be minimised at the points of the simplex. The most frequently performed step

is the simple reflection, with the reflection and expansion performed when possible to allow the algorithm to take larger steps in the expanded direction.

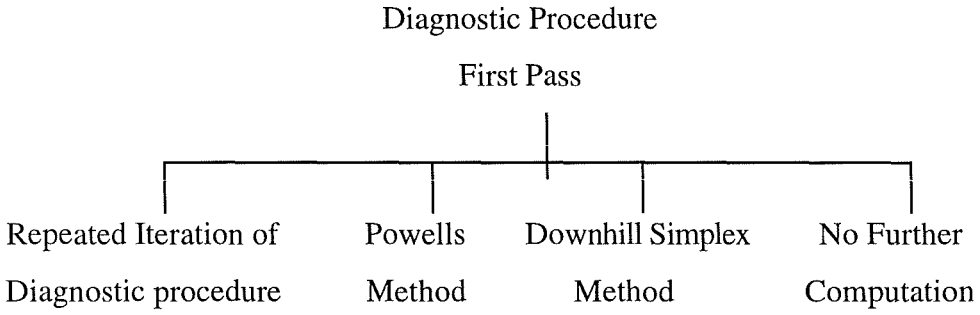
Contractions are used when the simplex reaches a 'valley' in the values of F, and the simplex contracts itself in the direction across the valley and then continues to move in the direction along the valley floor. Multiple contractions are used for more extreme cases, where instead of a valley, the simplex encounters a narrow area or 'hole' in which the values of F are better and the simplex shrinks itself down, around its lowest point in order to fit this 'hole'.

3.4.4.3 Convergence Criteria

The convergence of the Downhill Simplex method can be detected by several methods, e.g. by the fact that the 'best' value of the function F over all the points of the simplex has not changed by more than some specified tolerance, or by calculating that the vector distance moved by the simplex itself is less than some other specified tolerance.

3.4.5 Drawbacks And Advantages Of Each Method

As shown in the flow chart below, all of these methods have been incorporated as options into the diagnostic algorithm.



All approaches are computationally intensive and, if applied to every candidate which fails to provide an acceptable solution using the diagnostic algorithm, would cause the time

needed for a full run to be increased dramatically, although this is much more pronounced in the case of Powells method.

Repeated iteration requires few iterations, but each iteration requires large sections of the diagnostic procedure to be performed, (excluding re-building of the global Jacobian, since only the columns under investigatation need to be recalculated). Compared to Powells method, re-iteration is much less computationally intensive, but is not guaranteed to find a solution which will be acceptable according to the final tolerance tests used.

Powells Method requires many simulations to be performed, an example tested required 4 iterations of Powells method, but within this, a total of 324 actual simulations were performed (due to the many one dimensional minimisation's that need to be made at each step). If the simulation is over a long time period this would be highly expensive, but this method has the advantage that it is reasonably good at avoiding local minima of the residual function, and the function chosen is very likely to give a solution that is acceptable by the diagnostic procedure, should one exist.

The Downhill Simplex method is generally regarded as being less efficient than Powells method, even though the algorithm used for Powells method is more complicated, but for this example, the Simplex Method requires significantly less calls to the simulation procedure. The robust nature and complexity of Powells Method may be excessive, and for the test case below, the Simplex Method was found to be sufficient to reach the same answers with considerable saving on computational time.

A comparison on the number of simulation calls made to the simulation by Powells method and by the Downhill Simplex Method are shown in Table 3.3.

It is possible that situations may occur where the desirable properties of Powells method may be of use, so the option to use either method is included within the diagnostic algorithm.

Number of Parameters in Search	Method Used	Number of Simulation Calls Made
1	Powells	73
1	Downhill Simplex	17
2	Powells	387
2	Downhill Simplex	100
3	Powells	656
3	Downhill Simplex	136

Table 3.3: Number of simulation calls

3.4.6 Test Case To Illustrate Failure Of Simple Regression

The test case under examination is a simple abrupt incident comprising an unexpected rise in level of a product storage tank, which has sensors present for level, temperature and density. The error due to the rise in level is accompanied by a less significant error in the density measurement for the tank. The nature of the problem is such that a single parameter solution, representing the addition of acid to the tank, should be found to diagnose the problem.

The basic one pass diagnostic algorithm failed to find any one parameter solutions, but was successful for a two parameter search, which found six candidates. Expanding the run by using repeated iteration of the diagnostic algorithm found no additional solutions for this case, but the use of Powells method managed to find two one parameter solutions which had been previously rejected.

The candidates found by Powells method were :

addition of acid

addition of PuNO3

The addition of PuNO3 would be rejected as part of the interpretation/quantification process, since the addition of PuNO3 is not permitted as a solution unless acid is added simultaneously. The addition of acid solution is perfectly acceptable, and the reason that the first pass and re-iterated diagnostic procedure failed to find this result needs to be explained.

The candidate from Powells method specified a perturbation value, V, of 0.94492 for the variable in question, i.e. the flow of acid required is 0.94492 times the default value. The sum of squared errors for this solution is 16.91449, and the errors remaining in the relevant measurements are shown in Table 3.4.

Measurement	Final error	Maximum error allowed
Level	0.227173	2.3088
Density	-4.10361	10.9331
Temperature	0.152557	0.704698

Table 3.4: Powells method solution (V=0.94492)

This solution is very close on level and temperature measurements, with a larger error in the density reading, although since all errors fall within allowed tolerance values, the solution is accepted.

The first pass of the diagnostic algorithm set V to be 0.826844, and performing a simulation with the flow of acid determined by this value failed the final tolerance check, causing the solution to be rejected. The sum of squared errors for this solution is 9.19976, and the errors remaining in the relevant measurements are shown in Table 3.5.

Measurement	Final error	Maximum error allowed
Level	2.88806	2.3088
Density	-0.916199	10.9331
Temperature	0.139473	0.704698

Table 3.5: Basic regression solution (V=0.826844)

As can be seen from the table above, density and temperature errors are well within tolerance values, but the solution is rejected since the level measurement is slightly outside of its permitted range.

After performing 3 more iterations of the diagnostic algorithm, the new V suggested is 0.828223, which brings the sum of squared errors to 9.09206, and the effect on the measurements is shown in Table 3.6.

Measurement	Final error	Maximum error allowed
Level	2.85718	2.3088
Density	-0.953461	10.9331
Temperature	0.139626	0.704698

Table 3.6: Iterated regression solution (V=0.828223)

Again, the solution is very close on temperature and density, but fails on the level measurement. Further iterations seem unlikely to improve the solution successfully, since after the second iteration, the V values chosen were such that they caused the final, cumulative V to become very slightly smaller, rather than continuing to increase the value toward the successful value found using Powells method, summarised in Table 3.7 below. (Cumulative V represents the net effect of applying the calculated V value at each iteration step.)

Iteration number	V value calculated	Cumulative V
1	0.826844	0.826844
2	1.00167	0.828224
3	0.999999	0.828224
4	0.999998	0.828223

Table 3.7: Cumulative V values calculated using Powells method

The regression algorithm continues to find 'improved' solutions each iteration, since the sum of squared errors is falling each time, which is the 'best' solution as far as the regression algorithm is concerned, but Powells method works by minimising the sum of

number of standard deviations away from the correct solution, and so finds a result that is successful, even though the sum of squared errors is larger than that found by the regression algorithm. Similar results can be shown by applying the downhill simplex method, for exactly the same reasons.

3.4.7 Possible Improvements

Although using the above approaches as stated is very computationally expensive, there are possibilities for improvement, particularly in the selection of candidates that would benefit from the application of further iterations or Powells method, rather than the blanket approach currently employed which applies the methods to either all or none of the candidates. Some possible criteria for choosing which parameter combinations are most likely to yield a successful solution are listed below.

- Any solution which corrects a significant number of measurements present in the error vector on the first pass.

- Any solution which reduces the sum of squared errors by a significant amount on the first pass.

- Choice of a particular set of parameters chosen by the user. This would allow the user to select certain parameters which may seem particularly likely to be involved in a solution. This would of course require the user to have some experience with recognising particular classes of problems and the typical solutions, and so is less appealing than the options detailed above, as the diagnostic procedure should ideally be as automated as possible.

CHAPTER 4

4. MODELLING AND AUTOMATIC GENERATION OF COMPUTER SIMULATIONS

4.1 Introduction

A central feature of the preceding chapters has been the concept of a simulation as a means of representing activities occurring on the plant. The simulation attempts to mimic the physical behaviour of the plant in such a way that meaningful conclusions can be drawn by examining the discrepancies between the simulation predictions and the actual data received from the sensors installed on the plant. The use of an automatic model generator greatly increases the flexibility and applicability of the diagnostic procedure, allowing it to be used on a variety of plant configurations with the minimum of user modification.

4.2 Background

One of the obstacles to the practical implementation of model-based fault detection and diagnosis schemes is their reliance on dynamic simulations; it is debatable whether plant operators would be prepared to commit resources to their development. Henry and Clarke (1993) state that '*Fault detection is expensive because hundreds of hours of expert labour are required for each application and a software system must be constructed in parallel with, and interfacing to, the control system*'. Although, ideally, models should come directly from an existing description of the plant (Milne, 1991), this might not be possible and/or might not be practicable; for instance, the models might not be available or might be of a detail that is incompatible with requirements. The comments made by Ham (1979) when detailing the need for a model generator program are still valid today: '*Most plants are dynamic and experience either day to day changes in plant operation or are subject*

to less frequent expansions or modifications. These changes are sufficient to invalidate the existing models and require changes to the actual program code'. It is against this background that an automatic model generator has been written to produce both a simulation and other information required to implement the diagnostic method, without the need for extensive coding by the user.

4.3 Model Based Diagnosis

4.3.1 General Principles

The basic framework behind model based diagnosis is shown in Figure 3.1. Simulated data from a model of the plant under inspection is compared with real data measurements from the plant, and the diagnostic system examines the differences between the two data sets. The importance of this comparison is stressed by Leitch et al (1993), where they state that '*Diagnosing a physical system crucially relies upon the discrepancy detection between the observed and predicted behaviours of the system*'. Many different model based fault detection and diagnosis schemes have been proposed; Frank (1990) gives an overview of the most significant diagnostic approaches, while Isermann (1994) details numerous different fault detection schemes. AbuHanner et al (1992) propose a framework for the integration of multiple model types, to benefit from the advantages of the individual models by switching between them.

Bell et al (1995) propose combining model-based diagnosis with knowledge based reasoning, using the model to provide additional information to the knowledge base when an incomplete hypothesis is formed, or the help differentiate between multiple hypotheses. The wide applicability of model based detection and diagnosis is illustrated by Isermann and Ballé (1997), where a list of published applications of various schemes is presented.

In order to make use of mathematical models of plants, various features need to be defined, such as

- the equations representing the process occurring on the plant, which can often be obtained by applying laws of chemistry and physics;
- values for the various parameters included in the equations;
- boundary conditions which are needed to *solve* the equations;
- the structure of the simulation, defining the various elements used and their relationships to each other.

Of the above, Section 4.4 details the equations for the plant elements considered for this implementation. The structure of the simulation is an important part of the model generation process, and is discussed in Section 4.6. Issues relating to the verification of various parameter values and the boundary conditions required to solve the simulation are discussed in detail in Howell and Scothern (1995a), and are not repeated here.

4.4 Modelling Issues

This section describes the form of the models that have been adopted. It is important to remember that, during any diagnostic search, situations might be hypothesised that are physically impossible. Although the diagnostic program should reach this conclusion after deliberation, the simulation must be robust enough to continue predicting in some *sensible* manner in the mean-time. One fairly obvious occurrence of this is when a tank empties but a perturbation from the diagnostic procedure is made such that further output is specified.

The reader is referred to the nomenclature at the beginning of this report for a description of the variables. In all of the models used in the following sections, it is assumed that there is perfect mixing of the solution.

4.4.1 Liquor Balance

A liquor balance is applied to each element of the system, and is used to model the total mass of solution present in each element :

$$\frac{dM_{liq}}{dt} = Q_{in} - Q_{out} \tag{4.1}$$

This equation can result in negative values for M_{liq}. There are two options within the program that can be followed should the mass in any system component drop below zero.

1. The mass in the component is set to zero, and any flows subsequently leaving are taken from the component's associated hidden inventory instead.

2. Negative mass is allowed to occur and any flows subsequently leaving are assumed to be acid at ambient temperature. The amount of acid entering in such a way is monitored.

The second option is used during the model perturbation phase of the diagnostic process, where it is important to avoid discontinuities. The first option is more realistic and is hence used otherwise.

4.4.2 Evaporation Of Tanks

Evaporation causes the mass in a particular tank to decrease while the concentrations of the various materials, such as plutonium, within the solution increases to keep the total amount of concentrate present constant, and can be modelled by simply adding an extra term to the mass equations:

$$\frac{dM_{liq}}{dt} = Q_{in} - Q_{out} - E \tag{4.2}$$

where E is the rate of mass reduction caused by the evaporation. Evaporation can be exaggerated due to the other activities which are occurring in the tank, such as sparging or mixing, and these effects are here grouped together as a single term.

4.4.3 Plutonium Balance

The balance of plutonium mass within the system takes the following form for each element of the system:

$$\frac{dM_{liq}C_{Pu}}{dt} = Q_{in}C_{Puin} - Q_{out}C_{Puout} \tag{4.3}$$

where C_{Pu} is the plutonium concentration in g/g.

This equation is valid provided the element contains liquor. If the element empties or reaches a negative mass, the concept of concentration is no longer valid so it is set arbitrarily to zero. Any additional liquid entering the system from hidden inventory to keep the flow rates as specified is taken to have a zero concentration unless specified otherwise. This maintains the total inventory of the system whilst causing a general dilution.

Similar balance equations may be used to monitor other materials dissolved in the liquor, e.g. for a reprocessing plant, it might be required to monitor uranium as well as plutonium.

4.4.4 Calculation Of Specific Heat Capacity

If temperature or energy balances are required in the model, it is necessary to calculate the specific heat capacities of the materials involved. The specific heat capacity of the solution is calculated from the specific heat capacities of the various components that make up the solution. If the liquor is a mixture of plutonium, nitric acid, water and other components then

$$M_{liq} = M_{Pu} + M_{acid} + M_{water} \ldots + \ldots others \tag{4.4}$$

and

$$\mathrm{Cp_{liq}} = \mathrm{Cp_{Pu}}\left[\frac{\mathrm{M_{Pu}}}{\mathrm{M_{liq}}}\right] + \mathrm{Cp_{water}}\left[\frac{\mathrm{M_{water}}}{\mathrm{M_{liq}}}\right] + \mathrm{Cp_{acid}}\left[\frac{\mathrm{M_{acid}}}{\mathrm{M_{liq}}}\right] \ldots + \ldots \mathrm{others} \tag{4.5}$$

where

$Cp_{Pu} = 0.156$ j / gm K

$Cp_{water} = 4.21$ j / gm K

$Cp_{acid} = 1.7444$ j / gm K

The specific heat capacity can then be obtained by making use of formulae like:

$$M_{Pu} = M_{liq} C_{Pu} \tag{4.6}$$

$$M_{acid} = \beta M_{water} \tag{4.7}$$

where $\beta = \frac{total\ acid\ mass}{total\ water\ mass}$ and hence, for 5 molar acid, $\beta = \frac{5 * 63.02}{1000}$. The value of 63.02 is present since the molecular weight of nitric acid is 63.02, from Wolf et al (1966).

4.4.5 Energy Equations

Energy equations are used to estimate the temperature within each element. The basic equation takes the form:

$$\frac{d(M_{liq} h_{liq})}{dt} = h_{liq_{in}} Q_{liq_{in}} - h_{liq_{out}} Q_{liq_{out}} + k(T_{ambient} - T_{liq}) \tag{4.8}$$

where k is the heat transfer coefficient for heat exchange with the surroundings. The above assumes that the energy lost through evaporation is negligible. If it can be assumed that pressure is constant, enthalpy can be replaced by temperature: $h = CpT$.

4.4.6 Connecting Pipe Equations

The flow rates specified for a particular transfer by the interface to the simulation are the flow rates out of the source element. The flows into the target element are calculated on the basis that all of the mass leaving the source element will pass into the connecting header(s), and from there into the target element. There are several issues that need to be taken into consideration: time skews caused by the time taken to pass material along long pipes, material hold-up in the connecting pipework, energy gains/losses due to material transfer (e.g. pumping) and heat transfer with the environment.

4.4.6.1 Time Skews

A time delay will be observed when material is transferred from one system component to another if the connecting pipework is of a significant length. This necessitates the inclusion of appropriate mass and energy balances for the pipework itself. In particular if there is a material transfer between two components A and B where

Q_A^* - specified flow rate out of the source element

Q_B^* - specified flow rate into the target element

t_{f_A} - time the transfer out of the source element finishes

t_{f_B} - time the transfer into the target element finishes

t_{s_A} - time the transfer out of the source element starts

t_{s_B} - time the transfer into the target element starts

$M_{liq\,p}$ - mass currently in the intervening pipe

then

$$\frac{dM_{liq_p}}{dt} = Q_A - Q_B \tag{4.9}$$

where $Q_A = \begin{cases} Q_A^* & t_{s_A} \le t < t_{f_A} \\ 0 & t < t_{s_A} \text{ or } t \ge t_{f_A} \end{cases}$ and $Q_B = \begin{cases} Q_B^* & t_{s_B} \le t < t_{f_B} \\ 0 & t < t_{s_B} \text{ or } t \ge t_{f_B} \end{cases}$

4.4.6.2 Material Hold-Up

The total mass arriving at the target element will depend not only on the mass leaving the source element, but also on the state of the intervening pipework. To avoid problems of material appearing to come from 'nowhere', it is assumed that the same residual amount of liquor, $M_{liq\,pi}$, always remains in the pipework at the end of every transfer. Flows are then modified to ensure that this occurs. The flow rate into the target element must then be corrected as follows:

$$Q_B^* = \frac{Q_A^*(t_{f_A} - t_{s_A}) + M_{liq\,p} - M_{liq\,pi}}{(t_{f_B} - t_{s_B})} \tag{4.10}$$

As can be seen from the above equation, if the current mass in the pipe is the same as that to left at the end, then all of the mass leaving element A will arrive at element B. If there is less material in the pipe than the initial level, then the flow rate into the target element will be reduced to leave some liquor behind. Conversely, if there is more material remaining in the pipe, then the flow rate to the target element will be increased to bring the amount in the pipe back to the correct level.

Flows which are explicitly stated as beginning or ending at a pipe do not use equation (4.10) above, but are allowed to affect the mass remaining in the pipe in the normal manner. In this way, the state of the pipe can have an effect on future transfers of material.

4.4.6.3 Energy Considerations

Heat transfer with the surroundings for the various elements is covered by the energy equations detailed in Section 4.3.5. The energy required to deliver the material transfers is modelled by arguing that there is an approximately constant heat input per unit mass transferred. Thus

$$h_{liq_{in\,B}} = h_{liq_{out\,p}} + \psi \tag{4.11}$$

This represents the pump heating the material during transfer. The value of ψ used will depend on the pump specified as responsible for the transfer.

4.4.7 Tank Measurement Model

It is assumed that measurements for level and density are made available in the form of manometer readings in mm of water. Some of the initial conditions for the simulation are obtained by converting these readings to actual masses and concentrations within the tanks. Conversely model predictions of mass and concentration need to be converted into actual measurement predictions so that residues, i.e. differences between plant

measurements and simulation predictions of those measurements, can be formed. The method used is as follows.

1. Level and density readings are corrected by the density of the solution present in the manometer tubes, ρ_t

$$l_l^* = l_l \times \rho_t \tag{4.12}$$

$$l_d^* = l_d \times \rho_t \tag{4.13}$$

where l_l is the measured pressure on the level pneumercator, l_d is the measured pressure on the density pneumercator, and l_l^*, l_d^* are the corrected level and density pressure readings in mm of water.

2. Actual density of the solution present in the tank, ρ_s , is calculated:

$$\rho_s = \frac{(l_l^* - l_d^*)}{\lambda} \tag{4.14}$$

where λ is the level difference between the ends of the level and density dip-tubes.

3. Actual level of the solution, *L*, is calculated

$$L = \frac{l_l^*}{\rho_s} \tag{4.15}$$

4. Level to volume is calculated according to the supplied calibration equations for the tank :

$$V = \alpha + \beta L \tag{4.16}$$

i.e. β is the slope of the linear equation and α is the intercept.

5. Mass is calculated from volume and density of solution

$$M = V\rho_s \tag{4.17}$$

6. Density of solution is related to concentration of plutonium by the following formula (Franssen, 1994):

$$\rho_s = 0.00147*[Pu]+0.034*[H+]+\rho_w \tag{4.18}$$

or

$$[Pu] = \frac{\rho_s - \rho_w - 0.034*[H+]}{0.00147} \tag{4.19}$$

where *[Pu]* is concentration of Pu in g/l, *[H+]* is the molarity of the nitric acid, typically 5 Mol, and ρ_w is the density of water at the measurement temperature, ranging from 0.9982 at 25°C to 0.9922 at 40°C.

7. The model requires concentration of Pu, C_{Pu}, to be specified in g/g:

$$C_{Pu} = \frac{[Pu]}{\rho_s} \tag{4.20}$$

or

$$C_{Pu} = \frac{\rho_s - \rho_w - 0.034*[H+]}{0.00147*\rho_s} \tag{4.21}$$

4.4.8 Solvent-Extraction Plant And Concentration Plant Models

4.4.8.1 Level Of Detail Required

So far as safeguards is concerned, it is important to appreciate that

- models are only needed to predict the material hold-up within individual units and to predict flows entering and leaving;
- the units are fed-from, and output to, tanks which 'smooth' out short term fluctuations.

It follows that the approach does not need accurate dynamic predictions of what is going on at individual locations within the units. However this does not preclude the use of more accurate models, increased accuracy should improve sensitivity.

4.4.8.2 Solvent-Extraction Plant

There would be considerable complexity in applying mass balances to the liquor passing through the solvent-extraction plant. This is because of the different streams entering and leaving. Since the plutonium balance is of primary importance, liquor mass balances are only applied when it is straightforward to do so.

The plutonium inventory in a solvent-extraction plant is largely determined by the flowrates of its various inputs. These tend to be varied together to maintain the position of the heavy metal front constant. Under these circumstances and to a first approximation,

$$\text{plutonium inventory} \propto \text{plant throughput}$$

Computer predictions carried out by Walford et al (1987) suggest that the inventory in the first cycle can be varied by between 0.8 to 4 times the design inventory by manipulating the solvent and scrub feeds. They publish a graph showing the steady state variation in inventory obtained by varying these two feeds separately. To a first approximation this can be represented by

$$\begin{bmatrix} inventory\ of \\ first\ cycle \end{bmatrix} \propto \left[\frac{L}{L_o}\right](1+\alpha_{sol}+\alpha_{scr}) \tag{4.22}$$

where $\frac{L}{L_o}$ is the fraction of the maximum load,

$$\alpha_{sol} = \begin{cases} -3\Delta Q_{sol} & \Delta Q_{sol} \geq 0 \\ 150(\Delta Q_{sol})^2 & \Delta Q_{sol} < 0 \end{cases} \tag{4.23}$$

$$\alpha_{scr} = \max(0.5\Delta Q_{scr}, 16\Delta Q_{scr} - 5.9) \tag{4.24}$$

and ΔQ_{sol}, ΔQ_{scr} are relative deviations in feeds from their nominal values.

Any feed or load changes will take some time to affect the inventory fully, and this can be modelled as

$$inventory_1 + \tau \frac{d\,inventory_1}{dt} = k_1 \left[\frac{L}{L_o}\right](1 + \alpha_{sol} + \alpha_{scr}) \tag{4.25}$$

where k_1 is the nominal full load inventory. Thus the rate at which plutonium leaves the cycle is given by

$$Q_{Puout} = Q_{Puin} - \frac{d\,inventory_1}{dt} \tag{4.26}$$

and the plutonium concentration output can be obtained by assuming that the flowrate of the aqueous solvent leaving the cycle is proportional to the load, L.

Clearly this is an approximation to the true dynamics and it is recommended that predictions derived on the basis of these models should only be compared with measurements recorded when the plant is relatively steady.

In practice,

- it is unlikely that either ΔQ_{sol} or ΔQ_{scr} will be known; in this event, the diagnostic program would be instructed to treat the variable, $\alpha: \alpha = 1 + \alpha_{sol} + \alpha_{scr}$ as an additional path variable and
- this plant model can be duplicated for both the medium and low cycles.

4.4.8.3 Concentration Plant

Although the equations presented here describe a particular, hypothetical unit, few changes should be necessary to model any other configuration.

- Although produced for a continuous concentrator, the equations below would be equally applicable to one operating in batch mode; the only change would concern the flowrate of the liquor out, i.e. $Q_{liq_{out}}$.

- The concentrator is assumed to consist of a storage tank and a separate heater with the unconcentrated liquor flowing directly into the storage tank and the concentrated liquor exiting from a T-junction installed in the downcomer connecting the storage tank to the heater, as shown in Figure 4.1.

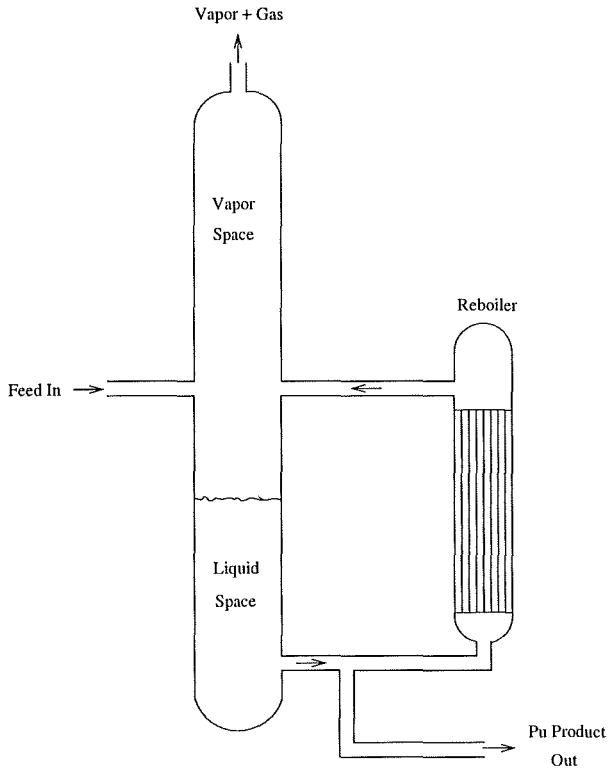


Figure 4.1: Concentrator schematic

- The unit's control strategy largely determines the way it is operated; here it is assumed that control systems invoke the following rules:

  If $C_{Pu} > C_{Pu_r}$ **then** liquor concentrated,

  If liquor concentrated **and** level > level_r

  then flow_out = some constant flow $Q_{liq_{out}}$ **else** no flow_out,

  If liquor concentrated **then** turn heat off,

where level_r and C_{Pu_r} are level and concentration 'set points'. Hysterisis is added to stop chatter. The concentrator continues to evaporate and output after its feed has been stopped until the liquor is homogeneous and of approximately the same volume and concentration as at the end of the previous cycle.

4.4.8.3.1 Concentrator Storage Tank

The liquor balance for the storage tank of the concentrator is given by:

$$\frac{dM_{liq}}{dt} = Q_{liq_{in}} - Q_{liq_{down}} + Q_{liq_{return}} \tag{4.27}$$

and the enthalpy balance is:

$$\frac{dM_{liq}h_{liq}}{dt} = Q_{liq_{in}}T_{in}Cp_{liq_{in}} - Q_{liq_{down}}h_{liq} + Q_{liq_{return}}h_{liq_{return}} - \alpha(T_{liq} - T_{ambient}) \tag{4.28}$$

The plutonium balance can be represented by:

$$\frac{dM_{liq}C_{Pu}}{dt} = Q_{liq_{in}}C_{Pu_{in}} + Q_{liq_{return}}C_{Pu_{return}} - Q_{liq_{down}}C_{Pu} \tag{4.29}$$

where $Q_{liq_{return}}C_{Pu_{return}} = Q_{liq_{hi}}C_{Pu}$.

4.4.8.3.2 Concentrater Heater

Equations that are required to simulate the heater section of the concentrator are as follows :

$$Q_{liq_{hi}} = Q_{liq_{down}} - Q_{liq_{out}} \quad ; \quad h_{liq_{ho}} = h_{liq} + \frac{heatin}{Q_{liq_{hi}}} \quad ; \tag{4.30}$$

$$x^* = \frac{h_{liq_{ho}} - T_f Cp_{liq}}{h_{fg}} \quad ; \quad Q_{evap} = x^* Q_{liq_{hi}} = x Q_{water} \quad ; \tag{4.31}$$

$$Q_{liq_{return}} = (1 - x^*) Q_{liq_{hi}} \quad ; \tag{4.32}$$

$$h_{liq\,return} = \begin{cases} h_{liq\,ho} & x^* \le 0 \\ T_f Cp_{liq} & x^* > 0 \end{cases} \quad ; \tag{4.33}$$

where $h_{fg} = 2258\,kJ/kg \quad ; \quad T_f = 99.6°C.$

In practice values for the 2 set-points, for the hysterisis and for *heatin* would be chosen to obtain not only the concentration and level observed but also the magnitude and frequency of the ripples observed.

4.5 Errors In Tank Calibration

4.5.1 Introduction

The calibration of a tank refers to the relationship between the volume of liquid in a tank and the level measurements obtained from sensors, which is primarily governed by the physical shape and dimensions of the tank. Accurate calibrations are difficult, since many factors could alter the calibration equations, such as the temperature or density of the liquid present within the tank. For simplicity, it is assumed here that the tanks have constant cross-sectional area, and can be modelled by a simple linear relationship. This assumption allows investigation of errors in the tank calibrations to be performed.

4.5.2 The Error Model

An appropriate error model can be derived by modelling the effect of transferring a sequence $\Delta V_1, \Delta V_2, \Delta V_3 \ldots$ of known volumes into and out of a tank. Let the contents of this tank have volume V and level l (mm) which is equivalent to a level measurement h (mm H_2O). As before, let ^ denote an actual measured quantity and ~ denote one that is estimated. In general, let a subscript denote a particular instance with o denoting the initial value. Thus for instance V_o, $\hat{V}_o$ and $\tilde{V}_o$ denote the true, measured and estimated volumes at the beginning of the period under consideration.

Assume the following.

1. The tank calibration equation is linear:

$$V = \alpha l + \beta \quad \text{where } \alpha \text{ and } \beta \text{ are (unknown) constants,}$$

which is initially modelled as

$$V = \alpha_o l + \beta_o \quad \text{where } \alpha_o \text{ and } \beta_o \text{ are known.}$$

2. Level measurements are noise free and unbiased i.e.

$$V = \alpha \hat{l} + \beta \tag{4.34}$$

At the start, the initial level is estimated as that measured, i.e.

$$\tilde{l}_o = \hat{l}_o \tag{4.35}$$

$$\Rightarrow \quad \frac{\tilde{V}_o - \beta_o}{\alpha_o} = \frac{V_o - \beta}{\alpha}$$

$$\Rightarrow \quad V_o = \alpha\left[\frac{\tilde{V}_o - \beta_o}{\alpha_o}\right] + \beta \tag{4.36}$$

Subsequently,

$$V_i = V_o + \sum_{k=1}^{i} \Delta V_k \qquad \text{and} \qquad \tilde{V}_i = \tilde{V}_o + \sum_{k=1}^{i} \Delta V_k$$

$$\Rightarrow \qquad \hat{l}_i = \frac{V_o + \sum_{k=1}^{i} \Delta V_k - \beta}{\alpha} \quad \text{and} \quad \tilde{l}_i = \frac{\tilde{V}_o + \sum_{k=1}^{i} \Delta V_k - \beta_o}{\alpha_o}$$

or $\hat{l}_i = \dfrac{\alpha\left[\dfrac{\tilde{V}_o - \beta_o}{\alpha_o}\right] + \sum_{k=1}^{i} \Delta V_k}{\alpha}$ and $\tilde{l}_i = \dfrac{\tilde{V}_o + \sum_{k=1}^{i} \Delta V_k - \beta_o}{\alpha_o}$

Thus

$$\hat{l}_i - \tilde{l}_i = \left[\frac{1}{\alpha} - \frac{1}{\alpha_o}\right] \sum_{k=1}^{i} \Delta V_k \tag{4.37}$$

Defining $\delta\alpha$ as a correction term: $\alpha = \alpha_o + \delta\alpha$

then $$\hat{l}_i - \tilde{l}_i = -\left(\frac{\delta\alpha}{\alpha\alpha_o}\right) \sum_{k=1}^{i} \Delta V_k$$

or $$\hat{l}_i - \tilde{l}_i = -\left(\frac{\delta\alpha}{\alpha_o}\right) \frac{1}{\alpha} [\alpha \hat{l}_i - (V_o - \beta)]$$

$$\Rightarrow \quad \hat{l}_i - \tilde{l}_i = -\left(\frac{\delta\alpha}{\alpha_o}\right) (\hat{l}_i - \hat{l}_o) \tag{4.38}$$

If both $\tilde{l}_i$ and $\hat{l}_i$ are measured in mm of water (as $\tilde{h}_i$ and $\hat{h}_i$)

then $$V = \alpha\left(\frac{\rho_w}{\rho_{sol}}\right)\hat{h} + \beta$$

and $$\hat{h}_i - \tilde{h}_i = -\left(\frac{\delta\alpha}{\alpha_o}\right)\left[\hat{h}_i - \left(\frac{\rho_{sol_i}}{\rho_{sol_o}}\right)\hat{h}_o\right] \tag{4.39}$$

This final equation can be implemented in the diagnostic algorithm by letting $-\left(\dfrac{\delta\alpha}{\alpha_o}\right)$ be a non-path parameter and then noting that since $\hat{h}_i - \tilde{h}_i$ will be one of the residues, the appropriate entry in the global Jacobian matrix (equation 3.3), will be $\left[\hat{h}_i - \left(\dfrac{\rho_{sol_i}}{\rho_{sol_o}}\right)\hat{h}_o\right]$. The appropriate subjective probabilities for such parameters are then represented as multiplicative errors of say 5%.

4.6 Automatic Model And Path Generation

4.6.1 Introduction

The automatic model generator's primary purpose is to reduce the amount of programming required by the user when preparing the diagnostic package for use on a new plant, or when the existing plant is modified. As with the diagnostic package itself, ease of use is of significant importance, and to accommodate this requirement, a graphical user interface for the automatic model generation routines was produced using G2 (Gensym). The steps required for the creation of a model are listed below.

1. Produce the basic plant schematic, consisting of the various nodes and the connections between them.
2. Specify the features of any pumps that may cause heating, and assign the connection pipes to the correct pumps.
3. Assign values to various parameters, such as number and type of concentrates that will be present in solutions, sizes of various matrices, what sensors are available for each node, and choose which parameters will be available for perturbation, along with the associated subjective probabilities.
4. Generate the model and compile the code.
5. Adjust features of the generated model if desired, such as various default values that will be used by the simulation.
6. Install the new models and update the diagnostic package to feature the new model and plant schematic.

Section 4.6.2 describes steps 1 to 3 of the above process, focusing on the features of the package from the end users perspective. The theoretical basis of the model generator, including the generation of all of the possible material transfer paths which are required by the diagnostic algorithm is discussed in Section 4.6.3.

4.6.2 Features Of The User Interface

The automatic model generator package can be accessed directly from the diagnostic package when the current plant needs modification, or can be started separately to design a completely new facility. An example of the main design area window is shown in Figure 4.2.

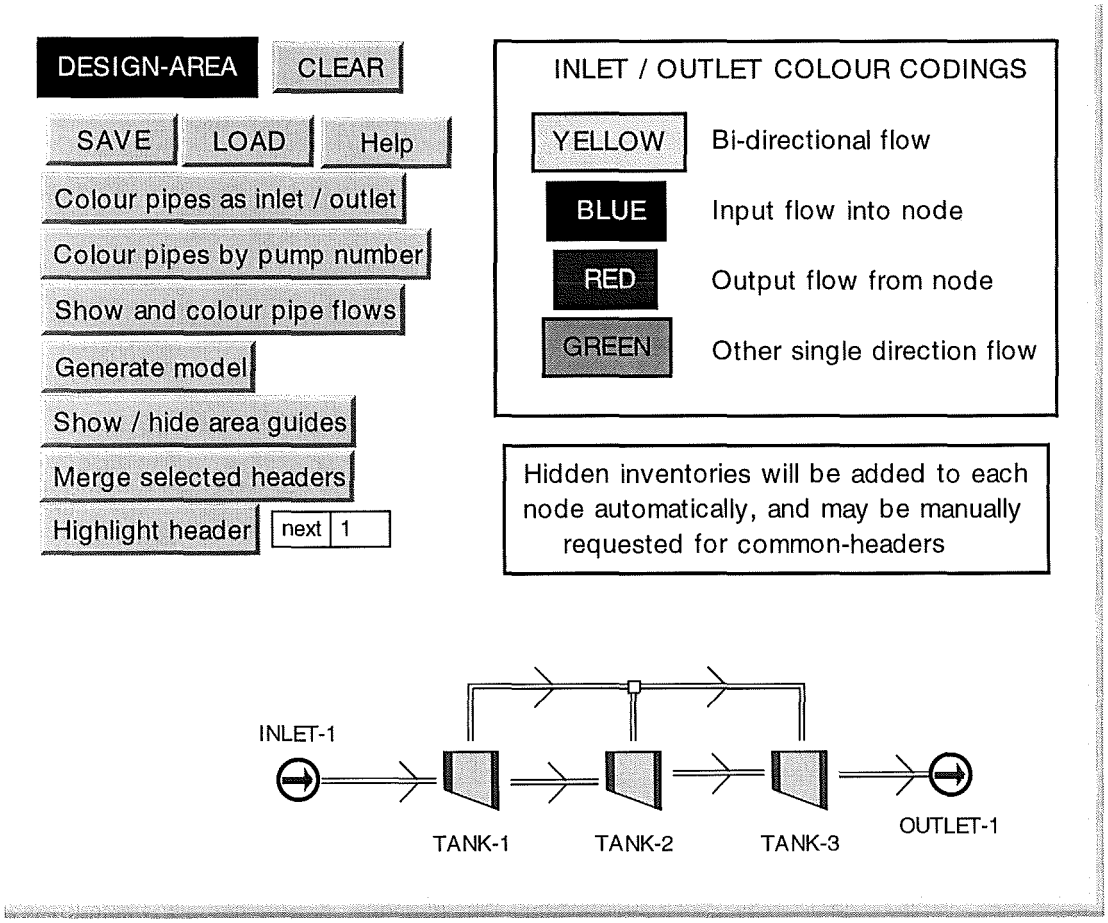


Figure 4.2: Automatic model generator main window

4.6.2.1 Node Creation

The user is provided with a palette of the various nodes available which can be selected and moved to the design area to form the basic layout of the plant (Figure 4.3). As the nodes are transferred to the main design area, they are automatically named. Once the icons are in place, they can be moved rotated, re-sized or deleted easily.

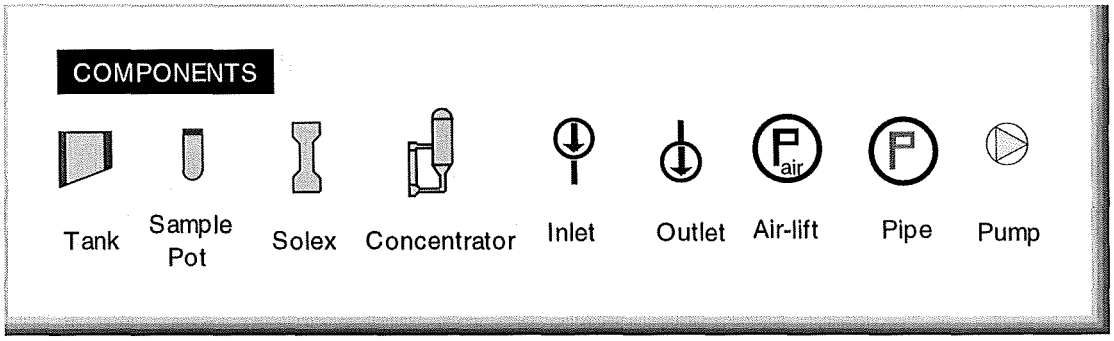


Figure 4.3: Palette of nodes

4.6.2.2 Pipe Creation

Connections between the nodes can be made by clicking on the location of the connection on the node itself, with the direction of flow permitted being specified by use of shift or control keys. Flows can be either one way only or bi-directional, according to the users perception of the plant. Pipes have various options available to them, such as whether material flows are permitted to begin or end in the pipes themselves, which can be of interest to nuclear materials safeguards, where material that is temporarily stored in pipes can be important.

4.6.2.3 Pump Creation

The effect of heating by the various pumps that are used to move liquor around the plant can be included by creating the required number of pumps, and specifying the rate of heating each pump will cause to any liquor flowing through it. After the required number of pumps are created, each pipe can be assigned to a particular pump, and any flows through that pipe will be heated within the simulation model according the rate of heating specified.

4.6.2.4 Display Options

To assist in the creation of the plant, various options are available to graphically illustrate the design so far, such as colouring pipes according to the pump number used, or according to whether the pipe is connected to an inlet of an outlet, to allow the user to see at a glance if the design is as intended.

4.6.2.5 Choice Of Sensors

Information describing the sensor types that are installed on the plant is entered via a simple point and click interface; the user chooses from a palette of available types, an example of which is shown in Figure 4.4.

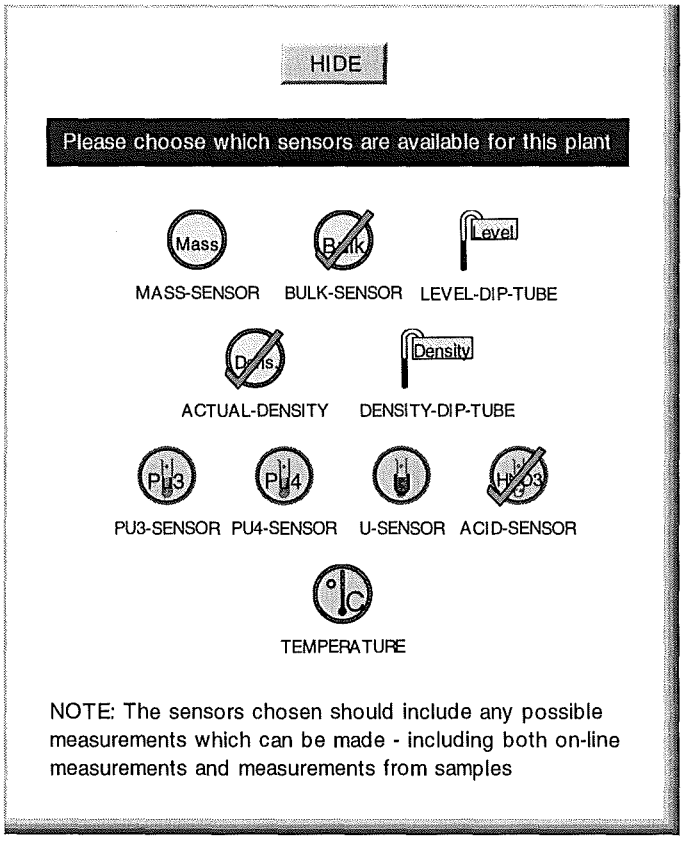


Figure 4.4: Sensor choice palette

4.6.2.6 Setting Parameter Values

Parameter values are easily viewed or altered by a hierarchy of windows showing the current values and providing boxes to type in the new values, or check boxes to switch logical values to true or false, for both pre and post model generation alterations.

4.6.3 The Basis Of The Automatic Model Generator

4.6.3.1 The Automatic Generation Of The Plant Simulation

A large part of the generator is concerned with generating the model that will be used to simulate the plant. Figure 4.5 shows the final structure of the model, and Figure 4.6 shows the path taken during its construction. The simulation views the plant as a number of process units that are connected via paths along which material flows. Each unit is represented by a particular model subroutine, and the core of the system is based around a 'flow' matrix of individual path flow rates over time. The simulation top level is the interface between the diagnostic procedure and the simulation, and the various node models present in the lowest level of Figure 4.5 make use of the equations detailed in Section 4.4. The current simulation is produced in FORTRAN (see, for example, Katzan, 1978), which requires such things as matrix sizes to be specified in advance, hence the use of automatically generated declaration files for each subroutine.

The computer simulation is produced in five main stages:

- generate all valid paths from the plant schematic;
- generate the simulation's top level procedure;
- generate declaration files and code sections to be included in various model code elements
- generate default parameter files and subjective probabilities
- generate script for compiling and linking all required routines

The generation of all valid paths is covered in Section 4.6.3.2. Further details of the structure of the model can be found in Howell and Scothern (1995a), and for additional detail on the automatic model generation process, see Howell and Scothern (1995b).

4.6.3.1.1 Simulation Top Level And Declaration Files

The procedures that simulate individual nodes have been designed to be as generic as possible to allow them to be valid for any configuration of the various elements involved.

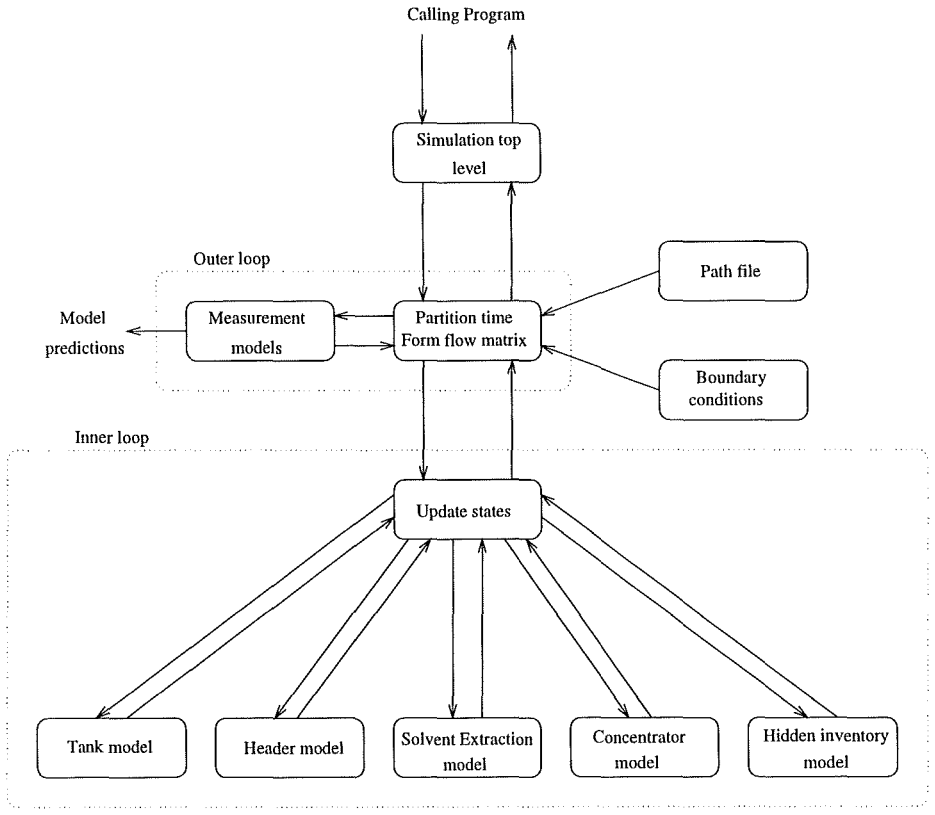


Figure 4.5: Structure of final simulation

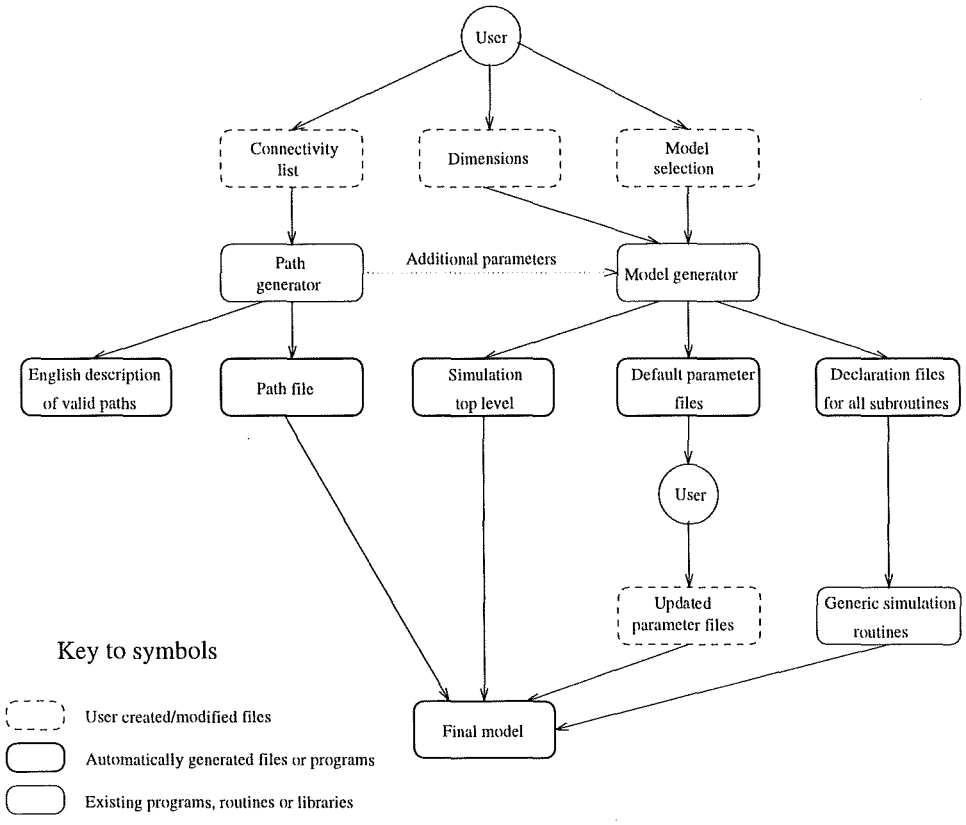


Figure 4.6: Automatic model generation flow diagram

However they still need to be linked together in accordance with the specification and this necessitates the generation of a top level procedure to initialise all of the model parameters, to set up common blocks and arrays and to initiate calls. Declaration files are generated for many of the subroutines used by the model; these ensure that all array sizes, common blocks etc. are generated consistently throughout the code. Although only comparatively minor changes to the code are required, these changes permeate throughout the entire simulation model, and must be applied to many different routines; the automatic generation process ensures that the changes made are consistent and applied wherever needed, without the need for extensive user coding.

In addition to the declaration files, sections of code that are required by various routines in the diagnostic algorithm and by the simulation are automatically generated. Some examples are the code that selects which measurement routine to call for each particular element in the plant, or the code that is used to update a particular physical state, such as plutonium concentration.

4.6.3.1.2 Simulation Default Parameter Files

Once the model is generated, numerous parameter files need to be supplied to quantify various parts of the system. In order to reduce the amount of work required of the user, default templates of many of these files are automatically generated. These files can then be easily tailored by the user to meet the requirements of the current plant; the user can work through a structured hierarchy of windows displaying the various parameters available and options for their alteration. For more details of the model generator and its user interface, see Scothern and Howell (1998).

4.6.3.2 Directed Graph Descriptions Of Plants

The diagnostic algorithm referred to throughout this thesis needs to know all possible paths along which material may be transferred within the plant. For a large plant with significant interconnectedness, it would be time consuming and impractical for the user to exhaustively specify every possible path, and so a method to automatically produce such a

list of paths is used. The method used is based on the concept of a 'directed graph'. The use of directed graphs to represent a process plant is well-established (see, for instance Tamhane and Mah, 1985), the graph is composed of nodes which represent the various process units which make up the plant together with connections which represent physically possible flows between them. Figure 4.7 shows the connectivity graph produced to represent the product storage area in a model reprocessing plant, Figure 4.8.

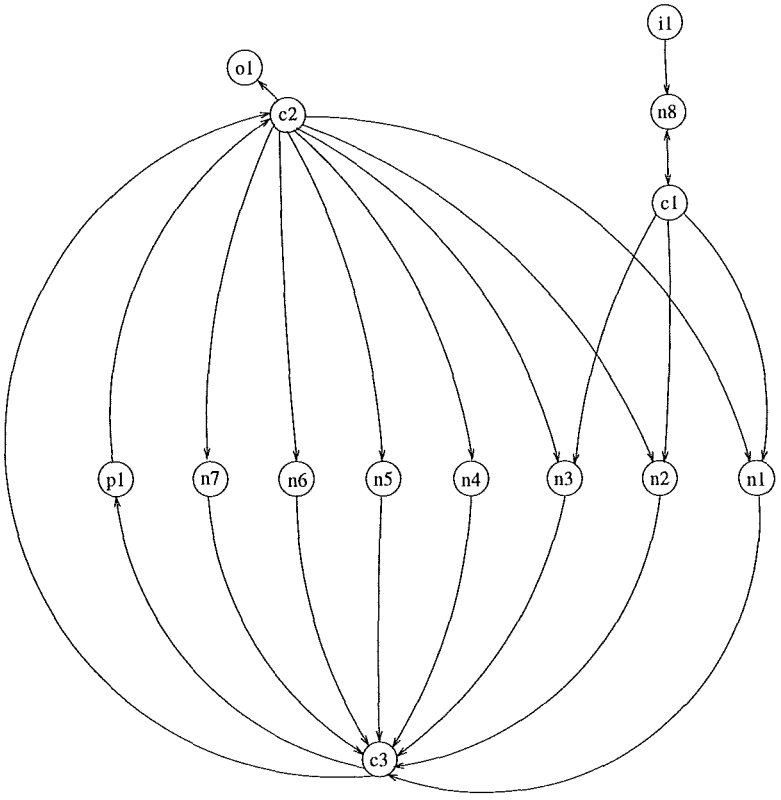


Figure 4.7: Connectivity diagram for a storage area

In Figure 4.7, the following representations are used; 'n' is a general node or tank, 'p' is a sample pot, 'i' is an inlet, 'o' is an outlet, and 'c' is a common header or pipe.

Once such a directed graph description is produced for a plant, it is straightforward to determine the possible connections from node to node through the intervening pipe work. For each element in the plant that is a valid start point, such as a tank or a sample pot, all paths to every possible end point are obtained by repeatedly examining the connectivity of the plant schematic for the next link in the path until a valid end point is reached.

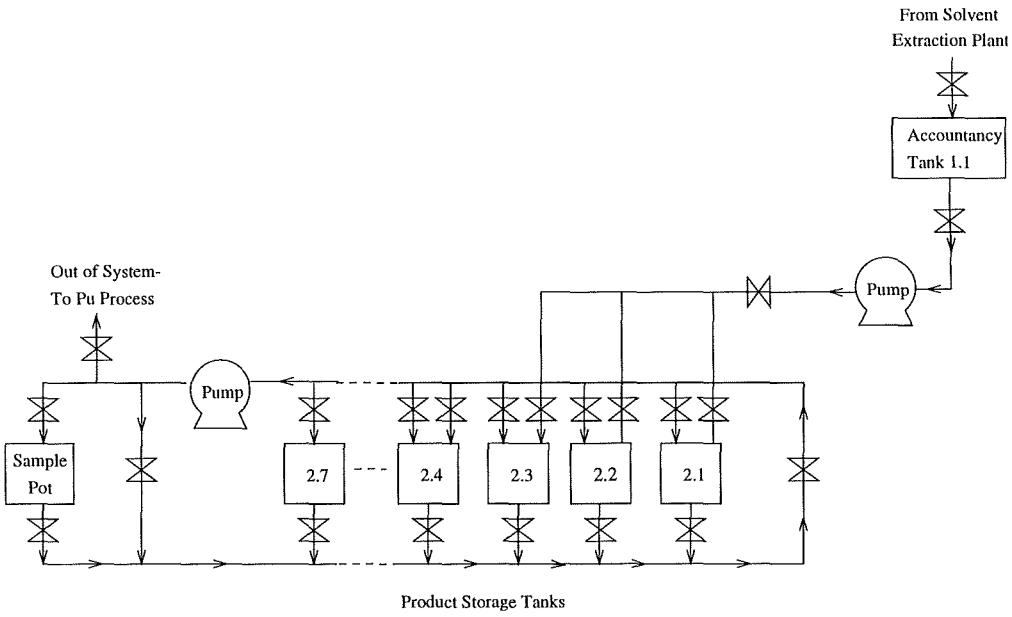


Figure 4.8: A model storage area

Each path may be simply one step, such as a direct connection between tank 1 and solvent extraction element 1, or may pass through several headers on the way, e.g. a path from concentrator 1 to tank 1 via headers 2, 4 and 1.

Connecting pipes can be modelled as separate nodes if the variation in hold-up is thought to be an issue. In these circumstances it is possible to have a flow of material which starts or ends in these pipes; if any such flows are to be permitted within the diagnostic algorithm, the specific pipes involved must be specified, explicitly, by the user when designing the plant schematic. This feature is of particular importance in the field of nuclear materials safeguards where material can transiently disappear into pipework. The reason that all pipes are not modelled, along with possible flows to and from them, is that this would increase the size of the model, and unnecessarily add extra elements to the list of possible paths.

CHAPTER 5

5. SOME EXTENSIONS

5.1 Introduction

The majority of the work presented in this thesis is based on the study of batch processes, for example a network of tanks where transfers between tanks are abrupt in nature. To be more generally applicable, continuous process elements such as concentrators and solvent extraction columns have been studied elsewhere (Howell and Scothern, 1998, Coulter et al, 1995), and some of the consequences of these studies are detailed here. The first relates to the monitoring of continuous process elements (Section 5.2) and the second relates to the question of false alarm handling (Section 5.3).

5.2 Continuous Processes

5.2.1 Introduction

The focus of the application of the diagnostic procedure to continuous processes was on the continuous operation of the concentration and solvent extraction areas. Basic models for these types of process elements were given in the preceding chapter, along with the underlying assumptions used in the solvent extraction models. The following sub-sections describe several changes that were required to the existing diagnostic procedures to allow analysis of such continuously operated plant elements.

5.2.2 Event Handling

Event information pertaining to continuous processes is as equally important to the user as is that pertaining to abrupt events. For continuous processes, the important features are :

- the time at which the node in question begins operation, and at what level, load or flowsheet;
- the times at which the load changes, along with the revised load;
- the time which the node ceases operation.

Each of these features is identified by separate events which appear on the event list for inspection by the user. Also, for days in which there is no change in the process from the previous day, an event signifying that the process is simply continuing will be available on the event list. This ensures that each day the event list represents all the processes occurring on the plant.

5.2.3 Interpreting Abrupt Events In Continuous Data

The presence of continuous flows into and out of tanks can cause difficulty in determining the flow rates of any abrupt transfers which occur into or out of the tanks during the time that the continuous flow is present. Consider the tank level transient shown in Figure 5.1.

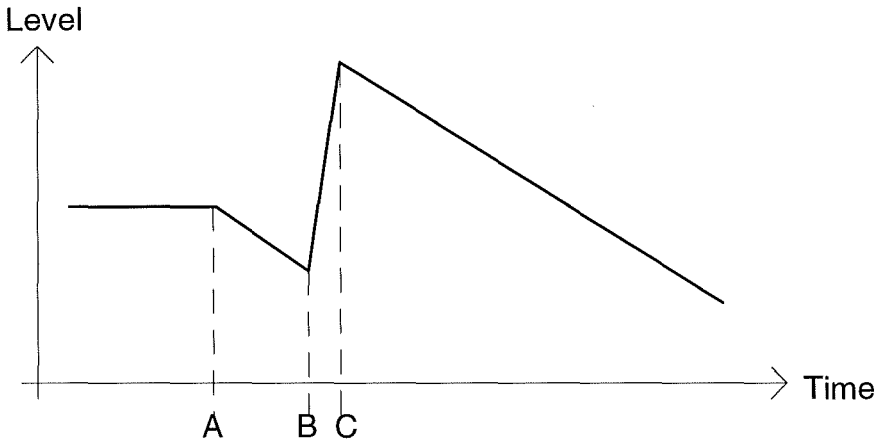


Figure 5.1: Level transient for feed tank with continuous operation

Here A is the time at which the continuous flow out of the tank begins, B is the start of the abrupt event, and C is the end of the abrupt event. Between A and B, and from C onwards, a value for the flow rate out of the tank can easily be determined, but during B

to C, the rates of both the flow out and the flow in are uncertain. Various approaches can be used to determine what the flow rates are, depending on the nature of the plant :

- if the source of the abrupt event is a monitored tank that is not being fed by any continuous flows, then the rate of flow in can be hypothesised as the same as the rate of flow out of the source tank;
- if the destination of the flow out is a monitored tank, which is not performing transfers during the time period under investigation, then the flow rate out can be estimated from the rise in level of the destination tank.

Both of these approaches depend very much on the layout of the plant, and the procedures occurring on the plant at the time of interest. An alternative approach that does not depend on neighbouring plant elements is to simply assume that the flow rate out of the tank during the abrupt event is equal to the flowrate that occurred just prior to the event. If this assumption is in error, the diagnostic procedure should be able to detect this when the abrupt event is analysed. The flow rate for the abrupt event can then be calculated using the following formula:

$$FlowRate = \frac{Level_C - Level_B}{Time_C - Time_B} - \frac{Level_B - Level_A}{Time_B - Time_A} \tag{5.1}$$

5.2.4 Enhanced Pipe Models

Lumped parameter models for pipes where material could temporarily be stored during transfers between process elements were described in the previous chapter. In order for continuously fed versions to function correctly, they must be able to handle a stream of material with variable concentration. For this reason, pipe models known as 'ring-buffers', in which the actual contents of various sections of the pipe over time are stored, are used instead.

5.2.5 Parameter Specification

Of concern when modelling a solvent extraction plant is the lack of knowledge pertaining to the various parameters needed. For commercial reasons, these are often not made available to the inspectors. For this reason, a parameter identification procedure was developed which made use of the plant simulation model described in Chapter 4. The model parameters in question were:

- the nominal full load inventory (mass of plutonium present when the solvent extraction columns are fully loaded),
- the time constant which determines how long it takes the full load inventory to build up during commissioning, and
- the amount of time it takes material to pass through the pipework from the source tank to the columns themselves.

Concentrators also require parameter identification, but this is limited to the determination of the pipe work time delays before and after the concentrator.

5.2.6 Automatic Parameter Identification Process

The specification of parameters for the models of solvent extraction areas obviously has a significant effect on the output of the simulation, and hence on the quality of the diagnoses that can be generated from it. It is likely that the user will not be in a position to give good estimates of the values of these parameters. For this reason, an automatic procedure was developed which can estimate the values of the required parameters using a combination of the process measurements and the simulation model. The central feature of the automatic process used to identify the required parameters is the facility to estimate the base load inventory of the solvent extraction areas. This parameter is estimated using an observer-based approach, (see, for example Jacobs, 1993), where a hypothetical valve, with associated integral controller, is installed on the path which links the receiving tank to its hypothetical hidden inventory, as shown in Figure 5.2. Plutonium is diverted/introduced to and from the hidden inventory to maintain the correct plutonium concentration in the receiving tank during the loading phase. Although, in the off-line studies, concentration

measurements were recorded frequently, the approach can also be applied when records are made less frequently, as on a real plant. The control diagram for the integral controller is shown in Figure 5.3

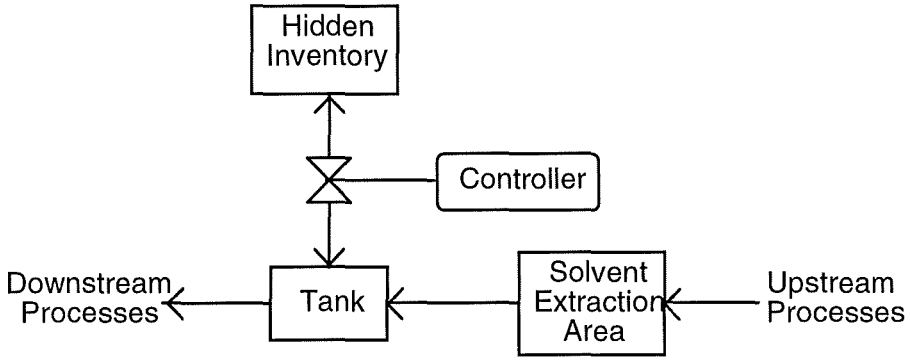


Figure 5.2: Use of hidden inventory to manipulate Plutonium content in tank

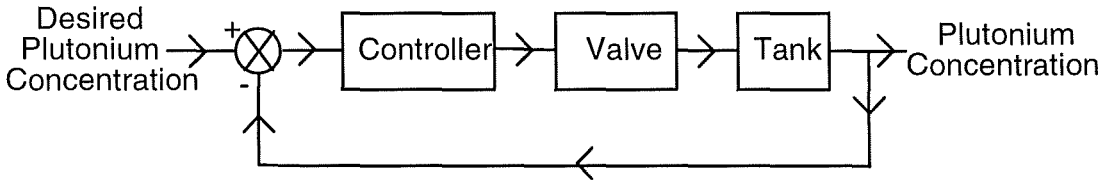


Figure 5.3: Controller diagram

The controller equations take the form shown below:

$$f_d = \frac{K}{\tau}\int (C_r - C_m)dt\,, \tag{5.2}$$

where f_d is the desired plutonium flowrate through the valve, K is the proportional gain, τ is the integral time constant, C_r is the reference concentration, and C_m is the concentration measured in the simulation. The controller is used to drive the value of the simulated plutonium concentration measurement, C_m, to the desired concentration, C_r, which is obtained from the plant. In order to use this system to estimate the desired parameters, the procedures described in the following sections are used.

5.2.6.1 Choice Of Initial Values

In order to perform a simulation, default values have to be chosen as a starting point for the analysis. In the absence of any user supplied information, the solvent extraction cycle time constant is set to 1 hour, and the time delay due to the pipe work is set to zero, as is the full load inventory. Setting the full load inventory to zero initially will have the effect that no plutonium will be transiently stored in the solvent extraction cycle during the simulation, and so all of it will be sent directly to the following tank; this will have the effect that after the simulation with the controller implemented, the contents of the hidden inventory will reflect what the contents of the solvent extraction cycle should be.

5.2.6.2 Estimation Of Full Load Inventory

A simulation of the 'loading' phase with the integral controller installed on the path to hidden inventory will generate transient data for the hidden inventory. This hidden inventory history then represents the modifications that need to be made to the history of the hold-up in the cycle, and summing these simulated histories will give the estimate of the true history of the solvent extraction cycle. The maximum value of this sum can therefore be used as an estimate of the full load inventory of the solvent extraction cycle, and the time taken to reach a fixed percentage of this value (typically 63%) can be used as the estimate of the cycle time constant. Clearly, in order to do this, it is important that the cycle has reached its steady state; if this is not the case, then the controller can remain on, and the rest of the commissioning process suspended until more data is available. A typical transient of the plutonium inventory in a solvent extraction cycle is shown in Figure 5.4.

5.2.6.3 Estimation Of Time Delay Due To Intervening Pipework

The pipe network in the solvent extraction areas can often be of significant length, and so material may transiently disappear into this pipework, and not re-appear until a significant time later. These time delays are obviously an important feature of the plant, and should be modelled as accurately as possible within the simulation, but often information on how long such pipe delays may be is not available.

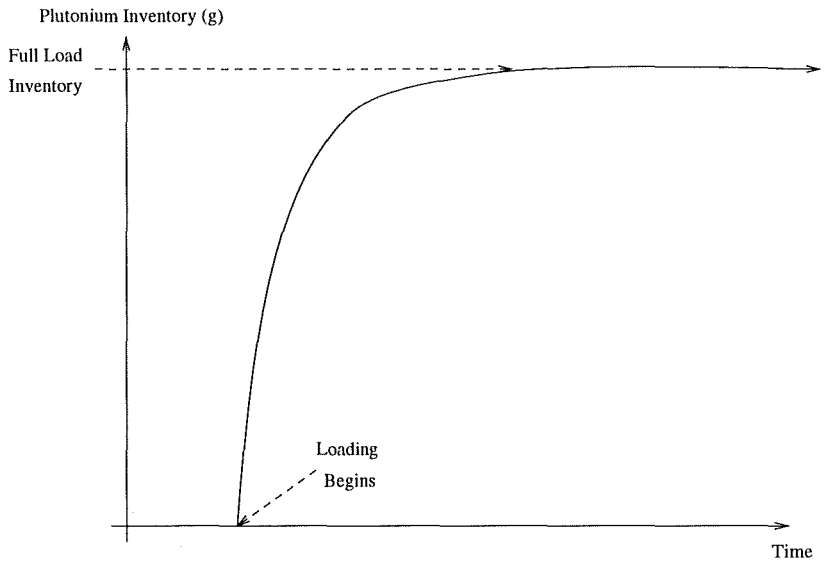


Figure 5.4: Plutonium inventory in a solvent extraction cycle

An estimate of this value can be obtained by again applying the simulation. After an initial estimate for the full load inventory has been obtained, this value can be used in the simulation to generate a time history of the plutonium concentration in the receiving tank. This time history can be examined: the difference between the time of the first measurement of plutonium in the receiving tank and the time at which the simulation first shows plutonium arriving, will give an estimate of the time delay due to the pipework, as shown in Figure 5.5.

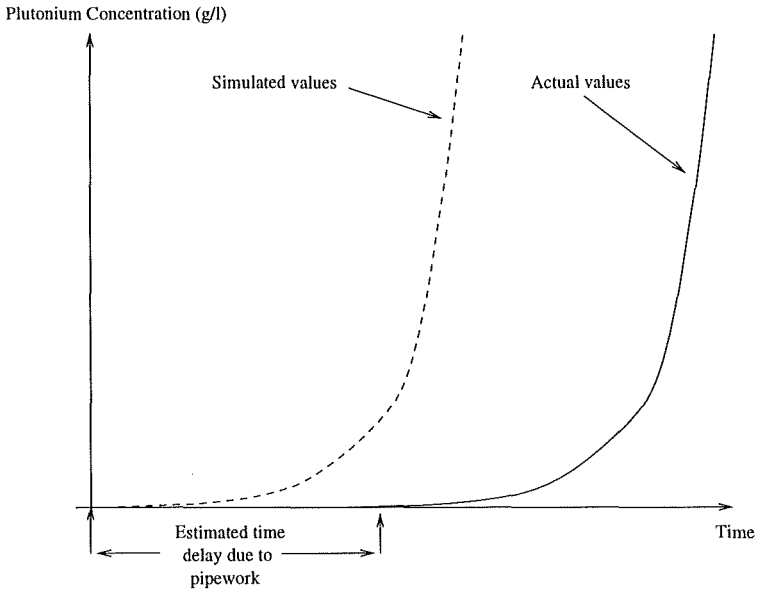


Figure 5.5: Estimation of time delay due to pipe work

5.2.6.4 Improving The Initial Estimates

The model-based diagnostic procedure described in Howell and Scothern (1995a), can be applied to the simulation to obtain more accurate estimates of the desired parameters. The estimated values of the full load inventory, the time constant and the pipe delay can be perturbed simultaneously to find the solution which gives the best agreement with measurements in the tanks downstream of the cycle. Since this is a complex, non-linear problem, Powell's method, as described in Chapter 3, is used to calculate the revised estimates; if no acceptable solutions are found, the diagnostic procedure is re-iterated, using the best of the failed solutions as the new starting point. In this way estimates of the values of the parameters required can be substantially improved.

5.3 False Alarm Handling

The occurrence of false alarms in traditional monitoring systems is a well known problem, as is the trade off between sensitivity and false alarm rate (see, for example, Owen, 1985, Maryak et al, 1997, or Stewart, 1998). In the realm of nuclear materials safeguards, the consequences of declaring a diversion of nuclear material are serious for the state or commercial organisation concerned, and so the handling of false alarms is of some importance. The structure of the expert system rules is such that a diversion will only be hypothesised whenever no other reasonable explanations can be found to explain the behaviour of the plant, but even in this case, noisy data can occasionally be misinterpreted and a diversion may be hypothesised where none has actually taken place. This problem was highlighted during extensive testing of the diagnostic procedures using noisy data.

When applied to large tanks with volumes of around 20,000 litres, which can be found after the dissolver in a commercial reprocessing plant, an error of 100 litres might occasionally arise. If the system is sufficiently sensitive then this would lead to the identification of the data spike as an actual transfer in or out of the tank, even though no such transfer actually occurred. An example of such a spike is shown in Figure 5.6.

Since this apparent loss does not correspond with a rise in any other tank, the diagnostic algorithm will be forced to conclude that either the event was a transfer of 100 litres out of

the tank or it was a measurement error. The correct answer is of course the measurement error, but since this answer could be applied to any feature of the data whatsoever, it is not automatically selected by the expert system, with the result that a flow to a hidden inventory would be hypothesised.

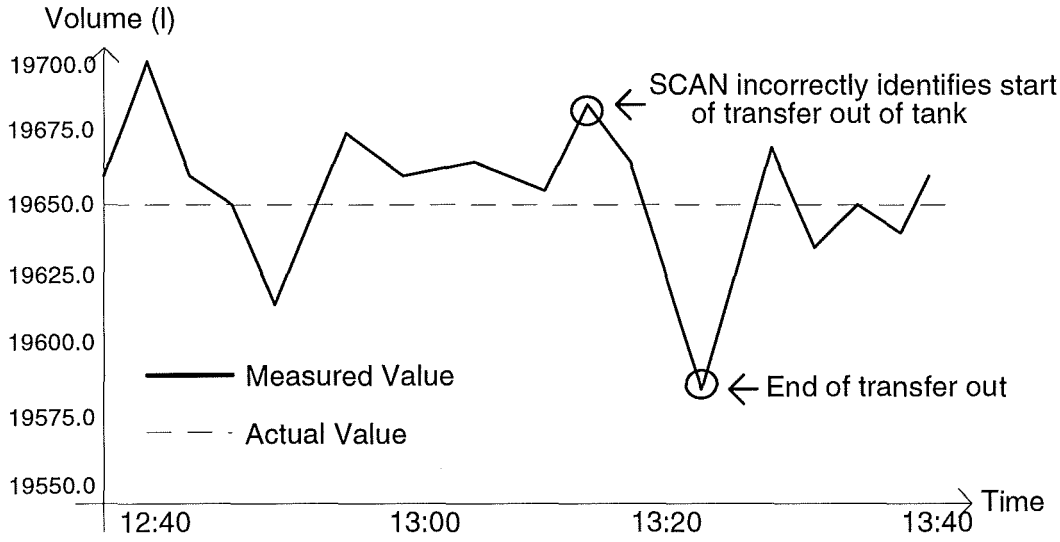


Figure 5.6: Incorrect identification of transfer

However, using model-based diagnosis, this type of false alarm will be identified the next time any transfer is made to or from the tank involved, since the diagnostic procedure will examine the transfer, and note that after the transfer, the volume in the tank is in error by the same amount that was wrongly transferred out due to the false alarm. The diagnosis will then be that material needs to be added to the tank from a hidden inventory to make up the loss. This diagnosis will be seen to cancel out the previous false alarm, indicating that either the transfer out never actually occurred, or that it was a transient effect, perhaps a transfer to pipework which subsequently returned and so has no safeguards implications.

This is illustrated in Figure 5.7; 100 litres is removed between points A and B due to the (incorrect) inclusion of the transfer to hidden inventory, and the shortfall will subsequently be detected by the diagnostic procedure at point C, where it will find that 100 litres needs to be added back into the system to give the correct measurements.

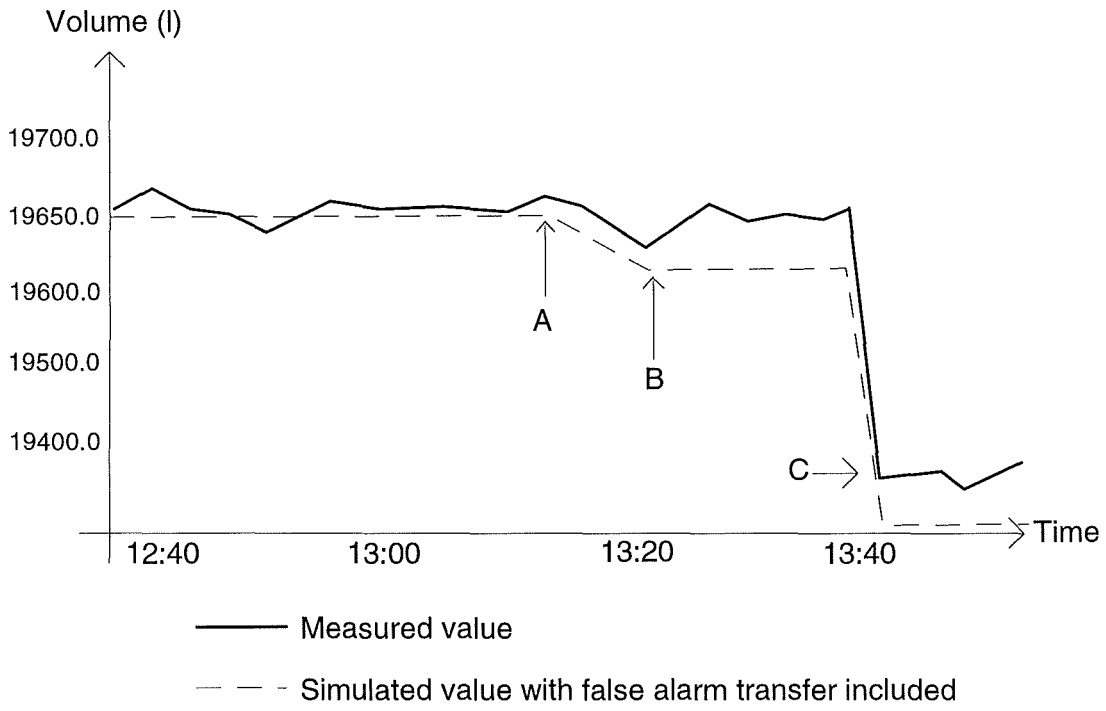


Figure 5.7: Effect of including incorrect transfer

The occurrence of these types of false alarms could be reduced by pre-filtering the data before it is sent to the diagnostic algorithm for processing, since if the only data present is the start and ends of transfers or events, such anomalies due to noise will not occur. It is also important to realise that examples like the one above can often be resolved automatically during 'stage 3' of the diagnostic procedure, i.e. the examination of the error time history, as described in Chapter 2.

CHAPTER 6

6. CONCLUSIONS AND FURTHER WORK

6.1 Solution Monitoring

In the planned Rokkasho Reprocessing Plant (RRP), the annual material balance standard deviation based on traditional monthly accounting will be too large to meet the protracted loss detection goal specified by the International Atomic Energy Agency (IAEA), as pointed out by Burr and Wangen (1996b). This demonstrates the need for systems that enhance the conventional accountancy approach, and one possible way of doing this, solution monitoring has been introduced in this thesis. The solution monitoring system proposed can fulfil many of the roles envisaged by Burr and Wangen (1996a), in assisting the safeguarding of nuclear material. The most significant role is the identification of all normal and abnormal process events, such as diversions of material. The emphasis is on events: what is an event, how does one re-construct all events from plant data and so on.

6.2 The Diagnostic System

The bulk of the diagnostic system was described in Chapter 2. After reviewing some existing model-based diagnostic systems, an overview of the entire diagnostic process was given, emphasising the order in which the diagnostic procedure needs to handle various events, specifically,

i) abrupt events,

ii) gradual events,

iii) hybrid events and any remaining errors.

This was followed by details of the specific elements of the system. Initially a scheme for classifying events was proposed; based on the principle that some events are more likely to

be acceptable to the operator than others. A methodology for the formation of the event list was given, consisting of the following steps:

i) examine raw data to extract features which need explaining (the sub-events);

ii) determine all possible causes for each sub-event using the diagnostic algorithms;

iii) examine permutations of sub-events over time to find all possible events which could explain the data;

iv) choose the most likely events from the list produced.

Problems which may arise from events which span the boundary of the time period under examination were considered, and methods for handling such events formulated. In order to effectively perform step iv) above, a scheme for ranking events based on Bayesian evidential updating was described. This included consideration of methods of supplying various probabilities that would be straight forward for the end user, even if multiple pieces of evidence were deemed to be mutually dependant.

Chapter 2 also contained a significant amount on the nature of the user interface, both for the diagnostic package, where it is vital that the user has the final say in accepting or rejecting all of the events hypothesised by the system, and also for the facilities available for creating and maintaining databases of rules which are used to identify, classify and rank the events. Subsequent sections covered the handling of gradual and hybrid events, and presented a methodology for correcting any significant errors that may remain after all gradual and abrupt diagnoses have been performed. The Chapter concluded with comments on areas where the diagnostic system was likely to fail, and included methods which had been used to overcome the difficulties.

The improvements and extensions to the diagnostic method presented in Chapter 3 allow the technique to be applied successfully in a greater range of situations, increasing its use as a diagnostic tool. The recommendations for the use of aligned vectors, and the option to use alternative methods for searching for acceptable diagnoses, allow the user to make

more efficient use of the method when attempting to resolve particularly difficult diagnostic issues.

Chapter 4 addressed the issue of the models used to simulate the plant. Physical equations for simulating the state of the process in the various plant elements were given, as was a method of representing errors in tank calibration equations, to allow the diagnostic procedure to attempt to diagnose such errors. An automatic generator for these models was presented, the availability of which, greatly increases the flexibility and applicability of the diagnostic procedure, allowing it to be used on a variety of plant configurations with the minimum of user coding.

The applicability of the diagnostic procedure to continuous process elements was discussed in Chapter 5, and an automatic method to estimate parameters for solvent extraction areas was presented. The issue of false alarms was addressed, and the diagnostic methods for dealing with them covered.

6.3 Summary

It has been demonstrated that solution monitoring has the potential to be a valuable aid for inspectors responsible for nuclear materials safeguards, providing additional assurance to supplement traditional materials accountancy methods. Working prototypes of all of the systems described within this thesis have been produced, and the user interfaces have been developed with considerable feedback from the IAEA. The systems have been evaluated using data sets pertaining to both real and hypothetical plants. This work is too detailed for presentation here, but some of the results can be found in Howell and Scothern, (1998). Features of the current system described within this thesis which are likely to be of particular use are:

- automatic generation of a hypothesis of plant operation, which may be used to verify the operators declarations;
- the ability to investigate the effects of alternative hypotheses;

- design verification assurance; this is achieved almost incidentally by the use of hidden inventories and the perturbation of all possible material transfer paths;
- the ability to view all plant measurement data in a graphical form, including superimposing simulation predictions on top of actual data to highlight discrepancies;
- consistency checks on transfers between monitored tanks;
- the estimation of hold up in un-monitored locations, such as pipes or solvent extraction areas;
- at a glance display of any events which may be of particular interest, or which may have safeguards applications;
- the potential to detect sensor malfunctions and calibration errors;
- the potential to detect long term problems on the plant, such as leaking valves;
- the diagnostic methods used are not easy to circumvent, even if the methods are known, which reduces the potential for diversion of material;
- high degree of automation, but all relevant information is available to the user, and any automatically generated hypotheses can be rejected or modified if desired, leaving ultimate control in the hands of the inspector;
- the methods used can be applied to information poor plants, where more traditional methods typically have problems;
- with the aid of user friendly graphical interfaces, the diagnostic package can be operated and understood with the minimum of additional training;
- event descriptions, including supporting evidence can be modified in an evolutionary manner, as the inspectors knowledge of the plant increases;
- the occurrence of false alarms due to incorrect identification of events is in many cases self-correcting;
- automatic model generation facilities give the package increased portability, and allow for its application on a wide variety of plants.

6.4 Recommendations For Future Work

The work presented in this thesis demonstrated a working prototype of a diagnostic package. There are many possible improvements and refinements which could be made to the system in the future, some possibilities are listed below :

- automatic generation and updating of rule sets by the system as data is received,
- real time tracking of the simulation instead of on a day by day basis,
- improvements to the diagnostic search algorithm (see Chapter 3), to increase speed of computation by using expert knowledge to reduce the search space;
- automatic 'tuning' of the various model parameters (this is already accomplished for some parts of the model, during the commissioning phase, see Chapter 5 for details).

REFERENCES

AbuHanna, A., Benjamins, V.R., and Janswijer, W.N.H. (1992). Integrating Multiple Model Types In Model Based Diagnosis, *Applications of Artificial Intelligence in Engineering*, pp.693-708.

Acton, F.S. (1990). Numerical Methods that Work, corrected edition, *Mathematical Association of America*, pp.464-467.

Annibal, P.S., and Roberts, P.D. (1989). Improvements In Statistical Techniques For Nuclear Material Accountancy, *11th Symposium on Safeguards and Nuclear Material Management,* Luxembourg, pp.345-349.

Bell, S.C., McDonald, J.R., McArthur, S.D.J., Burt, G.M., Mather, R. and Burt, S.M. (1995). Integrating Model Based Diagnosis into a Decision Support System for Protection Engineers, *Proceedings of the Universities Power Engineering Conference*, Vol.2, pp.423-426.

Benedict, M., Pigford T.H., and Levi H.W. (1981). Nuclear Chemical Engineering, 2nd Edition, *McGraw-Hill.*

Berger, J.O. (1985). Statistical Decision Theory and Bayesian Analysis, *Springer-Verlag, New York Inc.* pp.129.

Bernado, J.M., and Smith, A.F.M. (1993). Bayesian Theory, *Wiley Series in Probability and Mathematical Statistics*, ISBN 0 471 92416 4.

Boutilier, C. (1996). Abduction to Plausible Causes: An Event-Based Model of Belief Update, *Artificial Intelligence*, Vol.83, No.1, pp.143-166.

Brent, R.P. (1973). Algorithms for Minimisation Without Derivatives, *Englewood Cliffs*, NY, Prentice Hall, Chapter 5.

Buchanan, B.G., and Shortliffe, E.H. (1985). Rule-Based Expert Systems, *The MYCIN Experiments of the Stanford Heuristic Programming Project,* The Addison-Wesley Publishing Company.

Burr,T.L., Coulter, C.A., Hakkila, E.A., Ai, H., Kadokura, I., and Fujimaki, K. (1995). Statistical Methods for Detecting Diversion of Materials Using Near-Real-Time Accounting Data, *Journal of the Institute of Nuclear Materials Management* No.24, pp.1032-1037.

Burr, T. and Wangen, L. (1996a). Development and evaluation of Methods for Safeguards Use of Solution Monitoring Data, *Los Alamos National Laboratory*, LA-13185-MS.

Burr, T. and Wangen, L. (1996b). Enhanced Safeguards Via Solution Monitoring, *Los Alamos National Laboratory*, LA-13186-MS.

Candy, J.V., Rozsa, R.B. (1980). Safeguards Design For a Plutonium Concentrator - An Applied Estimation Approach. *Automatica*, Vol.16, No.6, pp.615-627

Chen, Z. (1995). Fuzzy Temporal Reasoning for Process Supervision. *Expert Systems*, Vol.12, No.2, pp.123-137.

Coulter, C. A., Burr, T. L., Hakkila, E. A., Ai, H., Kadokura, I., and Fujimaki, K. (1995). Estimating Reprocessing Plant In-Process Inventories by Simulation, *Journal of the Institute of Nuclear Materials Management* Vol.24, pp.738-743.

Davis, R. (1980). Meta-rules: reasoning about control, *Artificial Intelligence*, No.15, pp.179-222.

Dekens, J.P. et al (1995). An Integrated Safeguards System For Large Scale Reprocessing Plants, *The 5th International American Nuclear Society Topical Conference on Facility Operations-Safeguards Interface*, Wyoming.

Duda, R.O., Hart, P.E., and Nilsson, N.J. (1976). Subjective Bayesian Methods for Rule-Based Inference Systems, *American Federation of Information Processing Societies, Proceedings of the National Computer Conference*, Vol.45, pp.1075-1082.

Finch, F.E., Oyeleye, O.O. and Kramer, M.A. (1990). A Robust Event-orientated Methodology for Diagnosis of Dynamic Process Systems, *Computers Chemical Engineering*, Vol.14, No.12, pp.1379-1396.

Forbus, K.D. (1987). Interpreting Observations of Physical Systems, *IEEE Transactions on Systems, Man and Cybernetics*, Vol. SMC-17, No.3, pp.350-359.

Frank, P.M. (1990). Fault Diagnosis in Dynamic Systems Using Analytical and Knowledge-Based Redundancy - A Survey and Some New Results, *Automatica*, Vol.26, No.3, pp.459-474.

Franssen, F. (1994). International Atomic Energy Agency, Vienna. Personal communication.

Franssen, F., Foggi, C., and Hunt, B. (1995). Tank Data Acquisition and Evaluation in a Large Scale Reprocessing Plant, *Proceedings of the 17th Annual Symposium On Safeguards and Nuclear Material Management*, Ispra, Italy, ESARDA 27, pp.383-388.

Gaschnig, J. (1982). Prospector: An Expert System for Mineral Exploration. *Introductory Readings in Expert Systems, Gordon and Breach Science Publishers*, Chapter 3, pp.47-64.

Gensym. G2 - a registered product of Gensym, 125 Cambridge Park Drive, Cambridge, Ma, USA.

Gertler, J.J. and Anderson, K.C. (1992). An Evidential Reasoning Extension to Quantitative Model-Based Failure Diagnosis, *IEEE Transactions on Systems, Man and Cybernetics*, Vol.22, No.2.

Ham, P.G. (1979). Operation Data Reconcilliation: An Aid to Improved Plant Performance, *Proceedings of the 10th World Petrolium Congres*s, Vol.4, pp-281-286.

The Heath and Safety Executive (1995). 'Thermal Oxide Reprocessing Plant (THORP) - The Regulation of THORP by HM Nuclear Installations Inspectorate', *HSE Books*, Sudbury, Suffolk, ISBN 0717610047.

Henry, M.P. and Clarke, D.W. (1993). The Self-Validating Sensor: Rationale, Definitions and Examples, *Control Engineering Practice*, Vol.1, pp.585-610.

Himmelblau, D.M. (1978). Fault Detection and Diagnosis in Chemical and Petrochemical Processes. *Elsevier*, NY.

Howell, J. (1994). Model-based Fault Detection in Information Poor Plants, *Automatica,* Vol.30, No.6, pp.929-943.

Howell, J. and Scothern, S.J. (1995a). Model-Based Diagnosis As An Aid To Anomaly Resolution, *UK Safeguards R&D Programme Report,* UKAEA Report SRDP-R226.

Howell, J. and Scothern, S.J. (1995b). Automatic Model Generation For Model Based Fault Detection In Process Plants, *IFAC Workshop on On-Line Fault Detection and Supervision In The Chemical Process Industries,* Newcastle, UK.

Howell, J. and Scothern, S.J. (1996a). A Rule-Based Interpreter of Model-Based Diagnostic Results, *UK Safeguards R&D Programme Report,* UKAEA Report SRDP-R243.

Howell, J. and Scothern, S.J. (1996b). A Prototype Diagnostic Aid for a Pu Tank Monitoring System, *UK Safeguards R&D Programme Report,* UKAEA Report SRDP-R244.

Howell, J. and Scothern, S.J. (1998). Assessing Solution Monitoring System Performance Using Simulated Data, *UK Safeguards R&D Programme Report,* UKAEA Report SRDP-R261.

IAEA (1987), IAEA Safeguards Glossary, *International Atomic Energy Agency*, IAEA/SG/INF/1 (rev. 1), Vienna.

IAEA (1992). The Structure and Content of Agreements Between the Agency and States Required in Connection with the Treaty on the Non-Proliferation of Nuclear Weapons. INFCIRC/153 (Corrected), *International Atomic Energy Agency*, Vienna.

Ikawa K. et al (1983). Study of the Application of Near-Real-Time Materials Accountancy To Safeguards For Reprocessing Facilities, *Japan Atomic Energy Research Institute,* Report PNCT N841-33-26.

Isermann, R. (1984) Process Fault Detection Based on Modelling and Estimation Methods - A Survey. *Automatica*, Vol.20, pp.387-404.

Isermann, R. (1994). On the Applicability of Model-based Fault Detection for a Technical Process, *Control Engineering Practice*, Vol.2, No.3, pp.439-450.

Isermann, R. (1995). Model Based Fault Detection and Diagnosis Methods, *Proceedings of the American Control Conference*, Vol.3, pp.1605-1609.

Isermann, R. and Ballé, P. (1997). Trends in the Application of Model-based Fault Detection and Diagnosis of Technical Processes, *Control Engineering Practice*, Vol.5, No.5, pp.709-719.

Islam, B.M.N., Johnson, S.J., Sellinschegg, W.D. (1993). Meeting Timeliness Requirements in Reprocessing Plants, *JNMM,* October, pp.19- 24.

Jacobs, O.L.R. (1993). Introduction to Control Theory, *Oxford Science Publications*, Oxford University Press, ISBN 0-19-856249-7, Chapter 10, pp.216-235.

Jaech, J.L., (1974). Control Charts For MUF's, *Journal of the Institute of Nuclear Materials Management*, Vol.2, No.4, pp.16-28.

Katzan, H. (1978). FORTRAN 77, *New York London*: Van Nostrand Reinhold.

Kirillov, V.P. (1994). Constructive Stochastic Temporal Reasoning in Situation Assessment, *IEEE Transactions on Systems, Man and Cybernetics*, Vol.24, No.8, pp.1099-1113.

Kramer, R.A. (1981). Application of Computer Graphics to Nuclear Safeguards and Security Analysis, *Journal of the Institute of Nuclear Materials Management,* Vol.10, No.3, pp.41-42.

The LASCAR forum (1992). Report of the LASCAR Forum: Large Scale Reprocessing Plant Safeguards, *International Atomic Energy Agency*, Vienna, STI/PUB/922.

Leitch, R., Shen, Q., Coghill, G., Chantler, M., and Slater, A. (1993). Qualitative Model Based Diagnosis of a Continuous Process, *Applications of Artificial Intelligence in Engineering*, Vol.2, pp.291-309.

Lichtenberg, G. and Lunze, J. (1996). Identification of Discrete Event Models for Continuous-variable Systems, UKACC International Conference on CONTROL, *IEE Conference Publication 427/1*, pp.711-715.

Marayak, J.L., Hunter, L.W., and Favin, S. (1997). Automated System Monitoring and Diagnosis Via Singular Value Decomposition, *Automatica,* Vol.33, No.11, pp.2059-2063.

Milne, R. (1987). Strategies for Diagnosis, *IEEE Transactions on Systems, Man and Cybernetics*, Vol. SMC-17, pp.333-339.

Milne, R. (1991). Integration: the Key to Second Generation Applications. *IFAC Fault Detection, Supervision and Safety for Technical Processes*, Baden-Baden, pp.333-335.

Nelder, J.A. and Mead, R. (1965). *Computer Journal*, Vol.7, pp.308-313.

Owen, J.W. (1985). Setting Sensitivity Standards For The Facility Intrusion Detection System (FIDS), *University of Kentucky, Office of Engineering Services (Bulletin)*, pp 35-40.

Patton, R., Frank, P.M., and Clark, R.N. (1989). Fault Diagnosis in Dynamic Systems: Theory and Applications, *Prentice-Hall*, Englewood Cliffs, NJ.

Peng, Y. and Reggia, J.A. (1987a). A Connectionist Causal Model for Diagnostic Problem Solving. *IEEE Transactions on Systems, Man and Cybernetics*, Vol. SMC-19, No.3, pp.285-298.

Peng, Y. and Reggia, J.A. (1987b). A Probabilistic Causal Model for Diagnostic Problem Solving Part II: Diagnostic Strategy, *IEEE Transactions on Systems, Man and Cybernetics*, Vol. SMC-17, No.3, pp.395-406.

Powell, M.J.D. (1968). A FORTRAN Subroutine for Solving Systems of Non-linear Algebraic Equations, *United Kingdom Atomic Energy Authority*, AERE-R 5947.

Press, W.H., Teukolsky, S.A., Vetterling W.T. and Flannery, B.P. (1992). Numerical Recipes in FORTRAN, Second Edition, *Cambridge University Press*, Chapter 10.

Rai, A. and Weinroth, J. (1990). Search Space Reduction and Model Configuration. An Expert Systems Approach, *International Journal of Computer Applications in Technology*, Vol.3, No.1, pp.18-25.

Quinlan, J.R. (1983). Inferno: A Cautious Approach To Uncertain Inference, *The Computer Journal*, Vol.26, No.3, pp.255-269.

Scothern, S.J., and Howell, J. (1997). A Physical-Model-Based Diagnostic Aid For Safeguarding Nuclear Material In A Liquor Storage Facility, Journal Of Nuclear Materials Management, Vol. 25, No. 4, pp 20-29.

Scothern, S.J., and Howell, J. (1998). An Automatic Diagnostic Aid Generator, *UK Safeguards R&D Programme Report,* UKAEA Report SRDP-R262.

Shoham, Y., and McDermott, D. (1988). Problems in Formal Temporal Reasoning, *Artificial Intelligence*, Vol.36, pp.49-61.

Shipley, J.P. (1978). Decision Analysis For Nuclear Safeguards, *Nuclear Safeguards Analysis; Non-Destructive and Analytical Chemical Techniques*, Chapter 4, pp.35-63.

Siklóssy, L. and Tulp, E. (1991). Space Reduction Method: A Method to Reduce the Size of Search Spaces, *Information Processing Letters,* Vol.38, No.4, pp.187-192.

Speed, T.P. and Chulpin, D. (1986). The Role of Statistics in Nuclear Materials Accounting: Issues and Problems, *Royal Statistical Society Discussion Paper*, RSS(A) 97013.

Stefanini, A. et al (1993). Esprit Project 5143 (ARTIST): Achievements of the Project. *CISE Report Number 7838*, pp.35.

Stewart, N.A. (1998). Is it a False Alarm?, *IEE Colloquium (Digest),* No.221, pp.10/1-10/5.

Tamhane, A.C. and Mah, R.S.H. (1985). Data Reconciliation and Gross Error Detection in Petrochemical Process Networks, *Technometrics*, Vol.27, No.4, pp.409-422.

Vale, Z.A., and Machado e Moura, A. (1992). An Expert System with Temporal Reasoning for Alarm Processing in Power System Control Centers, *IEEE Transactions on Power Systems*, Vol.8, No.3, pp.1307-1314.

Walford, F.J., Mills, A.L., Waterman, M.J. and Boler, S.A. (1987). Variations in the Plutonium Inventory of Solvent Extraction Contactors, *United Kingdom Atomic Energy Authority*, England.

Wilsky, A.S. (1976). A Survey Of Design Methods For Failure Detection In Dynamic Systems, *Automatica*, Vol.12, pp.601-611.

Wolf, A.V., Brown, M.G., and Prentiss, P.G. (1966) Aqueous Solutions And Body Fluids: Their Concentrative Properties And Conversion Tables, *New York: Hoeber*, pp.D-238.