

BLLID No:- D66112/86

LOUGHBOROUGH
UNIVERSITY OF TECHNOLOGY
LIBRARY

AUTHOR/FILING TITLE

HOENIG, G

ACCESSION/COPY NO.

138646/02

VOL. NO. 1

CLASS MARK



- 1 JUL 1994

30 JUN 1995

28 JUN 1996

27 JUN 1997

- 2 JUN 1999

LOAN COPY

013 8646 02



A COMPUTER BASED ALARM HANDLING SYSTEM

FOR PROCESS PLANT

by

GARY HOENIG

VOL I

A Doctorial Thesis
Submitted in partial fulfilment of requirements
for the award of
Doctor of Philosophy of the
Loughborough University of Technology

August, 1982

© by Gary Hoenig

Loughborough University of Technology Library	
Doc	Dec 82
Class	
Acc. No.	138 646/02

ACKNOWLEDGMENTS

The author would like to express his gratitude to the Department of Industry (DOI) who financed contractual work from which the study in this thesis developed. In particular thanks are due Dr. I.G. Umbers, Dr. P.J. King and the staff of Warren Spring Laboratory, DOI whose technical support has been invaluable. The author is also indebted to Prof. F.P. Lees and Dr. P.K. Andow for their considerable advice and encouragement during this study. Special gratitude must be expressed to T.M. Neale whose considerable assistance made prototype construction possible. Further thanks are due Prof. D.C. Freshwater and all members of the Department of Chemical Engineering at Loughborough University of Technology.

A Computer Based Alarm Handling System for Process Plant

G. Hoenig

ABSTRACT

① The modern process plant is characterised by the use of computers for process control. Increasing reliability and diminishing capital investment costs have encouraged the use of process computers as the principal control mechanism. Greater reliability has also led to an increase and change in the tasks assigned to the computer. The relatively rapid advances in process control have understandably resulted in a carry-over of traditional practices which are often inadequate in the present day environment. A notable example of such a practice is the alarm system which is neglected in the literature and is frequently the least satisfactory aspect of a control system.

② Presented in this work is a review of the development of alarm technology in the process industries. The survey exemplifies the relatively limited literature available on the subject. Topics from a variety of disciplines are shown to be relevant.

An analysis of the role of alarms on the process plant is presented. ^{process} Aspects of alarm data generation and man-machine interface requirements are discussed.

④ An examination of the alarm techniques presently implemented concludes that many existing alarm systems are poorly thought out and are often inadequate, while others can be too complex and costly for process plant applications.

⑤ As a result of the foregoing analyses an alarm handling system for process plant has been proposed and developed which overcomes many of the identifiable shortcomings of existing systems. ⑥ The term 'handling' is used to distinguish the system from alarm analysis systems since it manipulates alarm/status information without performing prime cause analysis. ⑦ The system has been developed to combine features from conventional alarm systems with some simplified alarm analysis and attempts to deal with a wide variety of alarm types.

The software package runs on a dedicated microcomputer which will interface either to a process computer or plant contacts and sensors. The dedicated characteristics allow the unit to be added onto an existing plant without affecting the resident control system. This approach has the advantages that it allows simple retrofit and direct before and after comparisons of the effectiveness of the overall plant control scheme. Features such as these make the alarm handling system useful as a tool for further evaluation of alarm system methodologies.

TABLE OF CONTENTS

<u>Chapter</u>	<u>Page</u>
Acknowledgements	i
Abstract	ii
1. <u>Introduction</u>	1
2. <u>Literature Survey</u>	7
3. <u>The Role of Alarms and Alarm Systems</u>	18
3.1 Introduction to the Concepts of Alarms	18
3.2 Alarm Definitions	22
3.2.1 Categorisation by Plant Mode	22
3.2.2 Categorisation by Type	27
3.2.3 Categorisation by Causative Class	29
3.3 The Role of the Alarm System	30
3.3.1 Alarm System Functions	31
3.3.2 The Operator	32
3.4 Types of Available Alarm Systems	35
3.4.1 General Purpose	38
3.4.1.1 Alarm Annunciators	38
3.4.1.2 Computer Control System Based	40
3.4.1.3 Control Language Based	43
3.4.2 Application Specific	43
3.4.2.1 Alarm Handling	43
3.4.2.2 Alarm Analysis	43
3.5 Alarm CRT Displays	44
3.6 Alarm Information	46
3.7 Selection of Alarms and Alarm Parameters	49

3.8	The Need for an Alarm Handling System for Process Plant	51
4.	<u>Some Identifiable Alarm Detection Functions</u>	53
4.1	Introduction	56
4.2	Basic Alarm Detection	56
4.2.1	Absolute	56
4.2.2	Deviation	56
4.2.3	Band	57
4.2.4	Binary (ON/OFF)	57
4.3	Enhancing Basic Alarm Detection	60
4.3.1	Derived	60
4.3.2	Hysteresis	60
4.4	Advanced Alarm Detection	63
4.4.1	Deduced	63
4.4.2	Group	65
4.4.2.1	Information Overload	65
4.4.2.2	Other Interrelated Effects	66
4.4.3	Mode	71
4.4.4	Voting or Quorum Gate	73
4.4.5	Asynchronous Groups	73
4.5	Time Related Detection	75
4.5.1	Sequences	81
4.5.1.1	Simple Sequences	81
4.5.1.2	Conditional Sequences	82
4.5.1.3	Clock Linked Sequences	84
4.6	Combining Alarm Detection Functions	85
4.7	Validity and Verification of Process Data	85
4.8	Process Data Types	87
4.9	Versatility	87
4.10	Display Requirements	88

5.	<u>Using Events to Describe Alarm Conditions</u>	92
5.1	Introduction	92
5.2	Events	94
5.3	Defining Events	95
5.4	Combining Events in Enhanced Boolean Expressions	97
5.4.1	VOT Operator	99
5.4.2	ASG Operator	103
5.4.3	Time Related Events	103
5.5	Event Processing	106
5.6	User Programming and Processing Structures	111
5.7	Benefits of Event Descriptions	113
5.8	Storage of Alarm Handling Data	114
6.	<u>Implementation of an Alarm Handling System</u>	116
6.1	Introduction	116
6.2	Summary of the Problem	116
6.3	Alarm Handling	121
6.4	Assumptions	121
6.5	Projected Benefits	124
6.6	The Alarm Handling System	125
6.6.1	Overview	127
6.6.2	The Off-Line System	128
6.6.2.1	OFLAD	130
6.6.2.2	COMP	133
6.6.2.3	TRANSFER	134
6.6.2.4	Example Use of the Off-Line System	134
6.6.3	The On-Line System	152
6.6.3.1	Data Acquisition	159
6.6.3.2	Event Processing	160
6.6.3.3	Alarm Generation	160

6.6.3.4	Usage of On-Line System	161
6.6.3.5	Management by Exception	161
6.7	Hardware Selection	163
7.	<u>Discussion</u>	168
7.1	Introduction	168
7.2	On-Line System Performance and Improvements	170
7.2.1	Data Acquisition	170
7.2.2	Event Processing	174
7.2.3	Alarm Generation	175
7.2.4	Data Base Size	178
7.2.5	Overhead Tasks	179
7.2.6	On-Line Summary	181
7.3	Off-Line System Performance and Improvements	185
7.4	General Discussion	186
7.4.1	Security	186
7.4.2	Difficulties in System Development	188
7.4.3	Accuracy of an Alarm System	188
7.4.4	Time Resolution	189
7.4.5	Level of Alarming on Process Plants	190
7.4.6	Location of Alarm System Functions	192
7.5	Plant Acceptance	193
8.	<u>Conclusion</u>	195
	References	199
	Bibliography	205
	Appendices (contained in volume 2)	

CHAPTER 1

INTRODUCTION

Alarm systems on process plant have become increasingly important especially with the implementation of modern process control computers. The use of computers in process control applications began in the early 1960's. At that time computers were costly and unreliable. The role of the process computer was subsidiary to or parallel with accompanying analogue control equipment.

By the mid 1970's greater reliability and reduced capital costs encouraged the use of process computers as the principal control mechanism. The increased reliability also led to an increase and change in the tasks assigned to the computer. Today the role of the process computer is still evolving as capital investment costs for computers become less significant and computer reliability steadily improves. The relatively rapid advancements in process control have understandably resulted in a carry-over of traditional practices which are often inadequate in the present day environment. A notable example of such a practice is the alarm system which is neglected in the literature and is frequently the least satisfactory aspect of a control system (Lees 1980 [1]).

The problem with conventional alarm systems which is inherited by computer driven alarm systems appears to be that their role as a component in a control system has not been extensively examined (Andow and Lees 1974 [2]). Specific criticisms have come from Kortlandt and Kragt 1978 [3], 1980, [4]) who made an assessment of the alarm systems

of two process plant and found that they were poorly thought out and generally inadequate. Some of their conclusions included:

- 1) Inconsistency of alarm assignment
- 2) 'Oscillatory' alarms
- 3) Persistent alarms
- 4) Insufficient planning in the presentation of alarm information

These inadequacies contribute to the operators' uncertainty about the reliability of the alarm information presented to them and therefore undermines their confidence in the alarm system.

The consequences of poorly thought out or inadequate alarm systems on overall control system performance is exacerbated by the following developments in process plants which have increased the information load on the process operator:

- 1) The complexity of modern plants has resulted in an increase in the number of process parameters which are to be controlled.
- 2) Improved instrument technology has resulted in greater availability of plant status information.
- 3) An increased emphasis on optimisation, loss prevention, and safety has necessitated closer monitoring and control of plants.

The above analysis suggests that insufficient

consideration has been given either to the role of the process plant alarm system as a man-machine interface or to the importance of alarm systems in modern process plants. The alarm system needs to be structured so that it is capable of generating alarm information in such a way as to aid the operator in his tasks of fault detection, diagnosis, and correction, and therefore it has to be designed to accurately detect and display a wide range of plant malfunctions.

It is not difficult to identify aspects of process plant alarm systems which would be desirable to improve. Since the alarm system is principally a man-machine interface there are many ergonomic problems to consider which involve the presentation of alarm information to the operator. An efficient alarm system should attempt to satisfy some of the operator's information needs.

One of the first activities in the implementation of an alarm system is to determine what plant states constitute an alarm condition. It is important to select alarm conditions accurately to avoid false alarms. Additionally spurious alarms are frequently caused by the insensitivity of the alarm system to routine changes in plant operation for example at startup and shutdown. The inappropriate selection of alarm limits leads to the creation of spurious alarms.

A further consideration in the design of an alarm system is the information which should be conveyed to the operator when an alarm condition has been detected. The interpretation of alarm message contents can effect the operator's choice of corrective action to rectify plant faults.

Very little research work has been done on how alarm

information should be presented to operators. The traditional method of presenting alarms is through a hardwired annunciator panel, but this has the disadvantage that alarm indications are spacially fixed and physically separate from their associated plant instrumentation. Computer control systems have tended to utilize VDU's for presenting plant information, with alarm lists in chronological order in a series of alarm pages which are often found unsatisfactory by operators (Jervis 1980 [5]).

The work in this thesis developed from studies of computer driven operator display systems for small process plant. A project in conjunction with the Department of Industry involved the development of a highly flexible computer driven VDU system which could be used to study operator response times for various process information display formats. The system also provided a means of introducing computer technology gradually into process industries which were traditionally resistant to change.

It was apparent that for the display system to be useful in plant application, the quality and quantity of information presented to the operator was important not only in the display system but also in the control room generally. Aspects of operator displays or support systems were recognised as being a stiff problem to deal with.

It was decided that the development of the display system required additional features to generate the information to be presented. There are usually two types of plant information presented to the operator:

- 1) Plant variable data and
- 2) Alarm information

Of particular interest is alarm information since process data is relatively simple to obtain and as already noted process plant alarm systems have been neglected.

The purpose of the work described in this thesis was to investigate the various difficulties in alarm information generation and to propose a versatile and flexible general purpose alarm system which would be suitable for use on small process plant. The benefits of such a system can be readily hypothesised; however there are many outstanding questions which still require attention. A prototype computer based alarm handling system for process plant is proposed in the thesis which provides a wide variety of alarm facilities while also providing a tool for further studies of alarm systems in general.

The central theme of the thesis is (alarm handling) and the study is organised to reflect the work by emphasising the progression of studies from basic concepts to the final operational prototype.

The development of the alarm handling system evolved from studies of process plant alarms and alarm systems. The literature survey described in Chapter 2 reviews the history of alarm system technologies.

Chapter 3 examines the role of alarms on the process plant and proposes some alarm system definitions which are intended to consolidate alarm system terminology. A study of existing process plant alarm systems is also discussed.

In Chapter 4 the results of a study of some of the identifiable alarm detection functions which should be included in a comprehensive general purpose alarm system are discussed. The alarm detection functions are often complex and in Chapter 5 the problem of converting process data into

accurate alarm information is analysed.

In Chapter 6 a fully operational alarm handling system capable of dealing with up to 250 alarms is described. This system embodies the ideas developed in the earlier chapters.

A critical performance evaluation and discussion in Chapter 7 analyses the various features of the prototype alarm handling system.

In conclusion Chapter 8 summarises the study and reviews the problems that remain with some suggestions for further work.

CHAPTER 2

LITERATURE SURVEY

Presented in this chapter is a review of the pertinent publications directly concerned with alarms and alarm systems in the process industry. A search of the literature revealed only a small number of publications which are specifically concerned with process plant alarm systems. The majority of these papers are reviews or surveys of alarm system technologies offering few suggestions for design improvements while emphasising the need for further studies.

Due to the diverse nature of alarms there are a variety of related topics which necessarily effect alarm systems and the role they play in the overall plant control scheme. The subject of process plant alarms therefore encompasses topics which can be broadly categorised as follows:

- 1) Ergonomics of man-machine interface
- 2) Operator psychology, training and cognitive skills
- 3) Alarm and process information presentation
- 4) Alarm information generation techniques
- 5) Selection of the plant alarm locations and limits

All of the above topics are interrelated to some degree and usually publications discussing one topic include points from the other topics. The subject of this thesis, alarm handling, concerns principally the generation of alarm

information. This survey will be confined primarily to a review of the literature concerned with process plant alarm information generation systems and their applications. References to publications concerned with other topics will be inserted where relevant in the text.

Alarm systems can be classified generally as an operator support system since the system is intended to aid the operator in the detection of faults, the diagnosis of faults, and the selection of a corrective action strategy. Traditionally alarm systems have been neglected in the literature probably since their significance in the process control scheme was not clearly defined.

Before the 1960's alarm systems in the process industry essentially consisted of alarm annunciator panels and indicators. The alarms were located throughout the process plant as required to provide plant status information. Often equipment manufacturers mandated (as today) that alarms be placed on their equipment in order to maintain warranties. The prevalent attitude then (and now) appears to be that if a particular item might require attention under certain circumstances then an alarm was installed. Little consideration was given to the operator involvement in diagnostic tasks, consequently no real effort was made to define or improve alarm system methodologies. Furthermore there was a distinct lack of application of ergonomic principles. The above situation occurred principally for the following reasons:

- 1) Only moderate complexity of process plant
- 2) Low information flow
- 3) Decentralised operator control

4) Operator role not fully utilized

5) Optimisation, safety, and loss prevention not especially important.

Early studies of operator process control tasks by Crossman [6] in 1960 considered alarms as plant status indicators which could provide supplementary information to the operator when performing control and diagnostic tasks. This was one of the first times that alarms were recognized in the literature as a diagnostic tool.

During the 1960's computers were introduced on the process plant for data acquisition and automated process control, making a significant impact especially in the nuclear industry. Being a high risk industry the nuclear industry had the unique position of being able to try concepts that may not have been proven or cost effective. In early 1965 Welbourne [7] described the use of computer driven VDU's to display alarm information. By 1968 the increase in computer control had led to centralisation of the control and improved plant monitoring facilities. Since nuclear plants are very heavily alarmed the high alarm information load during abnormal conditions was already demanding methods for reducing alarm loads on operators. This would require some method of analysing alarm information. Once such system first applied to the nuclear industry is the First Out Annunciator System, developed by Westinghouse. Initially designed to complement alarm/event loggers, the system is very limited (Most alarm annunciator manufacturers now have first out systems.) This system can indicate the first alarm that occurred in a transient situation where many alarms are activated. The aim is to aid the operator in rapid recognition of the alarm that first occurred.

A further extension of the early First Out Systems was developed by the General Electric Co. in the USA and described by Shukla and Wong [8] as late as 1975. The Alarm Initiated Display (AID) recognizes preselected sequences of events. These sequences are selected to give the operator an early warning of conditions which, if not corrected, will lead to plant trips or pre-trip conditions. When an AID 'primary' variable is outside its predetermined limits, the variable is displayed to the operator along with the names and values of other variables which could contribute to an AID alarm condition. Generally, only a small number of 'primary' variables could be integrated into the AID system.

In the United Kingdom, the approach to alarm analysis has been more systematic and exacting. Computer based analysis techniques are used to analyse alarms and alarm sequences to determine 'prime cause' alarms. The potential of such an approach can extend far beyond the simple recording techniques of First Out and AID techniques. The first use of computer based alarm analysis techniques appeared at the Wylfa and Oldbury nuclear power stations in the late 1960's (Welbourne 1965 [7], 1968 [9]; Kay 1966 [10]; Kay and Heywood 1966 [11]; Patterson 1968 [12]). The systems use a computer controlled CRT display to provide the main alarm information operator display. The objective of the system is to inform the operator about deduced 'prime cause' alarms or causes of the disturbances and to maintain an updated list of the latest activated alarms. Other alarms related to the 'prime cause' alarms are usually suppressed on these displays, a technique referred to as 'alarm darkening'. Unlike the AID system all the plant alarms (3000) are integrated into the alarm analysis.

The alarm system methodologies on the Oldbury and Wylfa systems are based on fault tree and cause-consequence modeling and analysis. Cause-consequence analyses, which

relate the logical relationships between the alarms and their sequential appearance, are developed, and the results of the analysis are stored on the process computer in an alarm or fault tree structure. When an alarm occurs the program searches through the library of alarm trees to determine other alarms which can cause the disturbance. The program will also evaluate which of the activated alarms are the latest effect of the deduced 'prime cause' alarms. The approach using alarm trees can describe the typical alarm situations and it can also deduce non-instrumented or non-preselected alarms and alarm conditions. The analysis continues until as many of the activated alarms as possible are tied or associated with 'prime cause' alarms via alarm trees.

✓ The alarm tree development is performed manually by means of a careful examination of cause-consequence relationships in the Oldbury and Wylfa plants. ✓ The typical time required to develop the alarm trees for one plant has been reported to be about 10 man-years (Andow 1981 [13]), while the software development took about 25 man-years for one plant as reported by Welbourne [9] in 1968.

Still further developments were made to the UK approach by Gesellschaft fur Reaktorsicherheit (GRS) in Germany and the Halden Reactor Project in Norway. This system known as a STAR Disturbance Analysis System (DAS) is also based upon the cause-consequence analysis method and described by Øwre and Felkel [14] in 1978. It is called DAS since the system is intended to have the capability of analysing all plant conditions, both failure mode conditions and normal operational conditions. The major improvements over the Oldbury and Wylfa systems are:

- 1) Allows easier remodelling of cause-consequence relationships due to operator experience and component

change.

2) Incorporates time delay and probabilistic information.

3) Highly interactive operator communication allowing the operator to supply the system with information and allowing the operator to participate in the deduction and analysis of alarms.

The key to the DAS system is the off-line development of alarm/event trees. The German/ Norwegian approach has improved tree flexibility.

The Electric Power Research Institute (EPRI) in the USA [15] have been developing another DAS methodology closely related to the European version. The emphasis on operator involvement and probabilistic information has been decreased. The data base structure has also been modified. The EPRI-DAS also requires the development of cause-consequence relationships.

Alarm analysis techniques are still in the development stage. Due to the large number of man-years of effort required to implement such systems, it would appear that only plants with a large number of high risk elements could justify the expenditure. Until further advances are made in the development of the fault trees which form the data base for all analysis systems, alarm analysis systems will be limited largely to the nuclear industry.

By the mid 1970's the difficulties with plant modelling for the purposes of fault detection on process plant were well recognised as described by Lees, Andow, and Murphy [16] in 1981. Much work has been performed to improve techniques for modelling plants on the basis of event or fault trees.

This would be useful for many reasons including safety, loss prevention, and optimisation which have become of greater importance. Work continued in the nuclear industry to improve alarm analysis techniques in general. Bastl and Felkel [17] in 1981 reviewed the current status of alarm analysis systems. Their review suggests that no real further significant developments have occurred.

✓ Performing highly detailed alarm analysis began to appear less attractive by some researchers who started investigating possible alternatives. Less exact approaches to alarm information reduction were considered which would supplement alarm analysis techniques. Operator loads were still high due to increasing amounts of process information available. Several safety related incidents injected greater emphasis on alarm information systems, however the subject was broadening probably due to the lack of significant improvements of alarm analysis systems. A range of operator support system which are essentially types of alarm systems were introduced. The majority of these systems rely heavily on improving the presentation of alarm information. These safety related operator support systems are intended to assist decision making during malfunction conditions as follows:

- 1) Safety Panels
- 2) Safety Consoles
- 3) Critical Function Monitoring

Safety panels as described by Long, et al [18] in 1980 are used to display around 20 selected safety function variable values and recent history trends of these variables in one location in the control room with no alarm generating capacity.

Safety consoles also described by Long are expanded versions of the safety panels with over a hundred safety related variables displayed. Displays which are computer driven are organized in a hierachial manner. Some alarm information is generated from key safety plant variables.

Safety panels and consoles have been proposed as additions to the EPRI-DAS system to form an improved disturbance analysis and surveillance system (DASS).

Critical function monitoring (CFM) systems (Corcoran, et al 1980 [19]; Visuri, et al 1981 [20]) incorporate alarm logic algorithms into the safety console concept to identify which safety function needs operator attention. These algorithms take into account the operating mode of the plant. The system is intended to condense critical safety parameter information onto operator displays with a capacity of about 200 plant variables.

As illustrated these highly abbreviated alarm information systems are used to assist operator decision making by providing generalised plant status information by means of generating and displaying select safety variable data in the form of condensed plant status and alarm information displays.

A further development of the CFM systems discussed by Visuri et al [21] in 1981 is called HALO or handling alarms with logic. ^{Handling} The main function of the alarm handling system is to extract relevant alarms out of the large amount of process signals and to present these alarms to the operators in such a way that provides a clear overview of the process status. There is much emphasis on efficient information presentation utilizing human capabilities in pattern recognition. A plant overview VDU display is used which

concentrates plant and alarm status information on to a single display. The system has a broader application than its CFM counterpart since both safety and non safety related plant variables are logically combined by programable algorithms which detect only the alarms that are exceptions to normal plant operation conditions. The system uses a generalised on-line computer based program for generating status information and driving the display VDU's which is programed off-line by data corresponding to a particular plant.

The chemical processing industry did not express the same keen interest in alarm system technology. In 1965 the Instrument Society of America (ISA) [22] published guidelines on the use of general purpose alarm annunciators describing various colour coding, backlighting and alarm acceptance schemes. Techniques for generating alarm information from plant data were not discussed. Recall that in 1966 alarm analysis and computer driven VDU's were already heavily used in the nuclear industry. The application of alarm analysis techniques to chemical processes was clearly not sufficiently cost effective especially since chemical plants do not require the same high level of process monitoring. ..

Some interest in alarm analysis was expressed by Barth and Maarleveld [23] in 1967. A computer based experimental project was described based on cause and effect models of the plant. The basis of this approach was to divide the plant into small sections and to deduce the likely effects of various faults originating from both inside and outside these sections. For each variable a list of checks was then obtained which were executed when the variable drifts off normal. The technique was apparently successful on small plants where the potentially enormous volume of required data storage space could be kept to a minimum.

With the growth in chemical plant size and complexity the application of alarm analysis to process control was explored by Andow [24] in 1973 and later by Andow and Lees [25] in 1975. The earlier work involved the application of list processing techniques to process functional models of plant equipment to deduce prime cause alarms. Later developments in 1975 introduced a modified truth table technique containing probabilities for deducing prime cause alarms from plant data. In both cases fault tree modelling was used to generate alarm structures. In 1980 Andow [26] further investigated the use of mini-computers to assist the operator in diagnosing basic faults from patterns of alarms also based upon list processing.

* (At about the same time in 1975 and 1976 the British Standards Institute [27,28] introduced process plant alarm annunciator guidelines similar to those published by the ISA in 1965. Clearly the emphasis on alarm systems in the chemical industry was not as advanced as the nuclear industry at this point.)

✓ In 1977 the Insurance Technical Bureau published a method for monitoring process plant based on decision table analysis. Berenblut and Whitehouse [29] and Munday [30] describe the technique called 'anticipator' which is primarily intended for reducing the loss on process plant. During transient conditions on the plant a recording is made of process variable data which is later analysed by a decision table technique performed by an on-line computer. The decision table is also used to detect the disturbance which starts the recording and to select the data, sampling rate and time interval to be recorded. The decision table is in the form of rules comprised of combinations of plant variables in normal and abnormal states. The system is primarily used during postmortem examinations of plant

malfunctions however it is reported to have real-time capabilities as well.

The application of operator support systems such as developed in the nuclear industry to chemical processing plants has not been significant. A greater emphasis on operator training appears to be an alternative to the operator support systems developed.

In both industries much more attention is now also being given generally to operator training which is aimed at maximizing the operators' diagnostic capabilities with available alarm and plant data. This is of particular interest in the chemical processing industry where this low cost technique can produce remarkably satisfactory results as demonstrated by Duncan and Gray [31] in 1975.

From this survey it has been noted that alarm system technology has developed principally in the nuclear industry and that advanced alarm systems have had very limited application in chemical processing plants.

CHAPTER 3

THE ROLE OF ALARMS AND ALARM SYSTEMS

This chapter discusses the fundamental concepts of alarms and alarm systems. A review of the existing alarm system philosophies and available systems are discussed in addition to some general difficulties with the design and implementation of alarm systems.

3.1 INTRODUCTION TO THE CONCEPTS OF ALARMS

A survey of the literature reveals that there is no common terminology for the fundamental elements of alarms and alarm systems. In this section some of the basic concepts will be defined in a manner which attempts to be consistent with terms used in the literature. However, due to the lack of a common terminology many of the concepts defined here may not exactly correspond with the use of terms in the literature.

Any process plant at any given moment can be described by a set of discrete state variables. Each set represents a different state or condition of the process. Referring to Figure 3.1, all of the sets of variables which describe an undesirable plant state or condition are called FAILURE MODE SETS. An ALARM is an indicator of the occurrence of a failure mode set.

Ideally, the plant's control system should be able to identify and handle all the possible system states that can exist during a process. However, the typical plant may have

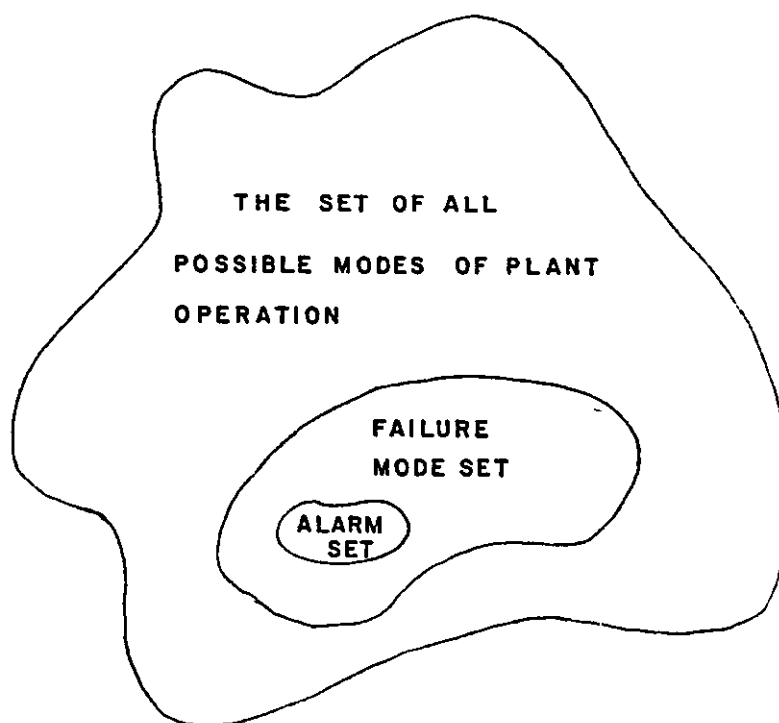


Figure 3.1 Set Model of Plant Operational Modes

a large number of state variables and sets of state variables. To illustrate, a small process computer, excluding the memory subsystem, can have 2^{100} to 2^{1000} different system states. The number of system states identifiable in an entire plant may soon become unmanageably high. An alternative approach is to identify selected key system variables and control these through the use of conventional control theory and techniques.

A major goal in developing a process control system is to design into the system the capability of identifying and handling as many system states as possible. The greater the number of identifiable modes of operation coupled with the ability to handle these modes, the greater becomes the ability to reduce the number of occurrences of failure mode sets.

The operator's task is therefore, to keep the plant operating with the fewest possible occurrences of failure mode sets. If an ideal control system were available then the need for human intervention would be virtually eliminated. The operator's presence is intended to improve the overall control system by increasing the number of modes of operation that can be identified and handled. To help the operator identify the undesirable modes of plant operation, alarms are used to draw the operator's attention to selected problem areas.

A more pragmatic description of a plant's overall control system is shown in Figure 3.2, where the operator is shown to supplement the control system. It is important to recognize that the operator forms part of the overall control scheme of the plant. The man-machine interfaces for information flow between the operator and plant and between the operator and control system form vital links in the overall plant control scheme. Alarms are one form of

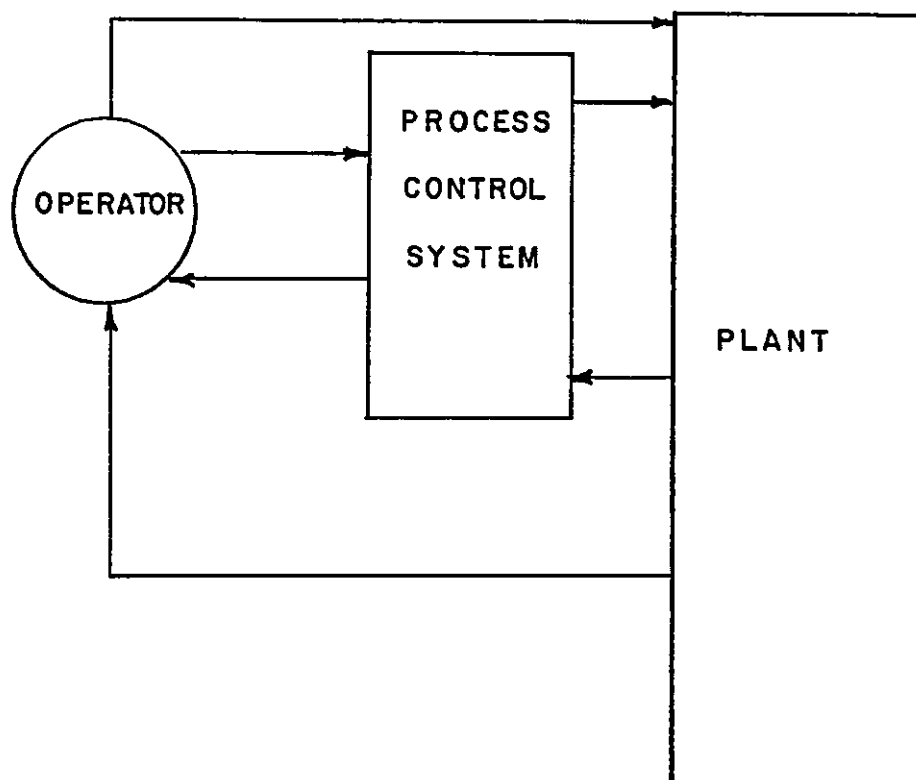


Figure 3.2 Information Flow in the Plant
Overall Control Scheme

operator interface in this information flow.

The purpose of alarms, as discussed here, is to provide the operator with information on the state of the process. There are three categories of information provided by alarms that assist the following operator tasks:

- 1) Detection of failure mode conditions by alerting the operator to an adverse condition.
- 2) Recognition of plant operational modes thereby assisting the operator in fault diagnosis.
- 3) Choice of operator action strategy to rectify the failure mode condition.

3.2 ALARM DEFINITIONS

It is necessary to begin an evaluation of alarms by describing some of their characteristics. Several basic aspects of alarms can be identified by inspection, and these are proposed below as tentative definitions. The first general alarm definitions relate to categories or groupings of alarms.

3.2.1 Alarm Categorisation By Plant Operational Mode

PRIME CAUSE ALARMS: When a failure mode condition occurs alarms are usually generated which correspond to various prespecified plant conditions. When an event occurs initiating plant alarms, the alarms presented to the operator indicate that the prespecified conditions for each individual alarm have been satisfied. As a result individual alarms may be symptoms of the occurrence of a

plant event while not specifying the initial fault. The alarms that represent the actual fault which caused the failure mode condition are called 'prime cause' alarms.

Consider the following example illustrated in Figure 3.3 where a pump is filling a storage tank. There is a level sensor on the tank, an inlet flow sensor, and a pump monitor. The following alarm conditions can occur and are specified:

<u>Alarm</u>	<u>Specified Plant Condition</u>
HI LEVEL	Tank Full
LO LEVEL	Tank Empty
NO FLOW	No Flow into Tank
PUMP STOPPED	Pump has Ceased to Operate (when it is assumed to be operating)

In the example, an alarm represents the condition of a stopped pump. If the pump has stopped due to a fault in the pump mechanism, the PUMP STOPPED alarm would be a prime cause alarm. If the PUMP STOPPED alarm has been caused by another fault the PUMP STOPPED alarm would not be a prime cause alarm. The concept will become clearer in a moment.

SECONDARY ALARMS: Secondary alarms are alarms which represent failure modes generated directly by the prime cause alarm. As in the example, the PUMP STOPPED alarm is assumed to be a prime cause alarm since there has been a pump failure. A Secondary alarm generated in the example would be NO FLOW. The NO FLOW alarm is a Secondary alarm to the PUMP STOPPED alarm since it is a direct effect of the pump failure.

TERTIARY ALARMS: Tertiary alarms are alarms which

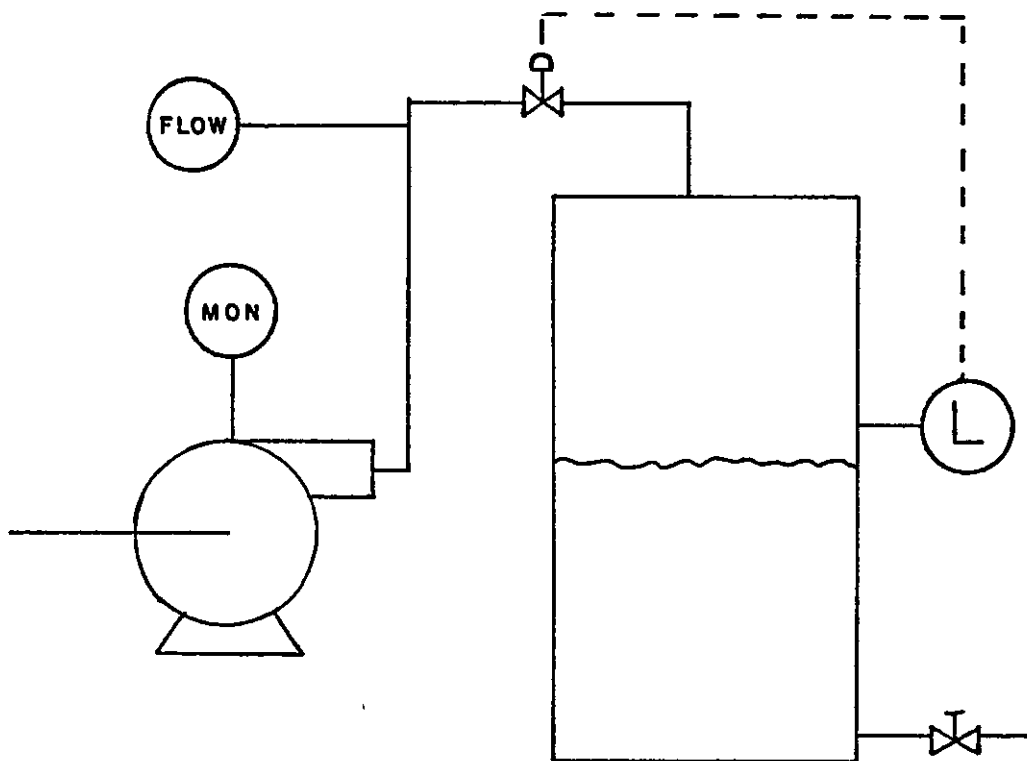


Figure 3.3 Storage Tank Example

represent failure modes generated by the prime cause alarm but not as an immediate result of the prime cause alarm. Referring to the example, a LO LEVEL alarm on the tank would be the the eventual effect of the PUMP STOPPED prime cause alarm.

The distinction between secondary and tertiary alarms may sometime be unclear. As a general rule the occurrence of prime cause alarms necessarily result in the occurrence of related secondary alarms. Tertiary alarms although possibly initiated by the prime cause alarms may not occur because of varying plant conditons. In the example, the LO LEVEL alarm is a tertiary alarm related to the prime cause alarm PUMP STOPPED. If the tank discharge valve is shut then the LO LEVEL alarm will not occur even though the PUMP STOPPED alarm has occurred.

HARD (Non-Recoverable) vs SOFT (Recoverable) ALARMS:

Hard and Soft alarms are general categories of alarms rererring to the recoverability of the normal operating mode of the plant. Hard alarms represent failure mode conditions which result in a non-recoverable system state. Soft alarms, on the other hand, represent recoverable failure mode states. The occurrence of a Hard alarm indicates the loss of plant equipment operation, loss of process material, shutdown of plant, or other non-recoverable occurrences. Hard or Soft alarms can be prime cause, secondary, or tertiary. Soft alarms can be easily rectified to bring the plant back into a normal operational mode.

Recoverability is of particular interest in batch or sequence processes where the failure mode condition dictates whether the process can be restarted and if so where in the process sequence of operations.

On continuous plants the operating mode may drift into a pre-trip state during which time the operator can rectify the situation and return the plant to within normal operating parameters. Alarms generated during the pre-trip plant conditions are soft alarms. Once a trip has occurred alarms then generated are often hard alarms.

HIGH and LOW PRIORITY ALARMS

Alarms can be categorised according to their relative importance with respect to the mode of plant operation. High priority alarms are defined as alarms which require immediate operator attention in order to avoid an undesirable or dangerous change in the mode of plant operation. Low priority alarms require operator attention however these represent plant conditions which have no immediate danger. The alarm priorities can be further grouped as follows:

- 1) Very Urgent - Require immediate attention or warning of a potential danger.
- 2) Urgent - Require immediate attention to avert undesirable change in operational mode.
- 3) Caution - Indicates change or pending change of plant conditions, operator attention is required.
- 4) Non Urgent - Indicates a change in plant operational conditions or a discrepancy from commanded plant operational mode, operator attention required.

Note that all alarm groups require operator attention. Often alarms are misused as status indicators resulting in a large number of standing alarms in the control room.

For example consider a plant in which a heavy polymer is being processed; a LO TEMP alarm would indicate that the process material may solidify. The LO TEMP alarm requires immediate attention to avoid loss of material, equipment, and possible shutdown. The alarm is therefore a high priority alarm. The LO TEMP alarm could also be considered a Soft alarm since by adding heat normal plant operation can be recovered. Alarms indicating pre-trip conditions are high priority alarms.

3.2.2 Alarm Categorisation by Type

The nature of the failure mode in a process plant is extremely diverse. In general, the most common failure mode conditions chosen for alarm representation can be categorised in one of the following groups:

- 1) Absolute
- 2) Deviation
- 3) Discrete State
- 4) Trend
- 5) Timeout Failures
- 6) Equipment Failures
- 7) Trip

8) Deduced

9) Informative and Other

1) Absolute - Alarms indicating that a measured parameter is above or below a preset value. Typical alarm messages include LEVEL HI, LEVEL LO, OVERFLOW.

2) Deviation - Alarms indicating that a measured parameter is outside a preset operating range. Typical alarm messages include INCORRECT TEMP, PRESS ERROR.

3) Discrete State - Alarms indicating that plant equipment is in the incorrect discrete operating state. Typical alarm messages include RUNNING, STOPPED, ROUTE INCORRECT, NO FLOW, OPEN, CLOSED, NO AIR AVAILABLE.

4) Trend - Alarms indicating that a measured parameter is changing too fast, too slowly, sporadically, or not at all. Typical alarm messages include TEMP CHANGE TOO LARGE, NO CHANGE.

5) Timeout Failures - Alarms indicating an event should have occurred within a prespecified time interval from when the event was commanded. Typical alarm messages include FAILED TO START/STOP/OPEN/CLOSE/EMPTY, FAILED RESTART.

6) Equipment Failure - Alarms indicating faulty plant equipment or failure to meet required operating specifications. Typical alarm messages include FAULT, FAILED PRESS CHECK.

7) Trip - Alarms indicating that the protective trip system for a plant equipment has been activated. Typical alarm messages include PUMP OVERLOAD TRIP, OVERTEMP CUTOUT.

8) Deduced - Alarms indicating the logical deduction of a prime cause or other alarm by means of an alarm analysis system. Typical alarm messages include any messages presented here with the addition of a prompt signifying a Deduced alarm: *, -, etc.

9) Informative and Other - Alarms indicating improper operator action, reminders, or other system conditions of interest to the operator. Typical alarm messages include ROUTE NOT AVAILABLE, BATCH REJECTED, END OF CYCLE.

3.2.3 Alarm Categorisation by Causative Classification

Most failure mode conditions are generated by one of the following events:

- 1) Sensor or Transducer Failure
- 2) Control Component Failure
- 3) Activated Device Failure
- 4) Operator Error

The causative classification of alarms is of great importance in alarm generation and display systems. Each class represents a location of a failure mode source in the overall plant control scheme. By classifying alarms in this manner the operator is given a valuable clue regarding the location and the nature of the failure mode source.

Sensors and transducers convert physical plant parameters into an electrical, pneumatic, or mechanical

signal. Sensors and their associated equipment can fail high, low, or maintain a constant value. These conditions are typically used to generate sensor or transducer failure alarms.

The control components in the loop receive parameter information from the sensors and manipulate this information according to specified control algorithms. The output of the control components is normally sent to an activated device through a manual/automatic selection device. Conditions which generate control component alarms can be used for example to instruct the operator to bypass the control components by switching to manual control.

Activated devices include all plant equipment excluding the instrument and control facilities. Alarms generated by failures of these components are classed as activated device failures. The majority of failure mode conditions are in this category.

As reported by Kortlandt and Kragt [3] a large number of alarms are often generated by operator intervention on the plant. Although alarms initiated in this manner are called operator error alarms in many cases it has been noted that operators use alarms as a feedback mechanism to assist in their control task.

3.3 THE ROLE OF THE ALARM SYSTEM

It is the function of the process control system to prevent if possible the development of failure mode conditions by detecting their occurrence and subsequently adjusting process parameters to rectify the situation. The responsibility for averting other failure mode conditions which the control system cannot accomodate falls largely to

the operator. The principal aid to assist him is the alarm system. The alarm system is therefore an extremely important component of the overall plant control scheme.

3.3.1 The Alarm System Function

An alarm system is a normal feature of conventional control systems. The plant alarm system is an operator support aid which has the purpose of assisting the operator to:

- 1) Detect plant failure modes.
- 2) Diagnose the faults.
- 3) Select an appropriate action strategy to rectify the fault.

The function of an alarm system as an operator aid suggests that the system must be capable of:

- 1) Accurately identifying the occurrence of failure mode conditions on the plant and generating the appropriate alarm information.
- 2) Displaying the alarm information to the operator in such a manner as to maximize the efficiency of the man-machine interface between the alarm system and the operator.

The alarm system therefore has two main functions:

- 1) Alarm information generation.
- 2) Alarm information display.

The greater the efficiency of these functions the

greater is the likelihood that the operator will be able to adequately perform his control tasks. To illustrate this point recent studies on the effect that alarm system efficiency can have on operator response times to failure mode conditions have been performed by the Electric Power Research Institute [32]. Referring to Figure 3.4 a reduction of the operator response times for the detection, diagnosis, and correction of abnormal plant conditions were shown to significantly reduce plant down time. In the study the alarm system was used to assist the operator generally but in particular the detection and recognition of pre-trip plant conditions were a major factor in down time reduction.

3.3.2 The Operator

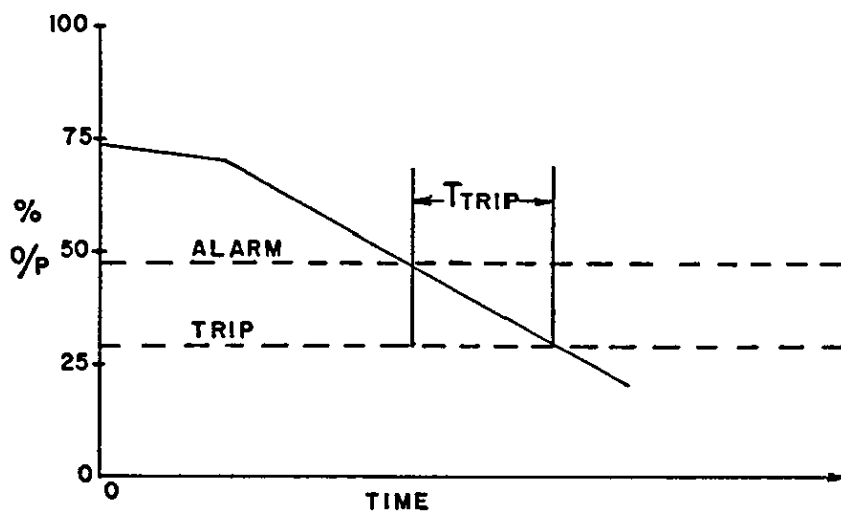
Unfortunately much of the understanding we have of how the operator perceives and executes his control task is anecdotal, and only a limited amount of work has been published on studies of alarm systems and of operator plant fault diagnosis.

The interface between the operator and the plant with its control system is vital. An efficient operator interface is necessary to make the operator an efficient part of the control system. There are however, several problems involved in designing an optimum interface.

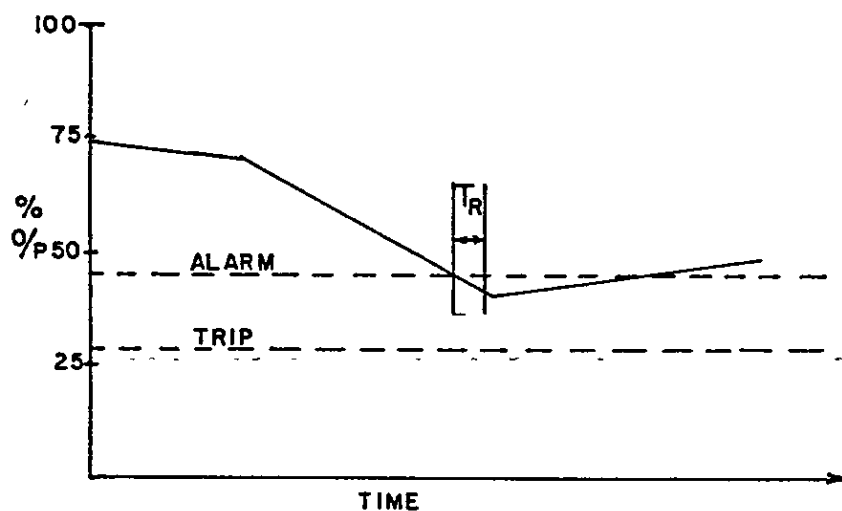
- 1) There is a lack of a clear understanding of a methodology for interfacing with an operator. Much work has been done in the field, but this has produced few meaningful results.

- 2) There is no unified approach to model the tasks required of the operator in a control room situation.

- 3) Finally, a model of the operator himself has not



WITHOUT OPERATOR RESPONSE



WITH OPERATOR RESPONSE

Figure 3.4 Operator Responses to Fault Conditions

been developed which is usable in complex control room situations.

A survey of the literature shows that although limited progress has been made in the operator modelling, there has been some work performed which evaluates the role of the operator in the control system. Edwards and Lees [33,34] have discussed the subject of man-machine interactions. Lees also has surveyed and reviewed the field in depth [35]. A discussion of the human factors involved in the control loop will not be undertaken here.

Kortlandt and Kragt [4] examined several process control systems which incorporated alarm systems. They showed that an improvement in the general alarm system philosophy was needed. They recommended two major additions:

- 1) The use of 'dead bands' around alarm levels.
- 2) The need for detection of operator initiated alarms and of groups of alarms.

The use of 'dead bands' or hysteresis around alarm limits prevents alarms from oscillating on and off when the measured variable is near the alarm limit. When alarms oscillate each new annunciation requires the operator's attention for acceptance. Oscillating alarms also clutter alarm logs.

Group detection of alarms and alarm sequences is not a new idea. Detection of alarm groups has been used in the nuclear industry. By identifying alarm clusters that occur with given faults, other relevant alarms not associated with the cluster have less chance of being missed by the operator. Kortlandt and Kragt found that many alarms are

generated by the operator's corrective actions that were taken in response to some previous alarm. They suggest that identification of operator initiated alarms can help the operator to better understand what effect his corrective action is having on the process.

The technology gap between available alarm handling systems and full alarm analysis systems is large. The major controls manufactures usually do not provide alarm facilities capable of dealing with alarm grouping, sequences or 'dead bands'.

3.4 Types of Available Alarm Systems

Alarm systems vary considerably in sophistication. A guideline for a design methodology of alarm system functions is outlined below. The list is ordered with respect to the sophistication of the alarm system, starting with the requirements of a basic traditional alarm system. It must be able to:

- 1) Handle Alarm Display and Annunciator Devices
 - a) Hooters
 - b) Alarm Fascia Panels
 - c) Mimic Diagrams and Displays
 - d) VDU Displays
- 2) Handle Alarm Register and Acceptance Routines.
- 3) Record Alarm/Event Time Information - Alarm loggers provide a time ordered record of alarms and events.
- 4) Perform group alarm identification.
- 5) Identify alarm or event sequences.

- 6) Identify operator initiated alarms.
- 7) Deduce faults from alarms and events.
- 8) Identify pre-failure mode operation.
- 9) Provide operator with instructions.
- 10) Ideally, initiate corrective action.

Alarm system structures can be classified as follows:

- 1) Basic Alarm Systems - Alarm systems composed entirely of passive alarm annunciators as found in the conventional control room.
- 2) Alarm Handling Systems - Alarm systems based on intelligent control or monitoring systems but only generating alarm condition or event information.
- 3) Alarm Analysis Systems - Alarm systems based on intelligent control or monitoring systems that provide complex alarm and event detection with appropriate operator action messages. The systems are usually based on fault tree or similar data base structures.

The level of sophistication of an alarm system structure lies somewhere in the classifications suggested in Figure 3.5. The simplest form of alarm system is the alarm annunciator or facia panel. These types of systems are commonly [3] referred to as conventional alarm systems. Conventional alarm systems are passive in nature and rarely provide the operator with more than an indication of the excursion of a measured parameter across an alarm limit. The sophistication of the alarm system increases moving to

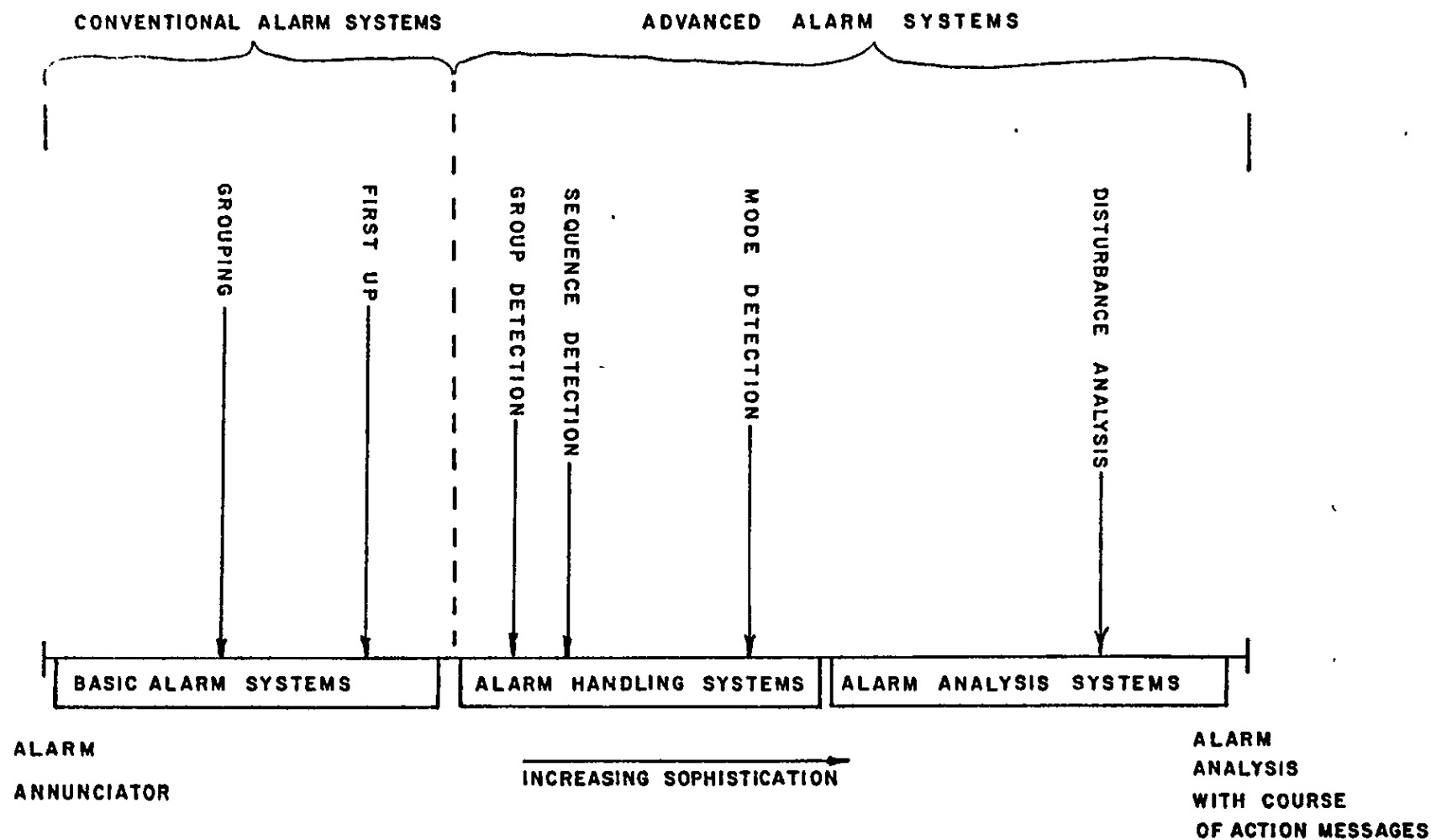


Figure 3.5 Degrees of System Sophistication

the right along the chart. The use of a process computer in the alarm system marks the transition into advanced alarm systems.

3.4.1 General Purpose Systems

Most conventional and some advanced alarms systems have general purpose application on the process plant. The systems are based on off-the-shelf modules connected as appropriate for a specific application. A description of the general purpose systems follows.

3.4.1.1 Alarm Annunciators

The simplest alarm system is the traditional alarm annunciator panel which consists of hardwired fixed alarm indicators. An alarm is displayed by the illumination of an indicator on which is engraved the alarm message text. When an alarm occurs the annunciator flashes and an audible annunciator sounds. The operator acknowledges the alarm at which time the audible annunciator is silenced and the illuminated indicator remains on steady until the alarm conditions disappear. Each alarm has a one-to-one correspondence with a measured variable, and has alarm limits which are absolute and fixed. Some annunciators have additional features such as first up and grouping. These features permit the detection of the first alarm to occur during a sequence of alarms or the detection of a preselected group of alarms.

Kortlandt and Kragt [3] reported that control room alarm annunciator panel configurations follow one of the two examples presented below:

Example 1. Alarm facia panels are located throughout the control room with one centralised audible signal. The

operator must scan the alarm panels after hearing the audible signal. During the scan the operator has to detect the visual alarm display. Kortlandt and Kragt found that often the operator failed to detect the alarm or simply overlooked it during the first scan. The extra time required to locate the alarm proved very stressful in alarm conditions. Also during alarm modes many alarms may arise, thus it is difficult to detect all of the newly arrived alarms.

Example 2. Control rooms may use a hierarchial alarm facia panel format. A central facia panel shows the number of the panel on which an alarm occurred. Local facia panels display the alarm message.

The severity of a particular alarm is often signified by the colour of the indicator. Although there are several guidelines on this point [22,27,28], a three tier colour scheme is often implemented. As an example, many Central Electricity Generating Board (CEGB) control rooms use the following colour code:

- 1) RED - Very Serious; requies immediate attention and correction.
- 2) YELLOW - Alarm condition requiring attention.
- 3) WHITE - Minor alarms and status indicators.

Kortlandt and Kragt also suggest that there are many unanswered questions relating to the design and use of the conventional alarm annunciator panel. There are many engineering and ergonomic factors that must be considered. This is an area for much work.

Andow and Lees [2] point out several disadvantages with

the alarm facia panel:

- 1) The system is dictated by the limitations of the hardware used.
- 2) It is inflexible.
- 3) Alarm types are restricted to absolute alarms unless the display is driven by the process computer.
- 4) There is a lack of distinction between statuses and alarms.
- 5) The information content is restricted.
- 6) There is an inability to recognize alarms that are associated with non-failure operating modes such as startup, etc.

The use of alarm annunciator panels varies significantly from the conventional control room to the advanced process control room. In conventional use alarm panels are driven directly by process parameters. Each panel alarm is individually monitoring a process variable. The alarm panel will have been constructed to look for a contact closure, rate of change, deviation, etc. In the advanced control room the alarm annunciator panels are often driven directly by the process computer as well as by the process variables.

In general, annunciators have limited flexibility, principally due to the fact that these units are hardwired thereby providing no facilities for remote selection of alarm limits or conditions.

3.4.1.2 Computer Control System Based

At a higher level of sophistication is the process computer-based alarm system which is more flexible than its hardwired counterpart and can more effectively handle alarm groupings, etc. This type of alarm system can be interfaced to a VDU, line printer, or annunciator panel thus providing greater flexibility in the methods of information display to the operator. Alarm information is obtained from the control language program in the process computer. Although computer-based alarm systems have great potential for generating and manipulating alarm information, they usually emulate traditional hardwired alarm systems and are therefore limited to handling absolute alarms. Typically alarm displays consist of alarm message text which appears on dedicated VDU's in chronological list form. The alarm lists are organised into pages which can be selected by the operator. More recently, (Jervis [36]) alarm information has been made accessible through a hierarchial format which gives higher quality alarm and process data information as more detailed levels of the information display structure are requested.

The major process control equipment manufacturers all implement similar approaches to the alarm system design. The trend in the packaged process control systems is towards management by exception. The philosophy of management by exception is that if a particular process parameter is performing normally, the parameter need not be displayed to the operator on the operator's VDU displays. However, management by exception necessitates the need for an alarm system which alerts the operator to off-normal conditions within the plant. There are no standard techniques for presenting these alarms, each manufacturer has developed their own which is usually some form of hierarchial alarm annunciation structure. See Figure 3.6.

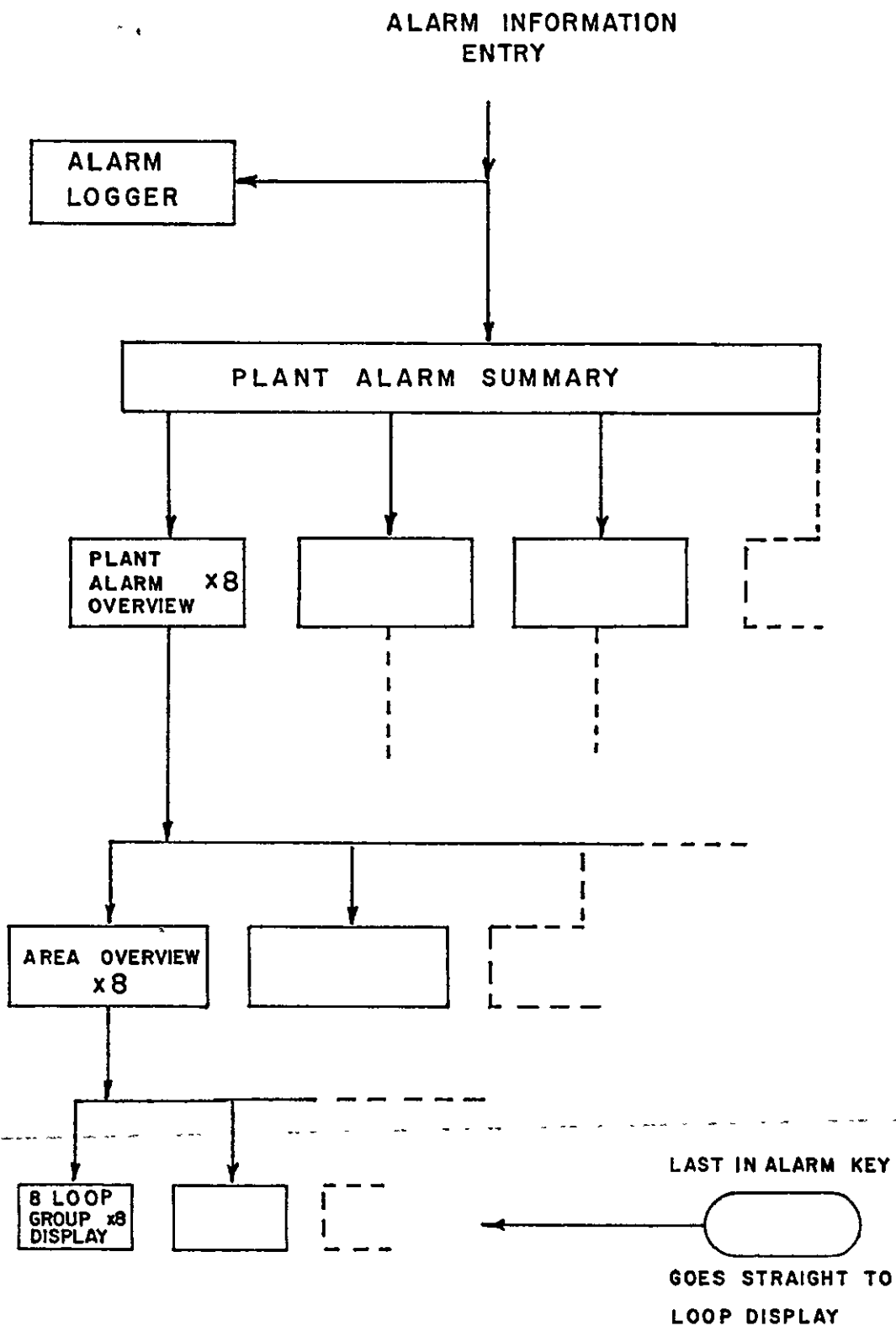


Figure 3.6 Typical Hierarchy of Commercial Alarm Display Systems

3.4.1.3 Computer Language Based

There are several process control languages available such as PCP (Plant Control Package from Software Sciences Ltd) and CASCADE (from SPL International). These software packages are intended to run on standard computer equipment thus permitting the user to custom build a process control computer system as required. The alarm features in these packages are similar to those found in the closely related computer control system based alarm systems.

3.4.2 Application Specific Alarm Systems

Special circumstances have encouraged the development of more exacting techniques for dealing with alarms. These systems are often difficult to implement and usually require custom designing.

3.4.2.1 Alarm Handling

The category of alarm handling systems has not been extensively developed for process plant applications as shown in Chapter 2. The major process control equipment manufacturers generally do not implement alarm handling features. In the nuclear industry Visuri et al [21] report the use of an alarm handling system to extract relevant alarms out of a large number of process signals and to present these alarms to the operators, however this system emphasizes information presentation.

3.4.2.2 Alarm Analysis

Automatic fault diagnosis, usually referred to as alarm analysis or disturbance analysis, represents the most sophisticated form of alarm system. These dedicated on-line computer-based techniques have been implemented in the

nuclear industry for a number of years with limited success (Welbourne [9]). As described by Bastl and Felkel [17] and Andow [13] the purpose of an alarm analysis or disturbance analysis system is to reduce the occurrences of undesirable plant conditions by improving the operator's response time and success rate in correctly diagnosing fault conditions and taking appropriate corrective actions. The system aids the operator in his control task by examining conditions on the plant along with plant alarms and determines which alarms are prime cause alarms with the aid of detailed plant models. On most systems the irrelevant alarms are suppressed thus reducing the quantity of information presented to the operator and thereby enhancing the quality of the alarm information presented (Visuri et al [20]). Failure prediction or anticipation functions and proposed operator action strategy messages are additional features found in some disturbance analysis systems. A major difficulty with these systems is the effort required to create the complex plant models and to determine how they should be implemented in the computer (Andow [13]). Furthermore, the integration of both the computer diagnostic functions and the operator's diagnostic tasks has proved to be a difficult human factor problem. For example, the operator's dependence on the accuracy of the computer diagnosis readily damages the credibility of the system whenever an incorrect diagnosis or action strategy is generated. For these reasons the method is generally regarded as being too complex and costly for chemical plant application.

3.5 ALARM CRT DISPLAYS

Cathode Ray Tube (CRT) displays have become the recent trend in operator display devices due to the increased use of computer control systems. A CRT display, also called a

Visual Display Unit (VDU), is basically a television screen. The screen is driven by the central computer. Many different types are available. There are four basic categories of CRT displays; colour and monochrome; graphic and non-graphic.

Human factors people have been interested in the various aspects of using CRT displays for many years. Concern has been expressed in developing display criteria to limit the strain on the operator. As with the other areas of alarms, it has been found that there is a lack of any suitable system of classifying and identifying operator tasks involved in the use of VDU's [37]. Again, not until a further understanding of the operator is established will it be possible to obtain the greatest efficiency from CRT displays. Umbers [38] has reviewed the subject of CRT displays and has outlined many of the parameters which should be considered when using CRT displays.

The CRT display can be used for the display of many forms of information making the device versatile. CRT's are used for the display of alphanumeric information such as alarm tables, process data, and control messages. More advanced graphic units also have the capability of displaying graphical figures such as mimic diagrams. Mimic diagrams are easily updated or changed on such a display since the display is driven by the control computer.

Recent trends in control equipment have shown an increase in the use of VDU displays as the primary operator interface. Jervis and Pope [39] point out the problem of 'keyholing' that can occur with some displays. The effect occurs when parallel information flowing from the plant to the operator is concentrated into a serial form as in the case of the VDU/CRT display.

Keyholing displays require that the operator search through the serial information format of such a display for the required information. See Figure 3.7. The scale of the plant or the amount of information to be displayed on a single display unit are indications of whether or not the keyholing effect will degrade the operators' performance.

Jervis and Pope continue by saying that there is a very distinct need for the balance between parallel and serial displays to be carefully examined. Although there is no methodology for determining the balance point, the greater the number of potential messages, the greater the risk of keyholing.

Visuri et al [20] incorporate a high information density alarm and plant status CRT display which uses colour shading changes to indicate changes in the operational state of the plant. These enhanced mimic displays have proven to be useful in the nuclear industry, although only limited experience has so far been gained.

3.6 ALARM INFORMATION

Designers of control rooms for complex process plants commonly express the intent to present all relevant plant information to the operator. As a result, the quantity of information becomes so great that the operator is overcome by the sheer volume. Thus one criterion in information display is to minimize the presentation of information, while another is to insure that enough information is displayed to the operator for accurate evaluation of plant situations.

With the increased efforts to introduce computer-based control systems with CRT displays, many of the information display problems are eased. However, the selection of the

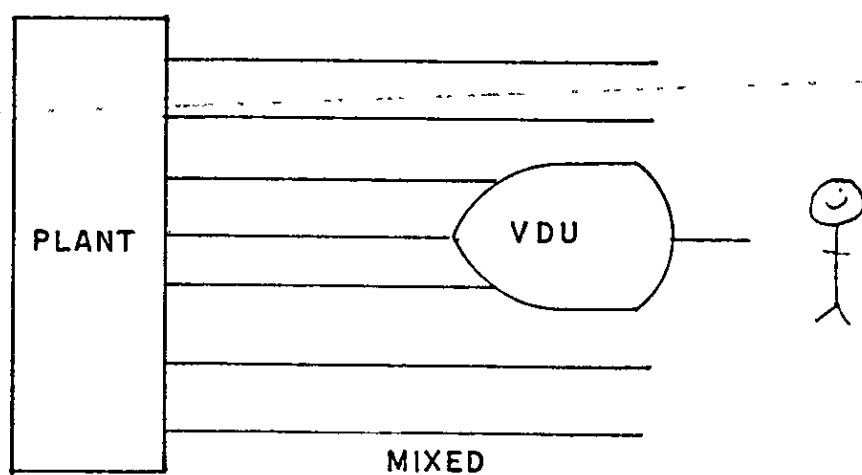
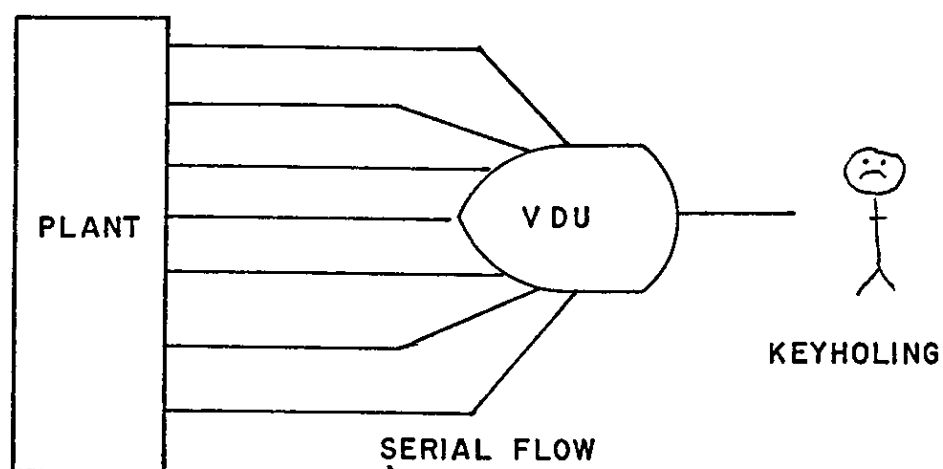
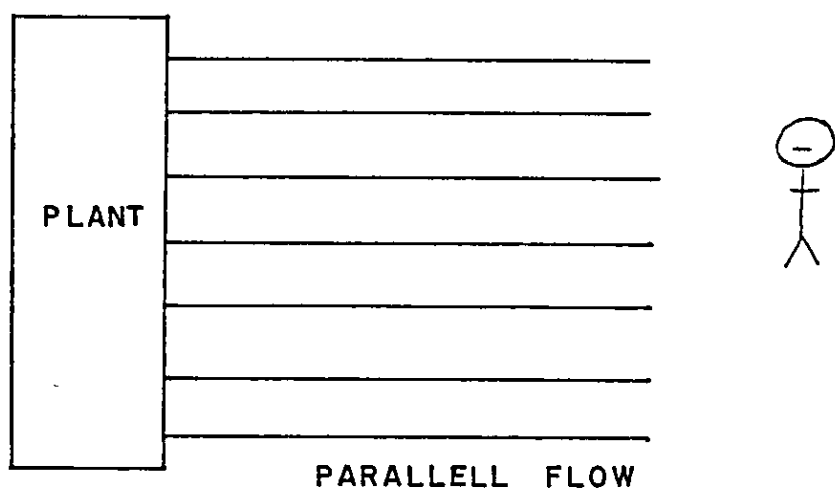


Figure 3.7 Keyholing

information to be displayed and the manner in which it is displayed has been another field of interest. This problem is especially important when displaying alarm information. The operator must be able to efficiently assimilate the alarm information as quickly as possible to aid in the operator's decision of action to be taken.

Information theory [40] has been used to select the relevant data to be displayed to the operator's CRT to maximize the operator's ability to deal with a particular plant condition.

Further work has been carried out to establish how this information should be displayed [41]. Preliminary results with CRT type displays indicate that the order of printed information to be displayed is important. In the case of alarm displays, the recommended order of appearance should be:

- 1) The variable English language descriptor,
- 2) Current point value/state,
- 3) Violated setpoint limit,
- 4) Alarm severity indicator,
- 5) Priority.

Items such as Time Occurrence, Point Identification Number, and Sequence Number seem to be of limited use to the operator. The Date of Occurrence information was found not to be useful.

3.7 SELECTION OF ALARMS AND ALARM PARAMETERS

There is no set procedure or methodology in the selection of alarms to be presented to the process operator. The decisions concerning where and when alarms are needed has traditionally been a best-guess approach by the designer. It is safe to say that most alarm systems are an afterthought as a result only alarm information sources readily available in the control system are used. An alarm system is often a collection of subsystems specified by designers of particular equipment on the plant, with the addition of some further alarms. Normally alarm selection follows from the following sources that are inherent in the control system:

- 1) Process equipment manufacturer warranty requirements. Equipment installation specifications often require that certain designated alarms must be displayed for the protection of the equipment. Process equipment will also have trips which are used as alarm sources.
- 2) Controllers and other control equipment which often have HI/LO and ZERO/FULL SCALE alarm mechanisms.
- 3) Process contact closures that are inherently required for process control.
- 4) Alarm information generated by DDC algorithms.
- 5) Alarm conditions stipulated for safety, loss prevention, or other reasons.

The format of the plant control system dictates to a large extent the process alarm information sources available.

The determination of alarm information sources is also generated by hazard analysis and operability studies. Lawley [42] has demonstrated a systematic procedure for identifying risk situations and elimination of the risk situations in the design stage. The methods, now widely used, also leads to the identification of modes of operation requiring operator attention, sometimes via alarms. The studies often identify parameters which are not normally accessible through the control system but which should be measured for alarm purposes.

Generation of fault trees for alarm analysis systems can also suggest which additional alarm information sources should be added in order to improve the alarm system

Lastly, when in operation it may be found from operating experience that particular alarms are required. This method of determination by default highlights the need for a systematic approach to alarm selection and systems design.

The total set of failure modes on a plant will be represented by preselected alarm conditons. These alarms will fall into one of the following classes:

- 1) Alarms which require very fast operator response time. These are usually implemented as trips.
- 2) Alarms useful to the operator.
- 3) Alarms too remote or expensive to worry about.

The trip alarms are alarms that are generated very quickly and require quick action by the operator. When the required operator response time becomes too short,

displaying the alarms no longer becomes useful. In these situations a trip device is used. This also applies to critical alarms in which case the risk that the operator may not react quickly enough or properly necessitates a trip. In intelligent or advanced control system, deduced alarms are rarely used for trips [32].

Many alarm conditions occur too rarely to justify the expense of detecting the alarm conditions. Some typical alarm conditions that fall into this category include damage caused by remote events such as military action, plane crashes, etc. Even the detection of certain alarm conditions may be very costly. If the cost of detecting a failure mode is greater than the loss incurred by the lack of detection of the condition, the alarm is not worthwhile.

The remainder of the alarms are alarms that are useful to the operator. These alarms are the ones that the alarm system must deal with.

3.8 THE NEED FOR AN ALARM HANDLING SYSTEM

The preceding review indicates that existing methods of dealing with alarms are either too complicated or inadequate. It would appear that an alarm system is required which is better able to satisfy the operators' information requirements than existing process computer systems, and at the same time is more-cost effective than the sophisticated alarm analysis and disturbance analysis systems.

As a result of the foregoing analysis it would appear that alarm system design philosophies are not satisfactory. Traditional alarm systems experience inflexibility due to hardware restrictions. The process computer based systems

which have great potential for improved alarm systems also appear to be inadequate. There are many aspects of alarms and alarm systems which require further attention.

Existing methods for dealing with alarms on process plants are often either too complicated or inadequate. It would appear that an alarm system is required which is better able to satisfy the operator's information requirements than existing process computer systems, and at the same time is more cost effective than the sophisticated alarm analysis and disturbance analysis systems. There is a need for an alarm system which exploits the capabilities of computer based alarm systems and therefore necessarily contribute to alarm system technology.

CHAPTER 4

SOME IDENTIFIABLE ALARM DETECTION FUNCTIONS

4.1 INTRODUCTION

It was decided that a study by performed of various types of process plant to evaluate the alarm requirements which could be encountered on process plant in general. Three generic plant types were chosen.

- 1) Batch
- 2) Continuous
- 3) High Reliability/ Fault Tolerant

The aim of the study was to see if there were any consistent methods used in the implementation of alarms systems and to establish alarm functions which would be useful in a generalised alarm system.

All three plants were designed independently thus providing a range of design and alarm philosophies. The study did not initially prove successful since it was noted that the combination of varying design and application of alarms to the plants did not yield consistent alarm requirements or philosophies. This was true even when portions of the different plants had similar operations.

The study became an evaluation of alarm requirements. The conclusions were as follows:

1) There appears to be no consistent methodology for assigning alarms or alarm levels. This is supported by findings in the literature [4] [13].

2) Alarms were usually placed where and when the designer felt them to be necessary probably with general guidelines as dictated by company policy or institute recommendations.

3) The form of the alarm detection and displays depended largely on the philosophy chosen in the control system and control room design. If the plant was computer controlled, then alarm displays were usually computer driven and alarm detection would be incorporated in the process control computer.

All plant types required some form of basic alarm detection. Each generic type required additional features to deal with special plant characteristics.

It was found that the majority of process plant alarms could be categorised as basic alarms. The relatively few situations where advanced alarm detection techniques were required suggested that a general purpose alarm system should be principally designed for basic alarm types while having the capacity to deal with a limited amount of advanced alarm detection.

----- This is a significant finding since it has a profound effect on the approach to general purpose alarm system philosophy. In particular the data storage and processing structures in a computer based alarm system which are efficient for basic alarm detection and limited advanced alarm detection are not necessarily practical for systems requiring a large amount of advanced alarm detection facilities.

Presented in this chapter is an analysis of some of the identifiable alarm detection functions which should be available in a comprehensive alarm system.

The function of an alarm system is to aid the operator in the detection of abnormal plant conditions, in the diagnosis of the fault, and in the selection of an action strategy to rectify the situation. The ability of an alarm system to fulfil these functions is dependent upon the features available in the system. An important attribute of any comprehensive alarm system is the ability to detect a wide variety of abnormal plant conditions. Without adequate provisions for detecting plant conditions, the alarm system may not be able to contribute accurate or sufficient information to aid the operator. Alarm detection includes the ability to collect the required plant data and to evaluate the data to determine whether an alarm condition is present. The method by which the alarm information is presented to the operator is also important. Interpretation of alarm information by the operator is a key factor in the overall performance of any alarm system. The methods of alarm detection and alarm information display are dependent on each other and therefore some account of the method of alarm information display must be taken when considering the methods used for generating the alarm information. A critical feature of a comprehensive alarm system is to have the ability to detect a wide variety of plant conditions in such a manner as to complement a wide variety of display methods. Presented in this section is an analysis of the types of alarm condition detection which would be useful in a comprehensive alarm system. The analysis covers detection functions identified from studies of existing alarm systems, intuition, and from analyses of the alarm requirements of various types of process plant.

4.2 BASIC ALARM DETECTION

As discussed in previous sections, there are a number of commonly recognized types of alarms which can represent some well defined plant failure conditions. These basic types of alarms can represent failure conditions in many process plants and provide a useful basis for alarm detection. Alarm detection is the process by which an alarm system monitors and detects the occurrence of a failure mode condition.

- 1) Absolute
- 2) Deviation
- 3) Band alarms
- 4) Binary (ON/OFF)

4.2.1 Absolute Alarms

Absolute alarms are the simplest type of alarm detection and are the most commonly used alarm in the process industry. They are easy to implement. As measured variables (MV) cross a predefined alarm limit the alarm is activated. The alarm condition is no longer present after the measured variable again crosses the alarm limit. See Figure 4.1.

4.2.2 Deviation Alarms

Deviation alarms provide a similar function. However the alarm condition is determined by the deviation of a process variable from a preselected value. Referring to Figure 4.2, the measured process variable is considered to

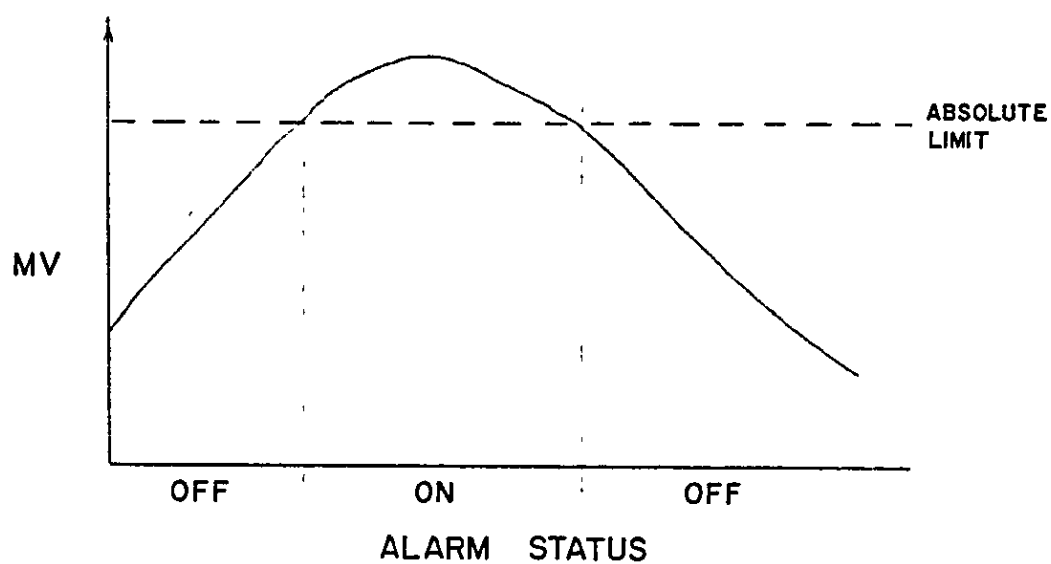


Figure 4.1 Absolute Alarm

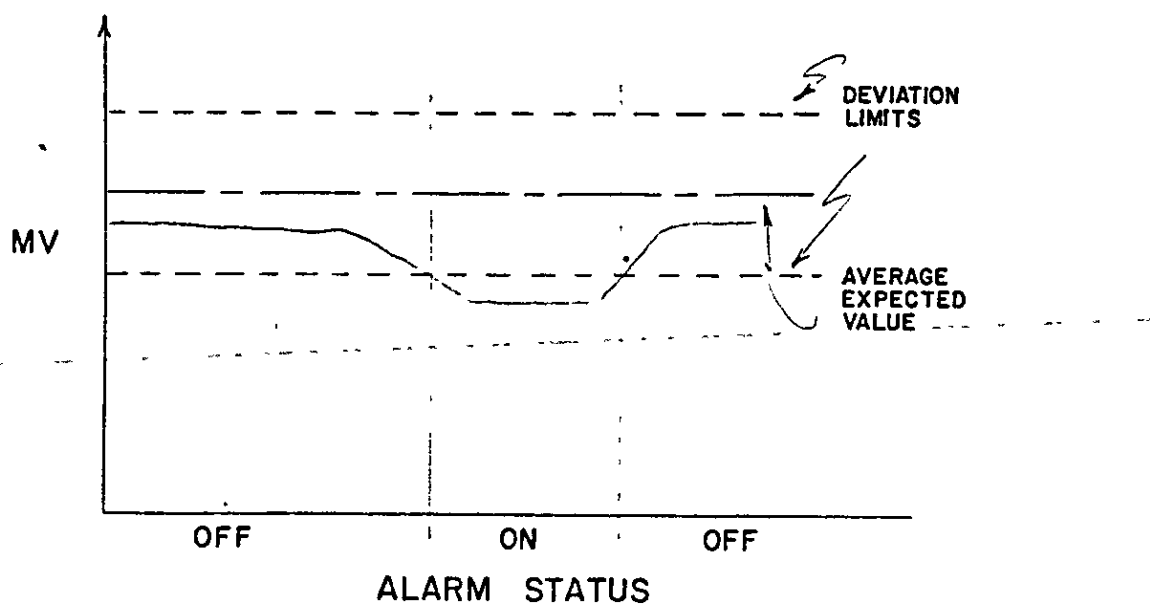


Figure 4.2 Deviation Alarm

be within normal operating limits when located between the upper and lower deviation limits. Alarm conditions are detected whenever the variable makes an excursion outside the alarm band.

Examples of both absolute and deviation alarms are common place and can be found in a wide range of process control products.

4.2.3 Band Alarms

In certain circumstances it is desirable to detect the existence of an alarm condition over a select section or band of a variable's operating range. A typical usage of alarm bands is in temperature alarms. As the temperature increases for example, the measured temperature will first initiate a HI temperature alarm. If the temperature continues to increase a second alarm limit may be crossed and thus initiating an XHI temperature alarm. It would be desirable to emphasis this change in status by removing the HI temperature alarm since the measured variable is actually beyond the band specified for HI temperature. The alarm band feature is similar to the deviation alarm except in reverse. Deviation alarms remain inactive while in the deviation alarm band limits, while band alarms are active while in the band limits. See Figure 4.3.

4.2.4 Binary (ON/OFF)

Many plant conditions are detected by switch contact closures. Binary or ON/OFF alarms utilize this discrete state as data for alarm generation.

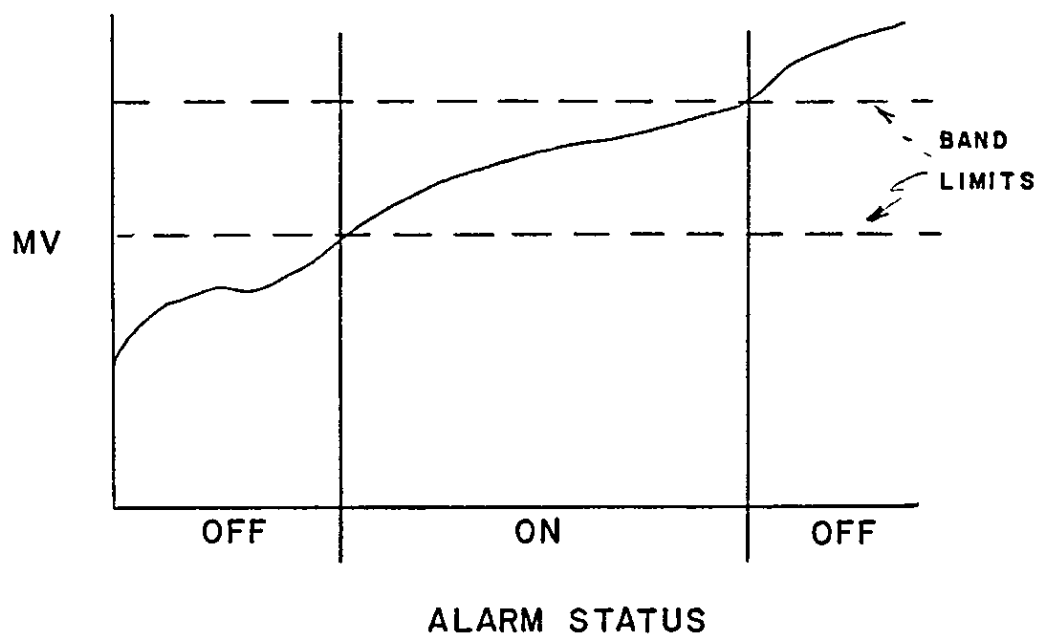


Figure 4.3 Band Alarm

4.3 ENHANCING BASIC ALARM DETECTION

Most alarm systems are capable of dealing with the basic types of alarm detection. Discussed in this section are two enhancement techniques which are not always included in existing alarm systems.

4.3.1 Derived Alarms

Often process data cannot be directly obtained from plant sensors. There are a number of reasons for this. For example the data may not be measurable. There may not be a suitable sensor or the location where a sensor should be positioned is inaccessible. In these situations the process data may be derived by calculating the variable using data from other plant sensors. Alarm limit conditions are then placed on the derived process data.

For example it is possible to calculate gas flame temperature in burners by measuring the flow rates of the combustion agents. The calculated flame temperature can then be assigned alarm limits.

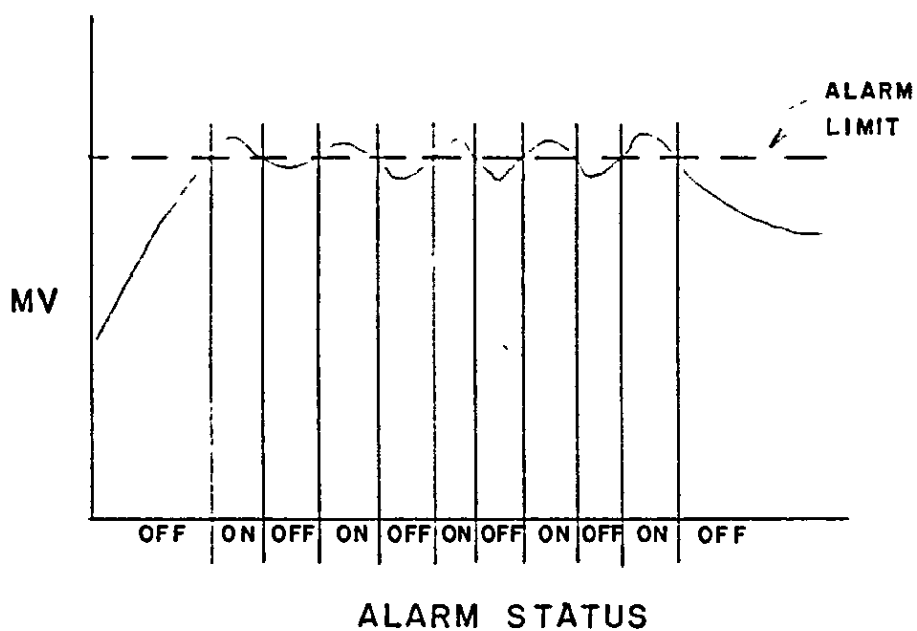
An alarm system capable of dealing with derived alarms must have the facilities to combine process data according to predefined mathematical formulae. If the relationship is simple the calculation may be performed by electronic hardware. For example some flow meters calculate the measured value from two pressure readings across an orifice. Complex relationships however require the processing power of computer based systems. In this case algorithms describing the calculations are programmed into the computer.

4.3.2 Hysteresis

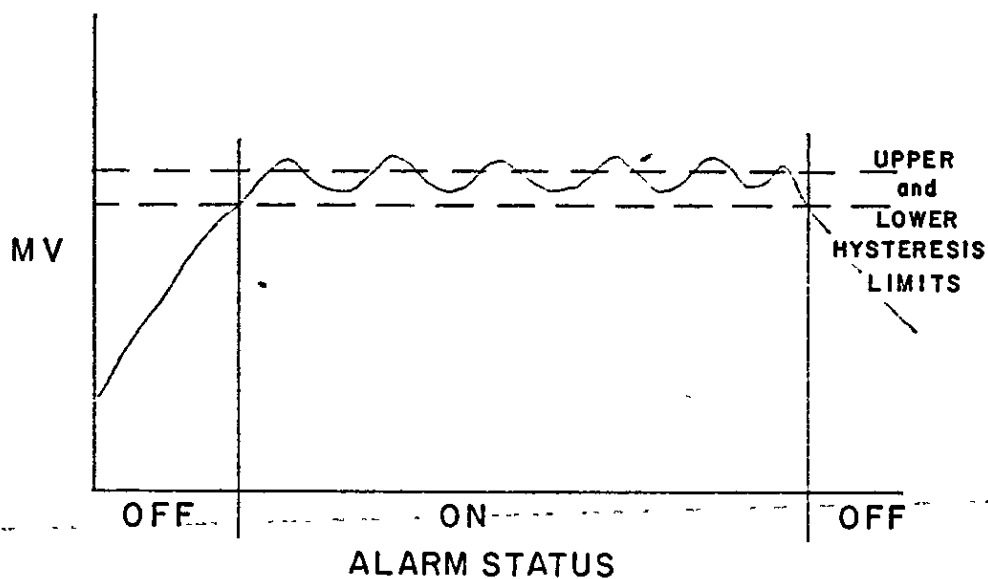
A common phenomena in the control room is alarm oscillation. As reported by Kortlandt and Kragt in 1980 [4], often alarm bands are set too close to normal operational levels of plant variables resulting in alarms displayed numerously and erratically as the measured variables made temporary excursions into alarm bands. It was reported that the oscillatory alarms are more often an annoyance to the operator because of the constant attention required to accept the alarm. Also the oscillatory alarms are often disabled by the operator. Alarm log listings are often cluttered with large numbers of these alarms. Although the literature stresses that alarm limits are often set too close, small fluctuations in process variables which necessarily run close to alarm limits can also produce oscillatory alarms.

An obvious way of improving the basic alarm types and reducing oscillation is to incorporate hysteresis in the alarm limits. Hysteresis provides a lag in the response of the alarm system by slightly altering the alarm limits depending upon the direction of the excursion of the process variable across an alarm limit. The resulting effect is to reduce the oscillation of alarms due to small process variable fluctuations near alarm limits.

Figure 4.4 illustrates how hysteresis on the alarm limits effects oscillation. Without hysteresis as the process variable fluctuated around the alarm limit alarms are generated numerous times as the variable repeatedly crosses the limit. With hysteresis as the process variable increases the upper hysteresis limit is in force. Once crossed the new alarm limit is the lower hysteresis limit. Fluctuations in the process variable between the upper and lower hysteresis values therefore does not result in alarm oscillation.



Alarm Limits Without Hysteresis (oscillation)



Alarm Limits with Hysteresis

Figure 4.4 Hysteresis Example

4.4 ADVANCED ALARM DETECTION

The detection of plant malfunctions can require the identification of a specific combination and/or sequence of symptoms on the plant. These symptoms can be in the form of plant data values or alarm information.

Detecting the occurrence of a complex relationship amongst the plant data and alarm information requires considerable effort on the part of the operator. There has been a large amount of work performed on the automatic detection of malfunctions of this type. The purpose of alarm analysis or disturbance analysis systems is to perform analysis of plant conditions based on plant data stored in alarm and/or fault tree plant models. The generation of the plant models is as complex as the evaluation of the models during operation.

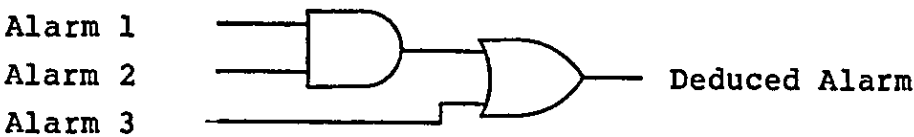
From these systems it is possible to identify some of the fundamental plant data processing techniques which would be useful to improve the capabilities of simpler alarm system philosophies.

4.4.1 Deduced Alarms

Deduced alarms are generated by logically combining other alarms or plant events to produce new alarms. The example in Figure 4.5 shows how three alarms can be combined into one deduced alarm and how the logic combinations can be expressed. There are many applications for deduced alarms. These applications can be broadly divided into the following classes:

- 1) Group Detection
- 2) Mode Detection

Logic Diagram



Truth Table Representation

A1	A2	A3	DA
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

1 = True
0 = False

IF-THEN Statement

IF ALARM 1 AND ALARM 2
OF IF ALARM 3 THEN DEDUCED ALARM

Figure 4.5 Deduced Alarm Representation

3) Voting or Quorum Gates

4) Asynchronous Group Detection

4.4.2 Group Detection

A common complaint about many alarm systems discussed in the literature is that during abnormal conditions on plants the operator is flooded with alarms and other plant information. The magnitude of the problem varies with the size, complexity and the total number of alarms fitted to the plant. A large number of alarms during high stress plant failure conditions can have a detrimental effect on the operator's ability to diagnose the faults on the plant for several reasons:

- 1) Heavy operator diagnostic demand due to a large amount of available information.
- 2) Conflict with operator training or experience during the recognition of clues and patterns of alarms and information.
- 3) Loss of alarm information due to alarms imbedded amongst other alarms and process data.

4.4.2.1 Information Overload

During abnormal plant conditions the operator is faced with a considerable amount of activity in the control room which under normal conditions would be quiet. Since abnormal conditions hopefully occur infrequently, the operator training becomes important. Usually a variety of abnormal plant conditions are simulated during operator

training so that the control room display messages and patterns are recognizably related to a particular plant malfunction. If on the other hand the operator doesn't recognize the pattern of events, the plant information and alarms play a more active role in the diagnostic procedure. Alarm messages and other plant information must be carefully examined and considered. This may not be an easy task especially under stressfull conditions. In this case the operator can become overloaded with alarm and plant information, some of which may not even be useful when major malfunctions occur. In addition the rate of appearance of new alarms is high, the operator's time is heavily occupied with accepting and attending to individual alarms leaving less time for diagnosis.

4.4.2.2 Other Interrelated Effects

When large numbers of alarms occur there are several other phenomena which can become evident as illustrated by the following three example cases:

Example 1: Loss of Information

The operator notes alarms as they appear. See Figure 4.6. The sequence of their appearance, the time between the occurrence of alarms, the pattern of alarms, linked with other clues and plant information has convinced the operator that a certain malfunction has occurred since he has experienced this condition before. An additional set of alarms has also been generated, however the operator does not take note. As a result the additional alarms are hidden by the other more numerous alarms. These additional alarms could indicate other malfunctions or possibly even invalidate the operator diagnosis. The patterns which the operator thought he recognized were in fact manifested by a different malfunction.

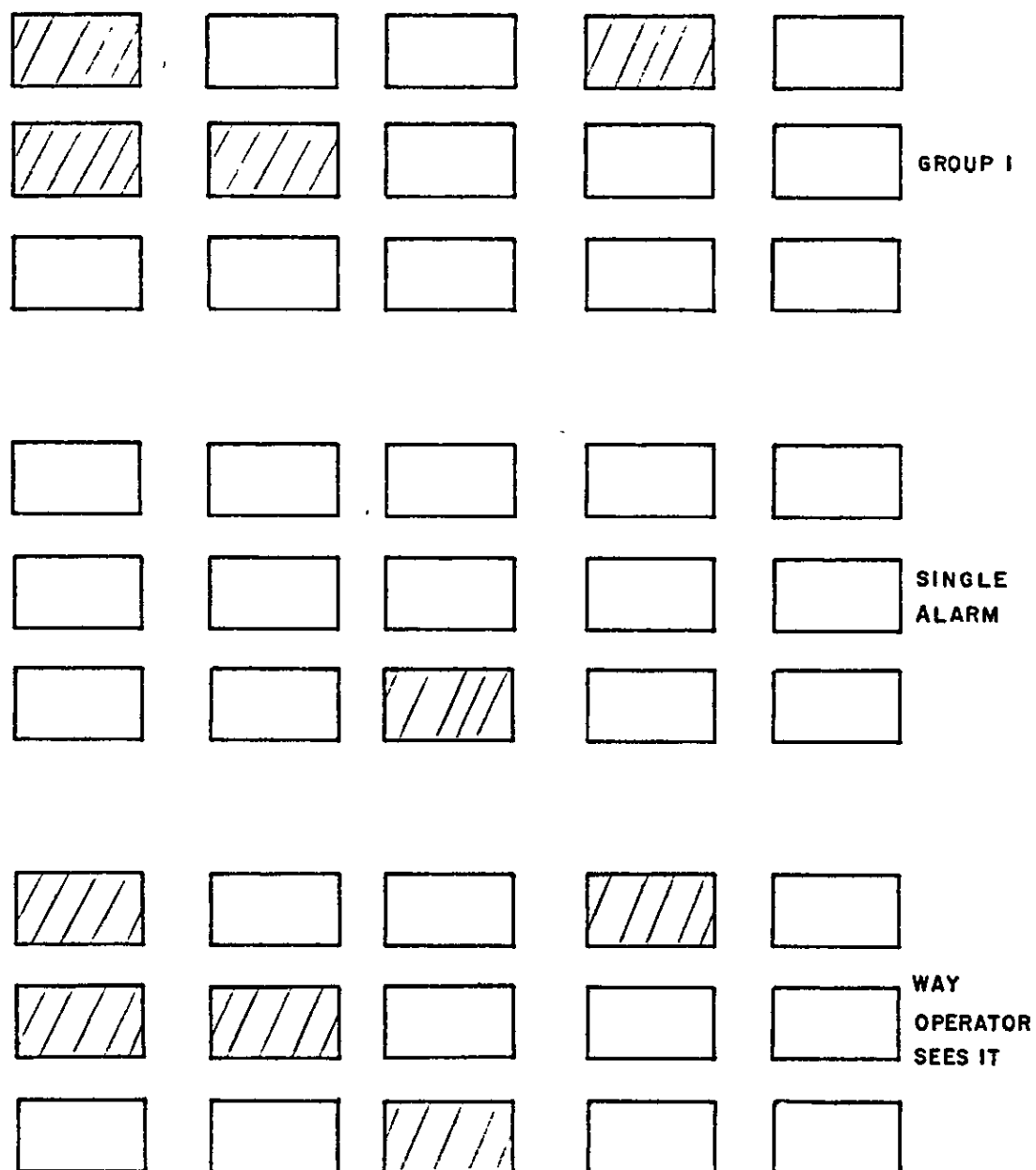


Figure 4.6 'Loss' of Information on
Alarm Annunciator Panels

Example 2: Multiple Malfunctions

Many alarms start appearing in the control room. See Figure 4.7. The operator does not recognize any pattern of events. Possibly his training has emphasized that when in doubt, shut down. In fact what happened is that two malfunctions occur, both readily recognizable by the operator. However since both events occurred close to each other the alarms representing the two malfunctions were mixed together resulting in confusion to the operator. The consequential shutdown could have been avoided if only the operator had recognized the situation.

Example 3: Mind Set

It has been noted that operators can become 'mind set' on a diagnosis of a malfunction even when confronted with information clearly indicating otherwise. In situations where large numbers of alarms and other plant information are presented, operators can inadvertently centre their attention on a small number of alarms, etc. and possibly formulate erroneous diagnoses simply because other data has been ignored.

The above examples have been necessarily simplified to illustrate the points presented. In reality the effects are overlapping and much less clearly defined.

Alarm systems capable of detecting groups of alarms can help overcome many of the difficulties discussed. There are three major applications of deduced group detection:

- 1) Detect and display additional group alarms.

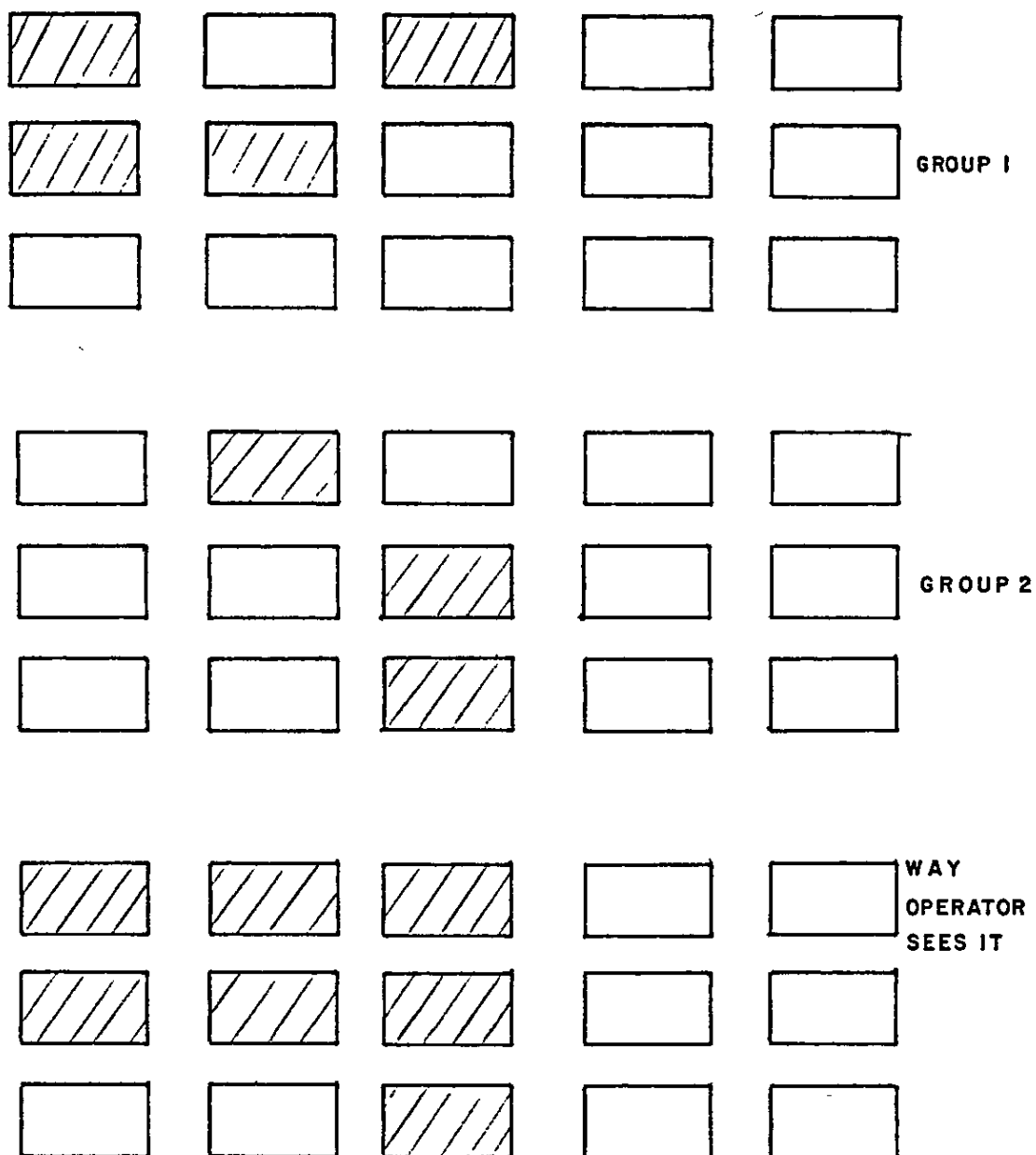


Figure 4.7 Multiple Malfunctions on Alarm Annunciator Panels

2) Reduce the number of alarms presented by suppressing alarms representing a predefined group and replace with a single alarm.

3) Identify alarms that should have occurred.

No doubt the more significant feature is the ability to generate additional alarms which represent the occurrence of a group of alarms. Alarm group indicators can reduce the confusion present when multiple malfunctions occur. Group alarms also reduce mind set phenomena by providing additional diagnostic information. This extra information can help to confirm or contradict the operator's diagnosis.

Group detection can be used to suppress alarms associated with a well defined malfunctions. In this case the primary objective is to reduce the number of alarms presented to the operator. Reducing the information load during serious malfunctions can relieve some simple diagnostic operator tasks. Group alarm suppression also will reduce the number of alarms lost amongst a multitude of alarms. Removing group related alarms results in a lower number of alarms thus increasing the chances that the operator will note the odd ones out.

Group detection is also useful for operator diagnosis of clusters of alarms. Because a group alarm will not be indicated when an alarm in the group is not active, an operator is less likely to diagnose a malfunction which he would usually associate with a similar group of alarms.

Group detection must be implemented with great care to ensure that the group of alarms truly does represent a unique malfunction. If the group can occur in several different circumstances, the results can seriously degrade the alarm system performance by misleading the operator.

Summarizing, group detection has the following benefits if carefully used:

- 1) It generally aids operator diagnosis.
- 2) It aids in confirmation of operator diagnosis.
- 3) It effectively reduces unnecessary alarm information.

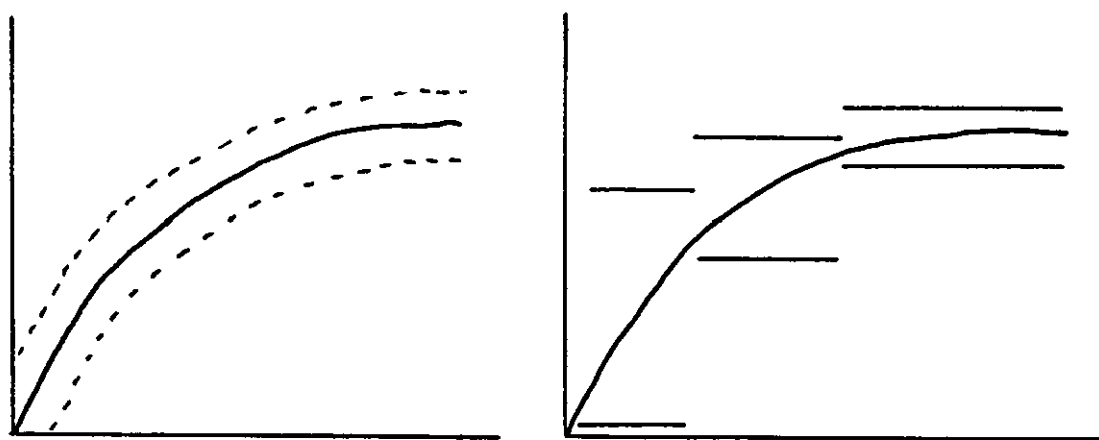
4.4.3 Mode Detection

The basic alarm types generally apply to steady state operations where process variables are expected to remain within predefined operating limits. Clearly the fixed nature of these alarm limits necessarily causes alarms to be generated inadvertantly during normal transient operations on the plant. Normal but also transient plant conditions most notably occur during startup and shutdown in continuous plants. Continuous plants may also experience temporary shifts in normal operating conditions for a variety of reasons such as maintenance, changes in throughput, etc. Batch processes are inherently transient. Where the shift in process variable values is predictable, the alarm limit could be dynamically adjusted to match the operational mode of the plant.

Ideally the adjustment of alarm limits should be continuous to meet the changing expected normal values of a process variable as shown in Figure 4.8. Practically dynamic alarm limits can be very difficult to implement. During transient conditions it may be difficult to establish the progress of the process and therefore the expected normal values of process variables. A less exact method of adjusting alarm limits during transient conditions would be

to establish generalised plant operational modes. Broadly defined operational modes are simpler to detect and still provide generous flexibility of alarm limits. For example, an operational mode may be defined as 'startup' mode or perhaps 'startup 1' and 'startup 2' modes. Linking operational modes with alarm limit selection can closely emulate fully dynamic alarm limits as shown in Figure 4.8.

Mode detection can be a useful facility in an alarm system to improve the accuracy of alarm generation. An alarm system must be capable of detecting operational modes and linking the mode with alarm detection.



Ideal Dynamic Alarm Limits

Operational Mode Linked
Alarm Limits

Figure 4.8 Alarm Limit Selection During Transient Processes

Another type of mode detection is found particularly in batch processes where sequences are used. Sequence steps can represent distinct identifiable modes of operation. Often alarm limits are associated with individual sequence steps. Identification of process sequence steps therefore can be utilized to establish alarm limits.

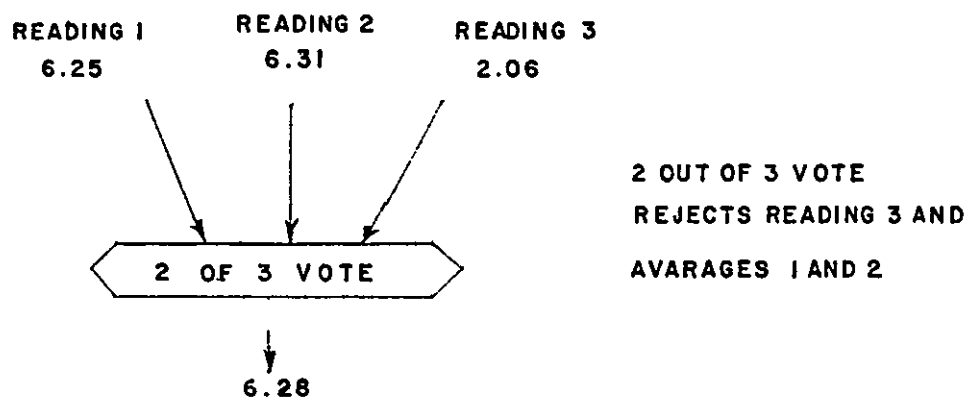
4.4.4 Voting or Quorum Gate

A characteristic of high reliability and fault tolerant plants is redundancy of many of the plant sensors, transducers, control systems, etc. Redundancy is the duplication of system functions. Using multiple equipments the probability that total equipment failure occurs is reduced. Normally the data obtained from multiple instruments coincide, however when a malfunction in one instrument occurs there is a conflict with the data from the other instruments. A voting technique is used to reject the suspect data by assuming that the majority of data is accurate.

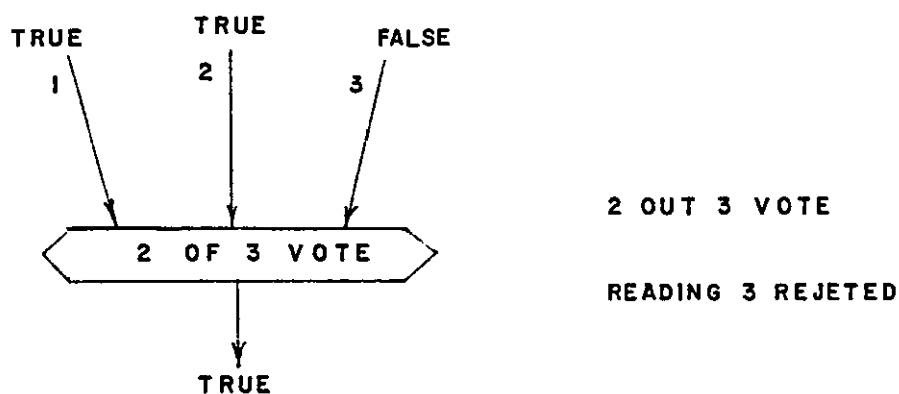
The example in Figure 4.9 illustrates how voting is applied to analogue process data. Binary data voting, also illustrated, may be used for plant contact status data or events on the plant. Voting may also be implemented as a type of group or mode alarm detection. In this case the vote is used to detect the occurrence of a group of N events or alarms out of M specified events or alarms.

4.4.5 Asynchronous Group Detection

A rather unusual form of deduced alarm detection is asynchronous group detection. The function, included for completeness, is best explained by example. Referring to the illustration, the group is detected even if the alarms



ANALOGUE VOTING



BINARY VOTING

Figure 4.9 Voting

or events do not occur simultaneously. Regardless of when the alarms or events occur, at the moment all alarms in the asynchronous group have been detected as having been active, the group alarm is generated.

Refer to Figure 4.10 for the following example. Assuming alarms A, B, and C are part of an asynchronous group, a deduced alarm is detected at times as indicated by pointers 1 and 2. Once an asynchronous group is detected, the group detection is reset. All alarms in the group must appear once again before the deduced alarm is generated.

4.5 TIME RELATED DETECTION

During the diagnosis of plant malfunctions operators can experience difficulty associating the order of appearance of alarms with specific fault conditions. The order and the time between changes in the alarm displays can give valuable diagnostic clues as to the nature of the malfunction. In control room situations operators can have difficulties interpreting and identifying information presented at varying time intervals especially when the magnitude of time between alarms is large. The difficulties are compounded as the number of active alarms increases. The operator may not associate recent alarms with alarms already standing. Operators may also lose significant alarms in a sequence of alarms representing a plant malfunction.

Operators presented with time-related or dynamic trouble shooting often interpret alarms and process data as representing steady-state or static plant operating conditions. As alarm conditions manifest over a period of time process variables are changing. These variables may make excursions into and out of alarm conditions as the

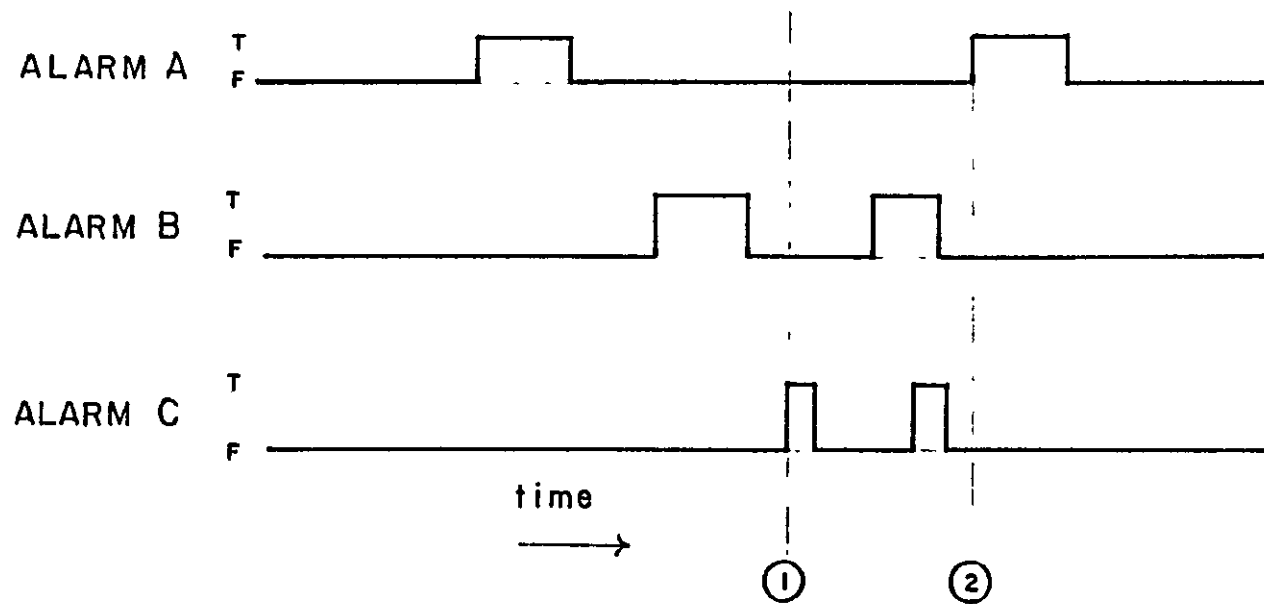


Figure 4.10 Asynchronous Group Detection

malfunction matures. The operator can be led to believe that at a given moment the plant malfunction has fully developed, that is, it had become static or steady-state in nature. Instead the malfunction is progressively growing worse. The time window during which an operator perceives the sequence of events on the plant may not be sufficient for him to make an accurate diagnosis of the malfunction. Early detection of drifting plant operational conditions may assist the operator to locate the difficulty before the malfunction worsens. Drifting plant conditions manifest themselves in the form of alarms that will appear and/or disappear in an order dependent upon the fault provided the alarms and alarm limits are carefully preselected.

In batch operations time dependency of alarms is markedly illustrated. Batch operations are characterised by sequential processes which by definition are time related. The generation of alarms is therefore dependent upon the progress of the process through the sequence.

Referring to the example in Figure 4.11, a plant malfunction occurs at time T_0 . As the malfunction begins to effect process variables, alarms begin to appear in the control room. At time T_a the operator notes that alarms A, B, and E are active. He can refer to the plant log for chronological information about the alarms however in this case they have appeared at roughly the same time. The operator may interpret the malfunction as static and base a diagnosis on the basis of these three alarms. It could be that a short time later, as the malfunction worsens, that new alarms appear while others disappear. At time T_b alarm B is gone and E, D, C, and A are active. This pattern of alarms could possibly represent a different malfunction from the operator's diagnosis. Additional information may be obtained by noting the order and time lag between alarm activity. The time ordered pattern of alarms in this

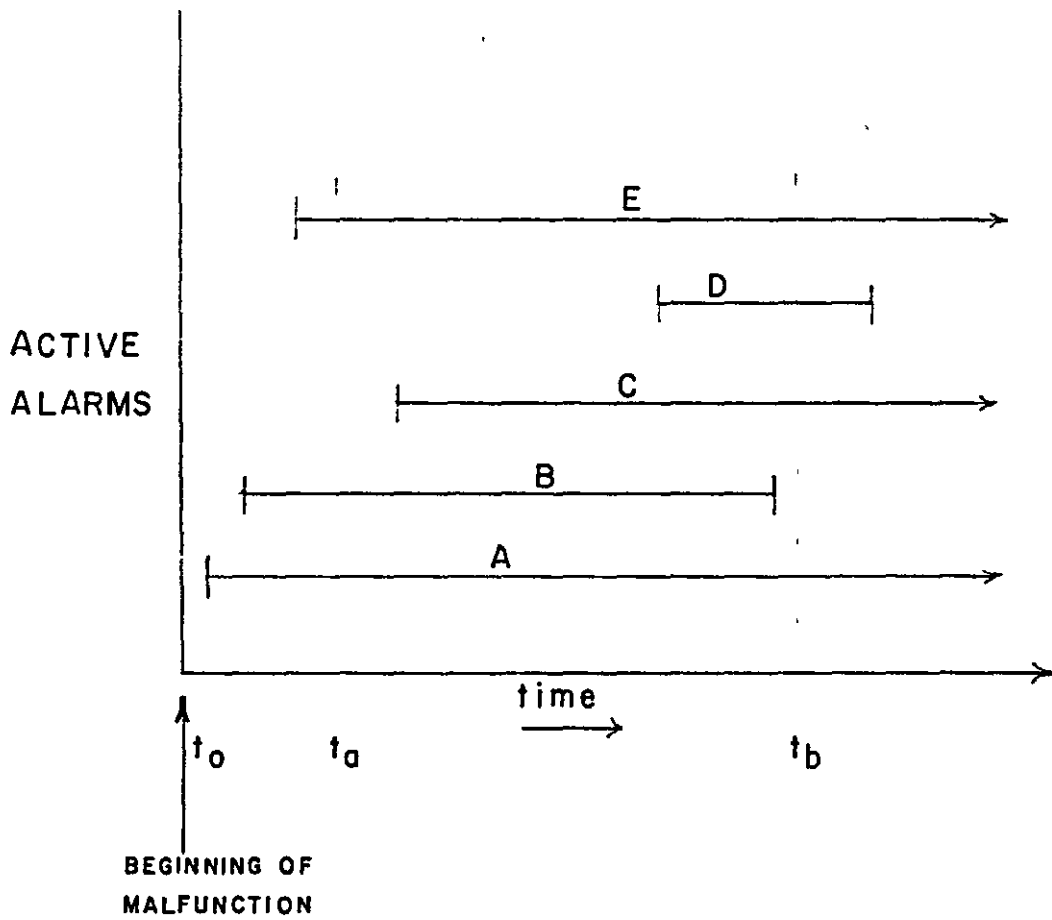


Figure 4.11 Active Alarms Representing a Plant Malfunction

example represents a specific malfunction.

Up to this point we have discussed the detection of alarms in static applications. The plant conditions are assumed to remain relatively constant with respect to time, i.e., steady state. Alarm definitions also remain constant with time. For convenience we will call non-time related alarms Static Alarms.

Conversely dynamic alarms are alarms whose conditions or limits change with time or are time dependent in some way. There are three major types of dynamic alarms:

1) Trend. Trend alarms are the most common form of dynamic alarms. The rate of change or trend of a process variable is established and compared with alarm limits. This calculated value can be subject to alarm detection functions as described previously. Trend alarm detection is available in many existing alarm systems. See the example in Figure 4.12.

2) Timeouts. In certain circumstances it is desirable to have the capability of placing time limits on the occurrence of an alarm. The best way to explain this is by example. A particular measurement on a plant is expected to reach a certain value and then recede during a normal operation. However, if the value is maintained after a period of time T , then the value represents an alarm condition. This type of alarm condition is defined as a timeout alarm. A typical application for timeout alarms could be on a furnace where a temperature must be reached within a specified time period. See Figure 4.13.

3) Sequences. Sequences are series of events which occur in time-ordered succession. Sequential operations on plants are transient procedures which are comprised of a

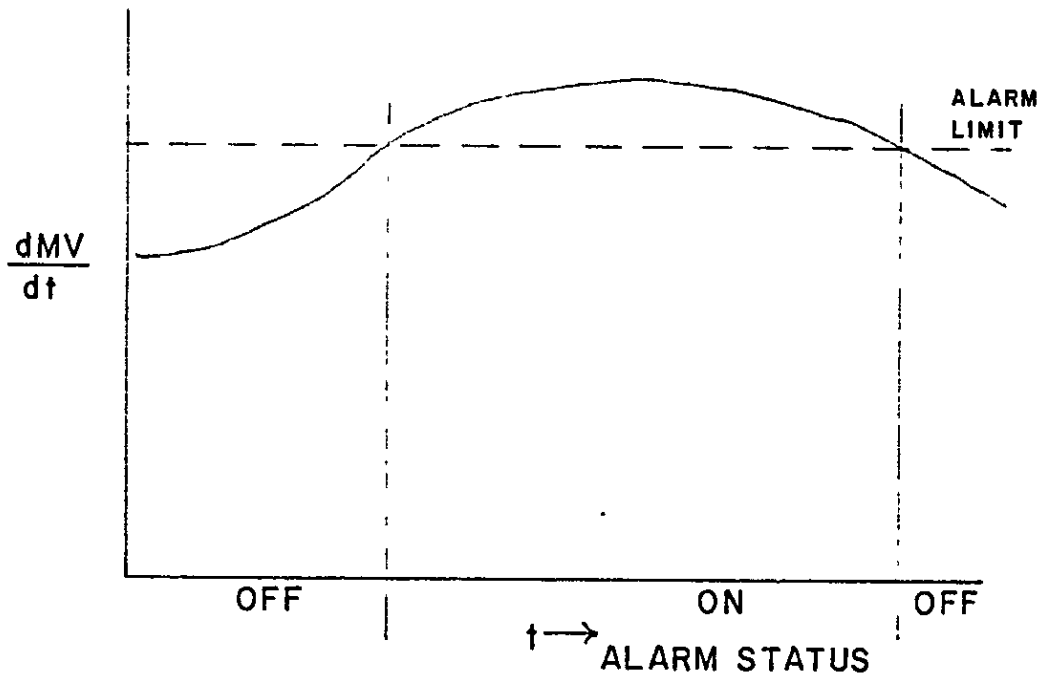


Figure 4.12 Using Absolute Alarm Detection for Rate of Change Alarm Detection

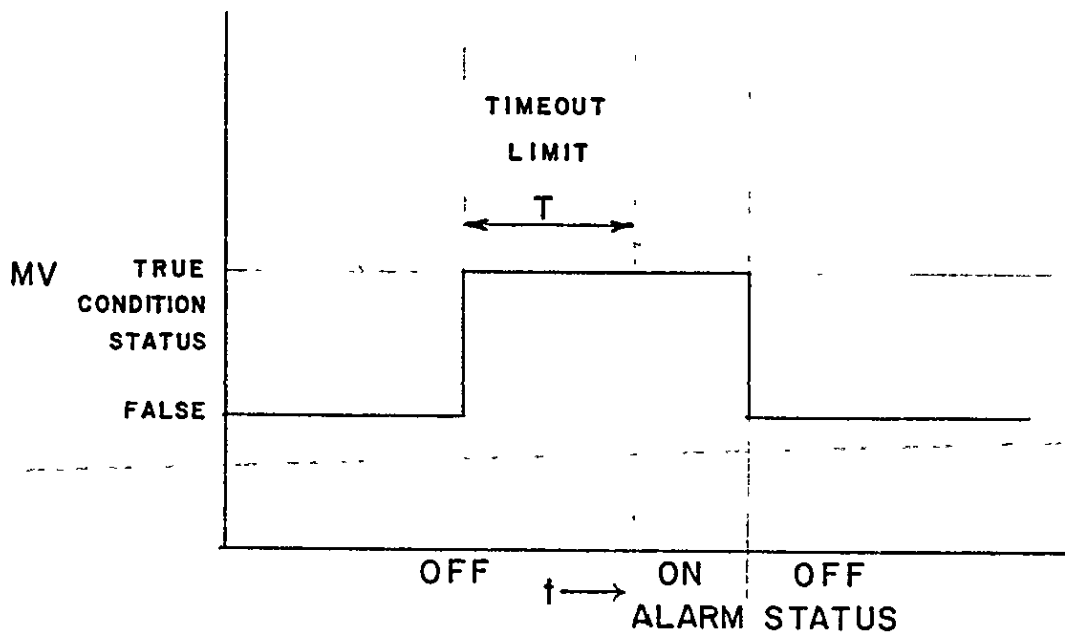


Figure 4.13 Simple Timeout Detection Example

series of step or continuous changes in the operational mode of the plant. Examples of sequential operations can be found on most plants. On continuous plant types, for example, the startup and shutdown procedures are sequential. Batch processes are comprised almost entirely of sequential operations.

4.5.1 Sequences

Sequential detection for alarm generation can be complex. It is difficult to establish sequences which represent unique plant malfunctions or operational modes.

The subject of plant sequences requires much more study and evaluation which is beyond the scope of this thesis. There are however some identifiable sequential capabilities that an alarm system could usefully implement.

Discussed below are three types of sequence detection which collectively are capable of dealing with many sequential operations on the plant. These three types are:

- 1) Simple sequences
- 2) Conditional sequences
- 3) Clock linked sequences

Sequence detection can subsequently be used to generate alarm information.

4.5.1.1 Simple Sequences

The basic sequence is a series of time-ordered events. Detection of simple sequences involves the examination of the time of occurrence of the events. The sequence

conditions have been satisfied when the times of occurrence of the events are in the correct chronological order.

$$T_a < T_b < T_c < T_d$$

In the above example the sequence conditions are satisfied when the time of event A, T_a , is less than the time of event B, T_b , and so on. The equivalent word description of the sequence condition would be as follows:

IF EVENT A THEN IF EVENT B THEN IF EVENT C THEN IF EVENT D
THEN SEQUENCE = TRUE.

The sequence condition statement is satisfied only when all events are correctly time-ordered.

4.5.1.2 Conditional Sequences

Simple sequences contain no time window restrictions. This can result in inaccurate sequence detection during long periods of operation where individual events may accidentally occur in the correct time order, but not as a result of an identifiable plant sequence. The example in Figure 4.14 illustrates how an event B must occur within a specified time window after event A has occurred. The conditional sequence is satisfied when event A occurs at T_a and then event B at T_b after N_0 seconds but not after N_1 seconds from the time of occurrence of event A. The sequence detection is therefore conditional upon events A and B occurring not only in the correct chronological order, but also event B must occur within a defined time window after event A. The conditional sequence can be expressed as:

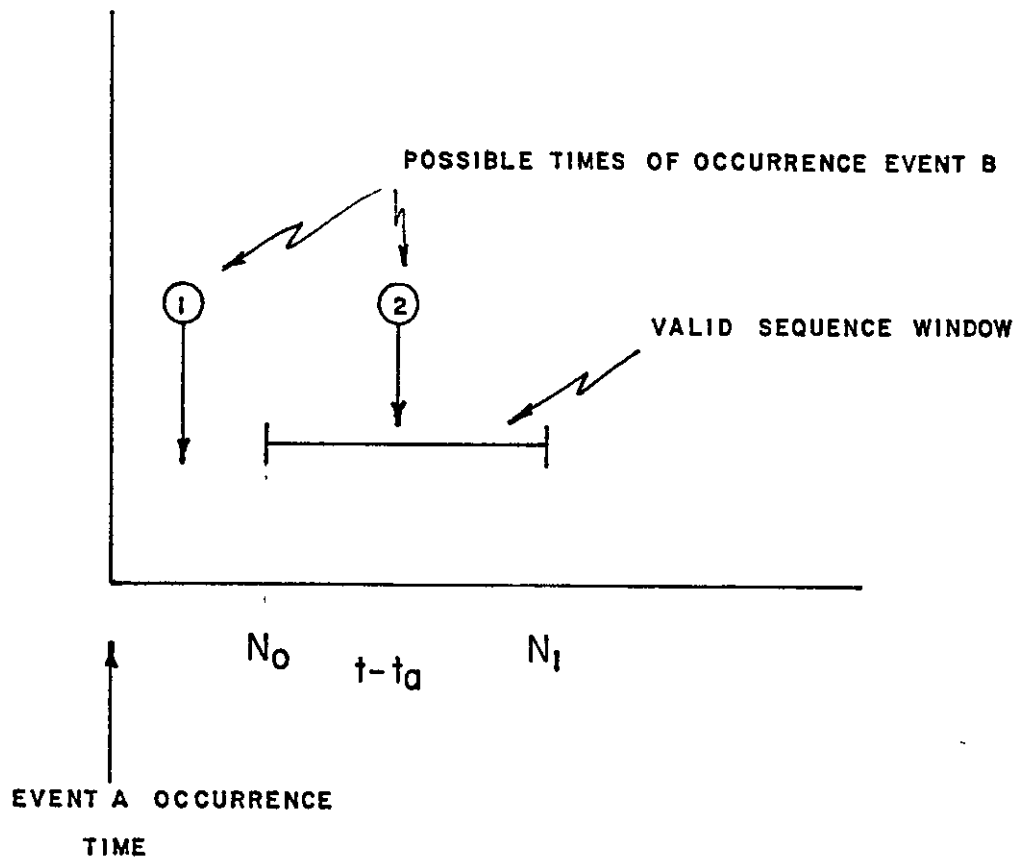


Figure 4.14 Use of Time Windows in Conditional Sequence Detection

$$T_a + N_0 < T_b < T_a + N_1$$

or

$$T_a < T_b - N_0 \text{ AND } T_a > T_b - N_1$$

Conditional sequences can also be used to limit the maximum time during which the sequence detection is valid after the first event has occurred in the sequence. A typical limited time window sequence could be:

$$T_a < T_b < T_c < T_a + N_2$$

In this example the sequence conditions are satisfied only when the sequence occurs within the time window T_a to $T_a + N_2$.

The selection of the time windows in sequence detection can be critical. The time window, for example, in which a sequence condition may be satisfied might be coincidental with other events or plant conditions which will generate similar sequences. The result would be an inaccurate sequence detection.

4.5.1.3 Clock Linked Sequences

As we have seen in the previous examples sequence detection relies heavily upon the detection of the occurrence of the first event in the sequence condition statement. Sequence detection must necessarily be initiated by such a leading event. The leading event or 'key' event within the sequence defines the time window and therefore must be carefully chosen for their reliability and accuracy. In some cases it may be useful for sequence detection to be initiated by the real time as obtained from a computer system's internal clock. In the example below an event time

of occurrence is replaced by a real time clock value T_{clk} . In this way the sequence detection is initiated at time T_{clk} .

$$T_{clk} < T_a < T_b$$

4.6 COMBINING ALARM DETECTION FUNCTIONS

Individual alarm detection functions have been discussed in the preceeding sections. It is not difficult to find example applications which require combinations and permutations of the functions discussed to define alarm conditions. Mode detection, for example, combined with an absolute alarm would be useful during startups. In this case the mode would be used to inhibit the absolute alarm until the startup was complete. Similarly, it may be desirable to gather different types of groups of alarms to produce yet another alarm. The variety of combinations is endless. A comprehensive alarm system should therefore provide some means of combining alarm detection functions as have been discussed here.

4.7 VALIDITY AND VERIFICATION OF PROCESS DATA

The ability of any alarm system to assess plant conditions is dependent upon the validity of the plant data that it receives. The reliability of plant sensors, transducers, and interfaces is therefore an important consideration when evaluating the performance of an alarm system. Ideally we would like an alarm system to be capable of detecting instrument malfunctions. This can be accomplished to some degree by examining the data received from the instruments. A comparison of instrument data with known performance characteristics of the instrument can be

utilized to assess its validity. Recent developments in instrument technology have produced instruments with 'health' signals which inform the process computer of the validity of data.

As discussed by Anyakora and Lees in 1972 [43] and Lees in 1980 [35], some instrument failures can demonstrate behaviour which is implicit of instrument malfunctions.

- Zero
- Full Scale
- Drift
- Sudden shifts in data
- Noise or erratic behaviour
- Lack of sensitivity

Instruments which fail in either the zero or full scale mode are readily detectable by comparing the instrument output with the known functional range of the instrument. A zero or full scale output could be indicative of an instrument failure.

Instrument malfunctions can be difficult to detect if the failure permits the instrument to function within its normal operating range. Drift, sudden shifts, and erratic behaviour in instrument data may either be symptoms of instrument failure or accurate process data. Additionally, an instrument can also fail in such a manner that little change in output occurs.

In situations where high reliability of instrument data is required, multiple instruments are used. Voting techniques as described previously can filter out faulty data. Data can also be checked by comparison with other types of plant data.

An alternative source of instrument failure information can be obtained from the operator. Upon malfunction notification from the operator, the alarm system can regard the appropriate plant instrument as faulty. This form of failure detection may be questionable since operators tend to abuse facilities such as this to disable or modify alarm systems.

Instrument failures have serious consequences for alarm detection. Inaccurate plant data is translated into inaccurate alarms. A comprehensive alarm system should be capable of performing some verification and validity checking of plant data. The effect of inaccurate data acquisition should be reduced to a minimum.

4.8 PROCESS DATA TYPES

Any process plant generates a variety of different types of process data. Analogue data from plant instruments can be in the form of a voltage or current value. Switch contacts represent binary ON/OFF status information. The host process computer can also generate digitally coded plant data. In cases where the alarm system is functioning independently of other plant data acquisition equipment, a versatile alarm system must have some data acquisition facilities capable of dealing with a wide variety of plant data types.

4.9 VERSATILITY

In order for any computer based system to be useful in a number of different applications, the complete system package must be flexible. The implication is that alarm

detection functions need to be readily programmable into the system in a form that is easy to modify. The alarm system should have sufficient versatility such that few significant alterations need to be performed to customize a system for a specific application. Experience has shown that the more universally applicable a computer system is, the greater the complexity. For an alarm system to be useful the complexity of programming and usage must be kept to a reasonable level. For example, the complexity problems of the alarm analysis systems has made their application to process plant difficult and unwieldy.

A compromise must be made between complexity and flexibility to produce a philosophy for a versatile and useful alarm system.

4.10 DISPLAY REQUIREMENTS

Alarm displays commonly in use can be divided into three categories:

- 1) Alarm Annunciator Panels
- 2) Computer Generated VDU Displays
- 3) Printers and Logs

A versatile alarm system should be able to provide sufficient alarm information to drive any of these display systems.

Alarm annunciator panels require only an output signal to indicate which panel indicator should be activated. The alarm text is inscribed on the indicator. Backlighting modes, acceptance procedures, and status are generally

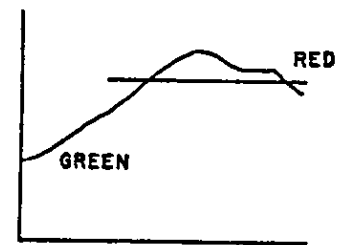
controlled internally by the annunciator system.

Computer generated VDU displays provide highly flexible display formats which can be comprised of many forms of alarm information. Some typical types of computer driven alarm information displays are illustrated in Figure 4.15. Additionally the organisation of the alarm information varies as illustrated in Figure 4.16. The alarm system must be able to generate sufficient alarm data to support these display formats.

* TEMP23 999.2 DEG C
 VLV34 OPEN
 LIC56 78 IM

MARKER

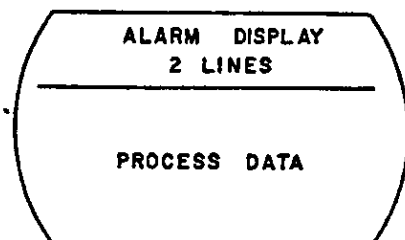
TEMP23 999.2 DEG C
 VLV34 OPEN
 LIC56 78 IM



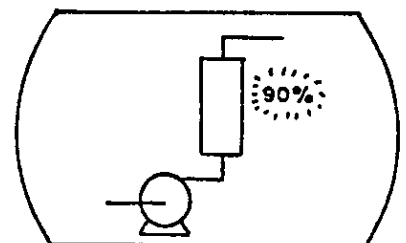
COLOUR CHANGE

FLASH OR REVERSE VIDEO

PROCESS DATA ENHANCEMENT



SEGREGATED ALARM-TEXT



ENHANCED MIMICS

Figure 4.15 Typical Alarm Information Display
 on Process Data VDU's

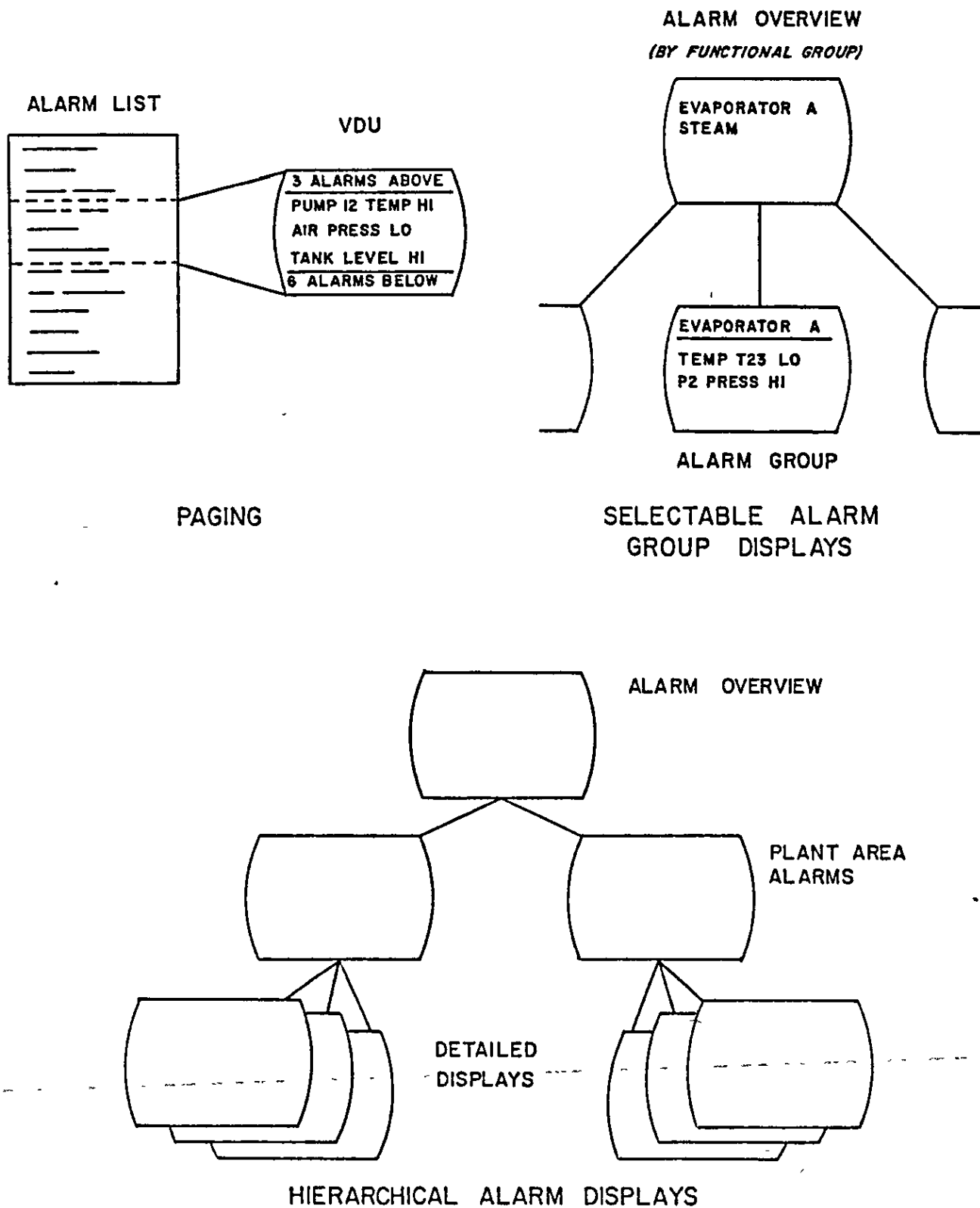


Figure 4.16 Organisation of Alarm Information Display
on Alarm Dedicated VDU's

CHAPTER 5

USING EVENTS TO DESCRIBE ALARM CONDITIONS

5.1 INTRODUCTION

In previous sections some of the identifiable alarm detection functions which should be incorporated in an alarm system have been analysed. The implementation of these detection functions in a computer based system as has been proposed requires careful consideration. In this case the requirements of the potential user and the performance characteristics of the operational alarm handling system are interacting factors which necessarily complement each other.

The alarm handling computer has limited capacity for data storage and limited processing time. Therefore the data and processing structures within the computer must be compromised to give adequate performance of the overall system.

On the other hand, if the proposed alarm handling system is to be user programmable, the programming procedure must be readily understandable to potential users who may not be familiar with computer systems.

There are therefore two major design aspects to consider which are dependent on each other:

- 1) The form and type of data input which the user must insert into the alarm system and
- 2) The functional structure of the alarm system

itself.

It has been noted that for the alarm handling system to be readily usable, the alarm system programming procedure must also be relatively simple. There are several alternatives, the two most significant ones being:

- 1) Utilize an alarm handling language which would include a repertoire of program statements which describe the available functions of the alarm system or

- 2) Provide interactive question and answer routines for the input of data.

In either case it is necessary to provide a means by which the user can fully assign all parameters, limits, etc. which in turn define how the alarm system should function. This topic is discussed in greater detail in the next chapter.

The alarm computer must process the alarm data programmed by the user. The program must store a full description of each alarm. The system must also process this data each time a scan of the alarm is performed. Therefore the more detailed and numerous the alarm descriptions, the more storage and processing time is required to evaluate all the alarms in the system. At some point the processing time required to perform one scan of all alarms may be greater than the desired scan period.

The point is that it would be useful to examine methods for simplifying programming of the system while also providing sufficient alarm data to fully define the operational alarm system. Additionally methods for storing and processing this data to minimize required data storage and processing time should be considered. In this

chapter a method of using events to describe alarm conditions which also suggests an efficient method for processing the alarm data based on the findings of the previous chapter is discussed.

5.2 EVENTS

The description of alarms or the alarm definitions can be complex as we have seen in previous sections. Alarm definitions which require multiple process data measurements and calculations can quickly become awkward and tedious to express. Since alarm conditions on a plant represent the occurrence of a particular event or a combination or series of events, the alarm conditions can alternatively be described in terms of plant events.

An event is defined as something that has happened on the plant. The event can be anything that represents an identifiable state or operational mode of the plant. Events can be described in terms of single measured variables or combinations of plant data which jointly describe a condition on the plant. For example an event can be defined as:

EVENT X = the temperature of reactor vessel 2 is over
100 degrees C.

In this case EVENT X is defined by a single measured variable.

EVENT Y = the boiler pressure is below 50 PSI and the
burner is off.

The complex EVENT Y is comprised of several items which collectively define, for example, a shutdown state. As

implied in the example, events are binary in nature, that is, the event has either occurred or has not occurred. The time of occurrence (TOC) of an event is defined as the first moment at which all conditions describing the event are detected. For convenience an event is TRUE if it has occurred and all conditions describing the event are true otherwise the event is FALSE. See Figure 5.1.

Event X and Event Y may represent events on the plant which singularly do not represent an alarm condition. However, if both Event X and Event Y are true then an alarm condition may exist. The alarm condition can then be described by the following word definition:

If Event X has occurred and Event Y has occurred then an alarm condition is present.

By defining alarm conditions in terms of events alarms can be expressed in the form of logical statements as follows:

IF EVENT X AND EVENT Y THEN ALARM CONDITION

The IF-THEN logic statement is a representation of Boolean logic expressions so the IF-THEN statement can be simplified to the Boolean expression:

ALARM = EVENT X AND EVENT Y

5.3 DEFINING EVENTS

The binary nature of events necessitates the conversion of continuous analogue plant data into a discrete status which is suitable for use in alarm condition statements. Some processing of binary plant data such as switch contact information may also be required to produce an appropriate

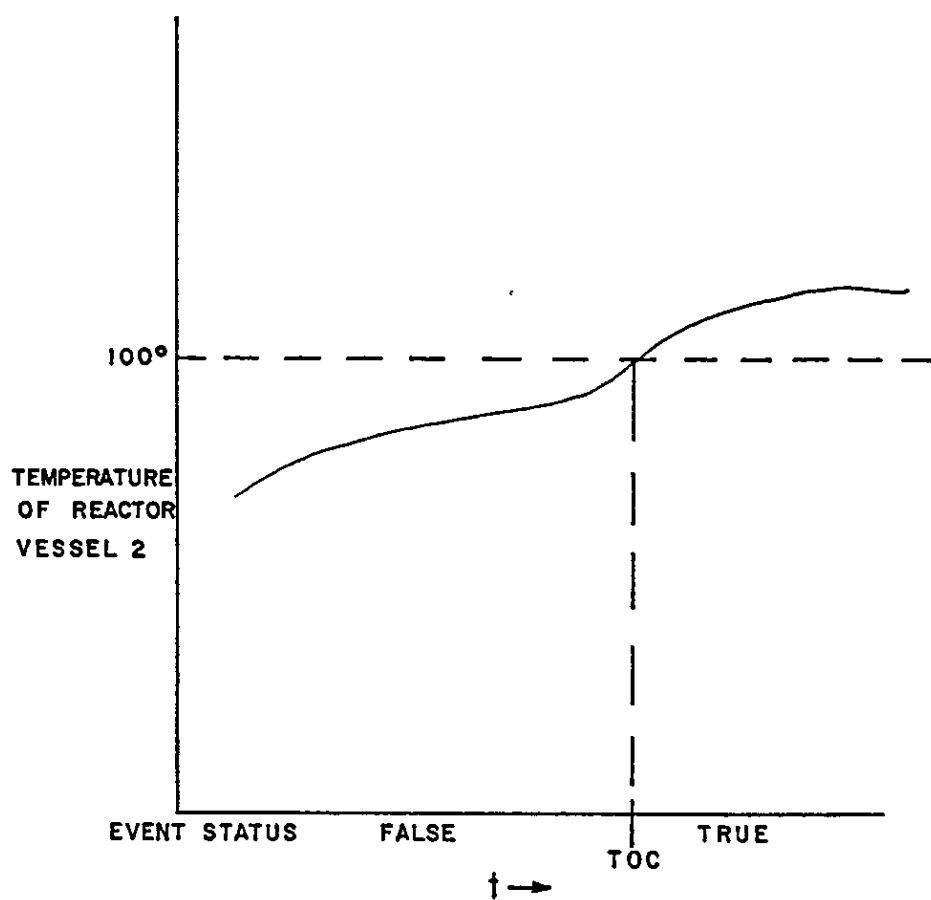


Figure 5.1 Example Event Detection

TRUE/FALSE event status.

Events represent a variety of plant conditions and can be categorized according to type. The event types shown in Table 5-1 identify the form of processing required to convert process data into the corresponding event status. The event types are derived from the basic alarm detection functions discussed in Chapter 4. Recall that the distinction between an alarm and an event is that an event may or may not represent an alarm condition on the plant.

Referring to the previous example:

EVENT X = the temperature of reactor vessel 2 is over
100 degrees C.

The name of the event is EVENT X, the event type is HI, and the event parameter is 100 degrees C. The evaluation of the process data is defined by the event type HI which specifies that the event is TRUE if the temperature of reactor vessel 2 is over 100 degrees C.

Subsequently an alarm definition could include this event thus forming a basic alarm detection function:

Reactor 2 Alarm = EVENT X

5.4 COMBINING EVENTS IN ENHANCED BOOLEAN EXPRESSIONS

Basic alarm detection can be implemented with events as illustrated, however, advanced alarm detection requires the combination of events. The opening example of the usage of events demonstrates how events can be combined in logical expressions.

<u>EVENT TYPE</u>	<u>PROCESS DATA TYPE</u>	<u>BASIC ALARM DETECTION FUNCTION</u>	<u>EVENT PARAMETERS</u>
[†] XLO	analogue	absolute	variable limits below which an event is true
LO	analogue	absolute	" "
HI	analogue	absolute	variable limits above which an event is true
[†] XHI	analogue	absolute	" "
ON	binary	binary	data state representing a true event
OFF	binary	binary	" "
DEVI	analogue	deviation	variable limits above and below which an event is true
BAND	analogue	band	variable limits within which the event is true

[†] XLO = LOLO, XHI = HIHI

Table 5-1 Basic Event Types

Boolean logic expressions are useful for representing the operations required to evaluate deduced alarm conditions. Boolean operators can exactly define most logic expressions required. The basic Boolean operators from which all other Boolean operations can be expressed are shown in Figure 5.2.

Figures 5.3 and 5.4 illustrate how some deduced alarm detection functions can be described with Boolean expressions. Logical combinations of events provide great flexibility for defining deduced conditions.

5.4.1 VOT Operator

Although many advanced alarm detection functions can be described, the usual Boolean operators do not provide sufficient operations to suitably express the functions required for voting, asynchronous group detection or for time related alarm detection. Some additional enhanced operators are proposed here to include these functions.

Alarm 6 = VOT n (EVENT A, EVENT B, EVENT C)

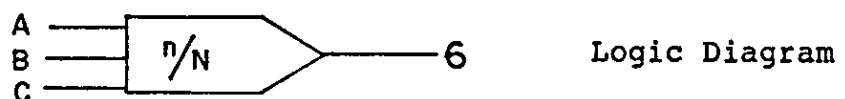


Figure 5.5 VOT Operator

The syntax of the VOT operator is as follows:

VOT<number true n>(<event list N>)

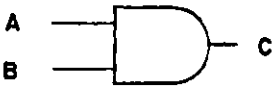



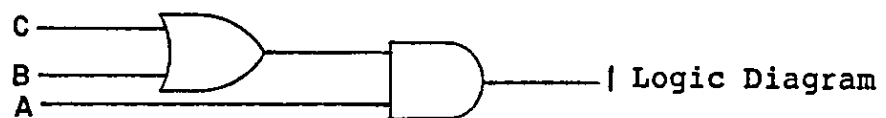
<u>Boolean Operator</u>	<u>Truth Table</u>			<u>Logic Symbol</u>
	A	B	C	
AND	0	0	0	
	1	0	0	
	0	1	0	
	1	1	1	
OR	0	0	0	
	1	0	1	
	0	1	1	
	1	1	1	
XOR	0	0	0	
	1	0	1	
	0	1	1	
	1	1	0	
NOT	0		1	
	1		0	

Figure 5.2 Some Basic Boolean Operators

ALARM 1 = EVENT A AND (EVENT B OR EVENT C)



IF EVENT B OR IF EVENT C THEN
IF EVENT A THEN ALARM1

IF-THEN
Statement

Figure 5.3 Example of a Simple Deduced Alarm

GROUP ALARM = EVENT A AND EVENT B AND EVENT C



Logic Diagram

IF EVENT A AND EVENT B AND EVENT C THEN GROUP ALARM

IF-THEN Statement

ALARM 1 = EVENT A AND NOT (GROUP ALARM)

ALARM 2 = EVENT B AND NOT (GROUP ALARM)

ALARM 3 = EVENT C AND NOT (GROUP ALARM)

Group Suppressed Alarms

Figure 5.4 Example of Group Detection Used to Suppress Alarms in Group

The VOT operator is followed by the number of events which must be true in the event list for the result of the function to be true. For the purpose of this work it was decided that an option should also be included such that if no number true parameter is specified that the operation default to a majority vote also known as a quorum vote.

5.4.2 ASG Operator

Similarly the asynchronous group detection can be expressed with the ASG enhanced operator:

Alarm 7 = ASG (EVENT D, EVENT E, EVENT F)

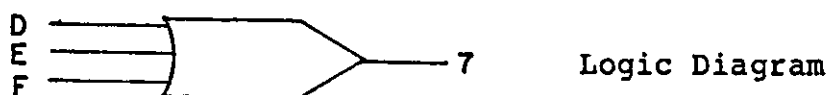


Figure 5.6 ASG Operator

The syntax of the ASG operator is the operator followed by the list of events in the group. Each time an event in the event list is true the ASG operator latches the corresponding event inputs. When all events in the list have occurred the operator is satisfied and indicates TRUE. The event inputs are then reset.

5.4.3 Time Related Events

Time related alarm detection requires another variable to be examined when evaluating the logic expression. Both the time of occurrence of the event and the state of the event are required. To describe the alarm detection discussed previously an additional two event types are also necessary.

The TREND event type indicates that the derivative of process variable data with respect to time is compared to event limits when evaluating the event status. Refer to Table 5-2.

For completeness the event type TDEVI is included which is analogous to the event type deviation (DEVI). The absolute and band basic alarm detection functions can both be adequately described with a single event type by careful assignment of the event parameters. This topic is discussed in the appendix (p 248).

Sequence detection requires the evaluation of a time ordered occurrence of events. The SEQ-TIL operator proposed here adequately describes simple and conditional sequence detection as follows:

Alarm 8 = SEQ EVENTA, [EVENTB], [EVENTC] TIL xx

The SEQ-TIL operator signifies that the times of occurrence of the events are used to evaluate the condition statement. Leading and succeeding parameters enclosed in brackets on the events within the event list define the time window within which the event must occur after the occurrence of the first event in the sequence. The detection of the first event in the sequence defines the valid time window during which the sequence detection is valid. For this reason the selection of the first event is critical as discussed in Chapter 4. The TIL operator signifies the end of the sequence detection and also assigns the time limit or maximum time window during which the sequence detection is valid. The first event may be substituted with the symbol TCK for clock linked sequences when the system clock is

<u>EVENT TYPE</u>	<u>PROCESS DATA TYPE</u>	<u>BASIC ALARM DETECTION FUNCTION</u>	<u>EVENT PARAMETERS</u>
TREND	analogue	absolute or band	variable derivative limits between which the event is true
TDEVI	analogue	deviation	variable derivative limits above and below which the event is true

Table 5-2 Time Related Event Types

selected to start the sequence detection. Note that the first event in the sequence can not be assigned a time window. The full SEQ-TIL syntax is as follows:

SEQ <fe>, [

fe = first event, can be substituted with TCK for
system clock

st = start of time window

et = end of time window

mt = maximum time for sequence evaluation

Note that there is no logic diagram equivalent for the sequence operator.

5.5 EVENT PROCESSING

The processing of events requires two procedures as illustrated in Figure 5.7:

- 1) Evaluation of events to determine if the event has occurred as defined by the event type.
- 2) Evaluation of alarm condition statements containing events.

Continuous and binary plant data is converted into a table of events containing the TRUE/FALSE event status as evaluated from event type definitions. The table represents the operational status of the plant in binary form and so is therefore called the event status image. This format is suitable for processing by enhanced Boolean expressions

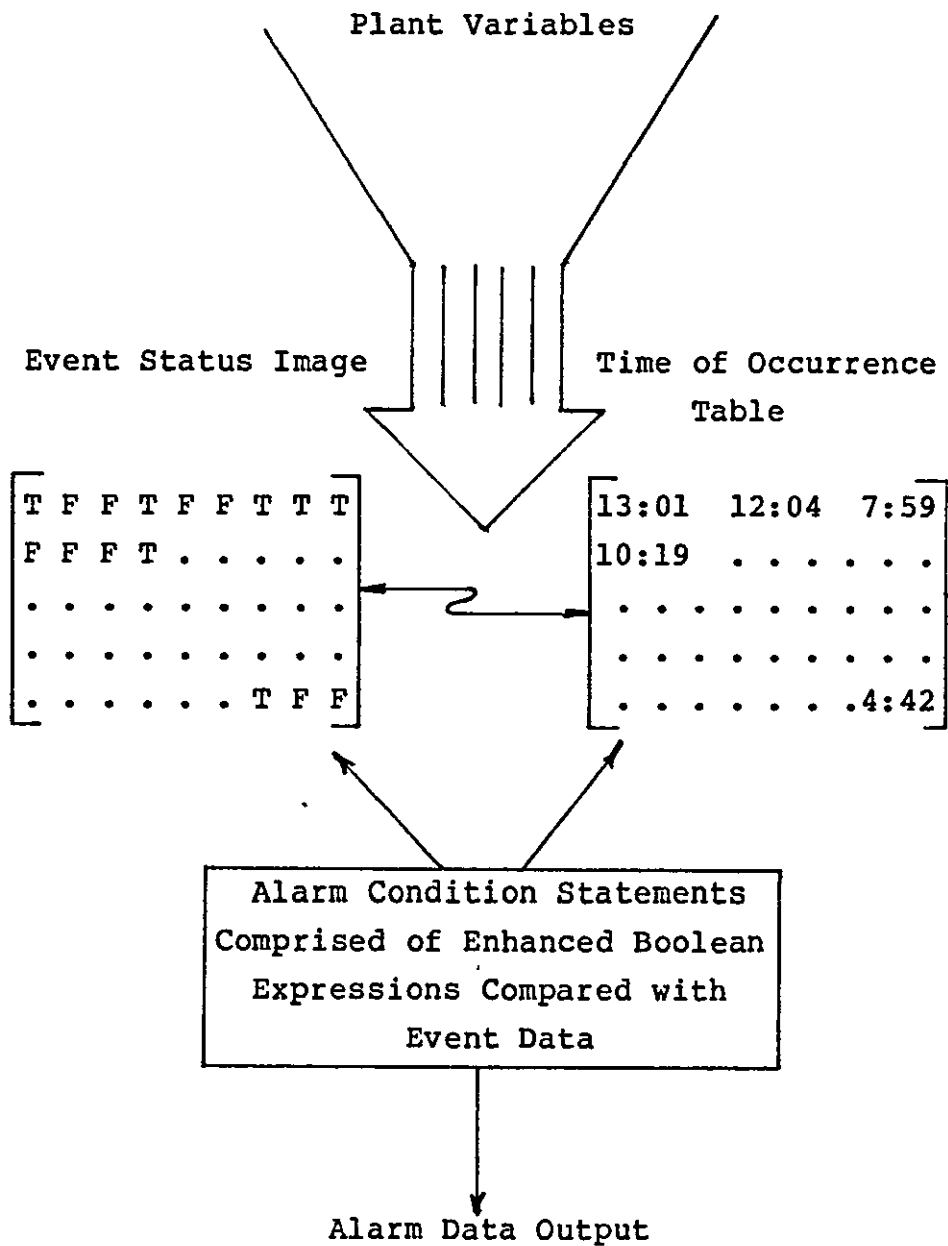


Figure 5.7 Intermediate Event Processing

which are used to describe and define alarm conditions.

Alarm condition statements can then be compared with the event status image to determine whether an alarm condition is present. Recall that the time of occurrence is also required for evaluating time related alarm detection operators. The event status image must therefore reference an additional table containing time of occurrence data for events in the image.

Up to this point the acquisition of data from the plant has not been considered. The proposed alarm handling system is intended to function independently of other plant equipment therefore necessitating to be performed by the alarm handling system. Data acquisition often requires a large amount of overhead in a computer system in addition to a significant amount of stored data including retrieval and processing information such as data source, range parameters, conversion algorithms, etc. It has been assumed that the data acquisition processing is performed as a task separate from event processing. Segregation of the data acquisition task means that event definition parameters are used to evaluate process data which has already been converted into a convenient data format. As a result, event definitions must also contain some reference to the process variables concerned.

The advantage here is that any one variable may be used in a number of event definitions. In the same manner any event can be used in a number of alarm condition statements. Figure 5.8 illustrates the versatility of this three step procedure.

Finally, to provide additional flexibility to the process, two alarm condition statements are proposed for each alarm. One statement is used to define the alarm ON

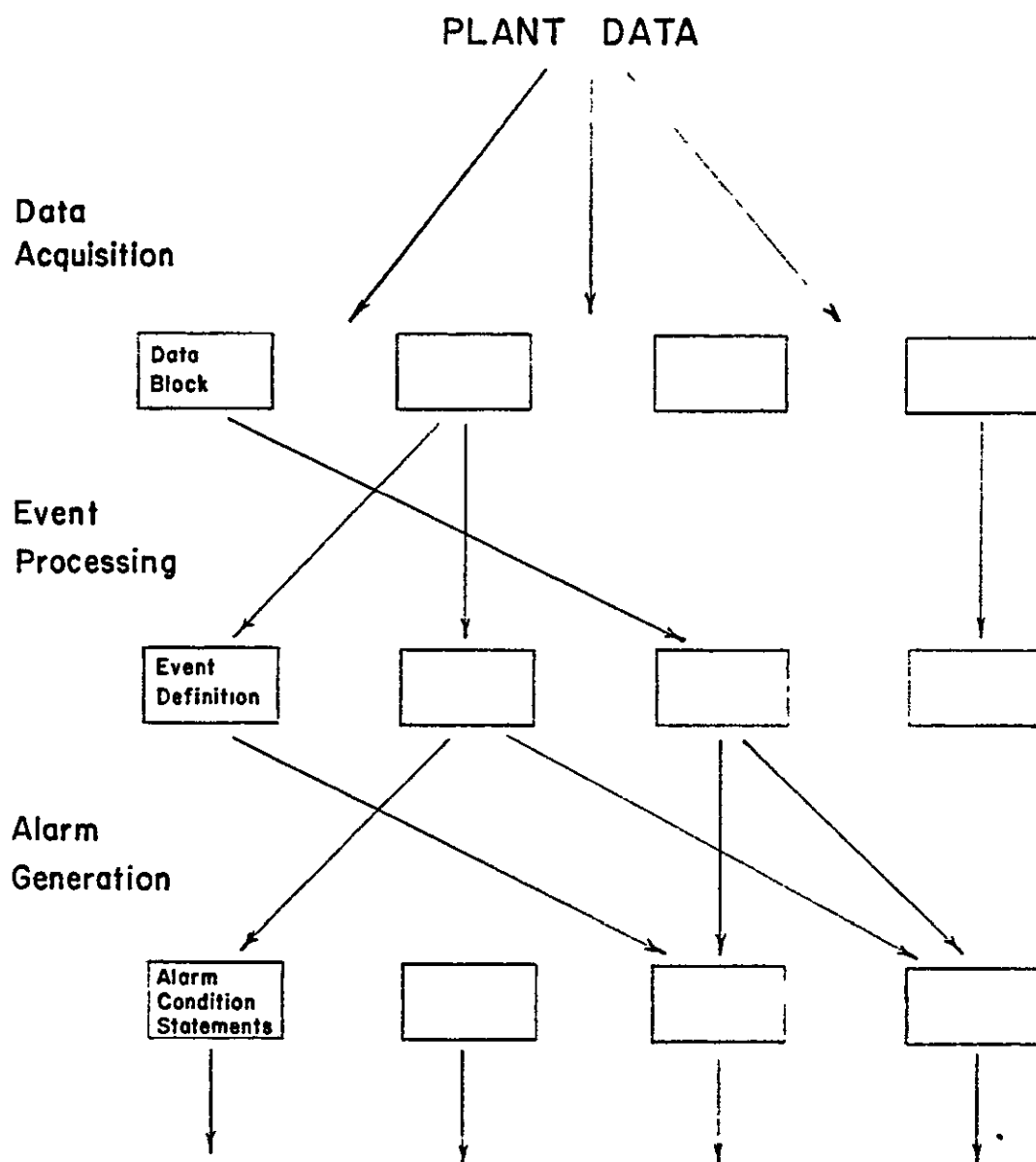


Figure 5.8 Three Step Alarm Detection Using Events

plant conditions and the other to define the alarm OFF plant conditions thus allowing one set of conditions to turn ON and alarm while another possibly different set to turn the alarm OFF.

Alarm detection using events as discussed here therefore suggests a three step procedure:

- 1) Acquisition of the appropriate process data from plant sensors and other sources. Data acquisition involves the collection of plant data and the subsequent processing of the data to produce usable data. This includes the ability to convert a variety of data types into a suitable uniform data structure. The system would necessarily require access to information about data sources such as data type, range parameters, conversion algorithms, etc.

- 2) The conversion of plant data into events consists of the evaluation of process data to establish whether an event has occurred and if so whether the event still exists. This process requires information regarding the plant conditions pertaining to the event such as the data acquisition sources, event parameters, event type, etc. The conversion of plant data into events produces a binary 'image' of the operating conditions of the plant as defined by the event definitions. This conversion translates the plant data obtained during data acquisition into a binary representation which is easy to process using enhanced Boolean alarm condition statements.

- 3) The translation of event data, the event status image, into alarm conditions completes the alarm detection process. The Boolean expressions are evaluated producing either a TRUE or FALSE result based upon event time of occurrence and event status information contained in the event status image.

5.6 USER PROGRAMMING AND PROCESSING STRUCTURES

The intermediate event detection process as described suggests both a user programming and an alarm detection processing strategy. The three tier structure implies the following programming procedure as illustrated:

1) Define data acquisition blocks:

DA BLOCK NAME: Reactor Vessel 2 Temp

DATA SOURCE: Defines where and how the system is to retrieve the process data.

CONVERSION INFORMATION: Algorithms for the conversion of data into a usable format.

RANGE INFORMATION: Needed for conversion and validity checking.

2) Define events using the data blocks:

EVENT NAME: Reac Temp HI

DA BLOCK NAME: Reactor Vessel 2 Temp - DA block to be referenced.

EVENT TYPE: HI - indicates form of data processing.

EVENT PARAMETERS: includes limit values, hysteresis percentage and timeout limits.

3) Define alarm conditions using events:

ALARM NAME: Reactor Vessel 2 Over Temp

OUTPUT CODE: alarm tag number to be passed on to the alarm display system.

ON CONDITION: Reac Temp HI

OFF CONDITION: NOT Reac Temp HI

The ON/OFF condition statements are the Boolean expressions containing events already defined.

Note that hysteresis and timeout features are implemented in the event definition. Hysteresis specifications effect the event range limit values and are therefore included at this point. The operational aspects of hysteresis are discussed in the appendix. Timeout is a function which limits the maximum time the event is to be considered true after the time of occurrence of the event. Consequently timeout is also an additional event parameter included in the event definition.

The alarm detection processing strategy is also a three tier structure which would best be implemented in a multi-tasking computer system based on three core tasks:

- 1) Data Acquisition
- 2) Event Processing
- 3) Alarm Generation

The programming and processing strategies of the proposed alarm handling system are discussed in detail in

5.7 BENEFITS OF EVENT DESCRIPTIONS

The use of events to describe alarm conditions can be useful for the following reasons:

1) Alarm conditions are relatively easy to express with events. As discussed in earlier sections, there are many parameters which must be assigned when defining alarm detection functions including data acquisition information, data processing, alarm limits, etc. By dividing the alarm definitions into smaller sections such as events, the complexity of alarm definitions can be reduced. This is advantageous from both the users point of view and data processing.

2) Events reduce repeated detection of plant conditions when identical plant conditions appear in more than one alarm definition. The event defined only once is referenced in alarm condition statements thus reducing the complexity of the statement while also reducing the amount of computer memory required to store the information and reducing the amount of processor time required. The same argument applies to the use of data acquisition blocks.

3) Events simplify the user's interaction with the alarm system during programming by reducing the amount of detailed information required for defining individual alarms. Once the user has defined data acquisition blocks, the blocks can be referenced for event definitions, and so on.

4) The most significant benefit of using events is that events can be readily translated from conventional

cause-consequence, failure mode and effect, or fault tree analysis of process plant. Although the three tier alarm detection process is not well suited for processing large amounts of this data, it does mean that the system can emulate simplified alarm analysis techniques.

5.8 STORAGE OF ALARM HANDLING DATA

There are two distinct methods of storing data in a computer system:

- 1) Data base
- 2) Special programs

The data base method uses a general purpose program which utilizes the data base to define the functions that the program is to perform. The data base is a personality module which selects the system functions to be performed as required.

An alternative is to write special programs for specific applications which define the alarm functions to be performed.

The data base method has many advantages as follows:

- 1) Alterations to alarm data do not require reprogramming of the system software.
- 2) Less memory space is required to store the condensed data base information.
- 3) The contents of the data base are more accessible to the user thus necessitating less direct collaboration

with software personel.

4) The execution of data base information is faster since the data can be coded in such a manner as to reduce processor time.

An additional program is required when using the data base method to supervise the insertion of alarm data and perform the subsequent operation to transform this data into a condensed form to build the data base. Additional programs are necessary for loading the data base into the general purpose alarm handling program.

Usually the practice is to implement two computer systems. The OFF-line computer system contains the program software for supervision of data base loading. The ON-line or target computer contains the general purpose alarm handling software. This technique is used in the implementation of the prototype alarm handling system described in the next chapter.

CHAPTER 6

IMPLEMENTATION OF AN ALARM HANDLING SYSTEM

6.1 INTRODUCTION

This chapter describes a proposal for a fully operational alarm handling system. The prototype design is based on findings discussed in chapters 3, 4, and 5. In chapter 4 some identifiable alarm detection functions have been analysed followed in chapter 5 by a method of using events to describe alarm conditions. As discussed in chapter 3 there would appear to be a need for a general purpose alarm handling system for process plant. The alarm handling system presented here implements these findings and provides a flexible study tool for further research on alarm systems in general. The examination of practical plant constraints, operator requirements, the shortcomings and virtues of existing alarm systems, and computer and instrumentation limitations clearly indicates an approach to system design. This chapter also discusses a justification for alarm handling systems along with a description of the subsequent prototype design.

6.2 SUMMARY OF THE PROBLEM

In the process plant control room alarms are used to indicate abnormal plant operational conditions to the operator. It is the operator's task to observe the alarms and other plant information displays and detect plant abnormalities. The operator should be able to diagnose the cause of plant malfunctions and to deduce the corrective

action which is required to rectify the situation. The function of the alarm system is to aid the operator in his control tasks. The design of an alarm system depends on a large number of factors. There are many questions which come to mind when examining alarm system designs. The effectiveness of an alarm system is of course dependent on a wide variety of factors which are often difficult to identify and even more difficult to define.

Viewpoints consistently expressed in the literature reflect these difficulties often adding the comments that the process plant alarm system is frequently inadequate and poorly thought out. However, the literature offers few suggestions for improving or even defining alarms and alarm systems.

Alarm system performance is known to be modified by the method of presentation of alarm and process information to the operator. The layout of the control room, information density and information accuracy are good examples of factors which significantly contribute to the effectiveness of an alarm system. Unfortunately much of the data on the effect on performance is empirical and anecdotal, primarily due to the involvement of the operator who is largely an unknown factor. The mechanisms of interaction between the operator and the alarm system have not been fully identified or defined. The interaction between the alarm system and other operator support systems also effects alarm system performance but again the mechanisms have not been clearly identified or quantified. The recognition that an alarm system is in fact a man-machine interface or an operator support device focuses the attention of the investigator on the ergonomic qualities of the alarm system. The integration of the alarm system into the plants overall control system necessitates that the alarm system designers have an adequate appreciation of the systems ergonomic

design and what effect their design factors can have on the overall performance of the system. The ergonomic design of a man-machine interface will have a significant effect on the ability of the alarm system to effectively communicate with the operator and vice versa. The question of how to design an alarm system with good ergonomic qualities is difficult to answer. However, from previous studies in the literature some important factors are known to have notable effects on system performance such as:

1) Spatial orientation of information. This is the combined effect of the layout of all operator displays in the control room including alarm annunciators and VDU's.

2) Accuracy of information presented, especially important when considering alarms. Inaccurate alarms or false alarms contribute to degrade the operator's confidence in the alarm system.

3) Irrelevant alarms which are superfluous or do not represent true alarm conditions can distract the operator.

4) Information overload. In some cases the operator can be overcome by large quantities of alarms and other process data during malfunction situations resulting in the loss of important alarm information or causing the operator to 'mind set'.

An analysis of alarm requirements for identifying alarm conditions in a wide range of plant types has identified that the plant type and process configuration to a large extent indicate the types of functions which should be available in a particular alarm system. Again though we are confronted with difficult questions regarding the interaction between the alarm system and the operator. The level of plant and/or process complexity also effects alarm

system design.

The level of plant operational risk effects the choice of the alarm system used. For example the nuclear industry uses processes which are relatively simple and easy to control yet due to the high operational risks, the alarm systems on such a plant have been given much attention. In the case of nuclear plants a principal operational risk is the release of radiation to the public. Alarm analysis or disturbance analysis systems have been a result of the keen interest in the use of nuclear plant alarm systems to reduce risks. The alarm system is a means of reducing the operational risk by increasing the operator's ability to detect dangerous conditions, to diagnose the plant fault, and to correctly develop an action strategy to rectify the situation.

The same idea applies to chemical processes where the operational risks may have different priorities such as equipment damage, process material loss, or personal safety. The goals of the alarm system design are similar however, where for example the emission of dangerous substances may not exist, the extra cost of having a comprehensive alarm system may not be justifiable. If the probability of a mishap is low, the cost of correcting the mishap, if it does occur, can be the same or less than the cost of upgrading the alarm system to detect the malfunctions. Also if the probability of a hazard occurring is very low, the expenditure for improving the alarm system cannot be justified.

Due to the large number of factors which contribute to the effectiveness of the alarm system, often the best approach is unclear. In general the designer can reasonably ascertain the category of alarm system required based principally on the plant complexity and the process risk.

However, the best design or configuration of the alarm system cannot easily be deduced due to the large number of ergonomic considerations, which are difficult to identify during the design stage. The alarm system design difficulties are compounded by the fact that much of the ergonomic principles in an alarm system are not fully understood, thus requiring the system to be 'tuned' or modified when in service.

Studies of existing alarm systems show that there are many improvements which could be made to enhance the performance of the traditional alarm systems. The studies also indicate that computer based alarm systems are frequently used to mimic traditional hardware systems instead of using their inherent computing capabilities more productively. The highly sophisticated alarm analysis or disturbance analysis systems are usually regarded as too complex and costly for most process plant applications.

Clearly there is a gap in the level of technology applied to alarm systems on process plant. At one end of the scale are the conventional alarm system and at the other end the complex alarm analysis or disturbance analysis systems. A computer based alarm system could readily enhance the simpler systems and provide some simplified forms of alarm analysis. A combination such as this would comfortably fill the technology gap which is now present. This approach would also be consistent with the flexible design requirements by facilitating a rich variety of alarm functions.

The objective of the exercise then is to propose an alarm system which will:

- 1) adequately deal with as many as possible of the identifiable types of process plant and process alarms.

2) fill the technology gap in existing methods for dealing with alarms on process plant.

3) aid in the identification of an alarm system design methodology by producing a basic tool for further studies.

6.3 ALARM HANDLING

The term alarm handling is used to describe the system presented here since the technique encompasses all commonly accepted means for dealing with alarms. Also, alarm handling is a passive system of dealing with process alarms, that is, no prime cause analysis or action strategy messages are generated. The alarm system manipulates or handles existing plant alarms and process information in such a way as to make the information displayed to the operator as accurate, concise and comprehensible as possible. The system should also provide the means to deal with all categories of alarms and as many varieties of plant process types as possible.

6.4 ASSUMPTIONS

As the term alarm handling implies, the system presented here is intended to implement alarm detection techniques. No attempt has been made to define methods of identifying alarm requirements on a plant or how to establish alarm limits, etc.

The alarm handling system should be an integrated part of the overall plant control loop supporting the operators in their control and diagnostic tasks. Before a system specification can be developed it is necessary to define the

alarm handling system functions in order to establish the borderline between the alarm handling system and other plant control systems.

A number of assumptions have been made with respect to the alarm system functions and the technological level at which the system should be aimed.

The type of hardware used to implement the alarm system also has to be selected. This selection is made from the range of technologies readily available.

The fundamental system assumptions presented here are based on judgement and conclusions of previous studies.

1) The function of the alarm handling system should be to aid the operator with his control task. The operator support will be in the form of aiding the

- a) detection of plant malfunctions.
- b) malfunction diagnosis.
- c) correction of plant malfunctions.

2) The alarm handling system will be passive in nature thus providing no prime cause analysis, consequence prediction or corrective action strategy messages.

3) The alarm handling system is an information system only. It is the operator's responsibility to make adjustments to the control system. The alarm handling system will provide no feedback to any part of the plant. Plant information flow will be from the plant to the operator only.

4) The system will present alarm information only in the form of status- i.e. binary, indicators. Any presentation of analogue process data information will be supplied by other operator support systems.

5) The system should have the capability to generate alarm information such as event or alarm status and be capable of logging such information. The system will not be considered to have event logging functions except in the case of events and alarms detected by the alarm system.

6) The alarm handling system will be self-contained and independent of external support.

7) The system will be computer based.

8) Computer driven displays including colour VDU's, coloured alarm annunciators and printers will be used to present alarm and event information to the operator.

9) The system will be capable of dealing with all types of commonly accepted alarm types.

10) The system will be capable of dealing with alarm and event information from both sequential and continuous operations.

11) The system will be targeted for small plant applications with an approximate limitation of 250 alarms.

12) The system time resolution, that is the time from event occurrence to the time that the system displays an event will be of the order of 1 sec.

The sort of functions to be available in a generalized alarm handling system are as follows:

a) Basic alarm detection including Absolute, Deviation, and Trend.

b) Deduced alarm detection including Group, Logical, and Mode.

c) Sequential and other time related alarm handling.

A principal objective of this project was to develop an approach to alarm system design which could be used as a tool to examine as many aspects of alarm detection, generation and display as reasonably possible. The areas of flexibility in design and operation therefore include:

1) The generation of alarms and alarm information.

2) Universal applicability to all types of plants.

3) Versatile provisions to display information to the operator which would include as many forms of alarm display presently used as possible.

4) Retrofit capabilities.

5) Parallel operation capabilities with existing plant control and alarm systems.

6.5 PROJECTED BENEFITS

Clearly the selection of an alarm system is difficult. Predicting the performance of an alarm system is also difficult because there are many unknowns.

We can however hypothesize the benefits of an alarm

handling system based on examination of the performance of existing systems for dealing with alarms:

- 1) Reduction the number of irrelevant alarms presented to the operator.

- 2) Provision of a means to readily change the system as required.

- 3) Improvement of the quality of alarm information.

- 4) General improvement of the man-machine interface.

The results would be:

- 1) A reduction in the operator's response time in the detection, diagnosis, and correction of abnormal plant conditions.

- 2) An increase in the number of correct operator action strategies.

- 3) A general improvement of the operator's ability to deal with plant conditions thus reducing plant loss, down time, etc.

6.6 THE ALARM HANDLING SYSTEM

The alarm handling system is comprised of two major sections, an OFF-line system and an ON-line system. The OFF-line system is used to generate the data base which describes the functions of the alarm system. The ON-line system is the operational portion of the alarm handling system, using the OFF-line generated data base. Separation of the system functions is useful for the following reasons:

1) It allows OFF-line data base development to be performed at ease without interfering with ON-line operation.

2) A variety of different alarm data bases can be developed, evaluated and archived.

3) The ON-line system capacity need not be as large since OFF-line development programs can require large sections of memory space, therefore necessitating a larger ON-line computer capacity which may not be required once initial development is completed.

4) Language capabilities of OFF-line; for example a different more appropriate OFF-line language can be implemented.

5) Conversational mode more easy to implement.

6) Can modify and test OFF-line without disrupting ON-line.

7) Location of OFF-line system more convenient to engineering staff.

The ON-line portion of the alarm handling system is located on the plant and performs the alarm handling functions in real time. The system is intended to be able to accomodate a wide variety of alarm systems and process configurations. The ON-line alarm handling system hardware, which remains the same for all system configurations, is programmed differently to meet individual plant requirements. Generally the core section of the ON-line alarm handling software also remains the same for all system configurations. The personality of the system is determined

by inserting appropriate data base modules. Therefore the specific alarm functions to be performed for a particular plant application are assigned by an alarm data base which is generated OFF-line. By using a data base to set the system functions, the hardware and software systems can be well defined. They can however be easily modified before or after commissioning.

6.6.1 Overview

The alarm handling system is comprised of two major software packages:

- 1) The Off-Line Alarm Data base generator (OFLAD)
- 2) The On-Line General Purpose Alarm Handling System

In brief the user programs the computer based on-line alarm handling system by inserting alarm and other plant information into the off-line system which builds a coded alarm data base for the on-line system. The on-line system is comprised of a general purpose alarm handling software package installed in a stand alone microprocessor based computer system. The on-line system is capable of executing alarm functions as coded in the alarm data base. Once the alarm data base is installed in the on-line computer, the alarm handling system is capable of performing all data acquisition, alarm detection and alarm display independently of other existing process control equipment.

All of the alarm functions discussed in chapter 4 with the exception of ASG have been implemented using the event detection method described in chapter 5. The alarm handling functions are discussed and summarized in chapter 7 (see tables 7-1, 7-2, and 7-3). The off-line system data input routines have been formatted in such a manner as to reflect the data acquisition, event definition, and alarm generation functional blocks. The off-line alarm handling system is

discussed here first to give the reader an idea of the type of data which is contained in the alarm data base that is subsequently used to define the operation of the on-line system. This is important since there is little interaction between the user and the on-line system to demonstrate the available functions.

6.6.2 The Off-Line System

The off-line alarm data base generator (OFLAD) is based on a Chromatics CG 1999 colour graphics microcomputer system which, for the purpose of the prototype, doubles as the on-line alarm display system. See Figure 6.1. The off-line software written entirely in Microsoft BASIC provides an operating system capable of performing all functions required for the user to:

- 1) Interactively load alarm and plant information into the computer via question and answer input routines. The data is stored in source files which can be stored or edited.
- 2) Manipulate and edit plant data source files as required for corrections or modifications.
- 3) Coordinate and execute the compilation of these plant data source files into a condensed alarm data base ready for insertion into the on-line system.
- 4) Supervise and execute the linking of the off-line system with its on-line counterpart and then transfer alarm data bases from the off-line to the on-line system.

The off-line program is restricted by the available memory in the off-line computer. As a result the software package structure is comprised of three separate BASIC



Figure 6.1 The Chromatics CG 1999
performing Off-Line duties

programs which interact without user intervention. Since it is desirable to maximize the amount of memory available for user data, the individual programs are kept as short and concise as possible. The resulting program modules maximize the memory space available for data handling. The three program modules are:

- 1) Off-Line System Monitor and Data Input Routines (OFLAD)
- 2) The Data Compiler (COMP)
- 3) The Data Base Loader (TRANSFER)

A detailed description of the operation of the complete off-line system can be found in Appendix B which contains the User's Guide for the Off-Line Component of the Alarm Handling System. Appendix C contains the Software Description for the Off-Line Component of the Alarm Handling System document which discusses details of the software including program listings. A summary is presented here of the operation of the off-line program modules with an example printout.

6.6.2.1 OFLAD

The off-line system monitor and data input routine program module comprises the off-line operating system and alarm and plant data input routines. The operating system recognises commands used to evoke the various function available in the off-line system.

After consultation with Dr. I.G. Umbers, an ergonomics specialist in the Department of Industry, it was decided that initially the best approach for inputting plant and alarm information into the off-line system was via question

and answer routines. An off-line operating system was developed to coordinate the input routines by means of system commands. The structure of the operating system closely follows the data input procedures discussed in chapter 5.

The data input routines are essentially data file editors which allow the user to perform various editing functions on any of the data file areas (working files) which correspond to the three major alarm handling functions; data acquisition, event processing, and alarm generation. These source data files can be built, examined, and stored. Similarly previously developed data files can be examined, modified, deleted, etc. The three working file areas are:

- 1) DA - data acquisition block definitions.
- 2) EP - event processor definitions containing event types, limits, etc.
- 3) AG - alarm generation definitions containing alarm condition statements.

It may be useful to refer to the example printout in section 6.6.2.4 while reading the following description. For a particular alarm handling system application, the user must fully define all data acquisition blocks available to the alarm system. Data acquisition definitions include all data describing where and how to obtain plant data from a particular plant data source. Each data acquisition block definition is identified by a 'plant code' which is used to reference the data acquisition block in the event definitions. A DA source file contains all DA blocks to be used in the alarm handling system.

The EP or event processor file is constructed in a similar manner. Question and answer routines guide the user in the input of event type, range parameters, DA block references, and event names. The event name is used to identify a particular event so that it can be referenced in alarm condition statements. Each event corresponds to an individual data acquisition block. A data acquisition block may be referenced as often as required. The present version of the alarm handling system only supports single data acquisition block references in an event definition.

Lastly, the alarm condition statements, one for the ON-condition and another for the OFF-condition, are inserted into the AG (alarm generator) source file defining all alarms in the system. This file contains the alarm name for user reference, the output alarm tag code to be sent to the alarm display system when a change in alarm status is detected, and the Boolean condition statements as described in chapter 5.

Each of the working files DA, EP, and AG can subsequently be stored or modified as required. Note that no alarm display data is included at this point. The alarm display system is treated as a separate unit as explained in section 6.6.3. There are three separate source files to facilitate editing and alarm data base construction.

The OFLAD system commands evoke all data input, editing, and file manipulation functions including the execution of the other two off-line program modules. Once all plant and alarm data has been inserted into source files, the system command COMP is entered to load the alarm data base compiler program module into the computer. With an alarm data base (ADB) successfully compiled it can be transferred to the on-line system via the TRANSFER command which loads the TRANSFER program module into the system.

6.6.2.2 COMP

The alarm data base compilation program module builds an alarm data base coded in such a manner as to minimize on-line processing time and required memory space. Refer to the example in Figure 6.4. The alarm data base is constructed from the three source files. A DA, an EP, and an AG source file must be specified for compilation. Any files may be used however all data acquisition blocks referenced in the EP file must be defined in the DA file. Similarly all event referenced in the AG file must be defined in the EP file.

During compilation all references are cross correlated and checked for errors. The functions performed during compilation are briefly described here. Data acquisition blocks are sorted according to scan rate and priorities and allocated memory locations in the on-line system. Event definitions are sorted and data acquisition block references are checked. Alarm definitions are sorted, event references checked, and the Boolean ON/OFF condition statements are evaluated for validity and then coded.

If any errors are generated during compilation the procedure is aborted and program control returns to the system monitor. After a successful compilation the condensed alarm data base is stored ready for transfer to the on-line system.

Often a trade-off must be made because minimum alarm data base memory space generally causes increased execution time and vice versa. The format of the ADB presently used is not necessarily the best. The ADB construction and format is discussed in Appendix E.

6.6.2.3 TRANSFER

The transfer program module supervises the transfer of the coded alarm data base to the on-line system. An example of the use of the software can be found in Figure 6.5.

The alarm handling system programming procedure is summarised in Figure 6.2. It has been noted that often there are modifications required to an alarm system during and after commissioning. Once an initial set of source files and the corresponding ADB have been built, modifications can be readily made to the system by adjusting the source files and compiling another ADB. On-line data base editing facilities have been included however it is not recommended that this be used except for prototype work.

6.6.2.4 Example Use of Off-Line System

Figure 6.3 illustrates a typical usage of the OFLAD system monitor and alarm and plant data input routines. Individual data acquisition blocks, events, and alarm definitions are loaded into working files and then the three working files are stored. In the example, one data acquisition block, two events, and one alarm are entered.

Figure 6.4 shows what output the user can expect during compilation of an alarm data base. The first listing shows a successful compilation, while the second illustrates a compilation with errors.

The transfer procedure is shown in Figure 6.5. Here a data base is being successfully transferred from the off-line system to the on-line system.

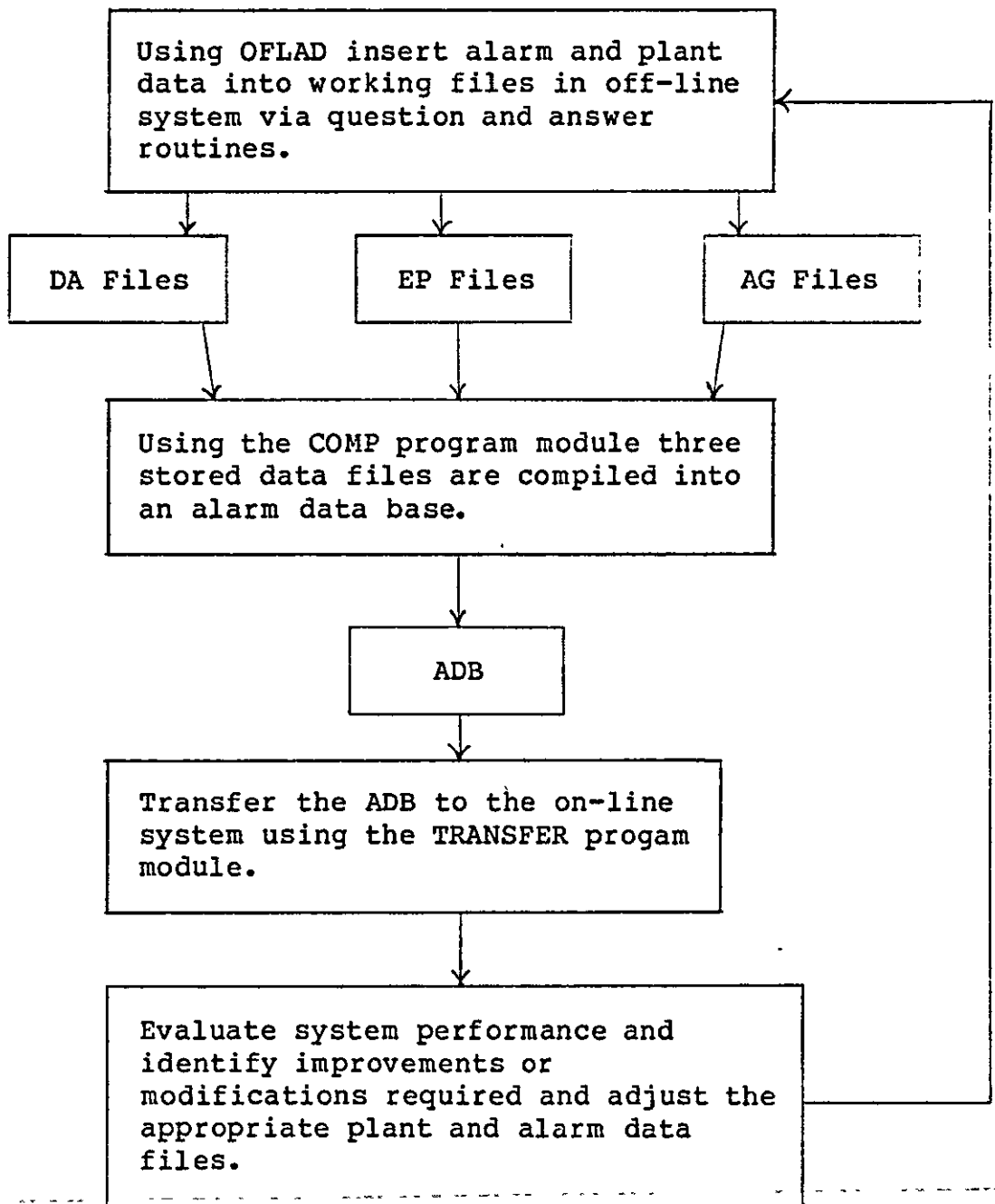


Figure 6.2 Summary of System Programming Procedure

---- FILE DIRECTORY ----
FILE NUMBER - NO. OF ELEMENTS

DA
1 - 10 5 - 2
EP
30 - 10 35 - 2
AG
60 - 10 65 - 2
ADB
90 - 235

COMMAND:HELP

ENTER
CHANGE
DIRECTORY
LIST
LOAD
STORE
HELP
FILES LOADED
COMPILE
DELETE
TRANSFER

COMMAND:LOAD

DA FILE NUMBER: 2
NEW FILE
EP FILE NUMBER: 31
NEW FILE
AG FILE NUMBER: 61
NEW FILE

Figure 6.3 OFLAD Example

COMMAND:ENTER

ITEM:DA

INPUT DATA ACQUISITION INFORMATION

PLANT CODE []:T610

NAME []:TEMP 610

INPUT DEVICE []:3

DATA TYPE []:A

CONVERSION ALGORITHM # []:2

RANGE []:32 212

SIGNIFICANT ABSOLUTE CHANGE []:.1

SCAN RATE []:1

SCAN PRIORITY []:3

END OF DA UNIT INPUT

COMMAND:ENTER

ITEM:EP

Figure 6.3 OFLAD Example (Continued)

INPUT ANALOG EVENT PROCESSOR INFORMATION

PLANT CODE []:T610

EVENT NAME []:TEMP V LO

EVENT TYPE []:XLO

ENTER RANGE LIMIT PARAMETERS

1 []:33.1

2 []:34

3 []:41.4

4 []:42.3

END OF ANALOG EVENT PROCESSOR INPUT

COMMAND:ENTER

ITEM:AG

INPUT ALARM CONDITION INFORMATION

ALARM NAME []:EVAP TOO COLD

OUTPUT CODE []:145

CONDITION ON []:TEMP*V*LO AND CONTACT2

CONDITION OFF []:NOT CONTACT2

Figure 6.3 OFLAD Example (Continued)

PERSISTENCY []:1

END OF ALARM CONDITION INPUT

COMMAND:ENTER

ITEM:EP

INPUT ANALOG EVENT PROCESSOR INFORMATION

PLANT CODE []:S202

EVENT NAME []:CONTACT2

EVENT TYPE []:OFF

ENTER RANGE LIMIT PARAMETERS

1 []:

2 []:

3 []:

4 []:

END OF ANALOG EVENT PROCESSOR INPUT

Figure 6.3 OFIAD Example (Continued)

COMMAND:CHANGE

ITEM:AG

ALARM NAME TO BE CHANGED:EVAP TOO COLD

INPUT ALARM CONDITION INFORMATION

ALARM NAME [EVAP TOO COLD]:

OUTPUT CODE [145]:

CONDITION ON [TEMP^V^LO AND CONTACT2]:

CONDITION OFF [NOT CONTACT2]:NOT (TEMP^V^LO AND CONTACT2)

PERSISTENCY [1]:

END OF ALARM CONDITION INPUT

COMMAND:STORE

RETURN = STORE NO CHANGE IN FILE NUMBER.

'N' = DO NOT STORE.

'NF' = STORE WITH NEW FILE NUMBER.

'K' = KILL WORKING FILE.

STORE DA 2 ?

STORE EP 31 ?

STORE AG 61 ?

COMMAND:

Figure 6.3 OFLAD Example (Continued)

----- FILE DIRECTORY -----
 FILE NUMBER - NO. OF ELEMENTS

DA
 1 - 10 5 - 2
 EP
 30 - 10 35 - 2
 AG
 60 - 10 65 - 2
 ADB

DA FILE NO.? 1

EP FILE NO.? 30

AG FILE NO.? 60

ADB NO.? 90
 ARE YOU SURE? Y
 HARD COPY (Y/N)? N

S202 CONTACT 2 2 N 4 7
 F234 FLOW 234 1 A 3 0 200 3 1 .3
 F111 FLOW 111 1 A 2 0 100 2 1 .2
 T610 TEMP 610 3 A 2 32 212 1 3 .1
 P690 PRESS 690 1 A 1 0 100 2 3 .2
 P333 PRESS 333 0 Y 4 1
 F111 FLOW 111 1 A 3 0 200 2 3 .2
 T890 TEMP 890 3 N 1 1
 F203 FLOW 203 1 A 1 0 100 1 10 .1
 S101 CONTACT 1 1 N 1 10

Figure 6.4 COMP Example

PLANT CODE	NAME	I/P DEV	TYPE	ALG NO.	RANGE	SCAN	PRIORITY
T890	TEMP 890	3	N		()	1	1
T610	TEMP 610	3	A	2	32 212 (.1)	1	3
F203	FLOW 203	1	A	1	0 100 (.1)	1	10
S101	CONTACT 1	1	N		()	1	10
*F111	FLOW 111	1	A	2	0 100 (.2)	2	1
F111	FLOW 111	1	A	3	0 200 (.2)	2	3
P690	PRESS 690	1	A	1	0 100 (.2)	2	3
F234	FLOW 234	1	A	3	0 200 (.3)	3	1
P333	PRESS 333	0	Y		()	4	1
S202	CONTACT 2	2	N		()	4	7

**** 1 ERROR ****

I/P ERROR 0

Figure 6.4 COMP Example (Continued)

P690 PRESS HI HI 70 75 89 91
 F111 FLOW HI HI 179 181 195 197
 S202 CONTACT2 ON
 F234 EVAP FLO LO 5 10 25 27
 F203 FLOW TANK TREND 4 4 8 8
~~T610 TEMP V LO RUN 40 42 50 52~~
 T610 TEMP V HI XHI 200 200 212 212
 F234 EVAP FLO LO 10 12.3 23.1 30
 S303 CONTACT3 OFF
 T610 TEMP V LO LO 33.1 34 41.4 42.3

EVENT CODE	EVENT NAME	PLANT CODE	TYPE	L. LIMIT	L. HYS.	U. LIMIT	U. HYS.
E0001	CONTACT2	S202	ON				
E0002	CONTACT3	*S303	OFF				
E0003	*EVAP FLO	F234	LO	5	10	25	27
E0004	EVAP FLO	F234	LO	10	12.3	23.1	30
E0005	FLOW HI	F111	HI	179	181	195	197
E0006	FLOW TANK	F203	TREND	4	4	8	8
E0007	PRESS HI	P690	HI	70	75	89	91
E0008	TEMP V HI	T610	XHI	200	200	212	212
E0009	*TEMP V LO	T610	LO	33.1	34	41.4	42.3
E0010	TEMP V LO	T610	RUN	40	42	50	52

**** 3 ERRORS ****

EP TYPE ERROR RUN

EVAP TOO COLD 145 TEMP^V^LO NOT TEMP^V^LO 1
 FLOW HI 130 FLOW^HI AND CONTACT2 NOT (FLOW^HI AND CONTACT2) 3
 TEMP VERY LO 120 TEM^V^LO NOT TEMP^V^LO 1
 TANK OVERFLOW 119 FLOW^TANK AND EVAP^FLO NOT (FLOW^TANK AND EVAP^FLO) 1
 PRESSURE HI 133 SEQ CONTACT2 PRESS^HI TIL120 NOT (SEQ CONTACT2 PRESS^HI TIL120) 3
 PUMP ON 138 CONTACT2 NOT CONTACT2 1
 RELIEF VALVE NOT OPEN 117 FLOW^HI OR NOT (EVAP^LO AND FLOW^TANK) NOT CONTACT2 1
 TEMP VERY LO 120 TEMP^V^LO NOT TEMP^V^LO 2
 RELIEF VALVE OPEN 116 FLOW^HI OR EVAP FLOW NOT (FLOW^HI AND EVAP^FLO) 2
 OVER TEMP 111 VOT TEMP^V^HI CONTACT2 PRESS^HI NOT TEMP^V^HI 0

Figure 6.4 COMP Example (Continued)

ALARM NAME: EVAP TOO COLD (145)
CONDITION ON: TEMP V LO,
CONDITION OFF: TEMP V LO, NOT,
PERSISTANCY: 1

ALARM NAME: FLOW HI (130)
CONDITION ON: FLOW HI, CONTACT2, AND,
CONDITION OFF: FLOW HI, CONTACT2, AND, NOT,
PERSISTANCY: 3

ALARM NAME: OVER TEMP (111)
CONDITION ON: TEMP V HI, CONTACT2, PRESS HI, VOT,
CONDITION OFF: TEMP V HI, NOT,
PERSISTANCY: 0

ALARM NAME: PRESSURE HI (133)
CONDITION ON: CONTACT2, PRESS HI, TIL, 120, SEQ,
CONDITION OFF: CONTACT2, PRESS HI, TIL, 120, SEQ, NOT,
PERSISTANCY: 3

ALARM NAME: PUMP ON (138)
CONDITION ON: CONTACT2,
CONDITION OFF: CONTACT2, NOT,
PERSISTANCY: 1

ALARM NAME: RELIEF VALVE NOT OPEN (117)
CONDITION ON: FLOW HI, *EVAP LO, FLOW TANK, AND, NOT, OR,
CONDITION OFF: CONTACT2, NOT,
PERSISTANCY: 1

ALARM NAME: RELIEF VALVE OPEN (116)
CONDITION ON: FLOW HI, *EVAP, *FLOW, OR,
CONDITION OFF: FLOW HI, EVAP FLO, AND, NOT,
PERSISTANCY: 2

Figure 6.4 COMP Example (Continued)

ALARM NAME: TANK OVERFLOW (119)
CONDITION ON: FLOW TANK, EVAP FLO, AND,
CONDITION OFF: FLOW TANK, EVAP FLO, AND, NOT,
PERSISTANCY: 1

ALARM NAME: *TEMP VERY LO (120)
CONDITION ON: *TEN V LO,
CONDITION OFF: TEMP V LO, NOT,
PERSISTANCY: 1

ALARM NAME: TEMP VERY LO (120)
CONDITION ON: TEMP V LO,
CONDITION OFF: TEMP V LO, NOT,
PERSISTANCY: 2

**** 5 ERRORS ****

**** COMPILATION FAILED ****

**** TOTAL ERRORS = 11 ****

Figure 6.4 COMP Example (Continued)

----- FILE DIRECTORY -----
 FILE NUMBER - NO. OF ELEMENTS

DA
 1 - 10 5 - 2
 EP
 30 - 10 35 - 2
 AG
 60 - 10 65 - 2
 ADB

DA FILE NO.? 1

EP FILE NO.? 30

AG FILE NO.? 60

ADB NO.? 90
 ARE YOU SURE? Y
 HARD COPY (Y/N)? N

S202	CONTACT	2	2	N		4	7		
F234	FLOW	234	1	A	3	0	200	3	.3
F112	FLOW	112	1	A	2	0	100	2	.2
T610	TEMP	610	3	A	2	32	212	1	.1
P690	PRESS	690	1	A	1	0	100	2	.2
P333	PRESS	333	1	Y		4	1		
F111	FLOW	111	1	A	3	0	200	2	.2
T890	TEMP	890	3	N		1	1		
F203	FLOW	203	1	A	1	0	100	1	.1
S101	CONTACT	1	1	N		1	10		

Figure 6.4 COMP Example (Continued)

PLANT CODE	NAME	I/P DEV	TYPE	ALG NO.	RANGE	SCAN	PRIORITY
T890	TEMP 890	3	N		()	1	1
T610	TEMP 610	3	A	2	32 212 (.1)	1	3
F203	FLOW 203	1	A	1	0 100 (.1)	1	10
S101	CONTACT 1	1	N		()	1	10
F112	FLOW 112	1	A	2	0 100 (.2)	2	1
F111	FLOW 111	1	A	3	0 200 (.2)	2	3
P690	PRESS 690	1	A	1	0 100 (.2)	2	3
F234	FLOW 234	1	A	3	0 200 (.3)	3	1
P333	PRESS 333	1	Y		()	4	1
S202	CONTACT 2	2	N		()	4	7

**** 0 ERRORS ****

Figure 6.4 COMP Example (Continued)

P690 PRESS HI HI 70 75 89 91
 F111 FLOW HI HI 179 181 195 197
 S202 CONTACT2 ON
 F234 FLOW 1 LO 5 10 25 27
 F203 FLOW TANK TREND 4 4 8 8
 T610 TEMP LO LO 40 42 50 52
 T610 TEMP V HI XHI 200 200 212 212
 F234 EVAP FLO LO 10 12.3 23.1 30
 S101 CONTACT1 OFF
 T610 TEMP V LO XLO 33.1 34 41.4 42.3

EVENT CODE	EVENT NAME	PLANT CODE	TYPE	L. LIMIT	L. HYS.	U. LIMIT	U. HYS.
E0001	CONTACT1	S101	OFF				
E0002	CONTACT2	S202	ON				
E0003	EVAP FLO	F234	LO	10	12.3	23.1	30
E0004	FLOW 1	F234	LO	5	10	25	27
E0005	FLOW HI	F111	HI	179	181	195	197
E0006	FLOW TANK	F203	TREND	4	4	8	8
E0007	PRESS HI	P690	HI	70	75	89	91
E0008	TEMP LO	T610	LO	40	42	50	52
E0009	TEMP V HI	T610	XHI	200	200	212	212
E0010	TEMP V LO	T610	XLO	33.1	34	41.4	42.3

**** 0 ERRORS ****

EVAP TOO COLD 145 TEMP^V^LO NOT TEMP^V^LO 1
 FLOW HI 130 FLOW^HI AND CONTACT2 NOT (FLOW^HI AND CONTACT2) 3
 TEMP LOW 121 TEMP^LO NOT TEMP^LO 1
 TANK OVERFLOW 119 FLOW^TANK AND EVAP^FLO NOT (FLOW^TANK AND EVAP^FLO) 1
 PRESSURE HI 133 SEQ CONTACT2 PRESS^HI TIL120 NOT (SEQ CONTACT2 PRESS^HI TIL120) 3
 PUMP ON 138 CONTACT2 NOT CONTACT2 1
 RELIEF VALVE NOT OPEN 117 FLOW^HI OR NOT (EVAP^FLO AND FLOW^TANK) NOT CONTACT2 1
 TEMP VERY LO 120 TEMP^V^LO NOT TEMP^V^LO 2
 RELIEF VALVE OPEN 116 FLOW^HI OR EVAP^FLO NOT (FLOW^HI AND EVAP^FLO) 2
 OVER TEMP 111 NOT TEMP^V^HI CONTACT2 PRESS^HI NOT TEMP^V^HI 0

Figure 6.4 COMP Example (Continued)

ALARM NAME: EVAP TOO COLD (145)
CONDITION ON: TEMP V LO,
CONDITION OFF: TEMP V LO, NOT,
PERSISTANCY: 1

ALARM NAME: FLOW HI (130)
CONDITION ON: FLOW HI, CONTACT2, AND,
CONDITION OFF: FLOW HI, CONTACT2, AND, NOT,
PERSISTANCY: 3

ALARM NAME: OVER TEMP (111)
CONDITION ON: TEMP V HI, CONTACT2, PRESS HI, VOT,
CONDITION OFF: TEMP V HI, NOT,
PERSISTANCY: 0

ALARM NAME: PRESSURE HI (133)
CONDITION ON: CONTACT2, PRESS HI, TIL, 120, SEQ,
CONDITION OFF: CONTACT2, PRESS HI, TIL, 120, SEQ, NOT,
PERSISTANCY: 3

ALARM NAME: PUMP ON (138)
CONDITION ON: CONTACT2,
CONDITION OFF: CONTACT2, NOT,
PERSISTANCY: 1

ALARM NAME: RELIEF VALVE NOT OPEN (117)
CONDITION ON: FLOW HI, EVAP FLO, FLOW TANK, AND, NOT, OR,
CONDITION OFF: CONTACT2, NOT,
PERSISTANCY: 1

ALARM NAME: RELIEF VALVE OPEN (116)
CONDITION ON: FLOW HI, EVAP FLO, OR,
CONDITION OFF: FLOW HI, EVAP FLO, AND, NOT,
PERSISTANCY: 2

Figure 6.4 COMP Example (Continued)

ALARM NAME: TANK OVERFLOW (119)
CONDITION ON: FLOW TANK, EVAP FLO, AND,
CONDITION OFF: FLOW TANK, EVAP FLO, AND, NOT,
PERSISTANCY: 1

ALARM NAME: TEMP LOW (121)
CONDITION ON: TEMP LO,
CONDITION OFF: TEMP LO, NOT,
PERSISTANCY: 1

ALARM NAME: TEMP VERY LO (120)
CONDITION ON: TEMP V LO,
CONDITION OFF: TEMP V LO, NOT,
PERSISTANCY: 2

**** 0 ERRORS ****

**** PASS 1 OK ****

**** COMPILATION OK ****

Figure 6.4 COMP Example (Continued)

ALARM DATA BASE TRANSFER ROUTINE

THE CHROMATICS MUST BE CONNECTED TO THE PDP 11/03.

THE ALARM HANDLING SYSTEM MUST BE INSTALLED AND RUNNING BEFORE PROCEEDING.

A LINK ERROR WILL OCCUR IF THE SET UP IS NOT CORRECT, THUS ABORTING THE TRANSFER.

---- AVAILABLE ALARM DATA BASES ---

ADB

90 - 235

ADB NO. 90

ARE YOU SURE? Y

TRANSFER COMPLETE

COMMAND:

Figure 6.5 TRANSFER Example

6.6.3 The On-Line System

The on-line alarm handling system is based on a Digital Equipment Corporation (DEC) PDP 11/03 microcomputer. The PDP 11/03 is built into a stand alone, roll-around cabinet containing a variety of Fisher Media plant interfaces, power supplies, plant trip detectors, and a small set of Highland Alarm Annunciator Panels. The Chromatics CG 1999 colour graphics computer used for the off-line system is also used for the system alarm display unit. Additionally a special purpose operator keyboard was constructed to be used as the principal operator/alarm system interface. Figure 6.6 shows a schematic of the on-line system configuration. Figures 6.7 through 6.9 are photographs of the prototype equipment. A discussion concerning the selection of the hardware is presented in section 6.7.

The on-line alarm handling software is a generalised program capable of performing alarm handling functions as defined in the alarm data base. The alarm handling system may be thought of as an operating system ready to be programmed for a specific user application. The software package is comprised of two major sections:

- 1) The alarm handling software
- 2) The alarm display software package

The alarm handling software is written entirely in SWEPSPEED II- a real-time, multi-tasking operating system and high level language. SWEPSPEED II was developed by the Southwest Region of the Central Electricity Generating Board who generously supplied the system for this project. The capabilities of SWEPSPEED II were found to be convenient for building an alarm handling system from a collection of well defined and structured program tasks. This was a feature

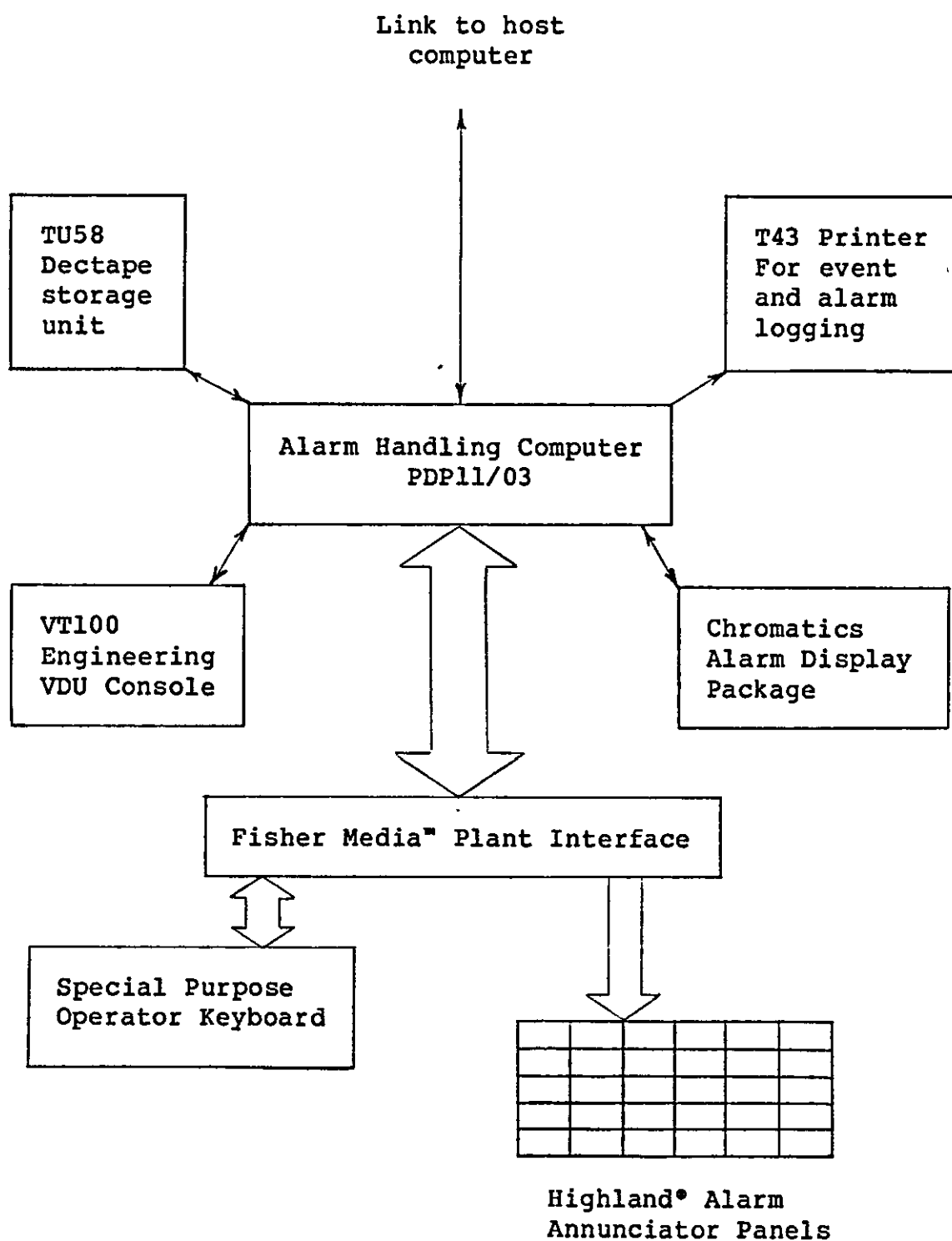


Figure 6.6 The On-Line System Hardware Configuration



Figure 6.7 The On-Line Alarm Handling System



Figure 6.8 Operator Keyboard

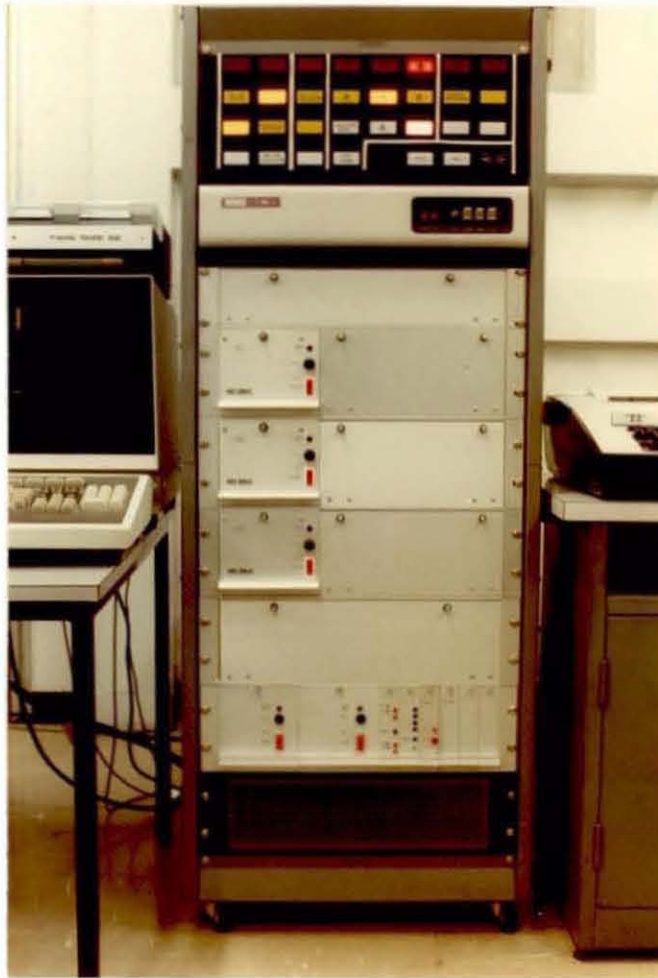


Figure 6.9 The Alarm Handling Computer with Media
Plant Interface and Highland Annunciators

that matched the project's requirements very well.

For the purposes of this project it was decided that the on-line alarm handling computer would be responsible for alarm handling functions excluding computer driven VDU alarm displays. It was considered that the presentation of alarm information was plant specific thus a general purpose display system may not be entirely suitable in this case. Additionally, the on-line display management package developed previously (see Appendix A) demonstrated that a general purpose information display system was feasible and useful. It was decided that the alarm handling system computer should be capable of distributing alarm information in a format suitable to interface with such display systems. Nevertheless to demonstrate that such a system could be implemented a special purpose alarm display software package was developed to reside in the Chromatics colour graphics computer. This display package written in Microsoft BASIC forms an alarm status information management system onto which software personality modules can be added to produce the desired display formats. Hooks are provided in the software to allow the user to write application specific personality modules. Two such modules were written for this purpose to support the following alarm display formats:

- 1) A Basic Alarm Paging Format
- 2) Alarm Annunciator Mimic Format

It would be desirable to adapt the on-line display management package to incorporate these features, however, this would require further consideration and a more detailed study of VDU based alarm display requirements.

A detailed description of the alarm display package and the alarm handling software package can be found in the

Appendix E which contains the Software Description for the On-Line Component of the Alarm Handling System. This document gives details of programs including listings and flowcharts.

Appendix B which contains the User's Guide for the On-Line Component of the Alarm Handling System also found in the appendix contains detailed instructions for the operation of the on-line system.

A summarised description is presented here of the functions of the alarm handling system. The alarm handling system software is comprised of many tasks running independently in a real-time environment. Coordination of tasks requires a global program structure capable of performing housekeeping functions such as inter-task and inter-computer communications, system startups, and other program task supervision. The alarm software is therefore comprised of 20 SWEPSPEED program tasks performing a variety of functions which can be classified as follows:

- 1) Supervision Tasks
- 2) Link Drivers
- 3) Device Drivers
- 4) Alarm Handling Tasks
- 5) Auxillary Tasks

Figure 6.10 illustrates the interaction of the system tasks. A queue communication network managed by the queue manager task (QMAN) supervises the transfer of standardised data packets to and from jobs within the system. Link driver tasks (LISN, TALK, CHROM) permit inter-computer

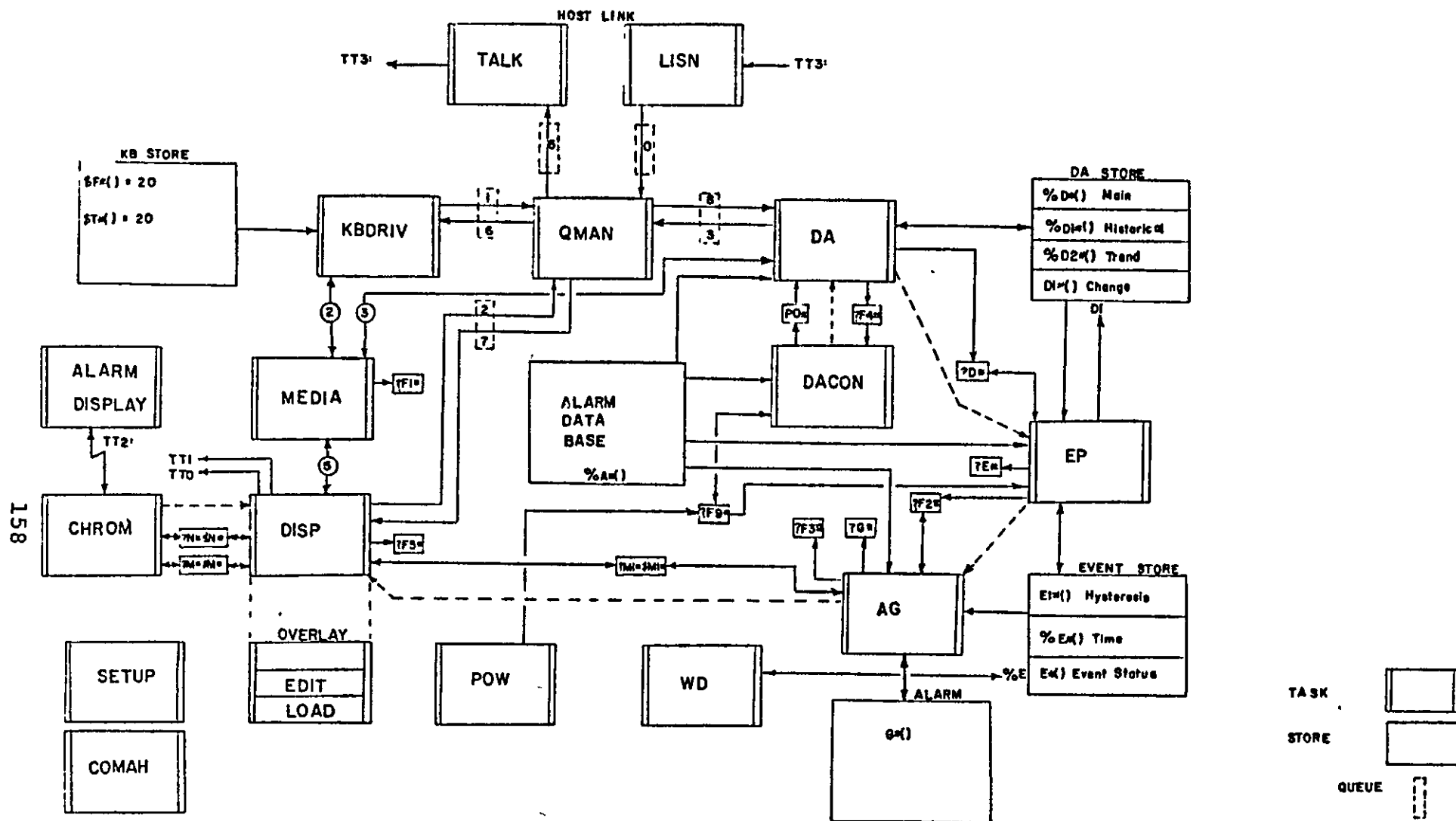


Figure 6.10 Alarm Handling System

communication with a host computer and the alarm display system in the Chromatics. The device drivers (MEDIA, KBDRIV, DISP) provide software support for interfacing peripheral devices with the alarm system such as the Fisher Media plant interface, special purpose operator keyboard, and alarm log printers or other display systems. Additional supervision and auxillary tasks perform functions such as startup control (POW), system command monitor (COMAH)- and system health checks and updating (WD watchdog).

The key alarm handling tasks are:

DACON Data Acquisition Controller

DA Data Acquisition

EP Event Processor

AG Alarm Generator

6.6.3.1 Data Acquisition

Based on instructions programmed by the user, the data acquisition control task (DACON) directs the operation of the data acquisition task (DA). Depending upon the system clock time, DACON selects the appropriate group of data acquisition blocks to be scanned and updated. In response the DA task supervises the data request message packets sent to plant interface equipment. The returning data packets are then processed by converting the basic process variable data into a useful form. This includes the extraction of data from message packets, conversion of analogue data via user defined conversion algorithms, and the adjustment of binary ON/OFF switch contact information to the correct logic form. Further, the task performs an initial evaluation of the process data to check its validity. The

check is rudimentary but useful. Historical information for each variable is recorded and updated as necessary along with trend and current value data.

Four scan rates are supported to maximize the resolution for rapidly changing process variables while reducing the processor load by spreading out the data acquisition of variables requiring less frequent scanning.

If a significant change in a process variable's value or status is detected the event processor is notified and started.

6.6.3.2 Event Processing

Again based upon instructions programmed by the user in the alarm data base the event processor (EP), once started by the DA task, examines data acquisition values as obtained from the data acquisition current value, historical, and trend storage. The values are compared with parameters as defined in the event definitions. Each event definition contains information concerning the form of processing required to perform the comparison with event parameters. The calculations take into account hysteresis by means of a decision table technique as described in the appendix E. Depending upon the result of the processing the event status image and time of occurrence table is appropriately updated.

If a change in event status is detected the alarm generator task is notified and started.

6.6.3.3 Alarm Generation

Using the event status image, time of occurrence table, and alarm condition statements coded in the alarm data base, the alarm generator task evaluates the status of

the alarms in the system. The alarm generator, started by the event processor when a change in event status is detected, steps through all alarm definitions in the alarm data base and evaluates the appropriate alarm condition statement. Depending upon the current alarm status of each individual alarm either the ON condition statement is evaluated when the alarm status is off, or the OFF statement when the alarm status is on. If the condition statement is satisfied, the alarm output code located in the alarm data base is sent to the display system along with an alarm status message.

6.6.3.4 Using the On-Line System

In general the on-line system once loaded with an alarm data base and then started requires no further user intervention. The alarm handling system startup procedures are described in Appendix C and illustrated in Figure 6.10. A demonstration of a simple example is shown in Figure 6.11. Once the system startup procedure is complete the system performs an initial data acquisition scan before alarm generation can begin. The system can be stopped or restarted as required by the user with on-line system commands. Minor modifications can also be made to the alarm data base. These procedures are performed through an engineering console to provide system security.

6.6.3.4 Management by exception

The on-line system software is organized such that the alarm handling system processing time is minimized by performing functions only when required. This management by exception of the system tasks means that if a data acquisition block changes significantly only then is the event processor started. Also the event processor will only evaluate the events using the changed DA blocks instead of

@173000G
Restart - 13:55
DAY = 6
MONTH = 8
YEAR = 82
HOUR = 14
MIN = 20
LOG IN & ACT14

\$LOG
Name?GOD
Password?

\$ACT14
NHRU

Figure 6.10 On-Line System Startup Example

Alarm Data Base	PLANT CODE	NAME	I/P DEV	TYPE	ALG NO.	RANGE	SCAN	PRIORITY
	115	SENSOR3	1	A	1	0 1 (.0001)	2	1
	157	CONTACT1	1	N		(0)	1	1
	158	CONTACT2	1	N		(0)	1	1
	159	CONTACT3	1	N		(0)	1	1
	EVENT CODE	EVENT NAME	PLANT CODE	TYPE	L. LIMIT	L. HYS.	U. LIMIT	U. HYS.
	E0001	CON1	157	ON				
	E0002	CON2	158	ON				
	E0003	CON3	159	ON				
	E0004	HI	115	HI	.5	.6	.7	.8

ALARM NAME: ALARM3 (22)
 CONDITION ON: HI,
 CONDITION OFF: HI, NOT,
 PERSISTANCY: 0

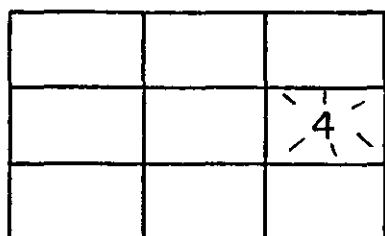
ALARM NAME: ALARM6 (25)
 CONDITION ON: CON1, CON2, CON3, SEQ,
 CONDITION OFF: HI, NOT, CON3, NOT, AND,
 PERSISTANCY: 0

Figure 6.11 Demonstration Example

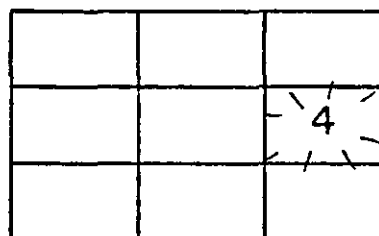
- 1) Prepare Alarm Data Base
- 2) Transfer data base to on-line system
- 3) Run on-line system using RU command
- 4) Simulate an event condition on plant code 115 (65% range)
- 5) Alarm 4 is activated and accepted (see panel A)
- 6) Simulate a contact closure on plant code 157
- 7) No alarm (see panel B)
- 8) Simulate a contact closure on plant code 158
- 9) No alarm (see panel C)
- 10) Simulate a contact closure on plant code 159
- 11) Sequence alarm 6 condition on statement satisfied.
Alarm 6 is activated and accepted (see panel D).
- 12) Simulate a 10% range on plant code 115
- 13) Alarm 4 is deactivated and removed from panel (see panel E).
- 14) Simulate a contact opening on plant code 159
- 15) Condition off statement for alarm 6 is satisfied.
Alarm 6 is deactivated and removed from panel (see panel F).

Demonstration Procedure

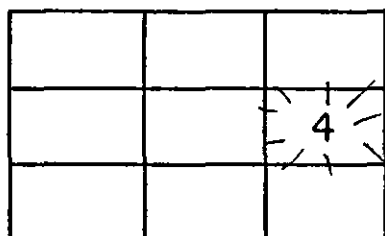
Figure 6.11 Demonstration Example (Continued)



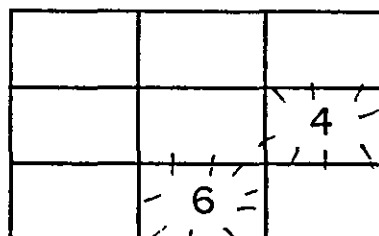
A



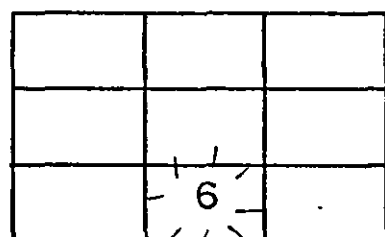
B



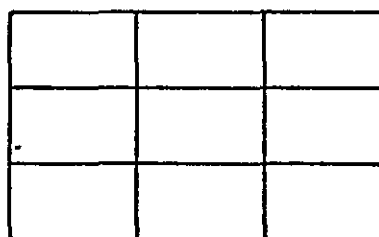
C



D



E



F

Alarm Fascia Panel

Figure 6.11 Demonstration Example (Continued)

STOR-A-FILE IMAGING LTD

DOCUMENTS OF POOR ORIGINAL HARD COPY

all event definitions.

The result of this form of task control is that processing time is minimized thus providing more time for overhead tasks and improved system response time.

6.7 HARDWARE SELECTION

The selection of hardware to be used for the ON-line section for the alarm handling system has been made based upon a compromise between specifications and available limited resources.

To maximize system speed the ideal hardware configuration would be comprised of separate processor units. Each processor unit would be assigned duties in such a manner that the execution time of the overall system would be at least one order of magnitude less than required system response time. Considering the probable size of the task the microprocessor technology would be adequate. The processors would store common memory when suitable effectively forming DMA data transfer links between processor modules.

Since the proposed alarm system is for prototyping, a sacrifice of execution and system response time in favour of a software configured system would appear attractive. Individual processor modules would be replaced by software modules which would be executed in a multitasking environment. In this case the system is readily reconfigurable since the software task modules can be easily added, deleted or modified as required. A system based on individual processor modules loses flexibility since the functional configuration of the system is confined to a large degree by the hardware configuration of the system.

Additionally a single processor would be less costly, more off the shelf, and generally easier to implement.

The on-line system is based around a Digital Equipment Corporation (DEC) PDP11/03 microcomputer. This 16 bit wide system is capable of supporting up to 28K words of memory along with a wide variety of accessory cards which support functions such as input/output interfacing. The alarm handling system prototype 11/03 contains the full complement of memory along with 5 serial I/O lines, 3 of which are RS-232 configuration. Two of the serial lines are configured for 20 mA current loop operation. In addition there is a bus extension option installed for interfacing with bus addressable devices. A floating point arithmetic unit has been installed to reduce the processor time required to perform real mathematical manipulations. To minimize difficulties encountered when booting the system, the 11/03 has been configured to perform this function automatically on command. Boot-strapping loads the necessary data into memory required to allow the computer to load program material into memory. This is especially useful when turning on the computer since the computer memory will not contain any executable code when first started. The boot-strap loads in data from an external storage device.

A DEC TU58 dual tape drive is used as the mass storage device for the system. This drive utilizes DECTAPE cartridge tapes similar to cassette tape. The unit is connected to the PDP11/03 via an RS-232 serial link running at 9600 BAUD. Cartridge tape storage systems are relatively slow compared to other forms of storage such as fixed disk or even floppy disk systems. The choice of a cartridge tape drive system was dictated by cost and reliability considerations. For prototype applications investment in fixed disk systems was not feasible. The short access time and high reliability of systems such as Winchester storage systems appear to be the

best choice and about the appropriate size for the prototype. Unfortunately funds were not available. Cheaper floppy disk systems were ruled out due to low reliability especially when used in hostile environments. Unpleasant experiences with floppy disks on the OLDMAN system discouraged their consideration. Although relatively slow, the cartridge tape system appeared to be the best alternative.

Plant data acquisition requires a significant amount of computer interface hardware. The alarm handling system uses Fisher Media Plant Interface equipment. The Media package is a digital monitoring and control system designed to function with a wide range of plant instrumentation. A data highway structure allows immediate access to interface cards located on the highway. This data highway provides random access to any interface in the system thus simplifying computer interfacing. The Media system is connected directly to the PDP11/03 bus. Individual Media interface cards are addressed via dedicated memory locations in the 11/03 I/O page. The system can be readily extended or modified by inserting appropriate input or output modules. In addition the Media system is used on a large number of plants in the UK. This point makes the selection of the Media interface system attractive since it means that the alarm handling system can readily be fitted to some existing plants without the need for additional computer interface equipment.

A Teletype T43 printing terminal is used for obtaining hardcopy output during system development and on-line system output. During system operation the printer is used as a log. A 20 mA current loop type serial link connects the printer to the PDP11/03.

A Chromatics CG 1999 19" intelligent colour VDU

constitutes the principal operator display. The Chromatics has adequately high resolution (512x512 pixels) to present most forms of operator displays. Since the unit is intelligent the majority of display software can be located within the unit. The Chromatics contains a floppy disk device, however, in operation this drive would not be used. The extensive graphic capabilities of the unit simplify the generation of display formats. There are more suitable display systems such as the intelligent RAMTEK units, however their costs are prohibitive for this project. Also, as in this case, the Chromatics can double as the off-line computer since the unit is a complete stand-alone computer system, a feature not seen in display dedicated VDU systems. The Chromatics communicates with the PDP 11/03 via an RS-232 serial line running at 9600 BAUD.

Another 20 mA current loop serial line is available to be used as a link to a host computer.

Attached to the Media interface system is a set of standard Highland alarm annunciator panels. These annunciators are connected to the Media via digital output cards. The annunciators can thus be implemented as an alternative means of displaying alarm information.

Communication between the operator and the alarm handling system is accomplished via a special purpose operator keyboard. The keyboard is driven by the Media system through the use of digital input and output interface cards. The keyboard was specially constructed for the alarm handling system and thus conforms with the flexibility requirements of the system. Physical layout reconfiguration of the keys is relatively simple. Key assignments are made through software. Refer to the keyboard driver document which can be found in Appendix D for more details.

Further detailed description of the hardware specification is given in the hardware documentation located in Appendix E.

The hardware configuration was developed to enhance the universality of the alarm handling system. Connecting to an existing process plant can be difficult. The hardware configuration allows three forms of plant interface.

- 1) Direct to plant sensors via Media plant interface unit.

- 2) Direct connection to bus driven plant interface devices. This is principally intended to allow the alarm system to be retrofitted to plants which already have Media plant interface systems.

- 3) Via a serial link to the plant host process control computer. This allows the alarm system to gain access to plant data buses in the process computer.

CHAPTER 7

DISCUSSION

7.1 INTRODUCTION

The alarm handling system described in this thesis is a prototype design and therefore points for improvement are likely to be found. This chapter evaluates the performance of the alarm system using the original design assumptions as a bench mark for comparison. Further evaluation requires more detailed long term plant application studies which are beyond the scope of this project, however some suggestions on this topic are discussed.

An overall performance evaluation of any form of alarm system is difficult to perform since overall performance is judged upon how well the alarm system assists the operator in the:

- 1) detection of a fault
- 2) diagnosis of a fault
- 3) formulation of an action strategy to rectify the fault.

Overall performance is therefore dependent upon a large number of factors which are difficult to identify and quantify. An alarm system philosophy which works well on one plant may not be satisfactory on another even when the plants would appear to be very similar since the levels of risk and other plant conditions vary. For a simple

performance evaluation it may be possible to take an existing plant and substitute the existing alarm system with the alarm handling system and then record the number of serious failure modes that occur with and without the alarm handling system. Parallel operation of the alarm handling system with the existing alarm system may be another alternative. Both of these alternative applications are well within the capabilities of the alarm handling system however in either case the results of the studies would be valid only for specific applications with very similar if not identical plant characteristics. Some of these factors for example include:

- 1) Plant type
 - 2) Control room configuration
 - 3) Level of operator training
 - 4) Operator work loads
 - 5) The quantity of available plant information
 - 6) Presentation of process and other information
 - 7) Level of plant risk
 - 8) Complexity of the plant
 - 9) The existing alarm system philosophy
- etc.

It would be useful to develop a methodology for evaluating alarm system performance under a variety of plant conditions. These studies are outside the scope of this project, however it is possible to evaluate the operational aspects of the prototype alarm handling system by comparison of functions available in the prototype with those proposed in the original assumptions. The operational performance evaluation can be judged by the ability to support the alarm detection functions discussed previously. In general the prototype alarm handling system performs well, however as in any prototype system there is room for improvement.

7.2 ON-LINE SYSTEM PERFORMANCE AND IMPROVEMENTS

Tables 7-1, 7-2, and 7-3 summarise some of the important functions of the prototype on-line system. Data acquisition, event processing, and alarm generation are the fundamental processing tasks in the system and therefore define the alarm handling functions available.

7.2.1 Data Acquisition

It was found that the data acquisition task consumed the most processor time of any of the alarm handling tasks. As a result the careful selection of scan rate for individual data blocks is important to spread the data acquisition load. Too many data acquisition blocks in the one second scan group can load the processor to the point where other overhead tasks such as servicing the operator keyboard become sluggish.

The type of data ⁿinput source must also be considered. For example slow response times experienced with multiplexed analogue inputs may not physically allow adequately fast scanning. The prototype system uses multiplexed inputs with a response of 50 ms. As a result it is not possible to have more than 20 such inputs in the one second scan group.

Serial links with the host computer also proved very slow for data acquisition. Data requests sent down the serial link are in the form of ASCII data packets up to 7 characters long. The responding data packet is much longer. The processing time required to process these packets, the link speed and the host processing time can greatly reduce the number of data acquisition blocks which can be retrieved via the host.

Another aspect of data acquisition in the prototype is that there is one data acquisition task. This means that when a slower scan group such as the 15 second group is due for data acquisition it must be scanned in conjunction with the one second group. The combined scan must not exceed one second so that the data acquisition task is ready for the next one second scan. This can cause difficulties depending upon the type of data source since the task must be capable of scanning all data acquisition blocks defined in the system within one second.

There are several alternative methods of data acquisition which would improve the situation:

- 1) Reduce the required system time resolution
- 2) Incorporate more data acquisition tasks
- 3) Utilize a separate processor for data acquisition management
- 4) Use high speed plant interface equipment
- 5) Utilize DMA data transfer equipment

Relaxation of the time resolution of the system would allow a greater number of data acquisition blocks to be scanned. This would however also increase the response time of the system. Rapidly changing process variables with response times less than that of the alarm system could not be monitored. This topic is discussed in greater detail in section 7.4.4.

Additional data acquisition tasks or a different data acquisition task structure could better manage the acquisition of data from slow responding plant interface

equipment. The space limitations in the prototype preclude this alternative.

As suggested in chapter 6 the use of multiple processors to perform the various alarm handling tasks could greatly improve system performance by spreading tasks to separate processors.

High speed plant interface equipment would be useful to improve the speed of the data acquisition task by reducing the time response of the plant interface.

Direct memory access (DMA) interface equipment is an obvious method of greatly improving both data acquisition from the plant and via the host computer. DMA eliminates processor time required to service interrupts generated by conventional communication interfaces. The prompting of plant interface equipment is also eliminated.

As shown in Table 7-1 the prototype alarm handling system is capable of dealing with most of the data types proposed in chapters 4 and 5. Derived process data facilities have not been included since the implementation would require additional on-line programs and a considerably larger alarm data base area for storage of coded algorithms. It was also considered that for prototyping purposes that the lack of the facility would not seriously impair the overall performance of the system.

Analogue conversion algorithms have been left to the user to implement in the on-line system. User specified algorithms do not necessitate the on-line system to store a large number of algorithms which may not be utilized in a particular application. The purpose is to conserve available memory space for maximum alarm data base size.

<u>Data Types</u>	<u>Available Functions</u>	<u>Comments</u>
Analogue	With user specified conversion algorithms. Linear scaling available with no extra programming required. No derived processing available.	Dependent upon Media Plant Interface Host link allows AHS to read variable data located in host.
Binary	Will support all types of switch contact and logic level inputs.	Selectable scan groups and priority within scan group.
Specified Parameters: Input device, plant code, data type, range, conversion algorithm numbers, significant change value		
Data Source: Fisher Media Plant Interface System and host computer.		
Data Rate: Via serial host link; 10 data blocks/sec when used with PCP commercial plant control package in host. Via Media Interface; 250 data blocks/sec.		
Data Validity Check: Rudimentary range check.		

Table 7-1 Data Acquisition Summary

Data validity checking is a topic which requires further consideration in the prototype system. Although rudimentary validity checks are performed by comparison of range parameters with process data, this is not entirely satisfactory. A better method could be implemented by performing cross checking of data by means of derived process data values. Additional program modules could be implemented to detect unusual process data excursions such as zero/full scale, sudden shifts, etc. Restrictions of available memory space make data verification procedures difficult to implement since large additional amounts of on-line programming and alarm data base space would be required. The processing time required for data verification has been estimated to be significant. Using a single processor computer for the prototype does not provide sufficient memory or processing resources to support this facility.

Additional facilities would be desirable and should be considered to allow the operator to input validity information for individual data acquisition blocks.

The techniques developed for alarm data base coding have demonstrated that there would be no difficulty in implementing any of the missing functions in the present system.

7.2.2 Event Processing

The prototype alarm handling system event processing facilities satisfy all of the functions discussed in chapter 5 with the exception of the enhanced basic alarm detection function 'timeout'. Recall that timeout is an additional specified event parameter which determines how long an event is to be considered true once it is detected. The time of occurrence table contains sufficient data for the

timeout function to be implemented however an additional SWEPSPEED task was found to be required to perform the necessary calculations. It was decided that the marginal benefits such a function could have did not justify the processing time and the alarm data base and programming space required to implement it.

The available event processing functions have been found to perform satisfactorily and are summarised in Table 7-2. It was noted that additional flexibility in defining events could be obtained by providing facilities to support multiple event definitions. Multiple event definitions would allow an event to be detected from a combination of events perhaps using simple Boolean expressions similar to those used to define alarms. The use of multiple event definitions would greatly reduce the processing time required to evaluate alarm condition statements especially where a particular event combination was repeatedly utilized. The required size of an alarm data base could also be considerably reduced. Multiple event processing would require a significant modification of the present on-line and off-line software structures. The processing techniques would be similar to those currently used for alarm generation.

7.2.3 Alarm Generation

Table 7-3 summarises the alarm generation facilities of the prototype system. Most of the functions discussed in previous chapters have been satisfactorily implemented in the prototype alarm handling system.

Difficulties are experienced when mixing time related and non-time related alarm detection functions. As a result the ASG, asynchronous group detection, facility is not available since the evaluation of this operation requires

<u>Event Type</u>	<u>Basic Alarm Detection Function</u>	<u>Data Used</u>	<u>Additional Specified Parameters</u>
XHI HI LO XLO	Band or Absolute	Analogue current value	Event range limits including hysteresis
ON OFF	Binary	Current binary status	Logic reversal available
TREND	Band or Absolute	Analogue trend value	Event range limits including hysteresis
DEVI	Deviation	Analogue current value	
TDEVI	Deviation	Analogue trend value	

Note: Event processing is performed only when a significant change is noted by the data acquisition task.

Specified Parameters: Event name, type, data acquisition block name.
No timeout event parameters may be specified.

Table 7-2 Event Processing Summary

ON/OFF Alarm Condition Statement Operators

<u>Operator</u>	<u>Type of Operation</u>	<u>Comments</u>
OR AND NOT XOR	Time independent Boolean	Can be combined as required.
()	Psuedo operators	
VOT	Enhanced Boolean	Must be used in separate alarm condition statements.
SEQ TIL	Enhance time related Boolean operator	

ON/OFF alarm condition statements comprised of enhanced Boolean expressions are evaluated to determine the current alarm status. Alarm generation starts only after the event processor has detected a change in the event status image. Expressions contain events and operators. Difficulties are experienced when mixing enhanced and standard Boolean operators.

Table 7-3 Alarm Generation Summary

both time of occurrence and event status information. Similarly time related operators cannot be mixed with non-time related operators in a single Boolean expression.

Enhanced Boolean operators which perform functions on an unspecified number of operands such as the VOT and SEQ/TIL operators are difficult to combine with single or double operand operators as encountered in normal Boolean expressions.

In the case of combining time related and non-time related operators in a single expression, the on-line software would require additional program tasks. It has been estimated that these extra tasks would degrade the system performance by increasing the average alarm detection times over one second. This would mean that during heavy alarm conditions some alarm information may be lost.

The above restrictions do not prohibit the user from using enhanced Boolean operators in alarm condition statements. Difficulties can be experienced when combining for example mode detection with sequence detection. This shortcoming has been considered to be of minor importance since the difficulty could be rectified through further studies of the representation and processing techniques of enhanced Boolean expressions. In general the Boolean ON/OFF alarm condition statement expressions perform satisfactorily.

7.2.4 Data Base Size

The maximum alarm data base size which can be installed in the alarm handling computer is dependent upon the composition of the data base. The current version of the alarm handling software permits 4500 words of memory to be used for data base and overhead assignments. Array sizes in

the alarm handling software must be assigned in the SETUP task. The sizes of these overhead arrays are also dependent upon the composition of the alarm data base. The total memory space required for a particular alarm data base is calculated as shown in Figure 7.1. The total memory space used must not exceed 4500 words. As illustrated in Figure 7.1 the total number of alarm conditions which can be stored in a data base varies considerably with content. The maximum number of single event alarms using binary events is approximately 250. Any additional complexity will reduce this number accordingly.

The current version of the alarm handling system uses real variables in the alarm data base. Real variables consume a great deal of memory space, much of which is not utilized in the present alarm data base structure. Improved data coding methods could reduce the size of the alarm data base to increase the capacity of the alarm handling system. This topic requires careful consideration since often the more condensed the data base becomes the greater is the required processing time to decode it. Real-time computer systems are usually plagued by this processing time versus memory space trade-off.

7.2.5 Overhead Tasks

The structure and available functions of the on-line system overhead tasks perform well. The device driver tasks such as the keyboard and Media driver tasks could be improved by writing these routines in assembly code. Unfortunately SWEPSPEED II does not support user written assembler coding. It would be desirable to have the keyboard driver written in assembler thereby reducing the processing time required to service the keyboard which is currently polled every 0.2 seconds. Alternatively it would be useful if the operator keyboard driver could be interrupt

Total Words of Memory Required for an Alarm Data Base
(maximum 4500 words) =

$$\begin{array}{lcl}
 \text{Data acq.,} & \left\{ \begin{array}{l} \text{DA} * 6 \\ + \text{EDB} * 3 \\ + \text{EDA} * 7 \\ + \text{AD} * 4 + (\text{total no. of ON \& OFF condition} \\ \text{statement elements}) \\ + 11 \text{ [data base header]} \end{array} \right. & \\
 \text{event,} & & \\
 \text{and alarm} & & \\
 \text{info} & & \\
 \\
 \text{Overheads} & \left\{ \begin{array}{l} + \text{DA} * 3 + \text{INT}(\text{DA}/16) \\ + \text{ED} * 1.5 + \text{INT}(\text{ED}/16) \\ + \text{INT}(\text{AD}/16) \end{array} \right. &
 \end{array}$$

DA = data acquisition block

EDB = binary type event definition

EDA = analogue type event definition

AD = alarm definition

ED = EDA + EDB

INT = integer

Figure 7.1 Calculating the Alarm Data Base Size

driven. This would mean that when a key is pressed the on-line processor would interrupt the current program to service the keyboard. Interrupt support is not provided by the SWEPSPEED II system.

The majority of processor time is consumed by the keyboard driver and the data acquisition tasks. Reduction of the keyboard driver processing time would increase the speed of the remainder of the system allowing an increased number of data acquisition blocks to be scanned in high scan rate groups.

Recall that the inter-task communication network in the on-line system is comprised of a queue system managed by a queue manager task. Tasks attached to the queue system pass message packets to one another. This data packet transfer scheme performs very well providing good inter-task communication. The queue system allows messages to be backlogged during occasional periods of heavy data transfer. The maximum backlog is determined by the size of the system Q array. In the current version of the prototype the maximum queue size allocated to each individual queue is 7 records. This limitation may require examination in applications where heavy data transfer rates are anticipated. The Q size is readily adjustable in the system however the larger the Q size the smaller the available alarm data base area. It would be desirable to have as large a Q as possible to prevent data transfer overload.

7.2.6 On-Line Summary

The preceding discussion of the performance evaluation of the prototype alarm handling system highlighted the shortcomings and difficulties with the current prototype. Frequent comments have been made

regarding the capacity of the on-line portion of the system. This is a common difficulty with many computer based systems. Functional aspects of the system can usually be improved or expanded by increasing the computer capacity with larger and larger computer systems. Processing times, for example, can be improved with greater word length capabilities or the use of multiprocessor based systems. Memory space is an important aspect of a computer. The microprocessor based systems such as used for the prototype are not only slower than larger minicomputers and mainframes but also can not support large amounts of memory.

It was decided that the alarm handling system should be based on a microprocessor system since the level of technology could support the majority of the alarm detection functions identified. The system is therefore relatively simple for general user applications while providing many advanced alarm system features. The alarm handling system costs are then kept to a minimum. In the case where users require more alarm handling capacity and/or facilities it may be desirable to consider implementing alarm analysis techniques. Figure 7.2 shows the intended level of sophistication which can be expected from the prototype system. Increased computer capacities can increase the level of sophistication of the alarm handling system. However, the performance may not be comparable with similarly sized alarm analysis systems.

The ability of the prototype alarm handling system to accommodate the alarm requirements of a particular plant application is dependent upon the following major factors:

- 1) The required size of the alarm data base
- 2) The time resolution required for alarm generation

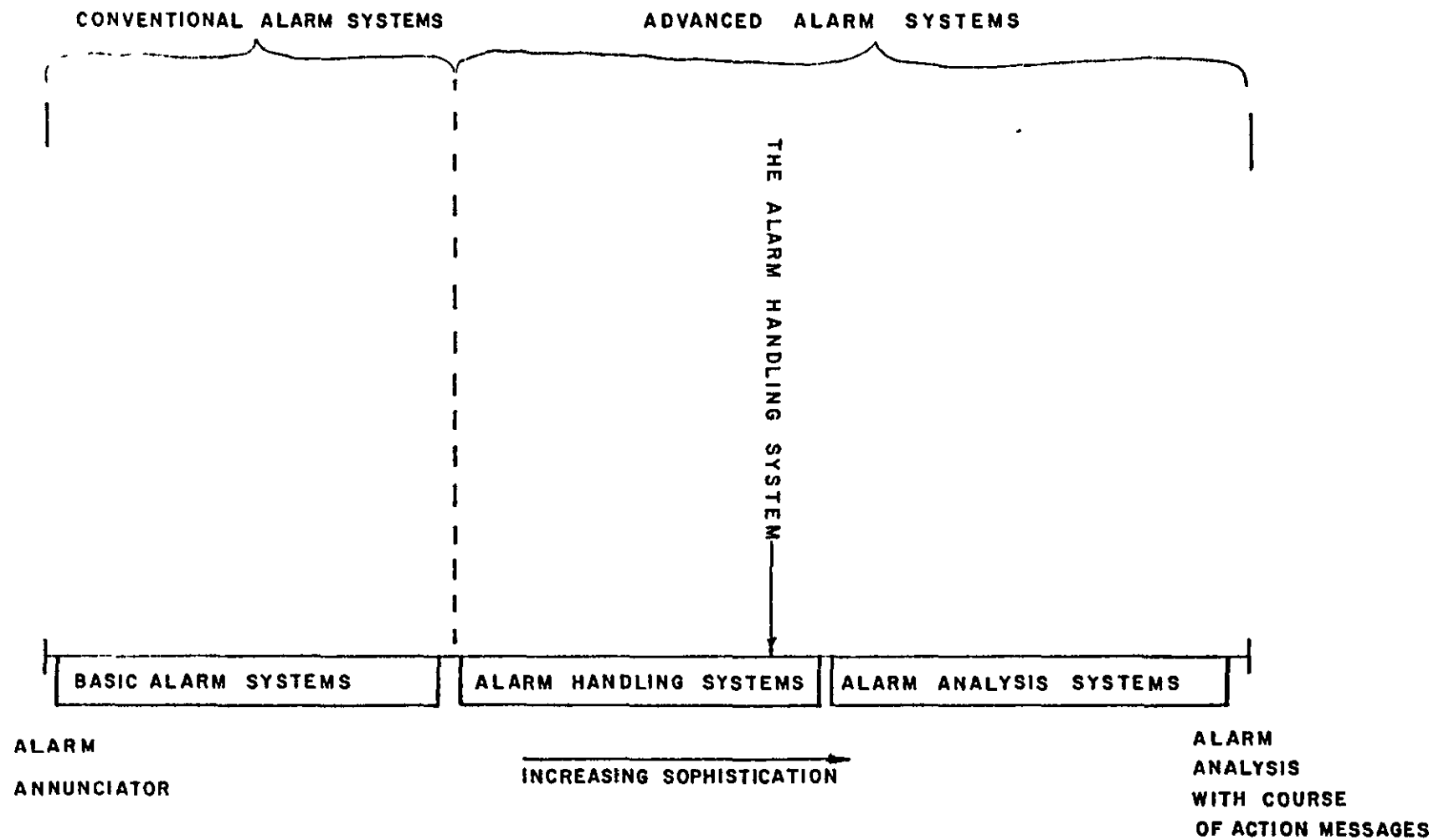


Figure 7.2 The Level of Sophistication of the Alarm Handling System

- 3) The capacity of the alarm computer
- 4) The form of data acquisition required
- 5) The complexity of alarms implemented
- 6) The format of alarm display

The alarm data base size is limited by the available memory space in the on-line computer. The size of the data base is dependent upon the content of the data acquisition, event, and alarm definitions. For example analogue events consume over twice the alarm data base space that a binary event requires. Similarly the length of alarm condition statement is proportional to the required data base space. In a specific application it may be possible to define many more events and alarms than in another less demanding application.

Time resolution considerations discussed in section 7.4.4 must be assessed for specific applications. If a large number of alarms require data scan rates to be included in the one second scan group, overloading may occur. Also if scan rates faster than one second are required then the alarm handling system is not suitable.

SWEPSPEED II will run in a variety of PDP 11 computers. Larger capacity systems will necessarily provide more memory space and possibly reduced processor times especially in multiprocessor PDP systems.

Data acquisition can be prohibitively time consuming especially when multiplexed inputs are utilized. It is important to assess the plant interface equipment used in a specific application to ensure that the required data scan rates can be supported.

Although the alarm handling system has great flexibility, numerous or highly complex alarm condition statements may not allow sufficient system response times for alarm generation. In applications where this situation may be encountered an alternative alarm system strategy should be considered. The alarm handling system will deal with complex alarm condition statements when slower scan rates are assigned.

The form of alarm display should be examined to establish whether the display system can maintain the data transfer rates which can be anticipated. When the on-line system detects a change in alarm status a message packet is sent to the display system. Many computer driven systems such as the alarm display package included in the prototype may not support sufficient transfer rates. This may be especially important during plant malfunction conditions when many alarms are generated over a short space of time.

7.3 OFF-LINE SYSTEM PERFORMANCE AND IMPROVEMENTS

The off-line alarm data base generation programs adequately provide the user with facilities to program, compile and transfer alarm data bases. The question and answer routines are useful since they guide the user during data input thus insuring that required data is not overlooked in individual definitions. It may be desirable to enhance the off-line system by developing an alarm handling language which could be subsequently compiled into an alarm data base. The structure and format of such a language requires further consideration.

The present version of the alarm handling system necessitates the physical connection of the off-line system

with the on-line system for alarm data base transfer. This configuration is convenient for prototype studies but restrictive for plant applications. A transfer medium such as magnetic tape or floppy disks would be desirable to eliminate the need for close proximity of the off-line system with the on-line system.

A Chromatics colour graphics computer was used in the prototype system for convenience. The Chromatics system, although suitable for prototype studies, has limited memory space and other facilities. It would be desirable to utilize a computer system with improved performance. In particular the implementation of a direct memory access display system would be useful to reduce display access and response time.

SWEPSPEED II performs satisfactorily and was found to be convenient for the prototype on-line system development. SWEPSPEED II appears to the user to be similar to the very user friendly language BASIC. Usually the execution time of such user friendly software systems is slower than other machine oriented real-time languages such as RTL/2. Overall system performance could be significantly enhanced by such a language to reduce system response times and improve the capacity of the system.

7.4 GENERAL DISCUSSION

7.4.1 Security

The security of a computer based system on a plant is an important consideration. Security can be evaluated from two general viewpoints:

- 1) Is the system 'crash proof'?

- 2) Can the operator inadvertantly or maliciously alter the operation of the system?

Crash proofing a computer system requires careful examination of the hardware and software comprising the system. Possible situations in which the system will cease to function or perform so inadequately that the system is not useful must be identified. During an evaluation of the prototype system it was noted that when very large alarm data bases are used it is possible to produce internal data transfer rates which, although not crashing the system, will impair the operation of the system.

Additionally the prototype is vulnerable to crashing during system startups if the startup procedure is not strictly followed. This is caused by the method SWEPSPEED II uses to check the amount of memory available in the computer during the boot-strap procedure. Some relatively simple hardware and software modifications would rectify this situation.

It is important that in plant applications, operators cannot inadvertantly or maliciously alter the system. For this reason the only operator/alarm system interface available is via the special purpose operator keyboard. This assumes that the computer is properly safeguarded. The keyboard driver has the ability to test operator inputs and prohibits any system alterations. During system startups the user must perform functions on the computer console terminal. This terminal has access to all system programs, etc., a feature inherent in SWEPSPEED II. It is important that this terminal be disconnected or locked after use to insure security.

7.4.2 Difficulties in System Development

As would be expected there were several difficulties experienced during the development of the prototype alarm handling system which should be noted. It was found that the hardware prototyping was excessively time consuming. The construction, trouble shooting, and commissioning of the prototype equipment required considerable time and effort.

The development of inter-computer link driver programs to allow not only different types of processors, but also different languages and operating system to communicate was found to be a formidable task. It would be advisable on improved alarm handling systems to avoid this difficulty by utilizing similar computers and languages for all components of the system.

As with any software operating system and language there are shortcomings. Although SWEPSPEED II is a useful package, it was evident that supporting the alarm handling system was just within its capabilities. Some functions which would have been desirable to include in the prototype were not principally due to SWEPSPEED II system constraints. It would be desirable to consider other multi-tasking real-time operating systems in future alarm handling systems.

7.4.3 Accuracy of the Alarm System

It should be noted that the ability of an alarm system to deal adequately with alarm situations on the plant is not only a product of the inherent facilities present in the alarm system but also the accuracy of the information used for alarm generation programmed into the system. The alarm handling system discussed here is a 'bare bones' system which can be compared to a basic computer. A computer has certain characteristics and performance abilities which are

programmed by the user to execute functions. The ability of the computer to deal with a specific application is partially a function of the quality of the program installed. Similarly the alarm handling system must be programmed. As in the computer example, the performance of the alarm handling system is largely dependent upon how the user has programmed the system. In this case the program is the alarm data base containing data acquisition, event processing, and alarm definitions. Although as in any computer based system there are limitations in size, speed and available functions the alarm handling system's performance is only as good as the program in the alarm data base.

The accuracy of an alarm system can be measured by the percentage of alarms that accurately represent plant conditions as compared to the total number of alarms generated. This accuracy however cannot be a measure of the overall performance of the alarm system since the output of the system is dependent upon how it has been programmed and how the output is translated into a real diagnosis by the operator. Interpretation of alarm system output is a complex problem and requires much more research.

7.4.4 Time Resolution of an Alarm System

There are several factors which must be considered when selecting process variables for use in alarm system generation:

- 1) The computer executes instructions stored in memory. These instructions are executed one at a time sequentially. Consequently there exists an inherent time lag as the program instructions are executed. This time lag also means that a computer can execute a limited number of

instructions over a given period of time. In the case of the alarm handling system data acquisition functions are frequently repeated. The finer the time resolution of the computer, the shorter the interval during which the computer can perform its functions. This limitation means that there is a maximum number of process variables that can be examined within a fixed time interval.

2) There also exists uncertainty about the time of sampling of a process variable. The response time of sensors, transducers, and interfaces can displace in real time the value that the computer eventually obtains. Additionally during a scan of plant sensors not all sensors are read sequentially by the computer as mentioned above. The result is that even though process variables appear to be read simultaneously, the readings are displaced in time from one another.

The above points are significant in some highly time sensitive data acquisition plant applications.

7.4.5 'Level of Alarming' on a Plant

The number of alarms which should be placed on a plant is obviously a function of the type of process, the size, and so on. Unfortunately there are several paradoxical considerations which should be noted. Firstly, the plant is assumed to be operating normally during the majority of time. The number of alarms or the level of alarming given this assumption would be adjusted such that the operator has adequate information about process variables and events to deal with minor abnormalities on the plant. It can be assumed that the number of alarms required for this approach is high as compared to the number of measured plant variables. The exact relationship depends on many factors such as risk. Secondly, the plant can and probably will at

one time or another produce a serious malfunction which generates far more alarms than normally expected. For serious malfunctions, the level of alarming should be less. If the plant has been heavily alarmed for detection of minor malfunctions, operators are easily flooded with alarms during serious malfunctions. Nuclear plants provide a good example of this phenomena. As has been noted, operators can become lost in the information or misinterpret information under these circumstances.

The question of level of alarming is difficult. However the specific plant application is an important factor. In the nuclear industry the difficulties experienced with high levels of alarms have prompted much work such as alarm handling to provide generalized plant health displays. Most significant of these programs has been the studies concerning 'Critical Function Monitoring' (CFM). CFM overcomes the high level alarming by providing a separate alarm system which monitors the status of the key plant functions with a low level of alarming. In other words a coarse alarm system supplements the main alarm system. This is particularly useful during severe plant malfunctions where the CFM generate a few generalized alarms to give the operator an idea of what may be going on. The prototype alarm handling system is useful for these sorts of applications.

The degree of severity and risk of anticipated plant malfunctions can then be said to be a major consideration in the level of alarm on a plant. Nevertheless it is difficult to ascertain the required density of alarms for a given plant. It is not possible to anticipate or identify all likely conditions and to train operators to recognize these conditions which may occur so infrequently that even if they were trained they would not correctly diagnose the fault. If the cost of detecting an unlikely malfunction is as much

or more than the cost of the malfunction developing and maturing, then there is usually no case for trying to detect the condition. Also the probability of an event occurring may be so small that it is no justification to anticipate the occurrence. Generally the level of alarming of a plant can be categorised as follows:

- 1) Minor alarms requiring individual attention.
- 2) Groups of alarms requiring operator pattern and clue recognition based heavily on training.
- 3) Groups of alarms requiring operator pattern recognition and bona fide situation diagnosis.
- 4) Many alarms requiring a more global approach by the operator to diagnose faults.

7.4.6 Location of Alarm System Functions

The locations at which the three alarm handling functions of data acquisition, event processing, and alarm generation are performed in various alarm system schemes vary widely. Some systems such as most alarm annunciators perform all three functions independently of other plant equipment. Other systems rely upon the process control computer to acquire the process data via data acquisition routines used for other purposes as well. Similarly the alarm displays are often integrated with process data displays. Interaction of this nature necessarily results in common mode failure difficulties. Separation of alarm detection, processing, and display functions from other operator systems increases the usefulness of the alarm system especially during abnormal plant conditions where the integrity of either or both systems may be in question. The

probability that both the process data system and the alarm system will yield inaccurate information increases when both systems share processing facilities.

The degree of duplication of system functions is dependent on factors similar to those involved in the selection of the type of alarm system to be implemented. The most desirable alarm system configurations would be capable of performing without the assistance of any other plant control system.

7.5 PLANT ACCEPTANCE

The functions available in the prototype alarm handling system have been shown to be a considerable improvement over traditional alarm systems. Nevertheless it can be difficult to convince both plant operators and managers that such a system may indeed be better than existing systems on the plant. Improved quality displays and alarm generation systems may be rejected on the grounds that they differ from the existing systems. The arguments for introducing a new improved system must be well founded. Often there is a good case for maintaining the existing system which includes such factors as the work force attitudes towards computer systems, operator training, and disruption of prevalent operating practices.

There must be clear evidence that the system will be beneficial. As discussed in previous chapters this can be difficult to prove at this stage and even then improvements may appear marginal to operators or managers.

Evaluation of the prototype system requires long term plant testing on existing plants which can also create difficulties with acceptance. Tampering with existing

working systems can pose serious problems and inconvenience to operational plants.

Although long term testing will identify the system's full potentials and shortcomings it may be possible to suggest an initial plant evaluation that would give an indication of the system's usefulness and general acceptance. The following topics require consideration:

- 1) Is the general concept of the alarm handling system useful?
- 2) Do operators and managers accept and use the system?
- 3) Does the alarm handling system provide sufficient alarm handling capabilities for small process plant applications?
- 4) Does the alarm handling system produce adequate quality alarm information to assist the operator in the:
 - a) detection of fault conditions?
 - b) diagnosis of faults?
 - c) development of action strategies to rectify fault conditions?

As discussed in this chapter the prototype alarm handling system has capabilities which should prove valuable in many process plant applications.

For a particular plant application the concept of management by exception for processing and evaluating plant data could possibly result in an overload of the alarm handling system. Since under normal conditions not all of the alarm processing software is executed, during a single data scan the time required to execute all the software and communications necessary for abnormal conditions may be excessive. The maximum number of alarms which can be handled by the alarm handling system without backlog or loss of alarm information is dependent on a number of factors principally:

- 1) the data scan rate
- 2) the number of data points scanned
- 3) the type of plant interface equipment implemented
- 4) the alarm handling system computer capabilities and communication configuration
- 5) the complexity of the alarm condition statements
- 6) the form of operator display used, for example, printers can be slow causing backlog

The prototype alarm handling system's performance was found to be limited by the plant interface equipment and the communication structure. Processing time required to execute alarm information was found to be insignificant as compared to communication and data collection times. The prototype alarm handling system is limited to the generation of 10 alarms per second as restricted by the communication hardware. If the alarm condition persists after the initial data scan period, the alarm generation software continues to produce alarm information restricted by this rate until all

alarm conditions have been notified. Improved communication structures are estimated to improve this rate ten fold. It should be possible to identify a credible alarm load for a particular plant application and perform a test to determine if the alarm load is excessive.

CHAPTER 8

CONCLUSION

In this thesis a [fully operational alarm handling system has been developed based upon studies of alarm system requirements on process plant and existing methods for dealing with alarms.]

It was noted that current practices of dealing with alarms appear to be inadequate or impractical for many process plant applications. A contributing factor is that computer control of process plant has advanced rapidly in recent years resulting in a carry-over of traditional control practices. Plant alarm systems are symptomatic of this problem and consequently the alarm system is often the least satisfactory aspect of the control system. Additionally a survey of the literature has shown that process plant alarm systems have been largely neglected.

[A study of the role of alarms on process plant showed that many aspects of an alarm system have not been extensively examined.] ^{especially in alarm system design.} Further it was concluded that it would be useful to develop an alarm system which would be capable of performing alarm generation functions found in a wide variety of alarm system philosophies from alarm annunciators through to alarm analysis. A study of alarm requirements on various types of process plant identified some alarm detection functions which would be useful in such a comprehensive alarm system.

The methodology for generating alarm information developed from the need to express and implement the alarm

detection functions in a working system. The resulting three tier procedure, data acquisition, event processing, and alarm generation, was found useful and was developed into an alarm system strategy as well as a plant and alarm data input structure for user programming of the system.

Using enhanced Boolean expressions the user can define complex alarm conditions on the plant which can be the result of a particular combination or sequence of events. It was found that additional operators were required to express and evaluate some of the alarm conditions resulting in the proposal of some enhanced Boolean operators.

Implementation of the alarm handling functions in a general purpose alarm system required careful consideration of the sort of plant applications which could be anticipated. It was decided that the system could be developed as a versatile and flexible stand-alone computer package which would have applications on small process plant. This assumption was convenient for justification of a microprocessor based system which could be useful and manageable not only by users on process plant but also as a tool for further studies of alarm systems in general.

[The resulting alarm handling system was found to be capable of supporting most of the alarm detection functions identified. The system comprised of an off-line alarm data base generation system and an on-line alarm handling system which can deal with up to 250 alarms with a one second time resolution.]

As would be expected there are some difficulties with the system and improvements have been proposed and discussed. Some of the more significant difficulties are the alarm data base structure and format and the difficulties with data acquisition which both require

further work. There is a need for further studies in the relationship of time related and non-time related events and the evaluation of these relationships.

Although the prototype alarm handling system would appear to satisfy many alarm information generation needs, more generally there are many outstanding problems concerning alarm systems on process plant which require further studies. Some of the important topics are:

- 1) The development of an alarm system methodology which would define the selection of alarms and alarm limits on a process plant. This includes the selection of the type of alarm system and the optimum 'level of alarming' for particular plant applications.
- 2) The formulation of a technique for measuring the performance of an alarm system.
- 3) The study of the operator and his role in the overall plant control scheme. Much more work is required to evaluate the operator's perception of alarm data, his diagnostic performance with various alarm systems, and his use of the alarm handling system in particular.

The prototype alarm handling system can contribute to the enhancement of alarm system performance by improving the three fundamental alarm system functions by assisting the operator in the:

- 1) Detection of fault conditions.
- 2) Diagnosis of faults.
- 3) Development of an action strategy.

In summary the alarm handling system provides a facility for extracting information from the plant and has adequate data manipulative power to generate a wide variety of improved quality alarm information for alarm displays. If properly utilized the alarm handling system has the ability to reduce alarm load and to generally improve alarm information accuracy. There are many aspects of process plant alarm systems which require further studies. It is hoped that the alarm handling system discussed in this thesis will aid in these studies as a highly flexible tool which can be used for further evaluation of alarm system methodologies while combining features from a variety of methods of dealing with alarms.

It is concluded that alarm systems can be considerably improved by using the alarm handling techniques developed and implemented in this thesis. The general purpose nature and unique flexibility of the alarm handling system provide a valuable contribution to the alarm system technologies available for chemical processing plants.

REFERENCES

1. Lees, F.P., 1980, "The Alarm Problem in Process Control", Proc. Course in Digital Control, Dept Chem Eng, University of Adelaide, Australia.
2. Andow, P.K., and Lees, F.P., 1974, "Process Plant Alarm Systems: General Considerations", Proc. 1st Int. Symp. on Loss Prevention, Hague, Netherlands.
3. Kortlandt, D., and Kragt, H., 1978, "Ergonomics in the Struggle Against 'Alarm Inflation' in Process Control Systems - Many Questions, Few Answers", Journal A, 19, 135-142.
4. Kortlandt, D., and Kragt, H., 1980, "Process Alarm Systems as a Monitoring Tool for the Operator", Proc. 3rd Int. Symp. on Loss Prevention, Basle, Switzerland.
5. Jervis, M.W., 1980, "Integrated Data and Alarm Systems for Central Control Rooms", Proc. Enlarged Halden Project Group Meeting, Report HPR-269, Paper 1, Lilliehammer, Norway.
6. Crossman, E.R.F.W., 1960, "Automation and Skill", DSIR, Problems of Progress in Industry, No. 9, HM Stationary Office.
7. Welbourne D., 1965, "Data Processing and Control by a Computer at Wylfa Nuclear Power Station", in Advances in Automatic Control, Inst. Mech. Eng., p 92.
8. Shukla, J.N., and Wong, R.H., 1975, "Nuclenet Control Complex", Proc. of the Specialists Meeting on Control Room

Design, IEEE, San Francisco, July 1975.

9. Welbourne, D., 1968, "Alarm Analysis and Display at Wylfa Nuclear Power Station", Proc. IEE, 115 (11), 1726-1732.

10. Kay, P.C.M., 1966, "On-Line Computer Alarm Analysis", Ind. Electron., 4, p 50.

11. Kay, P.C.M., and Heywood, P.W., 1966, "Alarm Analysis and Indication at Oldbury Nuclear Power Station", in Automatic Control in Electricity Supply, IEE Conference Publication 16, pt1, 295-317.

12. Patterson, D., 1968, "Application of a Computerised Alarm Analysis System to a Nuclear Power Station", Proc. IEE, 115 (12), 1858-1864.

13. Andow, P.K., 1981, "Disturbance Analysis Systems", 2nd Nat. Conf. on Engineering Hazards - Software, Systems and Costs, London, Jan 27-28, 1981.

14. Øwre, F., and Felkel, L., 1978, "Functional Description of the Disturbance Analysis System for the Grafenrheinfeld Nuclear Power Plant", Halden Project Report, HPR 221.14.

15. Meijer, C., and Frogner B., 1980, "On-Line Power Plant Alarm and Disturbance Analysis Sytem", Electric Power Research Institute, Palo Alto, CA., Report No. NP-1379.

16. Lees, F.P., Andow, P.K., and Murphy C.P., 1981, "The Propagation of Faults in Process Plants: A Review of the Basic Fault Information", Reliability Engineering, 1 (2), p 149.

17. Bastl, W., and Felkel, L., 1981, "Disturbance Analysis

Systems", in Rasmussen, J., and Rouse, W.B., ed., "Human Detection and Diagnosis of System Failures", Plenum Press, New York, USA.

18. Long, A.B, et al, 1980, "Summary and Evaluation of Scoping and Feasibility Studies for Disturbance Analysis and Surveillance Systems (DASS)", Electric Power Research Institute, Palo Alto, CA., Report No. NP-1684.

19. Corcoran, W.R., et al, 1980, "The Critical Safety Functions and Plant Operations", Int. Conf. on Current Nuclear Power Plant Safety Issues, Stockholm, Sweden.

20. Visuri, P.J., et al, 1981, "Handling of Alarms with Logic (HALO) and other Operator Support Systems", OECD Halden Reactor Project, Report HWR-24, Halden, Norway.

21. Visuri, P.J., and Øwre, F., 1981, "A Candidate Approach To A Computer Based Alarm Handling System (HALO)", OECD Halden Reactor Project, Report HWR-23, Halden, Norway.

22. Instrument Society of America, 1965, "Specifications and Guides for the Use of General Purpose Annunciators", ISA-RP18.1, Pittsburgh, Pennsylvania.

23. Barth, J., and Maarlevard, A., 1967, "Operational Aspects of a D.D.C. System", I. Chem. E. Symposium Series No. 24.

✓24. Andow, P.K., 1973, "A Method for Process Computer Alarm Analysis", PhD Thesis, Loughborough University of Technology, Loughborough, Leicestershire, England.

✓25. Andow, P.K., and Lees, F.P., 1975, "Process Computer Alarm Analysis: Outline of a Method Based on List Processing", Trans. Inst. Chem. Eng., 54, p 195.

26. Andow, P.K., 1980, "Real-Time Analysis of Process Plant Alarms Using a Mini-Computer", Computers and Chem. Eng., 4, 143-155.
27. British Standards Institution, 1976, "Colours of Indicator Lights and Push Buttons", BS4099, Part 1 of "Colours of Indicators and Digital Readouts".
28. British Standards Institution, 1977, "Flashing Lights, Annunciators and Digital Readouts", BS4099, Part 2 of "Colours of Indicators and Digital Readouts".
29. Berenblut, B.J., and Whitehouse, H.B., 1977, "A Method for Monitoring Process Plant Based on a Decision Table Analysis", The Chem. Engr., 318, 175-181.
30. Munday, G., 1977, "Anticipator; A Concept For Safety Surveillance in Process Plant", The Chem. Engr., 3, 181.
31. Duncan, K.D., and Gray, M.J., 1975, "An Evaluation of a Fault Finding Training Course for Refinery Process Operators", J. Occup. Psychol., 48, 199-218.
32. Frogner, B., and Meijer, C.H., 1978, "On-Line Power Plant Alarm and Disturbance Analysis System", Electric Power Research Institute, Palo Alto, CA., Report No. NP-613.
33. Edwards, E., and Lees, F.P., 1974, The Human Operator in Process Control, Taylor & Francis, London.
34. Edwards, E., and Lees, F.P., 1972, Man and Computer in Process Control, The Institution of Chemical Engineers, London.
35. Lees, F.P., 1980, Loss Prevention in the Process

Industries, Vol 1 & 2, Butterworth, London.

36. Jervis, M.W., 1980, "Integrated Data and Alarm Systems For Central Control Rooms", Central Electricity Generating Board, E/REP/143/1980.
37. Umbers, I.G., 1977, "A Review of the Human Factors Data on Input Devices used for Process Computer Communication", Department of Industry, Warren Spring Laboratory, Stevenage, Herts., England, Report No LR265(CON).
38. Umbers, I.G., 1976, "CRT/TV Displays in the Control of Process Plant: A Review of Applications and Human Factors Design Criteria", Department of Industry, Warren Spring Laboratory, Stevenage, Herts., England, Report No LR242(CON).
39. Jervis, M.W., and Pope, R.H., 1977, "Trends in Operator - Process Communication Development", CEGB Report, E/REP/054/77, Gloucester, England.
40. Kiguchi, T., and Sheridan, T., 1979, "Criteria for Selecting Measures of Plant Information with Application to Nuclear Reactors", IEEE Trans. on Systems, Man, and Cybernetics, Vol SMC-9 No 4, April 1979, 165-174.
41. Danchak, M.M., 1980, "The Content of Process Control Alarm Displays", Proc. Int. ISA Conf. and Exhibition, Houston, USA.
42. Lawley, H.G., 1974, "Operability Studies and Hazard Analysis", CEP, 70 (4), 45-56.

43. Anyakora, S.N., and Lees, F.P., 1973, "The Detection of Malfunction Using a Process Control Computer; Simple Noise Power Techniques for Instrument Malfunction", in "The Use of Digital Computers in Measurement", Conf. Pub. 103, Instn. Elec. Engr., London, England, 35.

BIBLIOGRAPHY

- A1 Andow, P.K., 1981, "Alarm and Disturbance Analysis Systems For Process Plants", U.N. Economic Commission for Europe Chemical Industry Committee, Seminar on Process Automation in the Chemical Industry, Noordwijkerhout, Netherlands, April 27 - May 1, 1981.
- A2 Andreiev, N., 1976, "Annunciators Hold Ground Against the CRT", Control Engineering, 23, 46-48.
- A3 Anyakora, S.N., and Lees, F.P., 1972, "Detection of Instrument Malfunction by the Process Operator", Chem. Engr., London, England, 264:304.
- B1 Bagchi, P.E., and Gottilla, S.C., 1981, "Application Of Human Engineering Criteria To Annunciator Display Systems In A Large Fossil Power Station", IEEE Transactions on Power Apparatus and Systems, PAS-100 (6), 2759-2765.
- B2 Bosley, M.J., et al, 1981, "SWEPSPEED User's Guide", S.W. Region CEGB, Report SSD/SW/81/N32-47, Bristol, England.
- B3 Burton, P.L., 1978, "Improving The Man-Machine Interface", Control and Instrumentation, 10, May, p 21-23.
- B4 Buttner, W.E., et al, 1979, "Function and Design Characteristics of The STAR Disturbance Analysis System", in "Procedures And Systems For Assisting an Operator During Normal and Anomalous Nuclear Power Plant Operation Situations", IAEA/NPPCI Specialist Meeting, Munich, W. Germany, December 5-7, 1979.
- C1 Carter, R.J., 1971, "On-Line Digital Control Systems-The Role of the Process Operators", Data Reduction

Symposium, Institute of Measurement and Control, London, March 1971.

C2 Considine, D.M., 1974, Process Instruments and Controls Handbook, McGraw-Hill Book Co.

D1 Danchak, M.M., 1977, "Alpha-Numeric Displays for Man-Process Interface", Advances in Instrumentation, 32 (1), 197-213.

D2 Danchak, M.M., 1976, "CRT Displays for Power Plants", Instrumentation Technology 23 (10), 29-36.

D3 Del Paine, N., 1974, "Rapid Association and Editing of Computer Monitored Alarm Systems", Proceedings of the Specialists Meeting on Control Room Design, July, 109-112.

D4 Desmonde, W.H., 1964, Real-Time Data Processing Systems: Introductory Concepts, Prentice-Hall, Inc., Englewood Cliffs, N.J.

D5 Diehl, W., 1976, "Process Control Software Review", Instrumentation Technology, March, 49-53.

D6 Duncan, K., 1981, "Training For Fault Diagnosis in Industrial Process Plant", in "Human Detection and Diagnosis of System Failures", Rasmussen, J., and Rouse, W.B., ed., Plenum Press, New York, USA, 553-575.

D7 Duncan, K.D., and Gray, M.J., 1975, "Scoring Methods for Verification and Diagnostic Performance in Industrial Fault-Finding Problems", J. Occup. Psychol., 48, 93-106.

E1 Edwards, E., 1979, "Flight Deck Alarm Systems", Feb, 11-14.

E2 Engineering Equipment Users Association (DOI), 1981, Guide to the Engineering of Microprocessor Based Systems for Instrumentation and Control, EEUA Handbook No 38-1981.

F1 Felkel, L., 1980, "Disturbance Analysis Systems - State of the Art", GRS Report, GRS-A-523.

F2 Felkel, L., 1979, "Analytical Methods And Performance Evaluation Of The STAR Application In The Grafenrheinfeld Nuclear Power Plant", in "Procedures and Systems for Assisting an Operator During Normal and Anomalous Nuclear Power Plant Operation Situations", IAEA/NPPCI Specialist Meeting, Munich, W. Germany, December 5-7, 1979.

F3 Fisher, C., and Gamble J.N., 1981, "The Development of an Intelligent Reliable Database Driven Alarm System at the ISR", IEEE Trans. Nuclear Science, NS-28 (3).

G1 Giloi, W.K., 1978, Interactive Computer Graphics, Data Structures, Algorithms, Languages, Prentice-Hall, Inc., Englewood Cliffs, N.J.

G2 Goodstein, L.P., 1981, "Discriminative Display Support For Process Operators", in "Human Detection and Diagnosis of System Failures", Rasmussen, J., and Rouse, W.B., eds., Plenum Press, New York, USA, 433-499.

H1 Henn, W.D., 1979, "Alarm Status Monitoring and Reporting", RCA Engineer, 25 (3), 47-49.

H2 Himmelblau, D.M., 1980, Fault Detection and Diagnosis in Chemical and Petrochemical Processes, Elsevier Scientific Publishing Company, London.

H3 Hoenig, G., 1981, "Real-Time Design Considerations for an On-Line Display Package", internal report, Department of

Industry, Warren Spring Laboratory, Stevenage, England,
June, 1981.

H4 Hoenig, G., 1981, "C.E.G.B. Alarm Systems: Past, Present and Future", Internal Report, Dept Chem Eng, Loughborough University of Technology, Loughborough, England.

H5 Hoenig, G., Umbers, I.G., and Andow, P.K., 1982, "Computer Based Alarm Systems", 4th Int. IEE Conference "Trends in On-Line Computer Control Systems", University of Warwick, 5-8 April, 1982.

H6 Hol, J.Ø., and Øhara, G., 1980, "Development of Guidelines and Recommendations for Colour Display Based Information Presentation System", OECD Halden Reactor Project, Halden, Norway, Report HPR-263.

H7 Hollands, D.H., 1977, "Display and Reporting Technique for Categorizing Alarms", IEEE, Power Engineering Society, Winter Meeting, N.Y., January 30-February 4, 1977.

H8 Huyten, F.H., 1981, "Development in Instrumentation and Automation of Chemical Plants", UN Seminar on Process Automation in The Chemical Industry, Noordwijkerhout, Netherlands, April 27 - May 1, 1981, CHEM/SEM. 10/R.14, 4 March 1981.

J1 Jenkins, B., 1978, "Alarm Systems", Control and Instrumentation, 10 (1), 24-25.

J2 Jervis, M.W., 1980, "Current Views on Alarm Handling and Alarm Analysis", Central Electricity Generating Board, E/REP/154/1980.

J3 Jervis, M.W., 1972, "On-Line Computers in Power

Stations", Proc. IEE, IEE Reviews, 119, No 8R, 1052-1075.

J4 Jutila, J.M., 1981, "Alarms and Annunciators: Technology Art", In Tech., Sept., 16-24.

J5 Jutila, J.M., 1981, "Guide To Selecting Alarms and Annunciators", In Tech., March, 35-43.

L1 Lambert, H.E., 1977, "Fault Trees for Locating Sensors in Process Systems", CEP, 73 (8), 81-85.

L2 Lambert, H.E., and Yadigaroglu, G., 1977, "Fault Trees for Diagnosis of System Fault Conditions", Nuclear Science and Engineering, 62, 20-34.

L3 Lawley, H.G., 1980, "Safety Technology in the Chemical Industry: A Problem in Hazard Analysis With Solution", Reliability Engineering, 1 (1980) 89-113.

L4 Lees, F.P., 1976, "A Review of Instrument Failure Data", in "Process Industries Hazards", I. Chem. E. Symposium Series 47, p 73.

L5 Lees, F.P., 1980, "Human Factors In Process Control", Proc. Course on Digital Control, Chap 9, Dept Chem Eng, University of Adelaide, Australia.

L6 Lees, F.P., 1980, "Studies Of The Operator In Process Control", Chap 10, idem.

L7 Lees, F.P., 1980, "The Display Problem In Process Control", Chap 11, idem.

L8 Lees, F.P., 1980, "Alarm Analysis by Process Computer", Chap 13, idem.

- L9 Lees, F.P., 1981, "Computer Support For Diagnostic Tasks In The Process Industries", in "Human Detection and Diagnosis of System Failures", Rasmussen, J., and Rouse, W.B., eds., Plenum Press. New York. USA. 369-388.
- L10 Lihou, D.A., 1981, "Aiding Process Plant Operators in Fault Finding and Corrective Action", *idem*, 501-522.
- L11 Lind, M., 1981, "The Use of Flow Models for Automated Plant Diagnosis", *idem*, 411-432.
- M1 Malone, T.B., et al, 1980, "Human Factors Evaluation of Control Room Design and Operator Performance at Three Mile Island - 2", US NRC Report NUREG/CR-1270 Vol. 1.
- M2 Marshall. E.C.. et al, 1981, "Panel Diagnosis Training for Major-Hazard Continuous-Process Installations", *The Chemical Engineer*, 365, Feb., 66-69.
- M3 Martin-Solis, G.A., et al, 1977, "An Approach to Fault Tree Synthesis for Process Plants", Proc. of the 2nd Int. Symp. on Loss Prevention and Safety Promotion in the Process Industries, Heidelberg, W. Germany, September 6-9.
- M4 Meijer, C.H., 1980, "Operational Support Systems to Improve Man-Machine Interaction in a Nuclear Power Plant", Enlarged HPG. on Water Reactor Fuel Performance and Application of Process Computers in Reactor Operation, HPR-269.
- M5 Munday, G., 1977, "On-Line Monitoring and Analysis of the Hazard of Chemical Plant". Loss Prevention and Safety Promotion, 2, 273.
- M6 Mulder, M.C., and Fasang, P.P., 1978, "A Microprocessor Controlled Substation Alarm Logger", IECI '78, Proc. Ind.

Applications of Microprocessors, March 20-22, 1978, 2-6.

M7 Murphy, H.N., 1969, "The Future Roll of Process Monitoring Display and Recording Systems", Proc. 24th Annual ISA Conference, Houston, USA, October 27-30.

Ø1 Øwre, F., and Felkel, L., 1980, "A Disturbance Analysis System and It's Operational Features". in "Automation for Safety in Shipping and Offshore Petroleum Operations", Aune, A.B., and Vlietstra. J., eds., North Holland Publishing Company.

P1 Pau, L.F., 1981, "Application of Pattern Recognition to Failure Analysis and Diagnosis" in "Human Detection and Diagnosis of System Failures", Rasmussen, J., and Rouse, W.B. eds., Plenum Press, New York. USA. 389-410.

P2 Pluhar, K., 1980, "Alarms and Annunciator Choices Range from Simple to Complex", Control Engineering, Oct., 87-90.

P3 Pope, R.H., 1978, "Power Station Control Room and Desk Design, Alarm System and Experience in the Use of CRT Displays", Proc. IAEA, Vol 1, Series 5, Nuclear Power Plant Control and Instrumentation, Cannes, France, April 24-28. 1978, p 209.

R1 Rasmussen J., 1981, "Models of Mental Strategies in Process Plant Diagnosis". in "Human Detection and Diagnosis of System Failures", Rasmussen, J., and Rouse, W.B., eds, Plenum Press, New York, USA, 241-250.

R2 Roach J.R., and Lees, F.P., 1981, "Some Features of and Activities in Hazard and Operability (Hazop) Studies", The Chemical Engineer, No 373, Oct, 456-462.

S1 Sheridan. T.B., 1981, "Understanding Human Error and

Aiding Human Diagnostic Behaviour in Nuclear Power Plants", in "Human Detection and Diagnosis of System Failure", Rasmussen, J., and Rouse, W.B., eds, Plenum Press, New York, USA, 19-36.

S2 Singleton, W.T., Easterby, R.S., and Whitfield, D.C., 1967, The Human Operator in Complex Systems, Taylor & Francis, Ltd., London.

S3 Skrokov, M.R., 1980, Mini- and Microcomputer Control in Industrial Process: A Handbook of Systems and Application Strategies, Van Nostrand Reinhold Co., New York, USA, 10020.

S4 Slack, C.B., 1964, "Considerations for Plant Monitoring", Instruments and Control Systems, Dec., 37 (12), 93-95.

S5 Smith, C.L., 1972, Digital Computer Process Control, Intext Educational Publications, London.

S6 South, G.F., 1974, Boolean Algebra and it's Uses, Van Nostrand Reinhold Co., New York, VNR New Mathematics Library 4.

S7 Stainthorp, F.P., and West, B., 1974, "Computer Controller Plant Start-Up". The Chemical Engineer, Sept, 527-530.

S8 Stewart, R.M., 1971, "High Integrity Protective Systems" in "Major Loss Prevention" 99.

S9 Swain, A.D., and Guttman, H.E., 1980, "Handbook on Human Reliability Analysis With Emphasis on Nuclear Power Plant Applications", NRC, NUREG/CR-1278.

T1 Twydell, D., 1978, "Alarms With TDC 2000", Control and Instrumentation, 28-31.

U1 Umbers, I.G., 1979, "Models of the Process Operator", Int. Journal of Man-Machine Studies, 11, 263.

U2 Umbers, I.G., and King, P.J., 1980, "An analysis of Human Decision Making in Cement Kiln Control and the Implications for Automation", Int. J. Man-Machine Studies, 12, 11-23.

W1 Wahlstrom, B., and Rinttila, E., 1980, "Inhibition of Alarms during Nuclear Power Plant Operation", Enlarged HPG Meeting on Water Reactor Fuel Performance and Application of Process Computers in Reactor Operation, HPG-269.

W2 Wollf, H.S., 1970, "The Hospital Ward - A Technological Desert", in "Instruments in Working Environments", Scientific Instrument Research Association, London, 90.

