AN INTEGRATED APPROACH INCORPORATING DYNAMIC AND STATIC SECURITY LIMITS IN OPTIMUM POWER DISPATCH

Thesis presented for the degree of
Doctor of Philosophy
at the University of Strathclyde

BY

TAK SHING CHUNG

B.Sc.(Eng.), M.Sc.

Supervisor : Professor K. L. Lo
Power Systems Research Group
University of Strathclyde
Glasgow, United Kingdom
(June 1993)

DEVOTED TO MY FAMILY

DECLARATION OF AUTHOR'S RIGHTS

SUMMARY

Optimum power dispatch is performed in a power system to determine the most economic power dispatch condition for a certain system loading. In this thesis the main focus is on the investigation of this problem and its improved application by including both dynamic security and static security limits in its solution. The aim is to develop an efficient and practical on-line method of optimum power dispatch with due regard to the necessary security requirements.

A critical review of the current practices of security and optimization in power system operation shows that they are essential elements in Energy Management System computer softwares. Since optimality and security present conflicting requirements on system operation, it is both logical and beneficial to develop an integrated approach to satisfy all the security limits in optimum dispatch. The classical approach to consider only the static security limits in optimum dispatch calculation is found to be insufficient in providing the essential informations on the dynamic security performance. This problem is causing increasing concern with the recent trend to load power systems more closer to their stability limits in order to achieve maximum economy.

A new formulation of the security constrained optimum dispatch problem with an integrated approach to consider both dynamic and static security limits is thus proposed in this thesis. The Optimum Power Flow (OPF) formulation uses a Recursive Quadratic Programming algorithm applied in the compact modelling of the system. This formulation consists of a decoupling process of the active and reactive power optimizations. The investigation into on-line security control shows that insufficient attention on dynamic security in present practice could endanger the system integrity in the contingency state. This leads to the development of a new scheme to integrate both dynamic and static security assessments. Direct application of classical transient stability assessment methods using numerical integration of swing equations is found to be too slow and a new method based on reduced dynamic equivalent is investigated. The method is based on an efficient dynamic security assessment scheme which assesses the on-line operating state of the system. A dynamic security margin is defined to measure the robustness of the system when it is subjected to a selected scenario of dynamic contingency. The method also identifies the critical machine or cluster of machines that would cause transient instability, and proposes preventive control strategies to improve the dynamic security performance. This is integrated in the approach as a preventive control module. The module aims to prevent the system from reaching probable system collapse due to contingency that could cause cascading tripouts in the system.

Extensive simulation tests are performed using the approach in several example networks together with validation case studies compared to full load flow and transient stability tests. The results demonstrate that the approach is fast and reliable with good potential for on-line application in stability limited power systems.

Acknowledgements

I am deeply indebted to my supervisor, Professor Kwok Lun Lo, Head of the Power Systems Research Group, for his keen interest, valuable guidance, advice and stimulating discussions.

My sincere thanks go to Hong Kong Polytechnic for providing financial support as well as study leave for me to complete this research work. I like to thank Dr. C. S Chang, who has acted as my local co-supervisor for the initial stage of this project when Dr. Chang was at Hong Kong Polytechnic. I also like to thank Dr. A. K. David and Professor M. S. Demokan for valuable discussions and encouragement.

I am grateful to my friends in China Light and Power Company and Hong Kong Electric Company for the discussions and comments.

I would also like to thank my colleagues of the Power Systems Group for their useful contributions.

Finally, I would like to thank all members of my family and all my friends who helped to make this work a success.

TAK SHING CHUNG

CONTENTS

Chapter 1 Introduction

Chapter 2 Secure and Optimum Power Dispatch - Definition, Role and Implementation

Chapter 3 Optimum Power Dispatch

Chapter 4 Dynamic Security Analysis

Chapter 5 A New Incorporated Dynamic Security and Static Security Limited Optimum Power Dispatch

Chapter 6 Development of A New Control Strategy for Secure and Optimum Power Dispatch

List of Principal Symbols

Unless stated specifically, throughout the thesis, block letters (heavily printed) denote vectors or matrices, capital letters or lower case letters denote scalars.

CCA	critical clearing angle
CCT	critical clearing time
DSA	dynamic security assessment
EEAC	extended equal area criterion
LP	linear programming
OMIB	one machine infinite bus model
OPF	optimum power flow
QP	quadratic programming
H	Hessian matrix
P	real power
Q	reactive power
T	transpose of matrix
N_g	number of generators
γ_i	initial accerleration of machine i
P_m	mechanical power
P_e	electrical power
δ_i	rotor angle of machine i
M_i	angular momentum of machine i

Chapter 1

Introduction

1.1 Background

Power system engineers are faced with the challenging task of operating one of the most complex engineering systems : the electric power system. Power systems have developed in size and complexity to the point where increasingly sophisticated tools are necessary for solving the numerous problems that arise in the control and operation of these systems. With increasing interconnections and new privatised operating environments recently, the control and operation of power systems are undergoing many revolutionary changes and new concepts are being evolved to meet new challenges. Increasing use of computers is the most significant development. In this context, the considerations of optimization and security are two key factors in the on-line computerised control and operation of power systems. In line with such developments, there are significant new changes in the consideration of optimization and security and their integration in the Energy Management System computer programs of a typical system control centre.

It is thus the main objective of this thesis to conduct a critical review of the two concepts of optimization and security in power system operation and to develop a new improved methodology to integrate both dynamic and static security limits in optimum power dispatch calculation. Firstly, the basic concepts of optimization and security are reviewed. In principle, optimization and security may present conflicting requirements on the system operating states [1]. It is both logical and necessary to coordinate security and optimization requirements to reach a compromise solution. The conventional approach is to find the system solution at the most economical operating condition within acceptable security limit by considering security as constraints in the optimization process. Mathematical optimization techniques such as Optimum Power Flow (OPF) have been applied to solve this problem formulation to a certain degree of success [1,2]. However, with the increasing trend to load power system closer to their stability limit in order to achieve increased economy, there is a justified need to re-examine the concept of security. This is especially the case with the dynamic security aspect which includes the phenomeon of transient stability and voltage collapse that could lead to cascading tripouts and system collapse. In the current literature, the subject of dynamic security assessment integrated in on-line optimum power dispatch operation has not been addressed. In this thesis, a new integrated approach is formulated to incorporate dynamic and static security limits in optimum power dispatch calculation to address this problem.

The main contribution of this thesis is thus to develop a new method that could automatically incorporate both dynamic and static security requirements in optimum power dispatch calculation suitable for use in modern Energy Management System computer programs in control centres. The core idea consists of a new technique to apply as an integrated module a dynamic security monitoring scheme in the on-line economic operation of stability limited power system. The formulation is based on an efficient dynamic security assessment program which assesses the on-line operating condition of the system after performing an optimum power flow (OPF) calculation. A dynamic security margin may also be derived to measure the robustness of the system when it is subjected to a selected scenario of contingency. The method will ensure that the state of operation is both economical and is of satisfactory security - referring to both static and dynamic security. The method also identifies the critical machine or a cluster of machines among the generating plants in the system that may invoke transient instability based on certain selected dynamic contingency. Hence preventive control actions are determined to avoid such cascading tripouts that may lead to system collapse. To apply the methodology effectively, the thesis also discusses the relevant fast direct methods of dynamic security assessment in current literature that may be used. A proposed scheme that uses a reduced dynamic equivalent is hence described and simulation results of sample power systems are presented to collaborate the conclusions.

1.2 Structure of thesis

In this section, the strucure of the contents of this thesis is presented. The main ideas of each chapter is explained in sequence. In Chapter 2, the definition, role and implementation of secure and optimum dispatch are described. The evolution of power system security concept is explained in the chapter. The provision of system security has been gradually accepted as a key indicator of quality in power system operation during the period from the Sixties to early Seventies [1,2,3,7,8]. One of the milestone in this development is a series of classical papers on power system security by T. E. Dy Liacco [2] in early seventies. It was at that time that the advent of computer application in power system control made a major impact in power control centre design. Recently power utilities are again undergoing another period of changes, notably in the increased competitive environoment as a result of privatisations and greater sharings of power system grids. The issues of transmission access and wheelings will invariably have impact on the conventional concepts of power system security and its control. This is witnessed by some recent reports, an example being by a Canadian utility reporting in IEEE on concerns with dynamic security infringements in applying on-line OPF programs [21,32]. In broad terms, the classical static security concept is found to have some deficiencies to ensure a completely secure operation on the occurrence of certain credible contingency. In this context, static security would not provide the necessary clue as to whether the power system would survive the transition from a normal pre-contingency steady state to a post-contingency state. This particular aspect is considered to be an important element of dynamic security of the system. However, due to both economic and other constraints, the dynamic security consideration is often neglected in real-time power system operation.

This is in great contrast with the static security control which has been well researched. [1,2,3] The dynamic security problem is causing concern with the increasing trend to load existing power systems which are highly interconnected to their stability limits in order to achieve maximum economy. In addition, the planned use of Optimum Power Flow (OPF) programs in on-line operation has reported problem of possible dynamic insecurity on contingency, with the recent report by the Canadian utility being a typical example [32]. In this respect, Chapter 2 aims to present a clear, updated definition and review of the security and optimization concepts. The implementation in flow diagram form of the integrated security and optimization techniques is also presented to illustrate its modern application format.

In Chapter 3 , a review of optimum power dispatch methods is reviewed and tested. OPF techniques have potential applications in power system operation, operation planning and planning environments. Recent advancements of their application have been extensively reported in the current literature. However, the consideration of security implications in on-line OPF usage has received less attention. This is especially the case for dynamic security considerations which include transient stability infringements and voltage collapse. The situation where on-line power system operators are required to make the correct operational decisions within the extremely short time span during real-time operations is thus causing concern. This is especially true in the case of finding a suitable compromise between economy and security in real-time power system operation. The advent of computer control has contributed a lot towards the ideal goal of a true secure and optimal operation. However, in this context a new concept in secure and optimum control is now possible with the new developments. This thesis hence attempts to lay the foundation of an approach to alleviate this problem based on on-line monitoring and control of the dynamic security integrated with an OPF program.

Conventionally, static security and dynamic security are analysed separately due to their differences in modelling and solution methods. [1,2,3] Static security defines the adequacy of the system's generation and transmission capacity to meet demand on contingency. Over the years many papers have been published on the formulations of including static security in OPF calculations.[1-4] In contrast, dynamic security is measured by the system's ability to withstand large , sudden disturbances and maintaining normal state of operation after the fault is cleared. Maintaining satisfactory dynamic security would help to avoid, on credible contingency, uncontrolled cascading tripouts that lead to system collapse. In this context, transient stability assessment is the principal component in dynamic security [5,19].

Despite the increased attention on dynamic security assessment, there is as yet no satisfactory practical solution to include it in OPF calculation in current literature.[13] In many utilities the current practice is to perform transient stability studies in the planning stage with detailed system models in order to predict the system's likely performance to those probable scenarios of disturbances. These off-line studies conducted through numerous computer simulations will be taken to establish the operational guideline limits of loading. However, in actual operations, the actual system loading conditions and parameters may be different from those assumed in simulations. Hence security constraints derived from those post-fault loadflow analyses are insufficient to ensure no degradation or even violation of system security. In order to ensure a truely secure operation, on-line security assessment with focus on its dynamic security is necessary.

In the investigation of this problem, it is found that the usual current trend in security constrained OPF techniques only considers the post-contingency line current limits (static security) and neglects the possible loss of transient stability during the transition from the pre-contingency operating state to the post-contingency state. This approach is not sufficient if the dynamic contingency would actually endanger the stable operation of the system. In some literature, for example [33], it is suggested to calculate the maximum loading limits of certain critical generators to avoid the above dynamic insecurity via off-line simulations. But this approach would also be inaccurate and does not work sufficiently well for a highly stressed system with stability problems ; for example, those cases of special loading conditions such as high abnormal loadings or unexpected outages already occurring in the pre-contingency state. It is thus proposed in the thesis that an on-line scheme to assess the current system state's dynamic security should be introduced as an integrated module in optimum power dispatch calculation.

A critical review is thus given in this chapter on the current practice of optimum dispatch techniques. The conventional methodology is to operate the system to determine the most economic solution within acceptable security limits by considering security as a constraint in optimization. Static security constrained optimization using the total generation cost as the objective function and static security requirements as constraints have been formulated and solved by mathematical programming techniques .[1-3] The a.c. load flow equations are then taken as the equality constraints and the security limits as the inequality constraints in the above optimization modelling.

Concurrently, dynamic security assessment (DSA) on-line is now on the verge of practical implementation,mainly due to the intensive research on fast direct methods of transient stability analysis.[31-33] This project proposes to extend the above concept to include the dynamic security constraint consideration in optimum dispatch calculation in order to meet the need for such dynamic security control in stability limited system. Use would thus be made of such fast direct method of transient stability calculation as an integrated module.

Chapter 3 thus further describes the use of an efficient optimum power dispatch method based on recursive quadratic programming. The theory, philosophy and the practical implementation of this OPF method is presented followed by case studies of several typical systems.

In Chapter 4 dynamic security analysis methods are described in more details. In the investigation of suitable on-line dynamic security assessment methods, a critical review is made on the current approaches in the literature to analyse dynamic security performance of power systems. The approaches may be broadly classified into three main types according to their analytical methodolgy. Firstly, extensive off-line case studies for a credible set of contingencies on the system may be performed by conventional numerical integration techniques to provide the operator with guidelines on line flow limits, interface line flows and generation limits. With the advent of parallel processing and new computer technology it may be possible to speed up this type of calculation and come closer to real-time use. However, the present thinking is to reduce the computing timing as much as possible by employing more efficient algorithms and using network reduction of dynamic equivalents. In addition, off-line study results may not be as reliable as originally designed since we may encounter special operating conditions due to unexpected events occurring.

The second type of approach makes use of the transient energy function calculations to identify the boundary of insecurity and is currently under intense research by researchers; for an example, Professor Fouad and his research group at Iowa [35] have been keen advocates of this approach. The method is in the process of refining its practical implemntation possibility but since the method basically finds the region of stability, it is not easy to formulate control action. [11] However further research work is continuing to improve its attraction and its on-line application could be a viable option in the near future.

Hence from the investigation in current literature,the third type of approach that is based on gross dynamic equivalencing of the external system is found to be the most promising for our application in Chapter 5. This method can also make use of a fast technique based on extended equal area criterion to the resultant reduced dynamic equivalent system[33]. One basic advantage of this method is that it shows promise to identify an energy margin for quantifying the dynamic security performance. The sensitivity of the energy margin to a system parameter may also be computed. These calculations can provide valuable guidelines to operators and may lead to the design of preventive control strategies as reported in Chapter 6. [33]

In Chapter 5 the rationale for using the adopted DSA method is described. The DSA analysis module in this thesis employs the above method to find the system's dynamic security performance based on the determination of the system critical clearing time on a contingency and to compare it with the designated security margin at the monitoring stage. The method also identifies the critical machine or cluster of critical machines for the contingency. This dynamic performance information is used to find preventive control actions to improve dynamic security if it is found to be unsatisfactory. An iterative method as an extension of the above monitor is also developed to determine the minimum power output change in order to satisfy the dynamic security constraint. Since the power system is carefully checked for its dynamic security and then reduced to an equivalent which consists of two machines, the analysis then proceeds to calculate the critical clearing time with a fast method called extended equal area criterion [33]. The method is tested to work well for large power system of practical real size network and for many possible operating conditions. In addition, since the method always obtains a two machine equivalent within reasonably fast time, the dynamic security calculation of its critical clearing time will not increase much in effort with increase in system size. This is an important consideration for real-time computing as the tests performed are based on small to medium size networks of up to 30 bus system. With this consideration in mind, the simulation results and the philosophy involved could be extended to very large networks.

The OPF problem is formulated as a Nonlinear Programming problem due to the nonlinearity of the objective function (for example cost curves of generators) and the highly nonlinear equality and inequlaity constraints. This formulation consists of the load flow equations as the equality constraints, the upper and lower bounds on generation outputs, and the functional constraints as the inequality constraints. The inequality constraints include the line thermal loading limits ,the equipment loading limits, and the busbar voltage level limits. Numerous papers have been published on applying various nonlinear programming methods to solve the formulation.[1]

In the investigation of suitable method in solving the optimum dispatch problem in this thesis, the algorithm of recursive Quadratic Programming (QP) method first suggested by Han-Powell [4,5,6] is applied. In this algorithm, an estimate to the solution of OPF at an iteration, is improved by taking a step length in a direction of movement. The direction of movement is obtained by solving a QP problem whose objective function is a second order approximation of the original objective function and whose constraints are first order approximation of the original constraints. In this thesis, the post-contingency static security limits such as line loading limits will be considered as the inequality constraints. This is incorporated as constraints by performing a D.C. load flow subroutine determine the line current changes in the post-contingency state. This method can thus incorporate preventive control of static security limits. The method also offers the following special features. The method offers a reliable and efficient technique for solving the optimum dispatch problem incorporating security limits. It can converge well even with infeasible starting values of control variables. With the use of a reduction technique to speed up the calculation time and reduce the order of magnitude of the required Hessian matrix , this is applicable in this OPF formulation since the state variables may be expressed in terms of the control variables by the load flow equations.[6] The static security may be expressed as the inequality constraint in this formulation. The consideration of loading limits may thus include both the pre-contingency and post-contingency steady state conditions.

A fast dynamic security analysis (DSA) methodology first derived by Xue,Van Cutsem and Ribbens-Pavella (1988) [33] is being adapted for use with a new, innovative scheme to determine the system's dynamic security with respect to preselected dynamic contingency in the network. The major steps may be summarised as follows. The multi-machine system is first subjected to a selected dynamic contingency. The initial acceleration of each machine is screened to identify the "critical " machine or cluster of critical machines. The system is subsequently reduced to a dynamic equivalent of the critical machine(s) and the rest of the external system. The resultant aggregate two machine equivalent may thus be analysed by extended equal area criterion method for its dynamic security performance. A security margin based on its critical clearing time to maintain transient stability is found. This is compared with the system dynamic security requirement (which may typically be the minimum protection time setting plus suitable time margin) to ascertain whether dynamic security is of satisfactory level or not. In this calculation it is necessary to evaluate dynamic security with preselected probable dynamic contingency. The usual practice of utilities is to use a pre-selected set of events. In our investigation, the most serious dynamic contingency with a three-phase short circuit at the generator terminal side of the transmission line followed by line switching to clear the fault is tested. When a system's critical machine or cluster is located, the case of a fault occurring at the terminal of that critical machine is tested for dynamic security performance.

As said the most serious dynamic contingency for the identified critical machine is a solid three-phase short circuit fault at the critical machine terminals followed by postfault line tripping for fault clearance. The identified critical machine(s) would be the machine(s) responsible for system separation should the contingency occur. Hence the following steps are used for the critical machine identification. Determine the initial acceleration of all machines on the occurrance of fault. Filter out the most probable critical machine candidates by comparing their initial accerleration values. Compute in turn the critical clearing times (CCT's) corresponding to each candidate machine. The machine that gives the smallest CCT is the most critical one and its value gives the resultant system CCT. The critical machine is modelled by a classical machine model while the remaining machines are modelled as an equivalent machine using the centre of angles concept [33].

The two machine equivalent is then transformed to an one-machine infinite-bus model for finding its CCT by an extended equal area criterion [33]. The computing speed of this module is extremely fast and is shown to have reliable results as compared to full multi-machine analytical study of swing curves using classical step-by-step numerical integration solution method. Also the computing time requirement will not increase drastically with increase in system size since a dynamic equivalent reduction is first performed, resulting in a simple two machine model being analysed for CCT at this stage. This would be an additional advantage from the real-time computing requirement point of view.

In Chapter 6 the development of the control strategy for secure optimal dispatch is presented. The main objective of designing the security preventive control module in this thesis is to determine the best system reconfiguration that can give acceptable dynamic security and at the same time the operation is the most economical. In this thesis, this module is arranged as an external loop to the OPF main programme. This approach is used for the following reasons. The OPF module is maintained as a separate module to retain its efficiency and good convergency characteristic. The preventive control module may be applied integrally or as add-on so that the dispatch engineer may regard the corrective action for dynamic security improvement as being consultative. As by-products of this calculation, the relative cost change, system CCT value change and the identification of critical machine(s) are available to the dispatcher.

Following this concept, extensive*p1307Xsimulationsare made including changing the limits of line flows, the power ouputs of generators etc to reduce dynamic insecurity. From the investigations it is found that the most effective parameter for this control is the active power output of generators and the following points are observed. The relative effects of line flows limits on the dynamic security are less significant than power generation changes in the systems which have been tested. In addition, the sensitivities of the security margin to the power outputs may also be computed analytically. In general, in an interconnected system, the critical generators that contribute to instability are those possessing more efficient operating characteristics but are also of relatively smaller inertia constant (smaller weight to capacity ratio for modern machine design). This makes the optimization results generally tending to load such machines more heavily and more close to their stability limit.

As a result, the strategy of reallocating the real power generations of machines is adopted in this thesis. In order to achieve the objective of minimizing total generating cost within the acceptable security limit, a new set of power generations is to be found and used as the new inequality constraint limits in the OPF loop. Since the operating conditions will be altered when the power generations of the critical machine(s) are changed, it is necessary to compute from the new load flow conditions the new security level. An iterative process for different generation values will be required. It is both inaccurate and unreliable to obtain a realistic solution just by trial and error; thus, a systematic iteration algorithm called Modified False Position Method [36] is used in this module. In principle, this algorithm extrapolates from some suitable initial assumed values,to obtain the best estimate of power generation that would give the required security level (in this case the critical clearing time). For a not too excessive range of input values, the algorithm works satisfactorily since the derivation of this algorithm assumes that the nonlinear relationship between the input and output parameters must be continuous. In this case, the input is the P generation of critical machine and the output is the system CCT found by calling the transient stability subroutine and a fast loadflow subroutine.

In this thesis, computer programs for the simulation tests are written in FORTRAN language and run in the VAX computer in Hong Kong Polytechnic. Several systems with a large number of operating conditions have been used so as to cover a variety of configurations with realistic operating conditions. They include a 5-bus test network , a 14-bus network and a 30-bus modified IEEE sample system. The disturbances considered are 3-phase short-circuit fault at the generator terminals followed by fault clearing by line switching. Simulated daily load curve is also used with test data to observe the tracking effects of parameter changes on simulated operating environment. Simulation of outages which might occur on the system is also tested.

In summary, the following types of simulations have been tested. A comparison of the OPF results before and after the DSA module is applied. This aims to highlight the change in the system parameters with respect to dynamic security enhancement. The parameters that are of interest include the total cost, dynamic security index(CCT of system), system losses, generator outputs etc. Secondly,under the same loading condition, the system is solved for OPF performance when the value of the real power generation of the identified critical machine is varied. This aims to show the change of parameters with respect to power generation changes in a OPF programme. Thirdly, the system loading is changed in steps according to simulated daily load variation and the complete OPF with DSA is applied. This aims to demonstrate the applicability of this methodology and the system parameter changes with load. Other tests that are performed include the case study with pre-selected line and generator outages to investigate the usefulness of the method under a stressed operating environment.

In this chapter the thesis contains a section on the analysis of test results with the observations. In essence, the DSA module works satisfactorily in our test cases based on small to medium size systems. It provides a suitable assessment and prior warning to operator of possible dynamic insecurity in the operating state. This is certainly the case with a system that has high loads and weak generator(s) and is prone to instability. The preventive action found by the methodology helps to alleviate the problem but it also results in relatively higher operating cost. This is in line with the philosophy of a compromise between cost and security of operation. There are clear indications that the dynamic security of the operating state is affected by a large number of factors, including the loading of generators, the loading of lines and their proximty to maximum stability limits, and the load pattern etc. It is not always possible to predict its dynamic security performance in extreme operating conditions. An on-line assessment is thus shown to be a justified need. This observation further supports the proposal of the scheme in this thesis.

In Chapter 7, the overall conclusions of the project and the recommendations for future work are described. In summary, a new method to include on-line dynamic security assessment in optimum dispatch operation of stability limited power system is presented in this thesis. This methodology possesses several innovative features. First, the formulation extends the conventional static security constrained OPF programmes to include the consideration of the dynamic security level of the on- line states. A dynamic security monitor and preventive control module are introduced to form a complete static and dynamic security constrained OPF scheme. The concept of security in power system operation is expanded to include dynamic insecurity prevention that could lead to a complete system collapse. It is believed that the implementation of such a newly formulated complete security control methodology would be useful to the enhancement of power system security. In particular, it is an additional tool to the system control engineer to make real-time decisions. It could be useful in avoiding the system from reaching an insecure state with possible catastrophic contingency to take place and without the prior knowledge of such danger being detected. The formulation proposed in this thesis is thus providing a step forward in arriving at a more realistic secure on-line operation of such power systems. Further refinements are expected to improve the approach to make it more effective in applying to large-scale real systems. One of the suggestions made is to investigate a new method to determine the dynamic equivalent of machines through time series expansion technique.

1.3 Summary of contributions

The contributions of this research project may be quantified and reflected in the following means : (a) The publications of papers.

(b) The contibutions to knowledge.

In (a), a total of five papers arising from the research findings of this project have been published , including two papers in refereed international journals and three papers in proceedings of international conferences. The papers are quoted in Reference section as reference numbers [39], [40], [41], [43] and [37] respectively.

For (b), the project makes several original contributions to a better understanding of the security and optimization problems in power system operation and control which may be summarised in the following three main areas.

Firstly, this project provides a new method to link up dynamic security and optimum dispatch of a power system. The research findings of this project give a better insight to the understanding of the requirements of security and optimization. With the advances in both on-line application of optimum dispatch and dynamic security analysis, further research in this direction would be of great promise towards the ideal of real-time secure optimum power system control.

Secondly, the new idea of including both static and dynamic security together when considering the security of a power system is of value to the knowledge of power system control. Conventionally, power system control centres are designed with real-time computer control to deal with static security only. Dynamic security analysis is not included due to the excessive computations involved. This philosophy of security would need to be changed with the recent new developments in fast dynamic security methods which are likely to make impacts on the real-time dynamic security monitoring and control.

Thirdly, the considerations of critical machines and their control in dynamic security analysis in this research project make contributions towards a better understanding of control of the power system in the dynamic state. For example, the identification of the critical machine and the formulation of a control strategy to improve dynamic security based on critical clearing time are the major new ideas being rigorously studied and reported in this thesis.

Chapter 2

Secure and optimum dispatch - definition, role and implementation

2.1 General

This chapter presents the definition, role and implementation of security assessments and optimum power dispatch in modern power system operations. Security assessments here include both static security and dynamic security and their needs in modern real-time system operation. Optimum power dispatch includes the optimization of the dispatch of both real power and reactive power and their needs in operation. In this context, the role and importance of a modern, computerised power system control centre are introduced first, followed by the implementation aspects of optimum dispatch and security assessments. The main objectives of developing an integrated approach in secure and optimum power system operation are also presented. In particular, the proposed methodology to integrate on-line dynamic security assessment with optimum power dispatch is introduced.

2.2 Role of control centres

In order to understand the role of security and optimum dispatch in power system control, it is essential to review the role of the modern, computerised control centre first. Since the early Seventies, the electric power industry has witnessed a dramatic transformation in system monitoring and control mainly due to the impacts of computer application and the use of telecommunication technologies. New control centres are being equipped with multiprocessor real-time computers scanning and controlling the generation and transmission systems via high-speed supervisory control and data acquisition (SCADA) systems, and interacting with the human operator via dynamic, colour, graphic displays.

Along with this development comes the application of suites of computer software , commonly called Energy Management System (EMS), to achieve an efficient and high quality service to the consumers. In this context, the considerations of security and economy in on-line operation are among the most significant functions to be applied. In the following sections a critical review is given on the development of strategies to achieve the security and economy functions for a large power system.

2.3 Role of economy-security functions in control and operation

In on-line operation of power system, an operationally secure system is by definition one with low probability of blackout or loss of supply. In economic operation the objective is, on the other hand, to find a feasible operating state at the minimum operating cost. To achieve the calculated minimum operating cost condition of operation, independently of security limits, there would be indirect adverse effects on the security level of the system. But the relations between them are extremely complex. With the enormous new developments in the two areas of security and optimization, there is an emerging trend to integrate these two considerations together in the recent literature,[1,2,3] which will be useful to satisfy this need. The new problem formulation is commonly referred to as the secure and optimum dispatch problem in the economy-security functions of Energy Management System (EMS) in power control centre computers. The basic reasons for this proposed amalgamation of security and economy of operation are as follows :

(1) Since security and optimality are normally conflicting requirements of power system control, it is inappropiate to consider them separately and independently of each other. It is logical and desirable thus to integrate them into a unified hierarchical problem formulation[1,2,3] so that a compromised solution can be found.

(2) The recent new developments in power networks' deregulations and transmission access issues are making impact on the operational practices of power utilites. There is an increasing trend to make a fuller use of the transmission capacity of existing networks. To achieve maximum economy, power systems are operated closer to their stability limits with the danger of security violations becoming more imminent. [1,32]

(3) On-line security assessments and optimum dispatch are becoming accepted as standard EMS functions in modern power system control centre designs. Concurrently, static security assessment and dynamic security assessment are on the verge of widespread practical implementation. For dynamic security this is mainly due to the intensive research on fast direct stability analysis [35] It is feasible

and timely now to interface OPF program with security analysis via the proper use of modern techniques.

The security-constrained optimum dispatch of electric power system is an extremely demanding task with complex requirements. The difficulty tends to increase with the growth in power system size and interconnections. In response to the challenges, modern power system control centres are installed with powerful computers with a large suite of application softwares to perform extensive on-line monitoring, assessment, and optimizing functions.

In this context, the economy-security operation is relatively still a young field with immense potential for development. Many of the practical and even conceptual aspects are evolving and to be fully expoited and its terminology has not yet been fully established. Due to this, a new concept of security control is proposed in this thesis to include both dynamic and static security aspects in optimum dispatch operation. A critical review of the developments of security concepts is given in the following sections to clarify the exact terminology and philosophy used.

2.4 Dynamic and static security

In this section, the security concepts as supported by state-of-the-art technology are described to clarify the presentations in the thesis. " Security " in power system operation has been used in a general sense as pertaining to the maintenance of supply to consumers and to avoid the loss of load. In the planning stage, the system's reliability is studied in detail by modelling the impact of probability of failure of equipment on the availability of supply. On the other hand, in the operation stage, an operationally secure system is one with a low probability of blackout or equipment damage. A power system is in an emergency condition of varying severity when operating limits are violated. The most severe violations are those resulted from contingencies. Hence, an important part of the security concept revolves around the power system's ability to withstand the effects of contingencies. A particular system state may be secure only with reference to one or more specific contingency cases, and a given set of quantities monitored for violation.

Overall speaking, security of operation is now generally accepted as a key indicator of the quality of supply. In this context, it is possible to sub-divide security into two main types, i.e. steady-state security (commonly known as static security) and dynamic security. Static security refers to the adequacy of the system capacity to meet the demand on contingency; while dynamic security is measured by the system's ability to*p794Xwithstand disturbance during contingency and maintaining normal operation after the clearing of the disturbance. So there is a difference in terms of time scale between steady-state and transient states in the two types of security considerations. Both the solution techniques and the models are significantly not the same as explained in the following sections.

In the context of studying dynamic security of power systems, the transients are analysed using many levels of modelling details. As the main concern in this thesis is the dynamic security following a credible contingenecy, the time scale of study is mainly up to a few seconds immediately after the contingency's occurrence; nonlinear numerical equations and simplified machine models that could sufficiently describe the dynamic performance of the system are used in the analysis. This is different from the subject of studying long-term transients, with periods of several minutes or more, commonly called " dynamic stability " that would involve the interaction between slow automatic controls and manual control by system operators.[61] Hence dynamic stability studies usually involve small-signal stability analysis methods that typically utilizes eigenvalue and eigenvector methods and are thus completely different from the large-signal, nonlinear analysis methods using simplified modelling techniques in this thesis.

2.4.1 Operating states

In the consideration of security in power system operation, it is postulated to define the operating states of the system according to some observations. The security concept gradually evolved to become a key indicator of power system quality. Many papers were published during the period from Sixties to Seventies, among which T. E. Dy Liacco, an eminent pioneer in power system security operation concept, published in IEEE Proceedings 1974 an important paper [2] on this issue. Power system security is defined as the ability of a power system in normal operation to undergo a " disturbance " without getting into an emergency condition. This is based on the consideration of static snapshots of the power system at a certain time instant. This definition of security actually includes both static and dynamic security ; but as pointed out in the paper, the speed of dynamic security analysis was at that time not fast enough to cope with the on-line requirement. So the main emphasis then was on achieving static security control.

Depending on its condition, a power system is classified as operating in three different states - normal, emergency and restorative states respectively. Fink and Carlsen [16] extended further this concept and proposed the state transition diagram shown in Figure 2-1. The diagram shows the possible transitions between states with a more clear definition of the condition of the system using the load demands as the equalities (E) and the operating limits as inequalities (I). It also shows the preventive control actions that are required to restore from alert state to normal state.

A classification of security levels is useful to define the objectives of security control and a diagram Figure 2-2 adapted from Stott's paper published in IEEE Proceedings 1987 [1] is used. In this diagram, the arrowed lines represent transitions between security levels 1 to 5 due to contingencies. The diagram is able to characterize the static security level of a system by the presence or otherwise of emergency operating conditions (limit violations) in its actual (pre-contingency) or potential (post-contingency) operating states. Levels 1 (Secure) and Level 2 (Correctively secure) represent normal power system operation, in the sense of being acceptable operational states. Level 1 is of ideal security since the system is able to survive any of the relevant contingencies without relying on any post-contingency corrective action. Level 2 is more economical; however, it depends on corrective functions to remove nonsevere violations within a specified period of time. When the system is in level 3 (Alert) preventive control action is needed to return the system to either level 2 or 1, depending on the operational security objectives. At level 4 (Correctable Emergency) the removal of violations will require corrective rescheduling or remedial action to bring the system to level 3. If the system has reached level 5 (Noncorrectable Emergency), some load will be lost by automatic switching control action or by directives from the control centre. In this context, both static and dynamic security contingencies are possible to be considered to assess the security status. A more detailed discussion on security control strategy is contained in the next section.

2.4.2 Strategy for security control

Security control is deemed to be of increasing importance and necessarity in operation due to the following reasons :

(1) There is an increasing trend to load the power transmission systems nearer to its maximum loading limits for higher economy.

(2) Increased tendency to allow more power transfer among interconnected systems.

(3) Longer distance of power transmission lines.

(4) Delay in new installations due to economy and difficulty to obtain right of access for transmission tower installations.

(5) More frequent occurrence of disturbances.

To fulfill the broad objective of keeping the power system secure for as long as possible in context of their increasing needs, it is necessary to design effective security control at the normal operating state. The preventive control needs to determine the actual operating condition of the system, assess system security for the two types of emergency (i.e. static security and dynamic security) and determine the corrective action to be taken in case the system were insecure. This leads to the following three important tasks : security monitoring, security analysis and security-constrained optimization.

Figure 2-3 shows the arrangement in time hierarachy of the security and optimization procedures in on-line power system operation incorporating the modern concepts of both dynamic and static security assessments. In this proposal the use of real-time security assessments of both dynamic security and static security are interacted with the on-line OPF by the following steps.

Security Monitoring: The first step is to obtain real-time measurements of the system states which are filtered and verified by state estimation techniques in order to perform on-line identification and dynamic display of the current operating condition of the system. It also involves the processing of the measured data to determine the system operating conditions and the violations of the operating constraints.

Security Analysis: After the current operating system states have been verified to be within operating limits, the second, much more demanding, function is to determine the security of the system based on a next-contingency set. The contingency analysis is performed on a list of credible contingency cases of either single or multiple equipment outages. In this context, the security analysis should be performed for both steady-state emergency and dynamic instability. The current practice [1,2] is to consider static security only by solving for the changes in the system conditions for a given contingency and checking the post-contingency values against the operating limits.

This approach suffers from the major drawback that dynamic instability may occur during the transition from the pre-contingency state to its post-contingency state. With the introduction of fast direct stability analysis on-line, the dynamic security should also be assessed at this stage, as proposed in Fig. 2-3 to ensure a smooth transition of steady-state security on the occurrence of contingency. This concept is further extended into the preventive control stage in the next sections where a new preventive control strategy for dynamic security is developed.

The general approach used by many utilities in North America [1] is to separate on-line contingency analysis into three stages : contingency definition, selection and evaluation. As shown in Fig. 2-3 the approach is now proposed to include both the static and dynamic security cases. Contingency definition is to define the contingency list to be processed and should include those cases whose probabilities of occurrence are deemed sufficiently high. The second stage of contingency selection is aimed at screening the original long list of contingencies by ranking them in the order of severity for reducing the excessive computational effort. At this stage, approximate models are usually employed [1] to give fast but limited-accuracy results. Finally, contingency evaluation with a.c. power flow programs is then performed on the selected, identified cases in decreasing order of severity until no post-contingency violations are encountered.

Preventive Control and Optimum Dispatch: If the system is found to be insecure in contingency analysis, the next problem is to determine whether the system can be made secure by preventive control action. Dy Liacco [2] suggested to use a security-constrained optimization approach where the best operating condition is found which satifies not only the equality and inequality constraints but also the security limits as additional inequality constraints.

The development of an effective preventive control enhances tremendously the ability of a system to stay secure and therefore minimizes the departures into the abnormal conditions of the emergency and restorative states. Both emergency control and restorative control (Fig. 2-3) are still needed for a complete security control system. Emergency control is to determine the proper corrective action to make the system normal again after it is identified that the system is in the emergency state; while restorative control is mainly to restore service to system load. Although there is a good deal of interest and intensive research performed on emergency and restorative control areas, they are more difficult to implement and are out of scope in this thesis. The present emphasis is on preventive control of security. [1,2]

2.4.3 Optimum Power dispatch with static security constraints

As explained in the last section, security-constrained optimum power dispatch (OPF) is the conventional approach to preventive control of static security in power system optimum operation. The optimization problem is formulated to find the best operating condition which satisfies the load constraints (equality constraints) and the operating constraints as well as the security constraints (inequality constraints).

That is, to minimize $F(x,u)$ (2-1)

subject to

$G(x,u) = 0$ Load constraints (2-2)

$H(x,u) \geq 0$ Operating constraints (2-3)

$S(x,u) \geq 0$ Security constraints (2-4)

where **F** is the operating cost function,

x is vector of dependent variables,

u is vector of control variables,

G, H, S are function vectors.

In OPF the load constraints are the load flow equations and the inequality constraints are the security limits of the state variables. The security function vector **S** consists of the load and operating constraints for each of the next contingencies whose occurrence would cause emergencies. [7,9] The security-constrained optimization process in equations (2-1) to (2-4) would find the best corrective action for making a system secure. For a large power system the optimization problem may be of large scale due to the number of variables involved. The extra cost involved in implementing this corrective action could be determined. Security cost may be presented to the control engineer who can then make decision on whether to carry it out or not.

2.5 Implementation of secure and optimum power dispatch

2.5.1 OPF implementation with security integration

In the implementation stage, the combined strategy of security monitoring, security analysis and security-constrained optimization is a pragmatic approach to on-line preventive control of security in power systems (Fig. 2-3). In this thesis, the security concept is further extended from static security consideration only, to consider also the dynamic security limits in equation (2-4) by a new integrated approach to monitor on-line dynamic security. A schematic flowchart shown in Fig. 2-4 gives the necessary main steps of such an approach and a further extension is shown on Figure 2-5 to elaborate the proposed dynamic security integration steps. The novel features of this proposed approach are as follows :

(1) The Optimum Power Flow with static security constraints is maintained as a computation module to maintain its efficiency and convergency property using a fast OPF program with screened security constraints.

(2) A suitable, fast dynamic security assessment program is applied to determine whether dynamis security of the operating state is satisfactory or not. A suitable security margin for dynamic security is to be determined in this stage.

(3) The preventive control module is applied if dynamic insecurity is found to be present in the previous step. As by-products of such analytical calculation, the relative security improvements and the system operating cost changes are found. By this arrangement, preventive control for dynamic security may be applied integrally or after consulting the other system effects.

(4) The formulation includes both the dynamic and static security limits in determining the optimum dispatch of power system.

However, in order to implement the steps in Fig. 2-4 effectively, there are problems involved, including especially the need to meet the stringent speed requirements and the need to derive an analytical index for defining dynamic security. In the investigations carried out in this thesis, a critical review has been made on the techniques to meet this goal. Further chapters will present the review and the detailed development of the new method of this thesis and its rationale.

2.5.2 Multi-level approach

The strategy of on-line preventive security control through the three stages of security monitoring, security analysis and security-constrained optimization is a typical application of multi-level control. It is a good illustration of the power of decomposition and multi-level organisation of a control system to accomplish a complex control objective. [1,2,40]

In practical implementation considerations, efficiency of the strategy is achieved through simplifying refinements of the algorithm.[1,2,3] First, the optimizing control is formulated as simply as possible in (2-1) using the load constraints and the necessary operating constraints (2-2) and (2-3). In most cases, the optimizing control can be decomposed into :

(1) Active power optimization (P-optimization or economic dispatch),

and, (2) Reactive power optimization (Q-optimization or var dispatch).

From operating experiences reported in the literature [1], there is less cost benefit to run var dispatch as frequently as economic dispatch. Var dispatch could even be treated as an open-loop adaptive control and run at less frequent interval as P-optimization, at say hourly interval. In this context, the P-optimization can be modelled with further simplification in the load constraints (2-2) by using a single equation equating the algebraic sum of power injections and the system losses to zero. In this thesis, the active power OPF or simply called optimum power dispatch is used.

The security monitoring function is designed to work independently of the P-optimization in detecting when certain operating constraints become binding or near-binding, i.e. limits are exceeded or not. When this happens the P-optimization model is modified to include the additional binding or near-binding constraints in the set of operating constraints. Hence, the size of the operating constraint set is adjusted with the number of actual or likely violations. Additionally, the security analysis function can be designed to work either independently or triggered by the security monitoring function. Security analysis then determines the system state's security. If insecurity is found, a security-constrained optimizing program would then be run to find the corrective action for preventive control.

2.5.3 Development of OPF tasks and tracking

In practical implementation of OPF tasks, it is necessary to review the OPF operation via time hierarchy. It is possible to achieve an improved secure and optimal sequence of operation through the exploitation of the OPF informations in a time hierarchy basis. The concept of this development is explained here and then the actual testing of this OPF tasks development and tracking will be presented in later chapters.

The main idea here is to combine three software modules on-line to achieve a more consistent secure optimum operation. They are namely, real-time power dispatch, load forecasting, and advance dispatch modules. (Figure 2-6) The on-line system states , confirmed by the state estimatiom program, will be used to initiate the load forecasting program. The load forecasting program outputs will be used to update the necessary load changes to the advance dispatch program where calculations are made to determine the effective security constraints. The security constraints which are binding or near-binding will be used to build up the reduced model for the security constrained optimum dispatch.

Since in on-line operation the computations are made frequently, the above procedure may be considered as an optimum tracking problem, where the knowledge of the previous solution gives the starting point for the next interval when loads are forecasted to change. In a typical operating condition, the number of actual constraints that may be violated and be included is usually much smaller than the total number of constraints. Hence it is desirable from the point of view of saving of computing effort to identify and store this result as a knowledge base at the advance dispatch stage , say half an hour interval ahead of the real time calculation.

Therefore in this way those lines that have security problems or those buses that have voltage violation problems should be screened out and continually monitored in order to justify their need to be considered as effective constraints in the calculations. This processing could eliminate the unnecessary calculations for those less important security cases and could save substantial computing efforts. A more detailed presentation of tracking test results is contained in chapter 6 on a typical daily load tracking simulation to illustrate the principles involved.

2.6 Conclusions

The increasing complex operational requirements of modern power systems warrant new approaches and new solution approaches to the secure and optimum operation in real-time mode. In this chapter, a hierarchical multi-level approach is presented to accomplish this complex control objective. In its basic three stages of security monitoring, security analysis and security-constrained optimization, the considerations of both static security and dynamic security are shown to be necessary components. A new concept to integrate the dynamic security assessment in optimum power dispatch is thus proposed in this thesis. It is proposed that this new approach is justified to ensure a secure, optimal operation with smooth transition of normal states on the occurrance of credible contingency. The practical considerations have been demonstated to favour the development of a decoupled optimum power dispatch approach with both static and dynamic security limits being integrated in its solution. Hence the development of such an optimum power dispatch method is the most important element of the new security control concept in this thesis. This is in line with the modern need of power system control centre where both the computing power and the economy-security functions are fully exploited as far as possible.

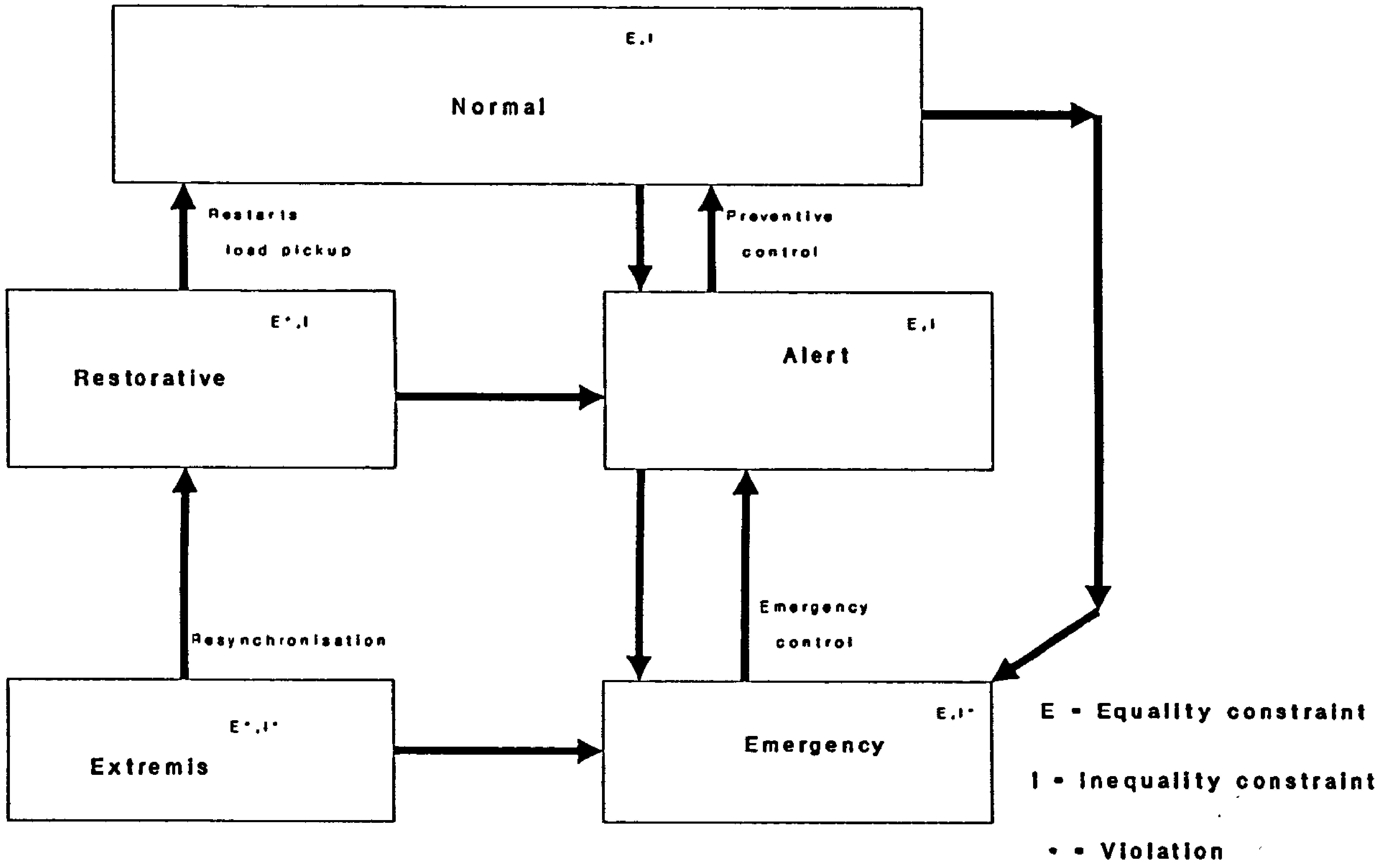


Fig. 2-1 Operation state transition diagram

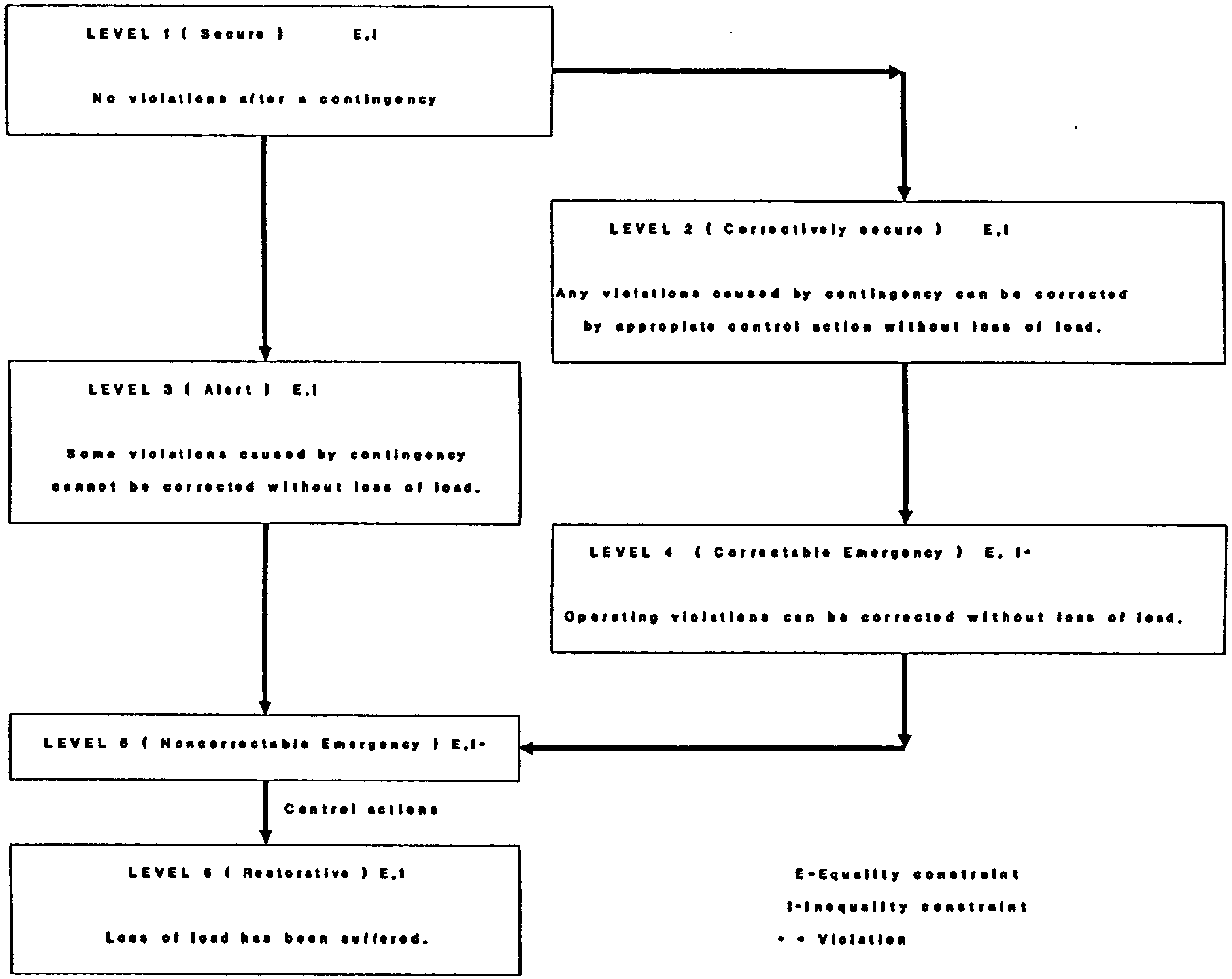


Fig. 2-2 Security levels including corrective action

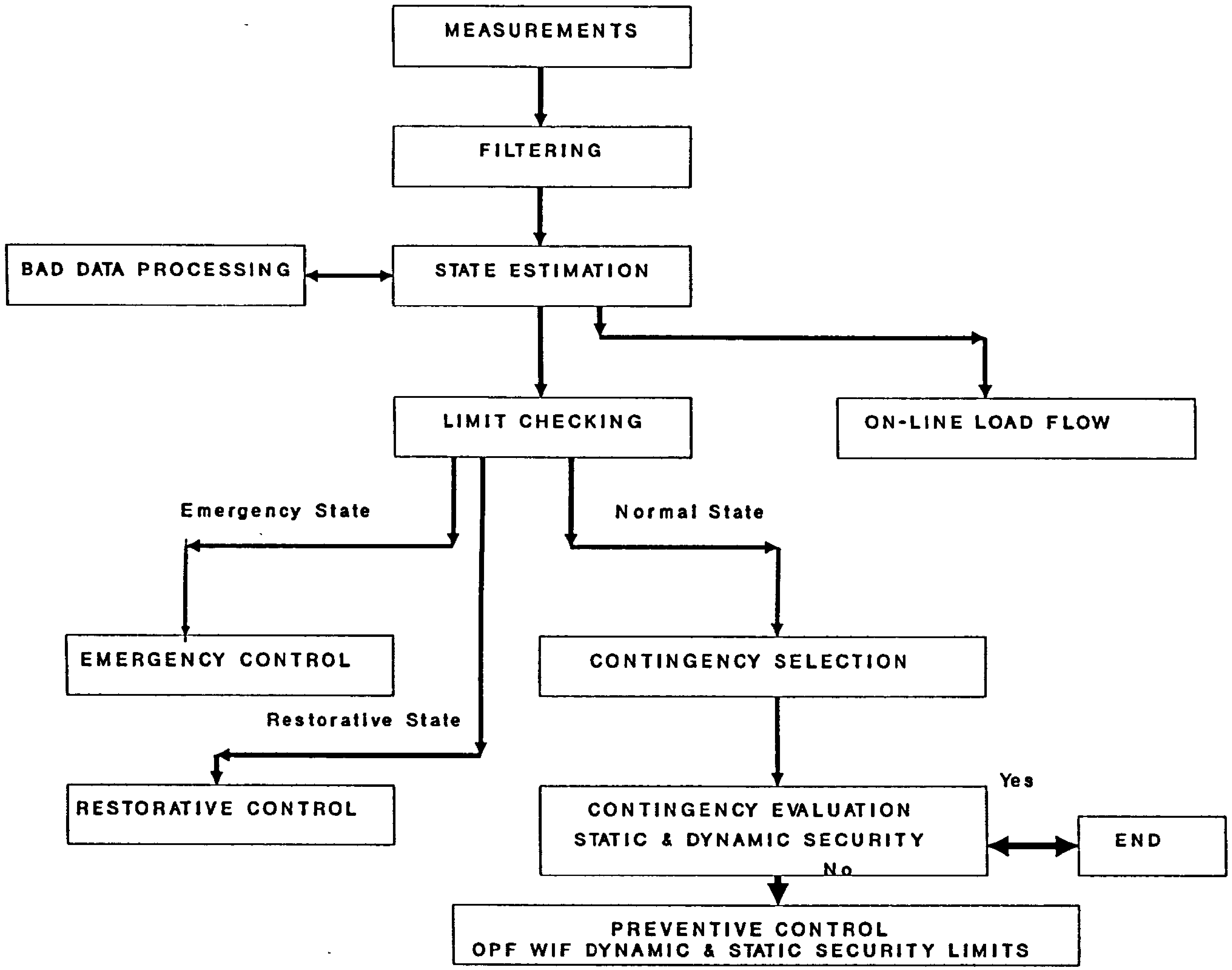
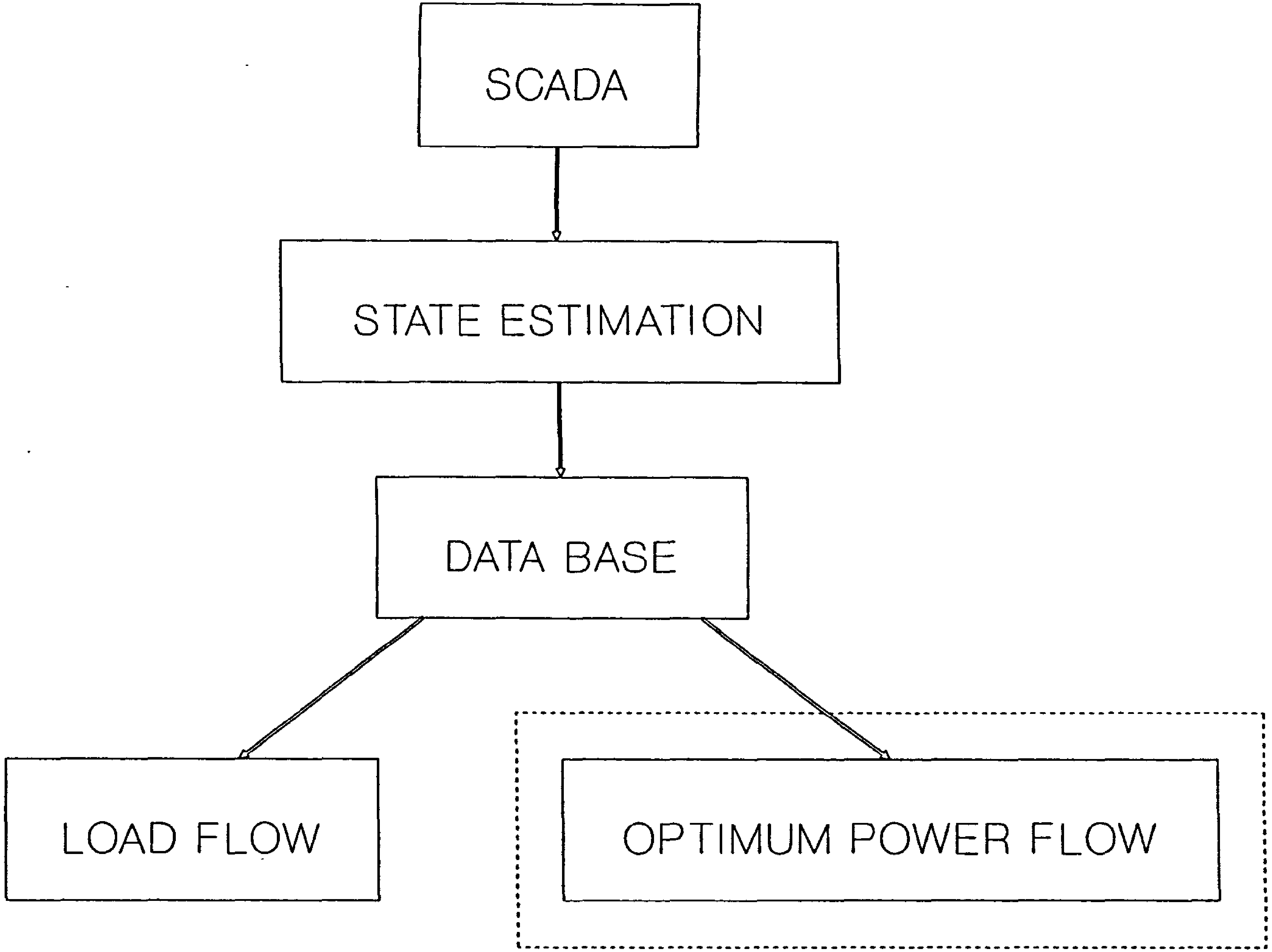


Fig.2-3 Flow diagram of security assessment and OPF on-line



Block to expand in Fig 2-5

Fig 2-4 Block diagram of OPF in operation

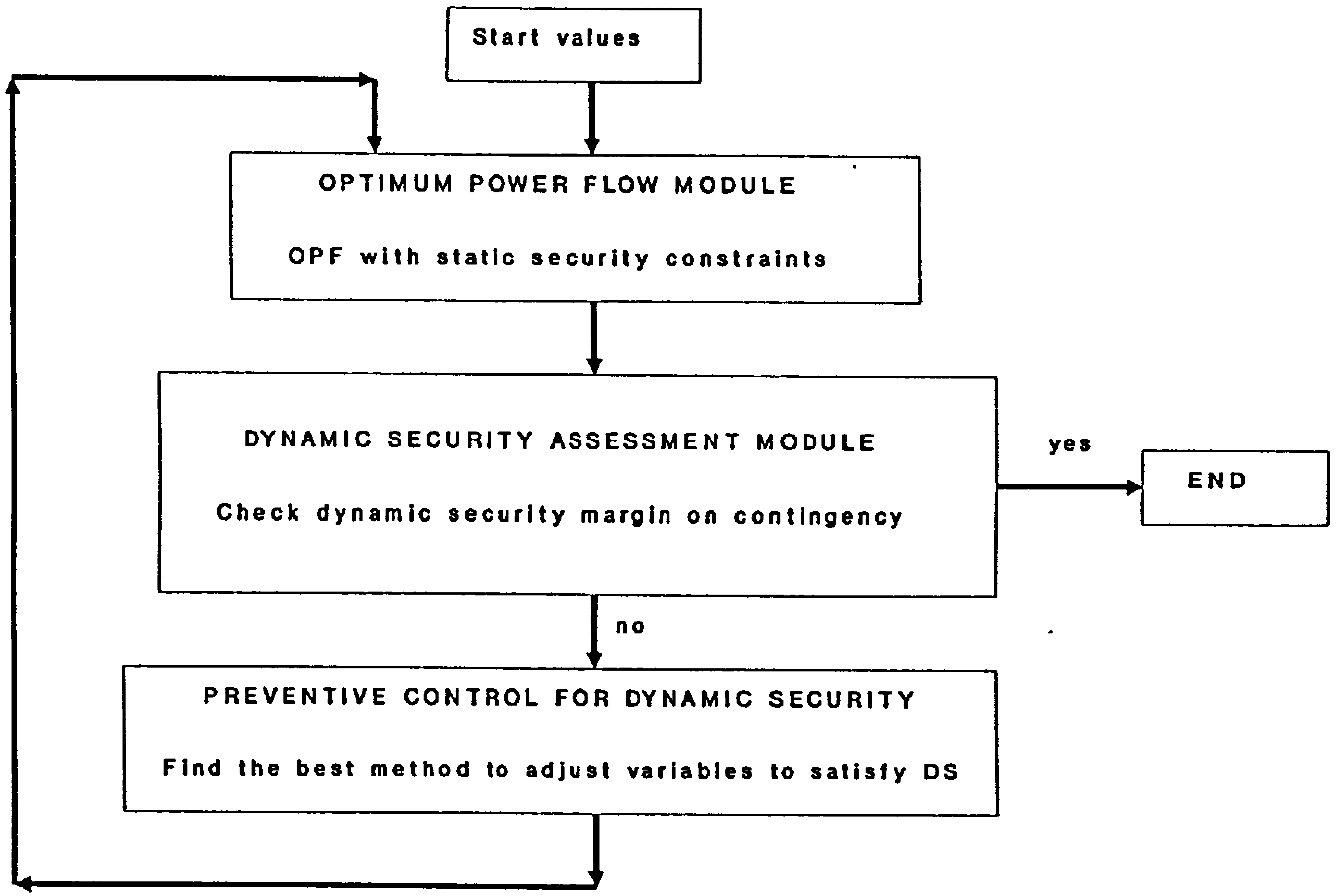


Fig 2-5 OPF integrated with dynamic security assessment

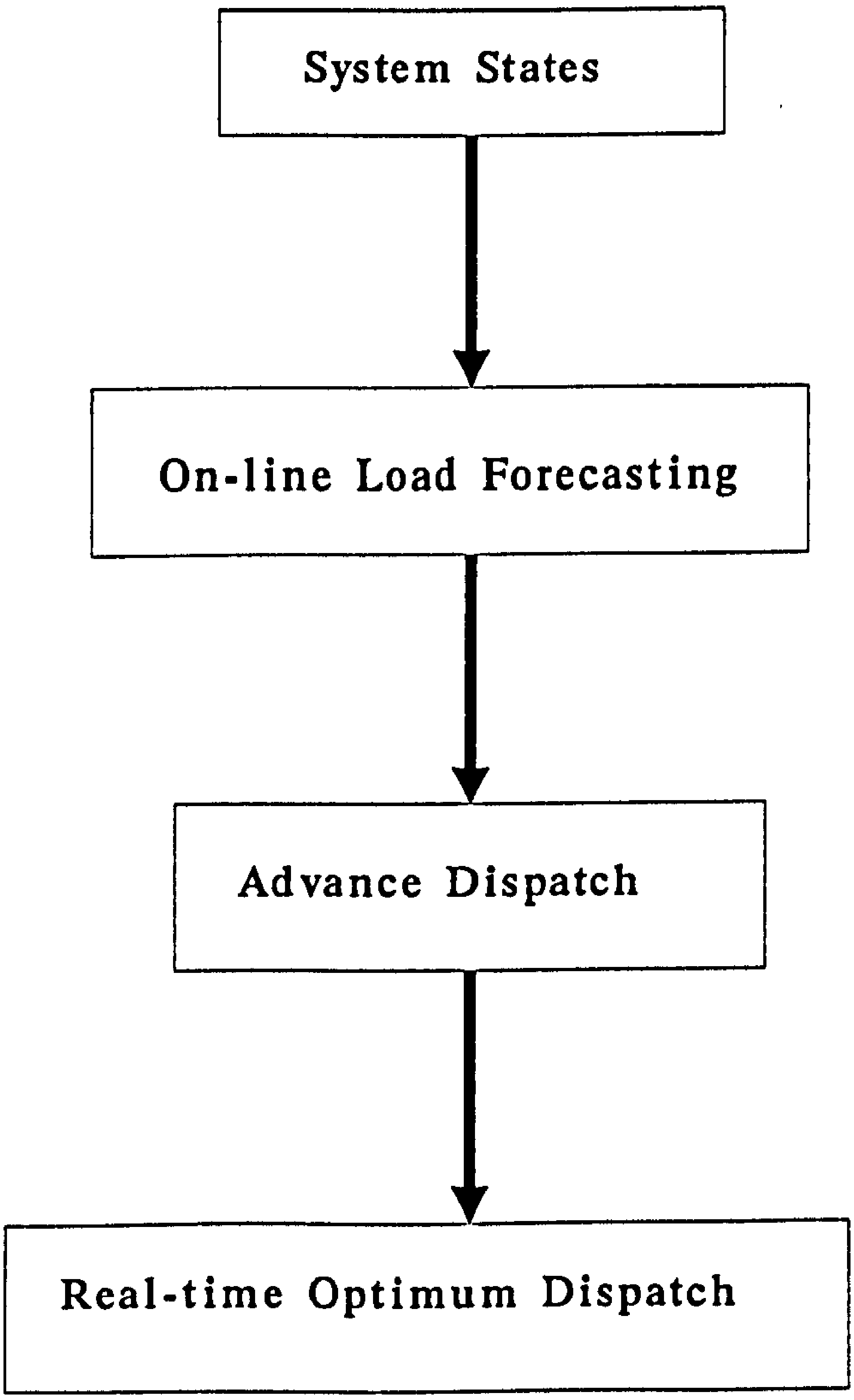


Fig.2-6 Advance dispatch flowchart

Chapter 3

Optimum Power Dispatch

3.1 General

This chapter describes the modelling techniques of optimum power dispatch and the techniques of solution. Firstly, a critical review of the techniques in the current literature being employed to solve the optimum power dispatch problem is given [1,2,3,4,5,6]. This would help to clarify the state of art and the relevance of the new formulation proposed in this thesis. In this context, the rationale for adopting a compact modelling technique combined with the application of Han-Powell algorithm is described.

This is then followed by the review on the static security assessments in on-line power system operation and the modelling methods in various modes of operation are described. The techniques as well as the problems whereby static security assessments are integrated with optimum power dispatch are discussed.

This chapter then presents the testing of a computer program to apply the optimum dispatch operation on typical sample power systems. The techniques used also include the assessment of static security limits by including them as limits of constraints in optimization called static security constrained optimum power flow (SCOPF) program.

3.2 Optimum power dispatch techniques

3.2.1 Review of existing solution methods

Optimum power flow (OPF) solution methods have been developed over a relatively long time due to the basic advantages of minimizing system operating costs. Early attempts were aimed at solving the economic operation problem when power generators were operated in parallel to supply the system load. The first practical successful attempt to solve this problem is by the classical equal incremental cost method.[1,2] This is then improved by the extension into the classical loss formula approach (e.g. B Coefficients method) in order to take transmission losses into account. These early classical methods enjoy the advantages of being simple to implement and relatively fast in computational speed for small power systems. However, in general, they suffer from the following drawbacks :

(1) They do not consider the security constraints in the power system both in the normal state and in the post-contingency state.

(2) The accuracy is limited since the loss coefficients are determined at typical loading conditions and are usually treated as constants. Due to changes in system operation conditions, the above coefficients may be quite different from the values assumed.

(3) Voltages changes in the system are usually not considered.

With the growth of system interconnection and the resulting complexity the disadvantages of these methods make way for the introduction of the modern optimum power flow (OPF) approach. [Ref. 1-8]

Optimum power flow is basically a power flow solution that minimizes the fuel cost or some other quantity, while recognizing the operating limits on power system equipments. Optimization methods, first developed in mathematical programming, gradually find applications in this area. As in mathematical programming, there are many solution methods of optimization and researchers work on suitable application techniques. The first major breakthrough in modern optimum power flow method is usually considered as the important paper published by Dommel and Tinney in IEEE Transactions in 1968 [8,9]. They reported an algorithm based on non-linear programming, where gradient search techniques are applied with the Newton-Raphson load flow to obtain the optimum values of control variables. The general formulation of the OPF problem is expressed in mathematical programming form and may be summarised as follows :

Minimize $f(\mathbf{x},\mathbf{u})$ (3-1)

subject to $\mathbf{g}(\mathbf{x},\mathbf{u}) = 0$ (3-2)

and $\mathbf{h}(\mathbf{x},\mathbf{u}) \geq 0$ (3-3)

where $\mathbf{u}$ is the set of controllable variables in the system,

x is the set of dependent variables,

f is the objective function and is a scalar quantity,

$\mathbf{g}$ are the conventional power flow equations,

$\mathbf{h}$ are the limits on the control variables $\mathbf{u}$ and the operating limits on the system.

The OPF method may be used to determine both the optimum values of the controllable real power outputs of generation plants and the optimum reactive power control variables such as voltage magnitudes and tap-changer positions. In particular, the method can satisfy the security constraints by introducing penalty functions in the optimization process.

The method's enormous potential attracted a large amount of research effort subsequently devoted to both improving its algorithm and exploiting other optimization methods to optimal power flow. To discuss them in more details,it would be desirable to classify the existing solution techniques, reported in the literature, into the following main types : namely, linear programming, nonlinear programming via gradient techniques, quadratic programming techniques. [4,9,10,11,12,13,14]

Linear programming techniques : Linear programming methods have been developed to solve optimization problems that have linear objective functions and linear constraints efficiently. In view of this , the OPF problem is solved via standard linear programming (LP) techniques by introducing linearized approximations of the functions involved. Dual simplex algorithms as typical examples have been reported by Stott, Marinho, and Alsac in IEEE Transactions, 1979 [13] to give a relatively fast solution. However, linearizations can lead to inaccuracies ; this is especially the case in reactive OPF calculations due to the nonlinear nature of the variables involved. In real time calculations when system conditions change smoothly an LP solution may be found to suddenly jump from one vertex to another on the constraint polyhedron. Thus LP may introduce artificial discontinuities that are undesirable in real-time OPF control. In view of the above drawbacks LP techniques ,although attractive for their speed and reliability, possess certain inaccuracies for real-time applications.

Gradient techniques : Gradient method is basically an important type of non-linear programming solution method. The general approach of this class of methods is to compute the gradient vector of the objective function expressed in terms of selected independent variables. A progression direction is thus defined as the opposite of the gradient vector called the steepest descent direction. Progression is carried out along this steepest descent direction until the objective function decreases or a new constraint is met. All the variables are then computed again from the new values of the independent variables and another iteration takes place.

Different modelling techniques have been applied ; typical results were published in Dommel and Tinney's reduced gradient approach [8] using sparse penalty modelling. In applications using the generalised reduced gradient (GRG) method [9], the set of independent variables may change at each step. Both sparse modelling and compact modelling have been applied.

In general, experience shows that gradient techniques with penalty function modelling could give rise to convergence difficulties and computational inefficiencies associated with large systems, so that the methods are not suitable for real-time control use. Applying generalised reduced gradient method to sparse modelling also could create difficulties in changing the set of independent variables; in practice no large scale problem with security constraints is efficiently solved by this approach. In summary, convergency difficulties and the inefficient treatment of security limits by penalty functions are the major drawbacks of this type of methods. The methods are not considered suitable for on-line control use.

Quadratic programming techniques : The basic formulation of this type of technique is to define the gradient of the convex objective function zero at the optimum point.

$$\nabla F(Z) - \nabla F(Z_o) + H^{\circ} \Delta Z = 0 \qquad (3\text{-}4)$$

H being the Hessian of F.

If the exact Hessian is used, the correction ΔZ is called Newton correction, but if an approximate Hessian is used the correction becomes a quasi-Newton correction. The approximation of H may typically be built by recurrence from the gradient at successive points through an updating formula. [4] The accuracy of results using QP is inherently better than LP since the functions used are quadratic which are more nonlinear, while the speed of computation and convergency are comparatively faster than gradient techniques. Especially for active power dispatch optimization, the application of successive quadratic programming with compact modelling has been shown to lead to fast computations.[4,3] They are thus potentially suitable for real-time OPF use.

Active and reactive power decoupling : The complete active-reactive power optimization problem is usually considered more complicated than the decoupled active power optimization problem. Also many authors have advocated that more efficient and reliable active power optimization solution techniques are available than the more nonlinear reactive power optimization. In view of this , active-reactive power decoupling has been exploited in OPF calculations. However, in order to account for the inter-relations of active and reactive power flows, it is suggested to employ a new decoupling method : the active Jacobian $\partial P/\partial \theta$ is computed as usual with constant voltage magnitudes, while the reactive Jacobian $\partial Q/\partial V$ is no longer computed with constant voltage phase angles but with constant active injections and practically constant active power flows. [10] This new process is more efficient and it combines the speed of decoupling and the accuracy of coupled computations. In particular, the reactive OPF is performed without computing voltage phase angles and disturbing the active power balance. It is necessary to start the reactive power optimization after an active power optimization has been accurately determined first since its accuracy depends on the resulting active power flow from such a preset condition. It is possible to use this methodology to obtain a consistent real-time active and reactive power control.

Security levels considerations in OPF : In light of the security considerations discussed in chapter 2, it is proposed here to classify the security requirements in the optimal dispatch operation of power systems into three levels :

(i) feasibility or security in the intact system,

(ii) security under contingency without corrective action, and

(iii) security under contingency with corrective action.

In the first level, it means that no operating limit should be violated in the intact system. This would typicaly include the limits on the control variables (e.g. power output limits of generating units) and the state variables (e.g. busbar voltage magnitude limits). In level (ii), secure operation further demands that no operating limit is violated in the system before or after a contingency; a contingency being an unavoidable event such as the outage of one or several elements (line, unit, or load) or a short circuit leading to transient phenomena. Most researchers tend to concern with flow or current limits in lines after a contingency [2,40] as well as voltage and reactive constraints after the contingency. Level (iii) extends further the security concept to mean that no operating limit is violated in the system before and after a contingency, taking into account a corrective action can take place after the contingency.

As discussed in the last chapter the dynamic security of the on-line operating condition is of concern and should be addressed. A detailed discussion of dynamic security will be presented in the next Chapter and only a brief summary of the current thinking is given here for completeness. The present research developments in dynamic security monitoring and control are far behind static counterparts. Most research regard the transient stability problem as a separate entity from the overall operation. [2,40] There are utilities that reported the problem of transient instability in on-line application of OPF and there is increasing concern on the importance of on-line dynamic security in their operation.[5,32]

In this context, the main proposal here is to incorporate dynamic security assessment in optimal on-line power system operation by means of an efficient fast direct method to find security margin. Conventional multi-machine stability analysis by numerical integration methods to find swing curves (referred to as indirect methods) are not suitable due to the computation speed requirement and the need to find a stability index. Recent research in the development of new tools for on-line dynamic security assessment is focused on the use of direct methods. In this context, the direct method using the concept of Transient Energy Function receives the greatest amount of attention. [19,23,35] With the advent of fast direct method of transient stability assessment the possibility of achieving optimal secure operation that can also satisfy dynamic security limit on-line is now feasible. A more thorough derivation of theory will be presented in the next chapter. Here an introduction of concepts is in order. In this thesis, a new formulation is proposed to assess transient stability on-line during OPF loop calculations. A method for evaluating the transient security margin is used as the monitor in the proposed OPF . If insecure cases are detected a corrective security control method is used to adjust the operation to an acceptable dynamic security condition. The method is designed as an extension to the static security constrained OPF program using decoupled recursive QP approach. After the base case of static security constrained OPF solution has been found, its dynamic transient stability margin is checked. The idea is to use a fast direct transient stability simulation of the on-line system to confirm whether satisfactory dynamic security is met for the possible contingencies. The possible criteria that are usable may include the transient energy function or possibly the critical clearing times (CCT) of the system. For a particular contingency the CCT may be the conventional measure of the system's robustness. In the report, a fast direct method is employed to determine the transient security margin. The procedure should be flexible and reliable within the simplified model's validity limit. The critical clearing time CCT and critical machine, as affected by the contingency simulated, would be found. The on-line information is used to direct the next OPF solution to satisfy dynamic security requirement. This is explained further and demonstrated in the next chapter using practical examples. It would demonstrate that the method is useful for maintaining security and avoiding the system from possible cascading tripouts . A better understanding is also achieved through the approach to arrive at an overall secure optimal operation of power system.

3.2.2 Mathematical modelling of OPF

This section first gives a description of the mathematical formulation of the complete and reduced security-constrained OPF problem, followed by the derivation of the recursive quadratic programming method based on Han-Powell algorithm developed for a decoupled real power optimization approach.[3,4,6,10,39]

In the general OPF statement, OPF techniques are used as general mathematical tools to determine the instantaneous optimal operation of a power system under the constraints which meet operating limits and security requirements. At a certain time instant, the generations, and the active and reactive loads are known. The variables that are at the disposal of control : (1) the active power of thermal or equivalent generating units, (2) the voltage magnitudes of generating units and synchronous compensators, (3) the variable transformer tap ratios, (4) other reactive power sources such as capacitors and reactors, (5) power pool link power flows, and (6) in special conditions, predetermined hydro powers, emergency start and load shedding. These variables will be defined as the control variables **u** of the problem. All the other variables to be added to define the state of the system will be termed the state variables **x**. They typically include the voltage phase angles at each busbar and the voltage magnitudes of load buses.

The state and control variables are linked by the load flow equations to meet the active and reactive loads of the system. These constitute the equality constraints **g**. The inequality constraints are the security limits both in the intact system (or called feasibility limits) and under post-contingency condition (or called "n-1 security"). Security in the intact system includes all the operating limits of the system such as bounds on the control variables, limits on the voltage magnitudes of load buses, limits on the reactive possibilities of generators and limits on line currents. Security limits under contingency imply that no operating limits are violated after a contingency. It includes current limits and voltage magnitude and reactive limits in the post contingency system case. Their limit values are defined and, in most cases, are the same in values as in the intact system. The most commonly defined objective function in OPF is the system total operating cost. Other objective functions such as minimum power losses and deviations from a given solution may be used, but the results of such objectives should be assessed with special care.

The following explains the modelling method used and the basic philosophy of its adoption. The basic problem formulation (sparse modelling)is represented as follows :

$$\text{MINIMIZE} \quad f(u,x) \qquad (3\text{-}5)$$

$$\text{SUBJECT TO} \quad g(u,x) = 0 \qquad (3\text{-}6)$$

$$h(u,x) \leq 0 \qquad (3\text{-}7)$$

$$u_m \leq u \leq u_M \qquad (3\text{-}8)$$

with the following symbols

u is the vector of the control variables,

x is the vector of the state variables,

(3-6) are the load flow equations,

(3-7) are the functional inequality constraints including x, and

(3-8) are the minimum and maximum bounds on the control variables.

Since both (3-6) and (3-7) are very sparse for a large power system, sparse modelling may be exploited with optimization process directly applied to the problem. The optimization problem is represented in terms of the control variables in a technique called compact modelling. This modelling method may take advantage of the efficient load flow solution technique available as follows.

$$\text{MINIMIZE} \quad F(u,x(u)) \qquad (3\text{-}9)$$

$$\text{SUBJECT TO} \quad g(u,x(u)) = 0 \qquad (3\text{-}10)$$

$$h(u,x(u)) \leq 0 \qquad (3\text{-}11)$$

$$u_m \leq u \leq u_M \qquad (3\text{-}12)$$

The modelling method is called compact modellig [9] in contrast to the sparse modelling in the previous classical model. Equations (3-9) to (3-12) are termed the reduced problem. It is also possible to express (3-10) and (3-11) through Taylor's Series development valid for a finite region of a load flow solution. With suitable constraint relaxation, this modelling results in much reduced number of constraints in both (3-10) and (3-11). As an example, for a n-bus system, sparse modelling results in 2n load flow equations and a large number of feasibility constraints and even more contingency-security constraints (typically equal to the number of lines plus load buses). In compact modelling, (3-10) is reduced to one equation of the active-power balance while (3-11) may include screened "binding or near-binding" constraints (i.e. constraints which are either close to or at the limits). The load flow equations (3-6) would be required to be solved in the reduced-model building. The resultant reduced model and the mathematical program to be solved are much reduced in size and would generally give much faster overall solution [9]. In addition, there are also further advantages :

(1) Security constraints are easily handled by a sensitivity approach.

(2) The reduced model provides a solution valid for a large region and is easy to use alone for real-time applications between complete optimizations.

(3) They are also suitable for decoupled real power optimization.

3.2.3 Han-Powell Algorithm [5,6,9,10]

The solution technique applied is the recursive quadratic programming method based on the Han-Powell algorithm with a variable reduction procedure to solve the compact OPF formulation. The **n** equality constraints in the OPF formulation is used to eliminate **n** of the variables. The resultant program will be reduced in dimension by **n**. The basic technique of Han-Powell method is to replace the original large scale nonlinear optimization OPF problem by a sequence of quadratic programming problems (QPP), which have quadratic objective functions and linear constraints. The latter can then be solved efficiently by quadratic programming (QP) algorithms. The main advantages of Han-Powell Method are as follows :

(1) Efficient quadratic programming (QP) algorithms can be applied to solve the nonlinear problem by incremental steps.

(2) The method is claimed to be fast, robust and have reliable convergency property. It has been shown to converge to final solution even when the starting point is in the infeasible region.

(3) The accuracy of using quadratic objective function is superior to linear function as in LP methods. Quadratic cost curves are usually considered to be acceptable to simulate the generators' cost/generation characteristic.

However, its main drawback is the need to calculate the Hessian matrix, **H**. This matrix is non-sparse and of dimension (m by m). In OPF problems m is large and the resultant **H** is too large to be conveniently used in normal QP codes. A variable reduction procedure is thus applied in this method. The formulation is derived as follows.

(OPF) Minimize $f(Z)$ (3-13)

subject to $g(Z) = 0$ (3-14)

$h(Z) \leq 0$ (3-15)

Here, f is an objective function that usually includes fuel costs but may also be selected to represent other functions such as losses and deviations from preset schedule.

Z is the vector of network variables.

g is function vector of dimension n . An element of g represents the total power entering a bus. They are equivalent to the equations of conventional load flow.

h is a function vector of dimension p. It includes equipment ratings, security limits, and post-contingency limits.

Iteration

In each iteration of Han-Powell algorithm, Z_k , an estimate to the solution of (OPF) at that iteration, is improved by taking a step of length "α" (scalar quantity) in a direction of movement S (vector). The improved estimate is obtained from

$$Z_{k+1} = Z_k + \alpha S \qquad (3\text{-}16)$$

The direction of movement S is determined by solving a Quadratic Programming problem whose objective function is a second order approximation of the original objective function and whose constraints are first order approximation of the original constraints. The QP Problem (termed QPP) has the form as follows.

$$(\text{ QPP }) \qquad \text{Min}_S \ \{f(Z_k) + \nabla f(Z_k)\cdot S + ½\, S^T H\, S\} \qquad (3\text{-}17)$$

$$\text{subject to} \quad g(S_k) + \nabla g(Z_k)\cdot S = 0 \qquad (3\text{-}18)$$

$$h(S_k) + \nabla h(Z_k)\cdot S \leq 0 \qquad (3\text{-}19)$$

where $\quad ^T$ denotes the transpose of a vector,

H is the Hessian of the Lagrangian **L** given by

$$L(S_k,\lambda_q,\lambda_q) = f(S_k) + \lambda_{qT}\cdot g(Z_k) + \mu_{qT}\cdot h(Z_k) \qquad (3\text{-}20)$$

,where λ_q, μ_q are the Lagrangian multipliers in solving the QPP.

H is updated from its initial estimate of unity by the information on the gradients of f. [5] The updating process is the identifying characteristic of Variable Metric (Quasi-Newton) Methods. Once (QPP) has been formulated it can be solved by a standard QP code to give S. Han has proved that if λ_q and μ_q are sufficiently large the overall method will converge even when the starting point is infeasible.[5] The method's main strength is speed and robustness. Moreover, it is neither necessary to begin with a feasible point nor to tighten the constraints at each iteration . Even with infeasible starting point the method rapidly converges to an optimum solution. Its main disadvantage stems from the need to calculate Hessian matrix approximation **H**. This matrix is nonsparse and of dimension m x m. In OPF problems, m is often very large. A variable reduction procedure is thus applied to overcome this problem.

Variable Reduction Procedure :

The basic idea of variable reduction is to use the n equality constraints in (OPF) to eliminate n of its variables. The m-vector of network variables , **Z** , is partitioned into two subvectors **X** and **U** so that **X** is of dimension (n) and **U** is of dimension (m-n). Accordingly the direction of movement vector **S** is partitioned into S_x and S_u . Then we eliminate the variables in **X** and find S .

Rewriting equations (3-13) to (3-15) in OPF in terms of **U** and **X** gives :

$$\text{(OPF') :} \quad \text{Minimize} \quad f(\mathbf{U},\mathbf{X}) \qquad (3\text{-}21)$$

$$\text{subject to} \quad \mathbf{g}(\mathbf{U},\mathbf{X}) = \mathbf{0} \qquad (3\text{-}22)$$

$$\mathbf{h}(\mathbf{U},\mathbf{X}) \leq \mathbf{0} \qquad (3\text{-}23)$$

Let $\mathbf{X} = \chi(\mathbf{U})$ be a solution to the equality constraints in equation (3-22) in (OPF') , i.e. $\mathbf{g}(\mathbf{U},\chi(\mathbf{U})) = \mathbf{0}$ (3-24)

By replacing **X** with $\chi(\mathbf{U})$ in (OPF') we get a smaller problem with n fewer variables, namely :

$$\text{(ROPF) :} \quad \text{Minimize} \quad f(\mathbf{U},\chi(\mathbf{U})) \qquad (3\text{-}25)$$

$$\text{subject to} \quad \mathbf{h}(\mathbf{U},\chi(\mathbf{U})) \leq \mathbf{0} \qquad (3\text{-}26)$$

Applying the Han-Powell recursive QP method to this reduced problem we get the QP problem whose solution , **S** , is the reduced direction of movement vector. This QP problem has the form :

$$\text{(RQPP): Minimize}_{\mathbf{S}} \; f(\mathbf{U},\chi(\mathbf{U})) + \nabla_{\mathbf{U}} f \cdot \mathbf{S} + \tfrac{1}{2}\, \mathbf{S}^{T} \mathbf{G}\, \mathbf{S} \qquad (3\text{-}27)$$

$$\text{subject to} \quad \mathbf{h}(\mathbf{U},\chi(\mathbf{U})) + \nabla_{\mathbf{U}} \mathbf{h} \cdot \mathbf{S} \leq \mathbf{0} \qquad (3\text{-}28)$$

,where **G** is a positive definite approximation to the Hessian of the Lagrangian of (ROPF). To assemble (RQPP) it is necessary to find f, **h**, $\nabla_{\mathbf{U}} f$, $\nabla_{\mathbf{U}}\mathbf{h}$ and **G**, all evaluated at $\mathbf{U} = \mathbf{U}_{old}$, the initial estimate for the decision variable vector. **G** is calculated from the gradients $\nabla_{\mathbf{U}} f$ and $\nabla_{\mathbf{U}}\mathbf{h}$. These are in turn obtained from the expressions as follows.

$$\nabla_U f = \frac{\partial f}{\partial U} + \frac{\partial \chi}{\partial U}^T \cdot \frac{\partial f}{\partial \chi} \qquad (3\text{-}29)$$

$$\nabla_U h = \frac{\partial h}{\partial U}^T + \frac{\partial \chi}{\partial U}^T \cdot \frac{\partial h}{\partial \chi}^T \qquad (3\text{-}30)$$

Explicit expressions for all the terms of the above two equations are available

except $(\partial\chi/\partial U)$. In addition we need to know χ in order to evaluate f and **h**. χ and its derivatives can be approximated by the results from Newton load flow calculations. Newton load flow generates the approximation $\chi(U)$ and its derivatives. The procedure proceeds as follows. $\partial\chi/\partial U$ can be expressed by expanding equation (3-24) into a Taylor Series with first order terms only :

$$\frac{\partial g}{\partial \chi} \cdot d\chi + \frac{\partial g}{\partial u} \cdot du = 0 \qquad (3\text{-}31)$$

thus

$$\frac{\partial \chi}{\partial U} = - \left[\frac{\partial g}{\partial \chi}\right]^{-1} \cdot \frac{\partial g}{\partial U} \qquad (3\text{-}32)$$

In order to achieve superlinear convergence the matrix **G** has to include second order derivative information, which is gained by the method used for revising **G**. In the first iteration of the Han-Powell process, the matrix **G** can be set to be the identity matrix. Thereafter, it is updated using the updating formula. The formula requires information on the change in independent variables **U** during the iterations :

$$\delta = \mathbf{U}^* - \mathbf{U} \qquad (3\text{-}33)$$

, where $\mathbf{U}^*$ and $\mathbf{U}$ are the values of independent variables during the current and previous iterations repectively.

The difference of gradients is given by :

$$\gamma = \nabla_U \{f(U^*,\chi(U^*))-\mu_{rq}^{*T}h(U^*,\chi(U^*))\} - \nabla_U\{f(U,\chi(U))-\mu_{rq}^{T}h(U,\chi(U))\} \qquad (3\text{-}34)$$

,where μ_{rq} = the vector of Lagrangian Multipliers which is obtained each time the RQPP is solved. U^*,μ_{rq}^* and U,μ_{rq} are the values of independent variable and Lagrangian Multiplier during the current and previous iterations respectively.

It is possible to choose the step-length α in equation (3-16) so that the scalar product $\delta\cdot\gamma$ is positive when there are no constraints. But when there are constraints, it can happen that $\delta\cdot\gamma$ is negative for all non-zero values of α. In this case, the usual methods for revising **G** would fail to make **G** positive definite. Therefore we replace γ by the vector of the form :

$$\eta = \theta\gamma + (1-\theta)G\delta \quad 0 \le \theta \le 1 \qquad (3\text{-}35)$$

that is closest to γ subject to the condition

$$\delta^T\eta \ge 0.2\,(\delta^T G\,\delta) \qquad (3\text{-}36)$$

Thus θ has the value as follows :

$$\theta = 1 \qquad , \delta^T\gamma \ge 0.2(\delta^T G\delta) \qquad (3\text{-}37)$$

The updating formula is given by :

$$\theta = \frac{0.8\ \delta^{T}G\delta}{\delta^{T}G\delta - \delta^{T}\nu}\ , \qquad \delta\nu < 0.2\delta^{T}G\delta$$

$$G_{new} = G - \frac{G\delta\delta^{T}G}{\delta^{T}G\delta} + \frac{\eta\eta^{T}}{\delta^{T}\eta} \qquad (3\text{-}39)$$

,where G is the previous value in the above expression.

Termination condition : The procedure is iteratively solved as a sequence of RQPP until the convergence condition is reached. The termination condition of the reduced Han-Powell algorithm is that the step size, α , is less than a preselected tolerance ϵ and the estimate of variables are satisfying the inequality constraints in equation (3-23).

3.3 Static security assessments modelling

Since security anlysis aims to determine the ability of the system to withstand the impact of certain postulated contingencies, the considerations of the static security should be studied for the post-contingency states. In this context, we are only dealing with the steady state aspect of security. The conventional approach for static security analysis involves the following three main steps :

(i) To specify the list of most probable disturbances (contingencies) to be included in the analysis. This list may be pre-selected (for example, assigned by the control engineer) or it may be screened out automatically with the aid of computer software already available in the computer system.

(ii) Repeated load flow calculations are performed for each contingency in the specified list in (i). Either full a.c. load flow or reduced load flow are used in this step.

(iii) The load flow results are compared with the static security limits. If all the security limits are satisfied in the event of each contingency the system is said to be secure.

While recognising the importance of observing security limits, this conventional approach is usually criticised for using up too much computing time of the system control computer. Hence many modern on-line operation research seek methods to reduce the computing effort. Much intensive research [17,18] investigates on the possibility of reducing the contingency list by creating a ranking list of contingencies before a full load flow is performed. The methods are called " contingency selection or ranking" or simply " ranking " methods.

Ranking Methods aim to select the critical contingencies out of the numerous probable contingencies without performing the full load flows. The critical contingencies are ranked in descending order of their severity with respect to the system security limit violations such that the most severe contingency is ranked first on the list. For this purpose the line flow MW limits and the bus voltage magnitude limits are usually employed as the security limits for ranking. The ranking methods which rank the contingencies on the basis of line MW flow limit violations are called MW ranking methods, while those methods which rank on the severity of bus voltage limit violations are called voltage ranking methods. A detailed review of the algorithms used in ranking methods is discussed by Lo and et al in references [17,18] and a summary only is attempted here. In MW ranking, two types of theory are used , namely DC load flow formulation and first iteration of AC load flow. [17] Since the main purpose of ranking is to reduce excessive calculations, various methods may give results of differing degrees of accuracy and speed. Depending on the application and on-line requirement practical applications are chosen to suit the system characteristics.

3.4 Test Results

3.4.1 Optimum power dispatch program testing

The above OPF theories were implemented onto the real power dispatch optimization problem of three typical power systems with case studies, and test results are also compared with the published results of other current methods. The formulation is derived below for compact reduced modelling of the system. Constant loads are assumed at a particular time interval. The hourly fuel comsumptions are to be minimized subject to following engineering constraints :

- the power balance equation,
- upper and lower bounds on the generator units,
- security constraints (maximum line flow limits) on the current flows in lines and transformers .

The limits are considered both for the intact system (called "N" security) and when the system is under contingency (called " N-1" security). The security constraints are linearised by their sensitivities (first- order sensitivity) of current flows with respect to real power, while the slack bus injection is approximated by second-order formulae which require first- and second-order sensitivities. The expressions are thus written as follows:

To minimize

$$\sum f_i \ (P_i) \quad (2\text{-}39)$$

,for i=1 to Ng

subject to :

$$[\frac{\partial P_{N_g}}{\partial P}] \delta P + 0.5 [\delta P]^T [H] \ [\delta P] + [P_{N_g}]^0 - P_N \quad (2\text{-}40)$$

$$[\frac{\partial J_r}{\partial P}]_0^T \ \delta P + [J_r]^0 - J_r{}^M < 0 \quad (2\text{-}41)$$

$$[\frac{\partial J_{rk}}{\partial P}]_0^T \ \delta P + [J_{rk}]^0 - [J_r]^{M^*} < 0 \quad (2\text{-}42)$$

$$P_{im} < P_i < P_{iM} \quad , \ for \ i=1,2,\ldots\ldots, \quad (2\text{-}43)$$

where

Ng	the number of generator units (slack bus is numbered last)
Pi	the real power delivered by unit i
$P_{Ng}{}^{0}$	the initial estimate of the real power in slack bus
$\delta P = P - P^{0}$	the vector of the displacements of the control variables from the initial values
P_{im}, P_{iM}	the lower and upper bounds of P_i respectively
f_i	the function of the hourly fuel consumption for generator i
Jr^{0}	the initial estimate of the current flow in branch r (intact system)
Jrk°	the value taken by Jr after a contingency of line k
Jr^{M}	the upper bound of the current flow in branch r (intact system)
Jr^{M*}	the upper bound of the current flow in branch r in a contingency state
$[\partial PNg/\partial P]^{0}$	the sensitivity vector of the real power injection in slack bus with respect to the control variables P
[H]	the Hessian matrix of the slack bus injection with respect to the control variables in the initial load flow

The sensitivity vectors in constraints are computed at the initial estimate by the available load flow Jacobian matrix. The Hessian matrix values are updated by quasi-Newton method.

Derivation of important terms

The objective function used is the total fuel cost of generation.

$$\text{Let} \quad f = \sum f_i (Pgi)$$

$$= \sum (a_i + b_i P + c_i P^2) \qquad (3\text{-}44)$$

where a_i ,b_i ,c_i are the cost coefficients of the generator i at bus i.

Relating δP_i to δP_{Ng} with Ng as the swing bus (defined previously) by means of an approximate linear sensitivity coefficient:

$$\delta P_{Ng} = (\partial P_{Ng} / \partial P_i) \delta P_i \qquad (3\text{-}45)$$

The coefficients may be found from the load flow Jacobian matrix elements at that iteration. For examples, the expressions $\partial P_{Ng} / \partial P_i$ may be derived from the real power balance equation as follows.

$$P_{Ng} = - \sum P_{gi} + \sum P_{di} + P_L \qquad (3\text{-}46)$$

,where P_{Ng} is generation at swing bus,

P_{gi} is generation at bus i ,for i=1,2,...,(Ng-1)

P_{di} is demand at bus i, for i=1,2,..,Ng

P_L is power loss.

Assuming an approximate linear perturbation concept to the above at a certain load flow solution, it may be derived that

$\partial P_{Ng} / \partial P_i = (\partial P_L / \partial P_i) - 1$, in vector form.

For the P-optimization (real power optimization only) the voltage magnitudes are assumed to remain fixed and the control variables are the voltage angles θi.

$$\partial P / \partial P_i = (\partial P_L / \partial \theta_i) . (\partial \theta_i / \partial P_i)$$

The second term ($\partial \theta_i / \partial P_i$) is available at the load flow solution Jacobian matrix and their values are not usually calculated explicitly but Gaussian elimination is used in the same way as we operate in the Newton load flow solution to find them.

The first term may be derived in terms of the most updated network variables as follows. The active and reactive power loss of a transmission network is given by :

$$P_L + jQ_L = V^T Y^* V \qquad (3\text{-}47)$$

Considering only the real part for an N-bus system,

$$P_L = \sum_i \sum_j V_i V_j Y_{ij} \cos(\theta i - \theta_j - \theta_{ij}) \qquad (3\text{-}48)$$

$$\partial P_L/\partial \theta_i = -2V_i [\sum_{j=2 \text{ to } N} V_j G_{ij} \sin(\theta_i - \theta_j)] \quad , j \neq i \quad (3\text{-}49)$$

Hence the values of $\partial P_{Ng}/\partial P_i$ may be found for i=1 to (Ng-1) from the above derivations that rely on the most recent Newton load flow solution.

The expression of $\partial J_r/\partial P$,the sensitivity coefficient of current limit, may be derived also from the most updated load flow Jacobian as shown below.

Consider a line r with voltages V_i and V_j at the two ends:

$$V_i,\theta_i \;\text{-------------------------->}\; V_j,\theta_j$$

$$G_{ij} + j\, B_{ij}$$

The current flow across the line is

$$J_r = (V_i - V_j) (G_{ij} + j B_{ij}). \qquad (3\text{-}50)$$

The square of current magnitude is used since its value is always positive and is thus independent of the current flow direction.

$$(J_r)^2 = [V_{i2}+V_j^2-2V_iV_j\cos(\theta_i-\theta_j)](G_{ij}^2+B_{ij}^2) \qquad (3\text{-}51)$$

$$\partial(J_r^2)/\partial\theta_i = (G_{ij}^2 + B_{ij}^2)(-2 V_i V_j \sin(\theta_i-\theta_j)) \qquad (3\text{-}52)$$

In P-optimization, only the voltage angles are assumed to change while the voltage magnitudes are assumed to remain fixed.

$$\partial J_r^2 / \partial P_i = [\partial(J_r)^2 / \partial\theta_i].[\partial\theta_i / \partial P_i] \qquad (3\text{-}53)$$

The first term is already expressed in terms of the network variables while the second term is also available in the load flow step as in the last section. So the current limit sensitivity can be calculated.

For the expression of $\partial(J_{r(n-1)})/\partial P$ which expresses the branch current sensitivity on the contingency of a branch outage (in this case the branch with the most severe effect as found in the MW ranking method), the constraint is to assure that its value would not exceed the maximum limit even on contingency. A linear approximation approach may be used to solve this. This is based on assuming that the pre-contingency and post-contingency line flow values are related by a distribution coefficient B as follows.

$$B_r = [J_{r(n-1)} - J_r] / J_0 \qquad (3\text{-}54)$$

, where J_r is pre-contingency current in branch r

$J_{r(n-1)}$ is post-contingency current in branch r

J_0 is original current magnitude in the outage branch

The B_r values may be obtained by a linearised load flow model called D.C. load flow. These values are then stored in the OPF program for use as required in the above expression. In case the power system condition does not change much we may use pre-assigned coefficient values to approximate the effects.

$$J_{r(n-1)} = (J_r) + B_r(J_0) \qquad (3\text{-}55)$$

$$\partial J_{r(n-1)} / \partial P_i = \partial J_i / \partial P_i + B_r (\partial J_0 / \partial P_i) \qquad (3\text{-}56)$$

3.4.2 Optimum power dispatch program tests arrangements

In order to find out the suitability of the method to achieve our final goal of secure and optimum power dispatch, testing of the OPF program is first carried out using the previous section's formulation. Computer programs are developed to test the performance of the proposed algorithm on a range of test power systems of IEEE 5-busbar, 14-busbar, and 30-busbar networks which have typical reported test results for comparison. The programs are written in VAX FORTRAN and implemented in the VAXCLUSTER Computer in Hong Kong Polytechnic. The system datas of the 5-bus, 14-bus, and 30-bus systems are contained in the Appendix. They are listed out as follows :

(i) System A - 5 bus system with 3 generators and 6 lines.

(ii) System B - 14 bus system with 5 generators and 20 lines.

(iii) System C - 30 bus system with 8 generators and 41 lines.

The system datas including loads, line datas, and generator datas are contained in the Appendix.

Real power OPF tests

The main developed program of optimum power dispatch OPF is a FORTRAN program which can solve a N-bus system with network datas defined according to its input data file format. This enables that different system conditions as well as different modes of operations can be tested. It is also possible to test for different security levels; i.e. power limits, maximum line current limits, and post-contingency limits may be arbitrarily specified.

3.4.3 5-BUS SYSTEM TEST RESULTS (System A)

The System A (5-bus test system) is first tested with the base case loading condition. Different start values of control variables were tested on the program and consistent OPF results were obtained. A typical set of starting and final values are shown below with 3 iterations :

TABLE 3-1 : Starting values of variables for 5-bus real power OPF.

Bus no.	Bus type	P_G (pu)	Q_G (pu)	Voltage (pu)	Angle (rad.)
1	1 (slack)	0.0	0.0	1.10	0.0
2	3 (gen.)	1.2	0.0	1.04	0.0
3	3 (gen.)	1.0	0.0	1.09	0.0
4	2 (load)	--	--	1.0	0.0
5	2 (load)	--	--	1.0	0.0

Table 3-2 OPF results of 5-bus system

Bus no.(i)	Voltage (pu)	θ_i (rad.)	P_G (pu)	Q_G (pu)
1	1.10	0.0	0.607	0.275
2	1.04	-6.25	1.067	0.603
3	1.09	-1.27	1.197	0.410
4	0.948	-11.86	--	--
5	0.956	-11.35	--	--

INITIAL GENERATION COST (before OPF)= 1187.4 units

* FINAL GENERATION COST (after OPF) = 1165.5 units

TOTAL REAL POWER LOSS = 0.071 p. u.

TOTAL P GENERATION = 2.871 p. u.

TOTAL Q GENERATION = 1.288 p. u.

TABLE 3-3 : LINE FLOWS OF 5- BUS SYSTEM AFTER REAL POWER OPF

Line (i-j)	$I_{(i-j)}$, pu	$I_{(n-1)}$, pu
1-3	0.536	---
2-3	0.077	0.081
1-5	0.46	0.568
2-5	0.318	0.425
2-4	0.44	0.548
4-5	0.07	0.186

TABLE 3-4 Variation of variables during iterations of OPF

Iteration no.	Cost (units)	P_{G1} (pu)	P_{G2} (pu)	P_{G3} (pu)
0	1187.4	0.666	1.20	1.0
1	1183.6	0.976	0.973	0.937
2	1166.4	0.504	1.102	1.264
3	1165.5	0.607	1.067	1.197

The variation of system values during iteration from start values to the optimized values are also plotted in Figure 3-1 to show the convergency pattern. It is observed that the objective function (cost) converges to its final value in 3 to 4 iterations. This convergency pattern is observed to be quite consistent with other start values. Other system variables were also observed to be varying within their constraint values during the iterations as shown in the tables. They demonstrate the validity of the algorithm.

TABLE 3-5 : VARIATION OF OTHER STATE VARIABLES DURING ITERATION

Iter. no.	I_{1-5}(pu)	$I_{1-5(n-1)}$ (pu)	Q_{G2} (pu)	V_4 (pu)	V_5 (pu)
0	0.128	0.463	0.556	0.9481	0.9558
1	0.206	0.579	0.629	0.9474	0.9538
2	0.210	0.560	0.595	0.9479	0.9558
3	0.212	0.568	0.603	0.9480	0.9556

DIFFERENT STARTING VALUES :

The starting values are varied from the base case in order to test the algorithm's reliability. Satisfactory results were obtained in all four cases and they are shown below. The state values are quite unchanged.

TABLE 3-6 : FINAL COST VALUES OF DIFFERENT START VALUES.

Case no.	cost (units)	P_{G2} (pu)	P_{G3} (pu)
Base case	1136.7	0.603	1.613
Case 2	1136.6	0.650	1.650
Case 3	1136.9	0.550	1.550
Case 4	1137.4	2.000	0.200

In the different cases studied in the above table, the start values are changed but the final converged cost value remains quite consistent, within less than 0.2 %.

DIFFERENT STATIC SECURITY LEVELS IN OPF :

The OPF base case of system A is tested with different static security requirements. The conventions used are in line with that of the theoy derived in the chapter and are defined as follows :

- Security level 1 is for power limits only in intact system.
- Security level 2 include power and line current limits in intact system.
- Security level 3 are to consider power, current limits in the intact system as well as the post-contingency current limits.

Test results at different security levels with the developed OPF program showed that the cost at optimum operation would increase with the steady state security level requirement. This confirms the concept security Vs economy that is postulated ; i.e.

maintaining security at a cost. Depending on the power utility's policy it may be possible to operate the system at a lower cost if less stringent security may be tolerated - a concept of security cost is observed here which will be important to the further development of this research.

TABLE 3-7 FINAL COST Vs STATIC SECURITY LEVEL IN OPF FOR 5-BUS SYSTEM

Security level	1	2	3
Cost (units)	1136.7	1141.0	1165.5

The above variation of cost with security requirement is also illustrated on a diagram in Figure 3-3.

It is also possible to run the program with different limit ranges for the line currents both in intact state and under contingency. Results were correctly showing that higher operating cost may be resulted if the limit ranges are defined more strictly as observed in the following table 3-8. The limit ranges are changed in steps of 10 % in the calculation.

TABLE 3-8 OPTIMISED COST Vs DIFFERENT LIMITS OF MAXIMUM CURRENT

Case no.	I_{limit} (pu)	$I_{(n-1)\,limit}$ (pu)	Cost (units)
1	1.0	1.0	1140.1
2	0.7	0.9	1150.9
3	0.5	0.75	1165.5

A comparation of the computing time requirement when different security levels are specified are shown in Table 3-9 below. The results show that more computing effort is required for higher security as more checking of the variables are needed during iteration.

TABLE 3-9 COMPUTING TIME FOR DIFFERENT SECURITY LEVEL OPF OF 5-BUS SYSTEM

Security level required	Computing time, (s) with VAX 11 computer
1	7.0
2	7.2
3	7.5

3.4.4 14-Bus System Test Results (System B)

As observed in the system data of the AEP 14-bus test power system listed in the Appendix, the cost coefficients of the generators are taken as quadratic functions as shown. For a typical set of load data (base case), and with the start values shown as follows, convergence is obtained in 4 iterations by the OPF program with satisfactory results.

TABLE 3-10 : START VALUES FOR 14- BUS SYSTEM.

Bus no.	Bus Type	P_G (pu)	Q_G (pu)	Voltage (pu)	Angle (rad.)
1	Slack	0.0	0.0	1.1	0.0
2-10	Load	---	---	1.0	0.0
11	Gen.	2.0	0.0	1.08	0.0
12	Gen.	0.0	0.0	1.04	0.0
13	Gen.	2.0	0.0	1.05	0.0
14	Gen.	0.0	0.0	1.06	0.0

RESULTS AT CONVERGENCY OF REAL POWER OPF :

INITIAL GENERATION COST	=	1837.50	UNITS
FINAL GENERATING COST	=	1169.20	UNITS
TOTAL REAL POWER LOSS	=	0.072	P. U.

TOTAL P GENERATED = 2.662 P. U.

TOTAL Q GENERATED = 0.842 P. U.

A large range of operating conditions are tested on the program to verify its validity for different loadings and different values of static security limit constraints. The results are generally found to be very satisfactory since consistent OPF results are obtained. The following generation limits are used : for bus 1, the maximum power generation is 2 p.u. and the minimum is 0.5 p.u.. For the other two generators, both have maximum generation limit of 1 p.u. and minimum of 0.2 p.u. The cost Vs iteration is shown in Figure 3-11 and the curve is plotted in Figure 3-4 to show the rate of convergency. The results are also shown in tabular form Table 3-12 below. The results agree very well with the published results using other methods of OPF solution. The effect of constraints on the optimised results also agree with the findings in the last section for the 5-bus system (System A) that higher operating cost is found for more stringent static security limits of constraints. A table showing the typical variation of the cost function with iterations is shown as follows.

-TABLE 3-11 : COST Vs ITERATION IN 14 - BUS OPF RESULTS

Iteration no.	0	1	2	3	4
Cost (units)	1837.5	1214.3	1182.0	1176.8	1169.2

TABLE 3-12 Optimized OPF results of 14-bus system (system B)

Bus no.	Voltage (pu)	Angle (degrees)	P_G (pu)	Q_G (pu)
1	1.10	0.0	1.08753	0.21768
2	1.02364	-3.336		
3	1.03352	-1.945		
4	1.05427	-4.796		
5	1.06423	-3.441		
6	1.02489	-2.355		
7	1.03583	-5.857		
8	0.99758	-5.721		
9	1.01117	-6.440		
10	1.00872	-5.712		
11	1.08	-1.995	0.61514	0.16117
12	1.04	-8.002	0.00	0.18864
13	1.05	-0.698	0.95921	0.12877
14	1.06	-5.857	0.00	0.14556

CURRENT CONSTRAINTS AND CONTINGENCY : The maximum line flow limits are set at various values to test the effectiveness. With the typical base loading case, the current limits are set at 0.9 p.u. and all the current values can be found to settle within the set limit; and under contingency they are also satisfactory showing that the static security level is satisfactory.

3.4.5 Tests with 30-bus system (System C)

The 30-bus test system (System C) is adapted from the IEEE 30-bus system and its data are as listed in appendix. This system has been used as an example system for testing in several papers and many test results are reported. There are 8 generator units in the system and their cost coefficients are represented by quadratic functions. The following constraints are used on the control variables.

TABLE 3-13: LIMIT VALUES OF P_G IN 30-BUS SYSTEM

Bus no.	P_G max. (pu)	P_G min. (pu)
1	2.0	0.5
2	0.8	0.2
5	0.5	0.15
8	0.35	0.1
11	0.3	0.1
13	0.4	0.12

LINE CURRENT LIMITS : The line current constraints are tested for several set values ; first with a more conservative value of 1 p.u. for all line flows and then followed by 0.8 and 0.7 pu respectively. The results show satisfactory trends of convergency in all test cases. The following start values are applied.

TABLE 3-14 : START VALUES OF VARIABLES FOR 30-BUS SYSTEM.

Bus no.	Bus type	P_G (pu)	Q_G (pu)	Voltage (pu)	Angle (rad.)
1	1	--	--	1.1	0.0
2	3	0.6	0.0	1.08	0.0
5	3	0.3	0.0	1.03	0.0
8	3	0.2	0.0	1.04	0.0
10	3	0.0	0.0	1.065	0.0
11	3	0.2	0.0	1.08	0.0
12	3	0.0	0.0	1.07	0.0
13	3	0.2	0.0	1.08	0.0
15	3	0.0	0.0	1.06	0.0
17	3	0.0	0.0	1.06	0.0
20	3	0.0	0.0	1.06	0.0
21	3	0.0	0.0	1.06	0.0
23	3	0.0	0.0	1.06	0.0
24	3	0.0	0.0	1.05	0.0
29	3	0.0	0.0	1.05	0.0
OTHERS	2	---	---	1.00	0.0

Note : Type 1 = swing bus, type 2 = P-V bus and type 3 = P-Q bus

INITIAL GENERATION COST = 816.3 UNITS

FINAL GENERATION COST = 807.000 UNITS

TOTAL REAL POWER LOSS = 0.076 P. U.

TOTAL REACTIVE POWER LOSS = 0.3130 P. U.

TOTAL P GENERATION = 2.910 P. U.

TOTAL Q GENERATION = 1.575 P. U.

Table 3-15 System values after OPF of 30 Bus System

Bus no.	Voltage (pu)	Angle (deg.)	P_G (pu)	Q_G (pu)
1	1.10	0.00	1.50657	0.18054
2	1.08	-2.691	0.58343	0.38351
3	1.0646	-4.411		
4	1.05636	-5.299		
5	1.03	-8.609	0.20636	0.14311
6	1.04714	-6.166		
7	1.03170	-7.655		
8	1.04	-6.069	0.29364	0.10591
9	1.06378	-7.963		
10	1.065	-9.738		0.09889
11	1.08	-6.394	0.15123	0.08628
12	1.07	-8.839		0.07380
13	1.08	-7.664	0.16918	0.07888
14	1.06033	-9.789		
15	1.06	-10.065		0.02119
16	1.06152	-9.506		
17	1.06	-9.898		0.02322
18	1.05479	-10.732		
19	1.05476	-10.945		

20	1.06	-10.786		0.07051
21	1.06	-10.361		0.13489
22	1.05975	-10.334		
23	1.06	-10.741		0.07162
24	1.05	-10.828		0.03848
25	1.04538	-10.619		
26	1.02819	-11.016		
27	1.05086	-10.244		
28	1.04396	-6.701		
29	1.05	-11.927		0.06456
30	1.03111	-12.518		

Cost function Vs iteration : In the base case, the cost of generation converges well with the number of iterations in OPF tests performed. The results are in line with the convergency pattern of the Systems A and B; pattern as in 5-bus and 14-bus systems. The cost reduction is large at the first iteration while in the next few iterations the cost function reduction is smooth until it levels off at around the fourth or the fifth iteration consistently. The overall convergency is reliable and satisfactory results are obtained in all the cases tested. Several different start values are also tested with satisfactory results.

TABLE 3-16 : COST VARIATION Vs ITERATION IN 30-BUS OPF.

Iter. no.	0	1	2	3
Cost (units)	816.3	809.45	808.21	807.00

Current and power limits : The OPF results show that all the power generations are within the required maximum power output limits. The line flow current limits are also observed both in the intact system and under single line outage contingency. Other test cases were also performed to further verify its validity. For example, limits of some line currents are lowered to 0.6 pu. Satisfactory results were obtained in all cases tested and they show the reasonable trends of current redistributions required to overcome limits imposed. It also shows higher operating cost is the penalty of optimal operation for stringent current limits - another support for the security cost phenomenon we have observed.

Different start values and load patterns : A series of tests were performed on the 30-bus system with varying loads and different start values to verify the robustness of the algorithm. Specifically, +10% , -10% , +20% and -20% load increases of the base case are applied to the main load buses. The tests all converge within 3 to 4 iterations with an optimum cost at the required security level (level 3 in the results that follows):

TABLE 3-17 : FINAL COST VALUES FOR DIFFERENT LOAD PATTERNS

Load	Base case	+10%	+20%	-10%	-20%
Cost (units)	808.62	816.66	820.05	806.98	801.61
No. of iterations to reach convergency	4	3	3	4	4

Curves may be plotted to show graphically the variation of objective function and P values during iterations of the above computations. Figures 3-11 to 3-12 are plotted for the purpose.

3.5 Conclusions

The optimum power dispatch calculation of power system is reviewed in this chapter and is proposed to be solved by a power system model employing Han-Powell recursive quadratic programming algorithm. This approach is found to be a suitable method for fast, on-line power operation for the following special charactistics :

(1) The compact formulation may be used which contains a single equation

representing the power balance equation in the power system with the reduced model. This represents a substantial reduction of the scale of the original problem.

(2) The Han-Powell algorithm is a fast, robust algorithm with good and reliable convergency property and is demonstrated for the several systems tested.

(3) Security constraints (for static security) are treated efficiently since their sensitivites are considered directly in the model. Screening of 'near binding' constraints may be processed in the program to improve computation time. These may be implemented with a predispatch procedure to set up the reduced model of the system. [43]

(4) The method shows good promise for real-time applications since it contains the characteristics of fast speed , reliability and accuracy which are the necessary requirements of such real-time applications.

From the observations of the tests performed, it is demonstrated that the method developed is of promise and potential for on-line power system operation. However, it is essential , as stipulated in our proposed security requirements, to consider the extra element of dynamic security. This is further discussed in the next chapter where dynamic security assessments are reviewed. This will then lead to the further development of OPF which includes both dynamic security and static security limits as well as the need for security control.

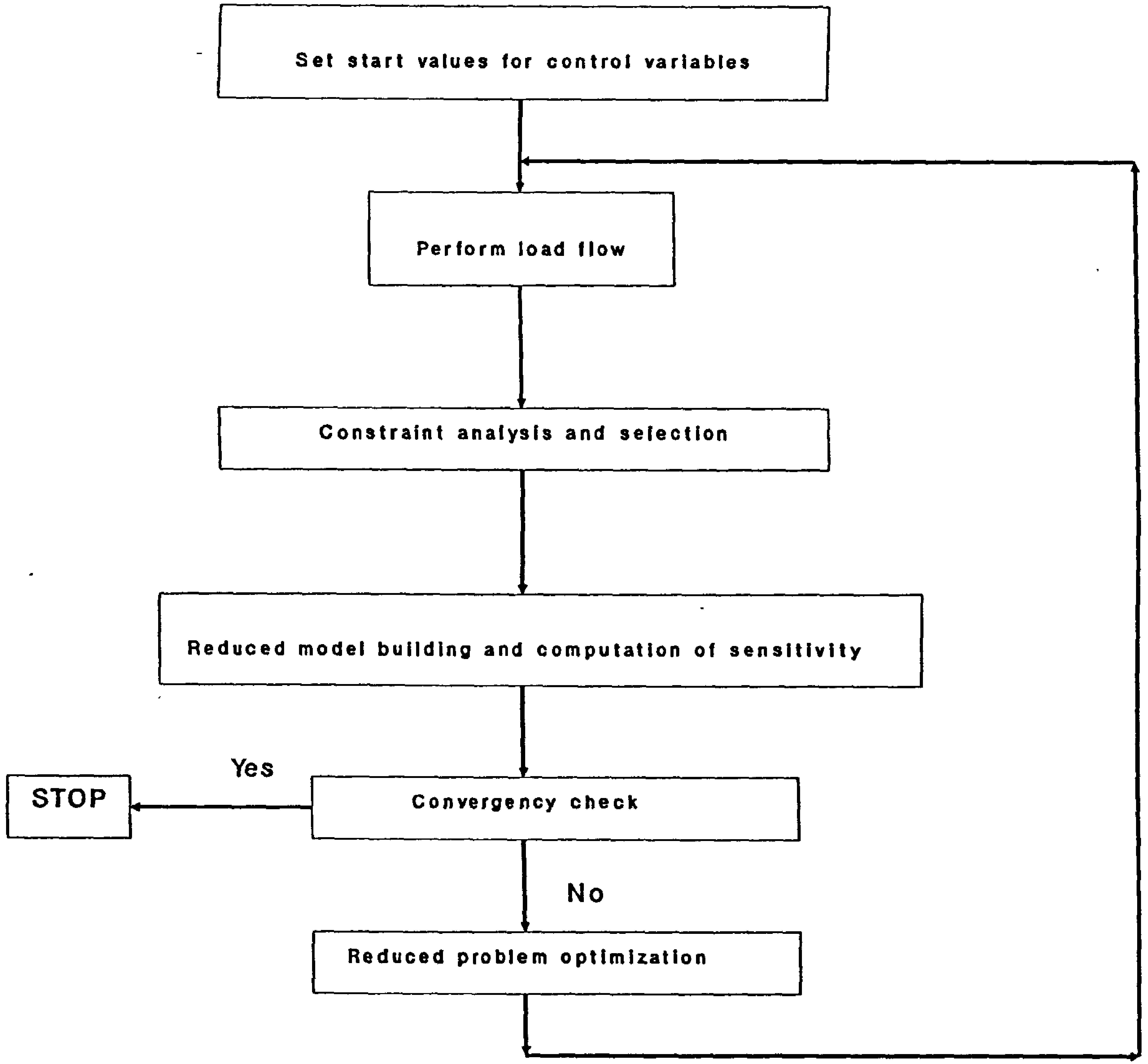


Fig.3-1 Flowchart for compact OPF method

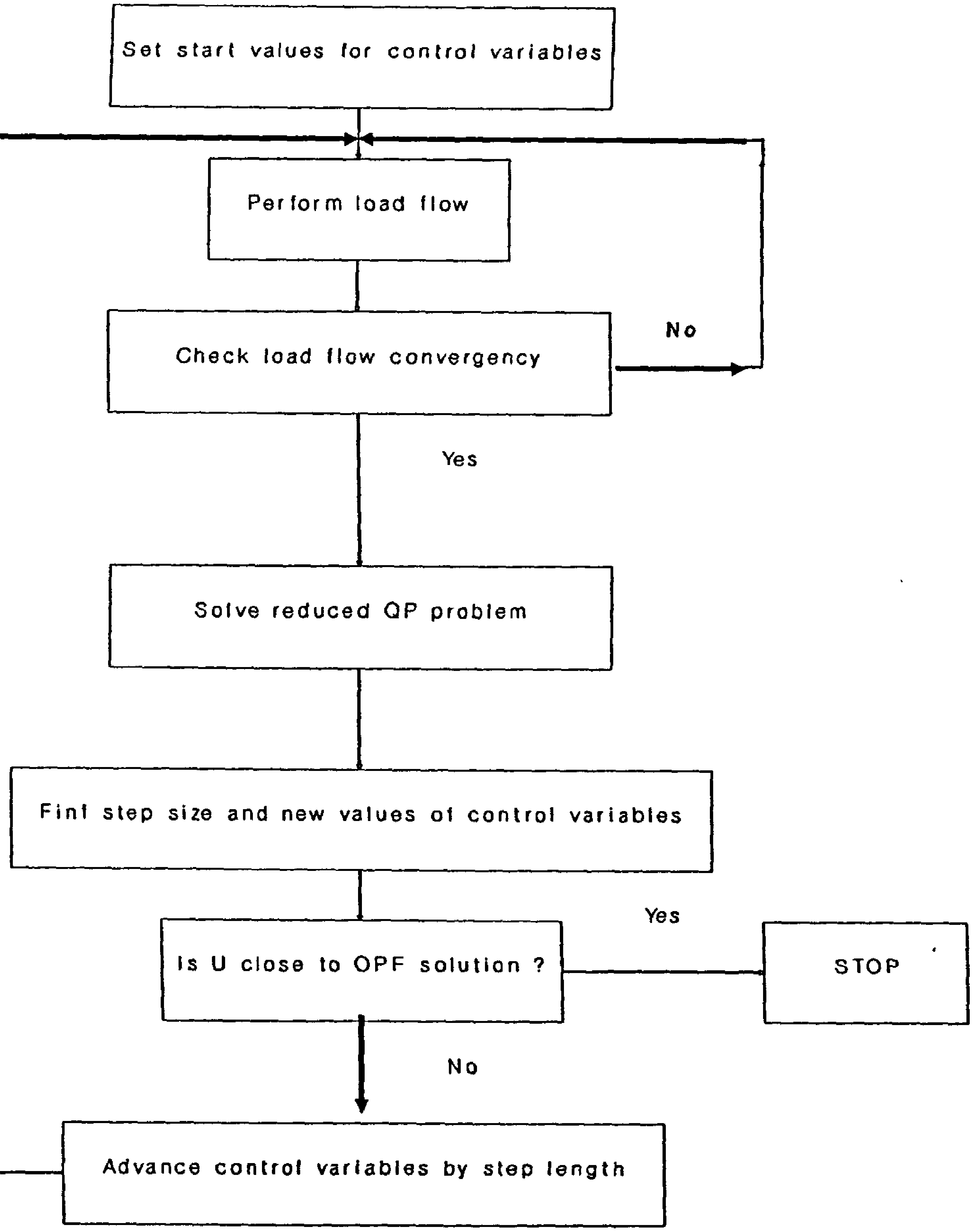


Fig.3-2 Flowchart of Han-Powell method applied to OPF

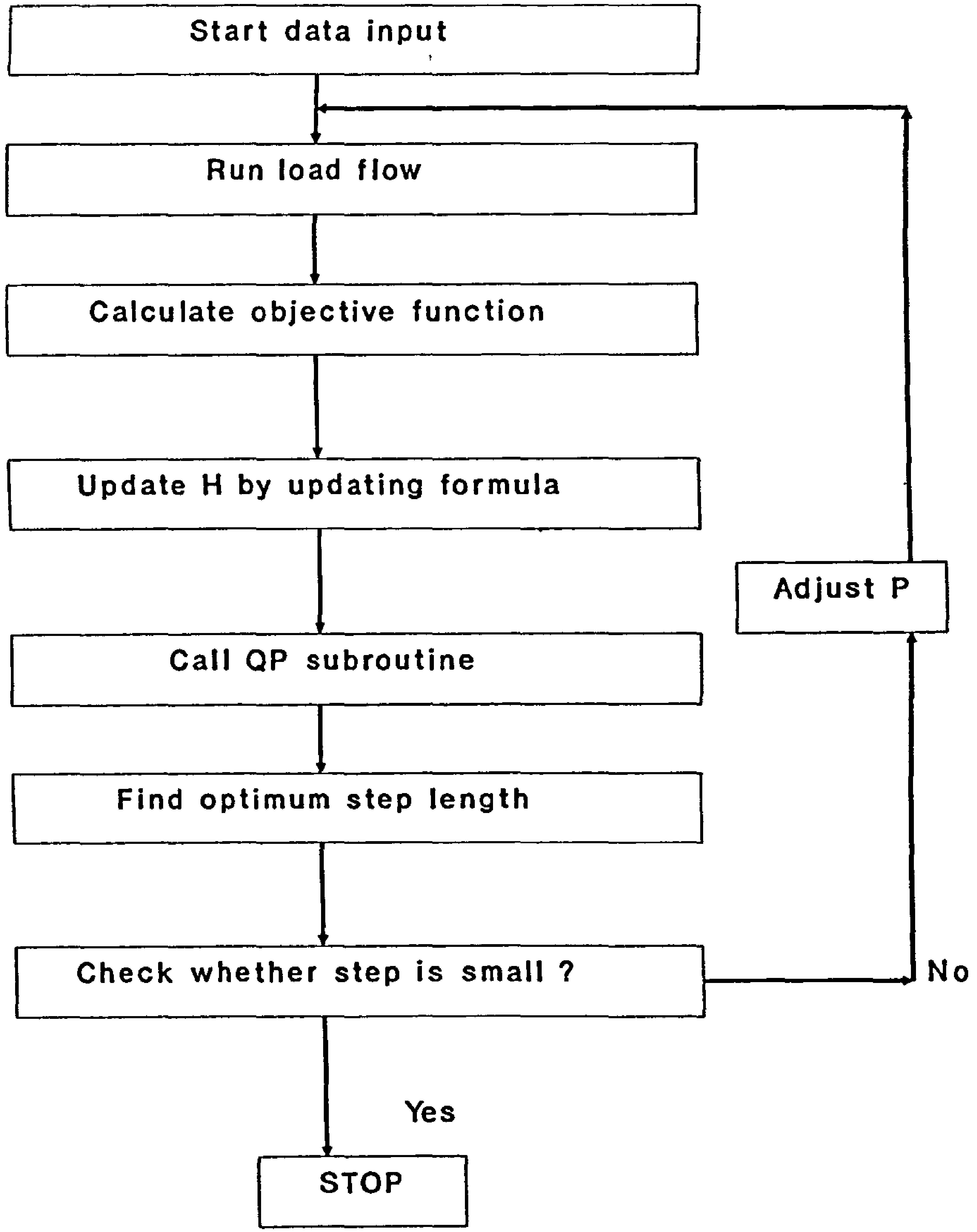


Fig.3-3 Flowchart of OPF program

Fig.3-4 Variation of variables Vs iter.
(5-bus system)

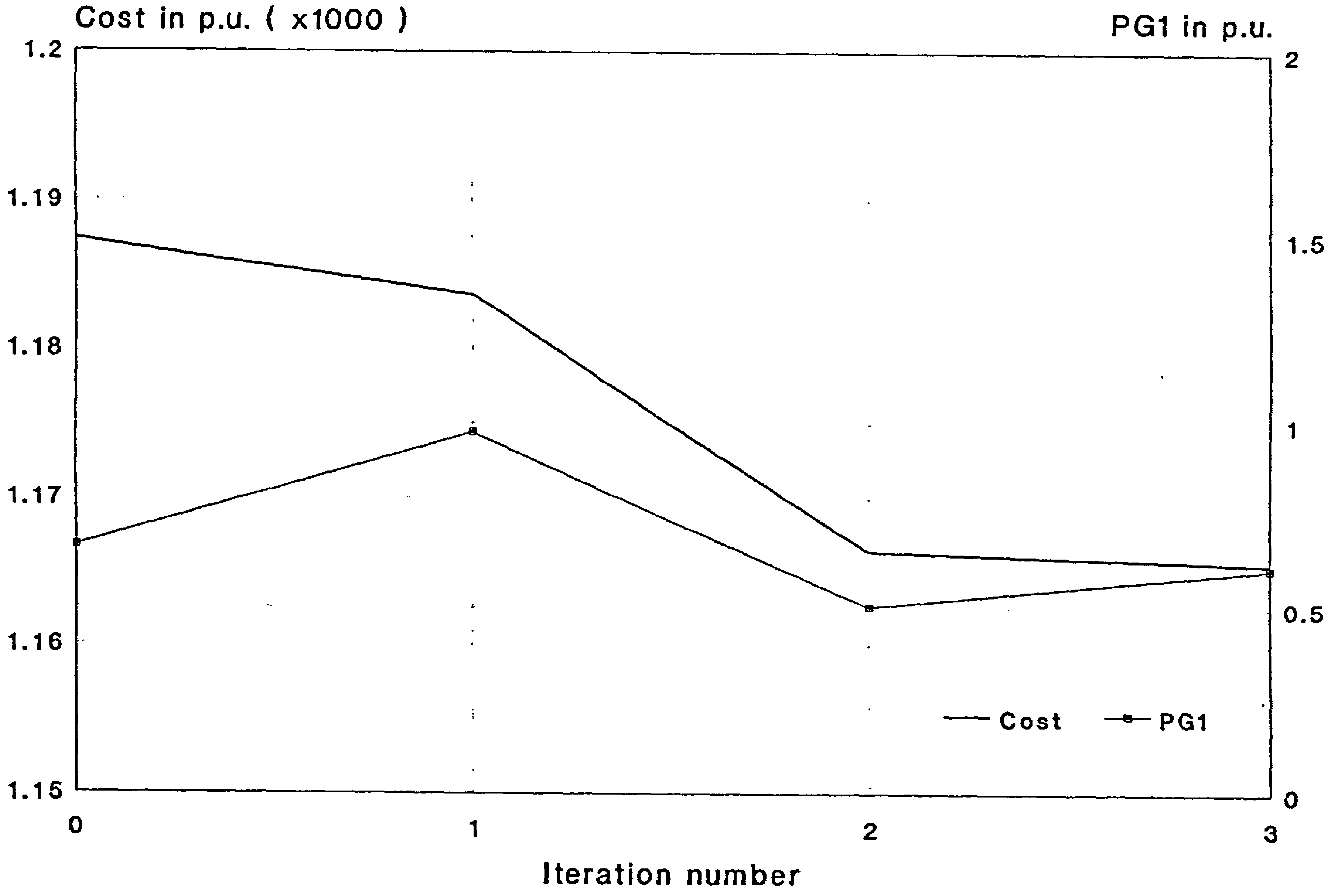


Figure 3-4

Fig.3-5 Variation of variables Vs iter.
(5-bus system)

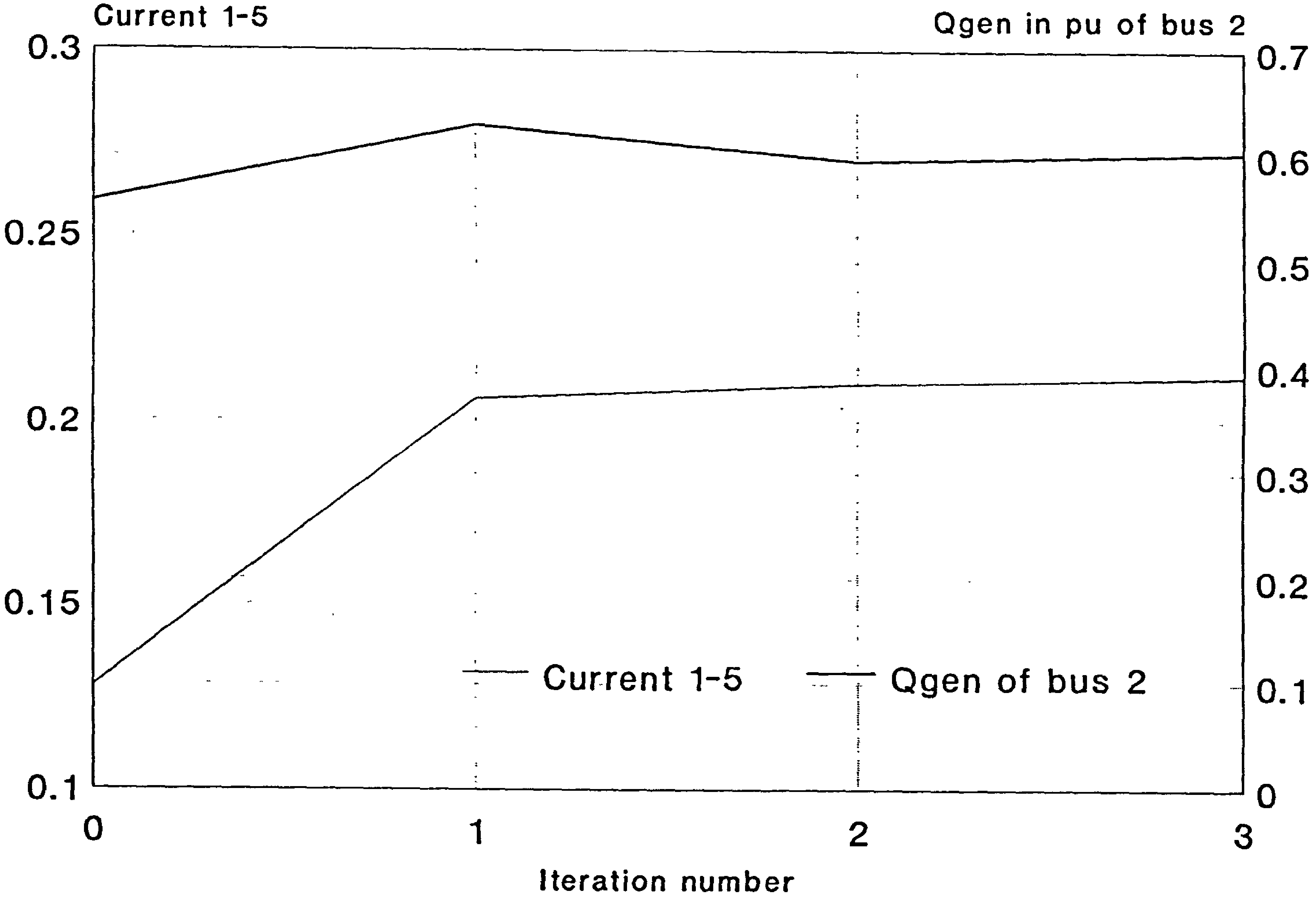


Fig. 3-5

Fig.3-6

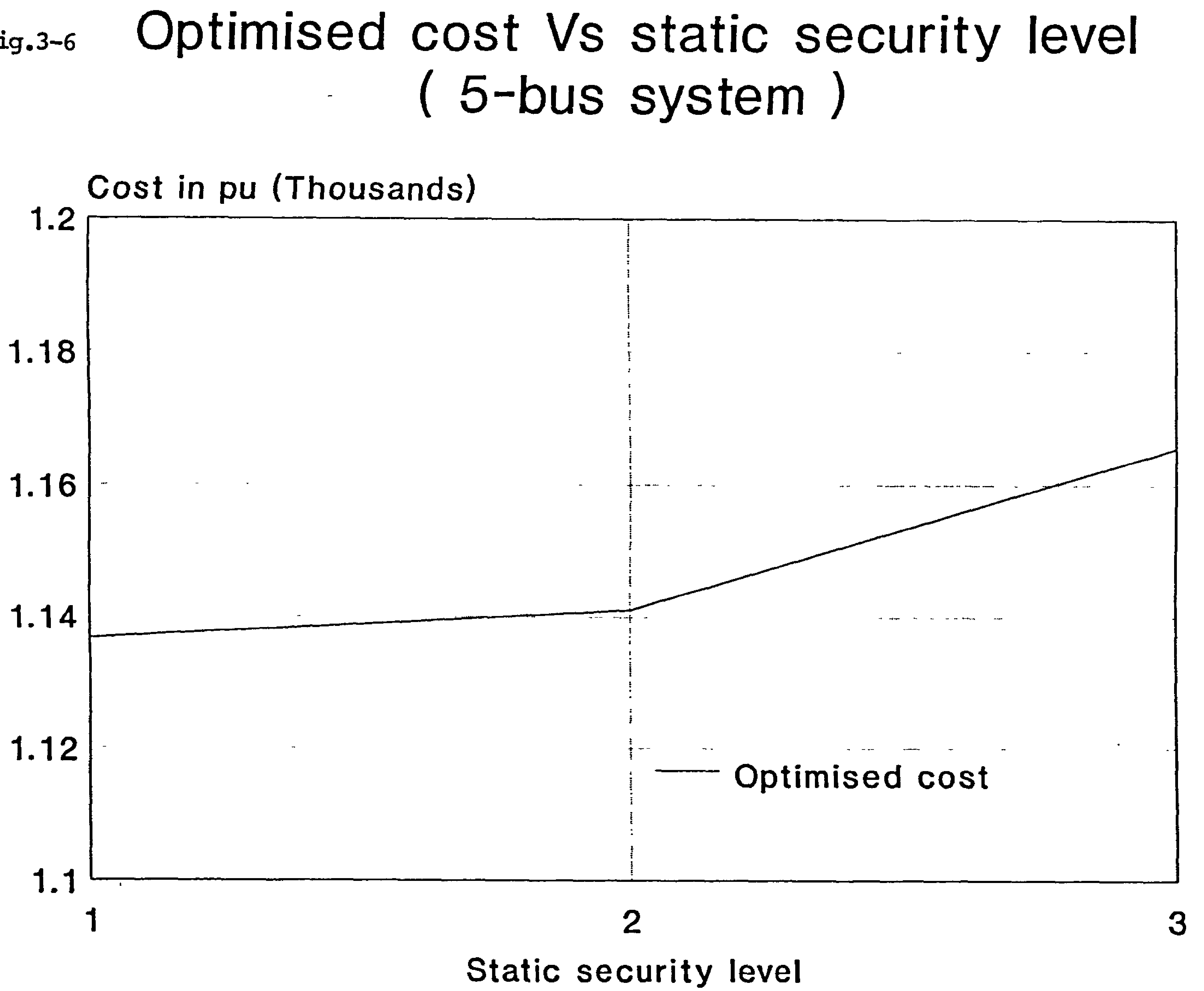


Figure 3-6

Fig.3-7 Cost variation Vs iteration
(14-bus system)

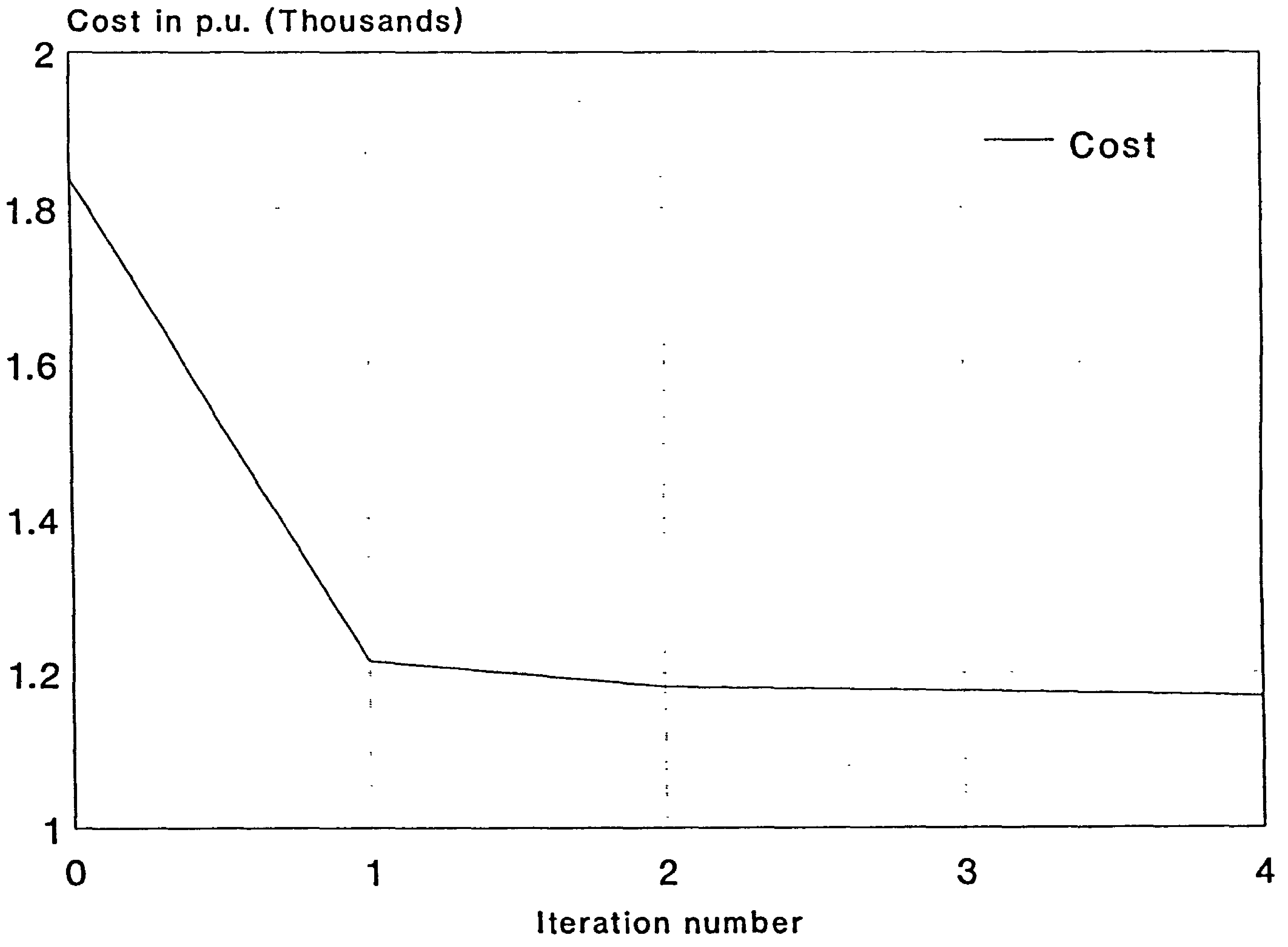
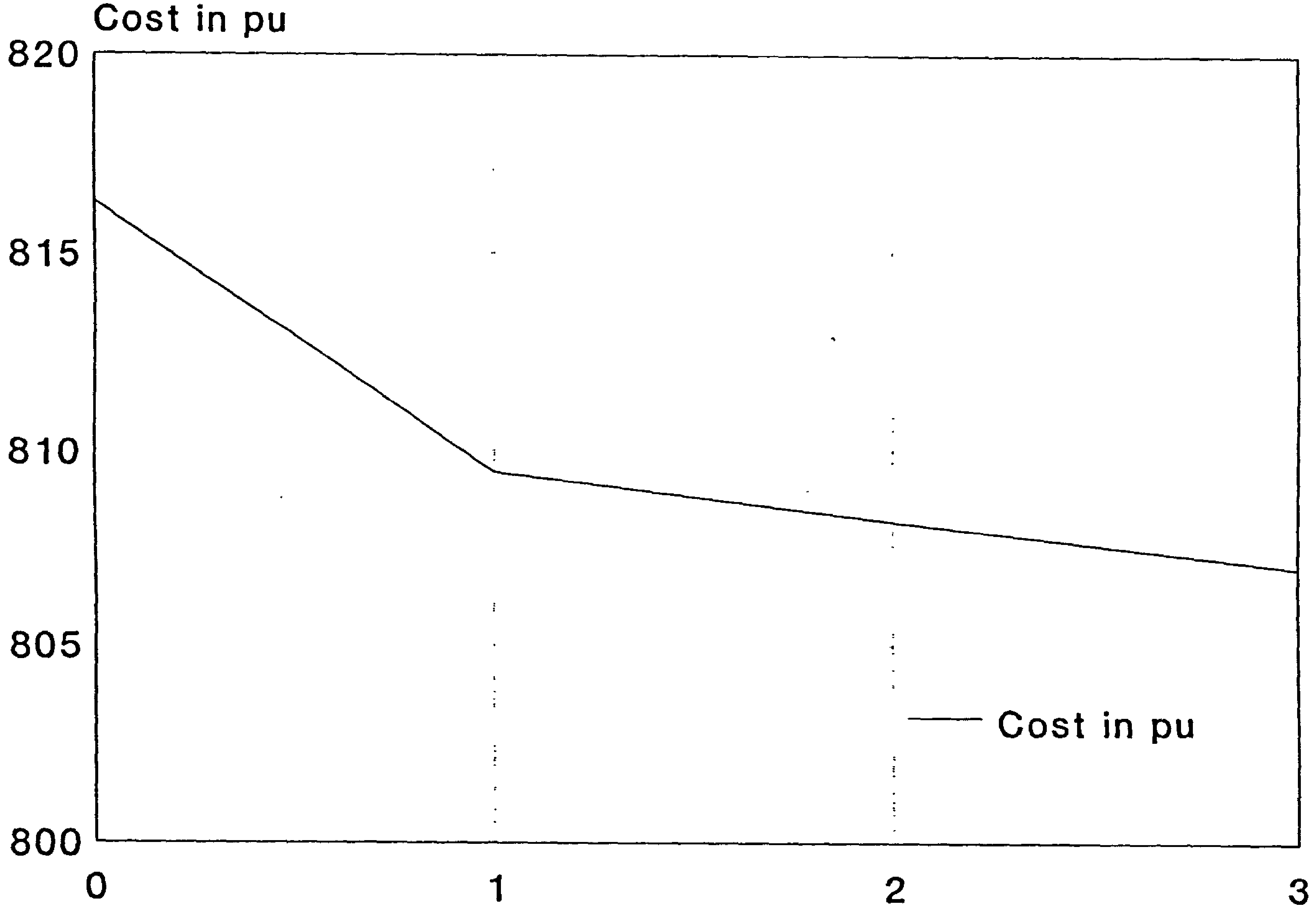


Fig. 3-7

Fig.3-8 Cost variation Vs iteration
(30-bus system)



Iteration number

Fig. 3-8

Fig.3-9 Cost variation Vs iteration
(30-bus system)

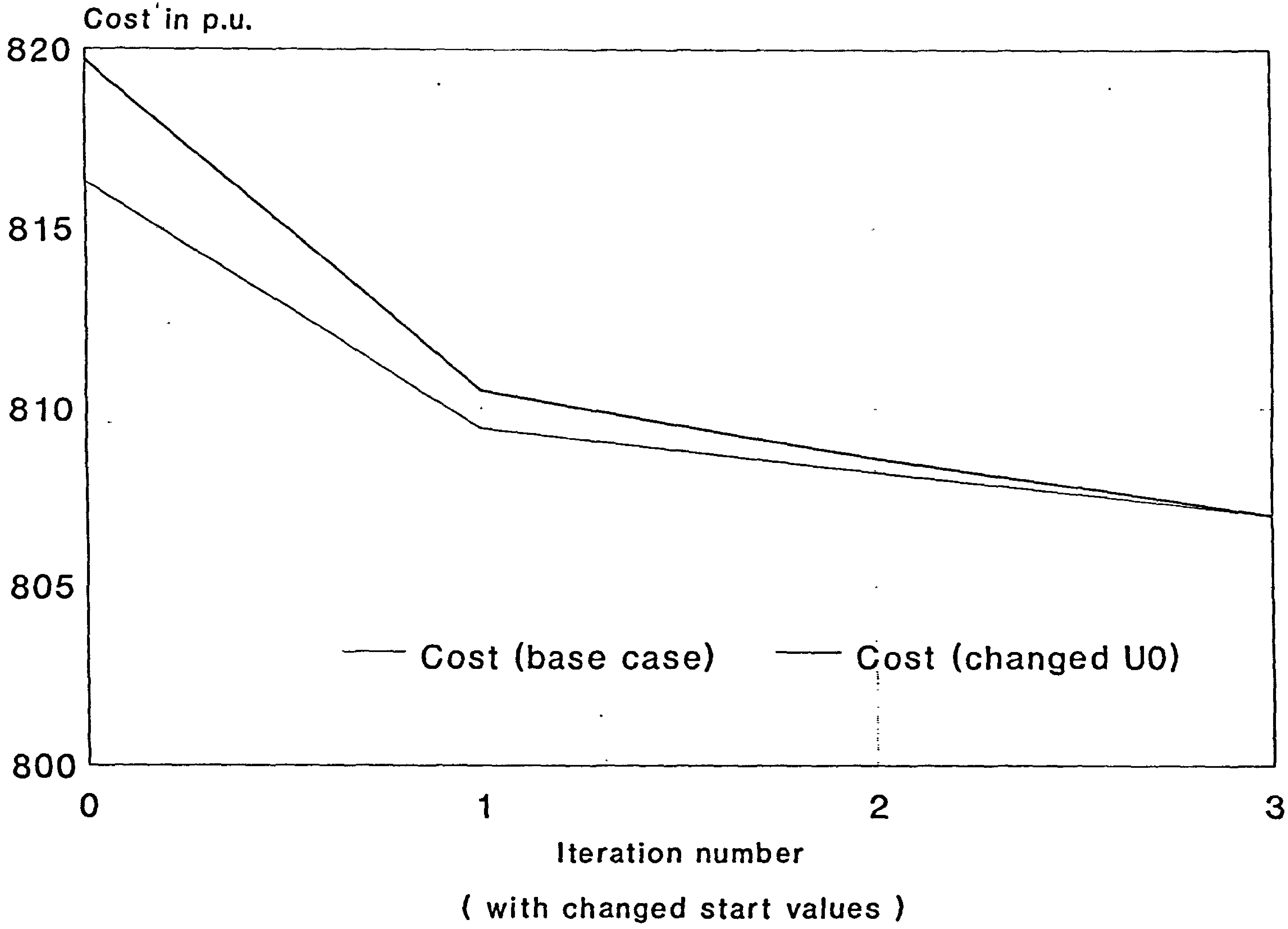


Fig.3-10 Cost Vs system loading level
(30-bus system)

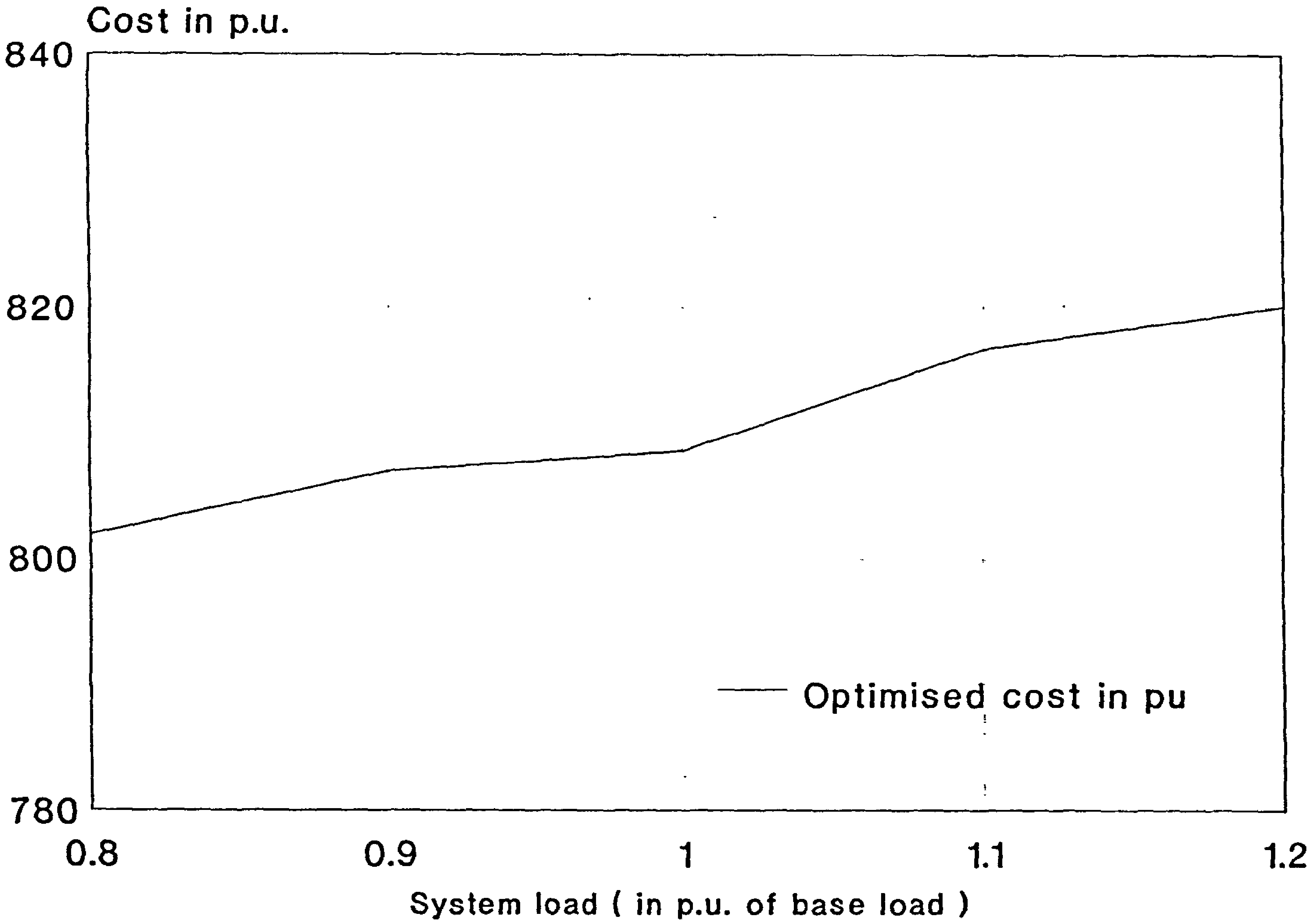


Fig. 3-10

Fig.3-11 Pg values comparison
(30 bus system)

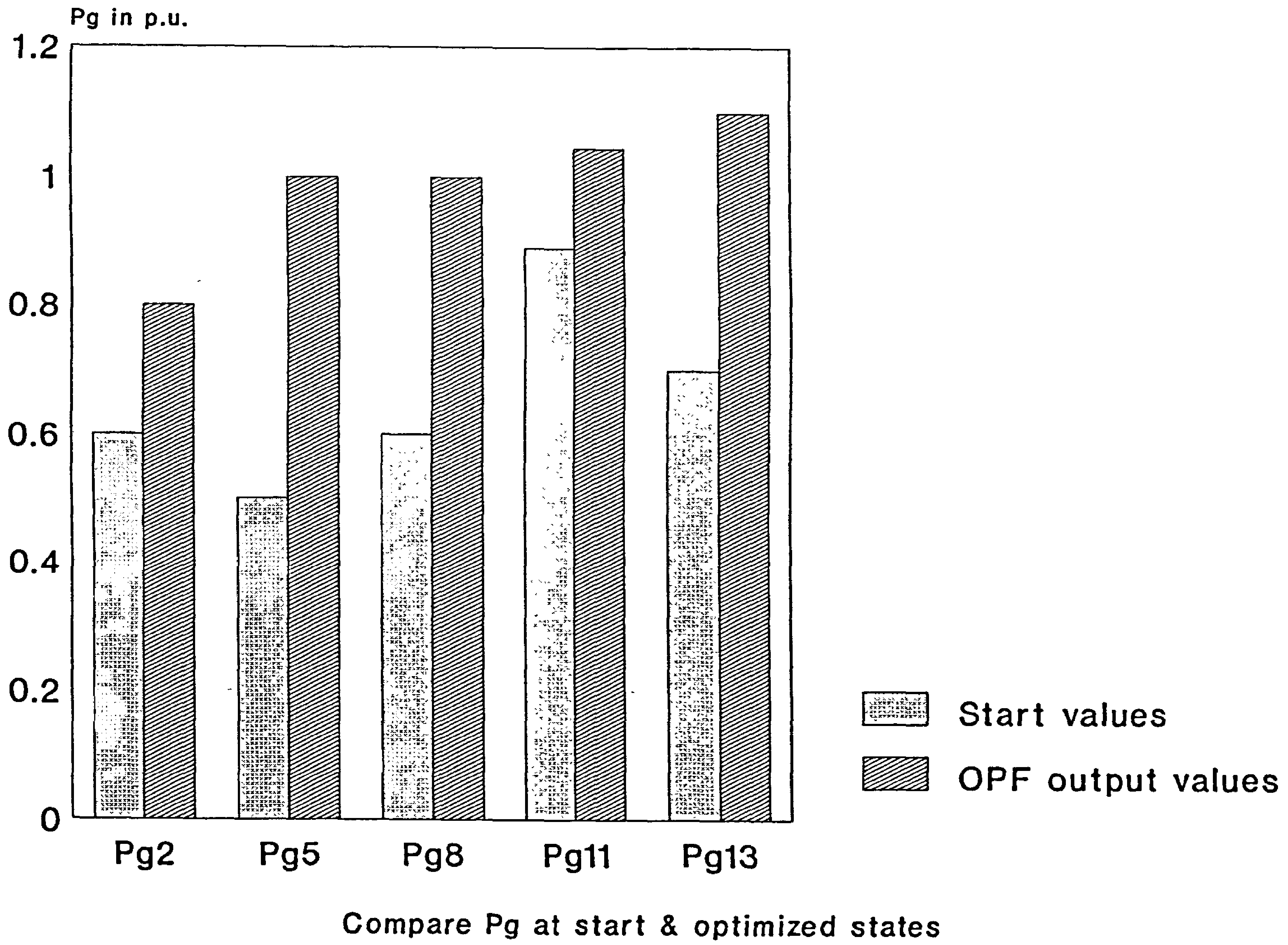
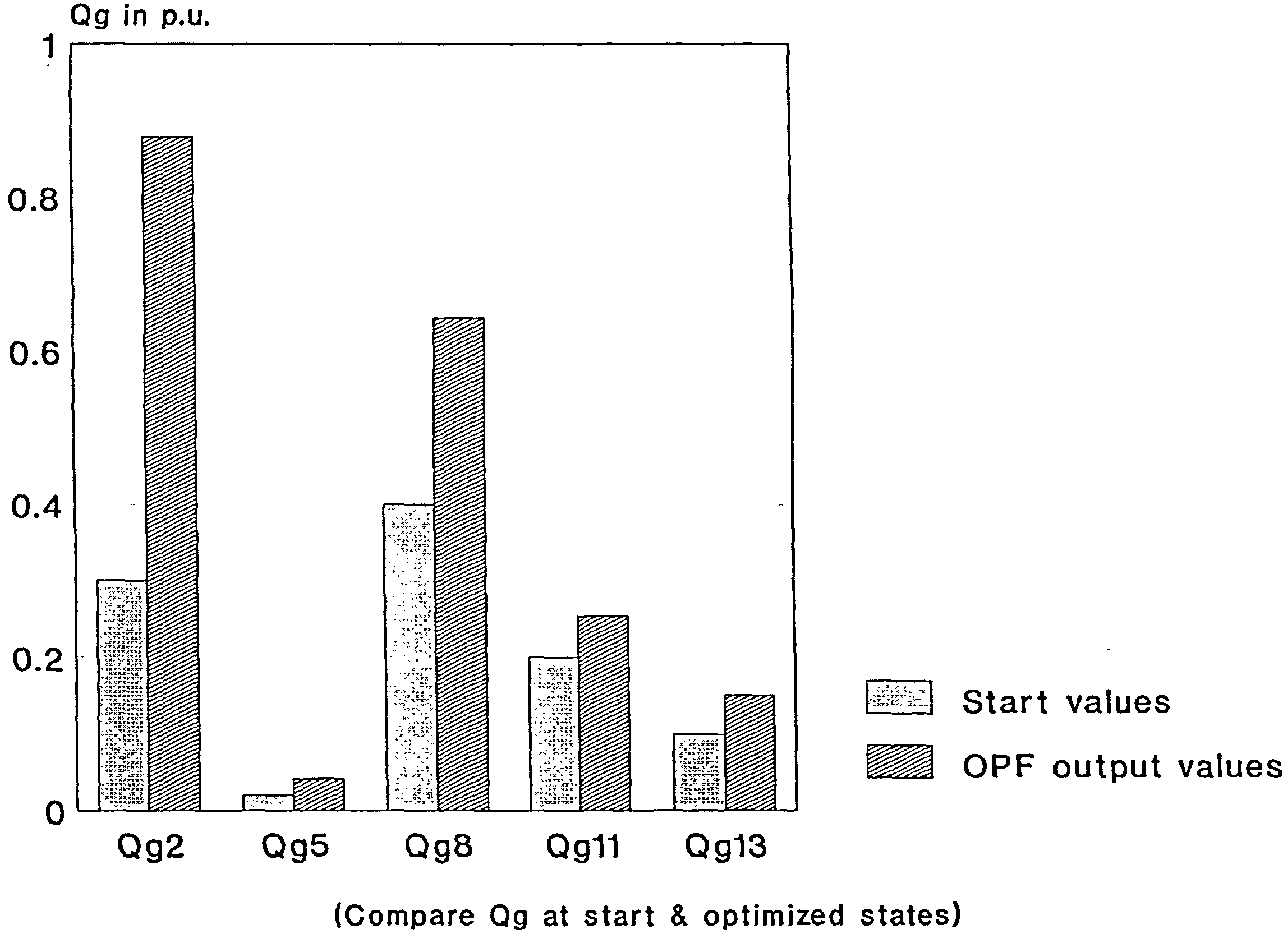


Fig.3-12 Comparison of Qg values
(30 bus system)



Chapter 4

Dynamic Security Analysis

4.1 General

In this chapter, the current methods of power system dynamic security analysis (DSA) are reviewed first, followed by discussions on the problems of applying the conventional methods to real time dynamic security assessment. Recent new research in this direction is then introduced. In particular, the rationales for applying a fast dynamic equivalent reduction method are discussed. The theory of dynamic equivalent and the derivation of critical machine identification are explained. Finally, test results on the test power systems are presented to illustrate the applicability of this proposed approach to fast dynamic security assessment.

4.2 The significance of dynamic security

The importance of maintaining security in power system operation and the topic of including static security limits in OPF programs have been discussed in the last chapter. As pointed out, dynamic security is measured by the system's ability to withstand large disturbances and maintaining normal state of operation after fault clearing. Maintaining dynamic security would avoid uncontrolled cascading tripouts that may lead to system collapse. It is thus important that in assessing the true security of a system, the dynamic security aspect should not be neglected. However, due to the need of performing very time consuming computations, such as in the traditional numerical integration methods, dynamic security assessment has often been neglected in real time operation. In this context, transient stability assessment is the principal component in dynamic security. With the increasing attention on dynamic security, there is as yet no satisfactory practical solution to include it in OPF and this is presently an open area of research. In many power utilities the normal practice is to perform detailed stability studies in the planning stage with detailed models in order to investigate the system's likely performance to those probable scenarios of disturbances. These studies would be taken to establish the operational limits of lines and machines through such repeated computer simulation of events. But, in actual operations, the system loading conditions and parameters may be different from those assumed. Hence security constraints derived from post-fault loadflow analyses are insufficient to ensure no degradation or even violation of system security due to the lack of consideration of transient stability limit on-line. In order to acertain a truely secure operation, an on-line dynamic security assessment scheme is thus desirable. In this chapter, a suitable methodology for an integrated approach incorporating dynamic security in OPF is aimed for and derivation of theory as well as test results are presented.

In our investigation of this problem, we have found that the current trend in security constrained OPF techniques only considers the post-contingency line current limits and neglects the possibility of loss of transient stability during the transition from the pre-contingency to the post-contigency state. This approach suffers from the serious drawback that dynamic contingency may endanger the stable transition of operation states of the system. In some literature, for example [20], it is suggested to express the dynamic security as preassigned limits of certain generator outputs via off-line simulations. But this methodology would not work reliably if we consider the cases of special loading conditions, such as high abnormal loads or unexpected outages already occurring in equipments. An adaptive scheme on-line to assess the current state's dynamic security should be introduced as an integrated module in OPF applications.

The main objectives of this chapter are thus as follows :

(i) To outline the philosophy of approach.

(ii) To describe the theory and formulation.

(iii) To explain the dynamic equivalent reduction method for dynamic security assessment.

As already raised in the first chapter, the economy and security of power system operation are normally two conflicting requirements. The normal practice is to operate the system to achieve maximum economy within acceptable security by considering security as a constraint in optimization. Static security constrained optimization using the total generation cost as the objective function and static security requirements as constraints have been formulated in the last chapter and solved by mathematical programming techniques. However, modern power systems are increasingly operated near to their critical stability limits and their danger of system collapse on certain credible dynamic contingency are causing increasing concern.

On the other hand, dynamic security assessment (DSA) on-line is now on the verge of practical implementation with the intensive research on direct methods of transient stability analysis. This chapter attempts to extend the above concept into a methodology that would consider dynamic security in OPF calculation in order to meet the need for such security control. Use would thus be made of such fast direct method of transient stability calculation as an integrated module in OPF in the next chapter.

4.3 DSA Solution Methods

It is relevant to review the current methods of dynamic security assessment here. There are three main types of approach to apply DSA and their applications in a dynamic security assessment scheme may be compared as in the following discussions.

(i) Numerical integration method to derive swing curves of machines.

(ii) Direct methods involving calculation of energy functions.

(iii) Extended equal area criterion method involving dynamic equivalent reduction.

In the first type, the evaluation of machines' swing curves by numerical integration of their swing equations is the most commonly used classical DSA method. This method has been successfully used for off-line planning work as it can be solved with detailed machine models and many system parameters may be studied in detail. For a credible set of dynamic contingencies, tests may be performed to provide the operator with guidelines on line flow limits, interface line flows and generation limits. It is usually considered that this classical method is suitable for planning purposes where time requirement is less important. For the present purpose of developing a fast on-line estimation of dynamic security this classical method is definitely too slow. With the advent of parallel processing and new computer technology it may be possible to speed up the calculation timing and come closer to on-line use.

However, the present thinking is the method is inherently too slow for on-line application where real time evaluation of the dynamic security is required. Moreover, the method cannot provide informations about the sensitivity of stability limit to the system parameters. Very often, planning engineers will rely on their own experiences and use trial and error method to determine the control action that can improve stability. Analytical solutions of this type are very useful to the required decision making of control engineers. Much more effort is required to reduce the computing timing as much as possible by employing more efficient algorithms and using network reduction of dynamic equivalents. In addition, off-line study results may not be as reliable as originally thought. The simulations may not be able to represent all the scienario of events. Special operating conditions due to unexpected events occurring may affect the predictions.

The present trend is to consider the use of direct methods of transient stability calculation for real time application use. The use of transient energy function methods to identify the boundary of insecurity region has been found to be a viable option.

Intensive research on computing controlling unstable equilibrium point (UEP) is being undertaken. Since the method finds the region of stability it is not easy to formulate control action. However further research work is continuing to improve its attraction and its on-line application could be a potentially suitable option in the future.

One of the most promising proposals in reducing the computational time requirement is by dynamic equivalent reduction; for example by gross equivalencing of the external system and to apply fast analysis to the resultant reduced model.[20] Current research shows promise to identify an energy margin for a contingency and given clearing time. The sensitivity of the energy margin to a system parameter is also computed. These can provide valuable guidelines to operators and lead to preventive control strategies which will be pursued further in the next chapter.

4.4 Dynamic equivalent reduction technique

The DSA module in this thesis uses the method (iii) to find the system's dynamic security performance and to compare it with the designated security margin at the monitoring stage. The method also identifies the critical machine or cluster of critical machines for the contingency it is extensible to find the required preventive control action if dynamic security is found to be unsatisfactory. An iteration method as an extension of the above monitor will also be developed to determine the required power output changes in order to satisfy the dynamic security limit in OPF and will be presented in the next chapter.

Essentially the proposed method can reduce the system to a reduced dynamic equivalent of two grouped machine only. Since the gross power system is carefully checked for its dynamic security and then reduced to an equivalent which consists of two machines, the analysis then proceeds to calculate a quantity which can quantify its dynamic security performane. In a later section, explanations will be presented on why the critical clearing time is chosen as that quantity. Here it is stipulated that the system critical clearing time is then evaluated for a contingency with a fast method called extended equal area criterion. The method has been tested to work satisfactorily for several power systems and for various possible operating conditions.

In addition, since the method always obtains a two machine equivalent with reasonably fast speed, the dynamic security calculation of its critical time will not increase much in effort with increase in system size. This is an important consideration for real-time computing as our tests are based on small to medium size networks. With this consideration in mind, the simulation results could be extended to very large networks.

As discussed, a fast direct method of transient stability assessment of the operating state as evaluated in the OPF module is now tested for its dynamic security. We have developed a method first proposed by Xue,Van Cutsem and Ribbens-Pavella (1988) [20] into an integrated scheme to determine the system's dynamic security with respect to the preselected dynamic contingency in the network. The major steps of the proposed dynamic equivalent method may be summarised as follows :

a) The multi-machine system is subjected to a selected dynamic contingency. The initial accelerations, just at the time when the disturbance occurs, of all machines are evaluated, screened and tested to identify the "critical " candidate machine or cluster of critical machines that are responsible for the instability. In this step, extra verification is required to make certain that the identification is valid. Then the system is reduced to a dynamic equivalent of the critical machine and the rest of the external system.

b) The resultant aggregate two machine equivalent may thus be analysed by extended equal area criterion for its dynamic security performance.

c) A security margin based on its critical clearing time to maintain transient stability is found. This is compared to the system requirement (which may typically be the minimum protection time setting plus some suitable time margin as security margin) to ascertain whether dynamic security is of satisfactory level or not.

The usual practice of utilities is to use a pre-selected set of event. We are applying a tactic of using the most serious dynamic contingency with a three-phase short circuit at the generator terminals' side of the transmission line followed by line switching to clear the fault. When a system's critical machine or cluster is located, the case of a fault occurring at the terminal of the critical machine is tested for the dynamic security performance.

4.5 Theory of method

4.5.1 Identification of critical machine

The most serious dynamic contingency for the said identified critical machine is a solid three phase fault at generator terminals followed by postfault line switching. The identified critical machine(s) would be the machine(s) responsible for system separation should the contingency occur. It is of importance that this method can identify the critical machine correctly. From many tests performed and from the current literature, it is found that immediately following the disturbance, the accelerations of the machines are of significance to its dynamic behaviour. The initial acceleration is thus a good indicator of the weaker machine that may go unstable later. Hence the following steps are used for the necessary critical machine identification.

(i) Assume a n machine power system. Determine the initial acceleration of all machines on the occurrence of fault and arrange them on descending order of magnitudes. Filter out the most probable critical machine candidates by comparing their values.

(ii) Further evaluate the dynamic security performance of those machines. Compute in turn the system critical clearing times (CCT) corresponding to each candidate critical machine. The machine that gives the smallest CCT is most critical and its value gives the resultant system CCT.

In developing the model, the classical machine model of an n-machine power system is used. This is considered to be relevant since the aim of model is for on-line dynamic security assessment and usually the first swing transient stability is sufficient for this assessment purpose. Each generator is represented electrically as a constant voltage source behind its transient reactance and each load as a constant impedance. The motion of i-th machine is described by

$$d\delta_i/dt = \omega_i \; ; \; M_i(d\omega_i/dt) = P_{mi} - P_{ei} \qquad (4\text{-}1)$$

,and $P_{ei} = (E_i)^2 Y_{ii} \cos\theta_{ii} + \sum_{j=1 \text{ to } n, j\neq i} E_i E_j Y_{ij} \cos(\delta_i - \delta_j - \theta_{ij})$ (4-2)

,where	δ_i	rotor angle
	ω_i	rotor speed
	M_i	inertia coefficient
	P_{mi}	mechanical input power
	P_{ei}	electrical output power
	E_i	voltage behind direct-axis transient reactance
	Y	admittance matrix reduced at the internal generator nodes
	Y_{ij}, θ_{ij}	modulus & argument of the ij-th element of Y

M_i, P_{mi}, E_i are assumed to be constant throughout the transient.

The initial accerlation γ_i of machine i in step (i) is defined as :

$$\gamma_i = \{ P_{mi} - P_{ei}(\delta(t_0^+))\} \quad / M_i \qquad (4\text{-}3)$$

,where P_m is mechanical input power,

P_e is electrical output power,

δ is rotor angle, and

M_i is angular momentum of machine i.

4.5.2 Reduction to two machine equivalent

The critical machine s is modelled by classical machine model as follows:

$$M_s \,(d^2\delta/dt^2) = P_{ms} - P_{es} \qquad (4\text{-}4)$$

, where the subscript s stands for the specific machine as the candidate critical machine.

The remaining (n-1) machines (assumed to be the set A) are modelled as an equivalent, aggregate, machine "a" using the standard centre of angles (COA) concept [20] as follows. A denotes the set of all remaining (n-1) machines. Machine s is excluded from COA.

$$M_a = \sum_{i\subset(n-1)} M_i \qquad (4\text{-}5)$$

$$\delta_a = \{ \sum_{i\subset(n-1)} M_i\delta_i \} / M_a \quad \text{and } \gamma_a = d^2\delta/dt^2 \qquad (4\text{-}6)$$

The motion of A is obtained by summing up the corresponding (n-1) equations as below:

$$M_l(d^2\delta_l/d^2t) = P_{ml} - P_{el} \;,\; l\in A \qquad (4\text{-}7)$$

By using equation (4-4) we get

$$M_a(d^2\delta_a/d^2t) = \sum_{l\in A} (P_{ml}\text{-}P_{el}) \qquad (4\text{-}8)$$

In the above (4-7) and (4-8), P_{el} is of the form in (4-4). Further simplification is obtained by setting $\delta_j=\delta_a$,for $j\in A$ (4-9)

$$\delta_s - \delta_l = \delta_s - \delta_a \;;\; \delta_j - \delta_l = 0 \quad ,\text{for } l,j \in A \qquad (4\text{-}10)$$

In this case, P_{el} can be expressed by

$$P_{el} = (E_l)^2 Y_{ll} \cos\theta_{ll} + E_l E_s Y_{ls} \cos(\delta_a - \delta_s - \theta_{ls})$$
$$+ \sum_{j \in A, j \neq l} E_l E_j Y_{lj} \cos\theta_{lj} \qquad (4\text{-}11)$$

The above assumption is physically sound and well validated by practice.

The motion of machine s is

$$M_s \, (d^2\delta_s/d^2t) = P_{ms} - P_{es} \qquad (4\text{-}12)$$

P_{es} is expressed by equation similar to (4-4) and in addition assumption (4-10) has been taken into account.

$$P_{es} = (E_s)^2 Y_{ss} \cos\theta_{ss} + \sum_{j \in A} E_s E_j Y_{sj} \cos(\delta_s - \delta_a - \delta_{sj}) \qquad (4\text{-}13)$$

4.5.3 Reduction to one-machine-infinite-bus model

The two machine equivalent above is then further transformed to an equivalent one-machine infinite-busbar (OMIB) model for finding its CCT by a fast procedure. To derive the OMIB model, we consider the relative rotor acceleration as follows :

$$\delta = \delta_s - \delta_a \ ; \ (d^2\delta/dt^2) = (d^2\delta_s/dt^2) - (d^2\delta_a/dt^2) \qquad (4\text{-}14)$$

Substituting equations (4-8),(4-12) into (4-14), we obtain

$$M \, (d^2\delta/dt^2) = P_m - P_e \qquad (4\text{-}15)$$

where $M = M_s M_a (M_T)^{-1}$; $M_T = \sum_{i=1 \text{ to } n} M_i$ (4-16)

$$P_m = (M_a P_{ms} - M_s \sum_{l \in A} P_{ml})(M_T)^{-1} \ ; \ P_e = (M_a P_{es} - M_s \sum_{l \in A} P_{el})(M_T)^{-1} \qquad (4\text{-}17)$$

Substituting expressions (4-11) and (4-13) in equation (4-15) then transforms it into the familiar expression of equivalent OMIB equation of motion as below :

$$M\ (d^2\delta/dt^2) = P_m-[P_c+P_{max}\sin(\delta-\nu)] = P_m-P_e \qquad (4\text{-}18)$$

where

$$P_c = [M_a(E_s)^2G_{ss}-M_s(\ \textstyle\sum_{l\in A}\{E_l\}^2G_{ll}+\ \sum_{l,j\in A;j\neq l} E_lE_jG_{lj})]/M_T$$

$$P_{max}=[\textstyle\sum_{l\in A}E_sE_lY_{sl}(M_s^{\ 2}+M_a^{\ 2}-2M_sM_a\cos2\theta_{sl})^{1/2}]/M_T$$

$$\nu = tg^{-1}\{M_T/(M_a-M_s)\}tg\theta_{s,a}-\pi/2 \qquad (4\text{-}19)$$

$\theta_{s,a}$ is the argument of the equivalent admittance between s and a

$$tg\ \theta_{s,a} = (\ \textstyle\sum_{l\in A} B_{sl}\ )\ (\ \sum_{l\in A} G_{sl})^{-1} \qquad (4\text{-}20)$$

B and G stand for the susceptance and conductance :

$$G_{sl}=Y_{sl}\cos\theta_{sl}\ ;\ B_{sl}= Y_{sl}\sin\theta_{sl} \qquad (4\text{-}21)$$

The OMIB formulation is usd in conjunction with the equal area criterion to derive means for fast transient stability assessment. The computing speed of this module is relatively fast and give reliable results as compared to a full analytical study of swing curve. In addition the computing time requirement will not increase drastically with increase in system bus size as a dynamic equivalent reduction is first performed, resulting in a simplified machine model. The calculation of CCT at this stage would be fast. This will be an advantage from the real-time computation requirement point of view.

4.5.4 Equal area criterion

The OMIB formulation as derived above is now used in conjunction with the classical equal area criterion and is further developed to derive fast transient stability assessment. In order to explain this it is necessary to define the terms used in classical equal area criterion, followed by the new extension of it in the extended equal area criterion method used in this thesis.

The P-δ curves provided by (4-18) are plotted for the pre-fault or original (O), during fault (D), and post-fault (P) configurations as illustrated in Figure 5-2. The figure is the basis of the well known equal area criterion. The original steady-state operation is defined by the rotor angle δ_0 located by the horizontal line $P=P_m$ with curve O. The value that the δ angle reaches at the fault clearing time defines the decelerating area. The areas shown accelerating area A_{acc} and decelerating area A_{dcc} denote the transient accelerating and decelerating energies in the transient operation. The equal area criterion recognises that the faulted system keeps capable of recovering stability as long as A_{acc} is smaller than A_{dcc}. The borderline case corresponds to when A_{acc} is equal to A_{dcc} , for which the system reaches the critical clearing angle (CCA or δ_c). The critical clearing time (CCT or t_c) is the time required by the faulted system to move from δ_0 ($t=t_o$) up to δ_c ($t=t_c$).

An analytical straight forward relationship between rotor angle and the corresponding fault clearing time is derived in Taylor Series form :

$$\delta_\tau = \delta_0 + \tfrac{1}{2}\gamma\tau^2 + (1/24)\gamma^{(2)}\tau^4 + (1/720)\gamma^{(4)}\tau^6 + \ldots\ldots \qquad (4\text{-}22)$$

where δ_0 is the original steady-state rotor angle. The successive derivatives $\gamma^{(2)},\gamma^{(4)},\ldots,$ are obtained at immediately after the fault inception. To get fast analytical expression of γ in terms of δ we may truncate the above expression after third right-hand side term without sacrificing too much accuracy. To derive the value of CCA (δ_c), it is by definition the angle at which $A_{dcc} = A_{acc}$. In Figure 5-2, assuming it represents the value of CCA, and

$$r_1 = P_{eD} / P_{eO} \qquad (4\text{-}23)$$

$$r_2 = P_{eP} / P_{eO} \qquad (4\text{-}24)$$

By evaluating the values of A_{acc} and A_{dcc} and equating them to solve for the value of CCA, it can be derived that

$$\cos \delta_c = \{(P_m/P_{eO})(\delta_m-\delta_0)+ r_2\cos\delta_m - r_1\cos\delta_0\}/(r_2 -r_1) \qquad (4\text{-}25)$$

Solving for τ the Taylor Series (4-22), truncated after the third RHS term, yields the following expression for $\tau=f(\delta)$ for small τ values,

$$\tau = [(-b \mp (b^2-4dc)^{1/2})/2d]^{1/2} \qquad (4\text{-}26)$$

where $d=\gamma^{(2)}=\gamma_s^{(2)}-\gamma_a^{(2)}$; $b=12\gamma$; $c=-24[\delta_\tau-\delta_0]$ (4-27)

4.6 Tests of dynamic security assessment

In order to verify the suitability and accuracy of the derived DSA method, tests are performed on the example systems with the following objectives which are designed to support our theory.

1. Test cases are derived from the examples of 5-bus and 30-bus system used in the last chapter on optimum power dispatch. These test cases have already been investigated for their performance in optimum dispatch. Based on those results it is advantageous to investigate the dynamic security at those conditions of

operation. This will ensure a continuity of our developments in this project.

2. The operating conditions are also taken on several scenarios so as to investigate the effects due to changes in economy of operation.
3. Since the static security level of the optimum power dispatch results have already been obtained in the last chapter, the first tests are based on those results. They are then developed into more detailed analysis with our proposed method.
4. In addition, the case studies are compared with numerical integration of swing curves to verify the accuracy of this approach.

In the course of investigation it is found that the identification of critical machine(s) is of prime significance to the success of this method. It will be demonstrated in the following section of test results that the accuracy is good when the identification of the critical machine is correct. This observation has led to the refined procedure of identification applied in this thesis. Additionally, to further illustrate this point the swing curves results are also shown with both detailed system as well as with a reduced dynamic equivalent system in the following sections.

4.6.1 Test results of 5-bus system

The datas of the 5-bus system are given in the Appendix. The test procedures are arranged in the the following sequence to investigate the efficiency and accuracy of the method. A comparison is also made with the detailed model system using step by step numerical integration of the classical machine swing equations.

1. With the base case of loading condition, the system's dynamic security is analysed using the dynamic equivalent reduction method and the Extended Equal Area Criterion approach.
2. For the same load, the output setting of the critical generator (G_3) is adjusted in several steps and the dynamic security analysis is repeated accordingly.
3. The variation of other relevant parameters during the above step is also tabulated.

For this series of tests, the following machine constants are used.

TABLE 4-1 Machine constants of Systm A (5-bus system)

Generator no.	1	2	3
H-constant (pu)	5	5	1.5
Transient reactance (pu)	0.125	0.215	0.215

For a three-phase fault at busbar 3 when the system is delivering base load, the transient stability performance of the system is studied using a standard program which uses numerical integration of swing equations of machines by step-by-step method. As shown in Table 4-2 that follows, the transient stability performance of System A (5-bus system) quantified by its system CCT is calculated with different static security levels in the system. In addition, the system is also studied by swing curve of the aggregate two machine equivalent (dynamic equivalent reduction) performed by the proposed method in this chapter and the swing curve results are shown in Figures 4-1 to 4-4 for the first two static security levels. It is clear that the results of CCT by the methods are very close to each other and the accuracy is good.

Table 4-2 Transient stability performance of System A at different static security levels.

Static security level	Cost (pu)	CCT (s.)	P_{G3} (pu)	P_m (pu)
1	1136	0.107	1.664	1.285
2	1165	0.141	1.197	0.823
3	1178	0.157	1.04	0.666

A graphical illustration of the above results is presented in the Figure 4-5. From the results it is obvious that the adjustment of the real power generation output of the critical machine (P_{g3} in this case) has a significant efect on the security and the economy of operation. In this particular case, the system security and economy trends are quite predictable since their variation conforms to the basic consideration of this project. In general this is in line with the normal behaviour of stability limited power systems where the stability margin is affected significantly by the operation condition. As the load sharing of the critical generator decreases, the system stability margin improves but the operating cost would become higher, at a cost of security improvement.

4.6.2 Test results of 30-bus system (System D)

A series of tests are performed with same objectives on a modified 30-bus system (System D line data and load data are given in the Appendix). The following Table 4-3 contains the dynamic constants including H-constants and transient reactances of machines respectively.

TABLE 4-3 H-constants and transient reactances of machines (System D)

Generator #	1	2	5	8	11	13
H-constants (s)	5.5	1.4	1.2	1.0	0.8	1.4
Transient reactance (pu)	0.187	0.310	0.350	0.480	0.500	0.430

In order to investigate the transient stability performance of the 30-bus system and its relation with optimum dispatch, the following modified cost coefficients of the generators are used for the modified 30-bus system (System D). System D has more heavy loading resulting in a more stressed system. System D and System C have the same line parameters. The differences are their loads and cost coefficeients which would affect the operating cost.

TABLE 4-4 Modified cost coefficients for System D (Modified 30-bus system)

Generator # (i)	A_i	B_i (/ MW)	C_i (/ MW^2)
1	0.0	200.0	88.5
2	0.0	175.0	175.0
5	0.0	100.0	625.0
8	0.0	325.0	103.4
11	0.0	300.0	150.0
13	0.0	250.0	180.0

TABLE 4-5 Limits of parameters in System D (Modified 30-bus system)

Bus # (i)	P_{Gi} (MAX) in pu	P_{Gi} (min) in pu
1	3.4	0.9
2	0.8	0.2
5	1.0	0.1
8	1.0	0.1
11	1.045	0.6
13	1.1	0.4

The OPF program is used to find the optimized power dispatch condition and then followed by DSA analysis to investigate its transient stability performance.

TABLE 4-6 OPF results of System D (Modified 30-bus system)

Bus # (i)	Bus voltage (pu)	Angle (degree)	P_{Gi} (pu)	Q_{Gi} (pu)
1	1.10	0.000	3.35315	-0.06179
2	1.08	- 6.126	0.80000	0.87936
3	1.04378	-10.995	-	-
4	1.03390	-13.300	-	-
5	1.03	-11.502	1.00000	0.04077
6	1.01717	-17.461	-	-
7	1.01039	-15.505	-	-
8	1.04	-16.286	1.00000	0.64260
9	1.05062	-21.935	-	-
10	1.06500	-21.630	0.00	0.42447
11	1.08	-10.891	1.04500	0.25359
12	1.07	-13.055	0.00	-0.05001
13	1.08	- 5.397	1.10000	0.15077
14	1.06425	-15.166	-	-
15	1.06	-16.678	0.00	0.08243
16	1.05808	-16.987	-	-
17	1.06	-20.522	0.00	0.06656
18	1.05319	-19.365	-	-
19	1.05413	-20.661	-	-
20	1.06	-21.069	0.00	0.08663
21	1.06	-22.327	0.00	0.13197

22	1.05981	-22.325	-	-
23	1.06	-19.838	0.00	0.08778
24	1.05	-23.158	0.00	0.11180
25	1.02266	-27.063	-	-
26	1.00508	-27.479	-	-
27	1.01829	-29.329	-	-
28	1.00630	-18.765	-	-
29	1.05	-32.078	0.00	0.18207
30	1.01666	-32.270	-	-

Initial generation cost = 4830.530 units

Optimised generation cost = 4041.193 units

Total P generation = 8.29815 pu

Total Q generation = 3.02899 pu

System P loss = 0.42015 pu

System Q loss = 1.76699 pu

The system security assessments are carried out with three different fault locations and the critical clearing times as well as P_G of the critical machine, identified as machine # 11 in all cases, are as follows. In addition, the transient stability of the test system D is also investigated with different outputs from the critical machine (Machine # 11) at the base load condition. The results are then plotted out in Figures 4-6 and 4-7 respectively, where it is observed that as the critical machine loading is increased, the system economy improves but the stability performance worsens (as the system CCT becomes smaller in value). This is in line with the idea put forward in this thesis on the conflicting requirements of economy and security and also the results of system A (refer to Figure 4-5 as discussed in last section).

Table 4-7 Transient stability performance of system D at OPF solution

Busbar fault located at bus # (on line i-j)	System CCT (s)	P_G from critical machine (pu)
Bus 1 (on line 1-3)	0.1298	1.045
Bus 2 (on line 2-5)	0.1302	1.045
Bus 8 (on line 8-6)	0.1329	1.045

The accuracy and reliability of the dynamic security assessment by the reduced dynamic equivalent model needs to be verified by comparing with bench mark solutions using the full system model solved by step by step numerical integration method. This is performed with the same system data as in the previous section of tests.

In addition the swing curves are also solved for a two machine equivalent model which includes a) the critical machine and b) the aggregate of the rest of the machines acting as an equivalent machine. Instead of using the Xue-Pavella method of further reducing the system , the solution is now by numerical solution of swing equations of the two machines to find swing curves.

The technique used is by repeated swing curves plotting to verify if the critical clearing time found in the reduced machine model is conforming to the full model or not. Swing curves for the two conditions are shown from Figures 4-8 to 4-13 respectively. The test results show that the identified critical machine is the machine which would be responsible for separation from the rest of the system when the critical clearing time is exceeded. One of the observations is that instability results from the weaker machine having a high loading level. The accuracy is good for the cases studied shown when the critical machine is being correctly identified.

4.7 Conclusions

The work reported in this chapter is crucial since the success of a model that can predict the dynamic security performance with speed and reliability is essential to achieving the objectives of this project. As discussed the choice and the investigations reported are favouring the dynamic equivalent reduction method as developed in this chapter for reasons summarised as follows.

1. The dynamic equivalent reduction gives a model which is fast and sufficiently accurate to assess its dynamic security.
2. The method identifies the critical machine which is responsible for the loss of synchronism when separation occurs. This initiation of instability is clearly something we like to prevent form happening on the event of contingency. Hence it gives the clue to finding a control strategy on the critical machine.

3. The dynamic security and its degree of margin as shown by the critical clearing time could be evaluated with speed by the method. This leads to the analytical solution of dynamic security limited OPF solution in the next chapter.

4. The accuracy and reliability of the method is quite dependent on the correct identification of the critical machine. For this reason a careful technique would be required for identification process in the application of this method. However for stability limited system where the application of this method should be made, the critical machine is likely to be quite easily identified by heuristic technique.

5 As demonstrated in the results, the critical machine is of great significance in the dynamic security performance. This important observation leads to the further development in the next chapter where this is exploited to integrate with OPF calculation.

The method is chosen for this research project in view of the main reasons stated above. In practical application, it is clearly desirable to extend the method to include a contol module that can find suitable preventive control action should dynamic security limits are exceeded. This will be the work that is to be reported in the next chapters. In addition the extension could bridge the gap for completing a closed loop of finding preventive dynamic security control in economic dispatch operation. Only by then would this research work constitute a complete application package.

SWING ANGLE WITH EQUIVALENT M/C

(1st config. with clearing time 0.10s)

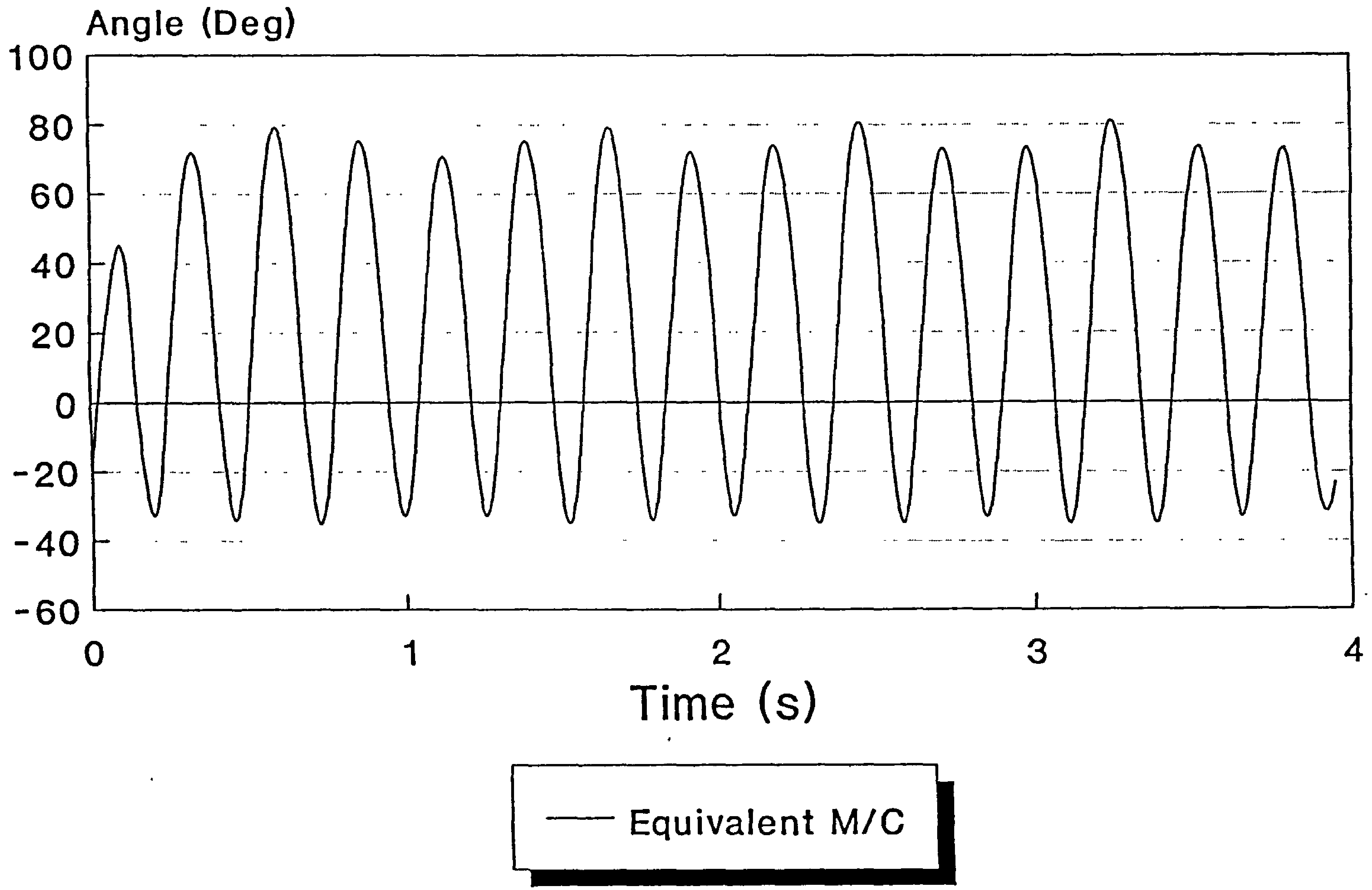


Fig. 4-1

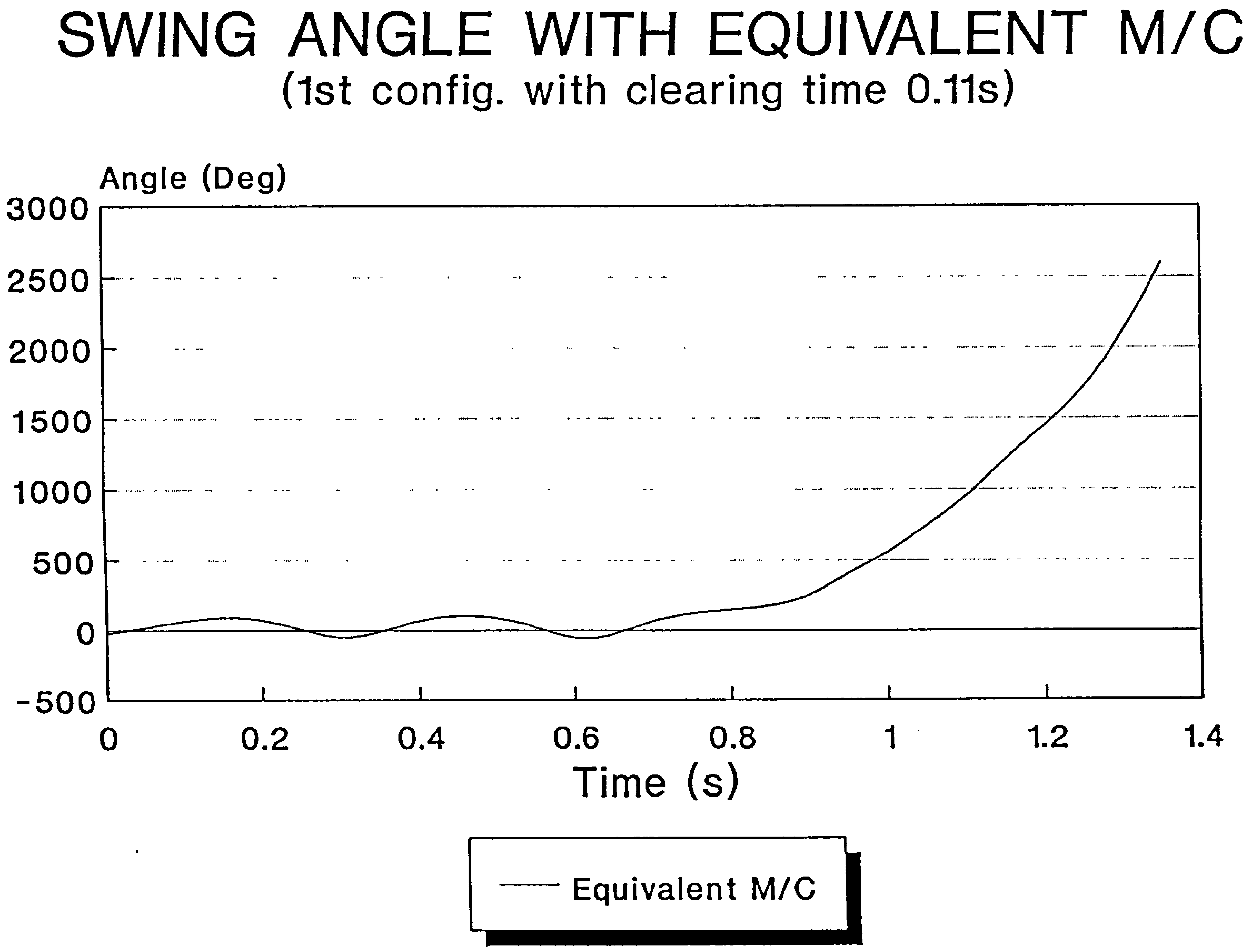
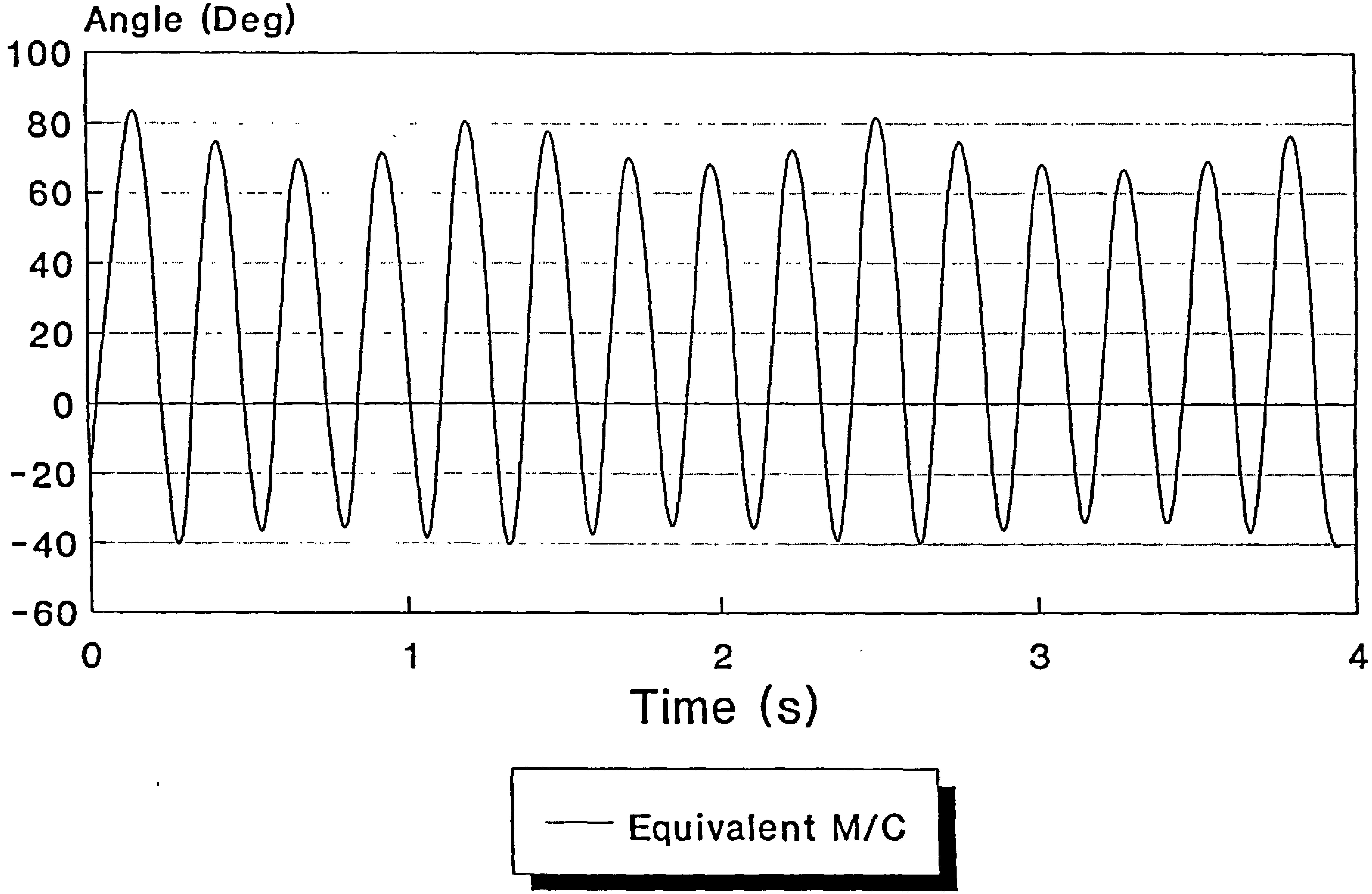

SWING ANGLE WITH EQUIVALENT M/C
(1st config. with clearing time 0.11s)
Angle (Deg)
3000
2500
2000
1500
1000
500
0
-500
0
0.2
0.4
0.6
0.8
1
1.2
1.4
Time (s)
Equivalent M/C

Fig. 4-2

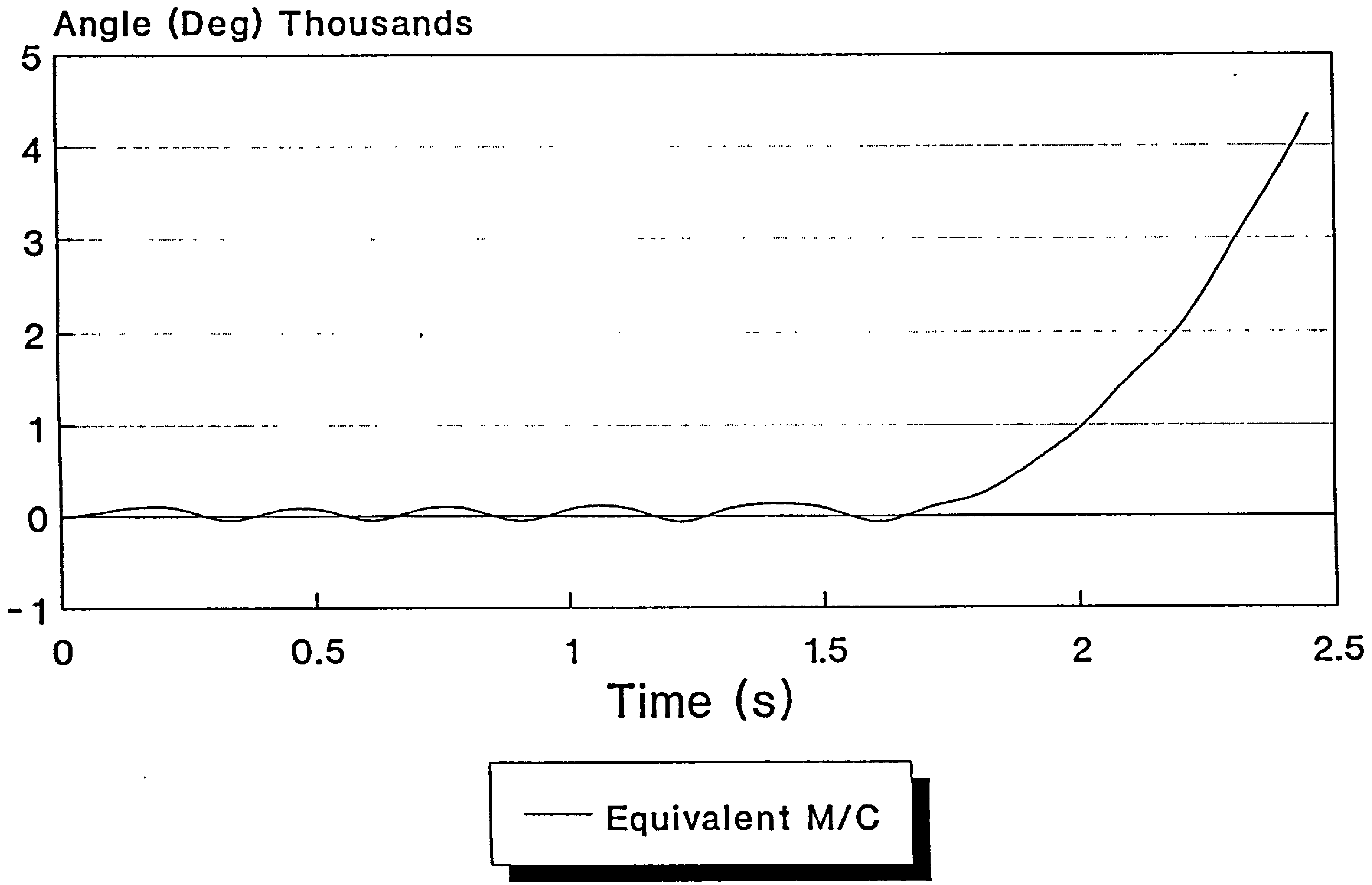


SWING ANGLE WITH EQUIVALENT M/C
(2nd config. with clearing time 0.14s)

Fig. 4-3

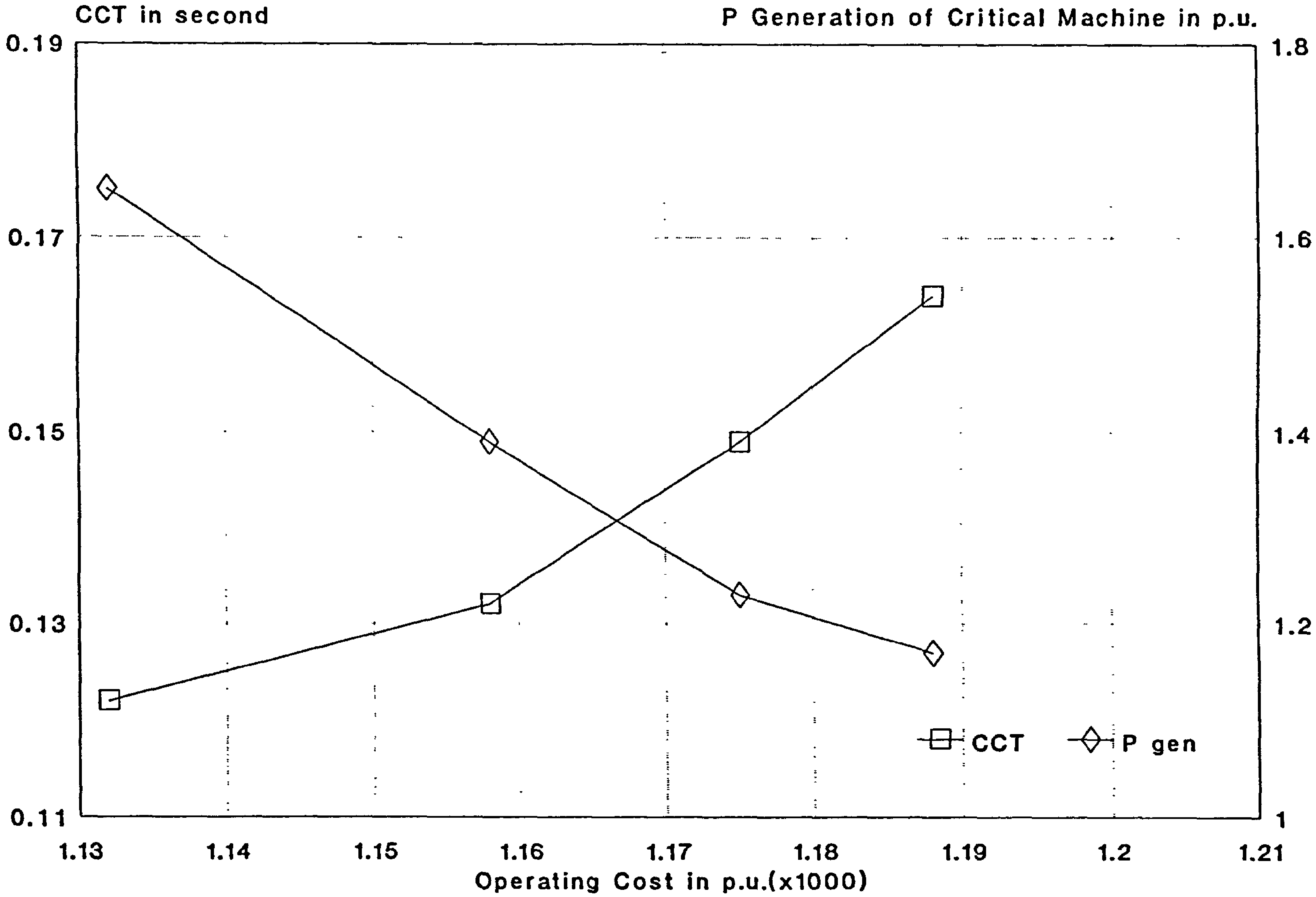
SWING ANGLE WITH EQUIVALENT M/C

(2nd config. with clearing time 0.15s)



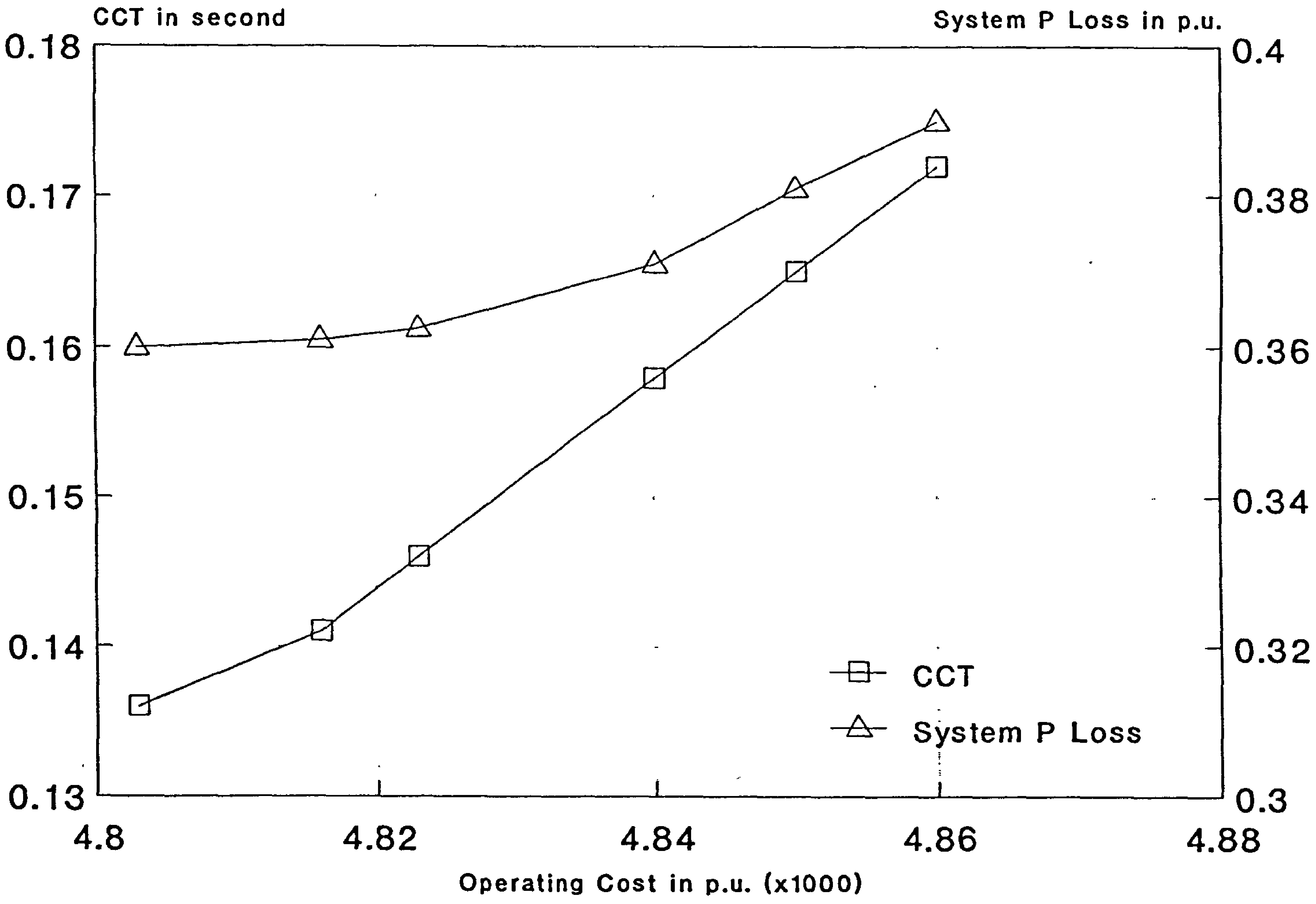
Fig,4-4

Fig 4.5 OPF results at fixed load
(5-bus system)



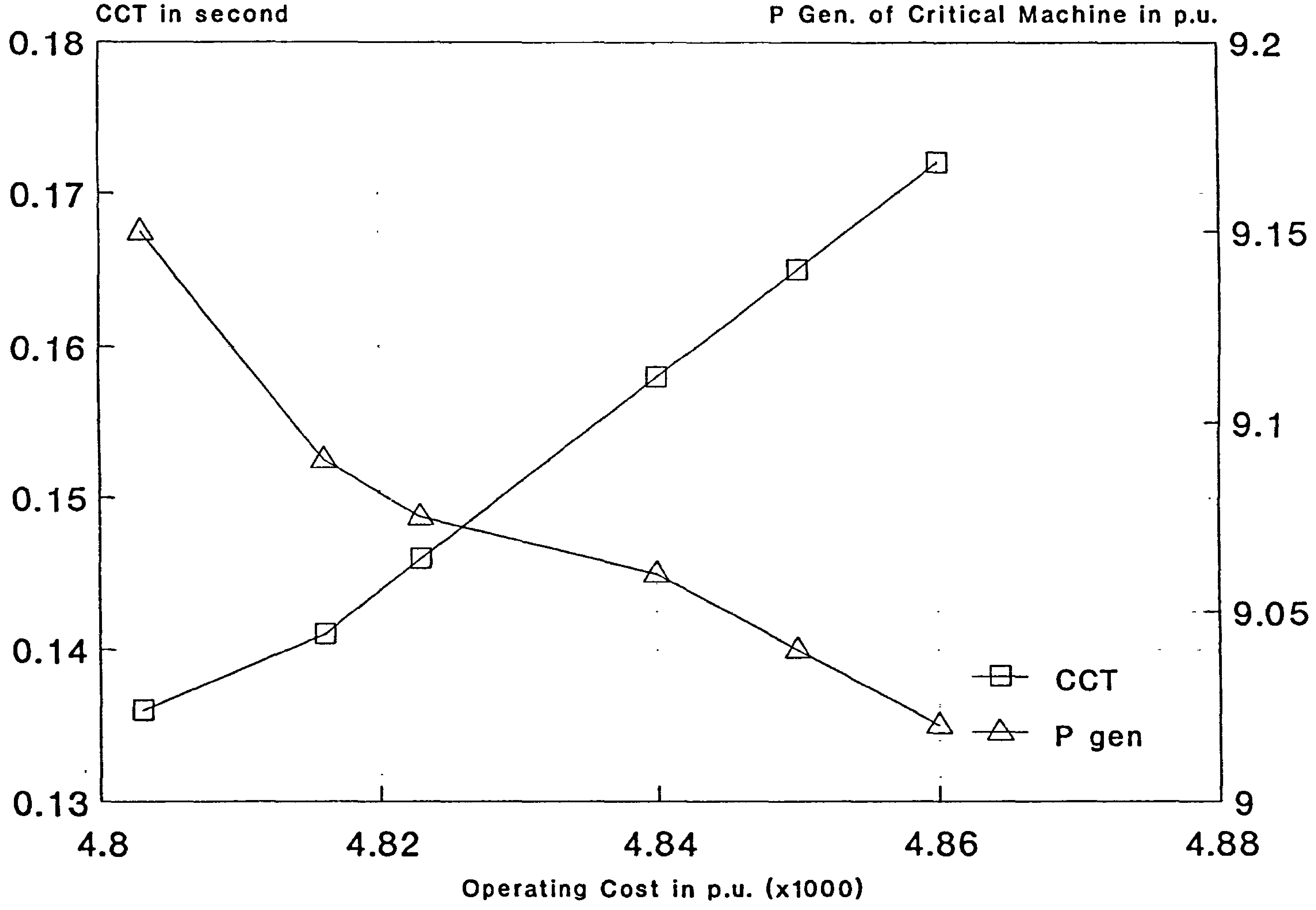
(Compare OPF results as Pg is changed)

Fig 4.6 OPF results at fixed load
(30 bus system)



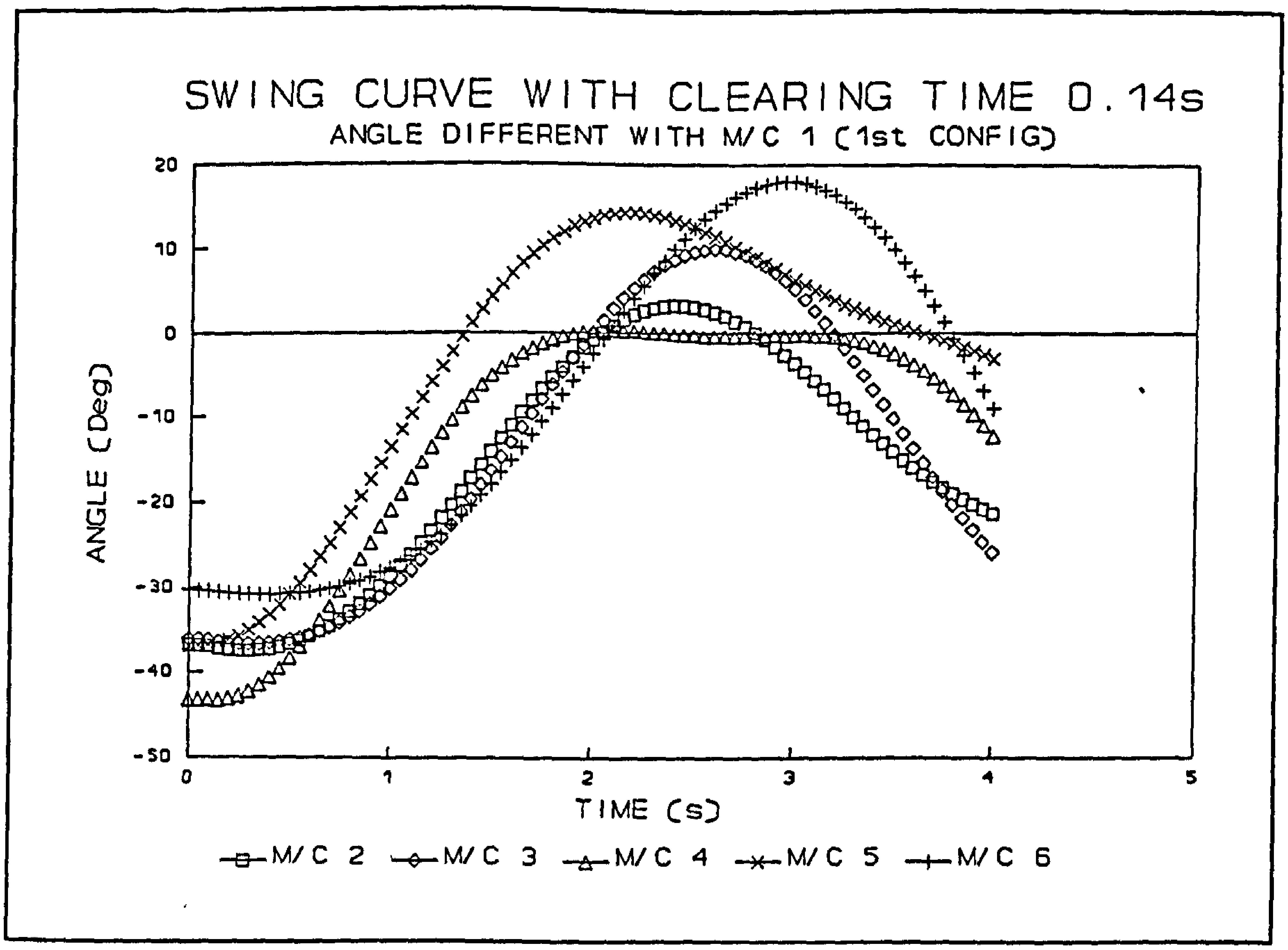
(Compare OPF results when Pg is changed)

Fig 4-7 Compare OPF results at base load
(30 bus system)



(compare OPF results as Pg is changed)

Fig.4-8


SWING CURVE WITH CLEARING TIME 0.14s
ANGLE DIFFERENT WITH M/C 1 (1st CONFIG)
ANGLE (Deg)
20
10
0
-10
-20
-30
-40
-50
0
1
2
3
4
5
TIME (s)
M/C 2
M/C 3
M/C 4
M/C 5
M/C 6

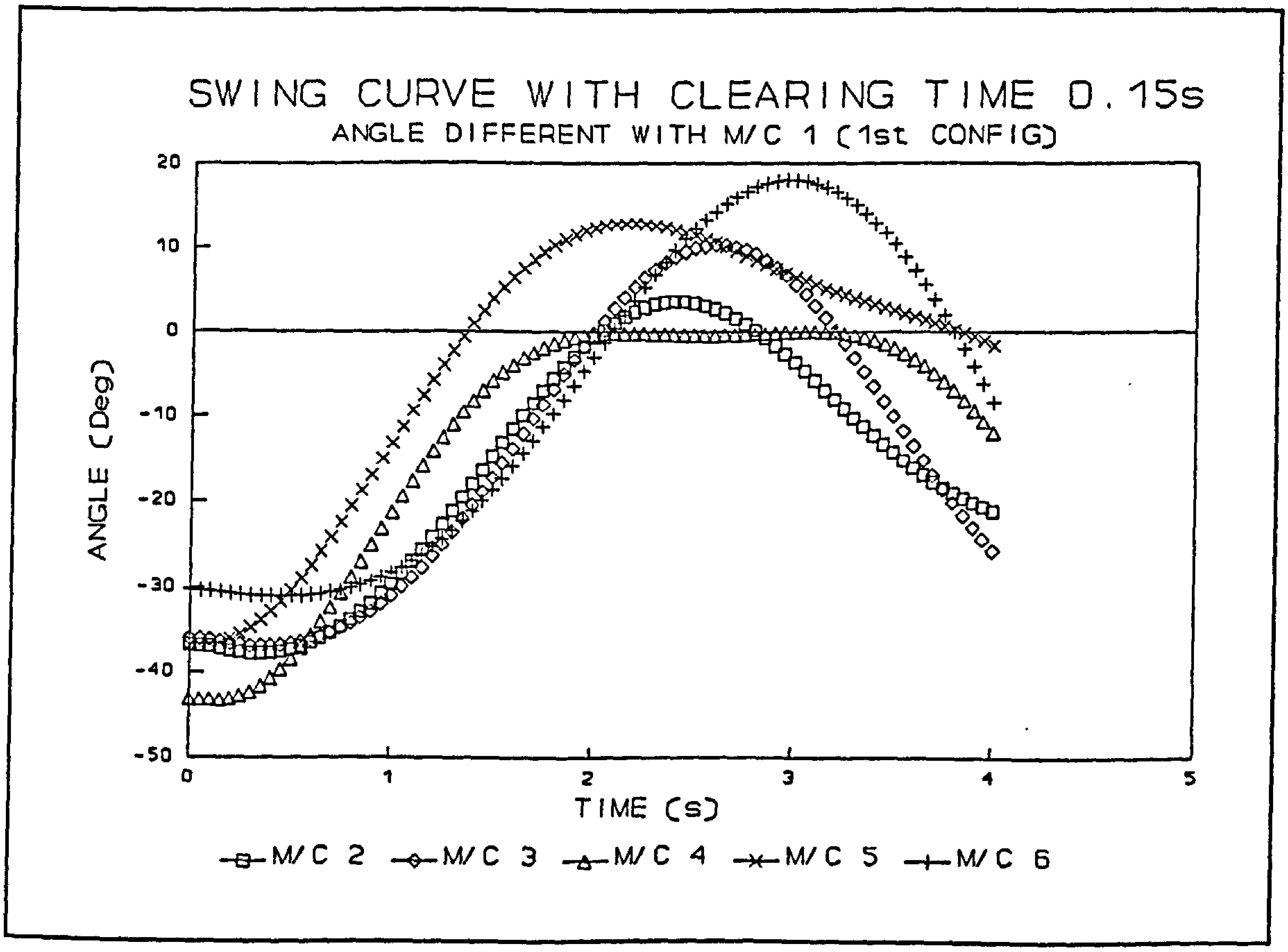

SWING CURVE WITH CLEARING TIME 0.15s
ANGLE DIFFERENT WITH M/C 1 (1st CONFIG)
ANGLE (Deg)
20
10
0
-10
-20
-30
-40
-50
0
1
2
3
4
5
TIME (s)
M/C 2
M/C 3
M/C 4
M/C 5
M/C 6

Fig.4-9

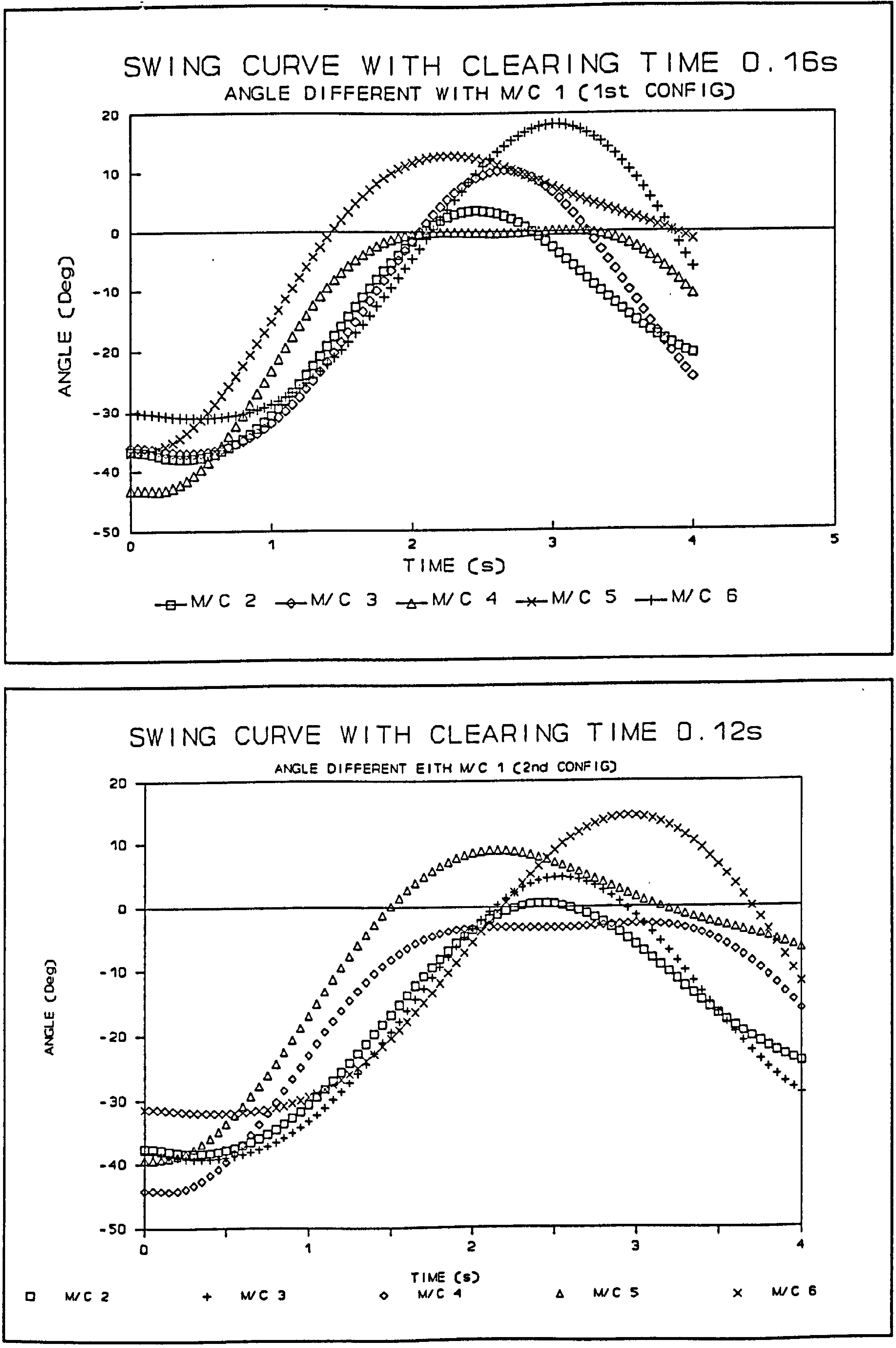
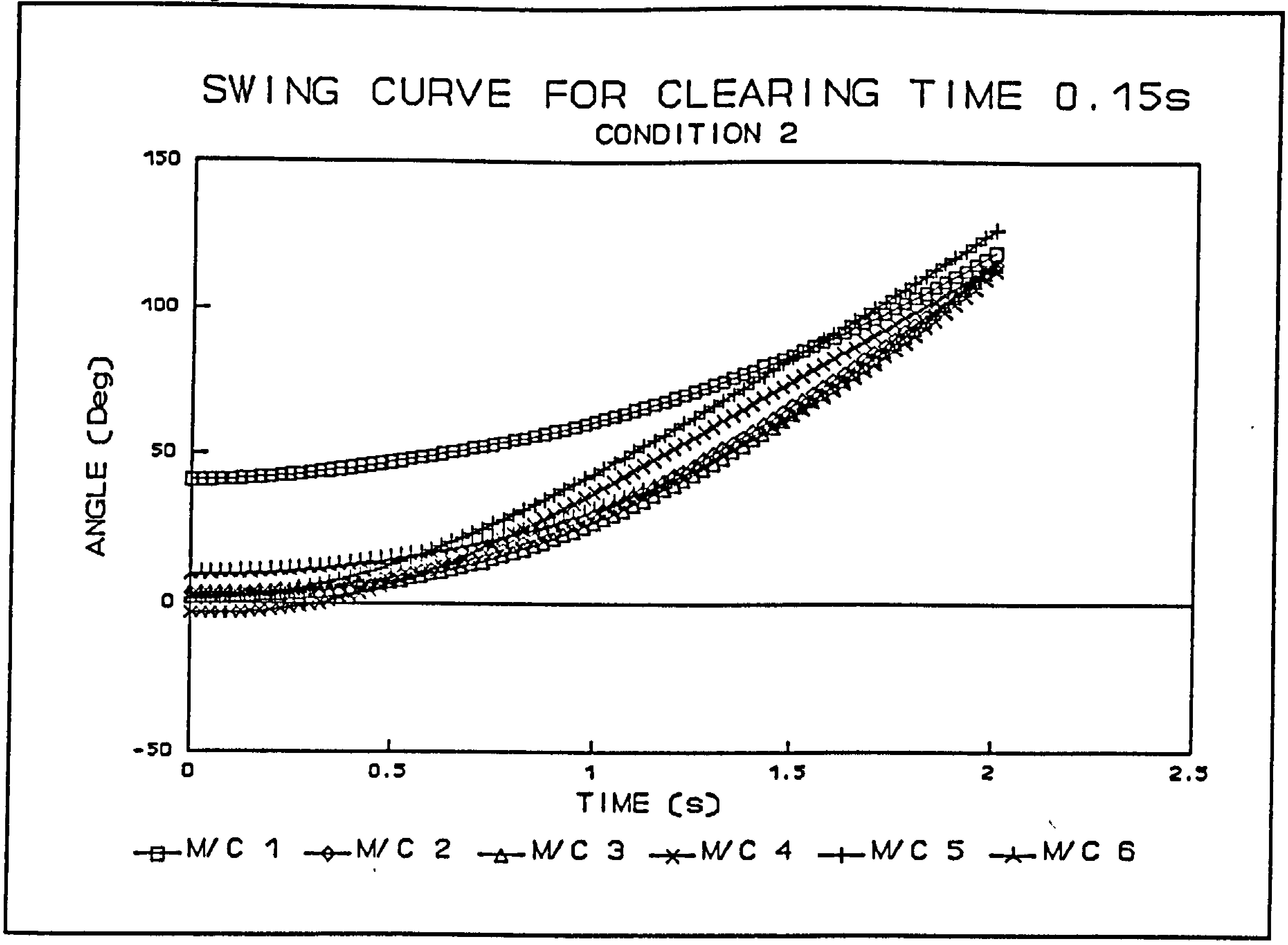

SWING CURVE WITH CLEARING TIME 0.16s
ANGLE DIFFERENT WITH M/C 1 (1st CONFIG)
ANGLE (Deg)
20
10
0
-10
-20
-30
-40
-50
0
1
2
3
4
5
TIME (s)
M/C 2
M/C 3
M/C 4
M/C 5
M/C 6
SWING CURVE WITH CLEARING TIME 0.12s
ANGLE DIFFERENT EITH M/C 1 (2nd CONFIG)
ANGLE (Deg)
20
10
0
-10
-20
-30
-40
-50
0
1
2
3
4
TIME (s)
M/C 2
M/C 3
M/C 4
M/C 5
M/C 6

Fig.4-10


SWING CURVE FOR CLEARING TIME 0.15s
CONDITION 2
ANGLE (Deg)
150
100
50
0
-50
TIME (s)
0
0.5
1
1.5
2
2.5
M/C 1
M/C 2
M/C 3
M/C 4
M/C 5
M/C 6

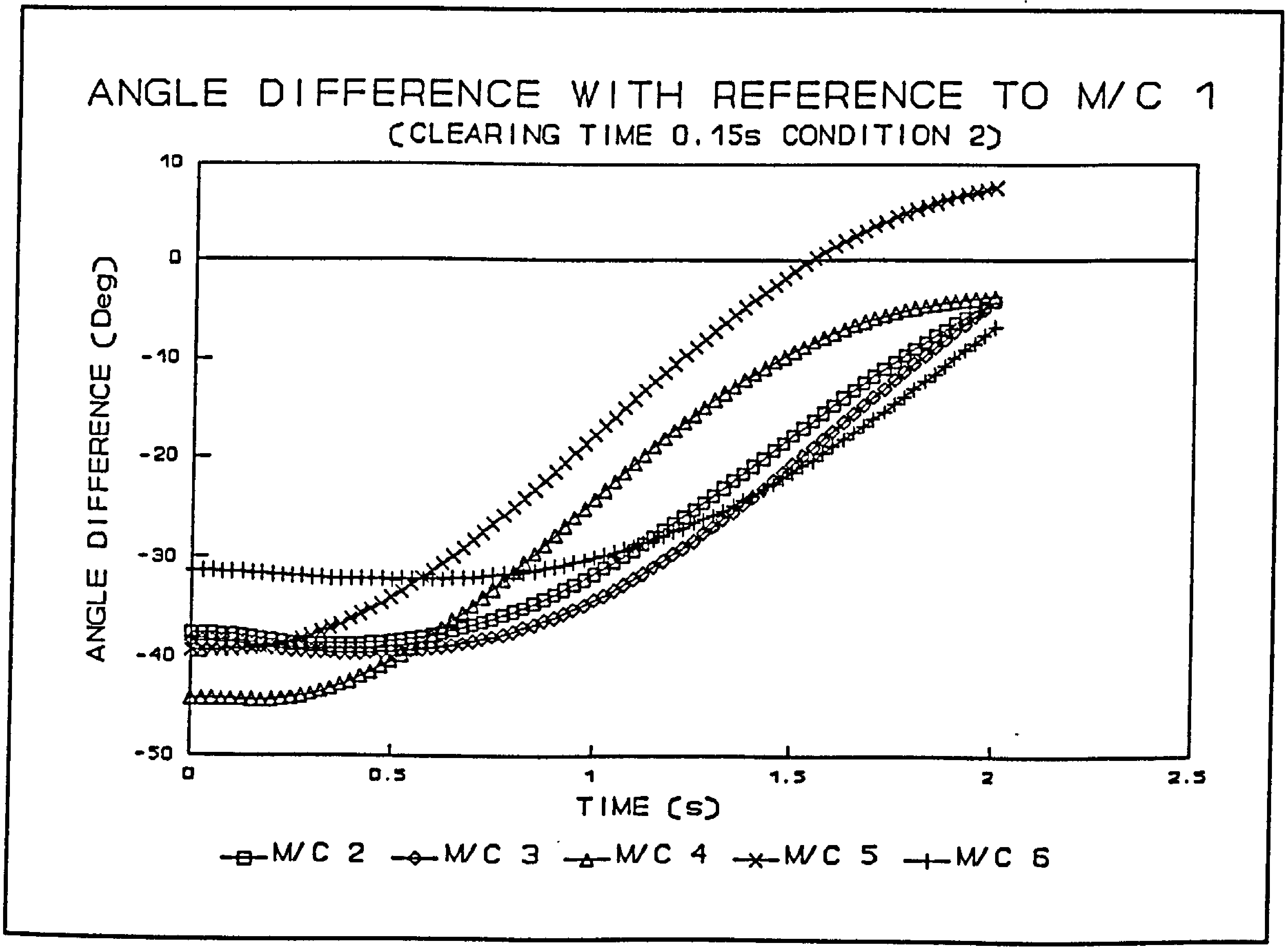
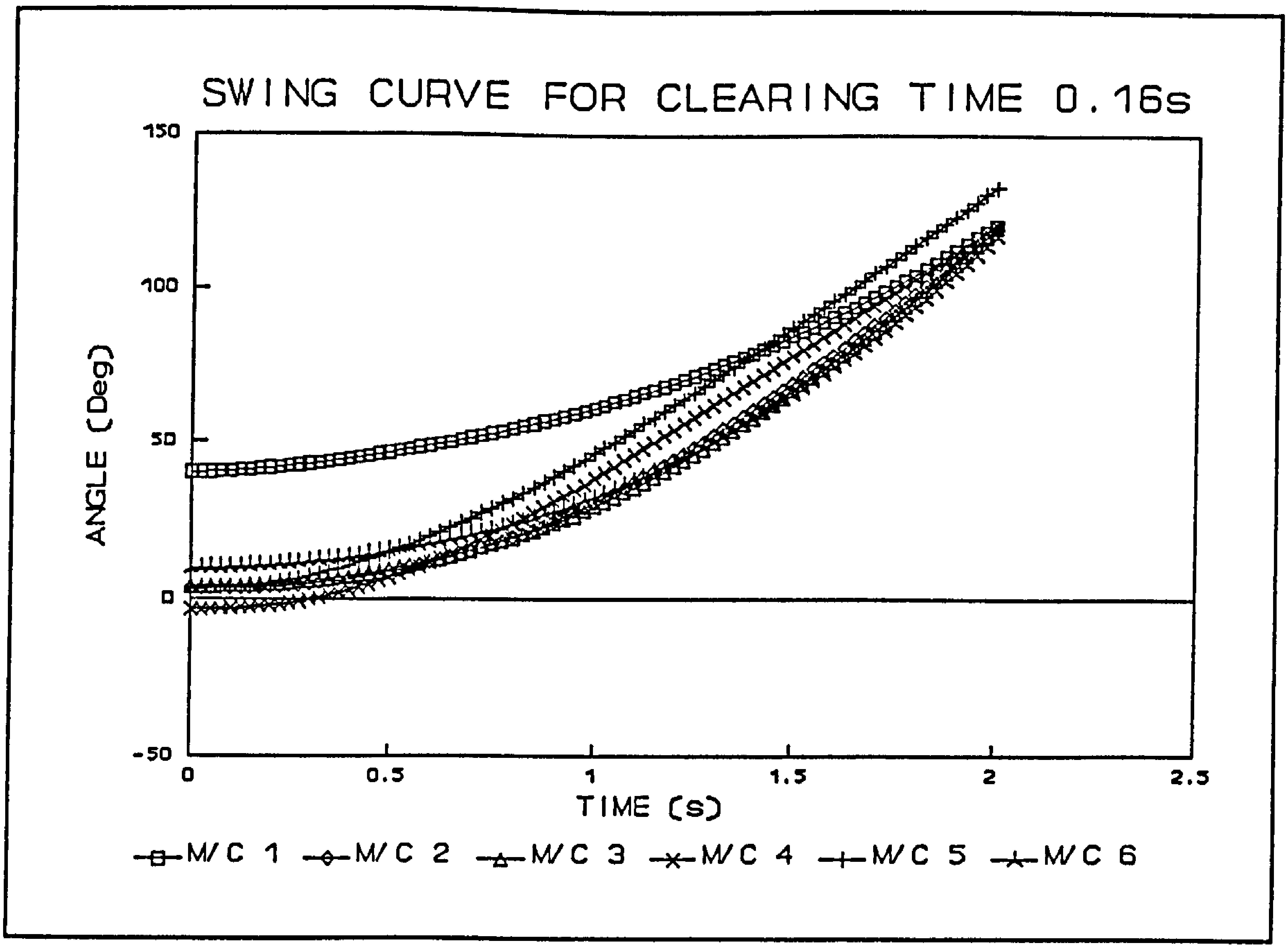

ANGLE DIFFERENCE WITH REFERENCE TO M/C 1
(CLEARING TIME 0.15s CONDITION 2)
ANGLE DIFFERENCE (Deg)
10
0
-10
-20
-30
-40
-50
TIME (s)
0
0.5
1
1.5
2
2.5
M/C 2
M/C 3
M/C 4
M/C 5
M/C 6

Fig.4-11


SWING CURVE FOR CLEARING TIME 0.16s
ANGLE (Deg)
150
100
50
0
-50
0
0.5
1
1.5
2
2.5
TIME (s)
M/C 1
M/C 2
M/C 3
M/C 4
M/C 5
M/C 6

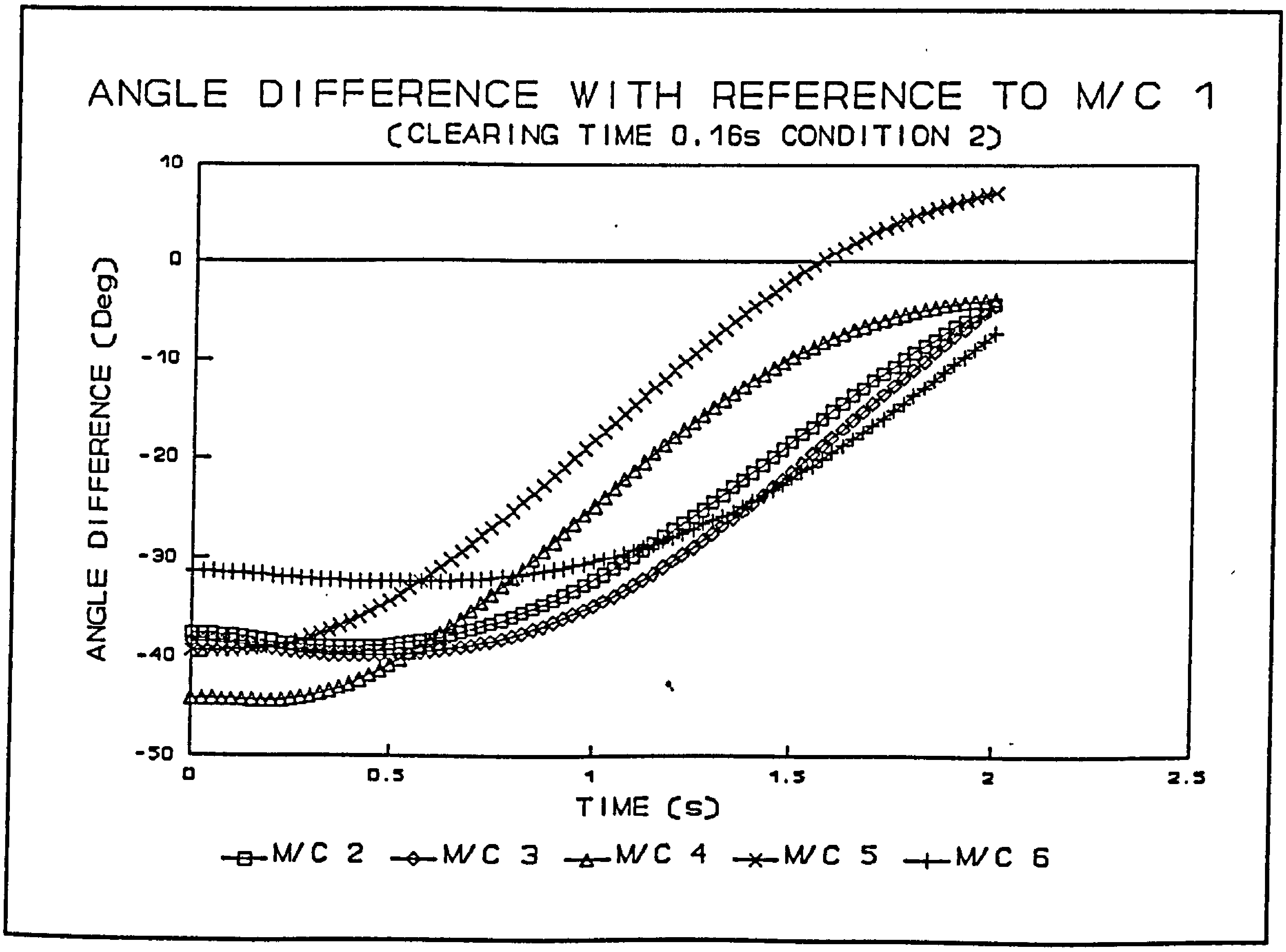
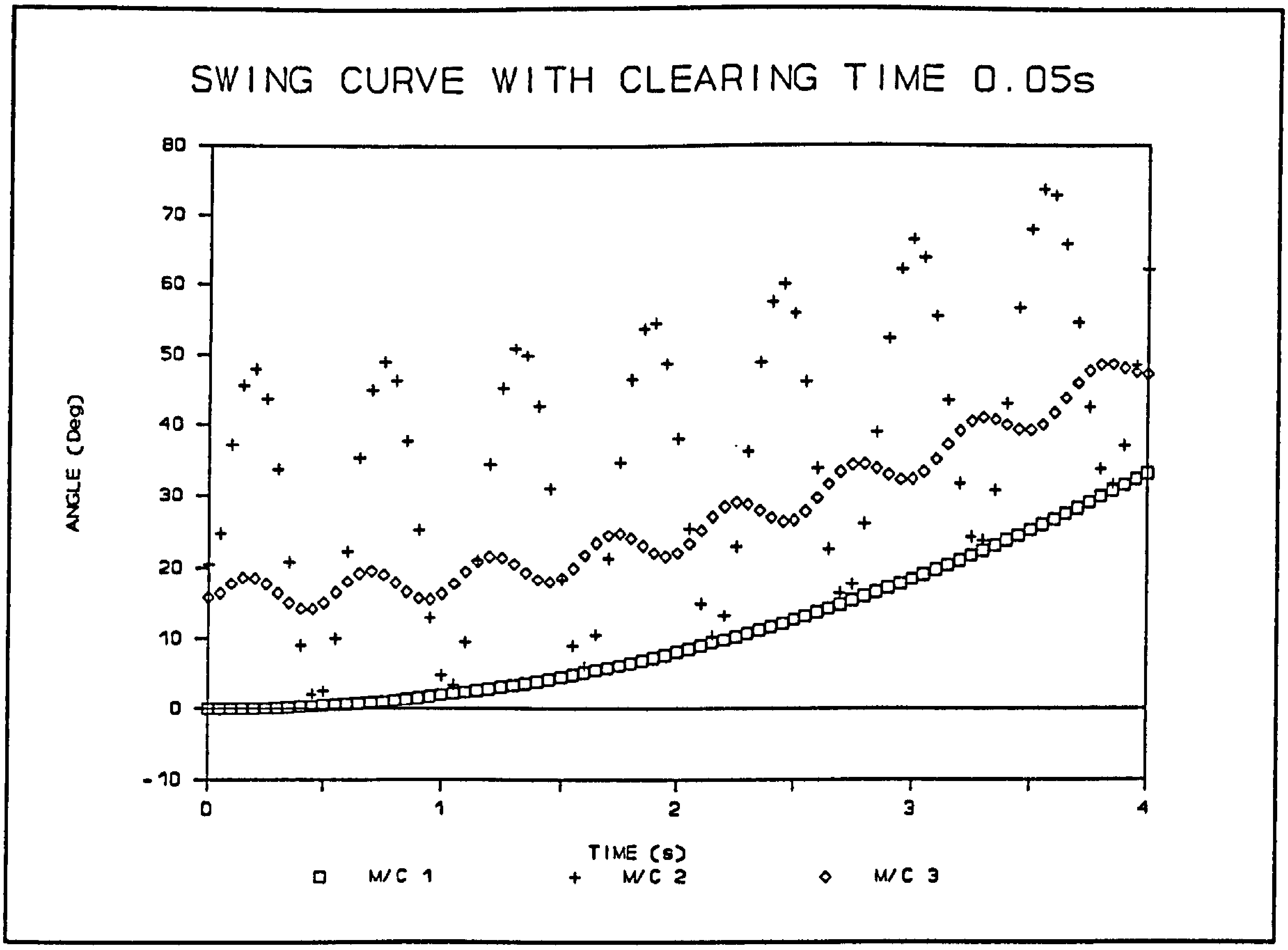

ANGLE DIFFERENCE WITH REFERENCE TO M/C 1
(CLEARING TIME 0.16s CONDITION 2)
ANGLE DIFFERENCE (Deg)
10
0
-10
-20
-30
-40
-50
0
0.5
1
1.5
2
2.5
TIME (s)
M/C 2
M/C 3
M/C 4
M/C 5
M/C 6

Fig.4-12


SWING CURVE WITH CLEARING TIME 0.05s
ANGLE (Deg)
80
70
60
50
40
30
20
10
0
-10
0
1
2
3
4
TIME (s)
□ M/C 1
+ M/C 2
◇ M/C 3

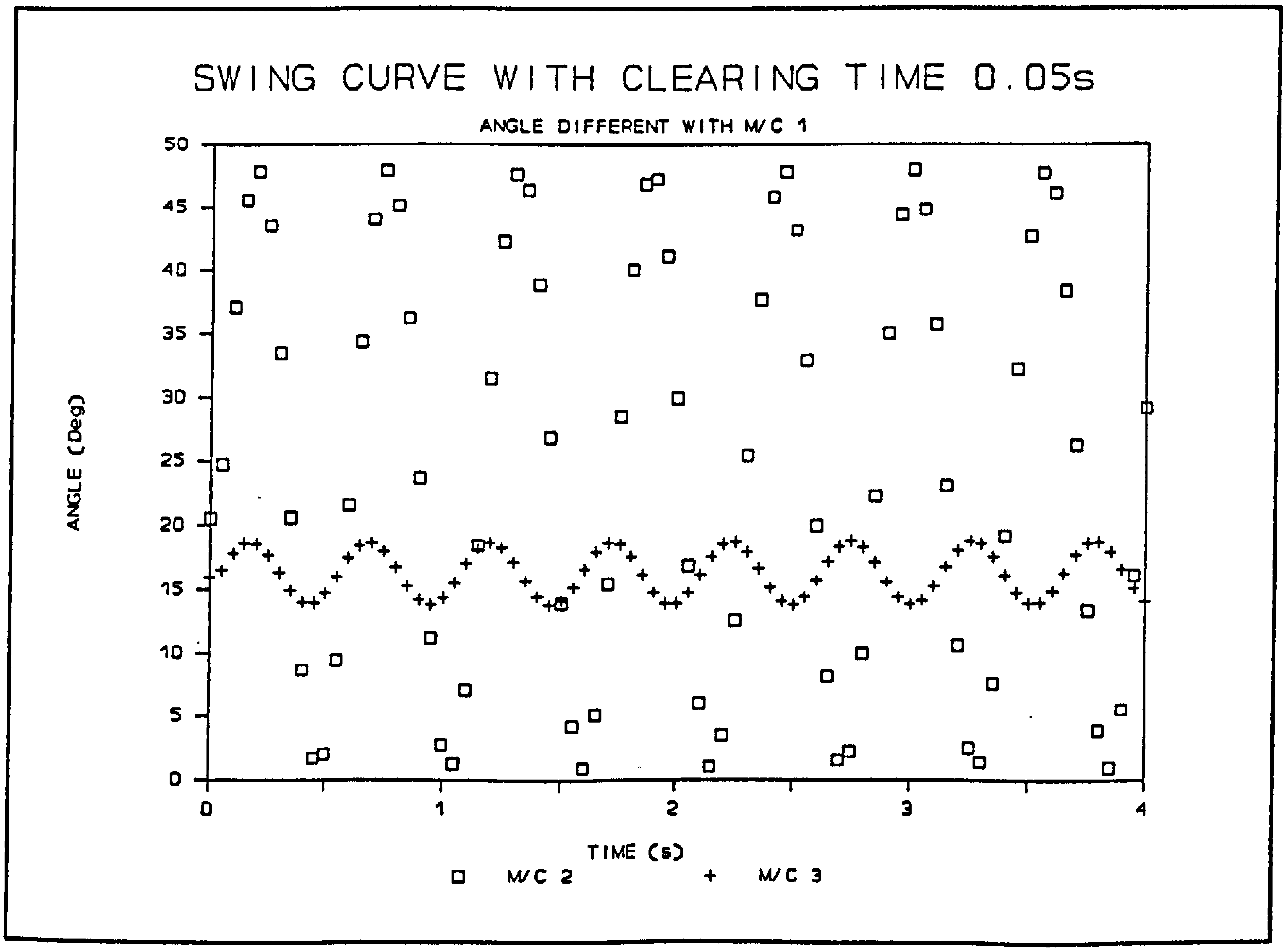
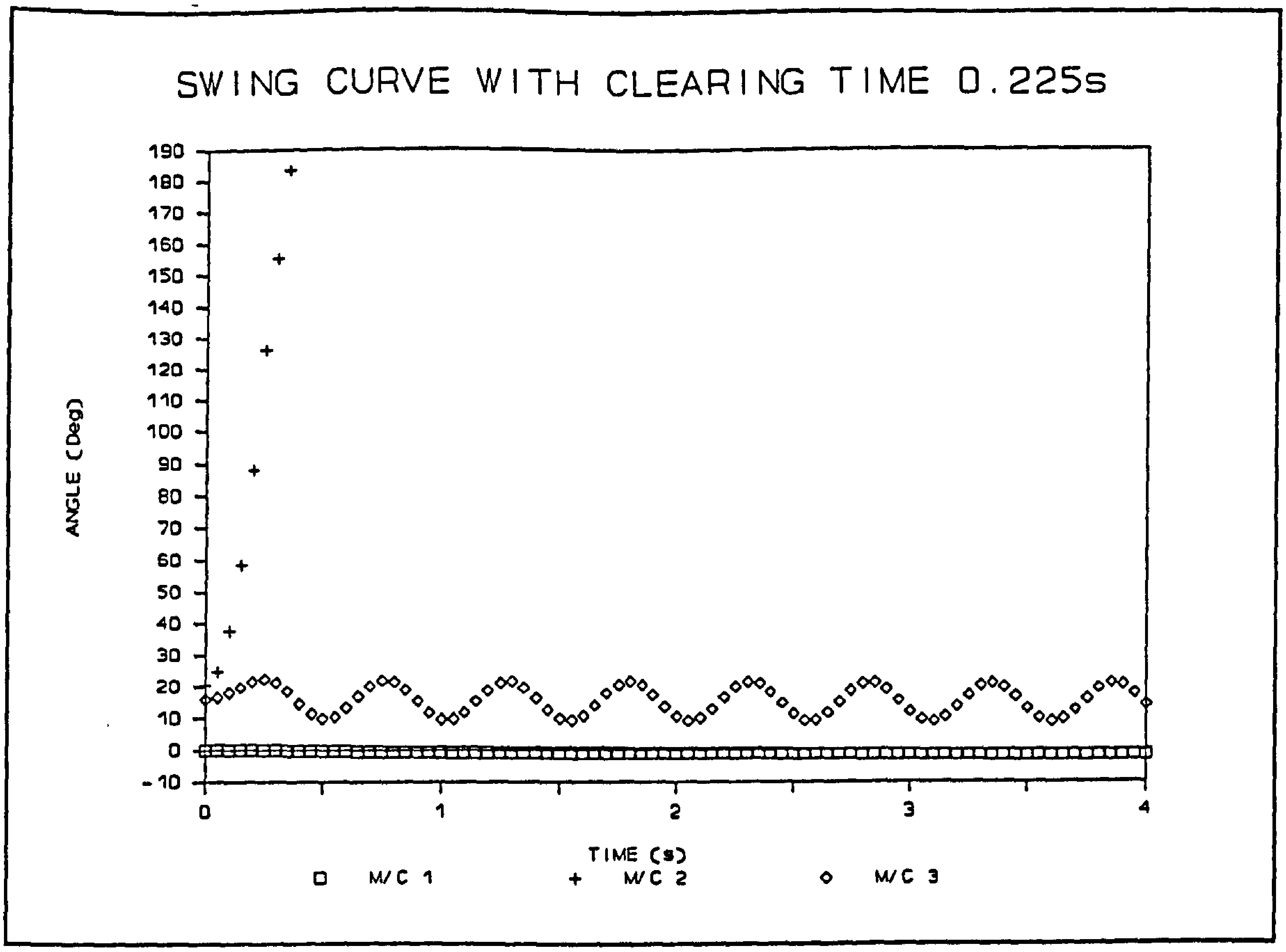
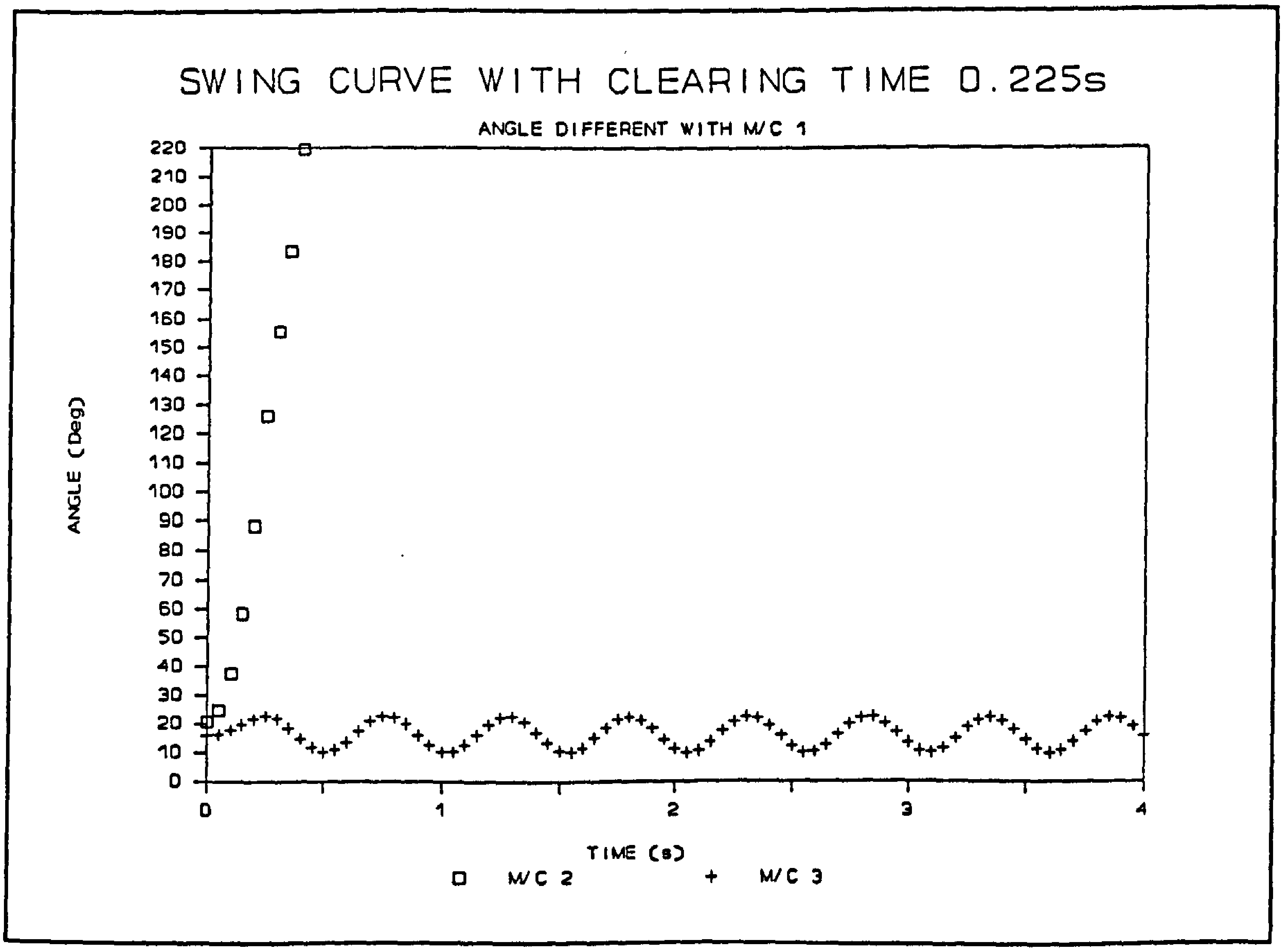

SWING CURVE WITH CLEARING TIME 0.05s
ANGLE DIFFERENT WITH M/C 1
ANGLE (Deg)
50
45
40
35
30
25
20
15
10
5
0
0
1
2
3
4
TIME (s)
□ M/C 2
+ M/C 3

Fig.4-13


SWING CURVE WITH CLEARING TIME 0.225s
ANGLE (Deg)
190
180
170
160
150
140
130
120
110
100
90
80
70
60
50
40
30
20
10
0
-10
0
1
2
3
4
TIME (s)
□ M/C 1
+ M/C 2
◇ M/C 3


SWING CURVE WITH CLEARING TIME 0.225s
ANGLE DIFFERENT WITH M/C 1
ANGLE (Deg)
220
210
200
190
180
170
160
150
140
130
120
110
100
90
80
70
60
50
40
30
20
10
0
0
1
2
3
4
TIME (s)
□ M/C 2
+ M/C 3

Chapter 5

A New Incorporated Dynamic Security and Static Security Limited Optimum Power Dispatch

5.1 General

This chapter would describe the development of the optimum power dispatch method that includes the consideration of both dynamic security and static security limits. This follows up from the investigation on fast, on-line dynamic security assessment method in the last chapter (Chapter 4) and the development of OPF technique in Chapter 3. Conventionally, static security and dynamic security are analysed separately due to their differences in modelling and solution methods. The consideration of static security limits in OPF programs has been reported .[1-4] In contrast, dynamic security limit associated with OPF operation has not been well studied mainly due to the traditional belief that dynamic security analysis usually demands excessively large amount of computing time.

In this context, transient stability assessment is the principal component in dynamic security. In many power utilities the normal practice is to perform detailed stability studies in the planning stage with detailed models in order to investigate the system's likely performance to those probable scenarios of disturbances. These studies would be taken to establish the operational limits of lines and machines through such repeated computer simulation of events. However, in actual on-line operations, the system loading conditions and parameters may be different from those assumed. Hence dynamic security constraints derived from post-fault loadflow analyses are insufficient to ensure true dynamic security. In order to provide a truely secure operation, an on-line dynamic security monitor is thus desirable. In this chapter, the rationale and proposed methodology for an integrated approach incorporating both dynamic security and static security limits in OPF are described and test results presented.

5.2 Dynamic and static security limits in OPF-a new approach

In the investigation, it is found that the current trend in security constrained OPF techniques only considers the post-contingency line current limits and neglects the possibility of loss of transient stability during the transition from the pre-contingency to the post-contingency state. This traditional approach suffers from the serious drawback that the dynamic contingency could endanger the stable operation of the system. In some literature, for example [20], it is suggested to express the dynamic security as preassigned limits of certain generator outputs via off-line simulations. But this approach would not work reliably, especially if we consider the cases of special loading conditions, such as high abnormal loads or unexpected outages already occurring in equipments. An adaptive scheme on-line to assess the current state's dynamic security should be introduced as an integrated module in OPF applications.

The economy and security of power system operation are normally two conflicting requirements. The normal practice is to operate the system to achieve maximum economy within acceptable security by considering security as a constraint in optimization. Static security constrained optimization using the total generation cost as the objective function and static security requirements as constraints have been formulated and solved by mathematical programming techniques. However, modern power systems are increasingly operated near to their critical stability limits and their danger of system collapse on certain credible dynamic contingency are causing increasing concern.

On the other hand, dynamic security assessment (DSA) on-line is now on the verge of practical implementation with the intensive research on fast direct methods of transient stability analysis. This chapter attempts to extend the above concept into a methodology that would consider dynamic security in OPF calculation in order to meet the need for such security control.

The proposed complete computational sequence consists of the following integrated modules :

a) Optimum Power Flow module
b) Dynamic Security Assessment
c) Preventive Control Calculation

In this chapter, the integration of the first two modules are described and the derivation of the third module on preventive control will be covered in the next chapter.

In order to ensure that the computation will be efficient and adaptive, the module

(a) on OPF is a static security limited OPF calculation as developed in chapter 3. This is then coupled to a dynamic security analysis module, as shown in Figure 5-1, to determine the dynamic security performance of the state of operation. In this DSA module, the dynamic equivalent reduction and fast determination of dynamic security margin such as the critical clearing time is used. The security assessment here is carried out for those dynamic contingencies which are considered to be essential to ensure that the system state is satisfactory. The selection of contingency list and the security margin will be available so that the actual level of dynamic security that the system can offer is at the discretion of the operator. Further to this concept, a preventive control loop may be designed to improve dynamic security should it be found to be unsatisfactory. This preventive control scheme will be discussed in the next chapter and in Figure 5-1 it is marked as an optional stage.

Associated with this design, it is essential to devise an analytical index to classify the degree of security. In the current literature several such indexes are being derived and the following discussion gives a comparison of their pros and cons in application.

5.3 Dynamic security margin and CCT

In the flowchart of Fig. 5-1, it is important to determine the dynamic security margin for a contingency. Usually, we are dealing with the situation of a fault occurring in a transmission line which is then detected and cleared by the protection system. For a certain fault clearing time, the question we usually ask is whether the system can remain stable after fault clearing, i.e. whether the generators can remain in synchronism. Traditional time domain numerical integration methods are only able to show transient stability with a yes or no answer with inspection of the swing curves. But in our case we require an analytical answer of the margin as an analytical clue to further control functions. Much new research work on direct transient stability analysis is centred on this issue and the fast dynamic equivalent method we use in this thesis can also provide a solution to this requirement.

Transient stability margin is an important concept for dynamic security assessment and in this context there are several possible proposals in the method used in this thesis. For a given fault and clearing time, the critical clearing time is an essential answer in transient stability analysis. In the the dynamic equivalent reduction method we propose, there are other quantities that can be adopted as security margin indicators. But they suffer from other drawbacks and they would be discussed in the next section. In the previous discussion, it is explained that the traditional method using swing curves calculation cannot give the required stability margin analytically. This is one of the main shortcomings of time domain solution. Before going into a more detailed discussion of the new technique used in this thesis, it is worthwhile to examine the traditional way of dealing with the problem. It is possible to run the load flow and the time simulation transient stability programs alternately. During the process, a correction is made for the mismatch in the predicted CCT and the relay settings; until a final set of proper operating conditions is obtained. This procedure is time consuming and too slow for real time applications.

In the dynamic reduction method we used, the following calculations have been performed and are useful here for the transient stability margin determination :

A) The critical machine is identified, and

B) The one machine to infinite busbar (OMIB) model has been determined.

In figure 5-2, which shows the power Vs angle curve of the system for pre-fault, during fault and post-fault conditions, the critical clearing angle and thus the critical clearing time are possible to be found for this equivalent system. At the critical clearing time the decelerating area (A_2) is just equal to the accelerating area (A_1) and the system is just able to retain synchronism. For fault clearing later than CCT the system will lose synchronism. So CCT is a practical index of how stable the system is. By comparing CCT with the system protection time setting, it is possible to find out if the system is able to retain stability after the disturbance. This classical definition is itself a conventional measure of the robustness of the system and a good security indicator.

Alternatively, the accelerating and decelerating areas are also functions of the energy involved during the transient. Since in our equivalent model, these areas can be found as by-products, it is possible to use them as security margin indexes. One proposal is to use either : $(A_2 - A_1)$ (5-1)

, or $(A_2 - A_1)/A_1$ (5-2)

as the margin indicator. This is because A_2 , the decelerating area is physically responsible for preventing the system from losing synchronism. A comparison of its value with A_1 which is the accelerating area gives an indicator of its stability performance.

In this thesis, the CCT value is chosen to be the transient stability index in dynamic security analysis module for the following reasons.

(1) As derived in the last chapter on dynamic security analysis, the CCT can be calculated with the dynamic equivalent reduction plus a fast procedure using algebraic expression of Taylor Series relating the critical clearing angle and CCT. This avoids the long integration and saves computer time.

(2) Other transient security margin in (5-1) and (5-2) requires calculation of the areas A_1 and A_2 by integration.

(3) Moreover, the CCT value is a well understood physical data in power system analysis, closely related to its robustness. By comparing the CCT value with the protection clearing time, one can easily establish whether system stability is at risk or not. By observing the margin between CCT and protection setting, the security margin may be monitored with ease.

(4) Excluding the critical machine from the aggregated COA model of the remaining machines is physically sound. Freezing all angles within the same group amounts to taking off the transient potential and kinetic energies that do not contribute to the separation in two subsets.

It is also relevant at this stage to discuss more on the significance of this dynamic reduction method. Besides offering a great potential to improve the much needed faster computing speed of transient stability in on-line operation, the method is also extremely suitable to assess security margin. One suggestion being investigated in the course of this research is the amount of critical machine's contribution to the instability margin. It is found that for a lot of operating conditions, the amount of generation from the critical machine is of dominating importance to decide on whether stability margin is maintained or not. This important observation is of much significance to the development of this research since, in the course of developing the dynamic equivalent, the critical machine is carefully identified already.

In the tests performed, it is also found that the CCT value thus calculated is not very sensitive to the distribution of the excess generation among other generation buses. Other factors such as increasing or decreasing loads and generation at other buses can in turn make comparatively smaller impact on the CCT value. By combining the observations with the extension of equal area criterion method will make the approach adopted in this thesis a valid and reliable approach to assess dynamic security level and to make corrective control action analysis in an on-line operating environment.

In the next section we can examine more on the CCT calculation step.

5.4 CCT Evaluation Method

In this section the calculation of Critical Clearing Time based on the dynamic equivalent reduction method derived in Chapter 4 is further discussed. In this context, we are assuming that in the on-line operating environment as encountered in this research objective, the first swing transient stability performance is required on a fast and sufficiently accurate basis. Within such operation, it is only necessary to consider the machine performance up to about 1 second after the disturbance has occurred. Hence it is acceptable to neglect the effects of automatic voltage regulators and governor controls.

The main objective is to assess the system's ability to retain transient stability should such disturbance suddenly occurs. Usually the system is equipped with automatic protection schemes that can react after a certain time delay due to relay operation and other factors. If the time needed to clear the fault is greater than the calculated CCT , the system will lose synchronism. By means of this on-line assessment to detect the possibility of this defect, some caution for adjusting system loads and generations aimed at increasing system stability margin is necessary. This is exactly the objective of our research but the consideration of economy of operation will also be considered at the same time so as to achieve the best compromise in security and economy of on-line operation.

It is derived that the most serious dynamic contingency for the identified critical machine in the dynamic equivalent reduction method is a solid three phase fault at its terminals followed by postfault line switching. The identified critical machine(s) would be the machine(s) responsible for system separation should the contingency occur.

Hence the following steps are used for the necessary critical machine identification followed by the system CCT calculation.

(i) For a n-machine power system, determine the initial acceleration of all the machines on the occurrence of fault. Filter out the most probable critical machine candidates by comparing their numerical values.

(ii) Compute in turn the critical clearing times (CCT) corresponding to each candidate machine. The machine that gives the smallest CCT is the most critical and its value gives the resultant system CCT.

In developing the method the classical model of an n-machine power system is used. Each generator is represented electrically as a constant voltage source behind its transient reactance and each load as a constant impedance. Besides the identified critical machine, the remaining (n-1) machines (assumed to be the set A) are modelled as an equivalent, aggregate, machine using the standard centre of angles (COA) concept [20].

Equivalent one-machine-infinite-bus model

The two machine equivalent is then further transformed to an equivalent one-machine infinite-busbar model for finding its CCT. The OMIB formulation is usd in conjunction with the equal area criterion to derive means for fast transient stability assessment. The computing speed of this module is relatively fast and gives acceptable results subject to several simplifying assumptions being valid, as discussed in the later section. In addition the computing time requirement will not increase drastically with increase in system bus size as a dynamic equivalent reduction is first performed, resulting in a simplified machine model. The calculation of CCT at this stage would be fast. This will be an advantage from the real-time computation requirement point of view.

An analytical relationship between a rotor angle and the corresponding fault clearing time is derived in Taylor Series form :

$$\delta_\tau = \delta_0 + \tfrac{1}{2}\gamma\tau^2 + (1/24)\gamma^{(2)}\tau^4 + (1/720)\gamma^{(4)}\tau^6 + \ldots\ldots \quad (5\text{-}1)$$

where δ_0 is the original steady-state rotor angle. The successive derivatives $\gamma^{(2)},\gamma^{(4)},\ldots,$ are obtained at after the fault inception. To get easy analytical expression of γ in terms of δ we will truncate the above expression after third right-hand side term.

In order to find out the suitability of the method, tests were performed with the following objectives.

1. Test cases are derived from the examples of the 30-bus system used in the last chapter. These test cases have already been investigated for their performance in optimum dispatch. Based on those results it is advantageous to investigate the dynamic security at those conditions of operation.
2. The operating conditions are also taken on several scenarios so as to investigate the effects due to changes in economy of operation.
3. In addition, the case studies are compared with numerical integration of swing curves to verify the accuracy of this approach.

In the course of investigation it is found that the identification of critical machine(s) is of prime significance to the success of this method. It will be demonstrated in the following section of test results that the accuracy is good for the correct identification of the critical machine which accounts for the losing of synchronisation. This observation has led to the refined procedure of identification applied in this thesis. Additionally, to further illustrate this point the swing curves results are also shown with both detailed system as well as with a reduced dynamic equivalent system in the following sections.

5.5 Simulation test results

The data of the 30-bus test power system are as given in the Appendix and are similar to those used in the last chapter for easy comparison. The test procedures are arranged in the the following sequence to investigate the efficiency and accuracy of the method. The test method is as shown in Figure 5-1 whereby the sample power system first goes through the static security constrained optimum power dispatch program and then the optimised results are inputed into our new dynamic security analysis program. The DSA program consists of the dynamic equivalent reduction and the extended equal area criterion method as developed in this chapter and the last chapter (Chapter 4). Hence the full output of this program will show the critical clearing time of the optimised system and thus whether the optimised system states will have satisfactory security performance or not. Since both static security and dynamic security performances have been tested, the optimised system state should be of satisfactory security level with reference to the new security level definition which is derived in this thesis.

To assess the accuracy of results, a comparison is also made with the detailed model system using step by step numerical integration of the classical machine swing equations. In summary the following general test procedures are applied.

With the base case of loading condition, the system's dynamic security is analysed using the dynamic equivalent reduction method and the Extended Equal Area Criterion approach. For the same load, the output setting of the critical generator is adjusted in several steps and the dynamic security analysis is repeated accordingly. The variation of other relevant parameters during the above step is also tabulated.

Test results of 30-bus system (System D)

The following shows the typical test results of the modified 30-bus network (i.e. System D). System datas of System D are the same as those used in last chapter so as to make comparation of test results more convenient and systematic. Referring to Table 4-6 and Table 4-7, which contain the test results of OPF and transient stability performance respectively, it is observed that the optimised system state at the typical loading condition has a system dynamic security performance of 0.1298 s critical clearing time for a three-phase fault at busbar 1 (on line 1-3).

Taking this condition as a typical operating state, the following system results are obtained by running the OPF and DSA programs. The OPF results are as shown in

Table 4-6 and the following details are as shown below.

Critical machine identified = Machine at bus number 11
Critical clearing time = 0.1298 s for fault at bus 1
P_G from critical machine = 1.045 p.u.
Total generation cost = 4041.193 p.u.

It is observed that the power generation of the critical machine (# 11) is at the maximum output limit of 1.045 p.u. Hence if we reduce the output limit of this critical machine, the system dynamic security should be improved at the sacrifice of higher operating cost. In order to observe how this change would affect the optimum operating condition, we set a new lower limit of 0.998 p.u. for the critical machine's power output (P_{G11}) and re-run the OPF program and the associated DSA program. A new set of optimised operating conditions is obtained with the following resulting conditions.

Critical machine identified = Machine at bus # 11
Critical clearing time = 0.140 s
P_G of critical machine = 0.998 p.u.
Total generation cost = 4060.989 p.u.

Comparing the two sets of results from the OPF and DSA programs, it is observed that the change of output limit of the critical machine has improved the dynamic security performance significantly. The following analysis shows the improvement.

CCT is improved from 0.1298 s to 0.14 s

(The percentage improvement in DS is about 8 %)

Cost is increased from 4041 pu to 4060.9 pu

(The percentage increase in cost is about 0.5 %)

The computing time requirements of the two programs in VAXCluster computer of Hong Kong Polytechnic is as shown in the following.

Running time of OPF module = 14.2 s (about 80 % of total)

Running time of DSA module = 3.6 s (about 20 % of total)

In general the test results are in line with the expected behaviour of stability limited power systems where the stability margin is affected significantly by the operating condition. As the load sharing of the critical generator decreases, the system stability margin improves but the operating cost would become higher, at a cost of security improvement.

The accuracy and reliability of the dynamic security assessment by the reduced dynamic equivalent model needs to be verified by comparing with a benchmark solution using the full system model solved by step by step numerical integration method. This is performed with the same system data as in the previous section of tests. In addition the swing curves are also solved for a two machine equivalent model which includes a) the critical machine and b) the aggregate of the rest of the machines acting as an equivalent machine. Instead of using dynamic equivalent reduction method of further reducing the system , the solution is now by numerical solution of swing equations of the two machines to find swing curves. The technique used is by repeated swing curves plotting to verify if the critical clearing time found in the reduced machine model is conforming to the full model or not. The test results show that the identified critical machine is the machine that would separate from the rest of the system when the critical clearing time is exceeded. One of the observations is that instability usually results from the weaker machine having a high loading level. The accuracy is good for all the cases studied shown when the critical machine is being correctly identified.

5.6 Conclusions

The work reported in this chapter is crucial to the development of the method used in this thesis since the success of a model that can predict the dynamic security performance with speed and reliability is very important. As discussed the choice and the investigations reported are favouring the dynamic equivalent reduction method with the extended equal area criterion technique as developed for the following main reasons summarised herewith.

1. The dynamic equivalent reduction gives a model which is both fast and sufficiently accurate to assess its dynamic security performance.
2. The method identifies the critical machine which is responsible for the loss of synchronism when separation occurs. This initiation of instability is clearly something we like to prevent from happening on the event of contingency.

Hence it gives the analytical clue to finding a preventive control strategy on the critical machine.

3. The dynamic security and its degree of margin could be evaluated by the method. This leads to the analytical solution of preventive control module in the next chapter.

4. The accuracy and reliability of the method is good when the correct identification of the critical machine is performed. For this reason an elaborate technique would be required for identification process in the application of this method. For stability limited system where the application of this method is to be made, the critical machine is likely to be easily identified even by heuristic techniques.

For the above reasons the method is chosen for this research project. In this application, it is clearly desirable to extend the method to include a preventive control module that can find suitable preventive control action should dynamic security limits are exceeded. This is the exactly the work that is to be reported in the next chapter. In addition the extension could bridge the gap for completing the closed loop of finding preventive dynamic security control in economic dispatch operation. Only by then would this research work constitute a complete application package in optimum and secure power system operation.

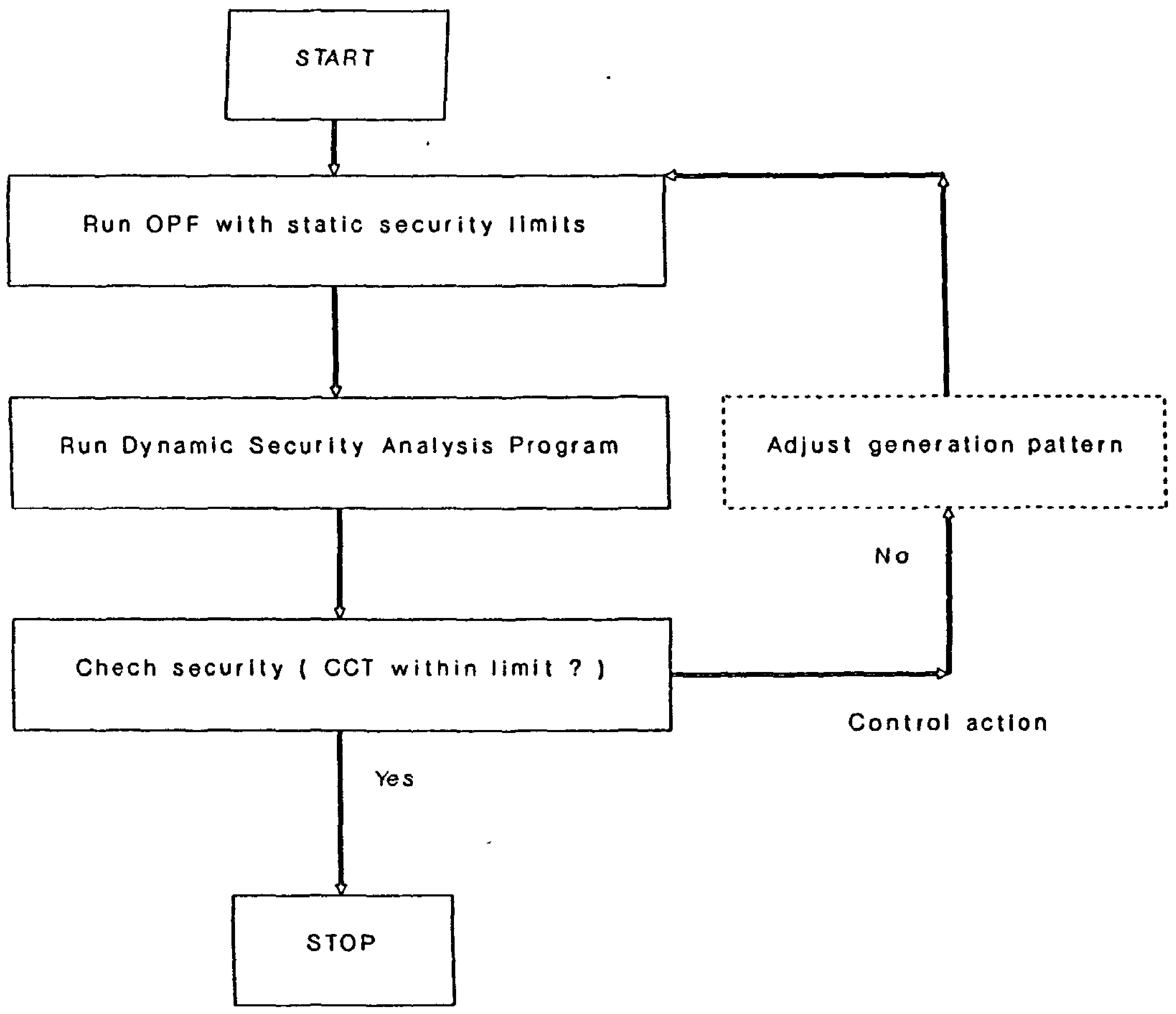


Fig.5-1 Flowchart of dynamic & static security limited OPF

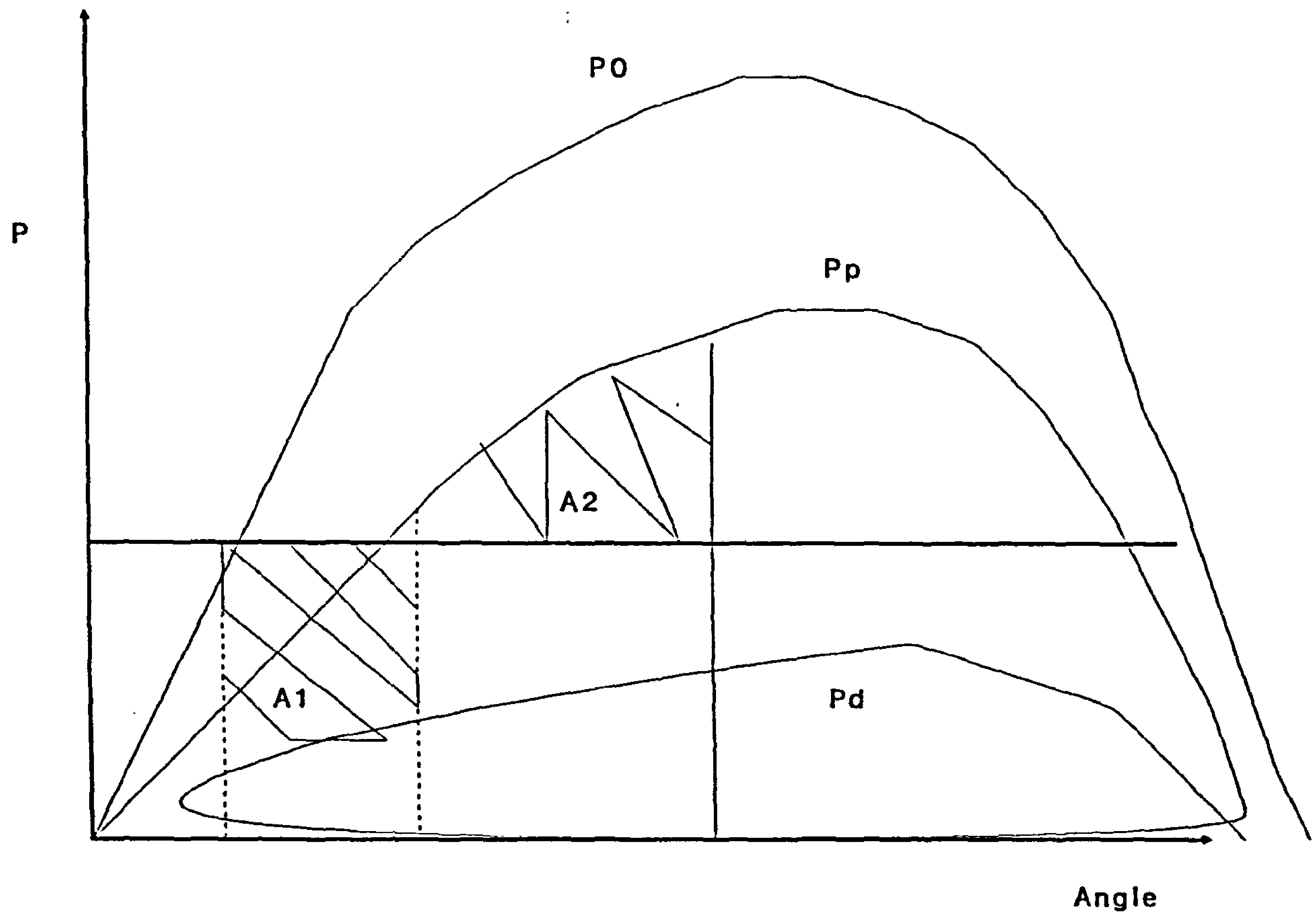


Fig.5-2 Power-angle curve illustrating equal area criterion

Chapter 6

Development of a Preventive Control Strategy For Secure Optimum Dispatch

6.1 General

This chapter describes how to incorporate the preventive control strategy for dynamic security control with the secure optimum power dispatch operation. The proposed algorithm incorporates the preventive control action to improve dynamic security performance should it be assessed to be unsatisfactory. A suitable assessment criterion is proposed for this assessment. Taking advantage of the identification of critical machine already being performed in the dynamic security assessment stage, the real power outputs of machines are adjusted to find the optimum solution of most economic operation that could satisfy the dynamic security limit of the system. Test of several typical power systems with various load data are performed to verify the validity of the new algorithm. Hence this chapter starts with a discussion on the role and overall strategy of the preventive control strategy for the proposed secure optimum dispatch methodology. This is followed by a description of the steps of solution and the implementation procedure of the algorithm. Test results showing the load tracking performance of a simulted system operation are shown to illustrate the scheme's applicability in real system operation.

6.2 Role and overall strategy of dynamic security preventive control

The main objective of the dynamic security preventive control module is to determine the best system reconfiguration that can give acceptable dynamic security and at the same time is at the most economic operation. In our design of the scheme this module is arranged as an external loop to the Optimum Power Flow (OPF) module. This approach is chosen for the following reasons.

a) The OPF module is maintained as a separate module to retain its efficiency and superior convergency property. In addition established OPF programs can be applied and used in conjunction with the methodology.

b) The preventive control module may be applied integrally or as add-on so that the dispatcher may regard the preventive control action of dynamic security being found as consultative. It may or may not be implemented depending on the technical judgement of the prevailing situation and the policy of the company.

c) As by-products of this calculation, the relative cost change, system CCT value change and the identification of critical machine(s) are available to the dispatcher.

Following this concept, we have experimented extensively with the example power systems by changing the limits of line flows, the power ouputs of generators etc to dynamic security. From our extensive test results we have found that the most effective parameters for this control are the real power outputs of the critical generators and the following points are also observed :

a) The relative effects of line flows limits on the dynamic security are much smaller than the real power generation changes in the systems we have tested.

b) In addition, the sensitivities of the security margin to the power outputs may also be computed analytically . [4]

c) In general , in an interconnected system, the critical generators that contribute to transient instability are those machines with more modern construction,i.e. they are of more efficient operating characteristic but are also of relatively smaller inertia constant (smaller weight to capacity ratio). This also makes the optimization result tending to load such machine more to their limit.

6.3 Steps and flow diagram

In this section, the main steps of the method are described with the aid of a flowchart (Figure 6-1). In a block diagram form the main steps include the three main modules of optimum power flow (OPF) program, dynamic security analysis (DSA) module and the preventive control module connected in a sequence as in Figure 6-1. The OPF module uses the Han-Powell method developed in Chapter 3 of this thesis and it will consider the static security limits of the line currents. This would ensure that the system will not have any violation of static security limits should the postulated contingency occur. This is the followed by the DSA module that uses the dynamic equivalent reduction method and the extended equal area criterion method to estimate its transient stability performance. If the transient stability performance is tested to be satisfactory, the system would be the most ideal answer , i.e. it is at the economic operating condition and satisfies the dynamic security and static security requirements.

The main concern here is what should be done when the transient stability performance test reveals that the system is not satisfactory. In that case our proposal is to determeine the required preventive control actions to make the system observe the dynamic security requirement. This is the main objective designed for the Preventive Control Module to be described in details in the next section.

It is obvious from the flowchart in Fig. 6-1 that the preventive control module is designed as a separate module from the OPF and DSA modules but it forms an important link between them. As derived in the last section, the control action has to depend on the results of the dynamic security analysis module. It is crucial to have correct informations on the critical machine and its stability margin. Hence the procedure for identifying the critical machine for a disturbance constitutes an important step in the solution. Its accurate solution would be vital to the success of the later steps. An elaborate and reliable scheme is required here. In the current literature, there are several criteria that have been applied, including the detection of the changes of those relevant variables such as velocity, accerleration, and phase angles etc. Several experimental tests have been done. The following refined method is chosen due to advantages of speed and accuracy.

The methodology is applied for a certain fault sequence occurring with the following steps :

(1) Calculate the initial accelerations for a list of the candidate critical machines. The initial accelerations of the machines immediately following the disturbance may be used to pre-filter the machines efficiently.

(2) Compute in turn the critical clearing times corresponding to each candidate machine applying the Extended Equal Area Criterion method which has been described in detail in the last chapter.

(3) The critical machine is identified as that giving the smallest CCT, which is considered to be the system CCT.

In practice, the filtering capbility of the initial accelerations criterion is reliable. Only a few machines would give the near values of largest accerlerations γ.

$\gamma_i = [\ P_{mi} - P_{ei}(\delta(t_0^+))]\ M_i^{-1}$

In the test cases there are usually 2 to 3 machines that are declared to be candidate machines. The step is very fast and is providing a speed-up step for the next stage of computing CCT of candidate machines. The final system CCT is thus derived efficiently.

6.4 Algorithm development for preventive control module

From the last section's discussions, it is obvious that the preventive control module incorporates an iterative algorithm to determine dynamic security changes when the system control parameters are adjusted. In this context, the strategy of reallocating the real power generations of machines is chosen. In order to achieve the objective of minimizing total generating cost within the acceptable security limit, a new set of power generations is to be found and used as the new inequality constraint limits in the static security limited OPF program. Since the operating conditions will be altered when the power generations of the critical machine(s) are changed, it is necessary to compute from the new load flow conditions the new security level.

An iterative algorithm for finding the dynamic security performance changes with different generation values will be required. It is both inaccurate and unreliable to obtain a realistic solution just by trial and error; instead, a systematic iteration algorithm for multi-variable nonlinear algebraic equations is to be applied to find the solution. In the project, a suitable numerical algorithm for repeated numerical adjustments at short continuous range of nonlinear variables [36] is applied in this module. An explanation of its application is described as follows. In principle, this algorithm extrapolates from some suitable initial assumed values,to obtain the best estimate of power generation that would give the required security level (critical clearing time in our case). For not excessive range of input values, the algorithm works satisfactorily since the derivation of this algorithm assumes that the nonlinear relationship between the input and output parameters must be continuous. Figure 6-2 shows the typical steps of iterations for the algorithm used.

In our case, the input is the P generation of critical machine and the output is the system CCT found by calling the fast transient stability subroutine used in the DSA module and the loadflow subroutine used in OPF/module. An illustrative explanation is contained here. The iterative function f(x) whose zero is sought must be continuous in the interval $[a_0,b_0]$. To ensure that the interval contains the zero, the criterion

$$f(a_0).\ f(b_0) < 0$$

must be satisfied. At each step, linear interpolation between the points is used to get a new point. In addition, the ordinate of a point staying in the range for more than one step is cut into half at each subsequent step. The endpoints of the interval containing the zero are chosen in the following way. After performing the dynamic security assessment module, if dynamic security is found to be not satisfactory, the Preventive Control Module is called for. The generated power of the critical machine is set as the upper point (b_0), and the other endpoint (a_0) is computed by subtracting the upper endpoint by a suitable constant in step until the condition

$$f(a_0).f(b_0) < 0$$

is satisfied. (Figure 6-2) From our tests it usually takes only a few steps (less than three steps) to find the satisfactory solution.

In the actual programming the solution of the critical clearing time is obtained in two steps. In the first step the critical clearing angle δ_c is an implicit function of P_G and the function f(x) is then that of equation (4-25). The approximated critical clearing angle is obtained by the modified false position method. The second step is to substitute the calculated δ_c into equation (4-22), which is now the f(x), to obtain the critical clearing time τ. Again the modified false position method is employed. Although in most tests, it is sufficient to use this model in the critical machine to approach a solution, it is also possible to extend the concept to other machines when either of the following cases are encountered. First, the limit of power output from the identified machine may be reached during iteration. Then the next weak machine should be controlled in sequence. Secondly, the relative sensitivity of other machines to security may be found to be of near magnitude which may justify a concerted control policy of more than one critical machines. One solution to this problem is to make use of their CCT (critical clearing time) values which have been computed in the previous step since their relative value is already an indication of their sensitivity to dynamic contingency concerned. Hence those more marginal cases can be solved with this technique.

6.5 Tests and results

6.5.1 Test Systems

Computer programs for the simulation tests are written in FORTRAN and run in the VAXCLUSTER computer in Hong Kong Polytechnic's Computer Centre. Two power systems, system A and system C used in this thesis, which are of small to medium size networks with typical stability limited characteristics and a large number of operating conditions have been used so as to cover a variety of configurations with realistic operating conditions.

They include the 5-bus test network A and the 30-bus modified sample system C whose system datas are listed in the Appendix. The disturbances considered are symmetrical 3-phase short-circuit faults at the generator terminals followed by fault clearing by line switching. A typical daily load curve is used as the test data to observe the parameter changes. A simulation of outages which might occur on the system is also tested.

In summary, the following types of simulations have been tested :

Type (i) A comparison of the OPF results before and after the DSA module is applied. This aims to highlight the change in the system parameters with respect to dynamic security enhancement. The parameters that are of interest include the total cost, security index(CCT of system), system losses, generator outputs etc.

Type (ii) Under the same loading condition, the system is solved for OPF performance when the value of the real power generation of the identified critical machine is varied. This aims to show the change of parameters with respect to power generation changes in a OPF program without a DSA module.

Type (iii) The system loading is now changed in steps according to daily load variation and the complete OPF with DSA is applied. This aims to demonstrate the applicability of this methodology and the system parameter changes with load.

Type (iv) Line outage(s) is simulated to have occurred and the system is operated at a stressed condition. This aims to show the vulnerability of the system security and the usefulness of this scheme with a more acute operating enviroment. The complete OPF with DSA is applied to show the variation of parameters.

Type (v) The outage of generator set(s) is simulated to consider the effects on security-economic operation. Unit commitment may be performed to pre-determine the taking out of certain less efficient generators at light load periods. Hence their effects on probable security implications are examined.

Simulation Results

A series of simulations are first performed for the 30-bus network by applying a 3-phase short circuit fault at the identified critical machine for testing its dynamic security. The OPF results are computed before and after the DSA module is applied to illustrate the differences. The main results are reported in Table 4.1 where the loads are chosen to vary so as to show both secure and insecure case. The security index may be arbitrarily fixed at a suitable value and is taken at 140 ms of system CCT in our case. In the cases shown, one or a maximum of two iterations of the outer loop of DSA is needed to reach a satisfactory solution. A small number of iterations are also needed for the preventive control module to work , typically two or three values are tried to reach the required value, in all the cases tested.

Table 6.1: OPF Results of 30-bus System before and after DSA is used

Parameter	Load 1		Load 2		Load 3	
	Before	After	Before	After	Before	After
Load (pu)	7.878	7.878	8.314	8.314	8.717	8.717
Initial cost (pu)	4830.5		5216.9		6218.9	
Optimised cost (pu)	4041.2	4055.6	4288.5	4298.0	4822.9	4844.3
CCT (ms)	133	141	132	141	114	141
Total P_{GEN} (pu)	8.298	8.307	8.60	8.605	9.099	9.129
Total P_{LOSS} (pu)	0.42	0.429	0.466	0.471	0.382	0.412
Total Q_{GEN} (pu)	3.029	3.048	3.328	3.34	3.558	3.611
Total Q_{LOSS} (pu)	1.767	1.786	1.932	1.944	1.792	1.845
Gen. #11 P_{GEN} (pu)	1.045	1.007	1.034	1.024	1.20	1.049

Figure 6-3 shows the OPF results for both cases of with and without the application of DSA module, for a wide variation of loads in the network. It shows the variation of parameters in a large range of load changes including light load and heavy load. If the dynamic security index is violated then DSA module is called for to rectify the security.

Figure 6-4 shows the OPF results for a typical fixed load and the real power output of the identified critical machine (generator 11 in this case) is varied to illustrate its effects on parameters. In particular the cost and security variation are of interest. For the 5-bus test network, similar systematic tests are also carried out and their results are of similar ranges to the above.

A further series of tests are performed for the 30-bus network with the stressed operating conditions of post-fault line outages already carried out. In Table 6.2 we have summaried illustrative results for a single line outage condition (i.e. line 16-17 has been switched out). The relative increase in operating cost and the worse situation of dynamic security are noteworthy . The typical computer running times of each module in VAX computer are listed in Table 6.3.

Table 6.2 : OPF results for one line outage before and after DSA application

Parameter	One line out case	One line out case	Base case (no line out)	Base case (no line out)
	Before	After	Before	After
Load (pu)	7.878	7.878	7.878	7.878
Initial cost (pu)	4849.4		4830.5	
Optimised cost (pu)	4053.4	4082.2	4041.2	4055.6
CCT (ms)	126	140	133	141
Total P_{GEN} (pu)	8.313	8.331	8.298	8.307
Total P_{LOSS} (pu)	0.435	0.453	0.420	0.429
Total Q_{GEN} (pu)	3.114	3.156	3.029	3.048
Total Q_{LOSS} (pu)	1.852	1.894	1.767	1.786
Critical m/c P_G (pu)	1.044	0.973	1.045	1.007

Table 6.3 : Typical computer time for solving 30-Bus system.

Module	*Time (s)*	*% of total time*
OPF module	*14.2*	*49.3*
DSA module	*3.6*	*12.5*
Preventive control	*11.0*	*38.2*

In the case of simulating generator outages, the results show that dynamic security are also affected by the outage but the effect does not show a definite clear proportional relation and is rather irregular. It is however clear that there is a higher possibility for insecurity to occur when the outage results in other weak generators having to take up a higher proportion of load. On the other hand, if the loading sharing does not significantly increase this effect, the change in CCT may not be large and may even be of opposite effect. This result, however, demonstrates that dynamic security consideration may not be as easily predictable and further justifies the need for on- line dynamic security monitoring of the operating state of the power system.

6.5.2 Load tracking tests

In order to further test the applicability of the proposed methodolgy, the test is extended to the 30-bus test system subjected to a simulated daily load variation. The load curve used is a typical load curve as shown in Figure 6-5 for a 24 hour typical day of the system. The system is calculated on a hourly basis the optimum power dispatch result to meet the load changes during the typical day. The main reasons for performing this test may be summarised as follows.

(1) The simulation aims to find out the cost and security variations both when the dynamic security preventive control is applied or not.

(2) As a comparison, it is possible to determine the effects of load and generation changes on the security operation and thus the merits of applying this preventive control scheme in practice. Both the cost differences and the improvement in security indices (in this case the CCT of the system) are obtained to demonstrate these effects.

Using the OPF program and the security limited OPF scheme developed in this project, the operation results of the system for 24 hours are plotted out in Fig. 6-6 and 6-7. Figure 6-6 shows the operating costs of the system both with and without the application of dynamic security control. Figure 6-7 shows the dynamic security index (the system CCT) variation for the same daily load curve as in Figure 6-6 and should be read in conjunction with the curves.

6.5.3 Discussions on results

From the analysis of the series of test results, the following observations are summarised.

(i) The DSA module works satisfactorily in our test cases based on small to medium size systems. It provides a suitable assessment and thus provide prior warning to operator of possible dynamic insecurity in the operating state. This is certainly the case with system that has high loads and weak generator(s) which is (are) prone to instability.

(ii) The preventive action found by our methodology helps to alleviate the problem but it also results in relatively higher operating cost. This is in line with the philosophy of a compromise between cost and security of operation.

(iii) There are clear indications that dynamic security of the operating state is affected by a large number of factors , mainly the loading of generators, the loading of lines and their proximty to maximum limits, and the load pattern etc. It is not always possible to predict its dynamic security performance in extreme operating conditions and a on-line security assessment scheme embedded in operation software would be a justified need. This observation supports the proposal of the scheme to include dynamic security monitoring and preventive control action analysis in this thesis.

(iv) In the daily load variation operation simulation results it is obvious that the methodolgy may work for continuous operation in a control centre to assist the power system operator to make justified decisions to prevent dynamic security form reaching dangerous levels while at the same time being able to maintain an economic dispatch operation. The cost effects are shown to be not excessive while the advantages gained by preventing dynamic insecurity to happen may be extremely important.

6.6 CONCLUSIONS

A new method to include on-line dynamic security assessment and preventive control in economic dispatch operation of power system is presented in this chapter. The tests showed promising results especially for systems with stability limitations. In summary the methodology possesses the following innovative features.

(i) The formulation extends the conventional static security constrained OPF programs to include the consideration of the dynamic security level of the on-line states.

(ii) A dynamic security monitor and a preventive control module are introduced to form a complete static and dynamic security constrained OPF scheme.

(iii) The concept of security in power system operation is expanded to include dynamic contingency prevention that could lead to a complete system collapse.

It is proposed that the approach is applicable to stability limited power systems and simulation results from small to medium size networks are confirming the arguments. Moreover, the implementation of such a security control methodology would be useful to the enhancement of power system security for on-line operation. In particular, the methodolgy appears to provide an additional tool in avoiding the system from reaching an insecure state with possible catastrophic contingency to take place and without the prior assessment of such danger being detected. In conclusion the formulation proposed is providing a step forward in the secure and economic on-line operation of power system.

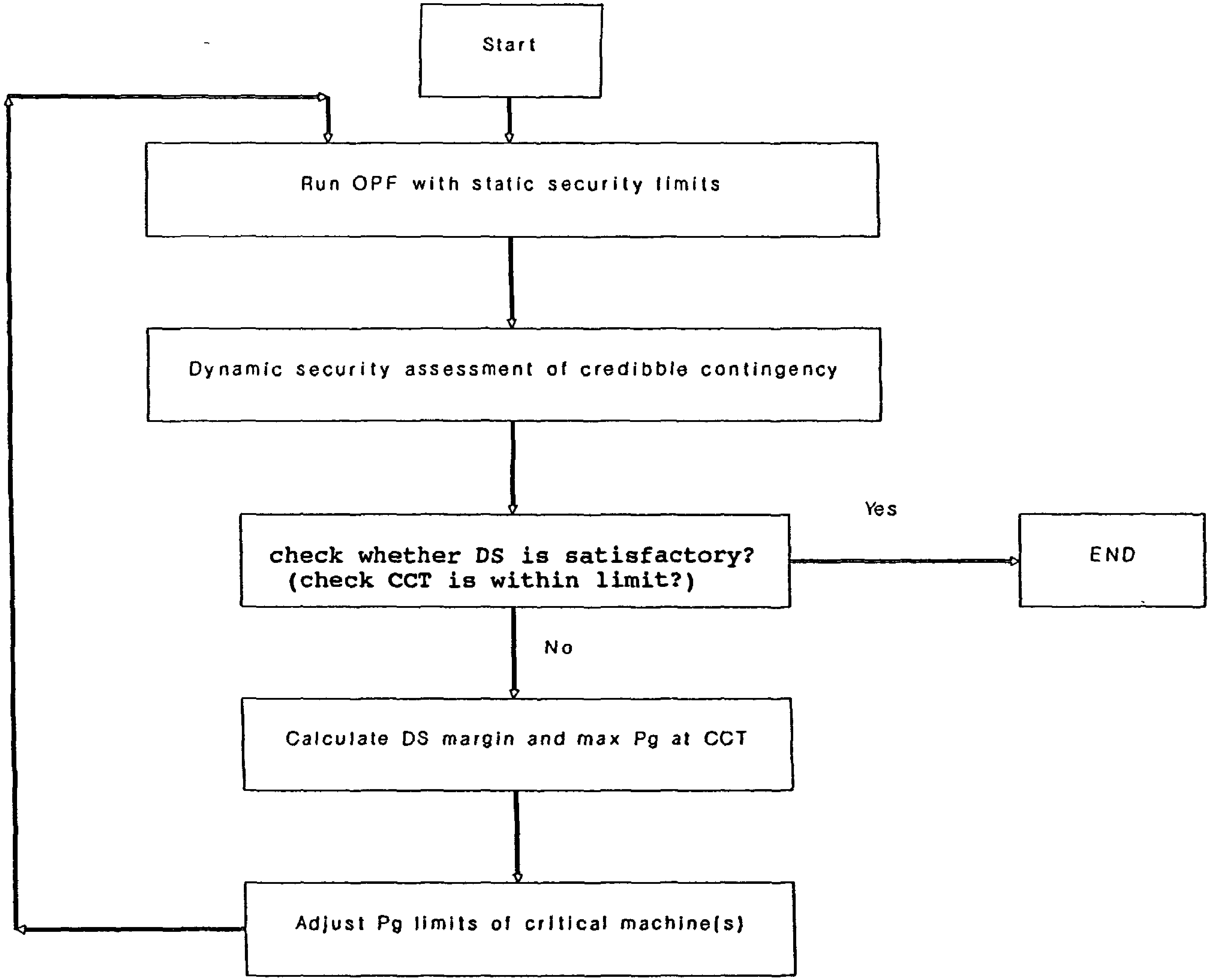


Fig.6-1 Flowchart of complete SCOPF with DS control added

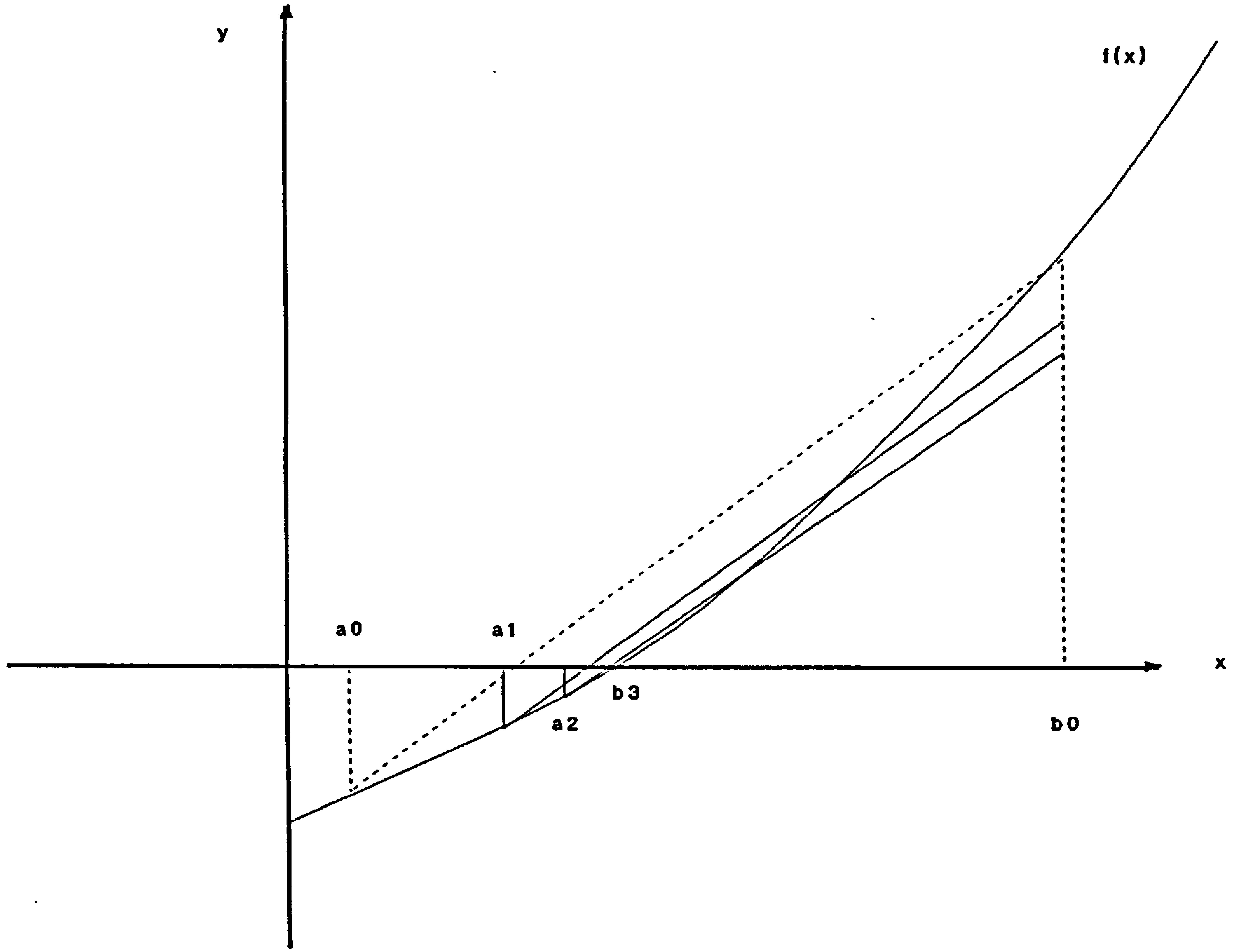
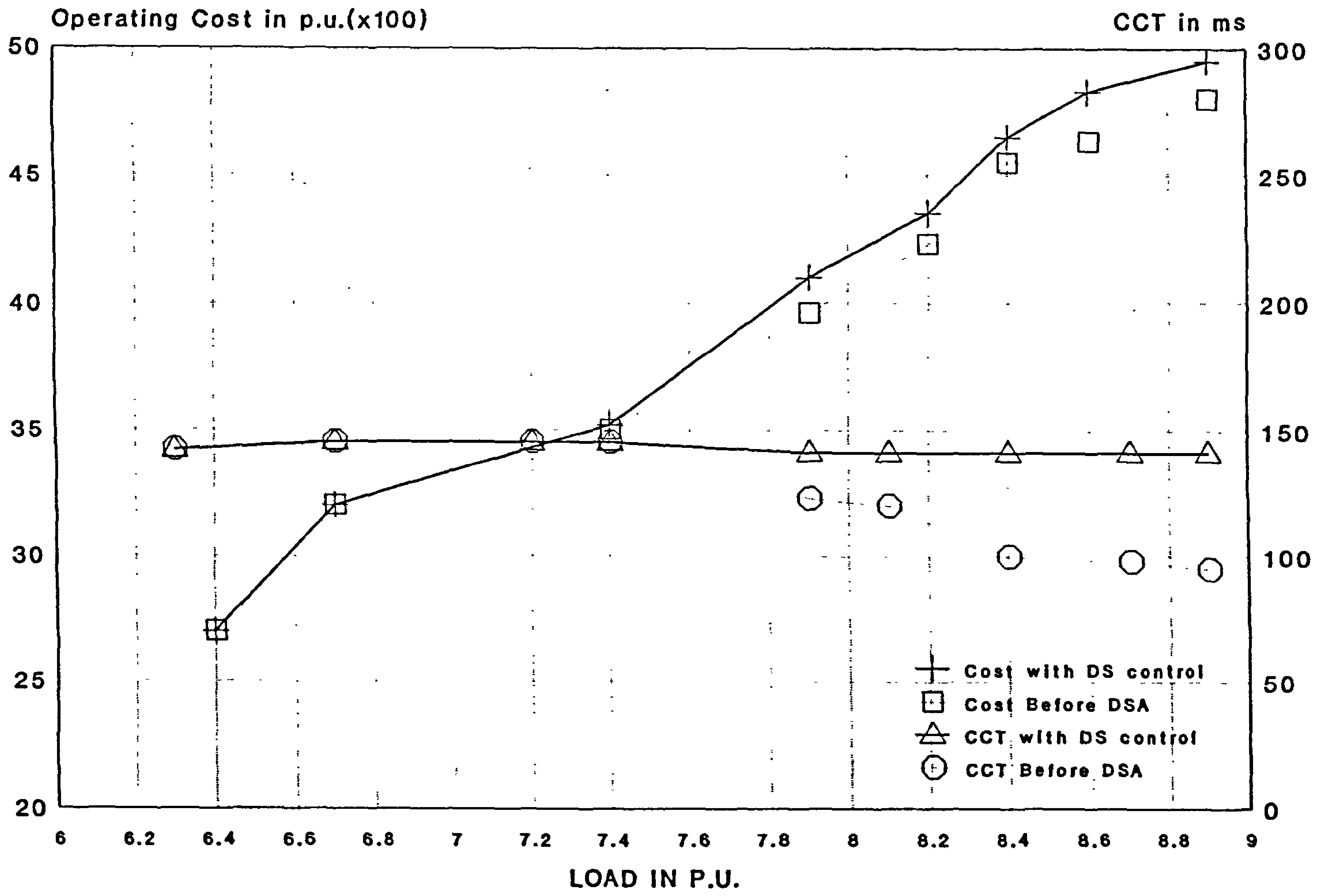


Fig.6-2 Algoritm for finding Pgen within DS limit

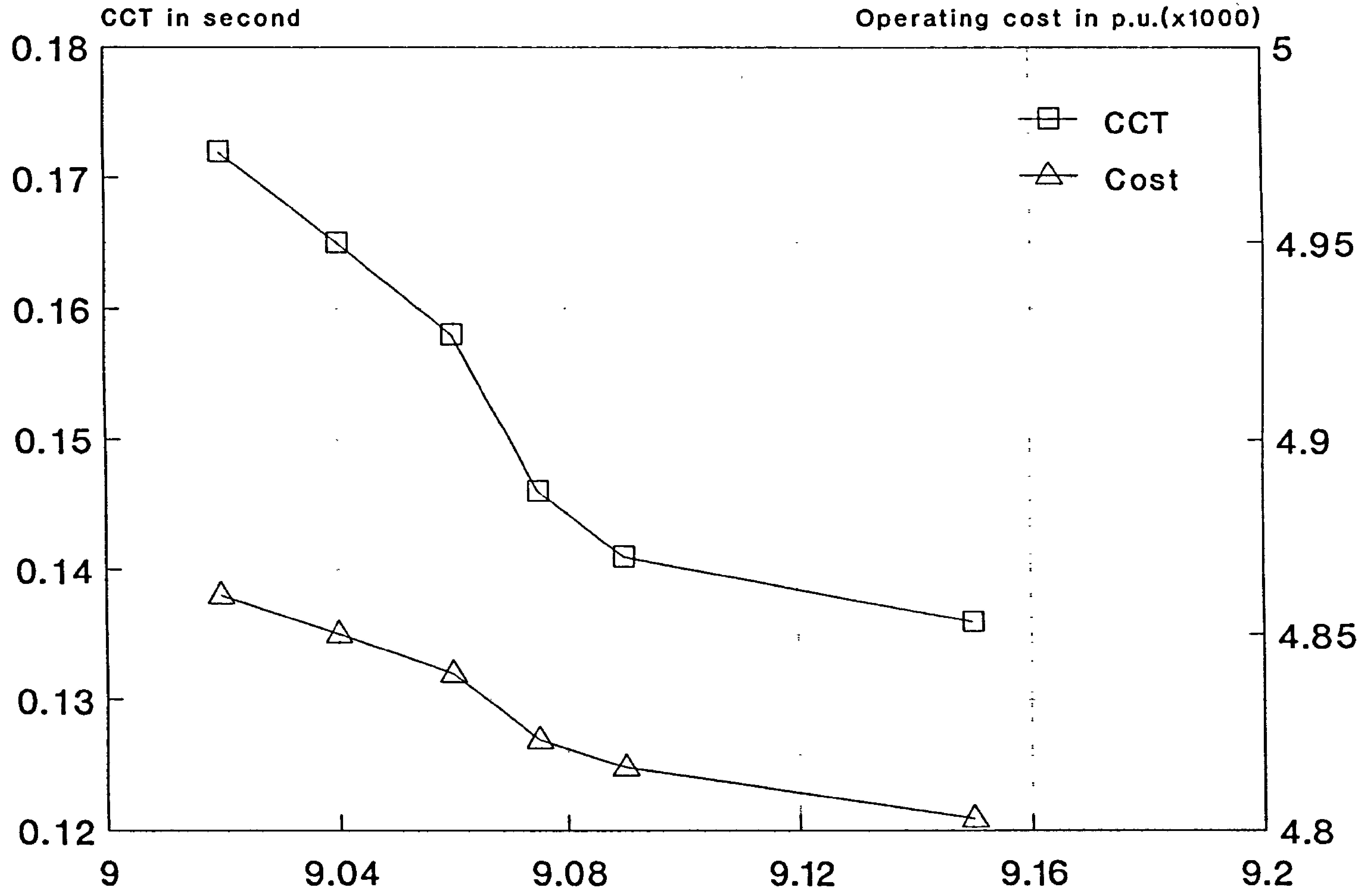
Fig 6-3 OPF results with DS control
(30-bus system)



(Compare results with & without DS cont)

Fig 6-4 Compare OPF results at base load

(30 bus system)



(compare OPF results as Pg is changed)

Fig.6-5 A Typical Daily Load Test Curve

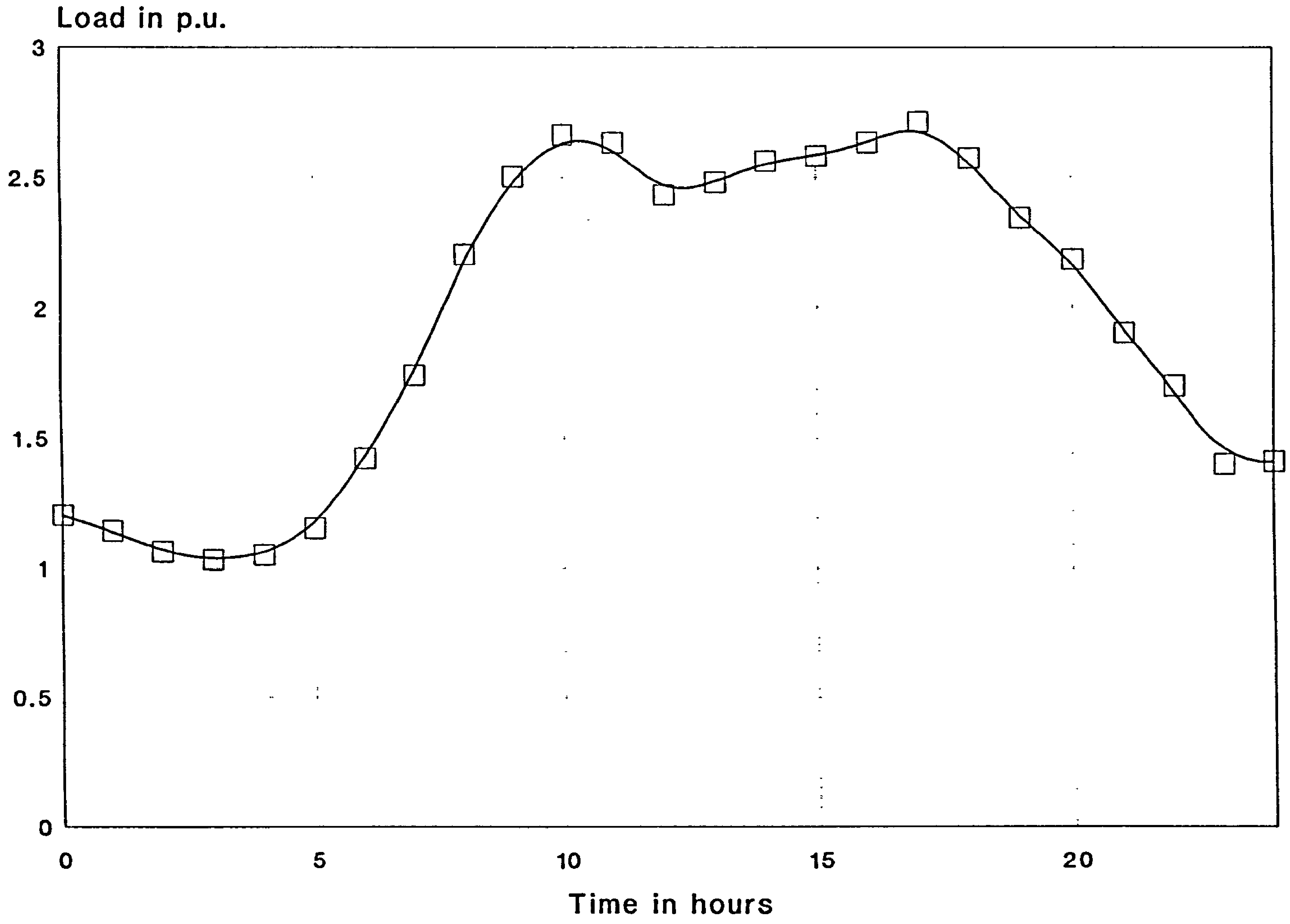
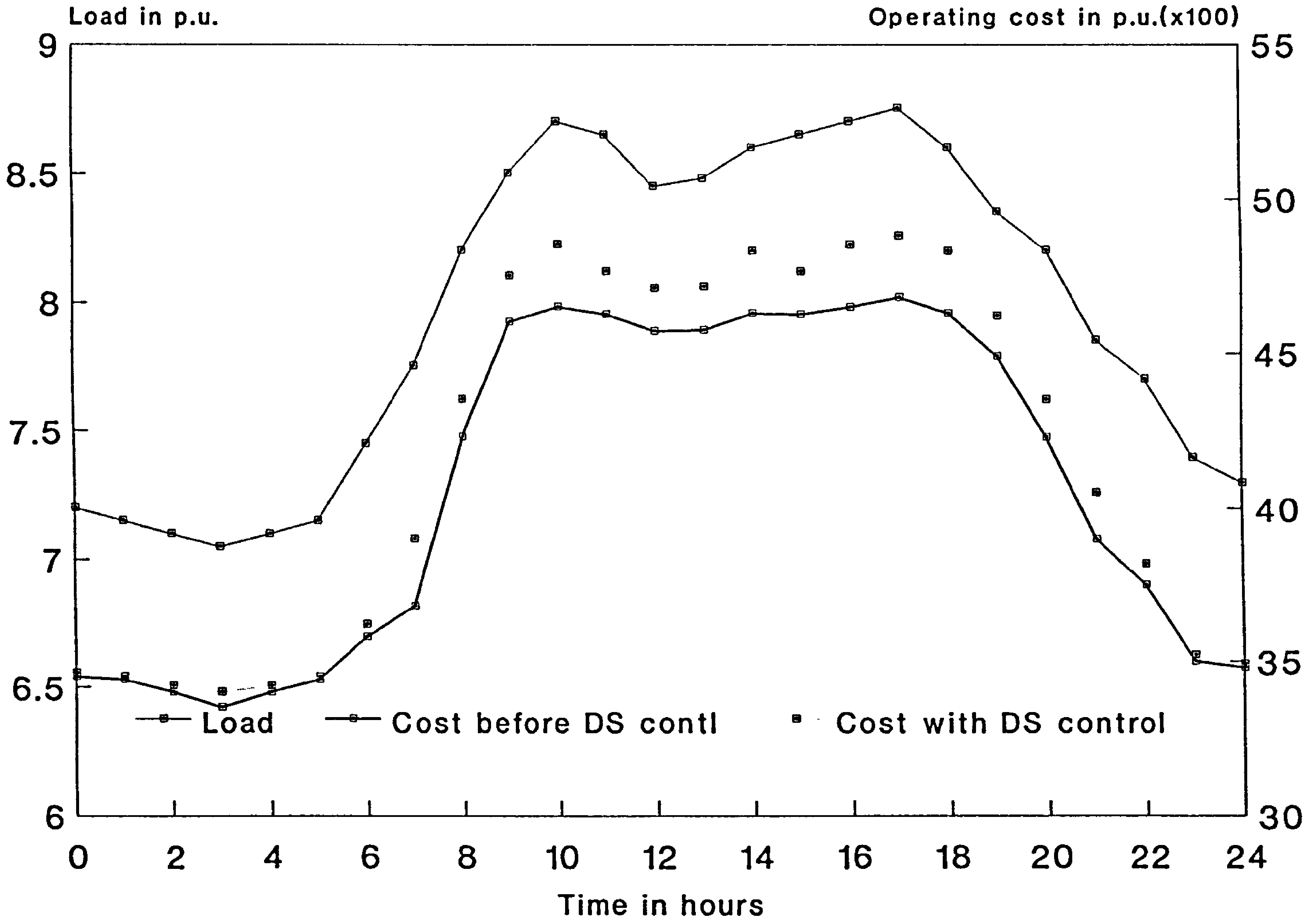
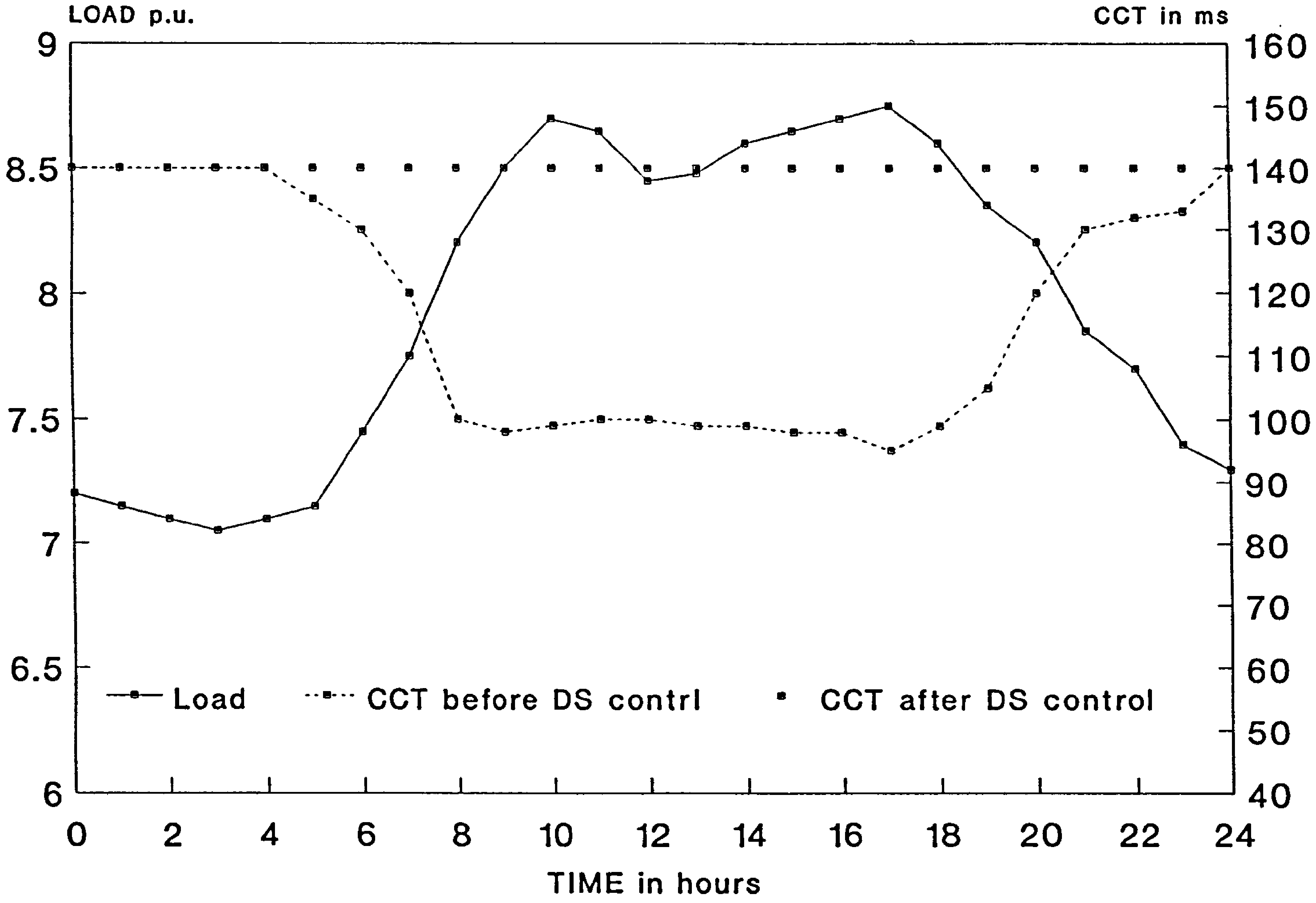


Fig.6-6 OPF Load Tracking Simulation
(30 bus system)



Compare costs with & without DS control

Fig.6-7 OPF Load Tracking Simulation
(30 bus system at typical daily load)



Compare CCT with & without DS control

Chapter 7

Conclusions and Suggestions for Future Work

In the computerised operation of large power system, the considerations of security and economy are of prime concern. In this thesis we have presented a new co-ordinated approach to analyse and consider system security and economy in real time power system operation. The approach is conceptually different from the existing conventional methods that make separate analysis of the two; and it represents a breakthrough in the conventional concept by linking up the two concepts of security and economy together in a rigorous mathematical modelling approach.

In the theory and test examples that were presented, it is shown that security and economy are two concepts that are interrelated and it would be desirable to make due considerations of them together in power system operations. On one hand, economy of operation has been studied through the conventional methods of Economic Dispatch and Optimum Power Flow in many papers. In the existing papers, some authors are aware of the need to consider maximum loading limits of power equipments and due checking of them are made during the optimization calculations; others however neglect these limits and make approximations (those earlier methods such as B-coefficients methods are of this category) on the basis of achieving fast computation speed at the expense of accuracy. This need was highlighted by the development of static security concept when Dy Liacco first proposed the new approach in Control Centre design in the early Seventies. Static security as defined, however, only checks for the adequacy of capacity when a selected contingency has occurred. No possible guarantee or prediction has been made on the dynamic security performance (i.e. transient stability) during the change of state, i.e. from the pre-contingency to the post-contingency state. This has found to be unsatisfactory in our analysis as this transient change of state could be the key factor to determine whether the system can maintain secure operation or not; if not it would mean a system breakdown or disintegration which may lead to collapse of system operation. But the analysis of such dynamic security of operation was beyond the capability of those real-time computers in the Sixties and the early Seventies when power system security concept was first proposed. However, as early pioneers in the field had indicated that the future need of including dynamic security checking in security operation will be a future worthwhile research topic.

The recent advances in the research on fast transient stability analysis has made this ideal become more near to practicality. In this work a survey has been made on the recent advances in this area. From the survey it is clear that the need to assess dynamic security is becoming critical in modern power system operation with the following contributing reasons.

1. Heavier use of existing transmission and distribution lines due to energy conservation and availability of remote energy sources.
2. Fewer transmission lines are being built due to right-of-way restrictions, regulatory restrictions and capital costs.

3. Power generation trends that affect stability adversely, including increased unit sizes, and lower inertia constants.

Model tests were extensively performed on choosing the suitability of dynamic security assessment application in linking with OPF models. The studies lead to the development in this thesis of a new integrated approach incorporating both static and dynamic security limits in Optimum Dispatch as a major step forward towards the secure and optimal operational goal of power system operation.

The other significant contribution of this approach is based on the revised definition of security concept in power system operation. The need to include a review of static and dynamic security in optimum operation constitutes a way of looking at security on its relation to cost of operation. A new definition of security cost is suggested to be a possible effective measure of security enhancement. As an example, power system operators may be presented with the informations on system security perfomance and the associated security cost for preventive action in order to enhance the knowledge on decision making.

The exact relation between static and dynamic security performance has always been complicated. Hence researchers have been used to tackle them separately with techniques that bear very little relation to each other. In this thesis we have made attempt to treat them systematically. The probable contingency list is located first, followed by the static security constrained optimization and then the dynamic security calculation based on the same identified contingency. The new approach improves the coherency of the system performance prediction especially when a key contingency list could be identified and the system is expected to be protected against such a key contingency. For real systems in operation this is deemed to be a pragmatic approach that could be realized with ease and with much benefit. The supporting rationales for the above are summarised as follows.

(1) The power system operator has much experience and knowledge about the system. The probable weakness of the system and the contingency causing breakdown could be easily identified.

(2) The operator when applying an OPF program alone would not have the information on the effects on dynamic security even when the cost saving achieved by OPF would be highly offset by an intolerable amount of security (especially dynamic security) degradation.

(3) The application of a complete dynamic and static security constrained OPF would improve the security standard of power system operation and reduce the risk of system collapse due to the excessive cost optimisation of OPF that does not monitor dynamic security of states.

In the course of this development the first component of developing an effective and efficient optimization program in power dispatch is achieved through a decoupled reduced model of the system and employing Han-Powell recursive quadratic programming algorithm. The method is found to possess the following special characteristics and advantages compared to other techniques.

(1) The compact formulation may be used which contains a single equation representing the balance of active power in the reduced model.

(2) The Han-Powell algorithm is a proven fast algorithm with good and reliable convergency property.

(3) Static security limits are considered efficiently through the use of their sensitivities in the OPF loop. The calculation time and the convergency property of the original OPF program is not increased.

In the dynamic security analysis stage much effort has been spent to identify the best approach to integrate the required dynamic security monitoring function. The Extended Equal Area Criterion is identified with the following considerations.

(1) The method is fast and produces reliable Critical Clearing Time of the system.

(2) The critical machine(s) is identified in the process and paves the way for a preventive control analysis based on the power generation control of the critical machine.

(3) The iterative solution of the preventive control module which is arranged as an external module to the OPF loop means that the efficiency of the OPF program will not be hampered.

(4) It will also provides additional information on the system security sensitivities and security cost should those external security calculations be performed as options.

In this investigation the EEAC method is found to give good CCT prediction for the simulated system contingencies. However, it is also observed that the accuracy of this depends very much on the correct identification of the critical machine(s). Xue and Pavella, the originators of the EEAC method, have also emphasised on this point in their papers and went on to argue on the basis that most system instabilities are resulted from the critical machine(s) starting to lose synchronism with the rest of generators in the short time period immediately following the fault. Hence the crucial point is whether that particular critical machine can be screened out correctly or not. The initial accerlerations of machines are used as the initial screening index here. They are found to be fairly reliable; coupled with the final calculation of CCT which actually assumes the several candidate machines as critical machine to compute the system CCT sequentially, there is very little dispute as to its final CCT value in test cases. However, some school of thoughts disputed the case. The case of more than one generators losing synchronism simultaneously in large power system is raised. Erroneous results due to this complication are found to exist in special cases. The errors are found to be due to the critical machine being incorrectly identified. If a detailed stability study is done and the correct critical machine is identified, the error will be largely eliminated and the scheme works well even for those marginal cases. In order to allow for such less predictable cases, it is proposed to enlarge the number of candidate machines in the screening stage in order to reduce the risk of error.

Further work is also possible on making a clearer distinction of those less clear-cut cases. The possibility of employing Expert System techniques is deemed to valid here. Since the identification of weak generators with probable stability problem comes out from operating experiences in many real system control, an Artificial Intelligence formulation to capture those knowledge is a possible future research topic. Then with this AI help, the correct identification of critical machine will be further improved and the method will be able to give even more reliable results.

The implentation of this integrated security concept is seen to be of benefit to both power authorities and the consumers. The power system controllers will have an additional tool to audit the security of supply while maintaining the cost of generation as economically as possible. And the consumers will be more reassured of the supply being maintained at the lowest possible rate being maintained with the lowest possible operating cost being achieved. Further work in the direction of cost benefit analysis may thus be undertaken to exploit the work of this project. The possibility of extending this work to spot pricing investigation is being examined.

The direct use of Extended Equal Area criterion method hinges on the belief that this is the best available choice at the time of investigation. However the continuing research work in direct method transient stability analysis has been progressing at a rapid rate. Further refinement of such techniques may improve the potential of using them as real time dynamic security monitoring module in the proposed integrated security analysis. Moreover, as the methodology of this thesis is flexible as to the dynamic security module, it is anticipated that future work could also incorporate the new advances in direct, fast methods of transient stability analysis.

References

[1] Stott B., Alsac O., and Monticelli A.J.," Security Analysis and Optimization ", Proceedings of IEEE, Vol. 75, No. 12, December 1987 , pp. 1623 - 1644.

[2] Dy Liacco T. E. ," Real-time Computer Control of Power Systems ", IEEE Proceedings, July 1974, pp. 884 - 891.

[3] Carpentier J.,"Towards a Secure and Optimal Automatic Operation of Power System," Proc. IEEE PICA Conference, Montreal, May 1987, pp. 2 - 37.

[4] Innorta M., Marannino P., Granelli G. and Silvesti A." Security Constrained Dynamic Dispatch of Real Power for Thermal Groups", IEEE Transactions on Power Systems, May 1988, Vol. PWRS-3, No. 2, pp. 774 - 781.

[5] Powell M.J.D. ," A Fast Algorithm for Nonlinearly Constrained Optimization Calculations," Report DAMTP 77/NA , Cambridge University, England 1977.

[6] Talukdar S. N. and Giras," A Fast Robust Variable Metric Method for Optimal Power Flows," IEEE Trans. Vol. PAS-101, Feb. 1982, pp. 415-420.

[7] Alsac O. and Stott B.," Optimal Load Flow with Steady State Security," IEEE Trans. PAS, May 1974, pp. 745 - 751. May 1974.

[8] Dommel H.W. and Tinney W. F.," Optimal Power Flow Solutions," IEEE Trans. Vol.PAS-87, No. 10, Oct. 1968, pp. 1866 - 1876.

[9] Carpentier J.," Optimal Power Flows," Int. Journal of Elect. Power and Energy Systems, Vol. 1, No. 1, April 1979, pp. 3 - 15.

[10] Carpentier J.," CRIC, A New Active Reactive Decoupling Process in Load Flows, Optimal Power Flows and System Control," Proc. IFAC Symposium on Power Systems and Power Plants Control, Beijing , August 1986, pp. 65 - 70.

[11] Burchett R. , Happ H. and Wirgau K.," Large Scale Optimal Power Flow," IEEE Trans., Vol.PAS-101, Oct. 1982, pp. 3722 - 3732.

[12] Sun, Ashley etc.," Optimal Power Flow by Newton Approach," IEEE Trans., Vol. PAS-103, Oct. 1984, pp. 2864 - 2880.

[13] Stott B. and Marinho J. L.," Linear Programming for Power System Network Security Applications," IEEE Trans., Vol. PAS-98, May 1979, pp. 837 - 848.

[14] Carpentier J.," Differential Injections Method : A General Method for Secure and Optimal Load Flows," Proc. IEEE PICA Conference, Minneapolis, June 1973, Paper No. TP VIII-E, pp. 255 - 262.

[15] Elacqua A.J. and Corey S. L.," Security Constrained Dispatch at the New York Power Pool," IEEE Trans.,Vol. PAS-101, August 1982, pp. 2876 - 2884.

[16] Fink L. H. and Carlsen K.," Operating under Stress and Strain," IEEE Spectrum, Vol. 15, March 1978, pp. 48 - 53.

[17] Lo K.L., Bismil M.A., McColl and A.M. Moffatt," A Comparison of MW Ranking Methods," Electric Power Systems Research, 15 (1988), pp. 157-171.

[18] Lo K. L., Bismil M. A., McColl and A.M. Moffatt," A Comparison of Voltage Ranking Methods," Electric Power Systems Research, March 1989, pp. 104 - 119 .

[19] Wu F. F. ," Real-time Network Security Monitoring, Assessment and Optimization," Int. Jour. of Electrical Power & Energy Systems, Vol. 10 No. 2 April 1988, pp.83-100.

[20] Xue Y., Van Cutsem,and M. Ribbens-Pavella," A Simple Direct Method for Fast Transient Stability Assessment of Large Power Systems," IEEE Trans. on Power Systems,Vol. 3,No.2, May 1988,pp. 400-412.

[21] IEEE PES Working Group on Dynamic Security," Dynamic Security Assessment Practices of Member Utilities of Power Networks of North America," IEEE Trans. on Power Systems,August 1988,pp. 1310-1321.

[22] Fischl R., Mercede, Wu and Chiang," A Comparison of Dynamic Security Indices based on Direct Methods," Int. Jour. of Electrical Power & Energy Systems,Vol.10 No.4 October 1988,pp.210-232.

[23] Wu F.F.,Tsai and Yu," Probabilistic Steady-state and Dynamic Security Assessment," IEEE Trans. on Power Systems, Vol.3, No.1, February 1988 pp. 1-9.

[24] Rios-Zalapa R. and Cory B. J.," An Expert System for Security Assessment in Operational Planning of Power Systems," Proc. PSCC Conference August 1988, Stockholm-Helsinki.

[25] Monticelli A. ,Pereia and Granville,"Security-constrained optimal power flow with post-contingency corrective rescheduling," IEEE Trans. on Power Systems , February 1987, pp. 175-182.

[26] Schnyder G.," Integrated Security Control using Optimal Power Flow and Switching Concepts," IEEE Trans. on Power Systems, May 1988 pp.782-790.

[27] Bacher R.," Real-time Optimal Power Flow in Automatic Generation Control with Security Constraints," IEEE Trans. on Power Systems, November 1988, pp. 1518-1529.

[28] Tinney W. F. ," Deficiencies in Optimal Flow Programs," IEEE Trans. on Power Systems May 1988, pp. 676-683.

[29] Christie R. D. and Talukdur," Expert Systems for On-line Security Assessment," IEEE Trans. on Power Systems, May 1988, pp.654-659.

[30] Sobajic D. J. ," Artificial Intelligence System for Power System Contingency Screening," IEEE Trans. on Power Systems, May 1988, pp. 647-653.

[31] Varaiya P., F.F. Wu and Chen," Direct Methods for Transient Stability Analysis of Power Systems : Recent Results," Proc. IEEE, pp. 1703 ,1985.

[32] Vaahedi E., El-Din H.M.Z.,"Considerations in applying Optimal Power Flow to power system operation," IEEE Trans. on Power Systems,May 1989, pp. 694-671.

[33] Xue Y., Van Cutsem T. and Pavella M.," Real-time Analytical Sensitivity Method for Transient Security Assessment and Preventive Control," Proceedings

IEE, Vol. 135, Part C, No. 2, March 1988, pp. 107-117.

[34] Carpentier J., Bornand P.," Towards an integrated secure and optimal operation of power systems," Proc. IEE APSCOM-91 International Conference, Hong Kong, Nov. 1991, pp. 1-16.

[35] Fouad A. A., Vijay Vittal," Power system transient stability analysis using the transient energy function method," Book published by Prentice-Hall, 1992.

[36] Rao S.S.," Optimization theory and applications," Book published by Wiley Eastern Ltd., 1984.

[37] Chang C.S. and Chung T. S.," Application of pattern recognition technique in power system security and optimization," IEEE Trans. on Power Systems, August 1990, pp. 467 - 473.

[38] Chang C.S. and Chung T. S.," An expert system for security control of distribution control and load allocation," IEEE Trans. on Power Delivery, Jan. 1990, Vol. 5, No. 1, pp. 467-473.

[39] Chung T.S., Lo K.L., and Chang C.S.," A method to monitor transient security in optimum dispatch," Proc. of IEE International PSMC Conference, June 1991, London, pp. 244-247.

[40] Chung T. S., Lo K. L. and Chang C. S. ," On the effectiveness of applying real-time dynamic security assessment in power system optimal operation," Proc. of IEE International APSCOM-91 Conference, Hong Kong, Nov. 1991, pp. 158 - 163.

[41] Chung T.S.,Lo K.L.,Chang C.S.," Application of knowledge based screening technique for optimum dispatch of power system," Int. Journal of Systems Science, Vol. 15, No.4, 1989, pp. 125 -133.

[42] Chang C. S. and Chung T. S. ," Algorithms for security/economy control of distribution system," Proc. of IEE International APSCOM Conference, Nov. 1991, Hong Kong, pp.431-436.

[43] Chung T. S.,Lo K.L. and Chang C. S.,"Secure optimal dispatch solution with an advance dispatch procedure by Han Powell algorithm," Proc. of CEPSI Confernce, Nov., 1988, Brisbane, Australia.

[44] Chung T. S. and Fang D. Z.," Fast transient stability margin assessment through simplified system and using large step numerical integration," Proc. of 9 th CEPSI Conference, Nov. 1992, Hong Kong, pp. 176 - 183.

[45] Dy Liacco T.E.," System Security: The Computer's Role ", IEEE Spectrum, Vol. 15, June 1978, pp. 43-50.

[46] Talukdar S.N. and Wu F. F.," Computer Aided Dispatch for Electric Power Systems", Proc. IEEE, Vol. 69, Oct. 1981, pp. 1212-1231.

[47] Saito O., Koizumi K. ,Udo and Sato etc.," Security Monitoring Systems Including Fast Transient Stability Studies", IEEE Trans., Vol. PAS-94, Sept. 1975, pp. 1789- 1796.

[48] Dy Liacco T. E.," The Adaptive Reliability Control System", IEEE Trans., Vol. PAS-86, May 1967, pp. 517-531.

[49] Wu F. F. and Kumagai," Steady-state Security Regions of Power Systems", IEEE Trans. on Circuits and Systems, Vol. CAS-29, November 1982, pp. 703 - 711.

[50] Kaye R. J. and Wu F. F.," Dynamic Security Regions of Power Systems", IEEE Trans. on Circuits and Systems, Vol. CAS-29, September 1982, pp. 612 - 623.

[51] Tinney W. F. and Enns M. K., " Controlling and optimizing power systems", IEEE Spectrum, Vol. 11, pp. 56 -60, June 1974.

[52] Schulz R. P. and Price W. W. ," Classification and identification of power system emergencies", IEEE Trans., Vol. PAS-103, December 1984, pp. 3471 - 3479.

[53] IEEE Working Group Report," Description and bibliography of major economy-security functions, Parts I, II and III", IEEE Trans., Vol. PAS-100, January 1981, pp. 211 - 235.

[54] Sasson A. M. and Merrill H. M.," Some Applications of Optimization Techniques to Power System Problems", Proc. IEEE, Vol. 62, July 1974, pp. 959 - 972.

[55] Carpentier J. and Cotto G.," Modern Concepts for Security Control in Electric Power Systems," Paper 102-01, presented at the CIGRE-IFAC Symposium on Control Applications to Power System Security , Florence, Italy, September 1983.

[56] Burchett R. C. and Happ H. H. ," Large scale security dispatching: an exact model," IEEE Trans., Vol. PAS-102, September 1983, pp. 2995 - 2999.

[57] Monticelli A., Pereira M. and Granville S.," Security-constrained optimal power flow with post-contingency corrective rescheduling," IEEE Trans., Vol. PWRS-2, February 1987, pp. 175 - 182.

[58] Wollenberg B. F. and Sakagushi T.," Artificial intelligence in power system operations," Proc. IEEE , December 1987, pp. 1678 - 1685.

[59] Schnyder G. and Glavitsch H.," Integrated security control using an optimum power flow and switching concepts," Proc. IEEE PICA Conference, Montreal, May 1987, pp. 429 - 436.

[60] Bae S. H., Yokoyama R., Morita T. and Sasaki H.," Multi-objective optimal generation dispatch based on probability security criteria," Proc. IEEE PICA Conference, Montreal, May 1987, pp. 414 - 421.

[61] Rogers G. J. ," Control for Stability in Interconnected Power Systems," IEEE Control Systems Magazine, Vol. 9, No. 1, January 1989, pp. 19 - 22.

[62] Hauer J. H.," Robust Damping Controls for Large Power Systems," IEEE Control Systems Magazine, Vol. 9, No. 1, Januarry 1989, pp. 12 - 18.

[63] Pai M. A. and Sauer ," Stability analysis of power systems by Lyapunov's Direct Method," IEEE Control Systems Magazine, Vol. 9, No. 1, January 1989, pp. 23 - 27.

[64] El-Kady M. A., C. K. Tang, V. F. Carvalho, A. A. Fouad and V. Vittal,"

Dynamic security assessment utilizing the transient energy function method," IEEE Trans. on Power Systems, Vol. PWRS-1, No. 4, November 1986, pp. 573 - 581.

[67] Anderson P. M. and Fouad A. A.," Power System Stability and Control," Book published by Iowa State University Press, 1977.

[68] Pai M. A.," Power System Stability," Book published by North Holland, New York, 1981.

Appendix

Test Power Systems Datas

(1) The 5-Busbar Power System (System A)

This power system consists of 5 buses, 3 generators, 6 lines and 4 loads. Bus 1 is the reference bus. Bus 2 and bus 3 are PV-buses. Bus 4 and bus 5 are PQ-buses. There are loads on buses 2 to 5 as shown in the following tables.

Fig. A1 Load datas on 100 MVA Base

Bus no.	P_{load} (pu)	Q_{load} (pu)
1	-	-
2	0.85	0.32
3	0.80	0.32
4	0.45	0.20
5	0.70	0.25

Fig. A2 Line parameters and charging data on 100 MVA Base

Line No.	From Bus	To Bus	R (pu)	X (pu)	B/2 (pu)
1	1	5	0.102	0.453	0.0
2	1	3	0.086	0.315	0.0132
3	2	3	0.06	0.22	0.0
4	2	4	0.09	0.29	0.0
5	2	5	0.11	0.37	0.012
6	4	5	0.035	0.14	0.0

The generation cost of the three generators are defined with the cost coefficients A, B and C as in the following equation :

$$\text{Cost of gen. } i = A_i + B_i P_i + C_i (P_i)^2 \qquad \text{(A-1)}$$

Table A3 Cost coefficients of generators

Generator no.	A_i	B_i (per MW)	C_i (per MW^2)
1	25.0	350.0	50.0
2	30.0	400.0	50.0
3	25.0	250.0	50.0

(2) The 14 Bus Test Power System (System B)

Fig. A4 Load data on 100 MVA

Bus	P_{load}(pu)	Q_{load} (pu)
1	0.000	0.000
2	0.035	0.018
3	0.061	0.016
4	0.478	-0.039
5	0.076	0.016
6	0.135	0.058
7	0.000	0.000
8	0.149	0.050
9	0.295	0.166
10	0.090	0.058
11	0.217	0.127
12	0.942	0.190
13	0.112	0.075
14	0.000	0.000

Table A5 Cost coefficients of generators (14 Bus system)

Gen. no.	A_i	B_i (/MW)	C_i (/MW^2)
1	105.0	245.0	50.0
11	44.0	351.0	50.0
12	0.0	0.0	0.0
13	40.6	389.0	50.0
14	0.0	0.0	0.0

Table A6 Line parameters on 100 MVA Base (14 Bus)

Line no.	From Bus	To Bus	R (pu)	X (pu)	B/2 (pu)
1	1	11	0.019	0.059	0.013
2	1	5	0.054	0.223	0.012
3	11	12	0.047	0.197	0.011
4	4	11	0.058	0.176	0.009
5	5	11	0.057	0.173	0.0085
6	4	12	0.067	0.171	0.0085
7	4	5	0.013	0.042	0.0003
8	4	7	0.000	0.209	0.000
9	4	9	0.000	0.556	0.000
10	5	13	0.000	0.252	0.000
11	2	13	0.095	0.198	0.000
12	3	13	0.123	0.256	0.000
13	6	13	0.066	0.130	0.000
14	7	14	0.000	0.176	0.000
15	7	9	0.000	0.110	0.000
16	9	10	0.032	0.084	0.000
17	8	9	0.127	0.270	0.000
18	2	10	0.082	0.192	0.000
19	3	6	0.220	0.199	0.000
20	6	8	0.170	0.238	0.000

(3) The 30 Bus System (System C) Data

Table A7 Load Data of 30 Bus System (on 100 MVA Base)

Bus	P_{load} (pu)	Q_{load} (pu)
1	0.000	0.000
2	0.217	0.127
3	0.024	0.012
4	0.076	0.016
5	0.942	0.190
6	0.000	0.000
7	0.228	0.109
8	0.300	0.300
9	0.000	0.000
10	0.058	0.020
11	0.000	0.000
12	0.112	0.075
13	0.000	0.000
14	0.062	0.016
15	0.082	0.025
16	0.035	0.018
17	0.090	0.058
18	0.032	0.009
19	0.095	0.034
20	0.022	0.007
21	0.175	0.112
22	0.000	0.000
23	0.032	0.016
24	0.087	0.067
25	0.000	0.000
26	0.035	0.023
27	0.000	0.000
28	0.000	0.000
29	0.024	0.009
30	0.106	0.019

Table A8 Line parameters (30 Bus System)

Line no.	From bus no.	To bus no.	R (pu)	X (pu)	B/2 (pu)
1	1	2	0.0192	0.0575	0.0
2	1	3	0.0452	0.1852	0.0
3	2	4	0.0570	0.1737	0.0
4	3	4	0.0132	0.0379	0.0
5	2	5	0.0472	0.1983	0.0
6	2	6	0.0581	0.1763	0.0
7	4	6	0.0119	0.0414	0.0
8	5	7	0.0460	0.1160	0.0
9	6	7	0.0267	0.0820	0.0
10	6	8	0.0120	0.0420	0.0
11	6	9	0.0000	0.2080	0.0
12	6	10	0.0000	0.5560	0.0
13	9	11	0.0000	0.2080	0.0
14	9	10	0.0000	0.1100	0.0
15	4	12	0.0000	0.2560	0.0
16	12	13	0.0000	0.1400	0.0
17	12	14	0.1231	0.2559	0.0
18	12	15	0.0662	0.1304	0.0
19	12	16	0.0945	0.1987	0.0
20	14	15	0.2210	0.1997	0.0

/continued on next page

Table A8 (contd.)

Line no.	From bus	To bus	R (pu)	X (pu)	B/2 (pu)
21	16	17	0.0824	0.1932	0.0
22	15	18	0.1070	0.2185	0.0
23	18	19	0.0639	0.1292	0.0
24	19	20	0.0340	0.0680	0.0
25	10	20	0.0936	0.290	0.0
26	10	17	0.0324	0.0845	0.0
27	10	21	0.0348	0.0749	0.0
28	10	22	0.0727	0.1499	0.0
29	21	22	0.0116	0.0236	0.0
30	15	23	0.1000	0.2020	0.0
31	22	24	0.1150	0.1790	0.0
32	23	24	0.1320	0.2700	0.0
33	24	25	0.1885	0.3292	0.0
34	25	26	0.2544	0.3800	0.0
35	25	27	0.1093	0.2087	0.0
36	27	28	0.0000	0.3960	0.0
37	27	29	0.2198	0.4153	0.0
38	27	30	0.3202	0.6027	0.0
39	29	30	0.2399	0.4533	0.0
40	8	28	0.6360	0.2000	0.0
41	6	28	0.0169	0.0599	0.0

The cost coefficients A, B, and C of the 30 bus system defined as follows :

Cost of gen. i $= A_i + B_iP_i + C_i\,(P_i)^2$

Table A9 Cost coefficients of 30 bus system

Gen. no.	A_i	B_i (/ MW)	C_i (/MW^2)
1	0.0	200.0	37.5
2	0.0	175.0	175.0
5	0.0	100.0	625.0
8	0.0	325.0	83.4
10	0.0	0.0	0.0
11	0.0	300.0	250.0
12	0.0	0.0	0.0
13	0.0	300.0	250.0

(4) Modified 30 Bus System (System D) Data

This system has the same data as system C but with load data changed as follows.

Table A10 Load data of System D (Modified 30 bus system)

100 MVA Base

Bus #	P_{load} (pu)	Q_{load} (pu)
1	0.0	0.0
2	0.217	0.127
3	0.05	0.012
4	0.076	0.016
5	0.942	0.190
6	3.000	0.0
7	0.228	0.109
8	0.30	0.30
9	1.50	0.0
10	0.058	0.02
11	0.0	0.0
12	0.112	0.075
13	0.0	0.0
14	0.062	0.016
15	0.082	0.025
16	0.035	0.018
17	0.09	0.058
18	0.05	0.009
19	0.095	0.034
20	0.022	0.007
21	0.175	0.112

22	0.0	0.0
23	0.032	0.016
24	0.087	0.067
25	0.0	0.0
26	0.035	0.023
27	0.50	0.0
28	0.0	0.0
29	0.024	0.009
30	0.106	0.019