316

DEFENSE PLAN AGAINST EXTREME CONTINGENCIES

Task Force
C2.02.24

April 2007

agré

N° ISBN : 978-2-85873-006-3

TASK FORCE MEMBERS

Jean-Marie Gagnon (CA)	Convener

Chapter Coordinators

Walter Lachs (AU)	Chapter 1
Paulo Gomes (BR)	Chapter 2
Miroslav Begovic (USA)	Chapter 3
Bermont Truchon (CA)[1] / Peter Donalek	Chapter 4
Gilles Trudel (CA)	Chapter 5
Novosel, Damir (USA)	Chapter 6
Madani, Vahid (USA)	Chapter 7
Chen-Ching Liu (USA)	Chapter 8

Main Contributors

Massoud Amin (USA)	Harrison Clark (USA)	Ian Dobson (USA)
Peter Donalek (USA)	Robert Grondin (CA)	Shinichi Imai (JP)
Danny Julian (USA)	Daniel Karlsson (SW)	Oystein Kirkeluten (NO)
Uhlen Kjetil (NO)	Borka Milosevic (USA)	Carson Taylor (USA)
Khoi Vu (USA)	Louis Wehenkel (BE).	

Reviewers

Sandro Corsi (IT)
Alfredo Vaccaro (IT)

---

[1] We are sincerely grateful to the late Bermont Truchon for his important contribution as the initial author of Chapter 4.

Acknowledgements

Sincere thanks to the Task Force members, and to the chapter coordinators in particular, for their support, dedicated work and immense contribution, and also to the reviewers for their in-depth comments.

Foreword

Secure operation of power systems in the new competitive market environment poses new challenges. In particular, there is a need for developing improved methods of coping with and minimizing the impact of extreme contingencies, i.e. contingencies that are more severe than the normal design contingencies. While a few utilities have developed defense plans to protect against some of the extreme contingencies that could occur on their systems, there are no widely accepted practices or procedures in this regard.

Even before the 2003 Northeast blackout in North America, the Italian or the Swedish blackouts, CIGRE Committee 38 had recognized the need to provide the industry with an extensive technical report on defense plans. Task Force 38.02.24 was created with the participation of international experts to carry out this important task. With the reorganization of CIGRE, C2 Committee recognized the operational impact of defense plans as well as their benefits to operations security, and mandated the Task Force to pursue its work as Task Force C2.02.24.

The general goal was to conduct a thorough review of the subject and to prepare a comprehensive technical brochure that would assist the industry as a whole in using a consistent and systematic approach for developing effective defense plans.

The result is this comprehensive technical brochure, *Defense Plans against Extreme Contingencies*. Even if there is much debate around such systems and their benefits, they are gaining acceptance worldwide because industry recognizes there are no economic alternatives to improving system security against wide disturbances and minimizing the risk of impending disturbances cascading to widespread blackouts. The report reveals that defense plans are now applied as a natural means to improve power system security and reliability.

As the technical brochure also mentions, we are now integrating new technologies such as synchronized measurement systems (using GPS signals) together with reliable telecommunication systems acting as a key enabling technology to enhance existing defense plan schemes or facilitate their development. Therefore, an integrated hierarchical network control structure is taking place alongside defense plans as an integral part of overall system development.

Achieving this vision and sustaining infrastructure reliability, robustness and efficiency are critical long-term issues that are strategic to the C2 Committee. Like other CIGRE committees, the C2 Committee looks forward to this challenge and will mandate its working groups to focus their efforts in areas that provide the industry with better tools and systems to secure overall system operation.

I take this opportunity to thank the Task Force contributors and its convener, Jean-Marie Gagnon, for the outstanding work they have done.

Michel Armstrong,
Chairman of Study Committee C2

EXECUTIVE SUMMARY

This comprehensive Technical Brochure provides a roadmap for the development of defense plans to mitigate extreme contingencies with the intent to lead power system professionals to improve electric system reliability and security of the grid.

The basic premise for protection against extreme contingencies is that a failure in one area of the grid should not result in blackouts elsewhere, and that such situations could be minimized by well designed, maintained, operated and coordinated power grids.

Many considerations and elements from concept to application—including engineering, design, implementation, documentation, operational training and maintenance—are covered in-depth. The report offers best industry practices to make use of such schemes. The industry has for many years implemented this concept in several parts of the world. However, the advantages of these schemes have not been fully recognized due to perceived drawbacks such as impact on operation and maintenance, unintended Special Integrity Protection Schemes (SIPS) action, complex technical training for operators and technicians, perceived high costs, etc. New technologies enable coordinated wide-area monitoring, protection, and control systems with pattern recognition and advance warning capabilities. Technology advances can be cost-effective solutions while offering user-friendly operational tools to system controllers and area coordinators.

The initial chapters of the report describe the evolution of the power system with its increasing dependence on the interconnected transmission grid, and explain how this dependence has introduced many challenges. The most pressing concern is improving power system operational security. In this context, the Defense Plan concept is introduced to provide effective measures that will reduce the likelihood of blackouts. Several of these schemes are then described, showing the wide application of Defense Plans on transmission systems throughout the world.

The continuing advances in development of analytical tools and study procedures for various types of disturbances are discussed. The values of sound system design, improved substation layout, operational readiness and training are highlighted as basic measures to mitigate extreme contingencies.

The report then presents all possible means of action that could be used in a defense plan. Practical techniques using available technologies with implementation examples are presented. Finally, advanced technology will play an important role in efforts to provide enhanced security that recognizes the unique attributes of electricity infrastructure.

The report also includes a wealth of references in each chapter for the interested reader and can be viewed as a complete bibliography on any of the subjects.

The contributors to this report believe that recent blackouts, in a number of countries, have reinforced the need for the implementation of defense plans. The basic philosophy is that large-scale cascading outages could be reasonably avoided, or when they occur, the systems should be quickly restored.

Electric power infrastructures are facing great challenges that require significant efforts. Although the development of a secure, reliable, robust power system represents a very ambitious goal that will not be fully achieved for several years, individual elements of such an advanced system have been and can be incorporated into the existing grid. It is hoped that the comprehensive methods proposed in this report, for designing and implementing well-coordinated defense plans, will lead to more widespread development of these defense schemes.

Achieving this vision and sustaining infrastructure reliability, robustness, and efficiency are critical long-term issues that require also strategic investments in research and development. These efforts should lead to a better understanding not only of the applicability and benefits of new system monitoring technologies to improve online system supervision but also their application to existing and future defense plan development.

TABLE OF CONTENTS

Foreword

Executive Summary

INTRODUCTION

Blackouts rarely occur. When they do, they are usually caused by a sequence of unanticipated and / or low-probability disturbances that are generally not planned by system designers and not expected by system operators, making a power system more susceptible to blackouts.

These types of events usually occur following sequential outages on a stressed system that is operated only marginally in compliance with planning criteria. The chain of events begins when equipment is removed from an already stressed system without sufficient levels of adjustment, or when faults occur. For example, some generators and/or lines are out for maintenance, and a line trips due to a fault; other lines get overloaded and start to sag, and another line comes into contact with a tree and subsequently trips; there is a hidden failure in the protection system (e.g. outdated settings or hardware failures) that causes another line or generator to trip. At this stage, the power system is faced with overloaded equipment, voltage instability, transient instability, frequency oscillations, and/or other instabilities. Depending on the power system condition in terms of operating reserves and equipment availability, the severity of the disturbance may cause parts of the power system to be islanded, or to lose synchronism and enter a complete blackout. If action is not taken quickly and proactively (e.g. load shedding, generation rejection, reactive support remediation, system separation), the system cascades into unplanned islands or collapses.

To minimize the potential for widespread blackouts, well-coordinated Wide-Area Defense Plans have been developed and implemented.

Even before the significant events of the blackouts in the Northeast, Italy and Sweden, CIGRE Committee 38 recognized the need to provide the industry with extensive technical reports on Special Protection Systems (SPSs).[2], also known as System Integrity Protection Scheme (SIPS), and that further work was needed in the field of Wide-Area Defense Plans against extreme contingencies. Task Force 38.02.24 was created as a result, with the participation of international foremost experts, to carry out the important task of preparing a Technical Brochure for engineers who require conceptual, planning, design, and implementation information pertaining to Wide Area Defense Plans. This report will also document existing schemes, demonstrating that this concept is already being applied all over the world. Each chapter is carefully prepared by subject matter experts and prepared as a continuation of the earlier chapters.

Chapter 1 describes the evolution of the power industry over the last 25 years, converging into the competitive energy market and deregulation of bulk power systems in the past 5 to 10 years. The changing character of the power industry, with its increasing dependence on the interconnected transmission grid, has created many problems, the most pressing of which is how to improve operational security. Recent events are described, showing that the analysis of so-called normal events, even though ensuring basic system strength and acceptable security limits, is not likely to provide a sufficient margin for the multiple simultaneous events that affect power transmission systems. In this context, the concept of Defense Plan is introduced as a method of providing effective measures that will reduce the likelihood of blackouts.

This concept is already being proposed and implemented on several networks around the world, as described in **Chapter 2**, which presents existing defense plans. The numerous schemes presented demonstrate that, despite geographical and regulatory differences, the concept of improving system security can evolve in multiple ways. This chapter presents the summary description, basic philosophy, and coordination issues related to these various schemes.

Chapter 3 addresses the complex issues of power system analysis from the perspective of extreme contingencies. Analysis of a power system that is at the edge of instability following multiple events is very challenging and of questionable accuracy. Analysis tools such as stability programs and model parameters must be assessed under these types of stress system conditions. The continuing advances in the development of analytical tools and study procedures for various types of disturbances are also discussed.

[2] Reference to TF 38.02.19 – "System Protection Schemes in Power Networks", TB 187.

It should be recognized that defense plans are not a substitute to sound system design and operational readiness when it comes to mitigating the likelihood of cascading outages and extreme contingency conditions.

Chapter 4 discusses these issues and identifies different ways to reduce the likelihood of extreme contingencies through more stringent design criteria and improved operational practices."

Chapter 5 lists and evaluates all possible means of action (that is, SPSs) that could be used in a Defense Plan to respond to extreme contingencies, and offers guidelines to help in the selection of the most appropriate one based on the type of instability encountered. It briefly reviews the main power system phenomena, SPS actions available, and the main factors to be considered in the selection of the most appropriate SPS.

Chapter 6 focuses on the design and deployment of an Overall Defense Plan that will help manage system disturbances and prevent blackouts. The relative time of action for different types of events varies from normal to extreme, depending on the nature and speed of the disturbance and the need for coordination. The deployment of an Overall Defense Plan requires implementation and coordination of a number of schemes and actions spanning various time periods. Building on the basic specifications, the plan must consider reliability issues, operational and maintenance criteria, redundancy, coordination with other plans, available technologies, and telecommunications.

Chapter 7 discusses architectural aspects and Engineering considerations. This chapter presents a comprehensive listing of analog measurements, status variables, a review of the types of telemetry applications (transducer, digitized, floating points) and transmission of the analog values, and descriptions of practical methodologies for automatic arming. Design based on available telecommunication and Information technologies are reviewed. Operational control system requirements are listed, including tools for visibility, event recording and automatic analysis. Considerations and challenges are explained in detail, including those involved in implementation, types of support software, various aspects of installation and commission testing, training tools and descriptions of operational documentation, and overall systematic test plans. Design and performance validation methods are discussed and practical techniques using available technologies are also presented along with implementation examples. A section of this chapter covers measures for addressing any possible regulatory compliance requirements.

Chapter 8 provides a broader perspective of the new mega-infrastructure that is emerging from the convergence of energy (including the electric grid and water, oil and gas pipelines), telecommunications, transportation, the Internet, and electronic commerce. New ways are being sought to improve network efficiency and eliminate congestion in the power grid and other critical infrastructures, without significantly diminishing reliability and security. Because of the unique attributes of the electricity infrastructure, advanced technology will necessarily play an important role in efforts to improve security. Assuming that individual utilities are already undertaking prudent steps to improve physical security wherever possible, technology can make a vital contribution by enhancing the inherent resilience and flexibility of power systems in terms of withstanding natural disasters or attacks.

Finally, the **Conclusion** summarizes the main topics that are addressed in the report, and presents the recommendations of the Task Force on Defense Plans.

1. CONCEPT AND DEFINITION OF DEFENSE PLAN

1.1 INTRODUCTION

Maintaining the integrity of the Extra High Voltage (EHV) transmission line grid is imperative for the effective operation of any interconnected power system. The present evolution of power systems is such that the interconnected grid has become an irreplaceable link between the consumer and the power station. Consequently, the grid has become both the strength and the weakness of interconnected power systems.

Under normal conditions, and with sufficient automatic supports, operators are able to adequately control power system operation. But in an emergency, the speed and complexity of post-disturbance phenomena makes control room operators even more dependent on the prompt reaction of automatic systems when it comes to dealing with the effects of severe disturbances. Therein lies a critical weakness.

The planning and development of interconnected power systems involve routine systematic studies of a broad range of severe disturbances. Specifically, tailored automatic measures or operational constraints are introduced to respond to disturbances that are found to be dangerous. However, these systematic studies examine only a fraction of the innumerable combination of possible contingencies that could strike the grid. No automatic responses exist for this myriad of unexamined extreme contingencies, and when one strikes, operators become the last, and often inadequate, line of defense. Only very rarely have operators been able to deal with such situations effectively; in the vast majority of cases, their slow reactions to rapidly occurring post-disturbance phenomena result in grid disruption and system collapses.

The challenge facing all interconnected power systems is how to effectively deal with the impact of unforeseen multiple contingencies. To meet this challenge, a new avenue is proposed for making use of the sudden changes that occur when any disturbance strikes.

1.2 THE CHANGING CHARACTER OF POWER SYSTEMS

During the 26-year period following World War 2, the planning criteria presently followed by the Electricity Supply Industry had been devised to cater for the sustained high rate of electricity growth. Electricity utilities could gain economies of scale with lowering tariffs and still have no difficulty in financing capital intensive programs on new power stations with larger generators and extending the power system network with extra high voltage (EHV) transmission lines.

In that era it was prudent to provide redundant elements as the high rate of load growth gave assurance that they would soon be adequately loaded. Redundant elements also provided an insurance against an unexpected growth spurt. In those halycon days, the purpose of EHV interconnections was to gain diversity of demand, providing savings in spinning reserves as well as emergency back up from neighboring utilities. Coupled with the fact that city power stations were at high outputs during peak periods, EHV interconnections only rarely were heavily loaded.

The 1973-4 oil shock pushed the world economy into recession, that at the same time curtailed the growth of electricity demand. Utilities were simultaneously saddled with heavy, but now unnecessary capital commitments and dramatic increases of generating costs at a time when electricity sales dropped well below projections. Adding to this problem was the strenuous opposition to the increased electricity tariffs needed to ease the utilities' financial burden. Actions taken at that time are still having an effect on operational security.

a. To minimize generating costs, oil-fired generator outputs were sharply reduced and replaced, when possible, by higher outputs from coal-fired generation,

b. This altered generator scheduling led to much heavier power flows on EHV interconnections with substantial interchanges between neighboring utilities,

c. Utilities could now less afford to introduce redundant equipment,

d. With shorter lead times, the main savings were made in canceling transmission and distribution capital works whereas, with their longer lead times, it was more difficult to curtail the construction of power stations.

From this point of time the EHV interconnected network assumed a more important role, yet the level of redundancy on this vital network could no longer be maintained. Although the oil shock produced the largest single impact on the Electricity Supply Industry, a series of events have followed, that taken together, are having a more serious effect:

- Since 1973-4, the health of the world economy has been seriously curtailed,
- Consequently there have been lower and very erratic rates of electricity growth,
- Electricity tariffs have risen markedly for some years after the oil crisis,
- This has focused public attention on the Electricity Supply Industry, culminating in increasing environmental constraints,
- Legislation has been enacted to de-segregate electricity utilities with political promises that it will lead to lower electricity charges.
- Financial difficulties in the industry have led to transfer of decision making from engineers to financial managers.

The environmental constraints now imposed on the Electricity Supply Industry have had a major impact on its operation and finances because it has led to:

- The permanent retirement of city power stations,
- Increases in power station operating costs to meet the more stringent emission requirements,
- Besides making it more difficult and costly to establish new power stations, the constraints have added considerably to their construction lead times,
- It is now extremely difficult and more costly to establish new transmission lines.

This changing character of the power transmission system with its increasing dependence on the interconnected transmission grid has created many problems, of which the most pressing is how to improve power transmission system operational security.

1.3 COMPETIVE ELECTRICITY MARKET [1-1]

The impetus for deregulation and the competitive electricity market was initiated in the Britain while Mrs. Thatcher was Prime Minister. The aftermath of the Falklands War had saddled Britain with a tremendous hole in its finances and no ready means of its replenishment.

The political solution was the privatization and deregulation of the Government owned Electricity Supply Industry, copying a South American initiative. (Government owned railway, gas and water companies were also sold off in Britain.)

Human experience often mirrors the swings of a pendulum, shifting from one extreme to another and subsequently swinging back again. In this respect the creation of the competitive electricity market provides a backhanded compliment to engineers with their success in giving reliable supplies of electricity to communities throughout the world. Politicians, aided and abetted by economic advisors have drastically altered the ground rules in legislating for the competitive electricity market, as they seem quite unaware of the difficult challenges to operational security that have been created by the changing character of power transmission systems. A number of the idiosyncrasies caused by the deregulation of the electricity industry that will later come to bite us are listed:

- New legislation has promoted financial aspects at the expense of technical issues,
- Inadequate weighting is given to the two key physical issues of electricity supply,
- Need for continuity of electric connection from the power transmission system to each consumer,

- Variations in demand that must be instantly met by changed outputs of AC power.
- Management decisions are now heavily slanted to financial issues. For example, even though the numbers engineers have been reduced since the 1973-4 oil crisis, large numbers are now deployed on financial issues for the electricity market, with a dramatic reduction of engineers dealing with technical issues,
- The greater emphasis on financial competitiveness now with the greater number of electricity organizations has undermined levels of technical cooperation,
- The consequent reduction of coordinated planning, particularly of the transmission grid, is having an impact on operational security,
- The legislative financial directives have overturned engineering considerations. For example, greater operational security can be gained by ready access to adequate levels of reserve generation. However the highest cost of electricity in the market (and some of the highest profits) results from a generation deficiency, the very situation when reliable supply to consumers can be in jeopardy.

1.4 PROCESS OF SYSTEM BREAKDOWN

When extreme contingencies have disrupted interconnected power transmission systems, the post-disturbance effects have led to number of distinct types of system breakdown. In the majority of cases the breakdown has been due to transient instability, angular instability, system voltage instability, under-frequency or cascade line tripping [1-2].

Incidents of collapse have reported an initial post-disturbance period during which the power transmission system remained intact. This prompts the obvious question: "How does the power transmission system break down?" The path to a new approach rests on resolving this question.

The power transmission system has sufficient resilience to withstand a direct fault on an EHV line, when the protection clears correctly. Yet when no fast protection acts, the danger of power transmission system breakdown arises. In exploring this question, it becomes evident that if the disturbance is not dealt with promptly, the uncontrolled after-effects will continue to flow through the power transmission system network and will actuate responses from back-up control devices.

Such control devices are widely distributed throughout the power transmission system and include turbo-generator governors, automatic voltage regulators, boiler-controls on coal-fired power stations and automatic transformer tap changing. During uncontrolled post-disturbance phenomena, these control groups have three intrinsic deficiencies:

i. Each group functions at a different speed, a fraction of a second to minutes,

ii. Each individually has actions responding only to changes in the immediate vicinity,

iii. Not one of them acts in coordination with any other.

Their disparate actions, in response to the chaotic post-disturbance phenomena, are actually the cause of power transmission system breakdown [1-3, [1-4]. The corollary is that breakdown can only be avoided by the timely control of post-disturbance phenomena. It is vital to diminish the post-disturbance phenomena to avoid the onset of dangerous uncoordinated responses of the back-up devices. Prompt automatic responses of appropriate intensity in the disturbance locality offer the approach that can best meet this need.

1.5 EARLY DEVELOPMENT OF DEFENSE PLANS

Considerable effort and resources are allocated by the Electricity Supply Industry to support interconnected power transmission systems against the danger of collapse. Apart from line power flow constraints, these predominantly fall into three categories:

- To avoid the loss of all or most generators should frequency fall excessively, under-frequency load shedding is in place.
- To ameliorate the worst consequences of dynamic angle stability, line protections are provided to island the grid.

- To respond to a number of foreseeable disturbances, purpose designed system protection schemes have been introduced.

These three areas are examined from the aspect of extreme contingencies on the interconnected grid and with respect to the main requirement of holding its integrity.

1.5.1 Under-frequency load shedding [1-5]

Power station auxiliaries in thermal and nuclear power stations can only function effectively within a limited frequency range. Should a heavy loss of generation cause frequency to fall below its nominal levels by 2 Hz or more, power station auxiliaries trip out causing power stations to shut down and leading to the collapse of entire power transmission systems. To counter this danger, under-frequency load shedding (UFLS) has been introduced. It is quite different from other types of protections insofar that it must deal with situations more severe than those considered by normal contingency criteria. When it was first introduced about 50 years ago, power networks were more compact than the present large interconnected systems. The philosophy underlying UFLS has recognized the advantage of keeping the network intact by timely tripping of selected consumers, rather than losing the network. So difficult decisions have been made in choosing consumers to be shed (up to 60% of system demand) but being careful to maintain all important and essential services.

Although spinning reserves are provided to cover the unexpected loss of the largest generator, situations have arisen when two or more large generators were lost in quick succession. Prior to the extensive interconnections of power transmission systems, this generation produced a dangerous frequency fall causing frequency to reduce uniformly throughout the then smaller networks.

This allowed relays that measured the frequency level or the rate of frequency decline, to be used for tripping the pre-selected loads scattered throughout the network. In the now extensive interconnected networks, entire power stations would need to be lost before a dangerous frequency reduction would occur. The character of power transmission systems has altered, yet the same style of UFLS is still adopted throughout the world's power transmission systems.

In the present evolution of interconnected power transmission systems, ties between utilities are small in relation to each utility's load and generation capacity. The consequent elasticity of the ties results in a different rate of frequency reduction in adjoining utilities following the loss of generation. Transient stability studies have indicated that a frequency wave can take from 1 to 3 seconds to traverse from one extremity to the other of a large interconnected power transmission system. The lowest frequency, before turbo-generator governors can react, would occur within the utility where generators had been lost. With heavy generator loss the possibility of frequency falling more than 2 Hz within this utility's network could create the risk of losing more generators.

A weakness of using UFLS on extensive interconnections was shown in November 1978, with the loss of an entire power station in Rome at a time when lines from northern Italy were carrying heavy power flows to the south [1-5]. Under-frequency relays shed loads throughout the north and south of Italy, leading to a marked increase in power flow on lines from Northern Italy. These higher power flows undermined system voltage stability and culminated in the collapse of the entire Southern Italian network. This incident demonstrates an inherent difficulty following the loss of generators, when the consequent low frequency leads to load shedding throughout the interconnected network. The utility having lost generation would then import additional power on its incoming tie lines, seriously lowering its voltage levels because only a small proportion of the load would have been shed within the utility's network.

1.5.2 Islanding

The danger to power transmission systems posed by the loss of system dynamic stability has initiated considerable efforts for dealing with this threat. The intrinsic problem arises whenever a change in operating conditions, such as higher line power flows, increases the power angle between different groups of generators within the grid. The larger angles reduce synchronizing forces between these different groups of generators. With no adequate precautions the altered condition could trigger inter-generator swings, disrupting synchronizing forces and lead to dynamic instability. As a safeguard against this, controls that damp their responses, automatic voltage regulators with power stabilizers have been introduced on rotating units. The damping factors are based on system eigenvalue studies that assess foreseeable disturbances to the grid. However, the values accorded to these damping factors

are significantly influenced by the network topology, so that if the topology were radically changed by an extreme contingency, damping responses could be inadequate to control dynamic stability.

As a fall back, and to avoid severe disruption to the grid, line protections are provided that can sense the angular swings at the onset of dynamic instability. These protections would open a number of lines, splitting the grid into islands and at the same time inhibiting the inter-generator oscillations. However, some islands would have more load than generation and others an excess of generation. Under-frequency load shedding may stabilize the former, but there may be a danger of losing generators from over-speeding in the latter islands.

The islanding strategy has proved unsuccessful following extreme contingencies that have led to system voltage instability. In the terminal phase of system voltage instability at the curtailment of rotating unit excitation, system dynamic instability is triggered. However, at this stage, voltage levels have been so depressed that rather than system islanding, there has been cascade line tripping and even when under-frequency load shedding occurs, system collapse still has not been averted.

1.5.3 System Integrity Protection Schemes (SIPS)

The SIPS encompasses Special Protection Systems (SPS), Remedial Action Schemes (RAS), as well as additional schemes such as, but not limited to, underfrequency (UF), undervoltage (UV), out-of-step (OOS), etc. SIPS involves same level of studies as any SPS and requires coordination amongst various SPSs.

1.5.4 Special Protection Systems (SPS)

Special Protection Systems (SPS) are generally intended to operate for rare, but foreseeable events that could otherwise undermine the integrity of the grid. Their function is quite distinct from the usual protection scheme that isolates an individual system element from the network when it has a fault. SPSs are generally a by-product of the system planning process when annual assessments check the ability of the power transmission system to withstand the disturbances considered by planning criteria. Special operating measures, such as line power flow constraints or SPS, would need to be invoked to deal with those of the disturbances found to be a threat. Generally, fairly elaborate software is required for each system protection arrangement so that it can correctly respond to the potentially threatening disturbance.

Considerable planning studies are necessary to create each system protection scheme, not only for effectively dealing with the specific disturbance, but also to insure against dangerous interactions with existing automatic arrangements. As the power transmission system develops, its character is gradually modified, giving a need for their re-examination so as to ensure the continuing effectiveness of the SPS.

Yet an analysis by the North American Electric Reliability Council (NERC) of major incidents between 1984 and 1991, uncovered the fact that 70% of these incidents were worsened by the responses of system protection schemes. This primary due to the fact that the conventional protective schemes are not designed or set to respond to extreme operating conditions. Likewise, the electrical system is not designed to withstand protection malfunction during stressed conditions (causes additional break-ups). There are innumerably more extreme contingencies than the foreseeable disturbances against which the system protection schemes have been devised and this highlights the serious problem in the present manner of dealing with system security.

1.6 DEFINITION OF DEFENSE PLAN

The Task Force proposes this definition of a Defense Plan:

Defense plans are a set of coordinated automatic measures intended to ensure that the overall power system is protected against major disturbances involving multiple contingency events, generally not caused by natural calamity. Defense plans are used to minimize and reduce the severity and consequence of low probability and unexpected events and to prevent system collapse. Defense plans are primarily used to increase power system security. A defense plan can be considered as an additional level of protection, designed to initiate the final attempt at stabilizing the power system when a widespread collapse is imminent. Individual System Integrity Protection Schemes (SIPS) such as automatic generation run back schemes, load or generation rejection, load shedding, reactive switching, bus or system splitting, etc. are then regarded as coordinated elements used within a defense plan.

The inability of control room operators to deal with the consequences of unforeseen extreme contingencies underlines the need for a different approach to power transmission system emergency control. The key objective of the defense plan is to be able to maintain the integrity of the interconnected grid, in spite of the loss of a number of elements. This objective can only be met with effective automatic responses to support operators in their unequal struggle against extreme contingencies. These automatic measures must counter the post-disturbance dynamic phenomena so that the interconnection then remains in a viable operating state when operators take over. It is vital that operators have enough time to consider further actions to avoid them being under pressure to take rapid actions when the probability of human error greatly increases.

With grid integrity sustained after the disturbance, generators would continue to function and provide electricity supplies to most consumers.

Operators would then more quickly regain normal operation and then be able to restore supplies to all consumers. This is in contrast with the considerable delays, sometimes more than a day, to reconnect all consumers when the grid first has to be resurrected and generators restarted.

The interconnected power transmission system has the resilience to withstand the initial impact of severe disturbances. An effective defense plan should make use of the sudden parameter changes to trigger timely responses to the prevailing disturbance. It must initiate automatic actions, capable of quarantining post-disturbance phenomena with timely responses in the affected region. The following chapters present different measures to be considered for defense plans.

The Electricity Supply Industry has already accepted the philosophy of emergency shedding by selecting non-essential loads for under frequency shedding. A useful perspective on the needs of a defense plan has been gained by examining three collapses that beset different power transmission systems during August and September 2003.

1.7 LEARNING FROM THE 2003 BLACKOUTS [1-6] to [1-13]

In August and September 2003, the inherent deficiency of system emergency control was forcefully shown on four of the world's interconnected power transmission systems. First, the eastern and mid-western portions of the United States and Canada experienced a blackout. (This occurred on 14th August, affected 50 million people and cost many billions of dollars. Next Sweden and Denmark lost power (affecting 5 million people), and in late September, most of Italy was plunged into darkness. Some outages lasted less than an hour, others more than a day.

Reports, providing extensive details of each of the blackouts have been prepared, describing the chain of events that culminated in the collapses. In each incident, for a variety of reasons, control room operators were unable to deal with the situation. These three extensive collapses could have been averted if faster responses had been taken but under the circumstances control room operators were unable make them. Social disruption and high costs of blackouts emphasize the extreme importance of providing automatic responses for dealing with extreme contingencies. To develop a path towards this objective, the following brief analyses focus on the initial stages of each incident and also examine the pre-disposing factors that significantly handicapped the operators.

1.7.1 North-East American Collapse – 14th August 2003 [1-6, [1-7, [1-8]

The triggering event that led to the cascading blackout was the tripping of three 345kV transmission lines from flashovers to adjacent trees.

These lines, in Ohio, are operated by FirstEnergy Corp, tripped separately between 15.05 and 15.36 on the afternoon and created the unstoppable cascading failures that culminated in the disruption of the North-East American grid.

The predisposing factor was the failure of FirstEnergy's energy management system alarm and logging software shortly after 14.14, about two hours before the blackout. Subsequently no valid alarms came in and no alarms were printed or posted on the EMS alarm logging facilities. Not knowing of the failure of alarms and indications, operators were unaware that key system elements were reaching and then passing the limits of safe operation.

The situation was compounded by the non-effective performance of system analysis tools at the Midwest Independent System Operator (MISO) that is the entity that coordinates power transmission in the region that includes FirstEnergy. Although measures had been prescribed – adjusting the output of power plant, taking customers temporarily off-line – to deal with potentially catastrophic overloads, with their lack of information, operators did not take these steps. As a consequence the overloads were moved to other unprepared lines, causing the disruptive effects to spread widely throughout the interconnected grid and culminating in its collapse.

Proposal for Automatic Emergency Response

Taking the view that automatic response would have been the most effective means for circumventing the oncoming events, the question is how to trigger the automatic actions. The critical predisposing and identifiable factor occurred when at least one line's power flow exceeded its continuous rating. If automatic actions could be taken at this point, to reduce the power flow before the line protection can function, then the danger of cascade line tripping would be averted. A proposal for rapid load shedding on the line's receiving end specifically to achieve this purpose, has been proposed in Reference [1-9].

1.7.2 Scandinavian Blackout – 23rd September [1-10]

Prior to the loss of a 1200MW power station in Denmark, pre-planned maintenance has some transmission links and power stations out of service. Five minutes after operators started switching to restore more secure conditions, a double bus fault occurred on a 400kV substation in Southern Sweden, due to mechanical failure of an isolator, causing the loss of four 400kV lines. This led to the loss of an 1800 MW nuclear power station, connected by two of the lines and the loss of the other two lines critically weakened the ties between central and southern Sweden. Increased power flow on the remaining lines, aggravated by generation ramping in Northern Sweden, Norway and Finland, resulted in a severe voltage decline in southern Sweden and eastern Denmark. As in previous situations of sharp voltage reductions leading to system voltage instability, and cascade tripping line protection relays acted, isolating central Sweden from Southern Sweden and eastern Denmark culminating in a blackout within seconds.

Proposal for Automatic Emergency Response

Once the double bus fault at the 400kV substation led to the loss of four 400kV lines, control room operators were no longer able to deal with the situation. The heavier power flows on the remaining lines led to cascade line tripping putting the situation beyond control. If the subsequent line power flows could be swiftly reduced before their protections could trip them, cascade line tripping could be prevented. A proposal for rapid load shedding on the line's receiving end specifically to achieve this purpose has been proposed in Reference 9.

1.7.3 Italian System Collapse – 28th September 2003 [1-11, [1-12,[1-13]

Events culminating in the collapse of the Italian power transmission system occurred between 3.00 and 3.30 a.m., a period when operators are often not expecting trouble.

At the time the Italian demand totaled 27,702 MW, which included 3638 MW of pumping. The Italian network was importing 6651 MW over 15 incoming 380kV and 220kV lines through Switzerland (3610 MW), France (2216 MW), Slovenia (638 MW) and Austria (191 MW) from generation mainly in Germany, France and Poland.

Power flows were influenced by the network impedances and created heavy loadings on the Swiss network within which the critical problems occurred. ETRANs, which is the Swiss coordinating body and not a transmission system operator, (as control other countries' networks,) relies on the seven Swiss grid operators for its data and corrective procedures.

A 380kV line in Switzerland, with a power flow at 86% of its nominal rating, tripped when a sagging conductor flashed over to a tree. The attempts of single-phase auto-re-closing were not successful so its protection disconnected the line. Operator attempts at restoring the line to service were also unsuccessful because of the high power angle (42'), resulting from the continuing high power flow through the grid into Italy. Blocking of the line re-connection is provided against too high a line phase angle difference so as to protect nearby generators against damage or malfunction due to high transient stress when switching on the network.

With the first line remaining out of service, another parallel 380kV line had an increase of power flow to 110% of its continuously rated current. Although operators of the Swiss network requested Italian operators to reduce imports by 300 MW, this response did not sufficiently reduce the critical line's power flow. 25 minutes after the first trip, conductors on the second line sagged sufficiently to produce a tree flashover and the loss of the second line.

This proved to be the final straw, and led to the cascade tripping of the remaining lines into Italy in the following 12 seconds. The frequency of the European network (UCTE) increased to 57.25 cycles, but it remained intact. Even though about 10,000 MW of load was disconnected in Italy, this was too late to prevent its collapse from system voltage instability within 2.5 minutes.

Proposal for Automatic Emergency Response

It is difficult to believe that control room operators of one of the seven Swiss grid operators could have an adequate comprehension of the UCTE network and the 15 lines, through five different countries, connecting it to the Italian power transmission system. Yet it is on their actions, at a light load period when probably fewer operators were on duty, that led to the Italian blackout.

In hindsight, it is easy to suggest that the dangerous overload on the second line could have been removed by tripping the pumping load in Italy. If an automatic arrangement had been in place to make such a response, this may have relieved the situation. However should an excessive power flow still persist on the most heavily loaded, the proposal for rapid load shedding on the line's receiving end, as proposed in Reference 9 would also need to be implemented

1.8 BY-PASSING THE MAJOR IMPEDIMENT

The prevailing approach for dealing with power transmission system security has a critical deficiency insofar that there is no provision for dealing with extreme contingencies – unforeseen multiple contingencies more severe than those considered by planning criteria. A key problem lies in the planning process that requires a systematic study of disturbances before countermeasures can be devised against any that pose a threat. This difficulty can only be overcome by a different planning approach that would assess a manageable number of representative extreme contingencies to verify its efficacy. The present approach requires measures to be in place for dealing with a disturbance but it cannot handle unforeseen disturbances. Accepting that not all disturbances can be foreseen, a realistic approach can only commence from the moment an extreme contingency strikes. At that point, abrupt changes of system parameters (e.g.: voltages, currents, frequency, etc.) occur and these changes have to be utilized for responding to each disturbance.

How then to avoid the futility of systematically assessing disturbances?

The starting point must build on the certainty that every disturbance causes abrupt changes. The following findings have been made in taking this approach [1-3, [1-4].

1) The pattern of the parameter changes (currents, voltages, frequency, etc) can identify the impending form of system breakdown.
2) Changes of voltage and current can delineate the locality and impact severity in the region first affected by the disturbance, without need for elaborate computations.
3) The initial parameter changes would be able to trigger timely responses.
4) Effective responses, tailored to meet the impending form of breakdown, can quarantine the post-disturbance phenomena within the initially affected region.

5) The grid would be sustained by curtailing the spread of disruptive phenomena.

These findings underpin strategies that can react to unforeseen severe disturbances and provides the foundation for devising automatic responses against such disturbances. Studies adopting such strategies have shown them to be effective in dealing with extreme contingencies, such as the simultaneous loss of multiple EHV lines. The grid would be sustained by timely reactions in affected regions.

Using these strategies in planning studies for the interconnected grid allows an assessment of their effectiveness against disturbances, much more onerous than those presently considered by planning criteria. This avenue would remove need for the systematic studies presently adopted for developing system protection schemes. Essential requirements of such an area-wide system protection scheme for averting system collapses and an approach for its development are presented in Reference [1-14, [1-17].

1.9 CONCLUSION

When responding to extreme contingencies, the critical objective is to keep the power system and especially the EHV interconnected transmission grid, cohesive and in a functional state. Achieving this objective would limit the number of consumers who experience service interruptions, and at the same time, maintain a viable level of system operation. In addition to the existing "event-based" control actions, there is also a need for "response-based" actions.

At the present time, operational system security is built on "event-based" controls, which are only able to deal with foreseeable disturbances. In this respect, these controls are based on system planning criteria that have been designed to make the power system sufficiently robust to withstand all foreseeable disturbances. But when unforeseen extreme contingencies strike, operational security measures have not been able to prevent the collapse of interconnected power systems. There is clearly a need for a different strategy that can elicit timely automatic responses in the precise region that is most affected by the extreme contingency. The feasibility of such an approach was graphically demonstrated by the events of July 3, 1996, when the North American Western Interconnection remained largely intact. An identical disturbance on July 2, 1996 disrupted the interconnection, but timely response by operators on July 3 avoided a repeat of the catastrophe [1-15, [1-16]. This event showed that there are identifiable changes in voltage and rotating unit reactive power output (to which operators responded) that a system protection arrangement can utilize to initiate automatic measures for safeguarding grid integrity.

What would be the consequences of implementing such an arrangement?

The full grid capacity would be available for normal operation, which would eliminate the need for line power flow constraints. This security measure of constraining line power flows for hundreds of hours per year has not been able to avert system collapses in the face of extreme contingencies. If the suggested automatic arrangement were in place, line power flow constraints would only occur for a short time (minutes per year), when extreme contingencies strike, and afterwards as automatic supports hasten the restoration of normal operation.

A number of proposals have been submitted since the August 14, 2003 Northeastern blackout, including the Republican Policy Committee Report, "Fixing the Power Grid", which suggested spending $56 billion over the next decade for new transmission lines [1-17]. This costly approach does not address the underlying problem.

As long as system operators continue to work without adequate automatic supports for dealing with unforeseen extreme contingencies, interconnected power systems will continue to suffer collapses. If such collapses are to be averted, there is no realistic alternative to implementing automatic operator supports or defense plan.

1.10 REFERENCES

[1-1] J.A. Casazza "An American's View of the Reorganisation of the ESI" Power Engineering Journal Vol.11 No.2 April 1997 pp.79-84

[1-2] W.R. Lachs - "Resolving the Impasse in Emergency System Operation" IEE Proceed-C, Generation, Transmission & Distribution Vol. 132 No. 5 Sept.1987. pp. 331-336.

[1-3] W.R. Lachs - "Controlling Grid Integrity After Power System Emergencies" IEEE Transactions in Power Systems PWRS No.17 No.2 May 2002

[1-4] W.R. Lachs – "A New Horizon for System Protection Schemes" IEEE Transactions in Power Systems PWRS No.18 No. 1 – February 2003 pp.334-338

[1-5] D. Prasetijo, W.R. Lachs & D. Sutanto -"A New Load Shedding Scheme for Limiting Under-frequency" IEEE Trans Power Systems Vol.9 No.3 August 1994 pp.1371-78

[1-6] Interim Report: Causes of August 14th Blackout in the United States and Canada U.S. – Canada Power System Outage Task Force November 2003

[1-7] James Varley – "Unearthing the Root Causes" Modern Power Systems Nov. 2003 pp. 15

[1-8] "Briefly Reviewing Recent Events" IEE Power Engineering Dec/Jan 2003/04 pp. 12-13

[1-9] W. R. Lachs "Transmission Line Overload: Real-time Control" IEE proceedings C Generation, Transmission Distribution Vol. 132 No. 5 Sept. 1987 pp. 342-347

[1-10] Janusz Bialek – "Are Blackouts Contagious?" IEE Power Engineering Dec/Jan 2003/04 pp. 10-13

[1-11] Daniele Biglino - "The path of Least Resistance" Modern Power Systems Nov. 2003 pp. 29-32

[1-12] "Interim Report of the Investigating Committee on 28 September Blackout in Italy" UCTE Report 27 October 2003.

[1-13] S. Corsi, C. Sabelli – "General Blackout in Italy Sunday September 28, 2003, h. 03:28:00", IEEE General Meeting, Panel Session "Main Blackout in Europe and USA", Denver, June 2004

[1-14] W. R. Lachs – "Area-Wide System Protection Scheme Against Extreme Contingencies" Proceedings of the IEEE Vol. 93 No. 5 May 2005 pp.1004-1027

[1-15] C.W. Taylor & D.C. Erickson -"Recording and Analysing the July 2 Cascading Outage" Computer Applications in Power Systems. Vol. 10 No. 1 January 1997 pp.26-30

[1-16] C. W. Taylor – "Improving Grid Behaviour" IEEE Spectrum Vol. 36 No. 6 June 1999 pp.115-127

[1-17] Jon Kyl, Chairman – Republican Party Policy Committee "Fixing the Power Grid" September 30, 2003

APPENDIX 1.1: LIST OF LARGE DISTURBANCES

Some of the Large Disturbances that have affected Power Systems:

Country or Region	Year	Loss of Demand
North East America	1965	100%
New England	1965	100%
New York City	1977	100%
France	1978	75%
Greece	1983	100%
Sweden	1983	63%
Netherlands	1984	100%
Portugal	1985	100%
United Kingdom	1986	16%
Tokyo	1987	21%
Belgium	1990	78%
Spain	1993	15%
Israel	1995	70%
Western USA	1996	4750MW

2. OVERVIEW OF EXISTING DEFENSE PLANS

2.1 INTRODUCTION

The new environment resulting from the deregulation of the power industry, characterized by the privatization and restructuring of traditional utilities and the introduction of new players, has led to greater use of power system resources, which means they are operating close to their limits, and this has had a negative impact on operational security. This statement reflects an international consensus that has been mentioned during IEEE and CIGRE debates, and reveals the international scope of the concern with respect to security management of power systems. The result of this concern is that each country has been engaged in the development and implementation of consistent and flexible defense plans. These defense plans are designed to increase the ability of the respective systems to withstand extreme contingencies, which are usually initiated by multiple faults, by single faults associated with multiple disconnections, or by successive tripping of transmission components.

This chapter contains excerpts from the documents mentioned in the References section pertaining to existing defense plans—which have been developed around the world despite geographical and regulatory differences. For each plan there is a summary description and a discussion of the basic philosophy and coordination issues.

2.2 HYDRO-QUÉBEC´S DEFENSE PLAN

Hydro-Québec's power system is one of the most extensive and complex in North America. Its main infrastructure, made up of more than 11,000 km of 735-kV lines, largely relies on dynamic shunt compensation, series compensation and automatic defense plans to maximize its reliability and security. The Hydro-Québec's power system current design is based on the following basic principles [2-1]:

- The system must be designed to support conceptual contingencies without service interruption or the assistance of special protection systems (conceptual contingencies are those most likely to occur).
- The system must comprise means of avoiding system-wide power failure under extreme contingencies.
- Strategic equipment must not sustain any damage in the event of a general outage to ensure that system restoration is always an option.

The decision to use automatic measures to minimize the frequency and extent of outages that could result from more serious but less common contingencies than conceptual contingencies is one of the important special features of the Hydro-Québec's design criteria.

All the automatic measures that ensure preserving the Hydro-Québec system, during extreme contingencies were combined under the name "Defense Plan". The goal of Hydro-Québec's defense plan, which was fully operational in 1998, is to detect and confine incidents that exceed the system's strength. It is entirely automatic and relies mainly on:

- A generation rejection and/or remote load shedding system (RPTC);
- A 735 kV shunt reactor automatic switching system;
- An undervoltage load shedding system;
- An underfrequency load shedding system.

2.2.1 Main characteristics of the Hydro-Québec system

Geographic constraints have played a decisive role in the development of the Hydro-Québec system. The fact that most of the generating facilities are large hydroelectric power stations located more than

1,000 km from the main centers of consumption led Hydro-Québec to design a very extensive, extra high voltage 735-kV transmission system.

The Hydro-Québec system has a number of characteristics that make stability and voltage control critical issues in the design of its transmission system. Among the most important of these characteristics are:

- The isolation of the Hydro-Québec system's (no synchronous link with neighboring systems);
- The large distances between generation and load centers and the concentration of generation at large hydroelectric sites (85% of total generation takes place in 3 large, distant hydroelectric complexes);
- The use of a 735-kV transmission system that is very extensive (more than 11,000Km of 735-kV lines) but has a relatively limited number of lines located in two main axes.

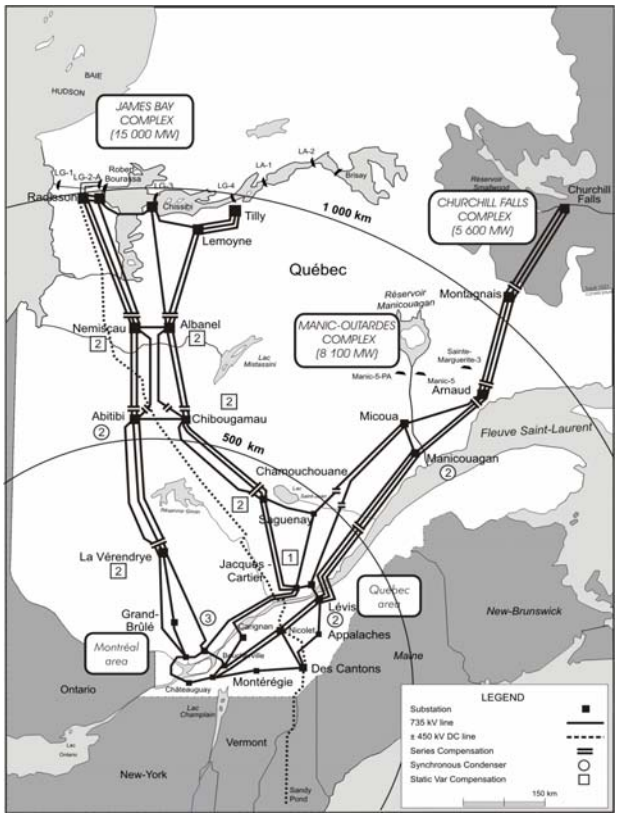


Figure 2.1 : Hydro-Québec's 735 kV transmission system

The system as planned for 2005 is illustrated in **Figure 2.1**. It includes the generation of about 37,000 MW on a system consisting of eleven 735-kV lines with series compensation (total of 11,200 MVAr), thirty 735-kV substations, one 1,200 km ± 450 kV direct current line and dynamic shunt compensation consisting of 11 static compensators and 9 synchronous compensators.

Because of its very extensive structure and the relatively small number of lines in its main transmission system (in comparison with the power carried), the Hydro-Québec system is sensitive to incidents that could cause chain reactions and the loss of several transmission lines. In fact, Hydro-Québec experienced three general power failures in the 1980´s caused by extreme contingencies.

The consequences of these system-wide power failures were deemed significant enough to justify the establishment of measures that would limit their impact. Hydro-Québec therefore decided to deploy a defense plan against extreme contingencies [2-1], **[2-2**]. The defense plan consists of all the automatic measures required to preserve the stability of the system and maintain acceptable voltage levels after extreme contingencies. It is the ultimate protection against the total collapse of Hydro-Québec's system following such an event. The total cost of this defense plan is less than 1% of the total transmission system assets.

Table 2.1 lists the various extreme contingencies used for power system planning and the level of performance required for each one. The required performance level depends on the probability of occurrence of each contingency and takes into account the characteristics of Hydro-Québec system's and operating conditions.

Table 2.1: Performance requirements for extreme contingencies

A: stable, service continuity, SPS with limited action;

B: stable, all SPS allowed;

C: stable at least at 75% power transfer level, all SPS allowed.

SPS: Special Protection Systems

Extreme Contingencies	Performance Requirements
Single line to ground (SLGF) with loss of two series or two parallel 735 kV lines	A
SLGF with loss of one or two parallel 735 kV lines and bypass of all series capacitor on the remaining parallel lines in the same corridor	B
ac-dc event : loss of a bipolar dc line caused by a SLGF with loss of a 735 kV line	B
SLGF with loss of all lines in a corridor: In Churchill-Manic section Elsewhere	 B C
Loss of all 735 kV lines emanating from a substation	C
Loss of all generation units at a station	C
Loss of a major load center	C
Three phase fault with delayed clearing	C
Unintended operation of a SPS for an event or condition for which he was not intended to operate	B

It is important to note that for some of these contingencies service continuity is required but the use of SPSs is allowed. These contingencies are thus considered similar, in terms of required performance, to conceptual contingencies. In these cases, SPS actions are limited and load shedding is tolerated only for voltage instability phenomena.

The contingencies in Table 1 cover almost all of the extreme situations that can occur on a UHV network. When they are applied to a system like Hydro-Québec they thus underlie most of the instability phenomena that can be encountered in an electrical power system. These contingencies can be divided roughly into two categories:

- Extreme contingencies that mainly affect the system's transmission capacity (e.g. the loss of several 735-kV tines) and that are generally expressed by transient or dynamic stability phenomena or by rapid voltage stability phenomena.
- Extreme contingencies that mainly affect the generation-load balance (e.g. loss of load substation or generating station) and that are generally expressed in over-frequencies, under-frequencies and long-term voltage or stability phenomena.

The automatic measures adopted by Hydro-Québec to deal with extreme contingencies must therefore cover all these forms of system behavior.

2.2.2 Philosophy and Design Principles of the Defense Plan

The philosophy adopted by Hydro-Québec for protection against extreme contingencies is that a general power failure must not be the consequence of a situation that could reasonably have been avoided. The objective is therefore to preserve the integrity of the electric system by using automatic measures that are simple, reliable and safe for the system and provide the most extensive possible coverage against all possible extreme contingencies.

At Hydro-Québec, preserving the power system after an extreme contingency is therefore based on the use of special protection systems. Since the actions required to preserve the system's integrity must often be both fast and massive, Hydro-Québec has defined a number of principles governing the design of its defense plan. The most important design principles are as follows:

- The means used to counter extreme contingencies must never put system or equipment safety in jeopardy during a false trip or unintended operation;
- The SPS must first and foremost be simple, even at the risk of loosing some selectivity. For this purpose, the various extreme contingencies possible in a substation must be grouped in a limited number of categories;
- The preference is for SPSs with local detection and action. Since there is a very large number of possible extreme contingencies, it is thus preferable to detect the consequences of a contingency on the power system (response based SPS) rather than try to detect the actual contingency (event based SPS);
- The preferred means are those with the least impact on service continuity. It is, however, preferable to voluntarily eliminate a portion of the load than to lose all of it by allowing the system's behavior to deteriorate. The use of remote load shedding must be minimized and requires a high level of security;

2.2.3 Main Characteristics of the Hydro-Québec Defense Plan

One of the main problems encountered in developing a defense plan against a set of extreme contingencies is to ensure the coordination of the various measures used. It is necessary for each measure to have a clearly defined task to perform, given the many situations and system behaviors that could occur. Thus, during complex extreme contingencies involving a number of automatic measures, no outside coordination must be required. Each system must be able to act as a function of its own contingencies, and the combination of actions should make it possible to preserve the stability of the power system. Detailed studies on all aspects of power system stability and behavior have made it possible to determine that the measures adopted contain enough flexibility to meet this important constraint.

The analysis of multiple extreme contingencies in relation to the design principle led to the recommendation of the following SPS:

- An under-frequency load-shedding system installed in about 150 distribution substations which can access over 13,000 MW of load;
- Automatic shunt reactor systems (called MAIS **[2-3]**) installed in twenty-two 735-kV substations which control about 15,000 MVAR;
- An SPS involving generation rejection, load shedding and remote reactor tripping at 735-kV. Called RPTC **[2-2]** this SPS is designed to detect multiple line losses or series-compensated capacitor bank tripping in 15 strategic 735-kV substations;
- An undervoltage load-shedding system able to shed 1500 MW of load, mainly found in 735-kV substations in the Montreal area.

The defense plan against extreme contingencies uses three levels of increasing automatic intervention, to counteract extreme contingencies of increasing severity.

1- The first level is based on limited generation rejection combined with tripping 735-kV shunt reactors. Together, they make it possible to preserve the system's stability without affecting service continuity after the loss of two 735-kV parallel lines during peak periods.

For the loss of two parallel lines involving voltage stability phenomena, undervoltage load shedding is also allowed.

2- At the second level of intervention, the effect of extreme contingencies is detected on the system. The automatic switching (closing or tripping, as appropriate) of 735-kV shunt reactors, undervoltage and underfrequency load shedding preserves the stability of the system for a very wide range of situations. These local means of detection and measures allow system integrity to be preserved for all extreme contingencies in at least half of the 735-kV substations. At this level of intervention, it is not always possible to avoid some load loss, but the loss is limited.

3- Finally, on the last level, direct detection of extreme contingencies is required. To ensure adequate efficiency, rapid and massive generation rejection and remote load shedding is required after event detection to counter transient and dynamics phenomena. The load loss will be large but it is the only way to avoid a total power outage.

All generation rejection and load shedding actions are modulated in real time by the system control centre to reduce the amount of actions at the right value while maintaining a safe level of operation.

Table 2.2 shows the possible operation of each measure for the various extreme contingencies as well as the role played by each of them.

Table 2.2 : Possible automatic actions to counter extreme contingencies

MAIS: automatic 735 kV shunt reactor closing or tripping.

UFLS: underfrequency load shedding.

UVLS: undervoltage load shedding.

RPTC: generation rejection (GR), remote load shedding (RLS) and remote tripping of shunt reactor (RTS).

	EXTREME CONTINGENCIES	MAIS		UVLS	UFLS	RPTC		
		Closing	Tripping			Limited GR	GR and RLS	RTS
LEVEL 1 Limited action	Loss of two series or parallel 735 kV lines		*	*		*		*
	AC-DC event : loss of a bipolar DC line with loss of one 735 kV line		*	*		*		*
LEVEL 2 Use of curative type SPS	Loss of a generation station or generation unit at a station	*			*			
	Sudden dropping of a major load center	*						
	Unintended operation of a Special Protection System	*			*			
LEVEL 3 Use of SPS with massive actions	Loss of one or two lines and bypass of all series capacitors on the remaining lines in the same corridor		*	*	*		*	*
	Loss of all 735 kV lines in a corridor	*			*		*	
	Loss of all 735 kV lines emanating from a substation	*			*		*	

2.3 BANGLADESH POWER DEVELOPMENT BOARD´S DEFENSE PLAN PROPOSAL

The Power System owned by Bangladesh Power Development Board (BPDB), the sole public utility for generation and transmission in Bangladesh, has evolved to a vulnerable position. The main reason is lack of funds for timely rehabilitation of the existing generation plants and transmission lines and installation of new ones to meet a demand that increases every year by approximately 10%. Also, unavoidable concentration of the majority of power stations in the country's eastern part, where indigenous gas and hydro reserves are located, has contributed to the vulnerability of this system. The consequent problems facing the operation of the BPDB system are drastic load shedding, lack of spinning reserve, low-voltage profile, and frequent disruptions varying from wide-area outages to total blackouts. Blackouts like the one that occurred on June 20, 1998 add to the inconveniences to consumers and cause irreparable loss to the national economy over and above what is caused by daily load shedding. If the BPDB system collapses for a fault, the generating units are restored one by one and synchronized with each other, taking almost a full day between the occurrence of the grid failure and the restoration of a sizable part. Also, considerable expenses are incurred in restoring the power plants from stalled conditions.

2.3.1 Main characteristics of the BPDB system

The BPDB grid is comprised of 24 power stations connected primarily by a network of 132 kV transmission lines plus a few 230 kV lines. The grid area consists of two geographical zones – the East and West, interconnected by a 230 kV double circuit line between GRSL-23 and ISHR-23 buses shown in red in **Figure 2.2** below. The generated electricity is distributed to approximately four million consumers of various categories by BPDB itself, Dhaka Electric Supply Authority (DESA), and Rural Electrification Board (REB).

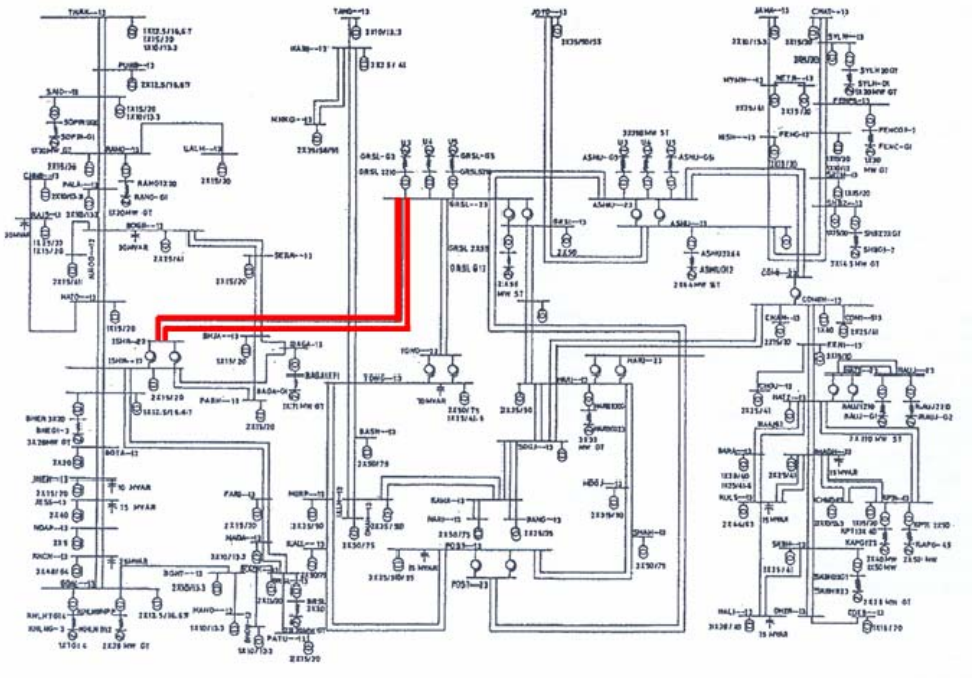


Figure 2.2 - BPDB transmission System 1998

2.3.2 Philosophy and Design Principles of the BPDB Defense Plan

Incidents of several blackouts in grid systems of a number of developed countries have been reported in the literature. The remedial measures suggested comprise generation shed, load shed, and islanding. It appears that splitting a grid system into a number of independent islands can be considered either as a

last resort or as a primary measure depending upon the structure of the system. The basis for islanding is never unique but rather depends upon the utility in particular. In some systems, postfault oscillations of the generators are identified for their grouping before forming the boundaries of the islands against a specific fault. However, for a more vulnerable system like the BPDB grid, an easy-to-implement and affordable method needs to be developed for islanding.

To avert the blackouts that commonly affect the BPDB system an islanding scheme was proposed with a focus on the following aspects **[2-4]**:

1. investigation into the viability of post fault islanding at pre-specified buses and lines of the grid system;
2. determination of the criteria based on which the decision for islanding can be taken in real time and determination of the number of islands to avert blackout;
3. supplementation of islanding by generation/load shedding, subject to the nature and location of the fault.

2.3.3 Main Characteristics of the BPDB Defense Plan

For the definition of the islanding scheme, the number of intersection lines among the pre-specified sections of the BPDB system is five. It is being proposed that these intersection lines be monitored constantly in real time by installing microprocessors at the substations at both ends of the respective lines. These microprocessors will record the megawatt (active-power) flow in each line at a convenient sampling rate, e.g., 1 kHz. If the difference between the recorded flow values for two consecutive instants of time t_1 and t_2 exceeds a threshold at both ends of an intersection line, then this line will be tripped. Line tripping will initiate system islanding.

This approach is used because exceeding the set threshold value can be considered as a possibility of a fault occurrence that requires such islanding. However, to make sure that the changes in line megawatt flow do not correspond to a transient disturbance, the microprocessor will provide the decision on line tripping after a delay for a suitable interval of time. Since the stability analysis for the crucial fault (blackout) has revealed that clearing a fault through islanding in 0.08 s (i.e., four cycles) can prevent a blackout in the BPDB system, the delay time can be set as 1.5 cycles (i.e., 0.03 s) so that the remaining 0.05 s (i.e., 2.5 cycles) will be enough for the operation of the line breakers in the BPDB system.

Line active-power (megawatt) flows between five sections of the BPDB system were determined in the June 20, 1998 blackout case so as to propose an appropriate threshold percentage for the BPDB system. In addition to this, five more assumed fault cases have also been studied separately in a similar manner. Each of the assumed fault cases was considered as occurring on an internal line of the corresponding section under the same pre-fault scenario (i.e., the peak operating condition existing at 19:00 h of June 20, 1998). An inspection of all of the intersection lines between two instants $t_1 = 0$ and $t_2 = 0.01$ s have revealed that the threshold may be set as 15%. Evidently, this threshold can always be reviewed from time to time when there are changes in system topology and generation/demand growth. Moreover, in the course of time, if wide differences between the peak and off-peak operating conditions of the system arise, a separate threshold may also be contemplated for faults occurring during off-peak hours.

The number of islands to be formed for a fault will depend upon the number of intersection lines in which the change in line flow between two sampling instants exceeds the set threshold. It should be noted that, if for a fault case, the active-power flow changes in all the specified five intersection lines are 15% or less, then the system will not be islanded for that fault case. So upon implementing the proposed scheme, a fault occurring in the BPDB system will result in two to five islands or none.

It is noteworthy that an alternative to islanding is, keeping the system intact where possible and resorting to load/generation shedding. Studies on this alternative option have also been made for each of the five assumed fault cases. Studies, for any fault case that causes more than 15% change in megawatt flow in an intersection line between two sampling instants, have revealed that mere load/generation shedding without islanding cannot avert blackout in the BPDB system.

For the implementation of load and generation switching to supplement islanding, there are two points to be considered:

- how much generation shed and/or load shed/injection is needed;
- how to realize these sheds or injections immediately after fault clearing through islanding

It was proposed that, to determine the amount and location of generation shed and load switching, transient stability studies could be made by the National Control Center. These studies would be performed in advance as part of security analysis for different cases and faults in the system, each with various numbers of islands under the same peak operating condition. The results obtained could be transferred to the computers of each area (section) control center. As soon as the grid system is islanded, the area control center transmits signals to its respective grid substations and generating unit control rooms to shed load and/or decrease generation in proportions near the values already obtained from security analysis. It should be noted that the decisions on load/generation shed or injection corresponding to peak-hours' operating condition usually act as guidelines for off-peak hours' operating conditions when the system is less constrained.

The underlying philosophy of the proposed scheme of islanding may also be implemented in other power systems using existing hierarchies of computerized control.

2.4 GREATER BUENOS AIRES´ DEFENSE PLAN

The Argentinean Interconnected Electric System (SADI) is vulnerable to some kinds of multiple contingencies. Therefore, because of that situation, the Independent System Administrator for the Wholesale Electricity Market of Argentina (CAMMESA) has decided that the respective market participants would study the extreme measures that were necessary in order to avoid the collapse in the different regions and to reduce the risk of a more generalized blackout. The electric system of the "Greater Buenos Aires" is one of such regions. This aim was achieved by the implementation of a defense plan called "Proyecto de lslas y Arranque en Negro" (Project for islanding and black start). The objective of this project is the alleviation of the consequences derived from the above mentioned extreme contingencies **[2-5**].

2.4.1 Characteristics of the Argentinean Interconnected System (SADI) and its Greater Buenos Aires Region

The Argentinean Interconnected System (SADI) is a set of transmission, transformation, compensation and operation facilities which form the High Voltage Transmission System (HVTS). Part of those facilities composes the Regional Transmission System (RTS) in the different geographic regions in Argentina.

The HVTS is a strategic network of 8,700 km of 500 kV transmission lines and 32 substations that transmits electricity from remote generation centers to consumers regions. The total installed generation capacity is 20,711 MW. The participation of the different generation types, to satisfy the demand during the year 2000, was: thermal generation 53%, hydraulic generation 40% and nuclear generation 7 %.

The main hydraulic power generation stations are located at the Comahue region, in the southwest part of the Argentina, with an installed capacity of 4,485 MW. Also, Salto Grande Hydro Power Plant, in the eastern region, and Yacyretá Hydro Power Plant, in the northeast region, both with a total power of 5,290 MW.

The SADI's major loads are located in the Greater Buenos Aires region representing almost 44% of the whole demand. The remaining load of the Buenos Aires Province contributes 13% and loads of the eastern region (the provinces of Santa Fe and Entre Rios) contributes 13%, reaching 70% of the total load.

The Comahue -Buenos Aires corridor has four 500 kV lines, with an extension of more than 1000 km each, and shows a history of severe faults caused by storms, tornados, vandalism or sabotage, etc.

Of similar nature and more bigger load supplying in intermediate substations are the transmission networks from Yacyretá-Salto Grande to Buenos Aires Since this corridor has limitations to transfer

electric power in case of both the line contingency or its elements, there are automatic generation disconnection schemes and underfrequency load shedding to maintain the SADI's stability.

The Greater Buenos Aires Region has a corridor of two 500 kV transmission lines which links the three 500/220 kV substations of Abasto, Ezeiza and Rodríguez. Those substations are the gate to the distribution electric systems of the EDESUR and EDENOR companies. The substations Ezeiza and Abasto, of EDESUR, are connected with the corridor Comahue –Buenos Aires, the major energy importer to the region.

The substation Rodríguez, of EDENOR, is connected with the Litoral -Buenos Aires corridor, of smaller energy import volume to the area. The substations Abasto, Ezeiza and Rodríguez are interconnected by 220 and 132 kV networks to the load substations and to the existent generating power stations in the region. In particular, from the Abasto substation there is a link at 220 kV to the distribution network of the EDELAP Company. The substation Ezeiza has six synchronous compensators rated +125/-120 MVAr each, while the substation Rodríguez has two static shunt compensators rated +160/-266 MVAr each. This compensation is used to maintain the voltage profile on 500 kV level. In the region an installed thermal power of 5786 MW exists, constituted by five combined cycles (3417 MW), conventional thermal machines (2110 MW) and gas turbines (259 MW). The maximum demand for the year 2000 has been of approximately 6000 MW, with about 5600 MW distributed almost equally between EDENOR and EDESUR and the rest, 400 MW, for EDELAP.

2.4.2 Philosophy and Design Principles of the Defense Plan

As outlined above, the electric energy systems can be affected by highly severe perturbations that could lead to a cascade of automatic actions with a possible uncontrolled network splitting and a consequent worsening of power quality for the final customers. In stressed system conditions, this may eventually cause partial or total blackout. These kinds of events can happen because in the common practice very severe perturbations are not included in the design of the electric systems, due to their low probability of occurrence or, merely, because they are a consequence of a cascade of multiple faults in the protection systems and controls that rarely occur. Due to the SADI electrical structure, certain types of events (contingencies) exist, that make the complete system vulnerable. As was pointed out before, the SADI is composed of different interconnected areas.

Therefore, it has been decided to set up an extreme backup barrier that is designed to avoid the collapse of some areas and reduce the risk of a more generalized blackout. The aim of the defense plan for the Greater Buenos Aires Region was to save it from collapse when a low probability fault occurs or a cascade fault happens on the transmission network. The objective of this project was the alleviation of the consequences derived by the extreme contingencies above mentioned. The adopted solutions were based on a mix of preventive and/or corrective measures, which shall be undertaken in real time, triggered by the early detection of the fault consequences. The main function of this backup barrier is to keep in operation as much as possible the generating units together with the associated loads even in the most critical situations. The experience acquired with the defense plan of the Greater Buenos Aires represents an outstanding project valuable for the implementation of a safeguard program oriented to preserve the security and power quality within a liberalized electric energy market, as in the case of the wholesale electricity market of Argentina.

The international scientific literature shows some experiences relevant to the implementation of defense plans against major perturbations. The policy applied for the determination of the control system procedures has been recently changed according to the following two objectives: (1) keeping the network meshed by means of the control of the so-called "critical sections" and (2) maintaining a generation-demand balance. This is achieved through a controlled load-shedding or an automatic generation disconnection (e.g.: the Italian case), splitting the system into islands that are balanced both in active and reactive power. Load and generation balance is expected to keep, as much as possible, the generators in operation, leaving consequently a sufficient regulating capability to obtain one or more islands in acceptable operating conditions. This will make easier the subsequent reconnection with the main transmission system.

2.4.3 Main Characteristics of the Greater Buenos Aires Defense Plan

The solution adopted for the electric system of the Greater Buenos Aires region is based on a mix of both the policies above outlined, obtaining a scheme structured on three hierarchical levels of controls. The controlled creation of the island starts from the detection of the incipient system collapse, based on the monitoring of the transient behavior of quantities, such as frequency and voltage, in the border stations of the regional island. These transients allow detecting, in an early stage, the system evolution towards a dangerous condition, and pointing out in an unequivocal way the need and suitability to start a controlled regional splitting from the main Argentinean Interconnected System. Once the electric island has been defined and created, it is necessary to warrant the most appropriate operating conditions allowing the regulating devices to properly operate in an islanded mode, with the aim of recovering the frequency and voltage close to the normal values for the subsequent system reconnection.

If a stable regional islanded operation is not feasible, then a second control level is triggered. This level involves a further controlled splitting up of the regional island in smaller subsystems, which, in their turn, will act to find a new stable operating state. All the subsystems not able to reach a stable condition will achieve the balance by creating "load islands" associated to the power plants. These load islands are obtained through the intervention of a third hierarchical control level. The final aim of the defense plan ensures the keeping in operation of as many generators as possible following a highly severe perturbation that affects the integrity of the overall system. As a consequence, the spreading of the fault effect is stopped and the risk of a generalized blackout is minimized.

Moreover, through suitable system separation, the subsequent reconnection can be achieved with a minimum time delay. The automatic systems designed for the creation of the balanced island in the Greater Buenos Aires region are suitably coordinated with the load shedding plans, already installed and based on minimum frequency and minimum voltage thresholds. Furthermore, the actions of the automatic system are integrated with other automatic devices able to change the network topology achieving at the end the compliance with the quality indexes established by the Independent System Administrator for the Wholesale Electricity Market of Argentina.

Bearing in mind the main objective of avoiding a partial or complete blackout, several control methods were applied. The control methods perform preventative actions capable of driving the regional system to safe operational conditions. In this framework, the automatic systems were designed with the aim of operating in a coordinated manner with other existing protection devices, such as the underfrequency load shedding scheme. In addition, complementary automatic systems were also considered for performing network topology changes able to keep a proper balance between generation and load within the islands. A practical implementation of the Defense Plan requires the automatic systems be able to perform preventive and/or corrective actions with the following characteristics:

- Centralized control logic based on PLC that handles analog variables taken from meters (voltage, frequency, real power, etc.) and local digital signals (network topology and station equipment status).
- Local actions following detection of an event with highest severity.
- Sending of local signals to remote locations (tripping signals and transmission line status).

Figure 2.3 presents an overview of the stations participating in the Defense Plan. The first hierarchical level comprises the three main 500 kV stations (Ezeiza, Rodriguez, Abasto) supplying the Greater Buenos Aires region from the rest of the interconnected system. These stations are located on the borderline of the regional island. Redundant PLC, capable of detecting the necessary conditions to create the islands, were planned to be installed in nine additional stations located in the inner part of the network. These control devices constitute the second control level, and are linked to each other by independent and redundant communication channels capable of performing a permanent interchange of signals between the PLC. These channels will be carrying tripping signals to 36 substations at the distribution level, belonging to the third hierarchical level.

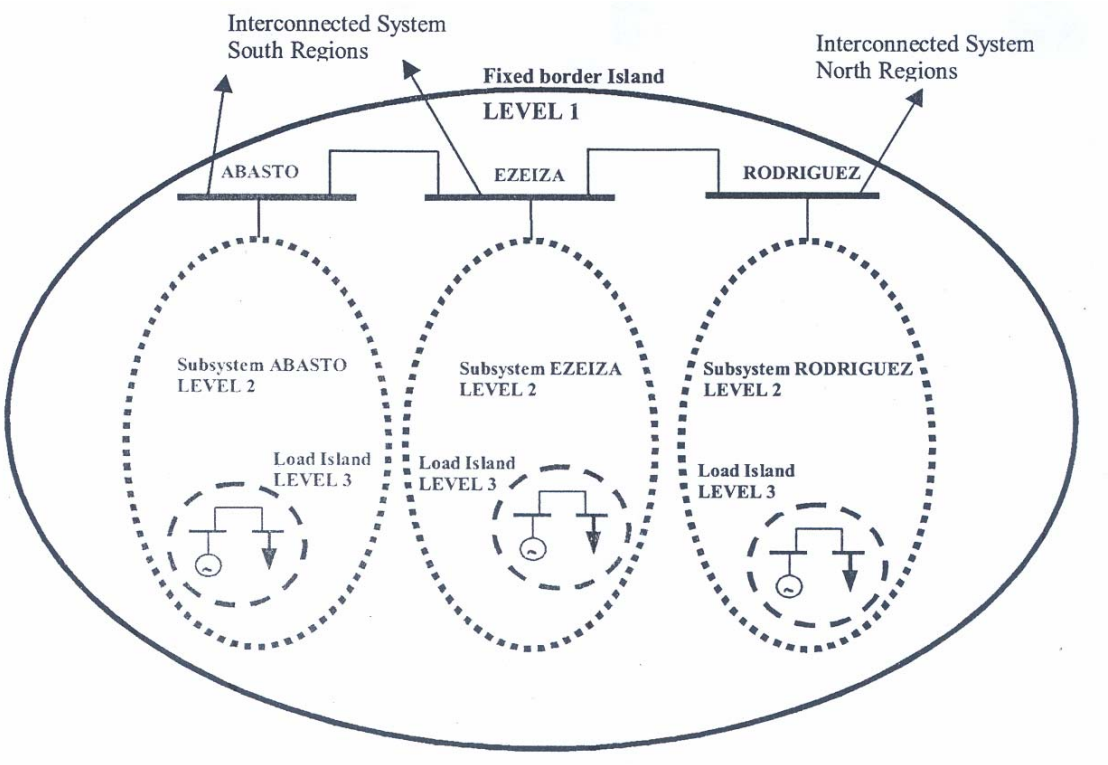


Figure 2.3 - Simplified scheme of the three hierarchical levels for the GBA region

Redundant PLC pertaining to the first and second hierarchical levels will be in charge of the following tasks :

- Local monitoring of relevant electrical variables from the power system, assuring an early and proper detection of a system collapse condition.
- Collapse condition acknowledgement by processing analog (voltage and frequency) and digital (network topology and substation equipment status) signals using suitable control logic.
- Real time decision making process for creation of the islands in some or all of the three hierarchical levels.
- Perform local actions facing the detection of an event
- Send local signals to remote sites, such as tripping signals and transmission line status.

Precise reliability targets were established for the designs of the Defense Plan to assure an accurate detection of the collapse conditions. The Programmable Logic Controller (PLC) located in the main 500 kV stations will be responsible for the detection of the events necessary to trigger the first defense actions. These actions mainly consist in a fast separation of the Greater Buenos Aires regional network from the rest of the Argentinean Interconnected System. Next, these PLCs will be initiating the process for creating subsystems or "load islands" in the inner part of Greater Buenos Aires regional network, every time it is not possible to keep a proper balance between local generation and load.

A dedicated and independent communication system should be implemented that achieves a reliable and efficient performance of the Defense Plan. Dependability and security constraints of the design establish that it is mandatory to keep the traveling time below 40 ms for signals transferred between sites. Transmission speed, distance between sites, security and redundancy requirements imposed to the

scheme, determined that optical fibers technology was the most suitable and convenient solution for this application.

The expected performance of the Defense Plan is measured in terms of the probability of success of each one of the three hierarchical levels of the scheme. In this context, 99.90% is the probability of success for the first level, 99.80% for the second and 98.80% for the "load islands", respectively. Therefore, the probability of successful operation of the whole scheme will be conditioned by the formation of "load islands", the third and last backup instance of the Defense Plan. This resulting figure is above the threshold of 98% of success established by the Independent System Administrator as the design acceptance limit. This level is lower than the maximum of $5x10^{-6}$ p.u. established by the Independent System Administrator for the acceptance of the design. Notice that performance assessment calculations were based on the assumption of having a blackout every ten years, assuming a mean duration of eight hours per event until complete service restoration is achieved to all users within the Greater Buenos Aires region.

In conclusion, the electric energy systems can be seriously affected by extreme contingencies that could lead to a cascade of automatic actions with a possible uncontrolled network splitting and a consequent degradation of power quality for the Ímal customers. In stressed system conditions, this may eventually cause a partial or total blackout. These kinds of events can happen because, in common practice, very severe disturbances usually are not included in the design of the electric systems, due to their low probability of occurrence or, merely, because they are a consequence of a cascade of multiple faults in the protection systems and controls that rarely occur. The Argentinean Interconnected System is vulnerable to these kinds of contingencies, being the regional network of the "Greater Buenos Aires" one of the most seriously affected. Therefore, to overcome the problem, it has been decided to set up a Defense Plan that should be acting as an extreme backup barrier to allow avoiding the collapse of some areas and reducing the risk of a more generalized blackout, whenever a cascading outage occurs in the rest of the Argentinean Interconnected System.

The adopted solutions were based on a mix of preventive and/or corrective actions that are being initiated in real time and triggered by the early detection of the fault consequences. The main function of this backup barrier is to perform a fast separation of the Greater Buenos Aires regional network from the rest of the Argentinean Interconnected System, keeping in operation as much as possible the generating units remaining in the islands, together with the associated loads, even in the most adverse conditions. The feasibility studies performed for the design of the Defense Plan were approved in general by the Independent System Administrator, who is responsible for the planning of the future works to be conducted for the implementation of the plan. This project is part of a more general safeguard program oriented to preserve the security and power quality within the Argentinean Wholesale Electricity Market. The Independent System Administrator is leading the efforts to achieve the objectives of this program, complying with a directive of the Secretary of Energy of the Federal Government. Full funding of the project is supported by all market participants.

2.5 NORTH CHINA REMEDIAL ACTION SCHEMES

As the load is increasing, some new plants such as Daqi, Fengzhen and Shalingzi Power Plants have been developed to achieve load/generation balance. However, coal resources of North China are located in the west region, so it is necessary to transfer the power by long distance transmission lines. New 500 kV transmission lines are required to be constructed from west resources to east load center, such as Fengzhen to Shalingzi, Daqi to Fengzhen and Datong to Fengzhen 500kV lines. Although such lines upgrade the power capability transferred to the load center, there will still be security and stability problems in the system during the periods of construction and line maintenance **[2-6**]

2.5.1 Characteristics of the 500kV power system of North China

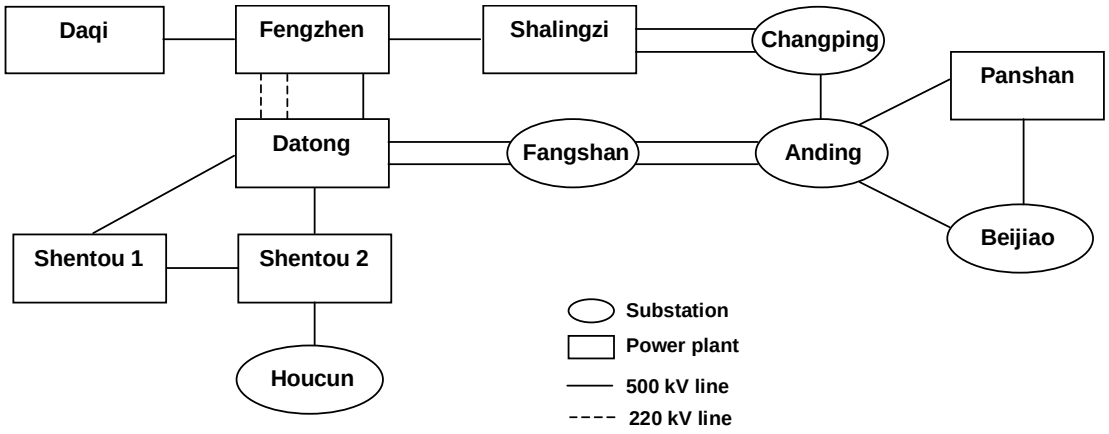


Figure 2.4 - 500kV power system of North China

Figure 2.4 shows the 500kV power system of North China. It accounts for one fourth of the total load supplied from west sources to east load center through Fengzhen to Shalingzi and Datong to Fangshan transmission lines. These long transmission lines will transfer much power flow, which will result in the following problems:

a. Overloading problems :

Two 220 kV transmission lines and main transformer in Fengzhen will be over the thermal ratings if the Fengzhen to Shalingzi 500 kV line is suddenly disconnected while Fengzhen to Datong 500 kV line being maintained;

- When Datong to Fangshan 500 kV single line is operating, if disconnection happens to it, the main transformer in Datong and in Fengzhen will be over the thermal ratings while Fengzhen to Datong 500 kV line being maintained;
- If 500 kV lines from Shalingzi to Changping or Daqi to Fengzhen are disconnected, the same happen to the main transformers in Shalingzi and Daqi.

b. Stability problems :

According to the planning criteria, each line has a limitation under the first contingency. If the transfer of power is over the limit, it will cause severely stable results while fault occurs in the system. Considering the second contingencies or multiple contingencies, the stability limitation will be lower. The power transfer on 500 kV lines from Datong to Fangshan, Fengzhen to Shalingzi, Shalingzi to Changping and Daqi to Fengzben will be restricted under the limitations, so that the transferring capability from west resources to east load center will be affected.

2.5.2 Philosophy and Design Principles

500 kV transmission lines play an important role in North China power system. The two major channels transferring power from west to east are Datong-Fangshan double circuit 500 kV transmission lines and Daqi-FengZhen, Fengzhen-Shalingzi 500kV transmission lines, which are connected by four power plants of Shalingzi, Fengzhen, Datong and Daqi. In order to ensure safe and stable operation, three measures may be taken:

- Construct new transmission lines;
- Reduce the power flow on the lines;
- Adopt remedial action schemes.

As we know, new transmission lines require financing. It is difficult to improve the network only by investment during development. Although it is safe to reduce the power transferred on the lines and operate below the transferring limit in order to guarantee stability, system efficiency may not be obtained for the output of some power plants should be limited Remedial action schemes can save much costs and increase the transferring power, improve system security and stable operation during the network construction.

Table 2.3 gives different investments, security and stability of operation and efficiency. The new 500 kV line cost is approximately $180,000 dollars per kilometer at present. Remedial action schemes need much less investment than new lines. Power reduction on the tie lines may limit the output of power plants, so the operating efficiency will be affected. Comparing the cases in Table 3, although all cases can satisfy the security and stability requirement, Case 3 (use of remedial action schemes) is the best option. It shows that both economy and reliability should be considered when the problems of system security and stability are under study.

Table 2.3 - Comparison of solutions

Items	Investment (million US$)	Stability & Security for system	Economy
Case 1- New lines	36	satisfied	bad
Case 2 -Tie line power reduction	-	satisfied	bad
Case 3 -Remedial action schemes	0.13	satisfied	good

The philosophy of the design for remedial action schemes was to take two measures:

- Reduce the output of generators or trip the generators when the facilities are overloaded.
- Trip the generators under the first contingency or second contingencies.

2.5.3 Main Characteristics of the remedial schemes

The remedial action schemes have been designed as shown in **Figure 2.5**.

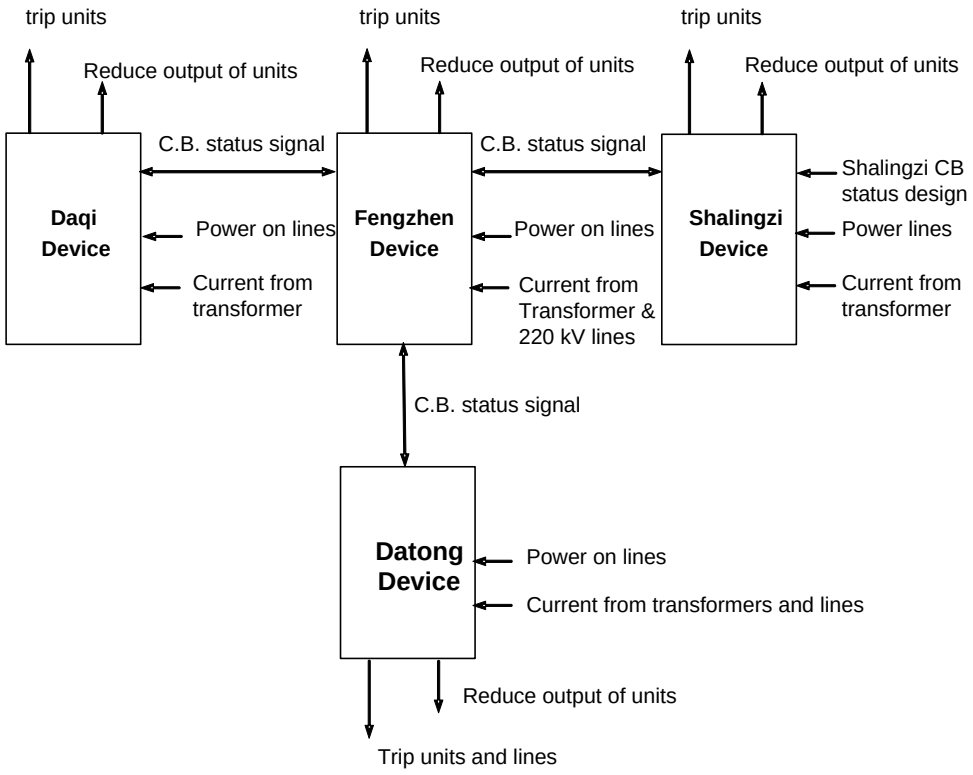


Figure 2.5 – Remedial action schemes

The remedial action schemes deal with the four power plants, seven 500 kV transmission lines and two 200kV transmission lines. The devices are designed under the simple, local, relatively independent and practical principles. The messages among the devices are only digital signals. Digital communication was selected because of its high-speed data transmission capability.

Two measures are taken: overload control and over power flow control (on the 500 kV transmission lines).

2.5.3.1 Overload Control

According to the specifications for the transformer and transmission lines (maximum current allowance), overload time and peripheral temperature are monitored. There are four setting values according to the over-current inverse-time characteristic:

- Alarm due to overload;
- Reduction of generator output, if overload can't be eliminated, and tripping of the units through a long delay time;
- Reduction of the generator output, if overload can't be eliminated, and tripping of the units through a short delay time;
- Tripping the units instantly.

2.5.3.2 Over Power Flow Control

As we know, there is a certain power transfer limitation for transmission lines. If the power transfer is over this limit, the system will be unstable when a fault occurs on a transmission line, and the limitation will be different if the network configuration is changed. So the control measures will be:

- Tripping units or lines according to the network configurations
- Tripping units or lines according to the type of fault (500kV system)

For each power plant a set of measures was devised as shown in **Table 2.4** :

Table 2.4 - Measures according to the severity of the contingencies

Power Plant	First contingency	Second contingencies	Third contingencies
Shalingzi	-	trip 2 units of 300 MW	trip 3 units of 300 MW
Fengzhen	trip 2 units of 200 MW	-	-
Datong	trip 2 units of 200 MW	disconnection of the 500kV and two circuit 220 kV lines from Fengzhen to Datong	-
Daqi	trip 2 units of 330 MW	-	-

In addition to the remedial action schemes, an out of step protection is to be installed in Fengzhen Power Plant as a backup measure and over-frequency relays are installed in the other power plants. Underfrequency and undervoltage relays are widely installed in substations to correct the variations of frequency or voltage.

The hardware of the devices in all substations or in power plants, which are based on industrial control computers, is similar. The various functions are completed by software. Both functions of overload and stability control are combined in the device. Local control principles were adopted:

- A fast relay for detecting small current on the lines,
- A "two out of three" logic as the initiating logic of stability control,
- Modification of settings on line,
- Self-checking if the device is faulty,
- Adaptive operating configurations and low cost for the device.

The expected operational results of the remedial actions schemes for the 500kV power system of North China are:

- Increase transfer capability on the tie lines;
- Prevent system from instability and facilities from overload;
- Increase operational efficiency;
- Decrease investment for new line construction;
- Meet the operational and reliability requirements of the system.

2.6 BRAZILIAN INTERCONNECTED POWER SYSTEM´S DEFENSE PLAN

Since ONS (Operador Nacional do Sistema Elétrico), the Brazilian Independent System Operator, was established, it has been concentrating efforts on the analysis of the Brazilian Interconnected Power System (BIPS). The objective of the analysis is to improve its operational security.

The analysis of two large disturbances that took place on March 1999 and January 2002 shows that all the ONS concerns about this subject are quite relevant. Despite some differences between such events, the good results of the work done in that meantime were encouraging. The main difference between these two disturbances lies on the relatively small area affected by the last one, which had its propagation restricted by previous measures that stemmed from the analysis of the first event.

The work – a huge effort – done so far has been directed in enhancing the BIPS capability to withstand extreme contingencies, that are usually started by multiple faults or by single faults associated to multiple disconnections or by successive disconnections of transmission components.

As a consequence, ONS is firmly dedicated to the preservation of BIPS integrity through the implementation of automatic measures, which were conceived under the concepts of simplicity, reliability and security, and takes into account all the possible extreme contingencies that could happen.

2.6.1 Characteristics of the Brazilian Interconnected Power System (BIPS)

The Brazilian Interconnected System has a total installed capacity of 75,000 MW (85% hydraulic) to meet a maximum demand on the order of 55,000 MW. To transport energy from the distant power plants, predominantly located in the interior of the country, to the load centers situated closer to the Atlantic coast, 73 000 km of transmission lines were constructed. They are interconnecting regions with high climatic diversities, allowing for hydrothermal optimization of dispatches and optimal use of reservoir storage, and by exploring basin hydrological complementarities. The optimal operation of the reservoirs adds synergic gains (more than 20% of the system assured energy) but requires the transferring of large blocks of energy between the BIPS subsystems. The peculiar characteristics of the BIPS make the matter of security a vital question for the operation of the system. The multiple losses of such highly loaded interconnecting transmission lines cause voltage and frequency deviations, accompanied by power oscillations that may lead to cascading outage of transmission elements ending up with system collapse. **Figure 2.6** is a map of Brazil and shows the extent of the BIPS.

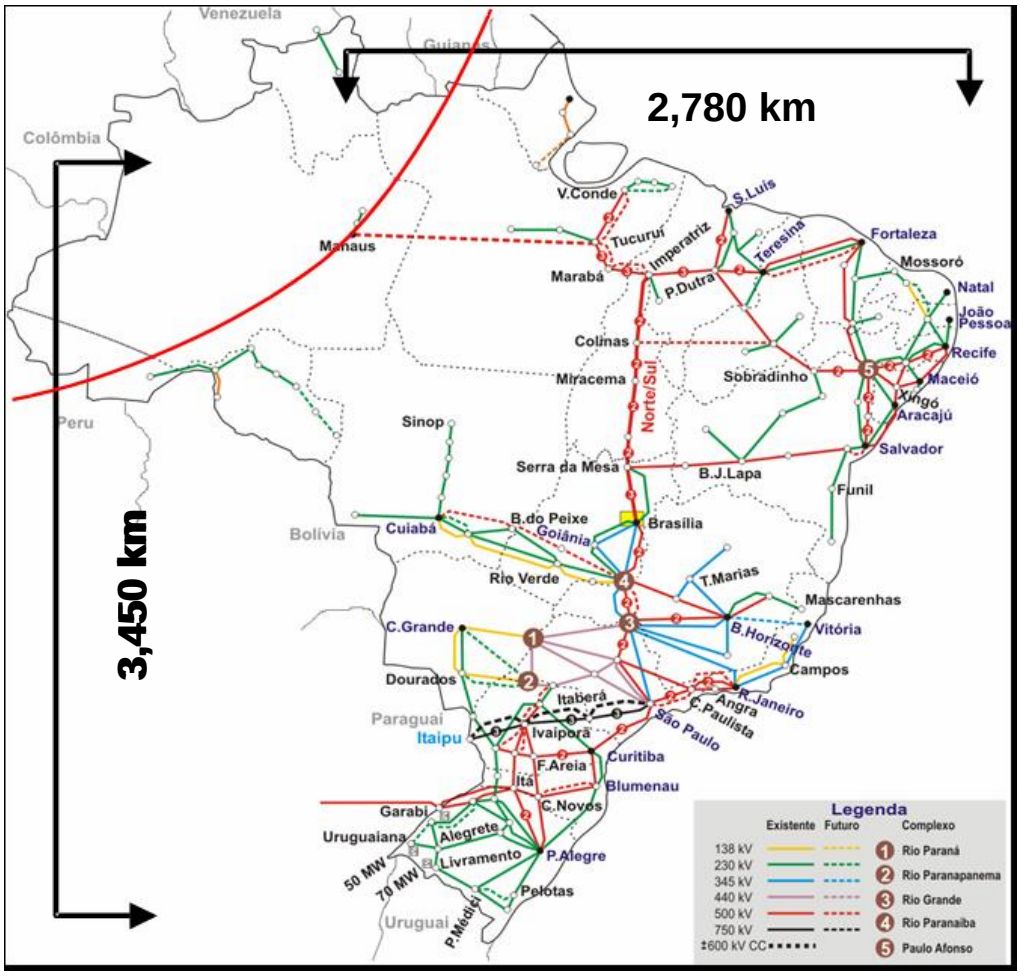


Figure 2.6 – Brazilian Interconnected Power System

2.6.2 Philosophy and Design Principles of the BIPS Defense Plan

Taking into consideration that there is no power system immune to blackouts and that the upgrade of the planning criterion from N-1 to N-2 would have a very high implementation cost, the BIPS Defense Plan which is being developed by ONS is based on three pillars **[2-7]**:

- Actions aimed to minimize the probability of the occurrence of large disturbances. Such measures are effective in reducing the severity of the events.
- Actions aimed to minimize the propagation of the unavoidable disturbances. Such measures are effective in restricting the immediate effects of the events.
- Actions aimed to optimize the restoring times. These measures are effective in reducing the load restoring times to levels that are considered acceptable from the consumer's point of view.

These three pillars may be visualized on **Figure 2.7**.

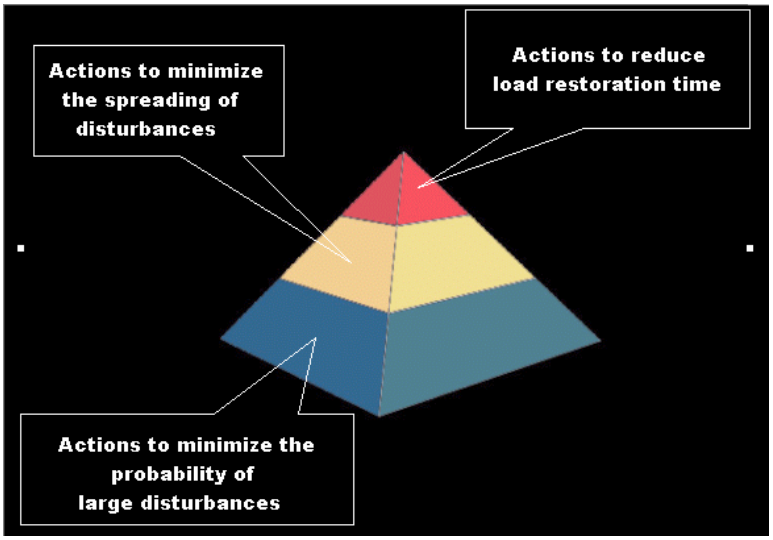


Figure 2.7 – The Pillars of BIPS Defense Plan

Regarding this last aspect, it is important to take into account the prolonged restoring period as one of the immediate negative effects of a blackout. The adverse consequences that are detrimental to the image of electricity industry under public opinion concerns are exponentially related to the restoring time, as shown in **Figure 2.8**.

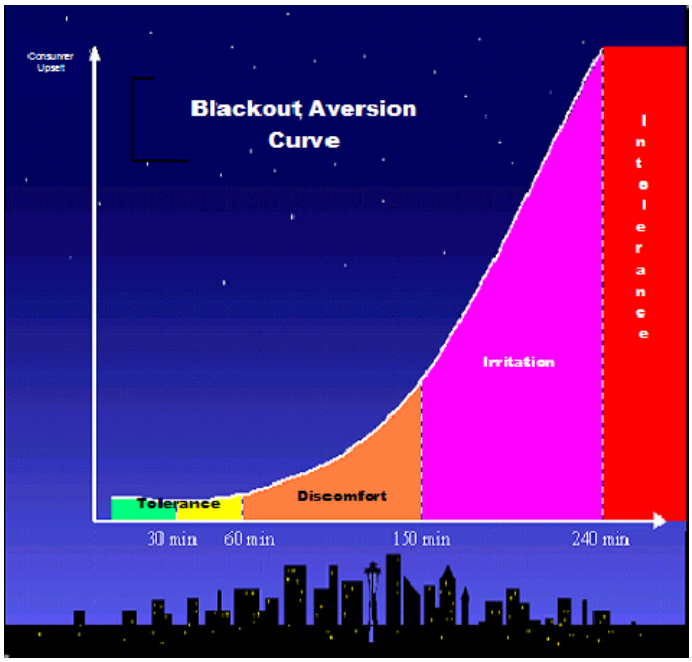


Figure 2.8 – Societal Reaction to Blackouts

2.6.3 Main Characteristics of the BIPS Defense Plan

The BIPS Defense Plan is based on a permanent concern over all time frames: expansion planning, operation planning, operation scheduling, real time operation and post operation. It comprises actions according to the three basic pillars stated above.

2.6.3.1 Action Aimed to Minimize the Probability of the Occurrence of Large Disturbances

- Studies of the definition of transmission reinforcements and reactive compensation for BIPS, to accomplish required Grid Procedures.
- Definition of the minimum requirements for the connection of new generators to BIPS (characteristics of excitation systems, power system stabilizer, generator capability characteristic and so on) as stated on the Grid Procedures.
- Periodic reevaluation of minimum requirements for new facilities (e.g. as a consequence of technological innovations).
- Improvement of intrinsic characteristics of the existing substations, by means of refurbishing busbar configurations, transposition of circuits and other measures aimed to reduce the impact of a large disturbance.
- Elimination of remote back-up protection by means of redundant protection schemes on each component, unit protection on the busbars and breaker failure protection.
- Implementation of automatic reclosing on all EHV aerial transmission lines and improvement of existing three-pole reclosing schemes into three/single-pole reclosing schemes.
- Yearly revision of the controller settings in BIPS major power plants and upgrading of controllers;
- Definition of an overload capability criterion for lines and equipment when subjected to emergency conditions.
- Identification of strategic installations related to system performance.
- Revision of specifications and setting policies for line protection, to reduce the influence of three-phase balanced phenomena, avoiding the disturbance propagation but maintaining the sensitivity to resistive ground faults.
- Evolution of the electrical studies criterion, according to the BIPS requirements and the international state of the art.
- Evolution of the procedures for the authorization of programmed disconnections of network elements.
- Implementation of a software tool to evaluate the BIPS security level, so that decisions can be made within the proper times and operation may be performed far away from risky conditions.
- Thorough disturbance analysis, reproducing the disturbances through digital tools for the identification of corrective measures and preventive actions, including a permanent follow-up of recommendations implementation.
- Statistical analysis and protection performance evaluation systems.
- Implementation of short and long term dynamic monitoring systems to increase the system's overview.
- Implementation of the coordinated automatic voltage control in strategic areas of the system.
- Identification of facilities which are vulnerable to acts of vandalism/terrorism.

2.6.3.2 Action Aimed to Minimize the Propagation of the Unavoidable Disturbances

- Enhancement of the use of Special Protection Schemes (SPS).
- Installation and/or adequate use of out-of-step tripping protections.

2.6.3.3 Action Aimed to Optimize the Restoring Times

- Revision of BIPS planning under the viewpoint of system's restoration (identification of additional shunt reactors aimed to ease the restoring process).
- Extensive use of underfrequency islanding for small and average sized hydro power plants with local loads.
- Identification of new power plants for the installation of black-start devices.
- Identification of substations that must be operated by attendants who can attend to and assist with the restoration process, avoiding the susceptibility to failures of telecommand and automatisms that may occur in unmanned substations.
- Identification of the BIPS vital substations, which will be subjected to a differentiated maintenance plan.
- Implementation of a schedule of periodic check-up tests of the black start devices in the power plants capable of self re-energization.
- Creation of qualification and training programs for operators and dispatchers.

2.6.4 Present status of the BIPS Defense Plan **[2-8]**

After the 1999 blackout, many actions were developed in order to provide a higher operational security level for the BIPS. A diagnosis of potential problems within the major EHV substations led to various improvements aimed to reduce the impact of a given disturbance, as for instance, the splitting of busbars to decrease the number of circuits to be disconnected in case of a busbar fault or breaker failure. Many of such actions are already implemented, so the risk of large disturbances is considerably reduced nowadays in the Brazilian Interconnected Power System. Just to give some examples:

- Concerning the actions aimed to minimize the probability of the occurrence of large disturbances : the improvement of the BIPS protection for each voltage class, by means of the identification of the deficiencies of line protections that must be replaced by new ones and the rearrangement of busbar configurations where applicable in the EHV network, beginning with the substation where the March 1999 disturbance started and in all similar substations.
- Concerning the actions aimed to minimize the propagation of the unavoidable disturbances: a plan was put into practice for the optimization of the Power System Stabilizer (PSS) settings of the main power plants, Special Protection Systems revision and installation, as well as the intensification of the use of out-of-step protections in the interconnections of the subsystems, so as to prevent the propagation of a large disturbance from one area to another. These measures were so successful that a major disturbance occurred in January 2002 did not affect the North and Northeast subsystems.
- Concerning the actions aimed to minimize the restoring times: the time spent in the restoring processes of the main transmission trunks during all the blackouts from 1984 to 2003 was evaluated, considering the adopted concepts, philosophies and criteria, leading to specific recommendations of actions ranging from expansion planning to the real time operation. As result of this work, smaller restoring times are not only envisaged but are possible right now thanks to the installation of maneuverable shunt reactors and or exchange of existing reactors for larger ones.

Such actions, individually or in conjunction, have already showed positive results for the performance of the BIPS. More recently, disturbances as severe as or even more severe than those verified in the

March, 1999 and January, 2002 blackouts, did not result in any consequences for the BIPS, not having been even noticed by consumers. Among such disturbances the following should be highlighted:

□ **August, 2003**: total loss of the 750 kV Itaberá substation, due to the automatic disclosure of the six circuits connected to it;

□ **September, 2003**: simultaneous disconnection of four circuits (two incoming and two outgoing) associated to 750 kV Itaberá substation.

□ **December, 2003**: total loss of 440 kV Bauru substation, due to an internal fault at one of the 440 kV busbar section, resulting in the automatic disconnection of ten 440 kV transmission circuits and two 440/138 kV step-down transformers.

□ **February, 2004**: simultaneous loss of two 440 kV transmission circuits between Bauru and Jupiá substations, followed by the disconnection of the 440 kV transmission line from Agua Vermelha to Ilha Solteira.

□ **September, 2004**: total loss of 500/345 kV Jaguara substation, resulting in the tripping of four 500 kV transmission lines, four 345 kV transmission lines, three 500/345 kV step-down transformers and four generators.

2.7 RUSSIA´S PLAN TO INCREASE POWER EXCHANGES BETWEEN AREAS OF THE UNITED POWER SYSTEM (UPS) ACCORDING TO SECURITY CRITERIA

The transfer from centralized energy sector management in the frameworks of the vertical integrated utility to liberal energy market with the creation of such companies as generating companies, Federal Transmission Company, distribution and resale companies, requires several concerns to be dealt with. The most important one for the United Power System (UPS) of Russia conditions is the definition of the network constraints for active power exchanges between areas within the UPS of Russia. This is caused by the fact that the transmission capacity of interarea links is often equal to only 5-10% of the area total load. As the approved security criteria cause network constraints, it becomes necessary to reduce them by defining possible ways to increase the loading of certain electrical links. In the UPS of Russia certain measures were developed, and respective schemes were implemented, to increase the power transfer capability and thus decreasing network constraints. These measures can be used if the involved market participants provide specific of ancillary services, and operate according to established security criteria. **[2-9**]

2.7.1 Security criteria in the UPS of Russia

There are two groups of security criteria in the UPS of Russia. They define the maximum permissible active power flows through the controlled sections and thus the network limitations of power exchanges between areas. The first one determines the rated stability margin standards on active power and voltage in the normal (initial) regime. The second criteria group defines the requirements for power system stability and takes into account normative perturbations (disturbances), i.e. transient stability, active power and voltage stability margins, permissible current overloads for equipment in the stabilized post fault regimes. A more detailed view of these groups implies the following items (according to "Guidelines on Power System Stability"):

1. Active Power margin factor at any boundary (section) for the given network topology should be no less than 0.2 (the original author notation is retained in the following equations).

This item is defined as:

P_{Lim} - the active power flow limit of the aperiodic static stability in the section;

$$(P_{Lim} - P_{OS} - P_M)/P_M \geq 0{,}2 \text{ or}$$
$$P_M \leq (P_{Lim} - P_{OS})/1{,}2; \text{ where:}$$

P_M - maximum permissible power flow in the section;

P_{OS} - amplitude of irregular oscillations in the same section;

where :

$$P_{0S} = k \times \sqrt{\frac{P_{\Sigma 1} \times P_{\Sigma 2}}{P_{\Sigma 1} + P_{\Sigma 2}}}$$

$P_{\Sigma 1}$ and $P_{\Sigma 2}$ are, respectively, the total load (MW) of each considered subsystem on each side of the section;

k - automatic/manual regulation (limitation) of the power flow in the section.

k , $\sqrt{MW} = 0.75/1.5$

Remark: The flow limit practically always depends on a variety of factors, some of them are of weak influence and others influence it considerably. Therefore it is represented in the general case as a function of influencing parameters:

$$P_{Lim} = \Phi(\Pi_1, \Pi_2, \ldots)$$

2. Voltage margin factor at each node i in the initial regime should not be less than 0.15, or:

$$(U_i - U_{CR})/ U_i \geq 0{,}15 \text{ or } P_M \leq P\,(1{,}15\ U_{CR}) \text{ ; where :}$$

U_i - voltage at node i at the same regime;

U_{CR} - critical voltage at the same node.

Remark: This condition means that the required voltage margin, in the case of exhausted reserve of voltage control, should be maintained by reducing the amount of power transfer through the relevant section.

3. Power flow at any boundary should not exceed the transient stability limit for all normative disturbances:

$$P_M \leq P_{Lim}$$

4. Active power margin factor for any steady state post-fault regime appeared as a result of a normative disturbance should be no less than 0.08 i.e.:

$$(P_{Lim}^{P/f} - P_M - P_{0S})/P_M \geq 0{,}08 \quad \text{or} \quad P_M \leq (P_{Lim}^{P/f} - P_{0S})/\ 1{,}08$$

where $P_{Lim}^{P/f}$ is the aperiodic steady state stability limit at the considered section in the post fault regime in case of tripping of a network element.

When considering an emergency imbalance the same criterion is presented as:

$$P_M \leq (P_{Lim} - P_{OS} - K_{im} * P_{imb}) / 1{,}08 \text{ ;}$$

where :

P_{Lim} – from item 1;

$K_{im} * P_{imb}$ -power increment at the boundary caused by the normative emergency power imbalance P_{imb} (here – deficit);

$$K_{im} = \lambda_{re} * P_{re} / (\lambda_{re} * P_{re} + \lambda_{ex} * P_{ex})$$

Where: λ_{re}, λ_{ex}, P_{re}, P_{ex} – accordingly, regulating energies and total loads of the receiving and exporting subsystems.

5. *In every node i and in every steady state post-fault regime after any normative perturbation the voltage margin factor should be no less than 0.1, i.e :*

$$(U_i^{p/f} - U_{CR}) / U_i^{p/f} \geq 0{,}1 \text{ or}$$
$$P_M \leq P^{a/f}(U_i^{p/f} = 1{,}1\ U_{CR})$$

where : $U_i^{p/f}$ - voltage at node i in the steady state post-fault regime (one may consider the node with the maximum voltage deviation).

At the ante-fault regime the transfer $P^{a/f}$ dependence from the minimal voltage at the steady state post-fault regime is based upon the numerical simulation of the disturbances and is determined by varying the power flow values at the ante-fault regime.

6. Current load of any network element after any normative disturbance in the steady state post-fault regime should not exceed the values permissible for 20 minutes, i.e.:

$$P_M \leq P^{a/f}[\ I^{p/f}(t = 20 \text{ min})]$$

This dependence is formed using the same principles as in criterion 5. It is assumed that during this time (20 minutes), operators should correct the post-fault regime with reduced

stability margins and/or equipment overloads (criteria 4-6) so that criteria conditions 1 and 2 are satisfied in the given situation.

Therefore, the maximum permissible active power flow at the boundary, under study is defined by the minimal value of criteria 1-6.

It should be mentioned that permissible power exchanges in the UPS of Russia are generally defined by synchronous stability and very seldom are they limited by minimal voltages or current overloads. That is the origin for the complexity of calculation algorithm. Network constraints could have been significantly reduced through the elimination of the bottlenecks and includes building new transmission lines, introducing controllable reactive power compensation, etc. Taking into account large geographical spread of the UPS of Russia, this option will be time-consuming and will require considerable amounts of investment. Besides the construction of very long transmission lines together with huge investments, this is limited by the growing difficulties for obtaining right-of-way and line routes.

At the same time the adopted security criteria could be observed by the use of Special Protection Systems, called Emergency Control Automatics (ECA) in Russia, to prevent stability violations at dangerous disturbances. These devices were duly tested in the UPS of Russia and do not require considerable investments, the use of these devices could ease the network constraints in a considerable way.

2.7.2 Philosophy and Design Principles of Emergency Control Automatics (ECA) to increase permissible transfer in electrical links.

The purpose of ECA implementation is that at the initial situation (N-0) the transmission capacity is used fully (with the normative margins on criteria 1-2) and, if in case of normative disturbance (i.e. in situation N-1) criteria 3-6 are violated, control actions are used to satisfy the established system performance criteria.

Because of the large variety of dangerous disturbances this automatic system uses two fundamentally different control methods:

- **Event based :** the occurrence of a predetermined disturbance is detected, and, depending on the system configuration and operating conditions, specially selected control actions are realized. The advantage of this method is that control can start immediately at the occurrence of a disturbance. Consequently, this type of control is very effective.
- **Response based:** the output of given parameter values, and/or their combinations, from the given stability domains, that characterize the degree of instability risk, is detected and control actions are activated. The advantage of this method over the first one is that the disturbance, causing the violation of stability, is not detected. Detecting the disturbance would be a difficult and expensive task, as it would require a complex network of emergency transmission signals. On the other hand, the control is less efficient, because it is delayed, when the transient state parameters have already reached dangerous values.
- **Production shedding (generator tripping)** ΔG in the exporting part of the power system by switching-off the generator breakers and/or fast valving on thermal units. Steam turbines are discharged through a control system using two inputs: a fast acting electrohydraulic converter and a slow acting turbine control mechanism. The unloading of turbines can be short-term, or impulse, through partial shutting of the control valves for several seconds, only for the duration of the transient state, with a subsequent restoration to the initial production level. It can also be long-term, with the reduction of the boiler output, when the network is weakened, for the duration of the post-fault operating conditions, constraining the power flow based on static stability. The power of the turbines can be reduced to several levels.
- **Load shedding and starting fast power reserves** in the importing subsystem, are usually used together. In this case load shedding ensures the speed and fast power reserves allow to restore the power supply of the disconnected consumers. It is to notice

for the purposes of emergency control special customers are disconnected, the ones that would not suffer disruptions of their technological process during a short term disconnection (sufficient for the start up of the reserve), such as electric furnaces and aluminum smelters. It should be underlined that load shedding is a forced control action. There is no alternative to load shedding for the emergency control purposes, if the importing subsystem is considerably smaller than the exporting one as the reserve activation is insufficiently fast and generator dropping in the exporting subsystem in this case would have been inefficient from the point of view of power flow reduction through the section, that is:

$$K_{PS} = \Delta P / \Delta G = \lambda_{re} * P_{re} / (\lambda re * P_{re} + \lambda_{ex} * P_{ex});$$

Where if $P_{re} / P_{ex} \rightarrow 0$, then $K_{PS} \rightarrow 0$,

Where K_{PS}, ΔP, ΔG, λ_{re}, λ_{ex}, P_{re}, P_{ex} are, accordingly, efficiency factor of ΔG, active power flow change in the boundary, amount of production shedding in the exporting subsystem, regulating energy of the receiving and exporting subsystems, total load of the receiving and exporting subsystems.

The control actions are distinguished by their duration: short-term control actions for securing transient stability (criterion 3) and long-term action for establishing the rated stability margins (criteria 4-6). Often control actions are used in different combinations. For example, as it is mentioned above, for ensuring the rapidity load shedding is used in the receiving subsystem, fast power reserves would have been ineffective for maintaining stability because of insufficient rapidity (60-300 sec), but it allows a comparatively fast restoration of power supply of the disconnected consumers. To provide the selectivity, the automatic system is made as a multi-step device carrying out minimal necessary control actions for the given situation or the system uses balanced control actions (e.g. generator dropping and load shedding) for the reduction of the caused power imbalances in one area that could lead to stability violations in other areas.

2.7.3 Main Characteristics of Emergency Control Automatics (ECA) for increasing the permissible transfer in electrical links of UPS of Russia

Practical realization of these principles could be very different from the simplest, e.g. in local automatic systems, where the main parts of this system (starting, logic and executive units) could be combined into a single device to centralized regional systems, most sophisticated ones, where these units are evidently separated. The example of this advanced system is given in **Figure 2.9**. In pre-fault regime on the base of telemetry (TM, TS) the state estimation for the given scheme is carried out, preset disturbances are simulated and necessary control actions are calculated and stored for every disturbance cyclically (blue dashed lines show the ante-fault information). When a disturbance is detected the corresponding starting unit activates the associated control actions immediately (red solid lines show the post-fault information commands).

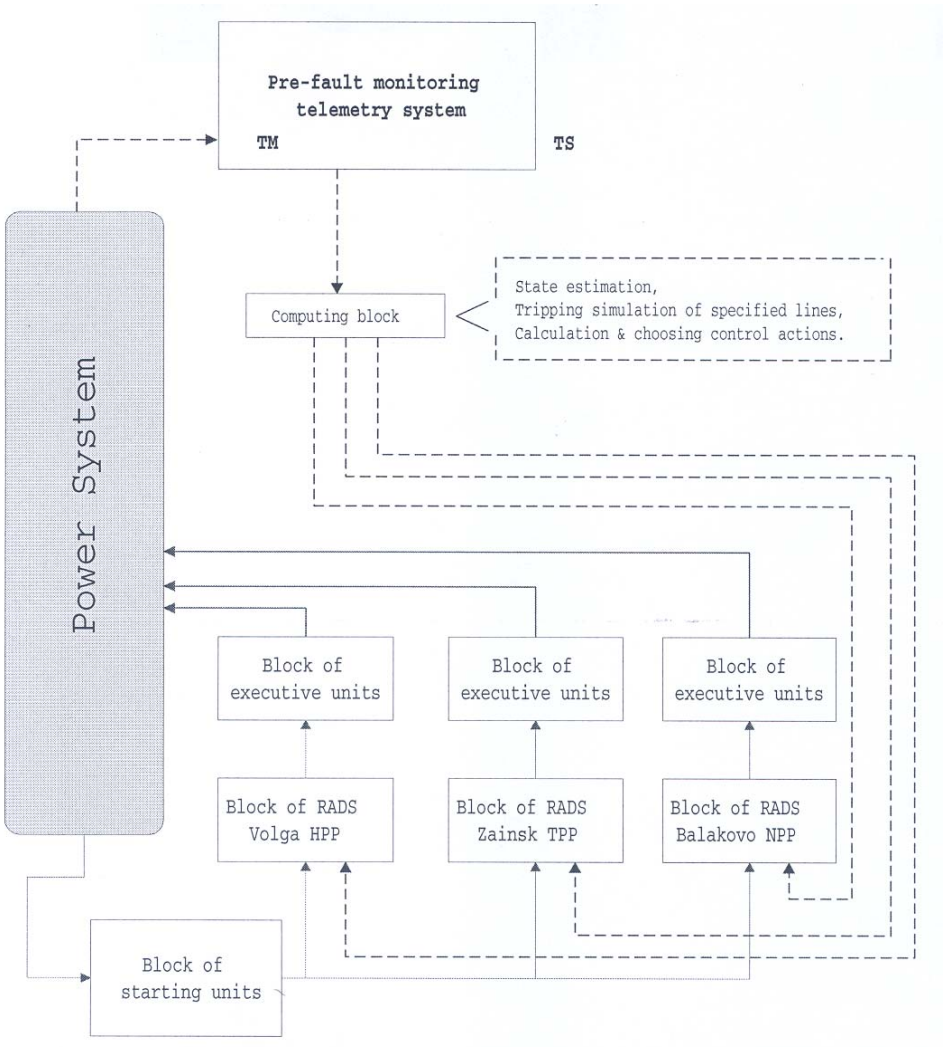


Figure 2.9 - Structural diagram of Central Emergency Control System of Middle Volga Integrated Power System (IPS) (RADS- remote unit for automatic control action dosage storing)

It is proposed to increase the power exchange via a bottleneck by implementing new ancillary service - ECA. Providers of this service could be:

1. Power plants, which provide their units for the needs of ECA (generation shedding, fast starting reserve, etc). The payment for them includes:

- Compensation cost for underproduction of electricity, because of generation reduction. It is defined by the probability of line tripping as well as power flow in the bottleneck and total restoration time;
- Additional operational and maintenance (O&M) costs due to the increase of the number of dynamic regimes;
- Installation and operational costs for ECA equipment.

2. Demand-side regulating consumers, which reduce their load upon ECA commands. The payment for them includes:

- Compensation of damage caused by underproduction;

- Compensation of additional O&M costs;
- Installation and operational costs for ECA equipment.

3. The Federal Grid company, which implements ECA on its facilities. Installation and operational costs for ECA equipment are covered at the expense of system service payments.

The ECA users are buyers, who are interested in increasing the power exchanges via the bottleneck because of the possibility to conclude contracts with cheaper producers in exporting area. This system service contracts are usually long-term, for one year or more.

Here is the simplest numerical example. Let us assume the following input data:

- Maximum load: exporting subsystem -15 GW;
- Importing subsystem - 40 GW;
- Interconnection by 3 lines (500 kV) with total length of 800 km.

According to first criteria group, the permissible transfer is 2200 MW, but according to second criteria group it is limited by 1800 MW. If there is ECA equipment, which would disconnect a 500 MW unit in the exporting subsystem in case of a line tripping when the transfer exceeds 1800 MW then the permissible transfer could be increased up to 2160 MW.

If one assumes that the difference in marginal costs is :

$\Delta T = 300 - 0.1P_{12}$, RUR/MWh, then cost cutting for the purchase of the same amount of electricity equals to:

$$A = 720 \int_{1800}^{2160} (300 - 0{,}1P_{12})\,dP_{12} =$$

$$720(300\,P_{12} - 0{,}05\,P_{12}^2) \Big|_{1800}^{2160} = 26{,}438 \text{ MRUR},$$

where :

720 h - assumed 2160 MW transfer duration (1 month);

P_{12} - power transferred between subsystems.

System service cost for the power plant : if one assumes that generator disconnection fee is e.g. 0.5 MRUR and line tripping probability for one 500 kV line is 0.0025 tripping / km-year then for 1 month (according to the example) we would get 0.0025 * 800 * 1/12 = 0.17 faults of at least one of three lines (and generator accordingly) per year, thus result in 0.085 MRUR as generator disconnection fees a year.

The ECA costs include capital costs, e.g. K = 1 MRUR (as we consider very simple systems we assume that they were built for 1 year period), O&M costs - approximately 20% of the capital costs or 0.2 MRUR.

Total expenses for the ECA – 1.285 MRUR for the first year, and 0.285 MRUR - for every other year.

Comparing cost cutting (in our example – 26.438 MRUR) with total ECA expenses one can evaluate the ECA efficiency.

2.8 EXISTING DEFENSE PLANS IN TOKYO ELECTRIC POWER COMPANY

In TEPCO's power system, three major generation centers located in northeastern, southeastern and northern areas are connected to a 500 kV bulk transmission grid. About 10 GW power on 500 kV power grid flows east to west in summer peak days. The peak demand is 64 GW. Western generation centers with major loads are connected to some 275kV radially operated transmission networks.

Three major Special Protection Systems (SPS) were installed in TEPCO's power system to withstand extreme contingencies **[2-10]**:

- A predictive out-of-step protection system;
- An islanding protection system with active and reactive power balancing control for Tokyo Metropolitan Power System;
- An undervoltage load shedding as wide area protection scheme.

2.8.1 Predictive out-of-step protection system

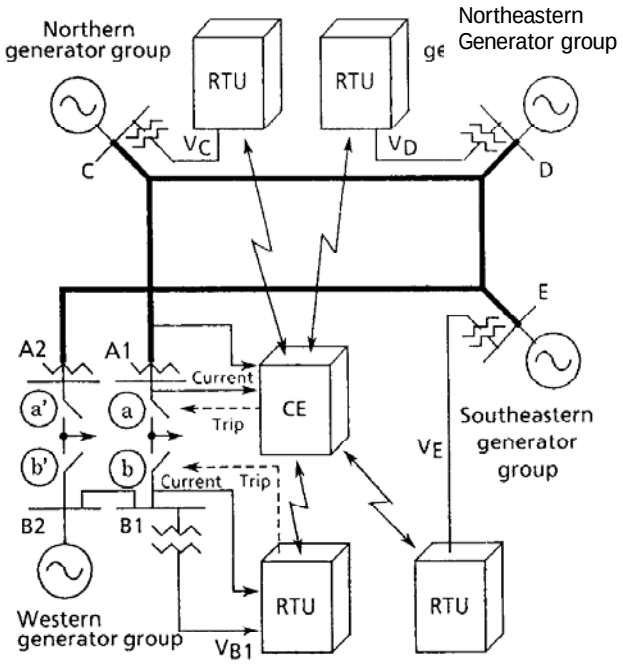


Figure 2.10 - System Configuration

Since very severe but rare contingencies may cause rotor angle instability between western generation centers and others, an SPS was installed in 1989. The SPS is based on the observation of phase difference between substations, and separates the western networks from major grid in case rotor angle instability is detected.

The SPS is a fully redundant system composed of two identical relaying systems for the purpose of separating two 275kV power systems. Each system has a Central Equipment (CE) installed in a 500kV substation near western generation centers, three Remote Terminal Units (RTU) installed in three substations located near northeastern, southeastern and northern generation centers, and one RTU installed in a 275kV substation near western generation centers. CE and RTU are connected as star topology through a microwave synchronized communication channel as shown in **Figure 2.10**.

The RTU simultaneously samples busbar voltages at 600 Hz, and the samples are transmitted to the CE. CE calculates in real time the phase differences between W-NE, W-SE and W-N. When two out of three phase difference values, predicted at 200ms in the future, exceed the pre-determined threshold value, the CE detects the loss of synchronism of western generation centers from main grid, and initiates the western system separation based on the tripping signal from CE.

2.8.2 Islanding Protection System with Active and Reactive Power Balancing Control for Tokyo Metropolitan Power System

In Tokyo metropolitan area, 275kV/154kV and 275kV/66kV substations are supplied from the main grid through radial operated networks composed of a 275 kV double-circuit overhead transmission line and triple circuit underground cables (see **Figure 2.11**). Each network has adjacent networks that can be connected by switching normally opened circuit breakers. Some of these networks include generation plants whose capacity is much smaller than load demands and others include no generation plants.

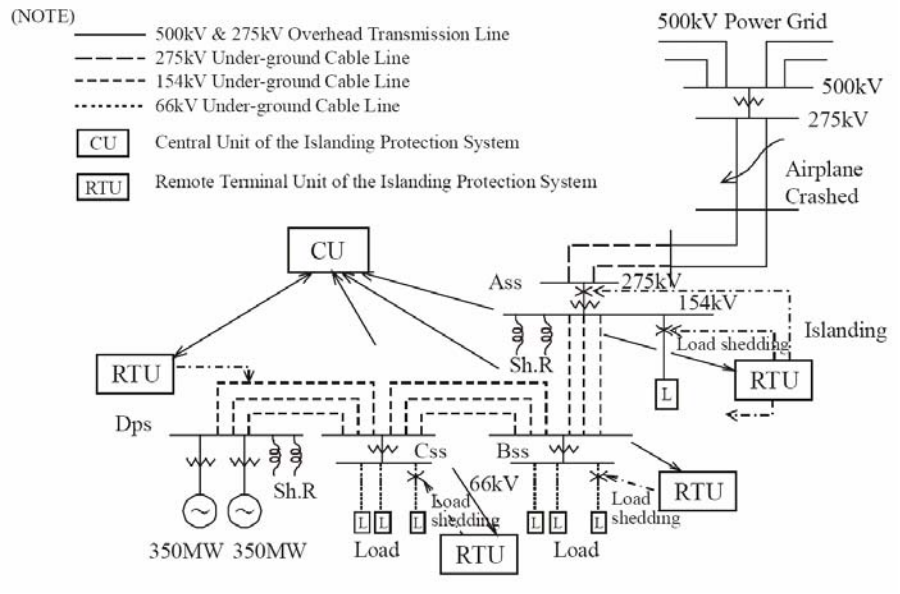


Figure 2.11 - System Configuration

In case of loss of double circuit line supplying a power system including generation plants, the power system is separated from main grid under extremely overloaded condition. Severe power imbalance may result in under voltage as well as under frequency situation. Saving a heavy overloaded system only by underfrequency load shedding programs would be very difficult. A SPS is needed to save the separated power system securely, which initiates intentional islanding at the point where heavy imbalance of active power exists is a much better approach. The SPS also initiates balancing control for both active and reactive power by load shedding and shunt reactor switching. If only active power balancing control is done, over voltage is adversely expected after load shedding because of the large amount of cable charging and reduction of reactive power consumption. Load shedding effect being diminished with voltage sensitive characteristics in overvoltage condition may introduce the failure to arrest frequency decay. The SPS is a fully redundant system that has a central unit (CU) and several RTU's. Each RTU acquires required information data like power flow at intentionally separated point and submits them to the CU. The CU cyclically computes the amount of load shedding and reactive power control based on the received information data from the RTU. A fiber optic network is used for the communication channel between CU and RTU. The RTU's are connected to CU in a star topology.

If the CU detects system separation by voltage angle difference and/or voltage magnitude, CU issues the control signal to RTU. The RTU which receive the signal perform the predetermined control procedure in very fast manner (on the order of 500ms).

The separation of particular power systems can be detected by the differences of voltage magnitude or phase angle away from those of the main grid. The SPS has also RTU installed outside possible islands for the purpose of measuring the voltage phasor as reference.

In November 1999, an air plane crashed into a 275 kV overhead transmission line resulting in separated system with a generation plant. The load demand was 2000 MW and total generation inside the island was 400 MW. This extreme overloaded condition caused very rapid frequency decay of 5 Hz per second. The SPS successfully detected system separation from main grid and took appropriate actions to form the island with better power balance, shed loads and switch shunt capacitors in 500 ms after the fault. As a result, the island, including vital areas, could be paralleled to the main grid in about fifteen minutes after the incident.

2.8.3 Undervoltage load shedding as wide area protection scheme

In July 23 1987, TEPCO experienced massive outages caused by voltage instability which was very long term (one over ten minutes order). Not contingencies, but rapid demand increment led to voltage instability and 8 GW loads were lost due to distance relay operation during voltage collapse, which prevented more cascading. After this system disturbance, the following actions were taken.

- System operation with 3 to 5% higher voltage profile
- Installation of numerous Switched Shunt Capacitors of 18 GVAr to EHV S/Ss
- Application of high speed high side voltage controller (PSVR) to about 80 generators connected to the EHV network
- Micro-processor based automatic Voltage-Q controllers (VQC) have been distributed to almost all of the 500 to 154 kV and 275 to 66 kV transmission substations
- Development and application of undervoltage load shedding (UVLS) as wide area protection scheme

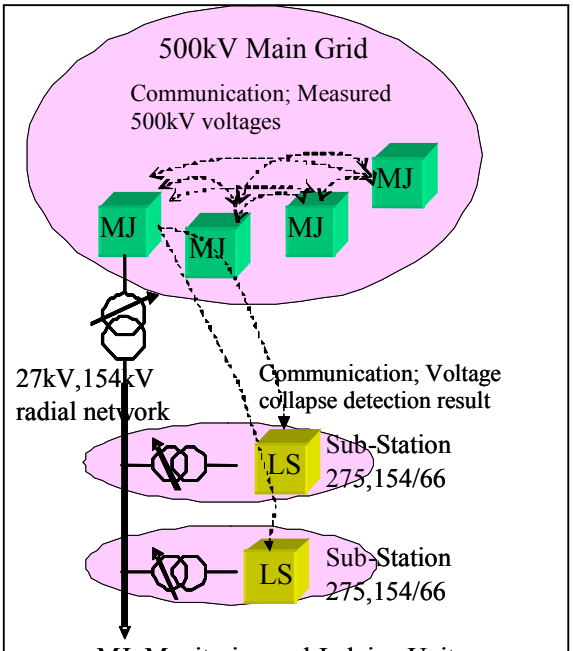


Figure 2.12- System Configuration

As represented in **Figure 2.12**, UVLS scheme is composed of Monitoring and Judging units (MJ) installed at four 500kV substations and load shedding units (LS) installed at several 275 or 154/66 kV substations. Each MJ unit is connected via microwave communication channel and LS units are connected to a MJ unit as star topology via microwave. Long term voltage collapse can be detected on the 500kV network, because 275kV or lower voltages are automatically regulated by tap changing on 500/275 or 154 transformers. Therefore, the SPS requires MS units measuring 500kV busbar voltages. For the purpose of security, the SPS uses 3 out of 4 decision making logic. The SPS does not use any SCADA information.

MJ units detect slow types of voltage collapse (ten seconds to minutes order) by using unusual continuous $\Delta V/\Delta t$ value obtained with the least square route value calculation technique for twenty sets of voltage values. The settings are determined so that the SPS never pick up normal voltage dip based on actual measurements. Fast voltage collapse can be also detected by $\Delta V/\Delta t$ calculation with one second of data window.

The SPS can be categorized as feed-back control, which means that feeders continues to be shed until recovery from undervoltage condition is detected. Since installation of this UVLS, voltage collapse itself has never been experienced in TEPCO's power system and there has been no unwanted operation during normal operating condition for over ten years.

According to TEPCO's philosophy, UVLS is recognized as a last resort to prevent cascading, following very severe contingencies like multiple outages during extreme weather and heavy load, which means outside planning and operation criteria.

2.9 DEFENSE PLAN TO FACE MAJOR INCIDENTS ON THE FRENCH ELECTRIC SYSTEM

The current French "Defense Plan" includes a SPS whose aim is to split the network into separate sub-networks in case of loss of synchronism (a "Defense Plan" is a set of ultimate measures to preserve system integrity when a system collapse seems imminent). It was recognized that the system was subject to potential weakness and a Wide Area Protection Scheme (WAPS) against losses of synchronism was designed and tested at the end of the 90s. While this system looked very promising, it was decommissioned in 2002 for reasons that will be explained later. But the study methodology and the defense scheme developed for the French system provide an interesting approach for any utility wanting to develop such a scheme **[2-11]**.

2.9.1 Current French Defense Plan

The current French system integrates about 400 out-of-step relays named DRS[3] which detect losses of synchronism, isolate out-of-step areas by opening the appropriate lines and therefore prevent the instability from propagating to other areas. The French system is divided into 19 "coherent" areas with regard to losses of synchronism. It means that in each area, in case of problem, all generators will loose synchronism together. The DRS are installed at both ends of the lines crossing the border of each area including the lines connected to the neighboring countries. The criteria used by these relays to detect loss of synchronism is the occurrence of voltage beats in the range 0.5 Hz – 3.5 Hz as shown in **Figure 2.13** (which means that they are simultaneously several voltage waves with different frequencies).

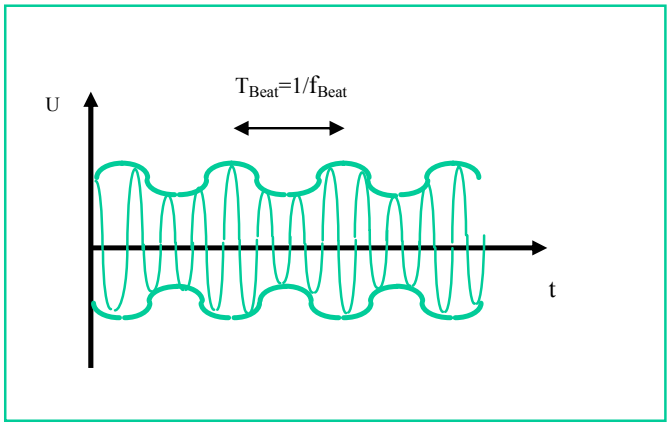


Figure 2.13: Voltage beats due to a frequency deviation between two areas

This system is a decentralized one, each DRS operates independently of each other without central coordination. It has been in operation satisfactorily for more than 20 years.

The DRS plan has acted in various occasions since its first commissioning during regional and national scale incidents. It has proved its advantages but also its limits; these limits confirmed by simulation.

During the 1980´s, the French 400 kV network has been reinforced, so that it implied the updating of areas topography and DRS adjustment. This updating has been reviewed on the base of simulations of losses of synchronism caused by three-phase short-circuits exceeding the critical clearing time. An accurate modeling of DRS was studied with the EUROSTAG software. The short-circuits have been applied to most of the 400kV substations of the formerly weakened EDF´s network in turn. They must be regarded only as a mean of causing losses of synchronism which should evidence the generic fragmentation diagram of the system. In a first modeling, non-activated (i.e. being unable to open the line) DRS relays have been connected in any node of the network. At the end of each simulation, the

[3] **French acronym for 'Débouclage en cas de Rupture de Synchronisme'**

number of voltage beats (which more or less corresponds to the number of pole slippings) detected by each DRS and their detection time have been listed. A list of the generation sites where a loss of stability occurred has also been worked out. The DRS areas have been determined through a review of all the study results. This analysis has also given the setting of each DRS, i.e. the number of beats causing line tripping. The reliability and the selectivity of the DRS protections were based on these choices.

Figure 2.15 shows the behavior of the network in the same condition as **Figure 2.14**, but when the system is equipped with DRS. The disturbance is now prevented from spreading throughout the network due to the DRS partitioning. The occurrence of ultimate line openings should however be noted.

Figure 2.14 – Without DRS

Figure 2.15 – With DRS

Validation tests have then been carried out to check the robustness and selectivity of the solution. All the simulations have been repeated with active DRS, namely controlling the line tripping for various short-circuit durations. The analysis of the operation of the DRS plan using checking scenarios showed moderate results. On 29 significant cases, 21 progressed satisfactorily, 17 or them (59%) without undesired line tripping, 1 (3%) with an islanding of sites where no loss of synchronism occurred, and 3 (10%) with undesired line tripping. The other eight cases (28%) were failures. The success rate therefore exceeded 70%.

Nevertheless, this system may be subject to potential weaknesses:

- voltage beats are only an effect of the loss of synchronism whose origin is angle instability,
- all the lines are not tripped simultaneously, the complete isolation of the out-of-step area may be delayed in some cases,
- furthermore, some lines may not be tripped because in some places the magnitude of the voltage beats stays under the predefined threshold,
- the voltage beats may be detected in a diffuse manner, far from the responsible generators, there is a risk of unwanted line tripping,
- once the out-of-step area is isolated from the rest of the network, the generation/load balance is not restored simultaneously.

Taking into account these weaknesses, it was proposed to replace this system by a new one based on the PMU/WAMS technology.

2.9.2 Philosophy and Design Principles of the New Scheme

Large scale incidents occurring on large-size systems are the outcome of always complex combinations of adverse factors; as there are a lot of factors involved, their combinative number is still greater.

Attempting to list these combinations for the purpose of deducing the most appropriate measures would be a considerable work doomed to failure. The only possible approach is different; it consists in identifying the potential rupture lines of the system, the prevailing electrotechnical phenomena involved and their sequencing for the determination of system collapse mechanisms.

Associated phenomena and sequencing will be referred to later as the system collapse mechanisms. Thus an incident will no more be characterized by its primary events, but by its mechanisms; in the same way the new defense devices will be designed such as they oppose these mechanisms.

First, the mechanisms have been identified from the worldwide collection of large-scale Incidents. Second their likelihood has been checked in the context of the French system. Finally, for each possible mechanism, curative actions have been proposed and tested. On the two last study steps many simulations of the system behavior have been carried out on the basis of incident scenarios representative of the mechanism under study. The simulations had to comply with strict specifications :

- recording of a large-size system,
- deep, far-reaching transients,
- display of mechanism sequencings corresponding to phases of possibly different durations,
- easy operation and test of new palliative measures.

Based on such specifications a preliminary study of deep incidents was conducted. About forty complex incidents, adequately documented, have been analyzed to take down their mechanisms. They occurred on the UCPTE, NORDEL (North European interconnected system), Great-British, North American or Japanese electric systems, mainly during the last decade. The mechanisms are confirmed to be :

- frequency drops,
- loss of dynamic stability (transient or long-term),
- loss of steady state stability,
- loss of voltage stability,
- transmission structure tripping especially owing to a cascade load transfer.

It also evidences some thirty detrimental factors. Some of these factors refer to the network states; the others concern the transitions that make the network quickly step from one state to another.

Lastly, a dozen of typical events prone to initiate the degradation process can be isolated.

A review of the 26 most significant incidents shows that between two and thirteen (five on the average) of these fundamental factors or events played a role in each collapse.

2.9.2.1 Detrimental factors and events

Only the occurrence percentages or the factors and events met in 20% at least of the considered incidents are presented, in order to alleviate this report.

a) Factors concerning the pre-incident state

- Incidents often occur along border areas (in the electrical meaning) of large: 31% (46% if the particular case of longitudinal networks is included);
- Existence of an intermediate busbar on a high power transfer axis : 31%, and, especially large-scale transmission of energy on parallel circuits: 27% ;
- System weakening resulting from circuits out of service: 31 %.

b) Events initiating the incident

- Standard faults such as line or busbar short-circuits: 42%,
- Tripping due to an overprotection of generators or to a disturbance of auxiliary services: 31 %,

c) Factors promoting the spreading of incidents

- Tripping due to cascade overload transfers: 35%,
- Poor setting of protections including an overprotection: 23%,
- Existence or creation of areas showing an important energy-related unbalance: 27%,
- Improper or ill-adapted load shedding: 27%,
- Voltage instability due to shortage of reactive power reserves: 20%.

2.9.2.2 Degradation Mechanisms

The degradation mechanisms listed above do not develop at the same rate. This characteristic is important, first from the analysis standpoint, as the same incident may involve several mechanisms; the simulation of their sequencing must be possible. On the other hand, if curative measures are proposed, the rate of the phenomenon plays a decisive role in the choice of technologies adapted to their implementation.

a. Fast system degradation : loss of synchronism

The fastest degradation processes within an electric system are the frequency drop and the loss of transient stability. With regard to frequency collapse, if the original energy-related unbalance is high, a frequency incompatible with the generator operation can be reached within a few seconds. The loss of synchronism is very fast, too; it may occur within a second after the original disturbance.

The high rate of such phenomena prevents any human action; curative action can be taken only using automatic devices. In France, these devices are known as “defense plan”. The existing French defense plan already comprises a number of actions against the two mechanisms mentioned above:

- a load shedding plan on a frequency criterion is aimed at fighting frequency collapses; it sheds nearly 60% of the load in four equal steps between 49 and 47.5 Hz;
- local relays called DRS (French acronym of “area islanding protections in case of loss of synchronism”) should detect any loss of synchronism and isolate immediately the ill network portion from the healthy one.

Frequency collapses have not been detailed, in so far as frequency is equivalent within the interconnected system, provided no loss of synchronism exists. Planning for changes in the existing curative actions would involve redefinition of the process for the whole UCPTE, whích was not the purpose of the study.

Loss of synchronism, however, has been studied. They tend to spread from an epicenter that is premonitory of remedies whose application to the only French network means an improvement for all the interconnected system. Such a behavior also enables, from the simulation standpoint, the French system and the nearby networks to be differently sharpened so as to be consistent with the quality of data supplied. The adequacy of DRS devices, as far as curative actions are concerned, has been checked.

b. Slow degradation of the networks : voltage instabilities

The other mechanisms listed may be considered to be slower. The collapse rate of a network, where cascade overloads occur, depends on the overload protection time lags. In the case of voltage collapse, inadmissible values may be reached within 5 to 20 minutes, and even less under adverse circumstances.

Curative actions with a human component are then possible; in France, these “safeguarding” actions consist in a fast rise of generator voltage and active power set points, in blocking network transformer tap changers or, lastly, in a load rejection (supply voltage drop and even load shedding). The rapidity of tap changer blocking has recently been improved by use of automatic devices.

Safeguarding actions might however not suffice if the above mechanisms developed more quickly. Such a possibility has been investigated, especially in the field of fast voltage collapses.

It must be emphasized that static or dynamic instabilities can be over lapped to slow the phenomena.

2.9.3 Main Characteristics of the New Defense Plan

2.9.3.1 Losses of Synchronism

Based on the above analysis, a new defense plan, better adapted to the operating conditions of the French system beyond the year 2000, was thought to fulfill the following functions:

- to ensure a reliable, simultaneous fragmentation of all out-of-synchronism areas;
- to promote the restoration of system balances under steady-state, and also transient, conditions immediately following the fragmentation of out-of-synchronism areas so as to avoid any induced incident.

The first function is an improvement of the existing defense plan; it is still based on the organization of the network into "islandable" areas. This improvement will be obtained through a loss of synchronism detection based on a criterion much closer to the feared phenomenon than the voltage beats: a comparison between the voltage phases measured within the elementary areas of the electric system. The architecture selected, which is best suited to this novel detection principle, is briefly represented in **Figure 2.16**. It uses network phase measurements that are pooled within a central computer. This computer decides the necessary fragmentation and delivers the appropriate orders for line tripping.

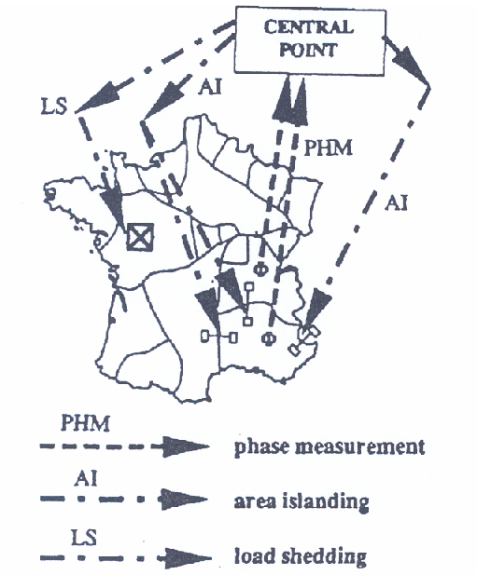


Figure 2.16 - Principles of the new system of Defense Plan against losses of synchronism

The second function is more unusual, it will aim at distributing the load shedding over the safe portion of the system which are necessary to speed up the balance restoration after fragmentation; the required load shedding algorithm (volume and distribution) implies the knowledge of the regional generation/demand unbalance state just before the incident; such knowledge supposes a global view of the system which can be achieved within the computer that is already responsible for the fragmentation.

This new defense plan has been modeled on the STABTRANS software. Simulations have then been carried out to test its effectiveness and to sharpen its characteristics and required performances. Thus, the response time of the device, from the physical occurrence of the loss of synchronism (characterized by an inter-area phase difference above 180º) up to fragmentation and load shedding actions, must be as short as possible to be fully efficient. In view of the technological possibilities, 1.3 second seemed a judicious compromise.

Simulations also enabled the load shedding operation rule to be redefined; this rule is based upon an inter-area pre-disturbance phase deviation criterion. Such criterion is representative of the load flow

constraints applied to the system and of the possible topological weaknesses. In the load shedding areas, about 30 % of load can be shed.

Figure 2.17.a shows a good application of the coordinated plan, while **Figure 2.17.b** shows the unsatisfactory coordination between the partitioning and load shedding actions, leading to an unacceptable fragmentation of the network.

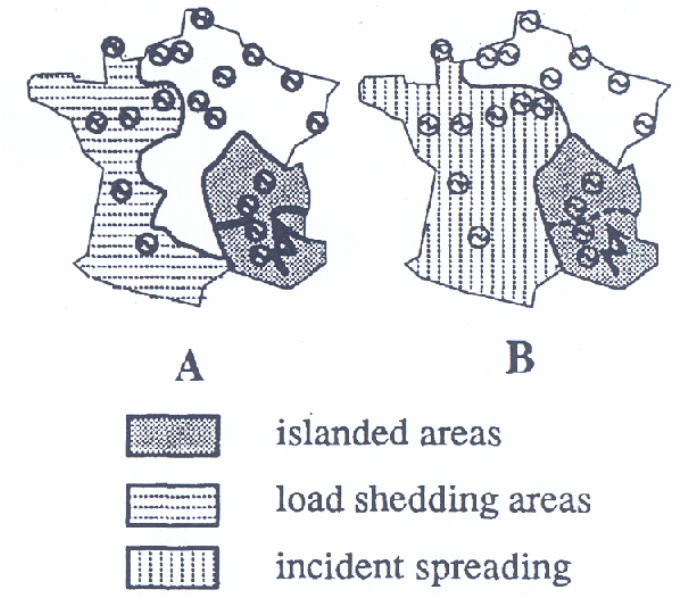


Figure 2.17 – Efficiency of new Defense Plan against spreading loss of synchronism

2.9.3.2 Voltage Instability

Among the network degradation mechanisms previously mentioned, voltage instability seems to be the most frequent cause of deep incidents in the large-size interconnected systems. Thus, a voltage collapse due to local reactive power shortages can lead to the loss of near by generating units, and aggravate the process.

Simulations made to investigate this mechanism required the greater modeling effort because of the various phenomena that might occur during the gradual voltage drop. Beyond the different automatic devices, mentioned earlier, a particular load model has been adopted. It incorporated an equivalent admittance behind a transformer with a continually variable transformer ratio that is automatically tuned. Furthermore, all the loads were distributed among areas, the loads within an area being capable of varying in the same ratio as a pilot load. A hand-operated remote load shedding device had also been added.

To study the phenomena associated with the voltage collapse, the western part of the French system has been considered. The opening of interconnection links and the unavailability of active and reactive power generating sets weaken this network. In addition, a rise in the demand at peak load of about 15 %, within one hour, was simulated so that the system was operated under unsafe conditions. Lastly, the manual or automatic safeguard actions described previously, to contain the slow degradation of voltage, have been deliberately inactivated. In such extreme conditions, the unscheduled loss of a generator in the F Power Plant as shown in **Figure 2.14** at $t = 4600$ s unavoidably causes a voltage drop and the successive islanding of several units. Within about two minutes, the voltage at the end of the 400 kV network drops to less than half its initial value.

The previous scenario results from an extremely severe combination of constraints, leading to a rather fast voltage collapse; only automatic actions could withstand such an incident; the functional features of this device have been explored.

In extreme conditions, near to voltage collapse, the load shedding is the ultimate solution. To be efficient and secure this load shedding must answer the triple question: “where, when and which load amount has to be shed”. To get this answer a global view of the system is necessary. Thus the location of the remote load shedding is determined by analyzing the trend of the marginal costs of the reactive power at each consumer node. This analysis is made during the simulation taking account of the actual situation of the generation units with regard to rotor current limitation or normal AVR operation. An optimal power flow program is used to compute the marginal costs. Loads are assumed to be independent of voltage and have their value defined for the simulation time considered. The marginal costs undergo a discontinuity just as the voltage instability occurs (corresponding to the criterion dQ/dV=0). The transition is very quick - within a few seconds, and can even be instantaneous in the case of topology modification (circuit tripping). After marginal costs inversion the load shedding becomes unavoidable. Load shedding must be performed in the substations where the reactive power marginal costs are the highest just before their inversion. Its amount is determined using a simplified modeling of each concerned area.

Analyses have shown that the later the load shedding happens, the greater its quantity must be to prevent the system from collapsing. The longer the load shedding is delayed, the more the system is weakened and the less it is capable of withstanding a large-scale load shedding without risking a loss of synchronism. Beyond a given period of time, these two constraints become incompatible and the recovery of the system is unfeasible. It is therefore mandatory to carry out the load shedding with a minimum delay to reduce the quantity of load rejected and to make the operation more likely to succeed. The example proposed in **Figure 2.18** shows the voltage variations in substation E (map in **Figure 2.14**) without load shedding and with one of the three following load shedding options:

- 15% of the load just as voltage instability is detected, (A)
- 20% with a delay time of 39 s, (B)
- 30% with a delay time of 60 s. (C)

The simulations have shown that even in the case of fast voltage instability, load shedding action can theoretically save the system from the collapse. However this action needs on-line computing of the system state from information that is not all available nowadays. This difficulty and the very small probability of this collapse (the existing safeguards actions have been considered out of service) have lead to not consider such an action.

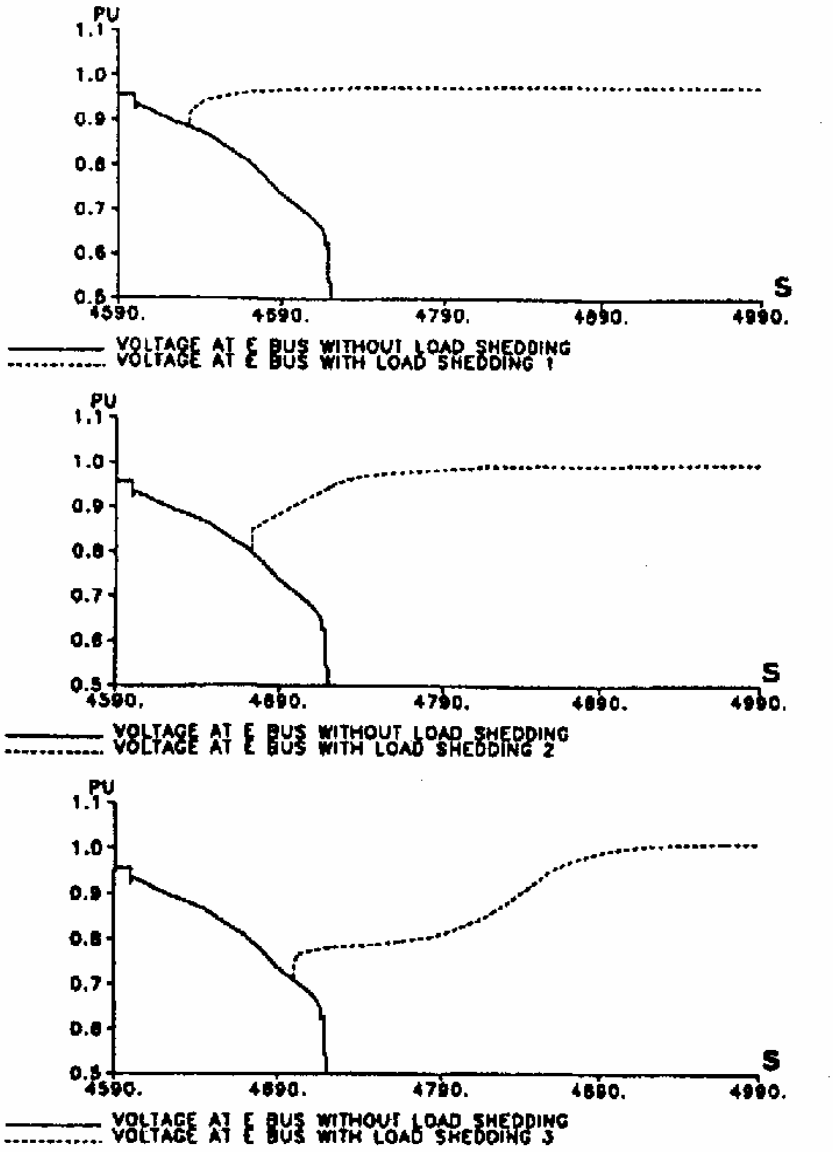


Figure 2.18 – Fast voltage collapse – Load shedding efficiency

2.9.4 Status of the New Defense Plan

This system was installed and tested in the French south-eastern grid at the end of the 90s. As mentioned above, it was abandoned in 2002. The main reasons are the following:

- the risk of unwanted line tripping was not negligible and could have had dangerous consequences,
- operational and maintenance costs were very high especially for the communication system. In such a system, the reliability of the communication system is essential. In this system, a two way communication system was used (wire and satellite).

Despite this abandon, the PMU/WAMS technology appears to be of great interest to enhance defense plans.

2.10 DEFENSE PLAN OF THE ITALIAN ELECTRICAL SYSTEM

TERNA (Transmissione Elettricità Rete Nazionale), the Italian Independent System Operator, puts maximum attention in the preventive study of the possible perturbations, in the analysis of the interruption of supply to consumers and in the definition and application of the operational security criteria. In spite of this, it is always possible that a modern complex electrical system, with plenty of production resources, operating in a regimen of precise security rules can evolve towards a partial or total interruption. The causes of a generalized interruption may be multiple, in general human errors also plays a role, but, after all, the electrical systems are always initially in a state of security and present a certain robustness of operation that, however, can be reduced due to a series of not reasonably expected events and therefore not programmed.

Thus, there must be preventative control strategies arranged to contain the effects of the events and to reduce the probability of occurrence of a generalized interruption. These strategies are organized in a Defense Plan of the Italian electrical system and are put into effect through Systems of Defense. Therefore, independently of the combination of causes that can lead a complex electrical system to evolve to an emergency state of operation, the following description will describe the systems and the apparatuses that are currently in operation at TERNA **[2-12**].

Considering the importance of the defense system for the operation of the national electrical system, TERNA reserves itself the possibility to carry out, at any moment, the verifications on their functionality, be it with its own personnel, or employing external consultancy.

As to its application field, the prescriptions herein contained refer to the systems that are employed, or that have suitable characteristics, to participate or to constitute the defense of the Italian electrical system. Particularly, these can be:

- generating units directly or not directly connected to the bulk network;
- distribution networks connected to the bulk network;
- transmission lines, transformation or sectioning substations, making part of the bulk network.

2.10.1 Characteristics of the Italian electrical system

The Italian national transmission network consists of approximately 45.000 km of lines (**Figure 2.19 and 2.20**) and 320 transformation and distribution substations. It includes 220/380 kV lines (some 22.000 km, AC, and 1.000 km, DC) and 150/120 kV lines (some 22.000 km). It also includes 17 interconnection lines that allow the exchange of electricity with the foreign countries (France, Switzerland, Austria, Slovenia and Greece). Its generation capacity is around 80.000 MW (73% hydro, 26% and 1% wind/photovoltaic) for a peak load of approximately 54.000 MW.

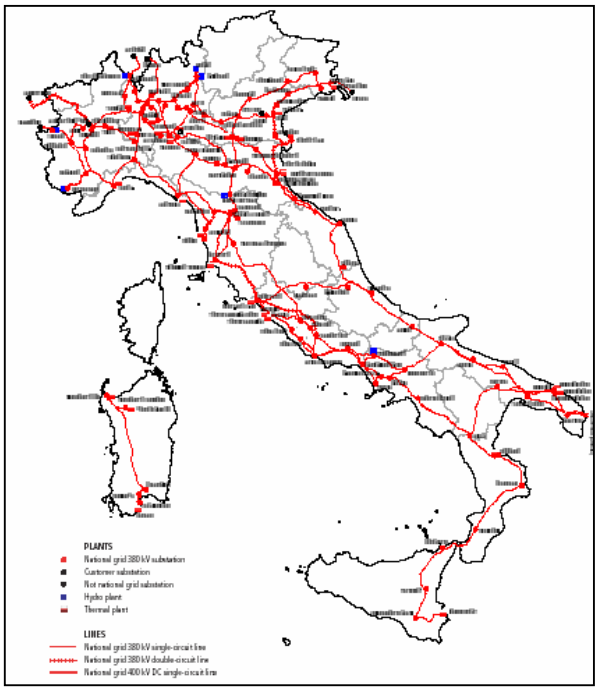


Figure 2.19 – 380 kV system

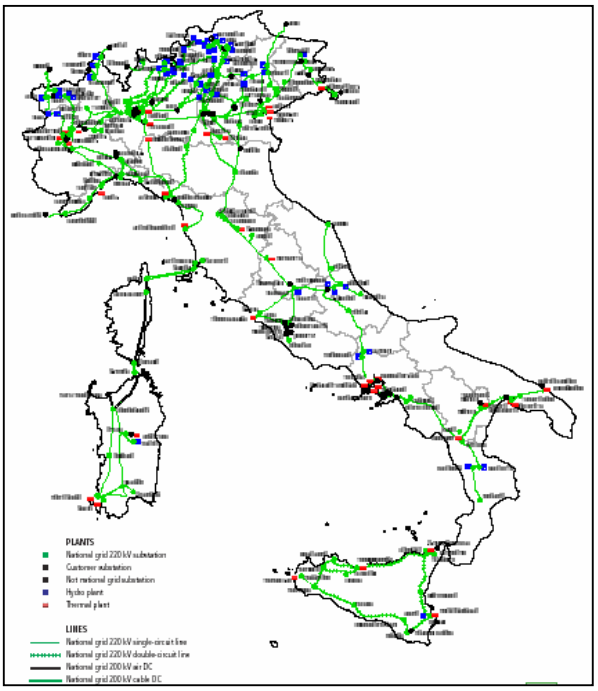


Figure 2.20 – 220 kV system

2.10.2 Philosophy and Design Principles

An electrical system is normally found in an operation condition that is defined *Normal* while all the electrical variables that define this state of operation are within predefined limits for all its components and there exists a correspondence between load demand and production within regulation margins. In such a condition the electrical system satisfies the N-1 criterion for evaluation of security, such that the lack of a single element, like a line, a transformer or a production unit does not cause violation of none of the operation limits and load is normally supplied.

The electrical system remains in this state until an event occurs that causes its evolution to another state of operation called *Normal of Alarm*. Among the possible events that could lead to this status are the loss of groups of generation, or the outage of 400 kV transmission lines and substations. In the *Normal Alarm* state the N-1 criterion is still respected and some violations of the operation limits of equipments or of the electrical system may exist. Violations of the electrical system include voltage levels out of the limits demanded by quality of the electric service or by the integrity of the facilities, or the network frequency, or a non-programmed exchange of power between areas.

In case of occurrence of ulterior events in fast and uncontrollable succession, the system can evolve to an *Emergency* condition, in which a more or less extended loss of load may take place.

The events that can degrade the operation of the electrical system, with variable timings from some hundreds of thousands of a second to minutes are the following:

- Large unscheduled load demands.
- Sudden loss of an important unit or a generation station.
- Loss of 400 kV lines in fast sequence, with separation of the networks.

These events may lead to:

- Large transient or permanent overload of lines or transformers.

- Conditions of degradation or collapse of frequency
- Conditions of degradation or collapse of voltage

Coherently with the above described, the system of defense of the national electrical system provides all control actions, automatic or manual, to:

- maintain in a normal state a condition of operation that is prone to evolve to an emergency state;
- restore to a normal state a condition of operation that itself had already evolved to a state of emergency.

Moreover, according to the events, defense systems are activated with suitable response times to bring back the electrical system to a secure state. In fact, phenomena of fast evolution ask for automatic interventions, phenomena of slower evolution can be managed in manual manner and, finally, phenomena expected for days ahead ask for programmed interventions. The Defense Plan of the Italian electrical system is based on a strategy that previews four *Lines of Defense* that are realized with the adoption of security procedures, devices and systems installed in the bulk electrical network and in the distribution networks.

The first line of defense is constituted, preventively, by the operation of the electrical system, through the programming of a normal and safe state of operation, according to previously defined security criteria. Moreover, it is continuously supported during normal operation by the generators regulation systems that react to the variations with respect to the forecasted production schedule. In particular, the violations of the active power balance are compensated with the primary (speed) and secondary (frequency/power) regulations, while the required voltage levels are maintained with the automatic primary voltage regulation of the units, primary voltage regulation of the plant and secondary area regulation. The hierarchical arrangement for voltage regulation, of which take part the primary regulation of the plant and the secondary regulation of the area, is a characteristic that is required by TERNA for the generation units of the Italian electrical system. The coordination of the production of reactive power represents an important contribution for the maintenance of an economic and secure operation.

At the occurrence of a serious disturbing event, the system operator of the involved electrical system must inform, in real time, the other operators of UCTE, so as to coordinate the common actions of mutual aid previously established for the electrical interconnection. The return to the normal state of operation must happen in the least possible time.

The second line of defense is constituted by the protection system, with the task of taking out of service in a fast, selective and reliable way, the elements that are the cause of the incidents and negatively influence the state of operation of the electrical system. Such system must always be efficiently maintained, being in charge of the holders of the facilities. TERNA establishes the protection criteria and the strategies of calibration of the protection devices.

The third line of defense is realized by systems and devices that execute the corrective control of the interconnection network, and attempt to prevent uncontrolled separations. In this line of defense, anti-oscillation devices are also foreseen to equip some line protections of the 400 kV network.

The fourth line of defense acts in conditions of separated networks in case of failure of the third line of defense. It is constituted by all automatic devices intended to maintain balance between production and demand.

Concerning the third and fourth lines of defense, the following main classes of systems are present in the national electrical system:

- System for the corrective control of the Critical Sections.
- Tele-supervision of the generating units and of intrinsically weak network sections.
- Automatic load shedding in the emergency regimes of under-frequency and minimal voltage (this system belongs to the fourth line).
- Apparatuses for manual load shedding executed on:
  - Industrial installations with interruptible load blocks.
  - Diffused and industrial installations with emergency load blocks.

- Emergency plan for the security of the electrical service by means of :
  - Cyclical load shedding of diffused installations in diurnal hours.
  - Cyclical load shedding, or reduction, of industrial installations in evening hours.
  - Formation of load islands.

Variation of the voltage references (set points) and blocking of the on load tap changers of transformers and auto-transformers.

2.10.3 Main Characteristics of the Italian Defense Plan

Next the details of the above listed defense systems will be described. It will be observed that these have been designed following a redundant and much coordinated strategy, being constituted of complex apparatuses and systems. In spite of this, it should be emphasized that the activation of the defense systems does not guarantee the restoration of the operation of the electrical system to a controllable state, whichever initial state or disturbing event of its equilibrium of operation.

The defense systems have various characteristics and multiple objectives. These can be illustrated by proposing some classifications. Specifically, as far as the strategy of use is concerned, the defense systems can be classified according to response time:

1. Preventive actions from emergency states, through the variation of set points, blocking of on load tap changers of transformers, a plan for cyclical load shedding and manual load shedding.
2. Contention Actions of an emergency state, by means of anti-oscillation devices, telemetering devices and automatic load shedding for the maintenance of the connection of critical sections.
3. Repressive actions against the evolution towards a generalized interruption, with automatic load relief according to frequency variation and minimal voltage, as well as the formation of load islands.

On the other hand, there are several defense systems that can be classified according to the state of connection of the network. In particular, the defense systems for a connected network are:

- Automatic corrective control of the critical sections.
- Telemetering of generating units and operatively weak sections.
- Load relief for low voltage.
- Maneuver blocks for manual load shedding.
- Plan for cyclical programmed load shedding.
- Variation of set points and blocking of on load tap changers of transformers.
- Installation of anti-oscillation devices.

In addition to the previous ones, the defense systems for the case of isolated areas of the network are:

- Automatic load relief in under-frequency regimens.
- Telemetering of the generating units of the electrical system of Sicily.

Finally, as far as the actuation modalities are concerned, the defense systems can be subdivided into the following three actions:

a. Defense systems based on automatic actions, such as:

a.1. Control of critical sections.

a.2. Load relief in underfrequency conditions.

a.3. Load relief for minimal voltage.

a.4. Telemetering of generating units and of the network (in some cases the triggering is manual).

a.5. Anti-oscillation devices against out of step conditions.

a.6. Devices for the formation of load islands.

b. Defense systems based on manual actions, in particular :

b.1. Insertion of shunt reactors.

b.2. Maneuver blocks for the disconnection of interruptible consumers in real time with previous warning.

b.3. Emergency Maneuver Blocks for the disconnection of diffuse consumers.

c. Defense systems based on programmed actions:

c.1. Variation of set points and blocking of on load tap changers of autotransformers and transformers.

c.2. Plan for cyclical programmed load shedding.

It should be noted that if the actions of the above listed defense systems were not sufficient to maintain the electrical system in, or restoring it to, a normal state of operation, or alarm, and should the same evolve towards a generalized interruption, yet on limited portions of the network, TERNA would promptly activate its Restoration Plan. This plan is structured and operated based on a very coordinated organization. Its objective is to restore the electrical system back to a state of normal operation, starting from a condition of complete interruption, not from an emergency state. Therefore, it cannot be considered a defense system. However in some occasions it is included among these and, in this case, it occupies a class apart - the one of Restoring Actions.

2.11 PROPOSAL FOR A new response-based Wide-Area stability and voltage Control System (WACS) FOR THE western North American interconnected power system

Bonneville Power Administration (BPA), National Systems & Research, and Washington State University are designing and implementing a Wide-Area stability and voltage Control System termed WACS **[2-13]**. WACS provides a flexible platform for rapid implementation of generator tripping and reactive power compensation switching for transient stability and voltage support of a large power system. Features include synchronized positive sequence phasor measurements, digital fiber optic communications from 500-kV substations, a real-time control computer programmed in the G language, running two algorithms in parallel, and output communications for generator tripping and 500-kV capacitor/reactor bank switching.

In contrast with Special Protection Systems (SPS), that include control for only pre-defined events and are burdened by complexity and relatively high cost, the WACS employs strategically placed sensors to react to the power system response to arbitrary disturbances, in such a way that the need for discontinuous action is determined and commanded, the power system response is observed, and further discontinuous action such as generator tripping or capacitor bank switching is taken as necessary. The WACS platform may also be used for wide-area modulation control of generators and transmission-level power electronic devices, and for control center operator alarms and monitoring.

2.11.1 Main characteristics of the Western North American Power System

The following proposal is oriented towards high power transfers from the Pacific Northwest (PNW—British Columbia, Washington State, Oregon) to California, but are adaptable to other applications.

Figure 2.21 shows the western North American interconnected power system. Connections to the eastern North American synchronous interconnection are by small back-to-back HVDC converter stations.

Long distance interarea transmission lines characterize the western interconnection. Major lines are 500-kV, 345-kV and 230-kV. There are two ±500-kV direct current links: the 3100 MW, 1360 km Pacific HVDC intertie from the Columbia River to Los Angeles, and the 1920 MW, 787 km Intermountain Power Project link from Utah to southern California. Hydropower predominates in the Pacific Northwest. Large coal-based power plants predominate in the eastern and southern portions of the inter-connection. Most generation in California is natural gas or oil based.

In spring and summer with good hydro generation conditions, the dominant interarea power flows are from the Pacific North West to California and also from coal-based generation in the eastern areas (Wyoming, Utah, Arizona, Nevada) to California. The northern California portion of the Pacific AC intertie comprises three series capacitor compensated 500-kV lines with non-simultaneous rating of 4800 MW for the three Oregon to California lines.

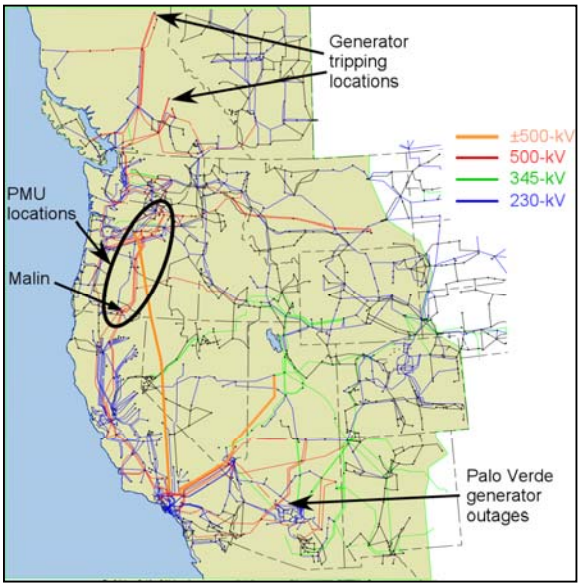


Figure 2.21 - Western North American Interconnected Power System

Large-scale power flow and transient stability simulations of potential disturbances are necessary to determine transfer limits for many defined transmission paths. Power flow (steady-state) simulations model over 10,000 buses (nodes representing generation and load injection stations, and transformer substations), requiring solving over 20,000 non-linear algebraic equations. Transient stability simulation adds thousands of non-linear differential equations. In defining simultaneous power transfer limits, major sensitivities are shown on nomograms. Portions of nomogram boundaries are limited by either first swing transient stability, transient damping of oscillations, or by post-disturbance voltage support criterion.

Control actions are mainly for detection of transmission outages, but also for some generation outages. The most complex scheme involves the Pacific AC intertie where high-speed outage detection of around fifty 500-kV lines is installed (detection at both line ends). Fault tolerant programmable logic controllers are at BPA's two control centers: one near Portland, Oregon and the other in Spokane, Washington. The most important control action is tripping of hydroelectric generators in the Pacific North West. There are few difficulties with tripping hydro generators and they can be rapidly returned to service. The generators are at the sending end of the PNW to California power transfer path, with the generator tripping braking remaining Northwest generators that are accelerating relative to southwest generators. For outages of either the Pacific AC or HVDC intertie, up to 2700 MW of generation may be tripped.

Other control actions are energizing 500-kV series and shunt capacitor banks, and disconnecting shunt reactors. BPA 500-kV shunt capacitor banks are in the 200–380 MVAr range.

Control actions take place as fast as 150 ms after the outage. The delay time includes detection time, communications to central logic, logic computer processing time, communications to power plants and substations, and power circuit breaker operating time. Communication of SPS activation signals use the same high-speed "transfer trip" used for isolation of transmission line short circuits. At BPA these are primarily frequency shift key audio tones over analog microwave. Newer systems use digital messages over digital microwave or fiber optics (SONET).

2.11.2 Philosophy and Design Principles of WACS

Power system stability controls are described in several books and reports. **Figure 2.22** shows a block diagram of the power system stability control environment, highlighting local and wide-area, continuous and discontinuous power system stability controls. Power system stability encompasses electromechanical (rotor angle) stability among groups of synchronous generators, and voltage stability involving load response to disturbances. RMS-type sensors are generally used—electromechanical oscillations and slow voltage variations amplitude-modulate the 50 or 60 Hz power frequency waveforms. Electromagnetic transients are not of primary interest except for sensor filtering considerations.

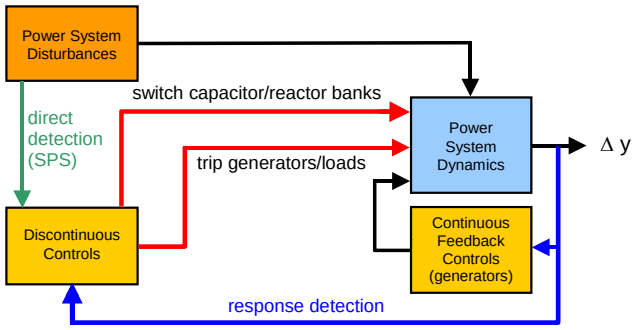


Figure 2.22 Local and wide-area, continuous and discontinuous power system stability controls

Most stability controls are continuous feedback controls at power plants: automatic voltage regulator and power system stabilizer for generator excitation control, and prime mover control (speed governor). Controls are largely the single input–single output type, designed via classical feedback control methods. Additional local continuous stability controls are at transmission-level and include power electronic devices such as static var compensators. There are also local discontinuous controls for reactive power compensation (capacitor/reactor banks) switching and load shedding.

Installed wide-area stability controls are mainly based on direct detection of selected outages. These emergency controls are termed special protection systems (SPS) or remedial actions schemes. The widely used special protection systems provide control for potential single and multiple-related outages identified in the power system planning process. Compared to the financial and permitting difficulties of transmission line construction, SPS are low cost and easy to install. A large increase in power transfer capability is realized.

As generation and load increase, however, without corresponding increase in transmission lines, SPS controls proliferate. At BPA there are many schemes for numerous operating and disturbance conditions. Tens of millions of dollars have been invested over many years. Additional schemes were added following the cascading power failures in summer 1996.

The consequences of SPS failure can be large-scale blackouts. Controls are clearly not as robust as additional transmission lines, and must be highly reliable by design. High redundancy in detection, communication, and logic computers is required.

The complexity of the SPS is ever increasing. BPA has a full-time operator devoted to pre-arming (enabling) and monitoring the many schemes.

Besides complexity, a shortcoming of pre-planned event driven control is that other disturbances may occur that have not been considered in planning. These may originate in other parts of the interconnected power system.

The philosophy of advanced wide-area stability controls is to measure power system response to disturbances. Feedback controls measure power system variables and can respond to arbitrary disturbances. Control can be continuous or discontinuous. .Discontinuous controls supplement the basic continuous controls by relieving stress for very large disturbances, providing a region of attraction and a secure post-disturbance operating or equilibrium point. Continuous controls then operate effectively after each discontinuous control step over a smaller non-linear range.

2.11.2.1 Phasor Measurements

Although various types of RMS sensors may be used, digital positive sequence, GPS-synchronized phasor measurements are most often considered for wide-area control. “Positive sequence” refers to transformation of an unbalanced set of three phase voltages or currents into a set of positive, negative and zero sequence “symmetrical components,” where positive sequence is a set of three-phase voltages

or currents with equal magnitudes, 120° phase difference, and normal phase rotation. In normal operation without short circuits or individual phase outages, the phase voltages and currents are nearly equal to the positive sequence voltages and currents.

Several manufacturers offer phasor measurement sensors. Typically, channels for multiple three-phase voltage and current measurements are provided. The positive sequence voltage and current phasors are computed and GPS time tagged once every two cycles, or in newer equipment, once every cycle of the power frequency (30 or 60 Hz data rate for 60 Hz power frequency). Power system frequency deviation from nominal is also computed, with GPS providing a precise time and frequency reference. There are tradeoffs between response speed and filtering. The phasor measurements are grouped, and data packets are transmitted to a central site where packets from several measurement locations (sub-stations) are organized by time stamp. Outputs from a "phasor data concentrator" (PDC) are networked to monitoring and control application.

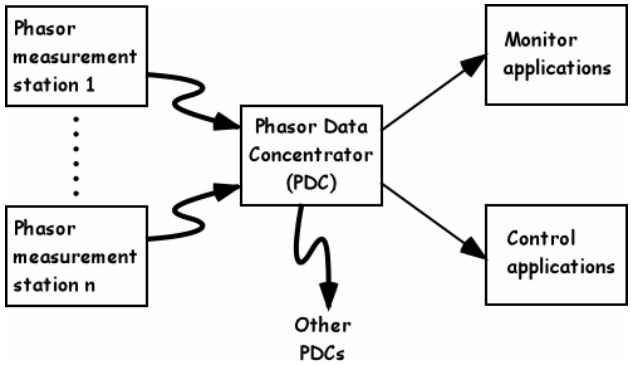


Figure 2.23 - Control center phasor data concentrator

From the voltage and current phasors, applications may compute active and reactive power.

In coming years, phasor measurements will become more common as part of advances in automatic controls and substation automation. The phasor measurements can be made available at small cost as part of other substation measurements, for example protective relaying.

Networked phasor measurements are a key part of BPA/U.S. Department of Energy/EPRI/Western Area Power Administration program for Wide-Area Measurement Systems. WAMS is valuable for power system identification, power system monitoring, control center state estimation, and power system dynamic performance analysis following disturbances—including large blackouts.

2.11.2.2 Continuous Wide Area Controls

Continuous wide-area controls offer observability and controllability benefits where conventional local continuous controls have shortcoming. Possibilities include "wide-area power system stabilizers" and controls for powerful transmission-level power electronic devices such as HVDC, thyristor-controlled series capacitors and static var compensators.

Wide-area controls are especially attractive for unusual system structures. Remote signals may augment control using local measurements.

Because of increased control leverage and continuous exposure to adverse interactions, caution compared to local control is required. Communications latency is one concern. Dynamics mimicking electromechanical oscillations are another. These may include sensor processing artifacts such as aliasing of network resonances or harmonics, or generator shaft torsional dynamics. Hydro plant water column oscillations may appear to be electromechanical oscillations. Extra monitoring and supervision of control is desirable.

2.11.2.3 Discontinuous Wide Area Controls

Compared to continuous control, discontinuous control tends to be safer—action is only taken when necessary. Discontinuous control has similarities with biological systems where stimuli must be above an activation threshold.

Similar to feed forward controls (SPS), feedback discontinuous controls initiate a large stabilizing action that improves first swing transient stability, reduces stress to improve oscillation damping, and provides a larger region of attraction for a more secure post-disturbance operating point.

2.11.3 Main characteristics of WACS proposed for the western North American interconnected power system

Figure 2.24 shows a pictorial block diagram of WACS. Selected existing phasor measurements are used for inputs, and existing SPS transfer trip circuits are available for outputs. The new development is the real-time controller.

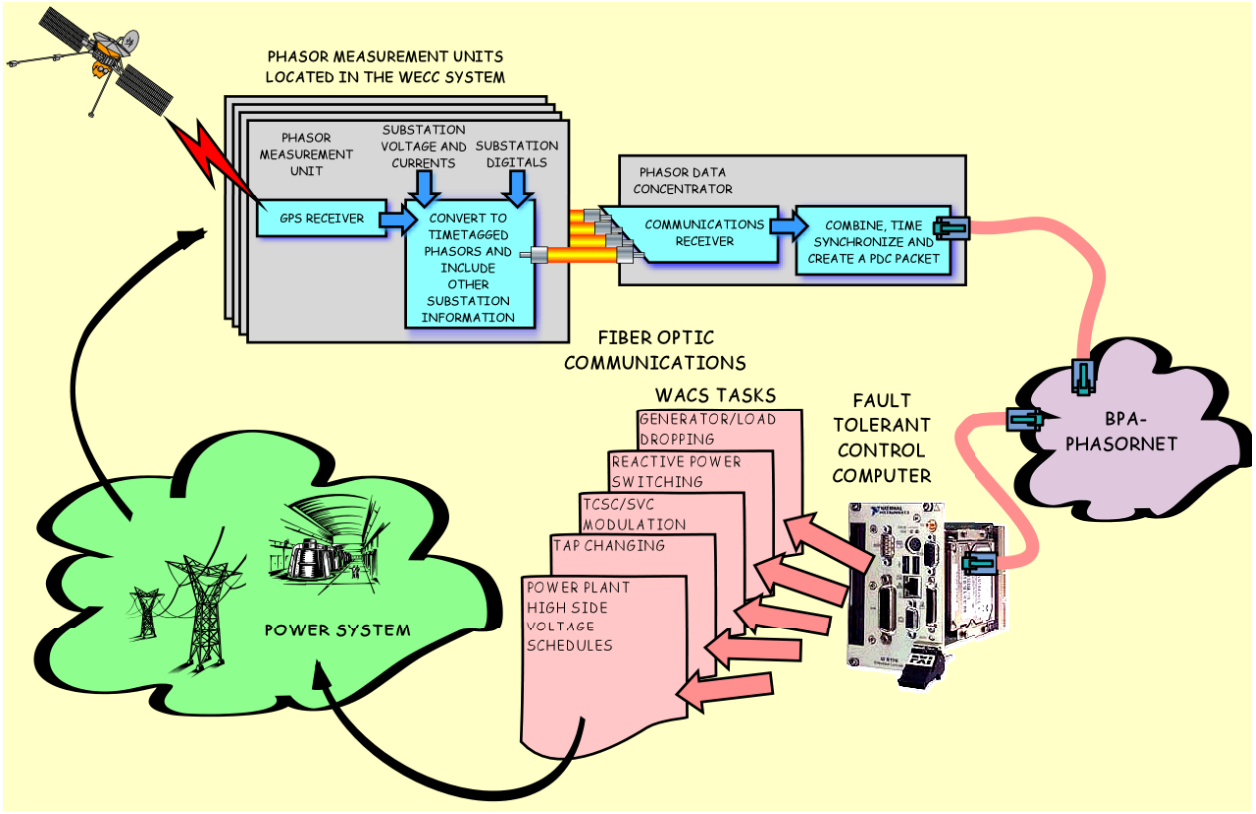


Figure 2.24 – WACS Block Diagram

Based partly on the August 10, 1996 cascading failure, the original BPA concept was to combine voltage magnitude measurements with generator reactive power measurements using fuzzy logic. The premise is that generator reactive power measurements can be a more sensitive indicator of insecurity than voltage magnitude—voltages can be near normal but generator reactive power outputs near limits indicate insecurity. Research at Washington State University showed, however, that a voltage magnitude based control is faster and simpler for transient stability. Both methods are now used. Recent field experience has actually shown that the two methods, Vmag and VmagQ algorithms, have similar speed. This is partly due to recent replacement of slow rotating generator field winding excitation equipment with modern thyristor exciters at two large power plants.

Twelve voltage magnitude measurements from seven 500-kV stations are used. Two stations are near the Oregon–California border (Malin and Captain Jack), one is in central Oregon (Summer Lake), and

three are near the Columbia River in northern Oregon or southern Washington (John Day, Slatt, Ashe, McNary). Fifteen generator reactive power measurements at five power plant switching stations near the Columbia River are used (Big Eddy, John Day, Slatt, Ashe, McNary). The hydro power plants feeding into Big Eddy, John Day, and McNary comprise 18, 16, and 12 generators, respectively; two to four generators are connected to a transmission line from the power plant to the switching station where phasor measurements are made.

WACS was designed so that loss of measurements from a single location or even multiple locations will only slightly degrade control. Measurements at widely spaced locations (hundreds of kilometers) provide spatial averaging or filtering against the aliasing effects discussed above. Spatial filtering along with discontinuous control action biases the phasor measurement requirements towards fast response rather than secure filtering.

2.11.3.1 Allowable Time for Controls Actions

For first swing transient stability, control action must be taken prior to the peak of the forward interarea angle swing—the sooner the better. For a simple second order undamped dynamic system with natural frequency of 1/3 Hz (3 second period), the step response peak is at 1.5 seconds. The impulse response peak is at 0.75 seconds. Most disturbances are closer to a step response than an impulse (the rare three phase short circuit approaches an impulse, but opening the faulted line provides a step response effect). Nowadays the frequency of the Pacific intertie mode is around 0.25 Hz (4 second period), allowing more time for control action. The oscillation frequency is even lower for high stress operation.

For transient stability, control action should be completed within around one second—especially for the less powerful capacitor/reactor bank switching.

The delay time for phasor measurement, fiber optic communications, phasor data concentrator throughput including wait time for slowly arriving packets, transfer trip, and circuit breaker tripping (of generators or shunt reactors) or closing (shunt capacitor bank insertion) are approximately 3, 2, 2, 1, and 2–5 60 Hz cycles respectively, or around 10 cycles for tripping and 13 cycles for closing (167 and 217 ms). Time for several control execution loops, intentional time delay, and throughput delay will be 67 ms or longer. Thus it appears that control action can be taken within 0.3 seconds after sufficient power system electromechanical response to the disturbance. For capacitor/reactor bank switching, the local supervising voltage measurement sensors will be responding during the same time as the WACS measurements and processing.

The more sensitive VmagQ algorithm may operate following longer time frame dynamics. In fact, need for the existing SPS action is determined by power flow simulation of a point in time several minutes after the disturbance. The SPS helps ensure post-disturbance voltage support for angle stability following generator overexcitation limiting, tap changing and other slower actions. Many seconds are available for taking sequential feedback actions as necessary.

The conditions existing in northeastern Ohio preceding the August 14, 2003 blackout were exactly what the VmagQ algorithm caters to. Voltage magnitudes were mildly depressed, but Cleveland area generators were at or near their reactive power limits. Automatic load shedding by control similar to WACS could have prevented the blackout.

2.11.3.2 Phasor Measurement Communications and Phasor Data Concentrator

BPA legacy communications is analog microwave. Transmission of phasor measurement packets using modems has high latency (60–100 ms) and relatively high dropout rates. Thus BPA-owned fiber optic communications (SONET) are used for WACS. BPA has an extensive fiber optic network, with links and terminal equipment still being added.

Figure 2.25 shows tests of fiber optic latency of less than 26 ms for a link from the Slatt switching station to a BPA control center. The link uses direct digital transfer into SONET.

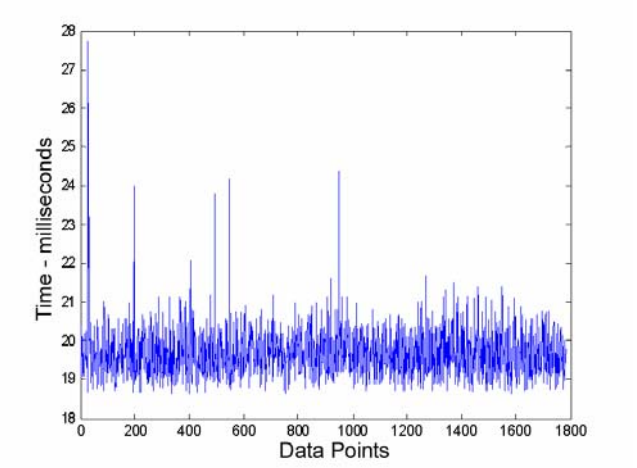


Figure 2.25 – Fiber optic communications latency over one minute, Slatt PMU to PDC.

2.11.3.3 Real-Time Hardware and Software

National Instrument's LabVIEW Real-Time (RT) hardware and software were selected. The software is a true dataflow language that prevents race conditions and allows for parallel tasking (multitasking and multithreading are supported). It has a many needed programming features and library components including data acquisition/processing/output, TCP/UDP, signal processing, filtering, math operations, execution logic and state machine, execution tracing and timing, display graphics, and fuzzy logic tools with graphical editors. The graphical code is largely self-documenting. Modular architecture aids the testing and certification of critical modules by designing virtual simulated "real-world" conditions around them.

Controller development is done on a PC, and code is then downloaded to real-time deterministic hardware and software. **Figure 2.26** shows the rack mounted WACS hardware. A full-featured Host PC that connects via Ethernet to the WACS RT Engine is available to monitor, test, develop and upload software, and to run model studies for tuning. This is important as the RT processor (engine) itself is always operated "headless" (no monitor, keyboard or mouse). A small text display status monitor and a sequence of events recorder are used.

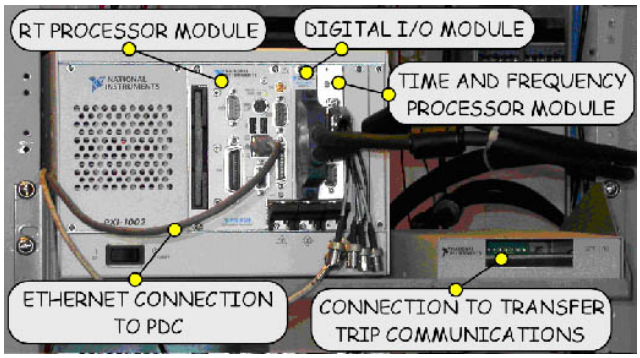


Figure 2.26 – WACS real-time hardware

WACS parameters are managed using an .ini file. This allows easy changes to the application for tuning the algorithms, defining station names, scale factors, etc. This is important in avoiding the pitfalls of "hardwiring."

1) Control execution rate: The rate at present is 30 control executions per second (33.3 ms intervals), which is the same rate as the phasor measurement packets. The time for a control execution cycle is around 8 ms, allowing addition of other features and moving to a future 60 packets per second data rate. For security against inadvertent actions during faults, measurement noise, and other disturbances, output must be above a threshold for two or more control executions.

2) Input processing: Tasks include reading and decoding the data from the UDP Ethernet connection to the phasor data concentrator (PDC), and data sanity checks for transmission errors, non-valid data, missing packets and extra long latency. Close coordination with PDC data processing is required, and a customized message of only the needed measurements is transmitted to WACS. For missing or corrupt data, there are two options: one is to block the data and not use it in the algorithm, and the second is to pad the data with the last valid packet for a few control executions. The former is used currently. Both fatal and non-fatal errors are managed and reports issued. Also the data is weighted and limit tested before being passed to the algorithm subroutines. The WACS software can also run in a library mode using simulation data or archived data from the PDC as inputs to the algorithms. This validates performance, facilitating certification.

3) Output processing: Following the algorithm computations, a pattern consisting of up to 32 isolated outputs is sent to a relay control stage where several masking operations are done before passing to the transfer trip communications. Any fatal or non-fatal error will mask outputs, with a user-defined mask available to disable one or more outputs either temporarily or long term, or to disable the results of either or both the fast or slow algorithms.

2.11.3.4 The Vmag Algorithm

The voltage magnitude based Vmag algorithm provides first swing transient stability stabilization and relieves stress to improve transient damping. For growing oscillations it will operate at some point for stabilization.

The algorithm is fairly simple, based on twelve voltage magnitude measurements at seven 500-kV stations. A weighted average voltage is computed from the twelve measurements, with highest weight for measurements close to the Oregon–California border where the voltage swings are usually greatest (Malin, Captain Jack, Summer Lake). A non-linear accumulator (integrator) computes volt-seconds below a threshold setting that is currently 525 kV for capacitor/reactor bank switching and 520-kV for generator tripping (normal voltage is around 540-kV). Accumulation is blocked for voltage recovery. Control action results when the volt-second accumulation reaches a setpoint; also the weighted voltage must be below 490 kV for generator tripping. The algorithm thus has semblance to PI (proportional-integral) control. Beneficially, faster operation results for more severe disturbances.

1) Critical disturbance:

A critical disturbance is near simultaneous outage of two nuclear generating units at a nuclear power plant in Arizona or California. Such events have occurred several times, and Western Electricity Coordinating Council (WECC) rules specify that cascading failure not result from these outages. Multi-generator outages at large coal-based power plants have also occurred.

The largest disturbance is outage of two nuclear generators at the Palo Verde nuclear plant near Phoenix, Arizona. The combined power loss is approximately 2700 MW. The lost generating capacity is made up by inertia power from rotors of all other generators (spinning reserve), and by response to decaying frequency by the speed governors of other generators. About half of the response comes from hydro generators in the northern half of the interconnected power system, resulting in a large increase in the Pacific ac intertie north to south loading. Instability (loss of synchronism between northern and southern generators) results if the initial intertie loading is high. There is no SPS for this outage.

2) Simulation of two Palo Verde generator outages without and with WACS

Figure 2.27 shows 500-kV voltage responses for the two Palo Verde generator outages with existing controls. The initial Pacific ac intertie loading is 4700 MW. The largest voltage swing is at the Malin station near the Oregon–California border, and the performance is considered marginally acceptable.

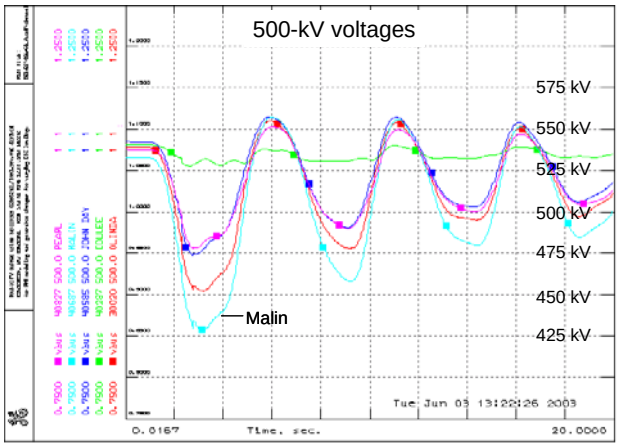


Figure 2.27 - BPA 500-kV voltages for outage of two Palo Verde generators with existing controls, with Pacific AC intertie loading of 4700 MW

Figure 2.28 shows similar response with WACS at an initial intertie loading of 5000 MW—a 300 MW gain. The main WACS action is 916 MW of generator tripping at two hydro power plants in British Columbia 1.4 seconds after the outage. WACS also inserted two 500-kV shunt capacitor banks 1.2 seconds after the outage. The transfer trip circuits from the BPA control center to the British Columbia power plants and capacitor bank locations exist as part of BPA's SPS. The higher oscillation frequency of Figure 28 tends to indicate improved stability.

Figure 2.28 - BPA 500-kV voltages for outage of two Palo Verde generators with WACS, and with Pacific AC intertie loading of 5000 MW.

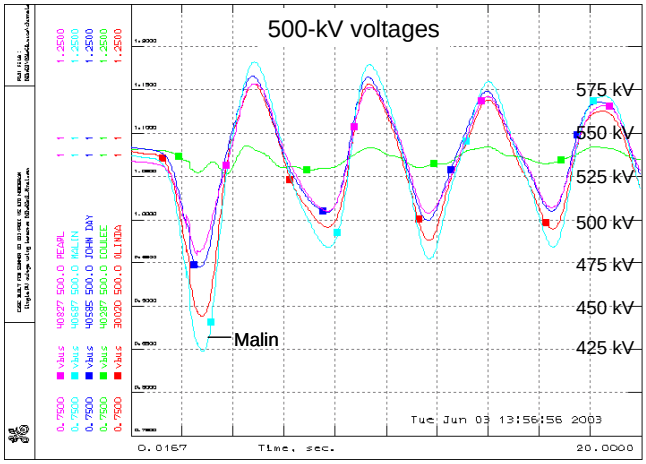
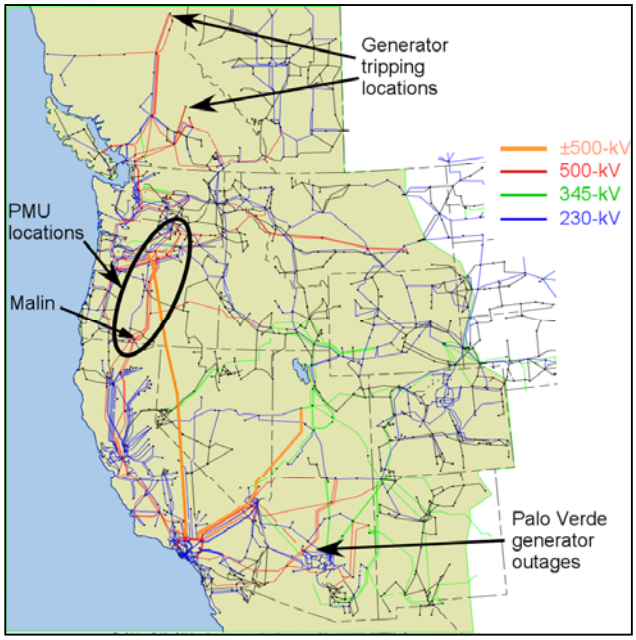


Figure 2.29 shows the wide-area nature: an outage in Arizona, measurements in Oregon and southern Washington, and control actions in British Columbia.

Figure 2.29 - Western North American interconnected power system showing disturbance location, and WACS input measurement locations and output action locations.



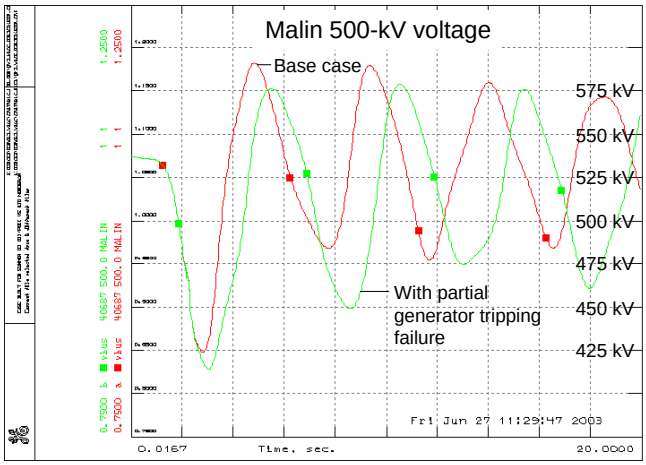
3) Partial failure of measurements

A failure of the most important phasor measurement device was simulated and used the 5000 MW intertie loading with WACS case as reference. The failure is two voltage measurements at Captain Jack near Malin on the Oregon—California border. Simulation results are nearly identical to the reference case, so they are not shown.

4) Partial failure of generator tripping

Figure 2.30 compares the reference case to simulate failure of a generator tripping at one of the two British Columbia power plants. Stability is maintained but performance is notably degraded. The oscillation frequency decreases.

Figure 2.30 - Malin voltage for outage of two Palo Verde generators with partial failure of WACS generator tripping.



Other sensitivity cases lead to improved tuning of the algorithm. We simulate other outages to verify expected performance.

2.11.3.5 The VmaQ Algorithm

The VmagQ algorithm combines voltage magnitude measurements and generator reactive power measurements using fuzzy logic. Similar to the Vmag algorithm, it is computed a weighted average 500-kV voltage magnitude from 12 phasor measurements at seven locations. More complicated is computation of weighted average reactive power from 15 transmission lines emanating from six large power plants. Active and reactive power flows for these lines are computed from the voltage and current phasors.

First, the number of connected generators is estimated—up to four generators per line may be connected on lines from hydro plants. While this information may be available at a slower data rate within a control center, interface and dependence on other data networks is avoided. The number of generators is estimated based on the normal loading range of individual generators. An estimation error on one of the many lines is not serious.

A normalization procedure follows, based on generator active/reactive power capability curves. Capability curves are mapped from the generator terminals to the transmission side where the phasor measurement sensors are located, accounting for station service load, and generator step-up transformer impedance and tap ratio. **Figure 2.31** shows this one-time mapping for a large nuclear plant generator.

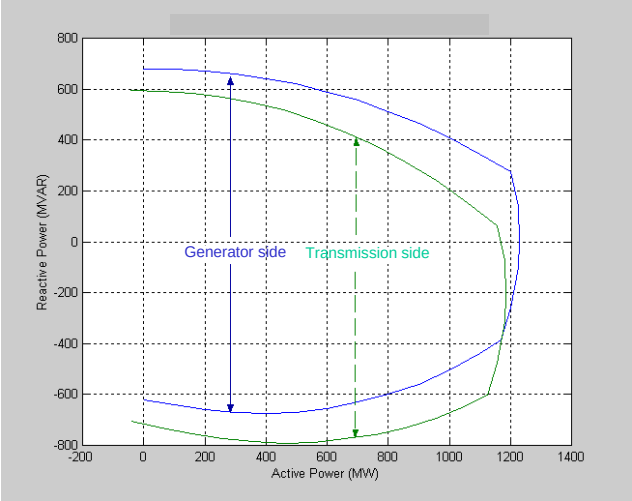


Figure 2.31 - Active/reactive power capability curve for a nuclear plant generator.

Normalization results in reactive power output on a scale of approximately ±1 (generator controls allow large temporary and small steady-state operation outside limits). The transmission-side reactive power limits corresponding to the active power are noted: $Q_{\max}$ and $Q_{\min}$. The normalized value from transmission side values is computed as follows:

$$Q_{\text{half}} = (Q_{\max} - Q_{\min})/2 \quad Q_{\text{zero}} = Q_{\min} + Q_{\text{half}}$$
$$Q_{\text{norm}} = (Q - Q_{zero})/Q_{\text{half}}$$

For example, for **Figure 2.31** with transmission side P = 1000 MW and Q = 100 MVAr, Q_{norm} = 0.77.

A weighted average of the normalized reactive powers is now computed. The individual weights are the product of the generator or generator group MVA rating and a factor. The factor is based on location and voltage support sensitivity. A higher value is given to generators providing more sensitive control of transmission voltage by automatic voltage regulator line drop compensation or by automatic high side voltage control.

Next the weighted average voltage magnitude and the weighted average generator reactive power are combined using basic fuzzy logic. Additional information on fuzzy logic application in the VmagQ controller is presented at Reference [2-13].

2.11.3.6 Tuning, Testing and Monitoring

Since large disturbances are rare, algorithm verification and tuning is normally via off-line large-scale simulation. The real-time controller is tested by inputting simulation results, and also by inputting archived phasor measurements from actual events.

2.11.3.7 WACS Response for a Large Real Event

At 07:40:56 on Monday morning June 14, 2004 a short circuit occurred near the Palo Verde Nuclear Plant west of Phoenix, Arizona. The fault was not completely cleared for almost 39 seconds! Approximately 4589 MW of generation tripped, at and near Palo Verde in the southern part of the western North American interconnection. All three Palo Verde units tripped.

Pacific intertie stability was threatened, but maintained. With one line between Oregon and California out of service, the intertie limit prior to the event was 3200 MW. North to south intertie flow swung from the initial 2750 MW to 5500 MW and settled at 4500 MW several minutes later. Malin and Captain Jack voltages near the Oregon–California border swung from the initial 548 kV to 443 kV at 07:41:21.6. Operators and an existing "response-based" scheme switched BPA series capacitors and shunt capacitor/reactor banks during the swings and the subsequent intertie power increase. The power increase is from governor action at Pacific North-west hydro plants, which carry large amounts of spinning reserve.

On June 14th, WACS was in a monitor mode at a laboratory installation five km from the control center and Phasor Data Concentrator. Adjusting for communications and PDC features that were not yet in service, WACS operated correctly on the forward angle swing, before a voltage swing minimum, as recorded by a sequence of events recorder.

To further validate the WACS algorithms, archived data from the June 14 event were played into the WACS code on a personal computer. One parameter was retuned to increase operating speed.

Figure 2.32 shows voltages that are WACS inputs, and includes the weighted average voltage computed by WACS (same weights used for both algorithms). For the Vmag algorithm, the accumulator thresholds for capacitor/reactor bank switching are 525 kV and the thresholds for generator tripping are 520 kV. Accumulator setting for capacitor/reactor bank switching is 2 kV-seconds and accumulator setting for generator tripping is 4 kV-seconds. For generator tripping the weighted average voltage must also be below 490 kV.

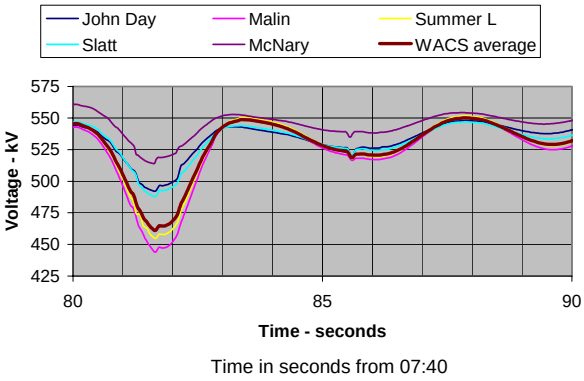


Figure 2.32 - Northwest voltages for first three swings.

For first swing stabilization, discontinuous control action should occur before the voltage minimum at around 81.6 seconds after 07:40. This time is estimated for the real signal without measurement delay (PMU timetags are at the last sample of the phasor computation window; the PMUs uses a four-cycle moving average filter with phasors calculated over one cycle).

Using the archived data as input to the real-time code, the WACS Vmag algorithm output for capacitor/reactor bank switching occurs at 81.033 seconds after 07:40. Adding 170 ms for communications, PDC, and circuit breaker delay, switching would be at 81.203 second or around 0.4 seconds before the real signal voltage minimum.

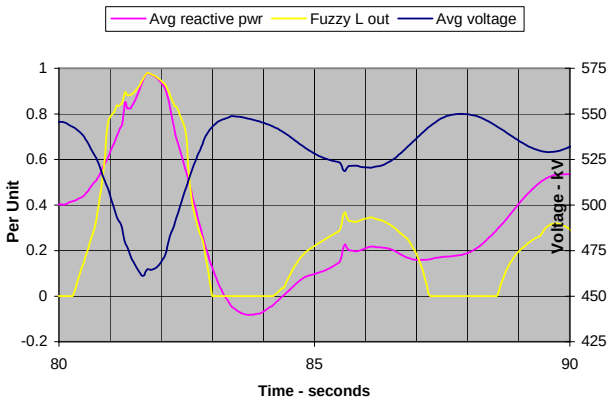
WACS Vmag algorithm output for generator tripping occurs at 81.233 seconds after 07:40. Adding 170 ms for delays, tripping would be at 81.403 seconds or around 0.2 seconds before the real signal voltage minimum.

For the VmagQ algorithm, **Figure 2.33** shows the weighted average voltage and weighted average reactive power that are combined using fuzzy logic. The crisp (center of gravity) fuzzy logic output is also shown. High fuzzy logic output correctly occurs for the combination of low voltage and high reactive power output. Fuzzy logic output above a threshold is accumulated. For capacitor/reactor bank switching the thresholds are 0.40 per unit. For generator tripping, the thresholds are 0.45 per unit. Accumulator settings are 0.05 per unit-seconds for capacitor/reactor bank switching and 0.2 per unit-seconds for generator tripping.

The VmagQ algorithm WACS output for capacitor/reactor bank switching occurs 81.033 seconds after 07:40 (same time as the voltage magnitude based algorithm). Adding 170 ms for communications, PDC, and circuit breaker delay, switching would be at 81.203 second or around 0.4 seconds before the real signal voltage minimum.

WACS VmagQ algorithm output for generator tripping occurs at 81.533 seconds after 07:40 (300 ms later than the voltage magnitude based algorithm). Adding 170 ms for the delays, tripping would be at 81.703 seconds or around 0.1 seconds after the real signal voltage minimum. While this will cause a larger backswing, the generator tripping reduces intertie loading and system stress.

Figure 2.33 - VmagQ fuzzy logic inputs and outputs.



Time in seconds from 07:40

The June 14 massive loss of generation was well beyond planning and operating reliability criteria. While unusual, power systems are continuously exposed to unusual events.

If stresses (Pacific intertie loading) were somewhat higher on June 14, instability would have occurred and caused controlled islanding with massive generation/load imbalance in the importing southern island that suffered the initial 4600 MW loss. Either massive underfrequency load shedding or a widespread blackout in California, Nevada, Arizona, and New Mexico would have resulted. Stress would have been higher later in the day as temperatures and load increased.

Events like the 14 June event are exactly what WACS can protect against.

2.11.3.8 WACS Status

Since March 2003 WACS has been installed in a laboratory with real-time phasor measurement inputs from a PDC and recording of contact outputs. Based on the following, a “proof of concept” was demonstrated. It was tuned and validated the real-time controller hardware and software:

- Large-scale simulations including playback of simulation results into real-time code

- Monitoring of real system performance over a two-year period
- Playback of archived data into real-time code, particularly for the June 14, 2003 massive generation outage event.

2.11.3.9 Conclusion

Automatic control experts state: "A modern view of control sees feedback as a tool for uncertainty management".

Given the many changes in the electric power industry with increasing complexity and reduced investment in transmission lines, the possibility and actual occurrences of large-scale blackouts are a worldwide concern. Clearly new means to improve power system reliability and robustness are desirable. The addition of wide-area feedback control to frequently used wide-area feedforward control is an effective additional layer of defense against blackouts, as well as facilitator of electrical commerce.

WACS exploits advances in digital/optical communications and computation. Specific advantages include:

- Control for outages and conditions not covered by feedforward controls (SPS).
- Potentially simplifies operations for changing system conditions—presently operators are required to reduce power transfers when unstudied conditions are encountered.
- Improved observability and controllability compared to local control. Discontinuous control reduces exposure to adverse interactions.
- Flexible, high reliability "open system" platform for rapid, low-cost control and monitoring additions, including wide-area continuous control.
- Provides a combination of reliability increase and power transfer capability increase.
- Caters to uncertainty in simulation results used to determine operating rules and limits.
- Future potential with cost reductions and further technology advances. Potential for application in meshed grid as well as intertie corridors. Control inputs and outputs may be extended over a larger geographical area such as the entire western North American power system.

Moving from WAMS to WACS (wide-area measurements to wide-area stability control) is a challenge in the new century.

2.12 CONCLUSIONS

Financial and economic imperatives stemming from new requirements and demand growth in the power industry are being imposed on electric utilities, exerting pressure to adopt operational policies that promote greater financial returns, to the detriment of operational security. This new environment is in direct contrast to older models, which sought to create operational strategies aimed at minimizing costs within the context of established security and reliability levels.

Recent blackouts in a number of countries have shown the importance of implementing defense plans to respond to extreme contingencies. The philosophy behind protection against extreme contingencies is that a general power failure must not be the consequence of a situation that could reasonably have been avoided. The objective is therefore to preserve the integrity of the power system by using automatic measures that are simple, reliable, and safe for the system, and that provide the most extensive possible coverage against all possible extreme contingencies, bearing in mind at all times that simplicity should prevail over selectivity in determining the scope of the actions to be carried out.

In general, even though a power system is planned and designed to withstand any credible contingency, it can also be affected by more severe disturbances than those for which it was conceived, eventually leading to a partial or total frequency and/or voltage collapse.

The work to be done – a huge effort – must be directed at enhancing the ability of the bulk power system to withstand extreme contingencies, which are usually initiated by multiple faults, but which

may also be initiated by single faults associated with multiple or successive disconnections of transmission components.

Depending on the geographical extent and relative number of transmission lines in its main grid, as compared to the power transmitted, each system will be particularly sensitive to disturbances that could cause chain reactions that lead to the loss of several transmission lines. In fact, over the past years, several countries have experienced blackouts provoked by extreme contingencies.

Power systems in developing countries suffer from a large gap between demand and generation, inadequate transmission capacity, and non-uniform location of load centers and generation sources.

2.13 REFERENCES

[2-1] G. Trudel, J. P. Gingras, J.R. Pierre, Designing a reliable power system: The Hydro-Quebec's integrated approach; Special Issue of the Proceedings of the IEEE on Energy Infrastructure Defense Systems, May 2005, vol 93, number 5

[2-2] G. Trudel, S. Bernard, G. Scott, "Hydro-Quebec's Defense Plan against Extreme Contingencies", IEEE Transactions on Power Systems, Vol. 14, Nr. 3, August 1999

[2-3] Bernard, S.; Trudel, G.; Scott, G.; A 735 kV shunt reactors automatic switching system for Hydro-Quebec network, IEEE Transactions on Power Systems, Volume: 11, Issue: 4, Nov. 1996, Pages:2024 – 2030

[2-4] S. Shahnawaz Ahmed, Narayan Chandra Sarker, Azhar B Khairuddin, Mohd Ruddin B Abd Ghani and Hussein Ahmad, "A Scheme for Controlled Islanding to Prevent Subsequent Blackout"

[2-5] L. Chiesa, L. Druker, B. Cova, A. Lazzari, J. L. Magaz, P. Raffaele, J. Fraga, R. Gomez, "Study and Project of a Defense Plan against Network Collapse within an Electric Energy Liberalized Market: an Regional System of Greater Buenos Aires", The First EPRI Latin American Conference and Exhibition, November 2001

[2-6] Guo Jiayang, Chu Bingnan and Wang Huiren, "Remedial Action Schemes for North China 500 kV Power System», North China Electrical Power Research Institute

[2-7] P. Gomes, "Power System Operational Security: Diagnostics and Perspectives due to Power System Restructuring", D.Sc. Thesis, Escola Federal de Engenharia de Itajubá (EFEI), 1999

[2-8] P. Gomes, "New Strategies to Improve Bulk Power System Security : Lessons Learned from Large Blackouts", IEEE 2004 General Meeting, Blackouts Panel Session, Denver, August 2004

[2-9] A. F. Bondarenko, V. P. Gerikh, L.A. Koscheev, N. Kucherov, A. Tikhonov, "Reliability problems in UPS of Russia regimes management in market and insufficient network transmission capacity conditions", CIGRÉ 39th. Session, August 2002

[2-10] Shinichi Imai, "Identification of Different Scenarios of Extreme Contingencies", Tokyo Electric Power Company

[2-11] C Counan, C.C. Trotignon, E. Corradi ; G. Bortoni ; M. Stubbe; J. Deuse ,"Major incidents on the French electric system: Potentiality and curative measures studies", IEEE Transactions on Power Systems, Vol 8, Number 3, August 1993

[2-12] R. Salvati, M.Sforna,"Piano di Difesa del Sistema Elettrico, Gestore della Rete di Transmissione Nazionale", Monografia Técnica, October 2004

[2-13] Carson W. Taylor, Dennis C. Erickson, Ken E. Martin, Robert E. Wilson, Vaithianathan Venkatasubramanian, "WACS—Wide-Area Stability and Voltage Control System: R&D and On-Line Demonstration", IEEE Proceedings special issue on Energy Infrastructure Defense Systems, May 2005

3. ANALYSIS OF EXTREME CONTINGENCIES: MODELING OF POWER SYSTEM, ANALYTICAL TOOLS AND STUDY PROCEDURES

3.1 INTRODUCTION

When a major disturbance occurs, protection and control actions attempt to stop power system degradation, restore the system to a normal state, and minimize the impact of the disturbance. Existing control actions are not designed to respond to a fast-developing disturbance, and may react too slowly. In addition, dynamic simulation software is only applicable to off-line analysis. The operator must therefore deal with an extremely complex situation, and must rely on heuristic solutions and policies. Today, local automatic control actions protect the system from the propagation of fast-developing emergencies, but are not equipped to consider the overall system, which may be affected by the disturbance. Because of new constraints imposed by economic and environmental factors, the trend in power system planning is to maintain tight operating margins with less redundancy. The concept of the Wide-Area Defense Plan offers better detection and control strategies, which lead to better management of disturbances and significant opportunities for higher power transfers and operating economies. Wide-area defense is a concept that involves using system-wide information and sending selected local information to a remote location to counteract the propagation of major disturbances. With the increased availability of sophisticated computer, communications and measurement technologies, more "intelligent" equipment can be used at the local level to improve the overall emergency response.

The modern energy management system (EMS) is supported by supervisory control and data acquisition (SCADA) software; by numerous power system analysis tools such as state estimation, power flow, optimal power flow, security analysis, transient stability analysis, and mid- to long-term stability analysis; and by optimization techniques such as linear and non-linear programming. In terms of applying these tools in real-time during an emergency, the time available for running these application programs is the limiting factor, and a trade-off with accuracy is inevitable. Real-time optimization software and security assessment and enhancement software do not include dynamics. Furthermore, propagation of a major disturbance is difficult to incorporate into a suitable numerical algorithm, which means that heuristic procedures may be required. For example, unexpected hidden failures in relaying equipment may cause unexpected multiple contingencies. Given sufficient time, the experienced and well-trained operator can recognize the situation and react properly, but often not reliably enough or quickly enough. In modern interconnected networks, fast-developing emergencies may affect a wide area. Since operator response may be too slow and inconsistent, local and rapid automatic actions are implemented to minimize the impact of the disturbance. Currently, local automatic actions are conservative, acting independently of central control and not taking into account the prevailing state of the whole affected area. Future power systems will encounter new components (energy storage, load control, and solar power), new systems (FACTS elements and HV DC integration), and regulatory changes (power wheeling, NUGs). An intelligent and adaptive control and protection system for wide-area disturbances is needed in order to enable full utilization of the power transmission network, which will then be less vulnerable to a major disturbance.

Historically, only centralized control has been able to apply sophisticated analysis, because computer and communications support could be technically and economically justified only at this higher level. However, with the increased availability of sophisticated computer, communications and measurement technologies, more intelligence can now be applied at the local level. The degree to which the gap between central and local decisions and actions can be closed will depend on the degree of intelligence that is put into local subsystems. Decentralized subsystems that can make local decisions based on local measurements and remote information (system-wide data and emergency control policies) and/or send pre-processed information to higher hierarchical levels are an economical solution to this problem. A major component of wide-area defense is the ability to receive system-wide information and commands via the data communication system, and to send selected local information on power system status to the SCADA centre.

3.2 POWER SYSTEM DISTURBANCES AND REMEDIAL MEASURES

Phenomena that create wide area power system disturbances are divided, among others, into the following categories: angular stability, voltage stability, overloads, power system cascading, etc. They are fought against using a variety of protective relaying and emergency control measures.

3.2.1 Transient Instability (Angular) Disturbances

Transient (angular) instability has been a concern to utilities since the early days of the electric power industry. The research on this subject is extensive and many approaches have been thoroughly investigated in order to predict it.

The angular instability is caused by the rotor dynamics of generators. It manifests itself either in the form of undamped electromechanical oscillations, or in the form of monotonic rotor acceleration leading to the loss of synchronism. The former type of instability is initiated by small disturbances (i.e. small changes in system loading), while the later is initiated by large disturbances (i.e., loss of a major generator unit, a fault on the high-voltage transmission network, etc.). The location and type of a disturbance, as well as the transmission configuration and operating conditions in a power system, dictate the type of the resulting instability. Transient (angular) instability may involve a large geographical area and thus is classified as a wide-area disturbance.

The protection against transient instability and consequent out-of-step condition is a major concern for the utility industry. As mentioned, transient instability develops as a result of excessive power imbalance between generation and load following a major disturbance. The loss of synchronism can take place either on the first-swing, or after multiple swings. The first-swing out-of-step is a faster phenomenon than the multi-swing one, and thus requires faster detection and correction measures. The first-swing type of angular instability may develop in a fraction of a second, while the multi-swing instability may take more than half a second to develop.

Out-of-step transient instability can occur in several forms:

1. A single generator losing synchronism.
2. A single power plant losing synchronism.
3. A whole area of the power system (several plants) losing synchronism.
4. Many areas of the power system losing synchronism.

Out-of-step protection, as it is applied to generators and systems, has the objective to eliminate the possibility of damage to generators as a result of an out-of-step condition. In case the power system separation is imminent, it should take place along boundaries, which will form islands with matching load and generation. Distance relays are often used to provide an out-of-step protection function, whereby they are called upon to provide blocking or tripping signals upon detecting an out-of-step condition.

In addition to the above, transient instability may develop as a so-called inter-area mode, which is associated with coherent acceleration or deceleration of one group of machines in the power system against the reminder of the machines. When two or more such groups are involved in the disturbance, the resultant system dynamics may lead the power system to a complete blackout unless complex remedial action (mitigation) is attempted in the form of multi-area system separation into islands with balanced generation and consumption. The dynamics of multi-area oscillations is usually much slower than the single machine modes of oscillation. This phenomenon usually happens when the system consists of groups of machines tied electrically close together and interconnected to other groups by week ties.

3.2.2 Voltage Stability

Voltage stability is defined by the System Dynamic Performance Subcommittee of the IEEE Power System Engineering Committee [3-1] as the ability of a system to maintain voltage such that when load admittance is increased, load power will increase, and so that both power and voltage are controllable. Also, voltage collapse is defined as being the process by which voltage instability leads to a very low

voltage profile in a significant part of the system. It is accepted that voltage instability is load-driven, as opposed to the transient (angular) instability, which is generator-driven.

The risk of voltage instability increases as the transmission system becomes more heavily loaded. The typical scenario of these instabilities starts with a high system loading, followed by a relay action due to a fault, a line overload or hitting an excitation limit. The consequences of collapse often require long system restoration, while large groups of customers are left without supply for extended periods of time. Schemes that mitigate voltage collapse need to use the symptoms to diagnose the approach of the collapse in time to initiate corrective action.

Voltage instability can be alleviated by a combination of the following remedial measures: adding reactive compensation near load centers, strengthening the transmission lines, varying the operating conditions such as voltage profile and generation dispatch, coordinating relays and controls, and load shedding. Most utilities rely on planning and operation studies to guard against voltage instability. Many utilities utilize local voltage measurements in order to design load shedding schemes as a measure against incipient voltage instability [3-2].

3.2.3 Cascading Events

Outage of one or more power system elements due to the overload may result in overload of the other elements in the system. If the overload is not alleviated in time, the process of power system cascading may start, leading to complete power system separation. When a power system separates, islands with an imbalance between generation and load are formed, with a consequence of frequency deviation from the nominal value. If the generators cannot handle the imbalance, load or generation shedding is necessary. A special protection system or out-of-step relaying can also start the system separation.

A quick, simple, and reliable way to re-establish active power balance is to shed load by underfrequency relays. There are a large variety of practices in designing load shedding schemes based on the characteristics of a particular system and the utility practices [3-3, [3-4].

While the system frequency deviation is a final consequence of the power deficiency, the rate of change of frequency is an instantaneous indicator of power deficiency and can trigger incipient recognition of the power imbalance. However, change of the machine speed is oscillatory by nature, due to the interaction among generators. The oscillations depend on location of the sensors in the island and the response of the generators. The problems regarding the rate-of-change of frequency function are [3-5]

- A smaller system inertia causes a larger peak-to-peak value for oscillations. For the larger peak-to-peak values, enough time must be allowed for the relay to calculate the actual rate-of-change of frequency reliably. Measurements at load buses close to the electrical center of the system are less susceptible to oscillations (smaller peak-to-peak values) and can be used in practical applications. A smaller system inertia causes a higher frequency of oscillations, which enables faster calculation of the actual rate-of-change of frequency. However, it causes faster rate-of-change of frequency, and, consequently, a larger frequency drop.
- Even if rate-of-change of frequency relays measure the average value throughout the network, it is difficult to set them properly, unless typical system boundaries and imbalance can be predicted. If this is the case (e.g. industrial and urban systems), the rate of change of frequency relays may improve a load shedding scheme (scheme can be more selective and/or faster).

Adaptive settings of frequency and frequency derivative relays may enable implementation of a frequency derivative function more effectively and reliably.

3.3 MODELING ISSUES AND LIMITATIONS

Figure 3-1 shows the time frames of the various phenomena involved in loss of either angular stability or voltage stability [3-6].

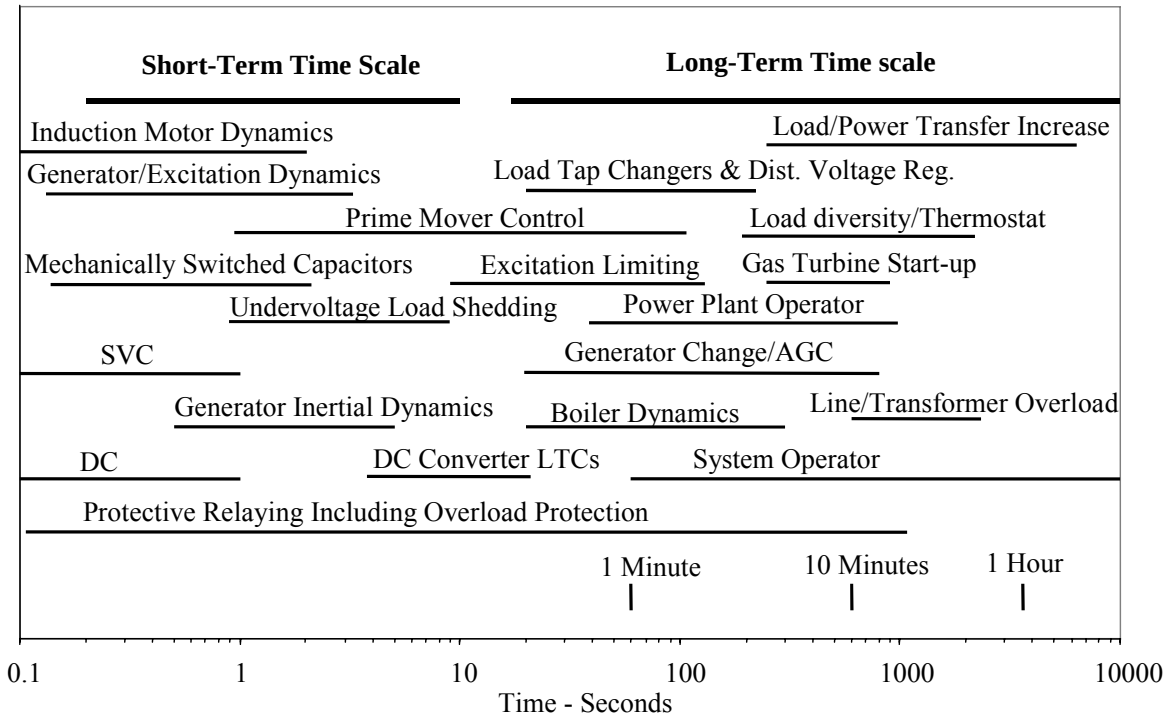


Figure 3-1 Time scales of power system dynamics (reproduced from [3-6]).

During the first ten seconds following a disturbance (short-term time scale), the system response is dominated by machine excitation systems and by the turbine-generator governors, as well as high Voltage Direct Current (HVDC) transmission, Static Var Compensators (SVC) and other fast acting devices. In this time frame, distinction between load-driven and generator-driven stability problems is difficult. Consequently, voltage stability and rotor angular stability problems require basically the same complexity of component models in the short-term time scale.

Simulation of the systems for more than about ten seconds (long-term time scale) requires modeling of the slower acting devices, such as under-load tap-changing (ULTC) transformers, generator field protection, power plant controls, boiler dynamics, AGC, etc., and the characteristics of the system loads. In this time frame there is a distinction between two types of stability problems: frequency problems and voltage problems. Frequency stability problems can occur following major disturbances resulting in the system islanding. They are related to the active power generation-load imbalance, but not to the network structure within each of connected areas. Following the initial response of the system, frequency is common throughout each island and the problem can be analyzed using single-bus equivalent, on which all generators and loads are connected.

Voltage stability problems are due to the electrical distance between generation and load and, therefore, dependent on the network representation. As such, voltage stability problems require a full network representation for their analysis.

3.3.1 Angular (Transient) Stability

The essence of the short-time dynamics is captured by the individual machine swing equations:

$$\frac{\partial^2 \delta_i}{\partial t^2} = \frac{\omega_0}{2H_i}\left[P_{mi} - P_{ei}\right] \quad i = 1, 2, \ldots, N \qquad \textbf{(3.1)}$$

where δ_I is the power angle of machine #i in the power system having N machines, H_i is its per unit constant of inertia, P_{mi} is the mechanical power delivered to the rotor shaft, and P_{ei} is the electrical power that the machine is delivering to the rest of the power system. It is a nonlinear function of the network state vector, consisting of the positive sequence voltage phasors at all system buses. In addition to the swing equation model, often used in classical transient stability analysis, more detailed models of machine dynamics include differential equations for prime mover and the governor, generator rotor circuit equations, excitation system, as well as stator equations (which are usually subjected to axis transformation before being incorporated into the transmission network equations.) The machine dynamic model is decided dependent upon the timescale of disturbances that it is supposed to analyze. As few as one differential equation (swing equation) can be sufficient to capture the essence of the dynamics in certain cases, whereas as many as 15 or more differential equations and machine may be needed to capture a more detailed nonlinear model of the dynamics, which may also involve dynamic load models.

The transient stability analysis involves a solution of a large set of differential and algebraic equations. Prefault power flow system analysis provides the initial values of network variables; the active and reactive power outputs and voltages at the generator terminals.

The overall representation of the dynamic power system model incorporates a more or less detailed model of the synchronous machines with the excitation system and the prime mover, the model of the transmission network which may incorporate static or dynamic load models, various motor loads (induction or synchronous motors are the most common types), as well as models of other devices, such as HVDC converters, static VAR compensators, and other FACTS devices involved in system operation. While a detailed analysis of the system model, especially synchronous machine model, would involve that a large portion of this report be dedicated to model development, we direct the reader to a reference [3-7], where such models are developed for different applications and with varying degrees of detail.

3.3.1.1 Load Modeling

Nonlinear loads are modeled as exponential or polynomial functions of bus voltage and frequency. Static loads are usually represented as loads with constant impedance characteristic and included in the network equations, while dynamic loads are represented as induction and synchronous motors.

3.3.2 Voltage Stability

Considering that voltage collapse can take place in different time scales (ranging from seconds to hours), the most effective approach for studying voltage stability is to introduce time-scale decomposition of the general power system model covering both the short and long term time scales.

3.3.2.1 Short-Term Time Scale

In the transient (short-term) time frame, voltage stability phenomena are often closely involved with angular stability phenomena. Low voltages in the system may result in loss of angular stability, and loss of angular stability may result in fluctuating voltages. In this time frame, voltage collapses are mainly caused by slowly cleared faults (for example, 3-phase fault with a breaker failure). Examples are the cascading collapse on August 22, 1987, that TVA experienced [3-8], and the significant voltage depression that Philadelphia experienced on July 1, 1992 [3-9].

The short-term time scale involves dynamics of synchronous generators, exciters, and controllers associated with generators (such as automatic voltage regulators and governors), induction motors, SVCs and HVDC.

A general power system model for the short-term time scale voltage stability analysis consists of the set of differential equations (modeling equipment behavior) that are constrained by the set of algebraic equations (modeling networks behavior) [3-10]:

$$\begin{bmatrix} \dot{\mathbf{x}} \\ \mathbf{0} \end{bmatrix} = \begin{bmatrix} \mathbf{f}(\mathbf{x},\mathbf{y},\mathbf{z_c},\mathbf{z_d}) \\ \mathbf{g}(\mathbf{x},\mathbf{y},\mathbf{z_c},\mathbf{z_d}) \end{bmatrix} \quad \textbf{(3.2)}$$

The function **f** describes the dynamics of the equipment and loads at the buses, while the function **g** describes the stator model, internal and external network model. The state variables **x** (such as generator angles, frequencies, and flux quantities, control state variables and dynamic load variables) are denoted as dynamic state variables. The algebraic variables **y** typically include the power flow variables such as the bus voltages and angles. The variables $\mathbf{z_c}$ and $\mathbf{z_d}$ represent the continuous and discrete state variable associated with slower acting devices. Typically, the transient stability program will assume that phenomena associated with these devices are slow and treat the corresponding state variables $\mathbf{z_c}$ and $\mathbf{z_d}$ as *constant*.

3.3.2.2 Long-Term Time Scale

Voltage collapses in the long-term time scale may result from loss of significant sources of local generation or reactive support, from loss of heavily loaded transmission lines, or from the fast load build-up. The example of the latter is the failure of the TEPCO (Tokyo Electric Power Company) system, which occurred on July 23, 1987 [3-11]. Voltage collapse in the long-term time scale can include effects from the transient time scale. A slow voltage degradation taking several minutes may end in a fast voltage collapse.

The long-term time scale captures dynamics of controllers (such as secondary voltage control, load-frequency control, ULTCs, shunt capacitor/reactor switching), protecting devices (such as over excitation limiters (OXLs) and armature current limiters), and phenomena (such as thermostatic and aggregate load recovery) that typically act over several minutes following a disturbance. The long-term dynamics are represented by continuous and discrete-time equations [3-10]:

$$\begin{aligned} \dot{\mathbf{z}}_\mathbf{c} &= \mathbf{h_c}(\mathbf{x},\mathbf{y},\mathbf{z_c},\mathbf{z_d}) \\ \mathbf{z_d}(\mathbf{k}+\mathbf{1}) &= \mathbf{h_d}(\mathbf{x},\mathbf{y},\mathbf{z_c},\mathbf{z_d}(\mathbf{k})) \end{aligned}, \quad \textbf{(3.3)}$$

where $\mathbf{z_c}$ and $\mathbf{z_d}$ represent the continuous and discrete long-term state vectors. The discrete variables change values from $\mathbf{z_d(k)}$ to $\mathbf{z_d(k+1)}$ at times t_k=k ΔT (k=, 0, 1, 2, …), where ΔT is a time step.

When studying long-term voltage stability problems, the Quasi Steady-State (QSS) approximation of the system model is used. The assumption is that the fast system is infinitely fast when dealing with the slow subsystem, and the short-term dynamic equations in (3.2) are replaced by the corresponding equilibrium equation (3.4):

$$\mathbf{0} = \mathbf{f}(\mathbf{x},\mathbf{y},\mathbf{z_c},\mathbf{z_d}) \quad \textbf{(3.4)}$$

Consequently, the QSS power system model for the long-term time scale voltage stability analysis is given as follows:

$$\begin{bmatrix} \dot{\mathbf{z}}_\mathbf{c} \\ \dot{\mathbf{z}}_\mathbf{d}(\mathbf{k}+\mathbf{1}) \\ \mathbf{0} \\ \mathbf{0} \end{bmatrix} = \begin{bmatrix} \mathbf{h_c}(\mathbf{x},\mathbf{y},\mathbf{z_c},\mathbf{z_d}) \\ \mathbf{h_d}(\mathbf{x},\mathbf{y},\mathbf{z_c},\mathbf{z_d}(\mathbf{k})) \\ \mathbf{f}(\mathbf{x},\mathbf{y},\mathbf{z_c},\mathbf{z_d}) \\ \mathbf{g}(\mathbf{x},\mathbf{y},\mathbf{z_c},\mathbf{z_d}) \end{bmatrix} \quad \textbf{(3.5)}$$

3.3.2.3 Load Modeling

Load characteristics are known to have a significant effect on the system voltage stability [3-12, [3-13, [3-14]. Loads are mostly voltage dependent and can provide considerable load power relief following a

voltage depression in the system caused by a system disturbance. In power flow programs, this effect is taken into account by modeling loads as a combination of constant impedance, constant current and constant power (ZIP model) or by using exponential load models (representing power consumption as a power function of voltage). However, static load models are sometimes insufficient to capture the dynamic behavior exhibited by many loads, such as motor-driven loads and thermostatically-controlled loads.

Induction motor loads have characteristics such that tend to maintain their active consumption and increase their reactive demand as the voltage drops. Induction motor loads are fast restoring loads (in the time frame of a second), and prone to stalling when voltage is low. As such, these loads can contribute to a fast voltage collapse following a fault and line clearing.

The *thermostatically-controlled loads* (e.g. space and water heating devices, industrial process heating devices, etc.) are voltage dependent and, therefore, reduce their power consumption following a voltage depression, but stay longer connected in other to maintain constant temperature. The aggregate effect of this is that thermostatically-controlled loads provide only temporary (10 to 30 minutes) load relief. The dynamic model of these loads have to be taken into account when running dynamic voltage stability simulations, especially if a significant number of LTCs reach their regulation limits following a disturbance.

When running dynamic simulations, it is appropriate to use generic loads that model the aggregate effect of many individual load devices and subtransmission system (such as series impedances of feeders, transformers between system buses and the actual loads, voltage control devices, etc.). An extensive bibliography on load models can be found in [3-15].

3.3.2.4 Network Modeling

The network power flows are usually modeled as instantaneous considering that the network transients are much faster than the midterm dynamics of equipment and load. The network model is expressed in terms of load flow equations. The real and reactive power balance equations for the load bus *i* are expressed as:

$$-P_{l,i} = V_i^2 G_{ii} + \sum_{j \neq i} V_i V_j Y_{ij} \cos(\delta_i - \delta_j - \theta_{ij}) \quad \textbf{(3.6)}$$

$$-Q_{l,i} = -V_i^2 B_{ii} + \sum_{j \neq i} V_i V_j Y_{ij} \sin(\delta_i - \delta_j - \theta_{ij}) \quad \textbf{(3.7)}$$

where j spans the buses adjacent to bus i, Y_{ij} is the modulo of *(i,j)* element of the bus admittance matrix Y_{BUS}, $G_{ij} = Re[Y_{ij}]$, $B_{ij} = Re[Y_{ij}]$, $\theta_{ij} = arg[Y_{ij}]$.

3.3.2.5 Power Flow Model

Most of the commonly used tools for voltage stability and security analysis relay on the conventional static power flow algorithm. Power flow algorithms for voltage stability analysis are based on a standard Newton-Raphson algorithm, which as any of the approximate techniques (decoupled, fast decoupled, etc.) reduces accuracy for the sake of speed, but in the situations where extreme nonlinearities abound (near stability boundary) such approximations are not acceptable.

$$\mathbf{0} = \mathbf{g(x, y)} \quad \textbf{(3.8)}$$

In traditional power flow programs, generators are modeled as voltage controlled PV buses, while the loads are modeled as constant PQ buses (which may be the source of significant problems and errors). Multiple slack buses are allowed for the situations where several infinite buses are present in the system. Also, a fixed real power dispatch of generators and fixed or instantaneously switched capacitors and reactors are assumed, along with instantaneous ULTC action. Constraints on generator

capability are most commonly applied as simple reactive power limits, although more detailed models are also used. For some applications, such as voltage stability analysis of the power system with highly nonlinear loads, load models need to be adapted to incorporate the dependencies to voltage deviations. In more than one case, such approach was needed in order to properly simulate the system behavior under complex voltage conditions (the problem was first recognized in the mid-80s, when a voltage collapse in Sweden could not be replicated in software simulations until appropriate changes in load models were introduced).

3.3.2.6 Hidden Relay Failures

Protection or relaying systems plays a very important role in events leading to power system blackouts or major disturbances encompassing wide areas. Failures or misoperations in various protection systems are very significant factor in the overall process of reported wide area disturbances. Of all the protection system failures, the ones that remain dormant or hidden until some unusual system events occur are the most important. A reason for that is since failures that lead to an immediate misoperation during normal power system states can be corrected right away and should not be a contributing factor in wide area disturbances. Of course, relays that are operating correctly according to their designed purpose can also contribute to the spread of large blackouts, especially if the blackout conditions are unusual or extreme.

The abnormal power system states are usually due to faults, heavy load, shortages in reactive power, etc. They can trigger the hidden failures to cause relay misoperations which can worsen the situation since the power systems may already be operated in an emergency state when those abnormal states occur, eventually leading to the wide area disturbances. A better understanding of the hidden failures is required to prevent or at least reduce the likelihood of the occurrence of the wide area disturbances due to the hidden failures.

Commonly used transmission relaying systems have been studied to identify possible hidden failures and their consequences on the power systems. A concept of region of vulnerability associated with each mode of hidden failure has been proposed. It is the region in which the hidden failure can cause a relay to incorrectly trip its associated circuit breaker. The relative importance of each region of vulnerability, called vulnerability index, is computed using steady-state and transient stability criteria. A larger value of the vulnerability index indicates that the relay, in which if that hidden failure mode exists, is relatively more important and can cause more serious wide area disturbances or has a higher possibility to cause the disturbances than the one with a smaller index. Therefore, more attention should be paid to those key relays to prevent the hidden failure and its consequences. A scheme of digital monitoring and control system is proposed for that task.

The analysis of North American Electric Reliability Council Disturbance Reports showed that around 70% of the reported wide area disturbances involved relaying systems or special protection systems. The involvement of the protection systems does not necessarily mean that they initiated the disturbances. Most of the disturbances were, however, initiated by some abnormal power system states due to severe weather, device failures, human errors, faults, heavy load, reactive power shortages, etc. The subsequent misoperations of the protection systems then further degraded the power system states and eventually caused the wide area disturbances. In other words, the hidden failures in the protection systems that had not been seen or detected prior to the disturbances were triggered by the abnormal events and caused the protection systems to misoperate.

A failure that results in an immediate trip without any prior events is not considered a hidden failure. The power system must be planned and operated to withstand the loss of any single element without exceeding the NERC criteria for reporting a disturbance. A hardware failure that results in a relay failing to operate its breaker and trip out a faulted line or device is also not considered a hidden failure since its backup protection must normally be provided for such contingency. A defect or malfunction that occurs at the instant of a fault or switching event, e.g., a hole in the blocking signal or an insulation failure caused by a surge, is similarly not considered a hidden failure since such a failure is not permanent and cannot be monitored or detected before hand.

After the regions of vulnerability have been identified, the next step is to calculate the relative importance of each region, called vulnerability index. One of the measurements that can be used to determine this index is the stability or instability of the system following some power system

contingencies: one caused by normal operations of healthy primary relays to clear a fault, and the other by the misoperation of a relay with a hidden failure.

One crude indication that the steady-stability limit is violated is the lack of a load flow solution. This can be determined by performing load flow calculations until no solution can be found. This process is time-consuming and it does not indicate how stable or unstable the system is.

It has been observed that of all the reported cases of major system blackouts (wide area disturbances) in North America, about 70% of the cases have relay system contributing to the initiation or evolution of the disturbance. On closer examination, it became clear that one of the major components of relay system misoperations is the presence of relays which have failed during service, and their failure is not known. Consequently, there is no alarm, and no repairs or replacements are possible. These *hidden failures* are different from straight relay misoperations, or failures that lead to an immediate trip. The hidden failures remain undetected (and substantially undetectable), until the power system becomes stressed, leading to an operating condition that exposes the hidden relay failures. For example, a common hidden failure mode may be an incorrect trip function supervised by a fault detector. If the system loading is not high enough to cause a pick up of the fault detector, the hidden failure of such a relay would not be exposed. On the other hand, during a stressed state, the fault detector could pick up, and now the hidden failure of the trip function would cause a false trip.

3.4 ANALYTICAL TOOLS FOR EXTREME CONTINGENCIES

3.4.1 Angular (Transient) Instability

The most common predictive scheme to combat loss of synchronism is the Equal-Area Criterion and its variations. This method assumes that the power system behaves like a two-machine model where one area oscillates against the rest of the system. Whenever the underlying assumption holds true, the method has potential for fast detection.

The objective of out-of-step relaying as it is applied to generators and systems is to eliminate the possibility of damage to generators as a result of an out-of-step condition; and, in the case of the power system, to supervise the operation of various relays such that when a system separation is imminent, it should take place along boundaries which will form islands with matching load and generation.

A careful analysis of the various types of out-of-step conditions shows that they can be lumped into two main categories: a two-area instability and a multi-area instability. The state of the art in out-of-step relaying has focused only on the two-area instability since it is a well-understood phenomenon and is easier to analyze.

The traditional "equal area criterion" is a graphical method of explaining one form of the out-of-step condition, when only one group of the generators accelerates against the rest of the power system. The equal area criterion also provides the mechanism to accurately predict, under some modeling assumptions, the critical clearing time of a disturbance. When the system instability exhibits itself as three or more groups of machines losing synchronism, the equal area criterion is inadequate for predicting the critical clearing time. Some attempts to extend the equal area criterion for multi-area instability exist in the literature under the title of "extended equal area criterion". The fundamental difference between two-area out-of-step and a multi-area out-of-step is that the machine angle motion is restricted along one direction in the two-area case, while it is allowed to move in any direction in a high-dimensional space in the multi-area case. Thus searching along one direction to predict instability is relatively easy for the two-area instability and is very difficult for the multi-area case.

If the out-of-step condition is manifested as only two groups of machines losing synchronism, then as the angle separation between the two areas increases, the apparent resistance measured by a relay at the mid point between them decreases and the voltage at the mid point sags. It is therefore beneficial for the power system to bring about an orderly breakup of the system as early as possible in the disturbance. However, the detection or prediction of out-of-step and subsequent system breakup should not be hastily done in order not to jeopardize dependability. Many approaches have been invented to quickly predict or monitor the angular instability.

3.4.2 Voltage stability

Voltage instability is typically manifested by several distinguishing features: low system voltage profiles, heavy reactive line flows, inadequate reactive support, heavily loaded power systems. Voltage collapse typically occurs slowly and then quickly, with, a symptomatic period that may last in the time frames of a few seconds to several minutes, sometimes hours. The onset of voltage collapse is often precipitated by low-probability single or multiple contingencies.

Studying voltage collapse requires complementary use of dynamic and static analysis techniques.

Dynamic analysis of the system provides an insight into the time responses of the system, such as determination of the time sequence of the different events leading to system voltage instability, especially following fast disturbances of the system structure, which may involve in equipment outages, or faults followed by equipment outages. Long-term dynamic simulation either with detailed dynamic modeling or simplified QQS modeling (3.4) allows an accurate assessment of critical power system problems. However, time-domain simulations are time consuming (in terms of CPU) and, therefore, impractical when considering a large number of scenarios and contingencies. In addition, dynamic analysis does not readily provide information regarding the sensitivity or degree of the system instability.

If the system parameters change slowly (for example, fluctuations of the system load), they cause the stable equilibrium of the system to move slowly, which makes it possible to approximate voltage profile changes by a discrete sequence of steady states. In other words, *static (steady-state) analysis* of the system is quite appropriate. Static analysis may include power flow methods, sensitivity analysis, as well as traditional local analysis (e.g., P-V and Q-V curves). Static analysis of voltage collapse mainly relies on bifurcation theory.

A useful compromise between static and dynamic analysis is midterm simulation [3-10].

3.4.2.1 Bifurcations and Voltage Collapse

Bifurcation theory describes typical ways in which a power system can become unstable. It assumes that the power system is described with a set of differential equations (3.9) and that system parameter λ varies slowly (e.g., load injections). Another assumption is that the system model has a stable operating point (equilibrium x_0) for a certain value of the load parameter vector λ_0.

$$\dot{x} = f(x,\lambda) \qquad \textbf{(3.9)}$$

As the parameter λ varies slowly, the stable equilibrium point x_0 moves in the state space and can become unstable or even disappear. In both case, the system loses its stability.

In the first case, the equilibrium point exists but becomes unstable following the parameter variation. The system loses its stability through abrupt appearance of self-sustained oscillations or a growing oscillatory transient. This type of oscillatory instability is consistent with Hopf bifurcation (HB), and is of less interest in voltage collapse, since voltage collapse is not often observed to be oscillatory.

In the second case, for some critical parameter value λ^*, a stable equilibrium point x_0^{λ} (see **Figure 3-2**a) disappears by coalescing with an unstable equilibrium point x_1^{λ} on the system stability boundary (see **Figure 3-2**b). This type of monotonicinstability is consistent with Saddle node bifurcation (SNB). The consequence of SNB is that system states dynamically collapse [3-16].

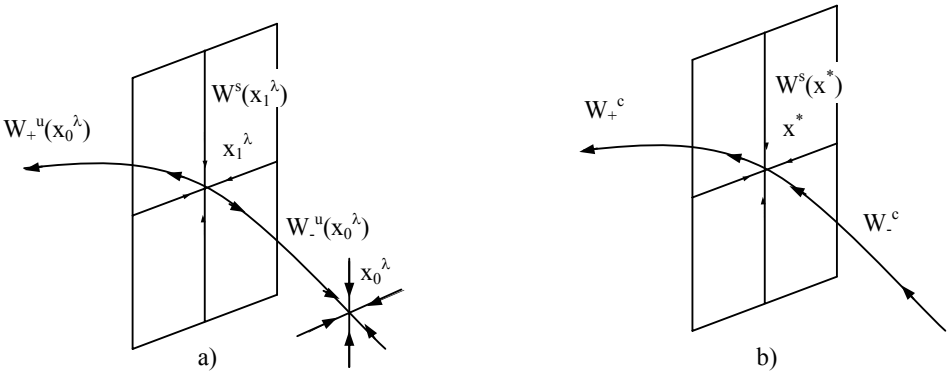


Figure 3-2 a) Just before bifurcation; b) At bifurcation.

The *Jacobian matrix* f_x of the system model evaluated at the operating point x^*, consistent with the critical parameter value(s) λ^*, is *singular* and has one zero eigenvalue and *n-1* eigenvalues with negative real parts (stable). The system state x^* has a one *dimensional center manifold* $W^c(x^*)$, along which the system state collapses, and *n-1* dimensional stable manifold $W^s(x^*)$. If load parameter λ increases beyond some critical value λ^*, then the stable operating point (i.e. equilibrium x^*) disappears and there are no other equilibrium points nearby to which the system state may transition.

Bifurcation does not account for the large disturbances found in some voltage collapses. However, some concepts of bifurcations can be reused to study large, sudden disturbances as well. One key idea is to split dynamics into fast and slow [3-10]. When studying the slow dynamics, the fast dynamics can be approximated as instantaneous. During the fast transients, the slow variables can be considered as practically constant.

Figure 3-3 shows a trajectory of the load voltage *V* when active (P) and reactive (Q) power change slowly and independently. The Figure also shows the active and reactive power margins as projections of the distances. The voltage stability boundary is represented by a projection onto the PQ plane (a bold curve). It can be observed that: *i*) there may be many possible trajectories to (and points of) voltage collapse; *ii*) active and reactive power margins depend on the initial operating point and the trajectory to collapse.

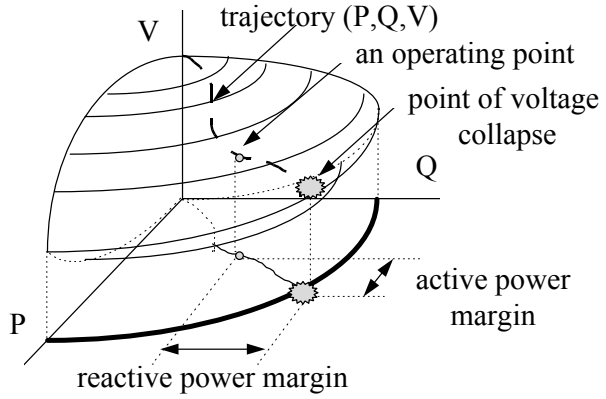


Figure 3-3 Symbolic depiction of the process of coalescing of the stable and unstable power system equilibrium (SNB) through slow load variations, which leads to a voltage collapse (a precipitous departure of the system state along the center manifold at the moment of coalescing). VPQ curve

representing the trajectory of the load voltage V of a 2-bus system model when active (P) and reactive (Q) power of the load can change arbitrarily.

3.4.3 Continuation methods:

Given current operating state of the system x_0 and corresponding system parameter λ_0, an obvious question is: "How far is the system from the stability boundary when load or a transfer is increased?"

Continuation is applicable to any power system model of form (3.1), (3.4) or any static power system model equivalent to some underlying different equivalent model of the form (3.5) and for any parameter space.

Continuation is a robust and efficient way to compute a series of load flow solutions as loading or transfer amount is increased. The continuation methods determine the bifurcation point, x^*, and the load margin, from the load flow equations, augmented by the continuation variable parameter(s). There are many variations of continuation methods, and the widely used are of the predictor-corrector type [3-17, [3-18]. A continuation algorithm starts from a known solution and uses the corrector-predictor scheme to find the subsequent solutions at different parameter values λ. It gives a continuum of power flow solutions for different values of parameter λ. The main advantages of the method are that it does not require a good initial guess; it can take account of generator reactive power and other system limits and operator actions as load increases and margin sensitivities are quick to compute [3-19, [3-20].

In the *predictor step*, it is assumed that load λ can be parameterized as a scalar. Suppose that the *i-th* step of the continuation process and the *i–th* solution (x^i, λ^i) are known. Then, an approximation of the next solution (x^{i+1}, λ^{i+1}) is found by taking an appropriate step in a direction tangent to the solution path. In the corrector step, a slightly modified Newton-Raphson algorithm is used to find the next iterative operating point after the predictor produces an approximation $(\overline{x}^{i+1},\overline{\lambda}^{i+1})$ of the next point (x^{i+1},λ^{i+1}). Since the predictor gives an approximation in a close neighborhood of the next point (x^{i+1},λ^{i+1}), a few iterations of the *corrector* usually suffice to achieve the needed accuracy. The only task left to do after the predictor-corrector step is to check whether the critical point has been overreached. The tangent component corresponding to the direction of load λ is zero at the critical point, and is negative beyond the critical point. Thus, once the tangent vector has been calculated in the predictor step, a test of its sign will reveal whether or not the critical point has been reached. Continuation methods are the most computationally economical way to obtain information about voltage stability in power systems. It is feasible to run continuation for practical sized systems to accurately compute the loading or transfer margin to voltage collapse under a range of contingencies (e.g. [3-21]). If the base case is obtained from a state estimator, these calculations can be done in near real time. An important advantage of these margin calculations is that the sensitivity of the margin is very quick to compute [3-19, [3-20] and can be used to quickly select controls to increase the margin or to determine the impact of uncertainty on the margin **[3-22**].

It is also possible to estimate a worst case direction of loading that causes voltage collapse (the closest bifurcation) and the corresponding minimum stability margin to voltage collapse. This can be done by iterating continuation and normal vector computations or by optimization or direct methods [3-23, [3-24, [3-25].

Another approach is to directly measure parameters that are indicators that correlate with voltage collapse. Although these measurements cannot address preventative control for contingencies that have not occurred, these methods are very fast and could be used in real time for emergency controls once the contingency has occurred. An example of such indicator is the sensitivity of the generated reactive powers with respect to the load parameters (active and reactive powers of the loads). When the system is close to a collapse, small increases in load result in relatively large increases in reactive power absorption in the system. These increases in reactive power absorption must be supplied by dynamic sources of reactive power in the region. At the point of collapse, the rate of change of generated reactive power at key sources with respect to load increases at key busses tends to infinity.

The sensitivity matrix of the generated reactive powers with respect to loading parameters is relatively easy to calculate in off-line studies, but could be a problem in real-time applications, because of the need for system-wide measurement information. Large sensitivity factors reveal both critical generators

(those required to supply most of the newly needed reactive power), and critical loads (those whose location in the system topology imposes the largest increase in reactive transmission losses, even for the modest changes of their own load parameters). The norm of such a sensitivity matrix represents a useful proximity indicator, but one that is still relatively difficult to interpret. It is not the generated reactive power, but its derivatives with respect to loading parameters which become infinite at the point of imminent collapse.

3.4.4 Voltage Stability Study Procedures

Utilities estimate voltage security of the power system based on the voltage security criteria accepted by the utility, such as:

1. *Voltage stability margin criteria* (e.g., the system VS margin must be larger than x% of the total system loading under all or credible contingencies).
2. *Voltage decline/rise criteria* (e.g., the post-contingency bus voltages must remain within ±x% of the nominal/pre-contingency voltages following all or credible contingencies).
3. *Reactive reserve criteria* (i.e., the reactive power reserves of individual or groups of VAr sources must be above x% of their normal (no contingencies) reactive output under all or credible contingencies).
4. *Maximum post-fault voltage dip criteria* (i.e., the post-fault bus voltage dips must be less than x% of their nominal/pre-contingency voltages).
5. *Maximum transient dip duration criteria* (e.g., following a fault, the bus voltages must recover above x% of their nominal/pre-contingency values for less than *N* cycles).

The system is considered voltage secure if the utility VS stability criteria are met for all contingencies.

For the sake of reducing CPU time requirements, a practical approach to voltage assessment is to use traditional contingency screening tools to identify contingencies that might cause voltage problems, under the certain operating conditions (e.g., peak load, 5% above peak load, etc.). Good candidates for more thorough analysis are the contingences that result in low post-contingency voltages and/or large voltage variations at the system buses, low generator reactive reserves, etc. Also, the contingencies for which the cases won't solve raise a flag. Further continuation analysis of the system for the selected outages and selected system loadings and transfers will provide a measure to how "robust" the system is, what the critical generator and voltage spots are, etc. One can also identify possible type and locations for compensation.

At this point, time-domain (dynamic) simulations are desirable to augment the continuation power flow results. Short-term dynamic simulations will reveal if there is danger of the system separation and fast voltage collapse, while long-term dynamic simulation will reveal what mechanism drives voltage collapse (slow protection schemes, load dynamics, LTCs, etc.) and how severe it is. Long-term dynamic simulations are typically run up to 5 minutes. To deal with the intrinsic complexities of large power system analyses, in recent years parallel processing on distributed environments using systems composed of pools of computers interconnected by commodity networks has been exploited. An example of that approach is presented in [3-49].

3.5 OVERLOAD AND POWER SYSTEM CASCADING

The overloaded elements need to be alleviated in a time range dependent upon line thermal limits, overload severity, temperature, and loading history. Outage of one or more elements may cause overload of other elements in the system. Thus, if overload is not alleviated in time, the process of power system cascading may start, leading to the formation of isolated areas (islands) with an imbalance between generation and load. An imbalance in active power results in a frequency deviation - either underfrequency or overfrequency. If the imbalance is very small only some generation adjustments may be enough to restore the frequency back to normal. However, if the imbalance is large but manageable, load or generation shedding is necessary. It is important to notice that centralized on-line AGC control, designed for normal operation, is not designed for an emergency.

The separation can also be initiated by a special protection system or an out-of-step relaying. A special protection or remedial action scheme may initiate the separation upon the loss of a critical line when its line loading exceeds a certain threshold.

Overload

Thermal overloading of system elements leads to a loss-of-life, and persistent overload needs to be alleviated either manually or automatically. The thermal capabilities for transmission elements are matter of engineering judgment. Utilities define Short Term Emergency (STE) rating and Long Term Emergency (LTE) rating. The time scale considered is in a range of several minutes to several hours. Outside temperature, loading history, and time constant of the overloaded element need to be considered for accurate assessment of the thermal violations. In addition, a transmission line may sag, causing a fault and a consequent line outage. Further, the load impedance may enter operating zone of the distance relays. Overload capabilities of the line may be limited by the settings of the distance relays.

Measures to relieve overloaded elements may be divided into primary and secondary. The primary measures for relieving overloaded elements are:

a. generation shifting,
b. phase shifting,
c. load shedding,
d. controlled power system separation,
e. line switching,
f. tie line rescheduling, and
g. starting gas turbines.

Last two measures are primarily for alleviating tie-line overload. The secondary measures for relieving overloaded elements are:

a. generation dropping,
b. capacitor/reactor switching,
c. load control, and
d. voltage reduction.

3.5.1 Controlled System Separation

If a loss-of-synchronism is detected, a controlled system separation is initiated by a pre-determined switching strategy. Separation points should be chosen with a goal to split a system into islands with a power system balance. However, since this is usually not possible, load or generation shedding needs to be initialized.

System studies, with some pre-determined system loading profiles, may show that an unstable swing will certainly develop due to the loss of a certain line. An immediate initiation of the separation will obviously be preferable to waiting for the unstable swing to actually develop before the initiation can take place. The latter is required for the operation of an out-of-step relays. The threshold setting, however, may be too low or too high since the current system loading profile may be quite different from the one used to determine the setting. In other words, the special protection system takes only the local information, which is the loading level of the line in concern, as its input, not the prevailing system states.

The overload and the rate-of-change of power on the tie line may be indicators of a power deficiency in the import area. Some utilities use rate of change of power relays and/or frequency relays to separate power system at pre-determined points to prevent complete blackout.

When a power system enters an "in extremis" crisis, islands with an imbalance between generation and load are formed with a consequence of frequency deviation from a nominal value. Firstly, a frequency response of a synchronous machine will be described. If losses in the machine are neglected, a frequency response of the machine may be calculated by solving following equation:

$$f * \frac{df}{dt} = \frac{f_n^{\,2}}{2H} * (p_m - p_e) \qquad \textbf{(3.10)}$$

where*:*

p_m (p.u.) is a mechanical input power (on the machine rated MVA basis)

p_e (p.u.) is an electrical output power (on the machine rated MVA basis)

H (MWs/MVA) is an inertia time constant (on the machine MVA basis)

f (Hz) is a frequency and f_n is a nominal frequency.

In a multi-machine power system, the generation deficiency is distributed among all machines. After a short period, this distribution depends on relative inertia constants of the machines. If frequency in the system is assumed uniform, equation (3.7) may still be used. Then, p_m, p_e, and H are total system load on the total power system rating basis, total system generation on the total power system rating basis, and a composite inertia constant, respectively.

An actual power deficit should be distinguished from an initial power deficit because of physical constraints in delivering a power from the generators to the loads (p_e in (3.10) is limited). Overloading of the generators is followed by decrease in system voltages. Voltage decrease causes considerable instantaneous decrease of the constant impedance load power. Other phenomena that follow active power imbalance are:

a. speed governing system of the generator unit tends to re-establish nominal rotating speed by increasing turbine output,
b. internal voltage and reactance of generator vary, and
c. dynamic load power decreases with frequency decline.

Thus, actual power deficit is always smaller than the initial one and a maximum rate of change of frequency is limited.

It is important to consider the hazardous influence of the frequency deviation on elements of the power system. Nuclear and thermal units are especially sensitive to frequency deviation. The limiting conditions are a possibility for turbine blade damage, due to the resonant vibrations and problems with the auxiliary equipment. The greater the deviation from the nominal values the shorter the turbine permissible operating time. The turbine damages are cumulative and turbine lifetime is shortened whenever frequency declines 2-3% under nominal.

3.5.2 Power laws and blackout risk

It is apparent that large blackouts are rarer than small blackouts, but how much rarer are they? We consider the statistics of major North American power transmission blackouts from 1984 to 1998 obtained from the North American Electrical Reliability Council (NERC) [3-27]. One might expect a probability distribution of blackout sizes to fall off exponentially. However, analyses of the NERC data show that the probability distribution of the blackout sizes does not decrease exponentially with the size of the blackout, but rather has a power law region [3-28, [3-29].

For example, **Figure 3-4** plots on a log-log scale the empirical probability distribution of energy unserved in North American blackouts. The fall-off with blackout size is close to a power dependence with an exponent between –1 and –2. (Note that a power dependence with exponent –1 implies that doubling the blackout size only halves the probability, whereas in a distribution with an exponential tail, doubling the blackout size squares the probability. A power law dependence with exponent –1 appears as a straight line of slope –1 on a log-log plot.) Thus the NERC data suggests that large blackouts are much more likely than might be expected from the common probability distributions that

have exponential tails. The power law region is of course limited in extent in a practical power system by a finite cut off near system size corresponding to the largest possible blackout.

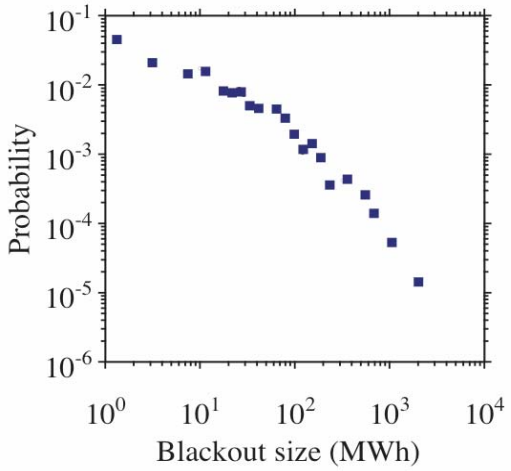


Figure 3-4 North American blackout size probability distribution.

Blackout risk is the product of blackout probability and blackout cost. One can assume that blackout cost is roughly proportional to blackout size, although larger blackouts may well have costs (especially indirect costs) that increase faster than linearly [3-30]. In the case of an exponential dependence, large blackouts become rarer much faster than blackout costs increase so that the risk of large blackouts is negligible. However, in the case of a power law dependence, the larger blackouts can become rarer at a similar rate as costs increase, and then the risk of large blackouts is comparable to or even exceeding the risk of small blackouts [3-31]. Thus power laws in blackout size distributions significantly affect the risk of large blackouts. Standard probabilistic techniques that assume independence between events imply exponential tails and are not applicable to systems that exhibit power laws.

3.5.3 Loading dependent cascading failure

Consider cascading failure in a power transmission system in the impractically extreme cases of very low and very high loading. Here "loading" refers to an overall system-wide loading of the power system components. At very low loading near zero, any failures that occur have minimal impact on other components and these other components have large operating margins. Multiple failures are possible, but they are approximately statistically independent so that the probability of multiple failures is approximately the product of the probabilities of each of the failures. Since the blackout size is roughly proportional to the number of failures, the probability distribution of blackout size will have an exponential tail. The probability distribution of blackout size is different if the power system were to be operated recklessly at a very high loading in which every component was close to its loading limit. Then any initial disturbance would necessarily cause a cascade of failures leading to total or near total blackout and the probability distribution of blackout size has all the probability concentrated near total blackout. The probability distributions of blackout size in the very low and very high loading cases are sketched in **Figure 3-5**. It is clear that the probability distribution of blackout size must somehow change continuously from the exponential tail form to the certain total blackout form as loading increases from a very low to a very high loading. One way that this transition can occur is that there is an intermediate loading at which the probability distribution of blackout size has a power law dependence as sketched in **Figure 3-5**. We call this loading a critical loading (this terminology arises from the analogous phase transitions in statistical physics). The critical loading transition can be observed in abstract models of cascading failure [3-32] and in power system models of cascading blackouts [3-33, [3-34].

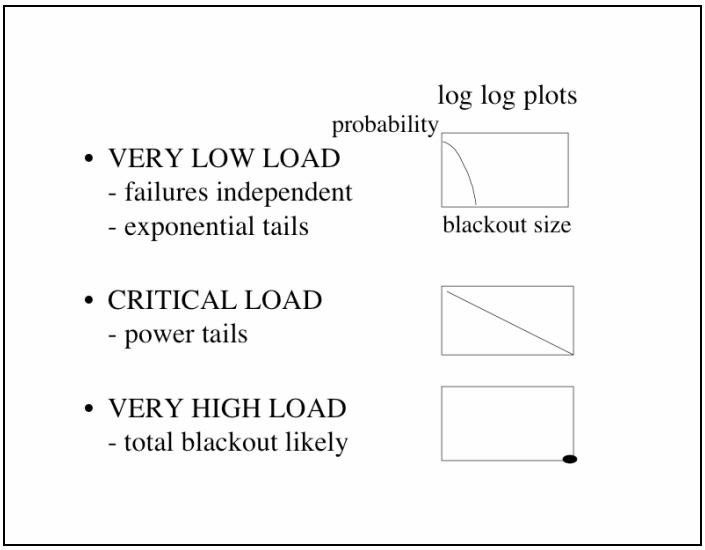


Figure 3-5 Qualitative effect of loading on blackout probability distribution.

Thus we arrive at a first level of qualitative explanation of power law behavior in the probability distribution of blackout sizes. Large blackouts are typically caused by intricate series of cascading rare events. The events are not independent because each event tends to further stress and weaken the system and make subsequent events much more likely. This dependence between events becomes stronger as overall system loading increases and makes the longer series of events causing large blackouts relatively more likely. At some critical loading, the power law region of the probability distribution occurs, and then there is substantial risk of a cascade of events that blacks out a substantial portion of the network. Well below the critical loading, the larger blackouts become much more unlikely and above the critical loading the largest blackouts become increasingly likely. The proximity to a critical loading could function as a margin for increased risk of cascading failure and an indicator of overall system stress. Development of methods to monitor or compute these quantities from real or simulated data is a current research goal [3-36, [3-37, [3-38]. The analysis of overall system stress with respect to cascading failure is complementary to deterministic n-k security criteria or more advanced probabilistic methods such as [3-39] that aim to reduce the risk of the initial cascading events.

3.5.4 Network evolution to near criticality

We now suggest how the slow, opposing forces of load growth and engineering responses to blackouts could drive power transmission systems to operate near criticality. Load growth is inexorable (about 2% a year in North America) and this slowly increases component loadings in the transmission system, decreases security, and increases the chances of cascading failure. If the system is at a suitably low overall loading, the chance of cascading failure increases only slightly. Moreover there is a strong economic incentive to increase component loading so that proper revenue can be generated from the infrastructure investment. Thus the system loading will increase. However, if the system load is near or above critical loading, large blackouts become much more likely. If a blackout occurs, then power system engineers make prodigious efforts to strengthen the parts of the system involved in the blackout by upgrade, repair and improved procedures and all these have the overall effect of reducing the power system loading relative to its capability. There are similar, but less intense, responses to simulated blackouts.

Thus load growth increases system loading, reduces reliability and causes blackouts, but blackouts cause increased reliability and in effect cause reduced system loading. It is plausible that the power system evolves to be operated at a complex system equilibrium that, although dynamically changing, hovers near a critical loading relative to the current power system capability. Indeed approximate models of these slow dynamics do converge to such equilibrium [3-40]. The implication is that strong economic, societal and engineering forces may be driving the power system to be operated near a critical loading at which there are power tails and significant risk of blackouts of all sizes. The idea that the system inherently converges to near criticality is found in a range of other physical systems and is known as self-organized criticality [3-41].

3.5.5 Blackout risk mitigation

The existence of complex dynamics in the evolution of networks may have important implications for efforts to reduce the risk of blackouts. For example, the dynamics can be such that apparently sensible measures to reduce the frequency of small blackouts can eventually lead to an increase in the frequency of large blackouts and even increase the overall risk of blackout. This can occur because the network and its loading are not fixed, and reducing the frequency of small blackouts will eventually allow higher loadings that make large blackouts more likely [3-31]. This possibility of these complex dynamics highlights the need to define the problem of avoiding blackouts as the problem of jointly manipulating the frequency of blackouts of all sizes rather than simply avoiding blackouts in general.

3.5.6 Automatic Restoration with Frequency Relays

Power system restoration after major disturbance is executed with well-defined procedures that require overall coordination inside the restoring area and with the rest of the system. There are a number of possible restoration scenarios and the operator tries to execute the optimal procedure with the help of the computer restoration software.

Some utilities use frequency relays to restore load which is shed by underfrequency protection. Only about 30% of the shed load is restored automatically and in small steps. Automated load restoration may be initiated in several frequency steps or at one frequency and several time-delayed steps. Coordination with frequency relays is crucial to avoid frequency oscillation and new disturbance (e.g., line overload). However, automated load restoration is rare because other factors beside frequency should be considered during restoration (priorities, synchronization with the rest of the system, disturbance propagation, etc.).

3.5.7 Possible Improvements in Control and Protection

Automated load shedding that will reduce overloading before the system is isolated is an improved solution in comparison to underfrequency load shedding. Although local measurements may suffice if tasks are simple (e.g., protection against few contingencies only), information communicated either from central location or from remote substation seems necessary for more sophisticated requirements.

Loss of an important line can cause severe problems. However, importance of the lines varies constantly with network conditions. The appropriate identification of the network state during an emergency can elude unintentional transitions or avoid unnecessary loss of customer load. For example, by delaying the trip of the overload protection for the critical line allows more time for corrective actions.

Schemes for controlled separation of the system should adapt their thresholds and separation points as the prevailing system conditions change. For example, separation points should be selected to achieve optimal balance between load and generation in each separated area. Appropriate switching actions may be pre-determined or calculated on-line. In addition, if shedding actions need to be initiated, it may be done simultaneously with separation initiation. In any case, load and generation need to be periodically calculated at central location and high-speed communication to and from remote location is required.

If power system blackout is imminent, generator units should be isolated with load to speed-up restoration procedure. Separation points should be selected based on load and generation conditions either by pre-determined or on-line calculations.

If underfrequency load shedding cannot be avoided, improvements may be achieved by avoiding drawbacks discussed in section 4.3.1.3. It may be done by providing additional information to local relays on prevailing load, line flow, and generation conditions. Although, remote information is usually necessary, additional local measurement may also improve protection. For example, voltage measurement may control problems related with overvoltage. Further, since load shedding is a measure for both underfrequency and voltage problems, more sophisticated device may improve protection for both phenomena.

Adaptive settings of frequency and frequency derivative relays may enable implementation of frequency derivative function more effectively and reliably. Development of an accurate estimate of average frequency derivative, indifferent to oscillations, may be needed.

3.6 MULTIPLE CONTINGENCIES AND FAST-EVOLVING BLACKOUTS

Transmission systems are designed to interconnect generation stations and distribution utilities and to transmit bulk power from generation stations to major load centers. An adequately designed transmission system operating with a sufficient security margin is capable of withstanding single or multiple contingencies without causing instability and cascading outages. The most commonly used reliability criteria for transmission planning and operation is the N-1 criterion, which requires a transmission system to be developed and operated at all load levels and meet the most severe single contingency in additional to any scheduled outages. As multiple contingencies are beyond the planned and operational limits of a power system, the occurrence of any multiple contingencies, may lead to overloading and cascading trips on the network.

3.6.1 Causes of multiple contingencies

- Evolution of a localized fault by trips initiated from conventional back-up protection, or false trips of protection relays, or due to hidden failures of relays.
- Sequential faults.
- Severe weather or geomagnetic induced currents.
- Natural disasters such as earthquakes.

3.6.1.1 Backup Protection & Multiple Contingencies

Conventional back-up protection is designed to protect a region of a network and is required to operate only when the main protection has failed to clear a fault. It is heavily skewed towards dependability as faults on the network must be cleared to maintain the operation of the power system. With a limited view of the protected network from the inputs measured locally, conventional back-up protection generally takes action to protect the local equipment without considering the impact on the entire network. It may trip a circuit breaker remotely (no-selectivity) and may operate under heavy loading conditions (misoperation). Multiple contingencies are the consequence of tripping initiated by conventional back-up protection relays. The interesting issue here is that conventional back-up protection may be operating as designed when multiple contingencies occur, pushing the power system beyond the planned limit. As loads on the disconnected lines are transferred to their adjacent lines, they may overload them and trigger cascading trips on the network leading to a widespread blackout. This issue is further aggravated in a competitive environment as transmission lines are pushed to operating close to their limit. It is more likely that overloading of lines leading to the trip of the associated circuit breakers will happen more frequently in a deregulated power system.

To prevent the occurrence of cascading outages on the network, it is necessary to vertically review and harmonize protection design practices in power system planning, operation and protection, particularly back-up protection. It is essential to ensure a power system is planned and operated in a way in which the power system can withstand contingencies caused by the designed protection actions, or that the protection system is designed and applied in a way in which it will not, at least in principle, push the power system beyond its design limit. Therefore, the protection system applied including back-up protection will not cause any multiple contingencies during a single localized event.

3.6.1.2 Wide-Area Back-up Protection as a Preventive Measure

There are two ways in which wide-area backup protection can prevent cascading outages [3-42], [3-43]: (1) Precise location of a fault and thereby so as to exclude unfaulted elements so that only the circuit breakers necessary to isolate the fault are tripped. (2) Avoidance of unnecessary trips, due to hidden failure, current reversing or overloading, by blocking the trip signals of conventional back-up protection relays. The essential element required to implement wide-area backup protection is the availability of system-wide information which requires inter- and intra-substation communications. The back-up protection expert system (BPES) implemented in the UK consists of a BPES data acquisition and communication system, a BPES monitoring system, an expert system and breaker tripping system, operates in a normal or an emergency modes. The BPES monitoring system stays active and monitors the operational response of conventional protection relays. On the detection of a fault, a timer will be set and the expert system will be invoked after a pre-set time delay of 200 ms has expired. The expert system, which usually is in an inactive state, analyses the action factors of the lines that are likely to be affected by the fault and decides on the best way to isolate the fault that has failed to be cleared by the main protection. The BPES blocks the trips that are additional to the fault isolation if blocking is allowed.

Dynamic equipment ratings are also important, since the need of providing a reliable and safe service has historically induced the asset owner to adopt a conservative strategy in loading power components. This worst-case approach decreases the risk of malfunctioning at the cost of a reduced power transfer capability. As a consequence, the conservative approach appears to be inadequate in the new scenario where the aim for reducing undesirable actions such as load shedding requires system operators to push to the maximum the exploitation of plants, especially during emergency conditions. In this scenario, a reliable assessment of load capabilities and an effective management of the associated risks appear to be crucial. The problem of supplying energy is time-varying in nature and demands therefore a dynamic solution in order to manage risks related to load levels exceeding component's nameplate values, especially in the presence of contingencies [3-50].

3.7 STATISTICAL APPROACH TO ANALYZING AND MITIGATING EXTREME CONTINGENCIES

The design of special emergency control schemes implies the identification of the main failure modes of the system, the determination of appropriate mitigating control actions, and the design of automatic triggering devices. These latter must be able to detect in real-time when the system is in the process of loosing its stability and send appropriate control signals quickly enough to avoid dramatic consequences. In particular, these systems must be robust with respect to changing operating conditions and other uncertainties related to measurement and modeling errors. To enhance system performance (i.e. to reduce failure risks), existing emergency control systems could be improved or replaced by new, more effective ones. It is also believed that the coordination of various such devices acting in different time frames or in different geographical areas of a power system should be improved.

Given the fact that power system failures are (luckily) very rare events, actual experience is slim and engineers in charge of the design of emergency control schemes rely mainly on simulation. Their approach thus classically consists in building up simulation scenarios in a manual trial and error fashion and analyzing the simulation results by hand. This is an intricate and time consuming activity which strongly relies on human expertise. Generally problems are decomposed into elementary subproblems (e.g. voltage vs angle stability, or region-wise) which are treated separately, often by different engineers. However, due to the faster changes occurring in today's power systems, the need for more regular studies increases while human expertise may quickly become obsolete and even misleading. Moreover, the fact that systems tend to operate closer to their limits may lead to more complex interactions among the different phenomena, making it even more difficult to find globally effective solutions.

But, above all, the principal shortcoming of this *deterministic* approach is its inability to take into account the stochastic nature of the causes of power system failures and the unavoidable modeling uncertainties. Indeed, all failure modes are not equally likely to happen, their consequences are highly variable in practice, and all simulation models are wrong to a certain extent.

In order to circumvent these difficulties, while taking advantage of existing computing power and modern simulation tools, this section describes a *probabilistic* approach to help engineers carry out such studies in a more systematic way. It is based on Monte-Carlo simulations screening a representative sample of security scenarios, and exploits automatic learning tools to extract useful information from the simulation results [3-45]. In this methodology, uneven prior probabilities of possible causes which could lead to extreme conditions are taken into account, the economic impact of their consequences is also evaluated, and various uncertainties about less well known system components are integrated in the decision-making process. Note that this approach can identify likely failure modes of a system, while in the deterministic approach this information must be known prior to the study. Although the probabilistic approach needs additional information and modeling work in order to define the random sampling probabilities, it is able to provide a more objective and a more anticipative view of possible failure modes of a system.

The approach consists of three steps:

(i) modeling probabilistically the causes potentially leading to extreme conditions (weakened operating conditions, abnormal operation of protections, multiple disturbances) as well as uncertainties (load behavior, external systems…);

(ii) using parallel Monte-Carlo simulations to sample scenarios according to this information (random combinations of operating conditions, dynamic modeling hypotheses (e.g. relay settings, malfunctions, external systems, load…), and disturbances);

(iii) building up a database of simulation results, collecting key variables and their temporal behavior, and using data mining techniques to extract from this latter synthetic information about the main breakdown modes and possible ways to improve emergency control schemes.

In the following subsections we first describe this general approach and then provide some particular ways of applying it to large scale problems of defense plan design, adjustment, and validation.

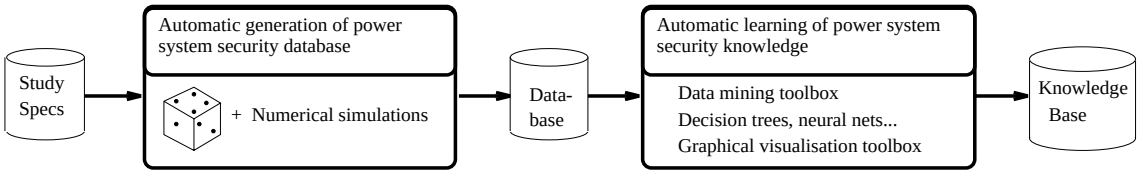


Figure 3-6. Overall probabilistic framework [3-44].

3.7.1 Principle of the approach

The overall framework is depicted in **Figure 3-6**. The approach proceeds by iterating the following elementary steps.

Study specification: setting up a detailed probabilistic model of the possible *causes* of insecurity: multiple disturbances, bad coordination and/or malfunctioning of protective devices, over-optimistic preventive security strategies due to uncertainties in modeling parameters…

Database generation: sampling representative combinations of these causes, and carrying out extensive simulations to determine the behavior of the power system under these assumptions.

Data mining: analyzing the database of dynamic simulation results to identify *a posteriori* the main weaknesses of the system and possible ways to mitigate them.

Evaluation: evaluating the identified countermeasures, e.g. in the form of new or modified special stability control systems, and validating them through a cost/benefit analysis on the scenarios stored in the database.

3.7.1.1 Study specification

The first step of the proposed methodology consists in specifying the range of scenarios that the particular study will address. While the approach aims at enabling the engineers to carry out broader

studies, covering more systematically all kinds of situations and dynamic phenomena, the scope of a particular study must be clearly defined a priori in terms of security scenarios.

A scenario has three components:

(i) its starting *operating point* (available lines and generators, load level and distribution, generation dispatch, voltage/var schedule…);

(ii) its *dynamic modeling hypothesis* (e.g. control loop gains, protections settings, malfunctions, load behavior, measurement noise…);

(iii) a sequence of *disturbances* (e.g. short-circuits, outages, load trends…).

Starting with the existing expertise and problem statement, the random sampling specifications are set up for each one of these components, generally through a sequence of discussions among experts in different fields, such as power system dynamics, protections and economic questions. Some base cases are selected, and a catalog of variable parameters which are important for the study under consideration is set up. Then for each parameter, a probability distribution is chosen, in order to screen its possible values; constraints among these parameters may also be defined in order to filter out unrealistic scenarios. For example, among the many parameters which could be handled in this way, let us mention line overload protections (the thresholds and triggering delays of which were randomized around their normal values) and load models (whose sensitivities to voltage were randomized).

The other part of the database specification concerns the choice of the *attributes* which will be extracted from the simulations and stored in the database: these are scalar and temporal parameters describing the dynamic behavior of the system and which will be used as inputs (e.g. candidate measurements) or outputs (e.g. evaluation of consequences) to the data mining tools, in order to extract synthetic information from the database. Examples of extracted attributes given are EHV voltages and generator rotor speeds, line currents…

3.7.1.2 Database generation

The database generation process can be carried out in a fully automatic way by dedicated software tool. It consists of two successive steps:

(i) random sampling of individual scenario specifications;

(ii) numerical simulation of the sampled scenarios.

The sampling of scenarios is essentially a sequential process building a so-called a priori database of individual scenario specifications. Only trivial computations are carried out here, and even for very complex problems the computing time required by the random sampling process is negligible with respect to time needed for the scenarios' simulation.

While the random sampling builds up the a priori database sequentially, the scenario simulation engine extracts successive specifications and launches their simulation in parallel, using a cluster of available workstations as simulation servers. A master process collects the results of the servers and gradually builds up the so-called a posteriori database with their results.

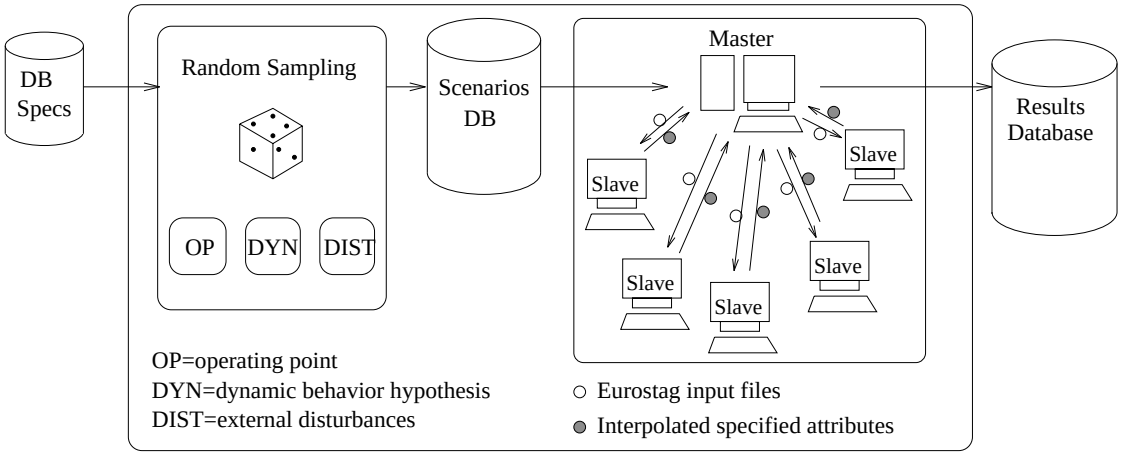


Figure 3-7. Parallel simulation of scenarios to generate the a posteriori database [3-44].

Notice that, depending on the size of the power system and the degree of refinement of the used dynamic model, the computational burden of these simulations may be rather high, which justifies their parallelization (see **Figure 3-7**). Moreover, the raw outputs of the simulation engine have to be post-processed in order to extract useful information in a format compatible with the data mining tool, and to save disk space if necessary by using appropriate compression techniques. For example, in the study described below the total amount of raw data generated was about 250 GB; thanks to extraction and compression the a posteriori database was finally only about 800 MB large.

Notice also that some of the scenarios generated by random sampling may not result in successful simulation, for example due to physical non-feasibility or numerical convergence problems. Thus, an a posteriori database generally corresponds to a proper subset of the corresponding a priori database.

Once a sufficient number of scenarios have been simulated successfully, a database release is created which can be exploited by the data mining module. Possibly, after having carried out some analyses on this database, the database can be completed by specifying new random sampling conditions and carrying out further simulations, thus yielding successive database releases which will be used successively in a trial and error fashion during the study and design process.

3.7.1.3 Data mining

The data mining process is itself composed of successive steps, aiming at extracting progressively more and more refined information from the simulation database. During this process a variety of visualization and statistical data exploration and modeling techniques are used [3-45].

Step "zero" in the data mining process consists in validating the scenarios which are contained in the database release. In particular, since some of specified scenarios may have been filtered out (e.g. because they could not be simulated properly due to physical non-feasibility or numerical convergence problems) it is necessary to check the representativity of the database. If validation is successful, data mining can be started in effect; otherwise database specifications may be modified and the database generation process is restarted in order to improve representativity.

The first step would be to rank the scenarios according to their severity. For example in the study carried out below, various measures of scenario severity were used, quantifying various undesirable consequences (number of transmission elements lost, amounts of lost generation, amount of lost load, variation in power flows in important ties lines). Some interesting (e.g. very severe) scenarios can be identified and analyzed by "hand" using the graphical visualization tools incorporated in the data mining software. For example, the temporal evolution of voltages, power flows, and other interesting variables may be displayed and it is possible to step through the various discrete events corresponding to the action of protections by using a one-line diagram automatic playback.

The next objective of data mining will be to determine the main weak points of the studied power system (i.e. the relative frequency of different types of behaviors~: stable, voltage collapse, cascading line tripping, loss of synchronism, frequency collapse, oscillations, dynamic instabilities...). This can be achieved using automatic unsupervised learning techniques, like clustering and correlation analyses.

Finally, further steps will consist in assessing how the different variables used to characterize the scenarios are interrelated, and identify automatically those which are useful to detect various undesirable phenomena. In particular, supervised learning and correlation analysis may be used to screen automatically a large number of variables and scenarios relevant for each task. Notice that at this step the engineer can try out various possibilities, being only limited by his imagination and the information contained in the database. In order to find out efficient ways to predict system failures, he may try out different ways of decomposing the overall problem into subproblems and test different sets of measurements and detection logics. Such detection rules may either be defined manually or automatically using supervised learning methods.

Eventually, the data mining process will lead to some changes in some existing special stability controls or to the design of new ones. If this is the case, the suggested improvements may be evaluated by incorporating them in the simulation model and generating a new "variant" of the database to simulate their effect. The comparison of this latter with the original database will allow the engineer to assess whether the system works, and if not, suggest some improvements until satisfactory results are obtained.

Thus the overall design process is essentially similar to the classical trial and error process used presently. However, the main difference is that at each step actions are evaluated in parallel on the

same statistically representative sample of scenarios. This makes comparisons among different possibilities much easier and more meaningful, while a lot of flexibility is gained. Moreover, the engineer spends his time carrying out interesting investigations rather than troubling around with running simulations and managing their input and output files.

Also, the fact that all analyses are carried out on a representative sample makes studies more transparent, makes it easier to exchange information among various engineers and allows one to easily refresh results if some parameter is changed (e.g. a new FACTS device comes into operation, or the dynamic models are modified).

3.7.2 Application examples

In this subsection we briefly describe the application of the above methodology to three important problems related to the analysis and mitigation of extreme contingencies.

Identification of likely blackout modes

Here the primary objective is to study the weak points of an existing system so as to:

(i) identify which are the most dangerous breakdown modes and weak areas;

(ii) decide whether existing emergency control schemes and/or defense plans need to be upgraded.

Since, for a given system it is generally not known in advance which among the faster or slower phenomena will be triggered by the combination of external disturbances and protection malfunctioning, and because in blackouts these phenomena typically interact with each other, it is necessary to develop a rather detailed short-term and long-term dynamic model in order to carry out scenario simulations. In addition, since large disturbances yield rather abnormal voltage and frequency variations, one must accept the idea that these simulation models will be rather inaccurate (particularly models of the load and of dispersed generation). Therefore, one should take care in the generation of the database to randomize those model parameters that are not well known (e.g. the exponents of exponential load models, as well as the settings of protective relays of dispersed generation, and large industrial plants).

Another important task consists in defining precisely the set of initiating and aggravating events that should be sampled. Typically, these will combine combinations of external disturbances and assumptions about hidden failures. Depending on the particular circumstances they can be sampled from probability distributions based on past statistics, correlated or not, or they can just be enumerated. Obviously, in most practical situations it will not be possible to generate all possible combinations of triggering and aggravating events, but nevertheless by combining optimal experiment design and variance reduction techniques (e.g., importance sampling), it is possible to generate a database composed of a reasonable number of scenarios (say a few thousand) and also containing useful information about the dynamic behavior of the system under very stressed and highly perturbed conditions. Notice also that the objective here is not necessarily to yield a statistically representative sample of what could possibly happen to the system, but rather to generate a rich enough set of highly perturbed dynamic system trajectories over a period of several minutes or tens of minutes. Such a sample of simulations may indeed be exploited to highlight possible problems in the system and understand whether in these situations the existing protective devices would operate more or less satisfactorily.

The next step consists in defining attributes, collected from the time-domain simulations, which allow one to assess the consequences in terms of geographical extension and depth of the blackouts, as well as their temporal patterns. Therefore it is necessary to collect macroscopic indicators of abnormal operation such as voltage drops at different EHV buses, amounts of disconnected load (by self protection, load shedding operation, or partial system blackout) and of lost bulk generation and transmission equipment. In addition, the temporal sequence of actions of protective devices that are triggered during the scenario need to be recorded in the database so as to enable the analysis of what happened in each scenario.

Once the database of simulation results is available the analysis uses data-mining tools to identify groups of similar scenarios according to two types of criteria:

(i) type and severity of consequences (similar amount of equipment disconnected, similar geographical extension of the problem…);

(ii) temporal patterns (e.g. fast vs. slow, voltage collapse driven vs. angle stability driven…).

Once the set of scenarios has been condensed into a number of blackout patterns, these can then be analyzed by experts in terms of likelihood and severity, allowing them to decide whether and where the emergency control and/or defense plans need to be upgraded.

References [3-44, [3-46] report details of a large scale study carried out with this methodology on the South-Eastern part of the EDF (Electricité de France) system. This study allowed EDF to identify five major modes of blackout with increasing severity.

3.7.2.1 Design of a new triggering rule for emergency control devices

Most existing emergency control schemes use local information only in order to trigger their control actions (patently load-shedding devices, but also out-of-step relays and generator protections). The reasons for this choice are numerous: reliability (specially, dependability), technical limitations (measurement devices and communications channels), difficulty to identify among the remote signals those that are useful and reliable indicators of impending instability.

Nevertheless, one of the possible ways to improve these emergency control schemes would be to use remote measurements in order to improve selectivity, sensitivity and speed of detection. Automatic learning methods may be used in order to systematically screen a large number of candidate measurements and identify those that are most effective indicators of the development of a specific instability, and to build detection rules which offer a good compromise between selectivity, sensitivity and speed of detection. To this end, the scenarios of a database are first classified into stable and unstable ones (using the outcomes of the simulations) and then a set of candidate measurements are defined that could be used as inputs to a triggering rule.

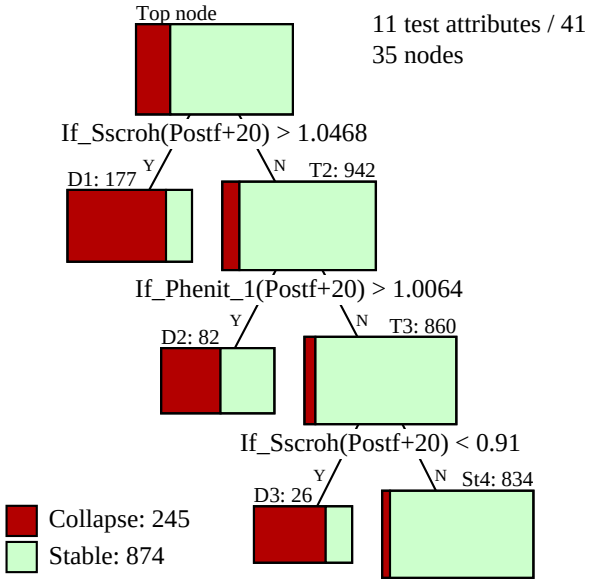


Figure 3-8. Example decision tree for early detection of impending voltage collapse [3-44].

To illustrate this possibility we report on **Figure 3-8** the first levels of a decision tree built with the method described in [3-45]. The purpose of this tree was to predict voltage collapse in the South-Eastern part of the French system, as quickly as possible and by using as input measurements the excitation currents of generators. Thus it was built by using as candidate measurements the excitation currents of all generators in the concerned area of the system. The complete tree has 35 nodes and

identifies among the 41 machines the 11 most important ones (the excitation currents of all other machines were found by the automatic learning method to be irrelevant or redundant to the detection of voltage collapse). Once constructed, such a detection rule can be compared on the database of simulation scenarios with the existing triggering rule used by load shedding scheme, so as to assess the value of using remote measurements, and eventually decide whether to upgrade the system.

3.7.2.2 Tuning of an existing special protection scheme

A variation of the statistical framework can also be used in order to fine tune thresholds and select criteria for event-based emergency control schemes. For example, references [3-47] and [3-48] report on the improvement of the RPTC scheme in use at Hydro-Québec. This scheme uses on-line (preventive mode) measurements of power flows and topology information in order to adapt the settings of a protection scheme designed for a specific event (e.g. a three-phase short-circuit followed by tripping two parallel lines), in terms of number of generators to disconnect and amount of load to shed to avoid loss of transient stability. References [3-47] and [3-48] report how the statistical methodology was used in order to improve these settings so as to minimize at the same time risk of over-shedding and of under-shedding. Transient stability simulations were carried out on about ten thousand SCADA snapshots collected over several months of system operation, in order to determine the minimum number of generators to shed for each case, and then automatic learning was used in order to build automatically a decision rule to adapt in on-line mode the relay settings to system conditions.

3.8 CONCLUSIONS

Repeated occurrences of low probability, devastating power system disturbances have brought about numerous mitigation tools (wide area protection and control systems). Successful applications require good modeling tools. Existing implementations use simple measurements. Sometimes the measurements are local only (e.g. out of step tripping or underfrequency load shedding). In other cases the measurements and actions use wide area information and communications systems. The more complex decision processes employ SCADA for information gathering, allowing a time frame of only several seconds for remedial actions. Preventive actions can be based on algorithms based on state estimator data. Higher speed wide area protection systems required to prevent angular instability or fast voltage collapse (e.g. direct load or generator rejection), respond primarily to contingencies identified in off-line planning studies, and are limited in effectiveness against unforeseen disturbances.

Better detection and control strategies through the concept of advanced wide area disturbance protection offer a better management (than existing) of the disturbances and significant opportunity for more reliable system performance under higher power transfers and operating economies. The continuing advances in development of analytical tools and study procedures for various types of disturbances discussed herein, along with developments in enabling technologies for monitoring and control, offer great opportunities for development of advanced protection by using system-wide information together with distributed local intelligence and communicating selected information between separate locations to counteract propagation of the major disturbances in power systems.

3.9 REFERENCES

[3-1] Voltage Stability of Power Systems: Concepts, Analytical Tools, and Industry Experience, IEEE Publication, 90TH0358-2-PWR, 1990.

[3-2] System Protection and Voltage Stability, IEEE Power System Relaying Committee, IEEE Publication, 93THO596-7 PWR, 1993.

[3-3] H. Fink, et al., "Emergency Control Practices," IEEE Transactions on PAS, Vol. 104, pp. 2336-2441, Sept. 1985.

[3-4] System Disturbances: 1986-1997 North American Electric Reliability Council, NERC Reports.

[3-5] A. Apostolov, D. Novosel, and D.G. Hart, "Intelligent Protection and Control During Power System Disturbance", 56th annual APC, Chicago, April 1994.

[3-6] C. W. Taylor, "Power system voltage stability", McGraw-Hill, 1994.

[3-7] P. Kundur, "Power System Stability and Control", EPRI Power System Engineering Series, McGraw-Hill, Inc., 1994.

[3-8] G. C. Bullock, "Cascading Voltage Collapse in west Tennessee, August 22, 1987", Proceedings of Western Protective Relay Conference, Washington, pp. 101-107, 1990.

[3-9] North American Electric Reliability Council (NERC), "1992 System Disturbances - Review of Selected Electric System Disturbances in North America", pp. 18-32, Oct. 1993.

[3-10] T. V. Cutsem and C. Vournas, "Voltage stability of electric power systems", Kluwer Academic Publishers, Boston, 1998.

[3-11] A. Kurita and T. Sakurai, "The power system failure on July, 1987 in Tokyo", Proceedings of the 27th Conference on Decision and Control, Texas, pp. 2093-2097, Dec. 1988.

[3-12] C. Concordia and S. Ihar, "Load representation in Power System Stability Studies", "IEEE Transactions on Power Systems", PAS 101, No. 4, pp. 969-976, 1982.

[3-13] M. K. Pal, "Voltage Stability Conditions Considering Load Characteristics", IEEE Transactions on Power Systems, Vol. 1, No. 1, pp. 243-249, Feb. 1992.

[3-14] T. J. Overbye, "Effects of load modeling on analysis of power system voltage stability", International Journal Electric Power and Energy Systems", Vol. 16, No. 5, pp. 329-338, Oct. 1994.

[3-15] IEEE Task Force Paper, "Standard Load Models for Power Flow and Dynamic Performance Simulation", IEEE Transactions on Power Systems, Vol. 10, No. 3, pp. 1302-1313, August 1995.

[3-16] I. Dobson, H. D. Chiang, "Towards a Theory of Voltage Collapse in Electric Power Systems", Systems & Control Letters 13 (1989) 253-262.

[3-17] V. Ajjarapu, C.Christy, "The Continuation Power Flow: A Tool for Steady State Voltage Stability Analysis", IEEE Transaction on Power Systems, Vol. 7, No. 1, February 1992.

[3-18] R.J. Jumeau, H.D. Chiang, "Parameterization of the Load-Flow Equations for Eliminating Ill-conditioning Load Flow Solutions", IEEE Transaction on Power Systems, Vol. 8 No. 3 February 1993.

[3-19] S. Greene, I. Dobson, F.L. Alvarado, Sensitivity of the loading margin to voltage collapse with respect to arbitrary parameters, IEEE Transactions on Power Systems, Vol. 12, No. 1, February 1997.

[3-20] S. Greene, I. Dobson, F.L. Alvarado, Sensitivity of transfer capability margins with a fast formula, IEEE Transactions on Power Systems, Vol. 17, No. 1, February 2002.

[3-21] H. Li, H-D. Chiang, J. Tong, "An on-line tool for voltage stability assessment and control of large scale power systems, IREP Symposium Bulk Power Systems Dynamics and Control, August 2004, Cortina D'Ampezzo Italy.

[3-22] J. Zhang, I. Dobson, F.L. Alvarado, "Quantifying transmission reliability margin, " International Journal of Electric Energy and Power Systems, Vol. 26, No. 9, 2004.

[3-23] C. A. Canizares, "Calculating optimal system parameters to maximize the distance to saddle-node bifurcations," IEEE Trans Circuits System I: Fundamental Theory and Application, Vol. 45, No. 3, pp. 225-237, March 1998.

[3-24] I. Dobson, L. Lu, "New Methods for Computing a Closest Saddle Node Bifurcation and Worst Case Load Power Margin for Voltage Collapse", IEEE Transaction on Power Systems, Vol. 8, No. 3, August 1993.

[3-25] F. Alvarado, I. Dobson, Y. Hu, "Computation of Closest Bifurcations in Power Systems", IEEE Transaction on Power Systems, Vol. 9, No. 2, May 1994.

[3-26] IEEE Power System Relaying Committee, Working Group D-10 Report, "Potential Applications Of Expert Systems To Power System Protection", IEEE Transactions on Power Delivery, Vol. 9, No. 2, April 1994, pp. 720-728.

[3-27] Information on electric system disturbances in North America can be downloaded from the NERC Disturbance Analysis Working Group (DAWG) website at http://www.nerc.com/dawg/database.html.

[3-28] B.A. Carreras, D.E. Newman, I. Dobson, A.B. Poole, Evidence for self-organized criticality in a time series of electric power system blackouts, IEEE Trans. Circuits and Systems, Part I. Vol. 51, Vo. 9, September 2004.

[3-29] J. Chen, J.S. Thorp, and M. Parashar, Analysis of electric power system disturbance data, 34th Hawaii Intl. Conf. on System Sciences, Maui, Hawaii, January 2001.

[3-30] R. Billinton, R.N. Allan, "Reliability evaluation of power systems", second edition, Chapter 13, Plenum Press, New York, 1996.

[3-31] B.A. Carreras, V.E. Lynch, D.E. Newman, I. Dobson, "Blackout mitigation assessment in power transmission systems", 36th Hawaii International Conference on System Sciences, Hawaii, 2003.

[3-32] I. Dobson, B.A. Carreras, D.E. Newman, "A loading-dependent model of probabilistic cascading failure", Probability in the Engineering and Informational Sciences, vol. 19, no. 1, January 2005.

[3-33] B.A. Carreras, V.E. Lynch, I. Dobson, D.E. Newman, "Critical Points and Transitions in a Power Transmission Model", Chaos, Vol. 12, Vo. 4, 2002, pp. 985-994.

[3-34] D.P. Nedic, I. Dobson, D.S. Kirschen, B.A. Carreras, V.E. Lynch, "Criticality in a cascading failure blackout model", Fifteenth Power Systems Computation Conference, Liege Belgium, August 2005

[3-35] IEEE Power Engineering Society, Power System Relaying Committee, System Protection Subcommittee, Working Group C-4, "Intelligent Systems In Protection Engineering", report, Feb 1999.

[3-36] I. Dobson, B.A. Carreras, D.E. Newman, "A branching process approximation to cascading load-dependent system failure", 37th Hawaii Intl. Conf. on System Sciences, Hawaii, 2004.

[3-37] I. Dobson, K .R. Wierzbicki, B.A. Carreras, V.E. Lynch, D.E. Newman, "An estimator of propagation of cascading failure", 39th Hawaii Intl. Conf. on System Sciences, Kauai, Hawaii, 2006.

[3-38] D. S. Kirschen, D. Jayaweera, D. P. Nedic, R. N. Allan, "A probabilistic indicator of system stress", IEEE Transactions on Power Systems, Vol. 19, No. 3, 2004.

[3-39] M. Ni, J.D. McCalley, V. Vittal, T. Tayyib, "Online risk-based security assessment", IEEE Transactions on Power Systems, Vol. 18, Vo. 1, pp. 258-265, 2003.

[3-40] B.A. Carreras, V.E. Lynch, I. Dobson, D.E. Newman, "Complex dynamics of blackouts in power transmission systems", Chaos, Vol. 14, No. 3, September 2004.

[3-41] P. Bak, "How nature works: the science of self-organized criticality", Copernicus books, 1996.

[3-42] J. C. Tan, P. A. Crossley, D.Kirschen, J. Goody, and J. A. Downes , "An Expert System for the Back-up Protection of a Transmission Network", IEEE Transactions on Power Delivery, Vol. 15, No. 2, pp. 508-514, April 2000.

[3-43] J. C. Tan, P A Crossley, P G McLaren, P F Gale, I Hall, J Farrell: "Application of a Wide Area Back-Up Protection Expert System to Prevent Cascading Outages", IEEE PES Summer Meeting 2001.

[3-44] L. Wehenkel, C. Lebrevelec, M. Trotignon and J. Batut, "Probabilistic design of power system special-stability controls", Control Engineering Practice, Vol. 7, No. 2, pp. 183-194, 1999.

[3-45] L. Wehenkel, "Automatic Learning Techniques in Power Systems", Kluwer Academic, 1998.

[3-46] C. Lebrevelec, L. Wehenkel, P. Cholley and J.P. Clerfeuille, "A probabilistic approach to improve security assessment", Proc. IERE Workshop on Future Directions in Power System Reliability, Palo Alto, pp. 243-252, 1997.

[3-47] J. Huang, S. Harrison, G. Vanier, A. Valette and L. Wehenkel, "Application of data mining to optimize settings for generator tripping and load shedding system (RPTC) in emergency control at Hydro-Quebec", Proc. of PMAPS-2002 (Probabilistic Methods Applied to Power Systems), 7 pages, 2002.

[3-48] J. Huang, G. Vanier, A. Valette, S. Harrison, F. Lévesque and L. Wehenkel, "Operation rules determined by risk analysis for special protection systems at Hydro-Québec", Proc. of CIGRE general meeting, Paris, 9 pages, 2004.

[3-49] M. Di Santo, A. Vaccaro, D Villacci, E. Zimeo:" A Distributed Architecture for on-line Power Systems Security Analysis", IEEE Transactions on Industrial Electronics Vol. 51, No 6, Dec 2004.

[3-50] Study Committee 23-CIGRE, "Dynamic loading of transmission equipment", Electra, No. 202, Jun 2002, pp. 63-73.

4 DECREASING THE RATE OF INCIDENTS: SYSTEM DESIGN AND OPERATING STRATEGIES

4.1 INTRODUCTION

This chapter reviews certain modifications that could be made to the bulk systems prior to or in conjunction with implementing a major technological defense system against extreme contingencies.

The following aspects are considered:

- Current operating strategies for normal operating conditions;
- Operating strategies to counter anticipated events;
- Operating strategies for emergencies;
- Protection settings for equipment (e.g.: lines, transformers);
- Impact on neighboring systems due to effects of automatic power system controls;
- Operating limits for in-service equipment under normal operating conditions and during single and multiple contingencies;
- Wide area system view.

Substation design criteria should be revised, or at the very least, the application of current design criteria (reengineering) should be verified.

Utilities should review the priority sequence of required improvements, based on overall interconnected system reliability.

It is crucial to understand that a new network protection system against extreme contingencies should not be a way to counter system operation at the limits of equipment ratings.

4.2 POWER SYSTEM OPERATING STRATEGIES

4.2.1 Revision of Current Operating Strategies

An electrical transmission system is usually operated according to clear and precise instructions that must cover all normal operating conditions.

When changes are made to the power system, operating strategy studies justifying such changes must be provided. The studies must be reflected in the operating guidelines (instructions and information) used by transmission system dispatchers (system control center) and facility operators (substations and generating stations). Maintenance work planners must be familiar with these guidelines so that they can take into account the need for service continuity and system reliability during single contingencies. In addition they must take into account contingencies attributed to equipment outages.

The guidelines must be critically reviewed on a regular basis to ensure that they conform to current operational reality. Similarly, when demographic changes affect the load flows of a bulk system, and the quantity of energy distributed to the facilities, special care must be given to system studies to adequately meet these changes. These changed conditions must also be reflected in the operating guidelines.

Furthermore, when changes to major power system equipment are made, the operating guidelines must be checked and revalidated so that they incorporate the impacts of these changes in terms of power system operation. The guidelines may have to be substantially updated.

Any changes to the facilities must be taken into account so that their impacts on neighboring systems or neighboring control areas can be assessed. The utilities or Control Areas that are interconnected must work together to solve problems involving the reliability of interconnected systems.

4.2.2 Former Operating System Strategies and Practices

Former system operating strategies and practices (whether in written form or not) must be reassessed when there are changes to infrastructures and new system reliability requirements come into force.

Power systems have a long history. Old facilities, including equipment such as busbars, transformers, circuit breakers, disconnect switches and power lines, are connected to more modern facilities. All of

these components must be compatible and must be capable of adequately meeting requirements pertaining to reliable system operation.

Out-of-date operating strategy studies can still be used. These studies, which date back to the time when the old facilities were commissioned, may not have been revised to take into account the current day's operating context. The studies on which the operating guidelines are based, with the latter not being thoroughly revised since the corresponding studies were not updated, could put a network's reliability at risk. It is imperative that these older studies be revised and updated so that they are relevant and compatible with present operating guidelines.

Moreover, utilities need to review operating practices that are not documented or supported by studies. These practices, which pertain to the "bulk" part of the utilities' respective systems, are all the more important to update and validate.

Each bulk system operating practice that is not supported by appropriate studies must be reviewed according to the reliability criteria of interconnected systems to validate their relevance and conformance to system reliability requirements.

4.2.3 In-depth Studies and Improvements to Operating Strategies

In-depth studies and improvements to operating strategies are needed to increase the degree of flexibility required when configuring facilities under different emergency operating conditions.

What is meant by power system emergency? This is simply a system operating condition that is not standard and which requires specific operating modes which go beyond standard practices used under normal operating conditions.

When emergency operating conditions must be used, some guidelines may prohibit the use of non-standard configurations since there are no strategic studies to back them up. Furthermore, non-standard configurations could be applied with minor modifications being made to equipment configurations and strategic studies prepared to validate them. Thus, non-standard configurations could facilitate the operation of the system under emergency conditions (e.g. degraded system condition, slow voltage collapse). Operators would thus have available avenues for countering extreme forecast contingencies, localized overloads, or major sudden events.

In short, operating guidelines should contain operating strategies backed by studies so that operators are given as many options as possible to configure the systems for operation under emergency and/or extreme contingency conditions. The studies would even validate the necessity for shedding specific load.

4.2.4 Devising Innovative Operating Strategies for Forecast Climatic Events

System operators have developed interesting tools to forecast major climatic events and to mitigate their impact. Some studies are proposing the employment of satellite based remote sensing for power systems disaster management (i.e. for disaster prevision, monitoring and damage assessment) **[4-1]**.

When catastrophic climatic conditions are forecast, that could put power system infrastructures in jeopardy, operators must have the option of reconfiguring system facilities such that the main power flows passing through infrastructures, that may be damaged, can be temporarily bypassed without affecting the continuity and quality of service to customers.

Such feats by operators are feasible if rigorous studies were previously done jointly with neighboring systems. What is needed, during extreme climatic conditions, is to avoid interrupting service to customers, to the greatest extent possible, regardless of where the customers are located while rerouting the power flows through other corridors, local substations or the facilities of neighboring systems. Thus, the remaining sections of the power system are not at risk, as they create little impact in the event of a loss, and are no longer a major problem with respect to the reliability of interconnected systems. A storm can occur without causing too much damage other than local physical damage and minor outages.

4.3 OPERATING AND MAINTENANCE CRITERIA FOR AUTOMATIC CONTROLS, SPECIAL PROTECTION SYSTEMS AND EQUIPMENT

4.3.1 Operating Criteria for Power System Components

The operating criteria for power system components allow systems to operate with a certain level of reliability under normal operating conditions and during single and sometimes multiple contingencies. This ability to overcome constraints is considered in an interconnected system context.

One of the reasons to have sound operating criteria for power system components is to minimize the risk to interconnected systems of cascading effects, domino effects, or untimely tripping as a result of sudden transient effects due to single or multiple contingencies.

4.3.2 Revising Maintenance Criteria

Current maintenance criteria could be revised to take into account changes to power systems as well as changes to systems in neighboring control areas. In this case, studies of various power system operating conditions could lead to integrating maintenance processes specifically to detect components that need to be improved to adequately meet changes to the power system and interconnected systems as well as to specific operating criteria under degraded system conditions. All power system component maintenance procedures should be revised on a case-by-case basis to incorporate this type of inspection.

Thus, the following aspects should be covered in the maintenance procedures revisions:

- Protective relay settings;
- Functionality of line protective relays: selectivity and speed versus impacts to/from the power system and/or to/from interconnected systems;
- Functionality of power system automatic controls.
- Power ratings of substation and generating station equipment (e.g. lines, busbars, transformers).

To ensure the preventive maintenance of support equipment (special protection systems and automatic controls), the process of verifying the functionality of protective relays could include an analysis of the context in which such relays are used with the actual settings that were defined. Thus, during the verification process, an assessment of changes made to power system facilities and even those of neighboring systems could lead to the revision of current settings or simply use the settings as is, without modifying them. In the event of a problem, studies would be done to redefine new settings.

During these inspections, protective relays would be checked using simulation tools that simulate actual cases of various faults. The simulations could reflect hypothetical cases of faults originating from local facilities, the bulk system or a neighboring interconnected system. In fact, faults of all kinds, both near and far, likely to occur and even with a potential impact on the facility (transformer, shunt reactor, busbar or circuit-breaker failure) would be involved. Hypothetical cases of transient disturbances absorbed on the network and of overloads located at various points of the power system could also be included in the simulations.

This new approach for the preventive maintenance of power system components requires that maintenance personnel are more experienced for this type of work. Should engineering departments be located closer to where maintenance work is being carried out while keeping contact with the overall department? This would allow maintenance work for this type of inspection to be optimized.

Furthermore, it would be useful to assess the possibility of making technological changes to basic protection systems for power system equipment. If there are still strategic facilities where major power flows pass through which use outdated technologies as basic protection systems for system equipment, it would be useful to determine the risks that this represents in the current interconnected system context. New technologies confer accuracy, consistency and reliability over the long term. These are characteristics that are not to be underestimated. In addition, these technologies provide flexibility of use, parameterization and adaptation to complex power system conditions. They also offer a multitude of options regarding data acquisition for power flow measurements, alarm generation, and the remote transmission of these data.

Now is for a brief discussion on the reliability of telecommunications systems. Telecommunications systems are a very critical aspect of power system reliability. If telecommunications systems fail, this puts whole sections of the power system at risk, with potentially a significant impact on the reliability of interconnected systems and control areas. This is mainly due to the loss of basic links of protection systems and automatic controls resulting from the loss of microwave or fiber-optic links, thus making the power systems vulnerable. Not to mention the loss of telephone communication links which system operators and dispatchers must deal with if these links use the same telecommunications systems. Moreover, during system restoration after a system-wide outage, telecommunications stations must have an independent power supply. This is to ensure that there are critical operational links, which include those of protection systems and the telephone systems of operators and control center dispatchers.

Maintenance procedures must include an inspection of the emergency energy supply of facilities required to restore the load to the bulk system. This also includes telecommunications stations and power system control centers.

Maintenance procedures must also include ways to reassess, on a case-by-case basis, power equipment when changes are made to interconnected systems. The various equipment in a facility may have to handle power flows in excess of previous levels to meet the requirements of new substation configurations and take into account changes to local networks or to neighboring interconnected systems. In an aim to meet the requirements of new substation configurations, that should allow operators to deal with extreme network operating conditions, equipment must be able to operate within their respective limits. Busbars must be capable of withstanding any normal high overload currents that are likely occur, circuit breakers must have adequate current breaking (interrupting) capacity for extreme cases, and transformers must be capable of handling temporary overloads, and so on.

4.3.3 Revising the Functionality of Automatic Controls versus the Impact to Interconnected Bulk Systems

Each interconnected system must be designed to meet and even exceed current design, operational and reliability criteria. By virtue of the fact that the systems are interconnected, it is imperative to comply with criteria that take into account impacts on neighboring systems.

The same applies to automatic controls. As these were developed, designed, installed and commissioned by certain transmission providers or control areas, there may be other utilities or neighboring systems which are not equipped with such automatic controls. Thus, when these automatic controls are triggered, undesirable disturbances may be transmitted to neighboring systems. If an automatic control belonging to another utility and installed for the utility's own needs is operating under extreme contingencies, the measures used to correct the situation may be extreme. The impact on the power system from the effects of such automatic controls may have repercussions on neighboring systems. However, if the measures applied to correct a situation would be spread out among the other utilities and interconnected systems or control areas, then the corrective effects would have a minimal impact on each one, and consequently on all customers.

Good automatic control designs developed by one utility will be enhanced when their impact is extended to neighboring systems. Expanding these automatic controls thus becomes beneficial to all, namely the customers.

4.3.4 Redefining or Verifying Operating Criteria under Degraded System Conditions for Power System Equipment

Certain degraded network conditions following multiple scheduled outages for maintenance purposes, and subsequent equipment failure, put the system's reliability to the test. In such cases of special operating conditions, there are system events likely to occur where additional complications could result in substantial equipment damage. For instance, in a degraded substation there could be an overload in a bus section resulting from a switching operation that completely modifies the busbar loop flow. An unexpected high power flow could melt down one section of the busbars even before the protection systems have had a chance to react.

Each installation should be carefully inspected by simulating various operating scenarios to detect any problems. The simulations should even involve cases that may appear bizarre at first glance but are

nonetheless technically possible when new configurations are involved during contingencies or through inadvertent switching operations during unusual operating conditions.

Once the problem cases have been identified, technical solutions can be applied to remedy the situation and thus increase the operational flexibility of the installations. Examples include increasing the power flow capacity of busbars and disconnect switches, the current interrupting capacity of circuit breakers, the capacity of transformers, etc. These significant gains could be used to better deal with extreme contingencies.

4.3.5 Interconnected System Studies: a Systemic Approach

The idea here is to allow power system studies to be coordinated using a systemic approach for utilities in interconnected systems regardless of their administrative borders. This is a sizeable challenge.

The implementation of new power system reinforcement solutions is fundamentally more effective when applied jointly with the various utilities from the different interconnected networks and control areas. Close cooperation is obviously desirable to meet this objective. The outcome could only be beneficial for customers everywhere.

Power system studies that yield solutions must be carried out while taking into account the entire bulk system. Thus, power system studies would lead to a neighboring system that extends beyond a mere description of electrical components. Studies have to be perceived as extending beyond the administrative borders of utilities and control areas so that efficient and impartial solutions can be found.

Ideally, a simulation tool would be needed that integrates all the power system components of all the interconnected systems. This would give more accurate simulation results and the proposed solutions would be better adapted to reality. This tool would have only one engineering center for all the interconnected control areas, which would constitute a major challenge from a data processing standpoint.

A concerted effort on the part of utilities, networks, control areas and service areas is needed. What is important to remember is that customers are all the same, regardless of where they are located. When a customer needs electrical power, it is the mission and responsibility of each utility to service him adequately.

4.4 REVIEWING MODIFICATIONS MADE TO EQUIPMENT, AUTOMATIC CONTROLS AND PROTECTION SYSTEMS

Another important aspect to take into account in maintaining power system reliability is to update and reassess the changes made to power systems in the past based on the current risk of impacts to interconnected systems. These modifications may have previously been done to fulfill operating strategy requirements in an aim to solve network problems at the time, while the existence of such modifications may now put interconnected systems and control areas at risk.

At a time characterized by rapid demographic change, electric utilities had to expand their power systems to adapt to new demand, a situation which presented a challenge to designers. Once the networks were built to meet demand, solutions were also implemented to correct any anomalies encountered during operation.

Some of these ingeniously implemented solutions can still be used while being updated to take into account changes made to power systems. On the other hand, there may be other solutions which are still being used which could fall by the wayside, partly as a result of personnel retirement. They may not be updated on the pretext that at first glance there is nothing that indicates that they need to be modified and they may be given low priority.

The solutions that have been implemented in the past may involve:

- Transforming capacity of certain facilities;
- Power-flow capacity in busbars during specific configurations for operating needs;
- Power-flow capacity of corridors under degraded interconnected system conditions or using special operating configurations;
- Operating guidelines based on outdated strategies;

- Strategies for using protection systems under degraded network conditions;
- Strategies that are especially applicable to situations characterized by telecommunications systems failure (telecommunications used by critical protection systems and automatic controls);
- The existence of old automatic controls designed to mitigate the impacts of major disturbances such as significant loss of load.

In short, meticulous research is required to track down any former modifications to facilities or forgotten strategy studies. Revisions would be needed to justify their use or their need to be updated.

4.5 RECONFIGURING SUBSTATIONS AND CORRIDORS

4.5.1 Modifications to Facility Components

It is imperative to take into account the many different physical modifications that can be made to facilities, including power equipment and protection systems, so that substations and generating stations can be operated with configurations and settings not commonly used in emergency operating conditions.

Based on the configuration of critical power lines in part of the interconnected systems, line and substation configurations could be modified to allow for increased flexibility to counter major contingencies that are likely to put the power systems and control areas at risk. Each case that is likely to occur must be studied and the proposed solutions, including modifications to the facilities, considered seriously.

Adding lines that are not in the same corridor, adding busbars to a substation, replacing circuit breakers with models with increased breaking (interrupting) capacity, adding voltage regulation controls and remotely changing the settings of synchronous and static var compensator regulators are all good solutions for improving the reliability of interconnected systems. One must not wait to be in a situation where power flow limits are being exceeded – which puts power systems at risk of experiencing cascading effects during single contingencies such as an overload – to understand the need for immediate action to improve the infrastructures. In-depth studies may help anticipate such cases. It is therefore prudent, based on the results of such studies, to ensure that necessary maintenance work is done.

4.5.2 Number of lines required in a corridor to allow uncommon power flows resulting from losses in other corridors

Transmission corridors are designed with a certain number of lines to transport energy under normal operating conditions, which requires an operating margin for emergency load flows. If a line is lost in this corridor, the remaining lines must be capable of carrying all the power with one less line. In such cases, the operator must take action to ensure that the corridor is capable of withstanding the loss of a subsequent line.

In interconnected power system, an area is generally fed from several corridors. It may be possible to design the system to the total loss of a corridor while the power balance would be maintained through the other corridors in the system. The bottom line question is: are we able to design sufficiently robust power systems capable of withstanding the loss of several lines in a corridor or total corridor? Ideally, yes. But whether it is financially feasible is another question. A compromise must be reached between cost and efficiency.

To complement the needed system margin for such events, the necessary measures must be in place to prevent any major voltage and frequency disturbances. Such measures must be implemented through sophisticated control systems as described in the following chapters.

4.5.3 Redesigning Lines to Improve Mechanical Strength for Extraordinary Climatic Events

Extraordinary climatic events such as the Québec Ice storm in 1998 or the French wind storm in 1999 or other extraordinary events worldwide may lead utilities to reconsider line design criteria. Improving line mechanical strength may be a needed step to minimize long restoration delays and help reduce the likelihood of extreme contingencies such as loss of line corridors.

For more information on this subject, see the information that was presented in **[4-2**].

4.6 WIDE AREA SYSTEM VIEW

Another aspect to minimize the likelihood of extreme contingencies is better system visibility through inter-company communication and sharing of data from various power system control centers. Open communication could represent useful opportunities in contingencies management especially for large scale power systems **[4-3**]. In particular, detailed information about the actual system operation and the estimated system vulnerability respect to unforeseen contingencies, such as unexpected modifications to the power system structure or a sudden change of the operational conditions, represent critical information for the secure and reliable system operation.

This information should be delivered, in particular, to the entire set of market operators that could plan new purchase/sale policies for electrical supplies in order to react to a predicted system outage or to the asset managers of neighboring power systems that could plan proper corrective actions in order to mitigate the effect of predicted critical contingencies. In this matter, it is interesting to underlie that the recent Italian blackout was originated for a critical contingency of the Swiss power systems propagated to the entire Italian network for a lack of information sharing between the two power system control centers. Inter-company communication and sharing of data from various power system control centers, power producers, energy trades, and market participants represents therefore key issues to enhance the security and reliability levels of electrical networks. This requires more extensive intra-and inter-utility information exchange, diffusion, and open access to a wide range of real time information **[4-3**, **[4-4**].

Information sharing among different utilities is difficult, complex and costly since they adopts proprietary software platforms and existing information management systems cannot satisfy the new challenges, as more and faster information has now become desired by many players **[4-4**]. Interestingly, some papers published in literature **[4-4**, **[4-5**] propose the use of Web Services (i.e. an interface that describes a collection of modular, self-describing and self-contained applications that are network-accessible through standardized XML messaging). Web services are technology platform-, language- and vendor-independent, thus an ideal candidate for use in integration of legacy power system applications.

4.7 CONCLUSION

To minimize the impact of disturbances that are liable to arise from extreme contingencies, it is necessary to think through and implement concrete measures aimed at reinforcing transmission systems using the rudimentary means and knowledge that we already have.

It goes without saying that power system simulation tools (transients and load flows) and sophisticated computerized tools are required to support the implementation of new facilities and new power system configurations. The operating margins of the various network components (e.g. compensators, generating set regulators) should be used optimally to help meet the target objectives.

However, it is also crucial to have system restoration plans on hand for all types of contingencies. Emergency power supplies at system control centers and telecommunications stations must be efficiently maintained, so they can be used in the event of a major outage on the bulk power system.

Finally, wide area system view through better inter-company communication and sharing of data is of outmost importance. Common telecommunication network can be used but when not possible, WEB base service is a new direction for the integration of legacy power system application.

4.8 REFERENCES

[4-1] V. Di Gesù, S. Ustin, "Eye on the Storm: Post-Disaster Damage Assessment" Disaster planning & mitigation technologies – EPRI technical Report, sep. 1998.

[4-2] "Ice Storm Mitigation Workshop: Preparation for Extraordinary Climatic Events," CAE Technologies Inc., October 2002, Montreal, Quebec.

[4-3] Su C.-L., Lu C.-N., Hsiao T.-Y-, "Simulation Study of Internet Based Inter Control Center Data Exchange for Complete Network Modeling", IEEE Transactions on Power System, vol. 17, No. 4, pp. 1177-1183, Nov. 2002.

[4-4] Zhu J., "Web Services provide the Power to Integrate", IEEE Power & Energy Magazine, Volume 1, Issue 6, pp. 40 – 49, Nov.-Dec. 2003.

[4-5] Kreger H., "Web Services Conceptual Architecture (WSCA 1.0)", IBM Software Group Internal Report, May 2001.

5 SELECTION OF SPSs FOR MITIGATING EXTREME CONTINGENCIES

5.1 INTRODUCTION

Extreme contingencies usually refer to events that result in multiple components becoming unavailable or cascading out of service, such as the loss of transmission lines on a common right-of-way or faults with delayed clearing (stuck breaker or protection system failure) on a bus section. Extreme contingency evaluations are usually conducted to determine their effects on power system performance and to measure the robustness of the power system. The use of Special Protection Systems (SPSs) to increase grid security is a world-wide practice for countering extreme contingencies in areas where experience shows that these events occur too frequently and/or cause severe impacts, such as loss of load or system collapse.

Of course, it is not feasible or even possible to predict or prevent all multiple contingency events that could occur randomly and lead to power system collapse. When the complexity of a system is relatively low, a small number of SPSs are probably sufficient to protect the system adequately. However, large systems require a set of coordinated measures (or a defense plan) whose design and operation must involve high levels of complexity. This is necessary in order to ensure that the system is able to cope with all possible major incidents.

The main purposes of this chapter are to list and evaluate all possible means of action (SPSs) that could be used in a defense plan to counter extreme contingencies, and to facilitate the selection of the most appropriate ones. **Figure 5.1** illustrates the most important factors in the selection of SPSs.

The definition of extreme contingencies varies greatly from one power system to the next, but all extreme contingencies involve power system instability if no mitigation measures are employed. Therefore, we have chosen to classify the various means of action according to the possible *power system phenomena*, instead of according to the contingencies themselves. The following sections will provide a short review of the main characteristics of these phenomena, of the main factors pointing to the type of SPS that will prevent a loss of system integrity, and of the various SPS action types.

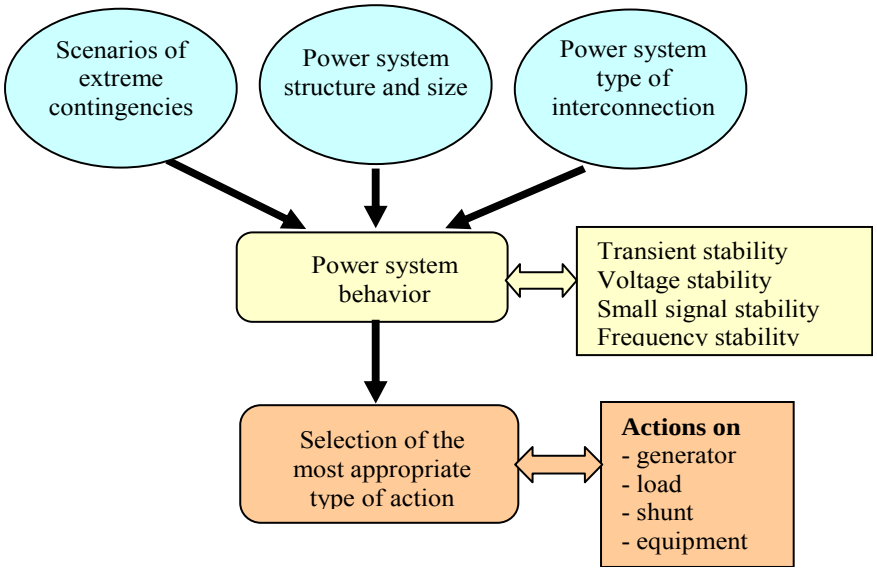


Figure 5.1: Main factors in the selection of the most appropriate SPS actions

5.2 SHORT REVIEW OF POWER SYSTEM PHENOMENA

The loss of power system integrity caused by extreme contingencies will always be characterized by one or more of the following phenomena:

- Transient angle instability;
- Frequency instability;
- Voltage instability;
- Small signal angle instability;
- Cascade tripping.

The main purpose of this section is to discuss main aspect of power system phenomena to help in the selection of the most appropriate SPS. Cascade tripping is not, strictly speaking, a power system phenomena but nevertheless discussed here considering its importance. It is also important to note that after a severe disturbance some of these phenomena will occur together. Reference [5-1] provides detailed information on these phenomena.

5.2.1 Transient angle instability

The transient stability of a power system describes the ability of all the generators to maintain synchronism when subjected to a severe disturbance such as a heavy current fault, loss of major generation or loss of a large block of load. The system response will involve large excursions in generator angles and significant changes in real and reactive power flow, bus voltages and other system variables. Loss of synchronism can affect a single generating unit, a power plant consisting of multiple units, a region of the network or several interconnected regions. The loss may appear suddenly (during the first swing) or after a series of divergent swings. The risk of loss is greater when the system is loosely meshed or power flows are high. The main consequences are major disturbances for customers (voltage dips, frequency deviations) and/or major transients (real power, voltage, frequency, etc.) on the generating units and power system. The latter may significantly increase the risk of fast disconnection of units and system separation due to faulty line protection operation.

5.2.2 Frequency instability

Frequency stability describes the ability of a power system to maintain the system frequency within an acceptable range during normal operating conditions or after a severe disturbance. If, despite the control actions taken to maintain the network integrity, network separation occurs, it is important to limit frequency excursions. Generators can operate without restriction within ± 0.5 Hz from normal frequency (50 or 60 Hz system) and for a limited time outside these values (according to manufacturer's constraints).

A major problem for a steam turbine is the frequency drop resulting from a sudden loss of generation. This is particularly onerous if pre-disturbance values of power transfer from one region of the power system to another are significant. If an interconnection or a power plant outage then occurs in the region with a generation shortage, a severe under frequency disturbance will result. Under frequency operation (frequency deviation exceeding -2.5 Hz) can lead to damage of thermal unit turbine blades and life-time reduction. The frequency drop can be so deep, that under frequency relays will disconnect thermal units from the network, increasing the power deficit.

For the region of the network with a surplus of generation, system frequency will start increasing. If the overfrequency is not reduced within a pre-set time period the unit will be tripped because of the unstable boiler condition. The problem of overfrequency is less troublesome than underfrequency because tripping of the unit will cause a frequency reduction. However, if the reduction is insufficient, further units will need to be tripped, with a possible underfrequency situation resulting if this is done excessively.

5.2.3 Voltage instability

Voltage stability involves the ability to maintain steady acceptable voltages at all buses under normal conditions and after being subjected to a disturbance [5-1, [5-2, and [5-3]. Voltage instability results from the attempt of loads to be restored above the maximum power that the combined generation and transmission system can deliver to them. This maximum power is directly influenced by electrical distances between generation and load centers, as well as by the reactive power limitations of generators. Voltage instability takes on the form of a progressive drop in voltage at the transmission level under the effect of load restoration. In turn, the sagging voltages may result in a system collapse which takes the form of generators losing synchronism and induction motors stalling.

Although the simplest voltage instability scenario is a load increase above the maximum deliverable power, most experienced voltage incidents are caused by a large disturbance. Voltage instability may be caused by a variety of single or multiple contingencies. With respect to long-term voltage stability, the main concern is the loss of transmission facilities (mainly in between generation and load centers) or the tripping of generators (mainly those located close to the loads and supporting the voltages of the latter). With respect to short-term voltage instability, the slow clearing of a fault may cause an induction motor dominated load (e.g. air conditioning) to become unstable.

5.2.4 Small signal angle instability

Small signal stability refers to the ability of the power system to maintain synchronism when subjected to a small disturbance [5-4]. Power systems contain many modes of oscillation due to a variety of interactions of their components. Many of the oscillations are due to generator rotor masses swinging relative to one another. Power systems with several machines will exhibit multiple modes of oscillations. These electromechanical modes usually occur in the frequency range of 0.1 to 2.0 Hz. Undamped electromechanical modes can be of a local type (frequency range of 0.7 to 2.0 Hz) or of inter-area oscillation mode (frequency range of 0.1 to 0.7 Hz). In many systems the damping of these electromechanical modes is a critical factor for secure operation particularly after an extreme contingency.

5.2.5 Cascade tripping

Cascading refers to an uncontrolled sequence of transmission line disconnections triggered by an incident at a single location. In some situations, a severe disturbance on a transmission system can initiate major oscillations in real and reactive power flows and instability in voltage levels. These oscillations may initiate the operation of some protection devices or control equipment, which can occasionally result in uncontrolled cascaded line and generator tripping. Overload or thermal problems may also cause cascaded line tripping. Cascaded line tripping will affect interties between power system regions and will be particularly problematic when one region is importing power and another is exporting. In such situations the consequence of a disturbance may spread over a wide system area and could result in the loss of supply to a large number of consumers.

Cascaded line tripping is most likely to occur after the protection system has responded to one or several faults by tripping a double circuit tie-line, multiple lines in the vicinity of the fault, one/more generating units or a busbar in a substation. Alternatively, cascaded line tripping can occur during an unexpected extreme increase in consumption or as a transfer effect between parallel tie-lines when one of them trips due to a fault or incorrect protection operation. This increases the power flow on the remaining lines and may result in load encroachment into the backup characteristics of distance relays or may be detected as an overload condition by a time-delayed phase over current relay. The system dynamics will determine which, if any, of the relays are involved: zone 3 elements in a distance relay will normally operate in approximately 1 s, while time-delayed over current relays set to detect an overload will normally operate in several minutes. To prevent cascaded line tripping it is important to ensure that there are adequate co-ordination margins between the operating characteristics of all the non-unit protection relays used on the network and also where possible to use high speed unit or communication aided protection schemes. The dependability, security and selectivity of the protection relays and schemes, including their communication systems, where appropriate, are of paramount importance in reducing the risk of cascade line tripping. However, improving the performance of conventional equipment protection may not completely eliminate the phenomena leading to cascaded line tripping and SPS may be required to counter their impact on the power system.

5.3 MAIN FACTORS IN THE SELECTION OF THE APPROPRIATE SPS ACTIONS

As shown in figure 5.1, the most important factors in the selection of the appropriate means of actions to prevent loss of power system integrity are:

- Scenarios of extreme contingencies;
- Power system structure (meshed, radial …) and size;
- Power system type of interconnection with its neighbors.

5.3.1 Scenarios of extreme contingencies

For reliable service, a power system must be capable of withstanding a wide variety of disturbances. Taking measures against all types of event is unrealistic due to the large amount of investment in necessary equipment. Therefore, power systems are generally designed and operated so as to be stable for more probable contingencies also often referred as design contingencies.

Survey of design and operating criteria [5-5] indicates that significant differences exist among utilities in the definition of these design contingencies. Moreover the majority of utilities plan and operates their power system such that with all transmission facilities in service and with normal operating procedures in effect, the normal customer load and generation would be maintained in service after a design contingency. A possible definition for an extreme contingency is therefore an event which exceeds, in severity, a design contingency.

Objective of extreme contingency assessment is to determine the effects of extreme contingencies on system performance. This is done in order to obtain an indication of system strength, or to determine the extent of a widespread system disturbance, even though extreme contingencies do have low probabilities of occurrence.

Extreme contingencies listed below are intended to serve as a means of identifying some of those particular situations that could result in widespread bulk power system blackouts. Scenarios of extreme contingencies are particular to each power system and must be based on knowledge of the characteristics of the power system and past experiences with major disturbances.

- *A fault more severe than the fault used in the design contingency with loss of a generator, a transmission circuit, a transformer or a bus. (Example: for design contingencies using phase to ground fault with loss of an element, extreme contingencies could be a three phase fault, with loss of the same element).*
- *A permanent fault (usually a phase to ground) with loss of multiple transmission circuits emanating from a generating station, switching station, dc terminal or substation including loss of all transmission circuits on a common right-of-way.*
- *Loss of generating station.*
- *The sudden dropping of a large load or major load center.*
- *The effect of severe power swings arising from disturbances outside the power system under study.*
- *The uncontrolled sequence of transmission line disconnections triggered by an incident at a single location.*

5.3.2 Power system structure and type of interconnection

The structure of the system and its type of interconnection with its neighbors are also among the most important factors in the selection of the appropriate means of action to counter an extreme contingency.

Indeed, some of power phenomena described in section 5.2 could be amplified or attenuated according to the system's various characteristics.

Power system structure depends mainly on the respective localization of loads and generation center and can be roughly divided in two classes:

- Densely meshed transmission systems with dispersed generation and demand;
- Lightly meshed transmission systems with localized centers of generation and demand.

Type of interconnection can also be divided in two class based on the relative size of the power system:

- A transmission system which is part of a much larger interconnection and is centrally situated within that interconnection;
- A transmission system that is not synchronously interconnected with neighbors or is by far the largest partner in any interconnection.

Table 5.1 combines power system structure and type of interconnection to form four power system types and highlight the dominant phenomena in each case to make it possible to appreciate the relations between all these aspects.

Table 5.1 Dominant phenomena in relation to power system types and structure.

	Densely meshed power system with dispersed generation and load		**Lightly meshed transmission systems with localized generation and load.**	
	Located in a large interconnection	**Not interconnected or by far the largest partner**	**Located in a large interconnection**	**Not interconnected or by far the largest partner**
Transient angle instability	*	*	***	***
Frequency instability	*	***	*	***
Voltage instability	*	*	***	***
Small signal stability	**	**	**	**
Cascade tripping	***	***	*	*

5.4 SELECTION OF THE MOST APPROPRIATE TYPE OF SPS ACTION

All SPS consist of three main parts:

- Inputs (level of physical magnitudes, status of circuits breakers, etc.);
- A decision-making system that initiates certain actions based on the inputs;
- Actions (such as generator or load tripping).

As defined in [5-6] special protection system (SPS) are designed to detect abnormal systems conditions that is known to cause unusual stress to the power system and to take some pre-determined action to counteract the observed condition in a controlled manner. Normally SPS act after an extreme contingency such as a too severe fault on transmission facilities, loss of large generation or loss of large load. The system response to such a disturbance normally involves excursions of frequency, voltage and generator angles. The SPS provides the required stabilizing force necessary to preserve the system from collapsing. For the purpose of this report, we distinguish SPS from continuous feedback controllers or closed-loop controls such as automatic voltage regulators or power system stabilizers.

However closed loop controls plays an important role in the task of maintaining power system stability after an extreme contingency and thus should be include in the available type of means of actions. A special class of action is then dedicated to these particulars means of actions.

In this section we will concentrate on action. The majority of SPS actions can be initiated either by a local detection system or by a wide area detection system. Detection is considered local when all the information required by the decision-making process is available at the same location where the action is performed. In a wide area detection system, the action is initiated by information acquired at one or more key buses located elsewhere in the power system.

A large variety of SPS are now in service in the world. However, type of actions could be group in a limited number of classes which are:

Class 1 - Actions on generation: generation rejection, turbine fast valving / generator runback, gas turbine / pumping storage start-up and actions on the AGC such as setpoint changes.

Class 2 - Actions on load: underfrequency load shedding (UFLS), undervoltage load shedding (UVLS) and remote load shedding.

Class 3 - Actions on shunt equipment: automatic shunt switching (shunt reactor/capacitor tripping or closing) and dynamic braking or braking resistor.

Class 4 - Actions on power system equipment: controlled opening of interconnection / area islanding, tap changers blocking and setpoint adjustment, quick increase of generator voltage setpoint and HVDC fast power change.

Class 5 - Closed loop controls: generator excitation control, power system stabilizer and supplementary controls in static Var compensators (SVCs) and HVDC. As mentioned, closed-loop controls are not considered as SPS but play an important role in the task of maintaining power system stability after an extreme contingency and thus should be include in the available means of actions.

The selection of the most appropriate type of action is generally based on the type of instability to counter. Following sections lists SPS actions most likely to be used to limit the consequences of transient angle instability, frequency instability, voltage instability, instability resulting from cascade line tripping and small signal instability. For simplicity, even though some of these phenomena may occur together, each will be discussed separately. **Table 5.2** presents a summary of the most used actions to counter power system instability. Finally, all SPS actions mentioned here are described in more detail in section 5.5.

5.4.1 Transient angle instability

To prevent loss of synchronism, rapid and massive actions based on the direct detection of the contingency are often required. The following actions have proven to be especially effective in this role:

- Generation rejection and fast valving;
- Dynamic braking;
- Reactor switching near generators;
- Automatic load shedding.

5.4.2 Frequency instability;

The types of SPS that have proven especially effective in the control of frequency are:

- Underfrequency load shedding used to stop or reverse a frequency drop. This must occur before the thermal power plants are underfrequency tripped. The main objective is to hold the system frequency above a pre-set level (58 Hz on a 60 Hz network) and keep the network interconnected with the power plants on-line.
- Automatic tripping of interconnection lines by underfrequency relays.
- Overfrequency tripping of some or all of the units in hydro power plants (f > 61.5 Hz).

5.4.3 Voltage instability

The following actions can be taken to counter voltage instability:

- Automatic switching of shunt capacitors or tripping of shunt reactors;
- Emergency control of LTCs: blocking, return on a pre-defined position, decrease in voltage setpoint;
- Modulation of HVDC power;
- Fast unit start-up;
- Fast increase of generator voltages (through AVR setpoints);
- The right amount of load shedding, at the right place and right time is very effective in preventing voltage instability from developing [5-7, [5-8].

5.4.4 Overload cascading

The following types of actions are used by some utilities to counteract cascaded line tripping:

- Preventive automatic load shedding or generation rejection based on circuit breaker status (open and closed) on some important tie-lines;
- Gas turbine start-up;
- Power swing blocking of distance relays;
- Undervoltage load shedding.

5.4.5 Small signal angle instability

SPS actions are associated with non-continuous controls and are not normally used to improve system behavior in the case of small signal stability problems. Counter-measures used to solve small signal stability problems rely for the most part on closed-loop controls by examples:

- Generator excitation control;
- Power system stabilizer;
- Supplementary controls in static Var compensators (SVCs) and HVDC

Table 5-2. Most used actions to counteract power system instability

Possible SPS Actions		Transient instability	Frequency instability		Voltage instability	Cascade line tripping	Small signal stability
			Over-frequency	Under-frequency			
Actions on generation	Generation Rejection	*	*		*	*	
	Turbine fast valving	*					
	Gas turbine start-up			*	*	*	
	Actions on the AGC				*	*	
Actions on load	Underfrequency load shedding			*			
	Under voltage load shedding				*		
	Remote load shedding	*				*	
Actions on shunt	Automatic shunt switching	*			*		
	Braking resistor	*					
Actions on power system equipment	HVDC fast power change	*	*	*	*	*	
	Quick increase of generator voltage set point				*		
	Controlled opening of interconnection	*		*	*	*	
	Tap changers blocking			*	*		
Closed loop controls devices	Excitation controls	*					*
	Power system stabilizers						*
	SVC voltage controls	*					*
	HVDC special controls		*	*			*

5.5 DETAILED DESCRIPTION OF VARIOUS SPS ACTION

This section presents an overview of the various actions that could be used within a defense plan. The intention is to provide a starting point for the detailed investigation of a particular means of action and to help designers of defense plan in the selection of the most suitable means for countering a specific phenomenon.

Chapter 2 of [5-9] and chapter 17 of [5-1] provide further information and additional details on these SPS action. Reference [5-10] is an annotated bibliography on power system stability controls including SPS.

5.5.1 Generation rejection

Generation rejection is one of the most widely used types of SPS [5-6] rejection schemes involve the tripping of one or more generating units. The practice of generator tripping is used on all kinds of units but especially on hydro-generator units. This is because they are quite rugged compared to thermal units and the risk of damage to the unit from a sudden trip is not as great.

Generation rejection improves transient stability by reducing the accelerating torque on the machines that remain in service after a disturbance. The concept behind the generation rejection is to increase the electrical power output of the remaining generators and thus to reduce their rotor acceleration. Generation rejection can also be used to reduce power transfers on certain parts of a transmission system and thus solve overload or voltage stability problems. Normally the power shortage in the load area is reduced to zero by bringing the spinning reserve on-line and increasing its output power to that provided previously by rejected units.

5.5.2 Turbine fast valving

Turbine fast valving is applicable to thermal units and involves closing and reopening of steam valves in order to reduce the accelerating power of generators that remain connected to the network after a severe transmission fault. It is an alternative to generation rejection when a slower reduction in generator output is acceptable. Generation rejection is usually used on hydro units and fast valving on steam turbines. The advantage of fast valving is that the unit remains synchronized, and for temporary fast valving it recovers to its pre-disturbance power level. Fast valving cannot be used on hydro turbines due to water inertia.

The degree of power reduction depends on several aspects: the type of short-circuit fault, the distance between the generator and the fault, the pre-disturbance conditions (active, reactive power and voltage at unit terminals) and the power flowing through the faulted line immediately before the fault occurs.

5.5.3 Fast unit and pumping storage unit start-up

Power support by fast unit (e.g. gas turbine) or pump storage start-up could be used at low frequencies or when there is a high risk of voltage collapse caused by inadequate generation. The latter may result from the tripping of important tie-lines that interconnect regions of high generation to regions of high demand. SPS that initiate gas turbine or pump storage start-up are very efficient in recovering from these stressed situations. The gas turbine start-up process takes several minutes or tens of minutes and consequently provides a solution to long-term critical situations. (In long-term voltage stability, tap changer blocking could be used to give enough time to start the gas turbine).

5.5.4 AGC set point changes

For satisfactory operation of a power system, the frequency should remain nearly constant. The main objectives of automatic generation control (AGC) are to regulate frequency to the specified value (e.g. 60 Hz) and maintain the interchange power between areas at their scheduled values. AGC perform its tasks by controlling the load reference setpoints of a selected group of generator units in the power system.

In interconnected power systems under normal conditions, the actions of AGC are confined to its individual area so that system frequency is constant and interarea power transfers are maintained at their scheduled levels. Due to a lack of generation in a certain area caused by a combination of line

trips, setpoint changes on AGC could be used to correct the generation-load mismatch. In such a situation, other areas may assist the affected area by allowing system frequency to depart from its pre-disturbance value or by permitting the inter-area power transfer to deviate from scheduled values.

5.5.5 Underfrequency load shedding

The most common type of SPS is the underfrequency load shedding (UFLS) scheme. Schemes of this type are used to preserve the security of both the generation and transmission system during disturbances that initiate a major reduction in system frequency. Such schemes are essential if a utility intends to minimize the risk of total system collapse, maximize the reliability of the overall network and protect system equipment from damage.

In the event of a loss of generation or the loss of a tie-line used to import power, UFLS schemes are employed to reduce the connected load to a level that can be safely supplied by available generation. Load shedding is initiated by underfrequency relays designed to trip blocks of load when the frequency drops below discrete frequency thresholds and/or the rate of change of frequency exceeds pre-set df/dt values. Load shedding is generally done in several steps to prevent excessive load dropping and to allow the frequency to recover before the next step. The settings for load shedding relays and their application philosophy are mainly based on turbine-generator underfrequency operation limitations and power plant auxiliary performance. Turbine generators must be disconnected from the system when the frequency drops below 55 to 57.5 HZ (60-Hz system); the exact value depends on the type of turbine. Main objectives of UFLS schemes are described in [5-11]; they include:

- Protecting the generating equipment and transmission facilities against damage.
- Achieving near equilibrium between generation and load following loss of generation.
- Providing for equitable load shedding among utility serving loads.
- Minimizing the risk of total system collapse in the event of system separation or generation loss.
- Permitting rapid load restoration and re-establishment of interconnections.

Due to the tripping of generators and the operation of UFLS, large voltage variations often come with large frequency deviations. When loads are shed suddenly during an underfrequency event, shunt capacitors that remain in service may cause serious overvoltages. The same situation may also happen on long UHV transmission lines because of the high levels of charging current. Because of this, shunt capacitors on the subtransmission system should either have automatic overvoltage protection or be tripped by underfrequency relays. If the overvoltages are severe enough, they should be tripped as an integral part of the UFLS scheme. When available, shunt reactors on EHV transmission systems could also be switched in by overvoltage relays used to control these overvoltages [5-12].

5.5.6 Undervoltage load shedding

Power systems with heavy loading on transmission facilities and limited reactive power control can be vulnerable to voltage instability. In extreme situations, load shedding when voltage collapse is imminent may preserve system stability. Undervoltage load shedding (UVLS) is analogous to underfrequency load shedding and provides a low-cost means of preventing system collapse. A UVLS scheme uses undervoltage relays to monitor the voltage level in a substation. Normally, an undervoltage relay will operate and trip a feeder circuit breaker when the input level falls below a pre-set threshold for more than a few seconds. It is expected that after the shedding, the voltage will recover to an acceptable value. Developing appropriate settings for the UVLS is a challenging problem. Load shedding is often initiated in steps to avoid over shedding and the selection of appropriate time steps is an important factor in effective undervoltage load shedding. Sections 3 of [5-13] and 4.5 of [5-7] provide much information and additional details on UVLS design and implementation. Discussions of several issues related to UVLS are also given in [5-8, [5-14].

5.5.7 Remote load shedding

Remote load shedding is similar in concept to generation rejection but is found at the receiving end of the power system. Remote load shedding is a dormant system designed to operate after extreme contingencies affecting the system's transmission capacity (e.g. loss of several transmission lines)

whose severity largely exceeds the robustness of the residual power system. This kind of extreme contingencies endanger transient, dynamic or short-term voltage stability. In these cases, rapid and massive actions based on the direct detection of the extreme contingency are required. Remote load shedding is one of the means that could be used to maintain power system stability in such a situation. The components of a remote load shedding system can be categorized as follows:

- Inputs: mainly direct detection of the disturbance.
- A central co-coordinating system: usually required to decide which action should be taken (quantity and localization of load to shed).
- Output: feeder tripping.

Remote load shedding involves direct tripping of low priority industrial, commercial or residential load. Remote load shedding can employ the same load shedding relays as used to perform underfrequency load shedding. These relays could have a dual function, allowing both the direct execution of remote load shedding orders and the execution of load shedding as a function of local frequency conditions.

5.5.8 Automatic shunt switching (shunt reactor/capacitor tripping or closing)

SPS are widely used to control the voltage levels in a substation. This is achieved by automatic switching of shunt reactors and capacitor banks. Shunt reactors can be installed at the HV busbar in a substation, or at the tertiary winding of a transformer in an EHV/HV substation. Depending on the measured voltage level, they can be tripped or reconnected. Capacitor banks are installed in many substations to improve the power factor of the consumer load or for feeder voltage control. They are automatically switched in accordance with the busbar voltage level. This is normally achieved using a minimum voltage relay.

Shunt reactors on the HV busbar in a power plant improve the transient stability of the generating units. They act like reactive power consumers and determine which generating units need to produce more reactive power. This results in a more favorable transient stability condition during a short-circuit fault. Switching out shunt reactors following a severe contingency also greatly improves transient stability.

In long radial power systems, voltage control is often a major concern. After a severe contingency, shunt reactor and capacitor automatic switching can be used to control the voltage. They can also be used to perform a complementary slow voltage control action when the dynamic range of the generator and shunt compensation equipment (synchronous and static compensators) is insufficient to restore the voltage to a normal range on the power system. Two basic functions could be performed:

- Overvoltage control: the closing of shunt reactors (or the tripping of shunt capacitors) could be used to deal with overvoltages created by events that cause a major reduction in the power previously flowing on the power system (e.g. generation and/or load losses).
- Undervoltage control: the tripping of shunt reactors could be used to deal with undervoltage created by events that mainly affect the system's transmission capacity (e.g. multiple losses of lines).

5.5.9 Braking resistor

Dynamic braking is the concept of applying an artificial electric load to a portion of the power system. It has been generally studied and applied as a switching in of shunt resistors. This usually applies to a fixed insertion time and occurs immediately after a fault has been cleared on the system.

The control system is generally referred to an "Accelerating Power Level Detector". A signal representing the total electrical output power of those machines, whose accelerating power is to be monitored, is fed into the control system. The braking resistor would only be energized for a sudden reduction in the electrical power input. The machines in the vicinity of a fault accelerate during system fault conditions which may lead to loss of synchronism. The increased power demand from the braking resistor will oppose the speed increase acquired during the fault incident and reduces the machine angle differences. This generally improves stability for faults in the vicinity of the braking resistor.

5.5.10 HVDC fast power change

HVDC transmission links are highly controllable devices and this unique characteristic may be used to improve the transient stability of the AC system. Power flow on HVDC links can be modulated by controlling the converters. HVDC modulation can provide powerful stabilization with active and reactive power injection at each converter.

During a transient disturbance such as a fault on an interconnected power system, generator rotors swing to new angles in response to accelerating power. If these oscillations are not attenuated, system instability could occur. The DC power can be controlled to improve transient stability by rapid discrete power level changes or to improve damping by using continuous proportional control. The DC power can be either ramped down or ramped up (taking advantage of short-term overload capability) to assist power system stability. The beneficial effect of DC modulation on the AC system is similar to the effect of generation rejection or load shedding. HVDC control modulation may be used to regulate reactive power, support dynamic AC voltage, damp frequency oscillations and improve transient stability. Reference [5-15] provides many descriptions of HVDC modulation controls in HVDC installations to improve the dynamic performance of AC systems.

The controllability of HVDC links is often cited as an important advantage of DC systems. This controllability can be valuable for improving the dynamic performance of AC systems but only if DC controls systems perform adequately for various disturbances and system conditions. These controls, which can be quite powerful, must not interact unfavorably with other high performance controls and systems. HVDC control robustness is therefore a major concern.

When the DC line is the major connection between two AC systems, the rapid modulation of the DC link could be effective in attenuating transient disturbances. A problem with this control method is that a disturbance on one AC system will be shared by both AC systems. That is, a disturbance on one system will appear as a sudden load change on the other system. Unless there is some mutual benefit, the unfaulted system may not care to share the disturbance of the other system. Rapid modulation would also require reactive power compensation capability on the AC system near each converter to maintain proper voltage during the DC power flow modulation.

5.5.11 Controlled opening of interconnection

Controlled system separation is generally a last resort for saving the power system following a major disturbance involving loss of generation or imminent instability between areas. Controlled system separation is applied when specific load and generating areas can be defined within a large interconnected system. The instability between areas is usually characterized by sudden change in tie-line power. The instability is detected by monitoring one or more of the following quantities: sudden change in power flow through specific tie-lines, rate of power change or change of bus voltage angle.

As interconnected systems grow, it becomes more difficult to define system separation points that will be applicable for all possible system emergencies. Controlled separation as a planned method to achieve power system stability is not widely applied, mainly because it is difficult to define points of separation that will be acceptable for all system conditions. Controlled system separation is mainly used for power systems where load and generation are reasonably matched and transmission tie-lines to external power systems are easily definable.

The opening of intra-area and inter-area transmission interconnections shall only be initiated after the coordinated load shedding program has failed to arrest frequency declines and intolerable system conditions exist. When an operating emergency occurs, the prime consideration shall be to maintain parallel operation throughout the interconnected power system. This will provide maximum assistance to the power system(s) in trouble. Because the facilities of each power system may be vital to the secure operation of the interconnected system, every effort must be made to remain connected to it. However, if a power system operator determines that operation is endangered by remaining interconnected, he may take necessary actions to protect his own part of the system.

Tripping tie-lines is not without risk. If the interconnection supports the individual system, then tripping the tie-lines will almost certainly mean total collapse for that individual system. If the individual system supports the interconnection, then tripping the tie-lines will put the interconnection at greater risk. Unless sophisticated relaying is implemented, there is no way for an individual relay to discriminate between the two conditions. However, the ultimate decision rests with the individual system. From an overall system perspective, the preferred option is to not trip interconnection lines.

When machines of two areas are electrically separated, pole slip protection should split the system at a location designed to improve the generation - load balance in each of the two isolated systems. Pole slip protection operates significantly slower than distance protection; consequently, distance relays may operate and prevent the pole slip relay from tripping at the desired location. Effective pole slip protection depends on the success of power swing blocking elements in conventional distance relays. Most pole slip protection relays have a lens characteristic and the time taken for the impedance vector to pass through the lens is the criterion used to decide if a pole slip condition has occurred. To initiate a trip, the impedance locus can enter the lens from the left or the right, but must cross completely through to the opposite side of the lens.

5.5.12 Tap changer blocking and setpoint adjustment

The main goal of on-load tap changers (LTCs) operating on power transformers is to supply the controlled side of the transformer (normally the lower voltage) with a voltage level within a given range, according to the dead-band and the setpoint value. Typically as load increases the LTC will cause the tap position to be raised in order to maintain the voltage level. The time delay between steps ranges from 10 seconds to 4 minutes. This ensures that the load voltage is restored following a minor disturbance to an acceptable value within a few minutes.

Following a severe disturbance, the voltages will be reduced over a regional area that may affect many substations. The LTCs applied to transformers at different voltage levels all operate on local criteria and all independently start the tap changing process designed to re-establish the controlled voltage. If the voltage reductions start to progress towards a voltage collapse the bulk system voltages will slowly decrease while the LTCs are trying to restore the distribution system voltages. The transmission system will be further stressed until a new steady state is achieved or voltage collapse has occurred. Depending on the number of levels of cascaded tap changers, and their settings, this process may take from a few minutes to dozens of minutes.

Tap changer blocking or setpoint adjustment can be beneficial for preserving system stability in stressed situations that are close to voltage instability. The effect depends on the load characteristics and the degree of shunt compensation. It is also necessary to control the tap changer that is closest to the customer. Generally, just lowering the voltage at the subtransmission or medium voltage level will make the situation worse, since the tap-changer nearest to the consumer will try to re-establish the load voltage. This means that the reactive power losses will increase in the distribution system at the same time as the reactive power generation from shunt devices will decrease.

5.5.13 Quick increase of synchronous condenser voltage setpoint

Synchronous condensers, SVC's and FACTS can generate or absorb reactive power depending on the control of their excitation system and are excellent voltage and reactive power control devices. The reactive power production of a synchronous condenser is dependent on the system voltage and the voltage regulator (AVR) automatically adjusts this reactive power to maintain constant terminal voltage. .However, the reactive power must be controlled by operator action or by a specific reactive power regulator [5-16,[5-17] such that the maximum dynamic reactive range is available to counter system events.

Following a severe event leading to voltage decreases, the synchronous condenser AVR performs a fast corrective action. In order to optimize the efficiency of the synchronous condenser to counteract voltage instability, automatic increases of its voltage setpoint could be used as a supplementary action. Several means could be used to increase the voltage setpoint (step ramp, PI control [5-18]) until the synchronous condenser reactive power reaches some percentage of the compensator capability.

5.6 CONCLUSION

Defense plans could be defined as a set of coordinated defensive measures whose main purpose is to ensure that the overall power system is protected against major disturbances and multiple contingency events. Individual SPS based on generation rejection, load shedding, shunt switching or system splitting must then be regarded as basic actions that are used within a defense plan. This chapter has presented all possible means of actions that could be use by SPS to improve power system stability and reliability. The intention was to provide a starting point for the selection of the most suitable SPS action to counter specific power system phenomena.

5.7 REFERENCES

[5-1] Prabha Kundur, *Power system stability and control*, McGraw-Hill, 1994.

[5-2] T. Van Cutsem, C. Vournas, *Voltage stability of electric powers systems*, Kluwer academic publishers, Norwell, MA, 1998.

[5-3] T. Van Cutsem, *Voltage Instability: phenomena, countermeasures and analysis methods*, IEEE Trans., special issue on "Technological foundations for ...", Vol. 88, No. 2, pp. 208-227, February, 2000.

[5-4] CIGRE, TF 38.01.07, *Analysis and control of power system oscillation*, December, 1996.

[5-5] CIGRE WG38.02.19, D. Karlson, et al., System protection schemes in power, June 2001.

[5-6] CIGRE WG39.05, B. K. Lereverend, et al., *Industry Experience With Special Protection Schemes*, Electra, No. 155, August, 1994.

[5-7] CIGRE WG 34.08, D. Karlsson, et al., *Protection against voltage collapse*, August, 1997.

[5-8] C. W. Taylor, *Concepts of Undervoltage Load Shedding for Voltage Stability*, IEEE Trans. on Power Delivery, Vol. 7, No. 2, pp. 480-488, April, 1992.

[5-9] CIGRE WG38.02.19, D. Karlsson, et al., *System protection schemes in power networks*, Networks," TB 187, June 2001.

[5-10] IEEE Special Stability Controls Working Group, *Annotated Bibliography on Power System Stability Controls: 1986-1994*, IEEE Trans. on Power Systems, Vol. 11, No. 2, pp. 794-800, August 1996.

[5-11] WSCC, *Co-ordinated Off-Nominal Frequency Load Shedding and Restoration Plan*, November, 1997. Available at http://www.wscc.com.

[5-12] S. Bernard, G. Trudel, G. Scott, *A 735-kV Shunt reactors automatic switching system for Hydro-Québec network*, IEEE/PES WM, Paper 283-2 PWRS, 1996; IEEE Trans. on Power Systems, Vol. 11, No. 4, pp 1024-2030, November, 1996.

[5-13] IEEE Power System Relaying Committee, *System protection and voltage collapse*, Special publication, 93-THO-596-7-PWR, June, 1993.

[5-14] C. Moors, T. Van Cutsem, *Design of load shedding schemes against voltage instability*, IEEE/PES WM Paper 2000 WM-241, Singapore, January, 2000.

[5-15] IEEE Committee report, *HVDC controls for system dynamic performance*, IEEE Trans., Vol. PWRS-6, No. 2, pp. 743-752, May, 1991.

[5-16] V. Arcidiacono, S. Corsi, A. Natale, C. Raffaelli, *New developments in the applications of Enel transmission system automatic voltage and reactive power control*, CIGRE Meeting - Paris, 1990.

[5-17] S. Corsi, R. Chinnici, R. Lena, G. Vannelli, U. Bazzi, E. Cima, *General application to the main Enel's power plants of an advanced voltage and reactive power regulator for HV network support*, CIGRE Conference, 1998.

[5-18] S.Corsi, *The Secondary Voltage Regulation in Italy*, Panel Session, 2000 IEEE PES Summer Meeting, Seattle, WA, USA.

6 DESIGN AND DEPLOYMENT OF A WELL-COORDINATED OVERALL DEFENSE PLAN

6.1 INTRODUCTION

The diverse nature and types of extreme disturbances, coupled with their infrequent and unanticipated occurrence, points to the need for automated actions to stabilize the system in a controlled and coordinated manner by deploying a defense plan. A well-coordinated overall defense plan is needed to prevent propagation of disturbances.

The relative time of action for different type of events varies from normal to extreme, depending on the nature and speed of the disturbance and the need for coordination. An example of a time line for various types of events is shown in Chapter 3 (Figure 3-1). This figure shows that the deployment of a well-coordinated overall defense plan requires the implementation and coordination of a number of schemes and actions spanning various time periods. As part of a defense plan, wide-area protection and control schemes detect abnormal system conditions (as compared to design conditions) and take automatic corrective action based on system analyses, with the goal of restoring acceptable system performance.

This chapter focuses on the design and deployment of an overall system defense plan that will help manage system disturbances and prevent blackouts.

6.2 STEPS FOR DEPLOYMENT OF WELL-COORDINATED OVERALL DEFENSE PLAN

The blackout events of December 14, 1994, July 2 and August 10, 1996, and Aug. 14, 2003 in North America; similar events in July 14, 1999, August 28, September 23, and September 28, 2003 in Europe, and other such events around the world underscore the need for increased investment and deployment of well-defined and coordinated overall defense and restoration plans. Any investment should consider the long-term impact associated with system adjustments, be backed and preceded by comprehensive system studies, followed by frequent coordination studies over the project lie cycle, and prudent analysis of the types of investments most necessary for successful implementation [6-1].

There is no silver bullet solution to preventing blackouts, but there are general measures than can and should be taken to minimize impact of wide area disturbances. Since any of the above referenced outages were caused by a complex sequence of cascading events, electric utilities, industry regulators, and state and Federal legislators and regulatory bodies should undertake the following recommended steps to determine the root cause (what happened), understand how each disturbance happened, and identify measures and support actions to prevent similar occurrences [6-1] - [6-8]. Some of the actions may require extensive legislative and governmental support due to possible environmental, financial, or intersystem or multi-national impacts.

6.2.1 Step One: Analysis & Audits

First steps in deployment of a well-coordinated overall defense plan is to analyze existing control and protection systems, particularly ones intended to restrict and contain power system disturbances (e.g. under-frequency load shedding). System protection design and performance evaluation and corrective actions are also needed to limit the impact of future blackouts. Critical alarm monitoring systems must be maintained in top operating condition, and newer alarm analysis technologies should be deployed to detect and to prevent the spread of major disturbances. Other equipment failures may be involved, requiring detailed failure and root cause analyses. Most important, however, inadequate flows of information between neighboring control centers may have resulted in an inexcusable time delay in reacting to an escalating problem.

Other reviews should also be conducted in the immediate term including audits of various engineering disciplines such as planning, operation, and protection as well as maintenance practices to identify the factors that contributed to the recent blackout. Measures should be implemented to allow for systematic study reviews and audits of the system. Transmission system capabilities for handling today's higher flow levels and the huge volume of transactions must be investigated thoroughly.

Fast restoring of power to the users is of paramount importance after the blackout and can significantly minimize consequences of outages. It took over a day to restore the power after the August 14th blackout in North America. Efficiency of procedures and SW tools supporting

restoration, with considerations for Cold Load Pickup (CLPU), need to be analyzed and audited to identify what improvements are needed.

6.2.2 Step Two: Preventive and Corrective Actions

The analysis and audit process identifies the set of actions required to minimize the possibility that outages will happen again. Fundamental upgrades, such as improved real-time monitoring and diagnostics and training for system operators, are "low-hanging fruits" in actions to prevent major blackouts. In addition, accurate and reliable monitoring systems with faster detection and wider communication capabilities play a key role as a part of a comprehensive system defense plan.

Following measures should be taken to prevent blackouts:

- Implement System Protection Schemes and Adaptive Protection
- Regular protection coordination studies as system conditions change, including studies between generator and transmission protection devices
- Identify adequacy of protection application on routine basis
- Test not only individual relays but system protection applications
- Improve monitoring, diagnostics, and control center performance
- Secure real-time operating limits on daily basis (e.g. dynamic line ratings)
- Perform dynamic voltage and transient stability studies on a regular basis as system conditions change
- Condition assessment of aging infrastructure and improved maintenance
- Operator training, including a coordinated approach among control areas
- Frequent and effective use of Dispatch Training Simulators (DTSs)
- Requirements for generation units to withstand abnormal grid conditions

An overall system protection and control defense plan helps manage system disturbances and minimizes the potential for wide area blackouts.

6.2.3 Step Three: Public Policy and Investments in the Equipment

Preventing major blackouts in the future will require a combination of long-term investments in the transmission system and continuous improvements in public policy. Significant investment in transmission grids around the world will need to be made in the next decade. Retirement and replacement of transmission equipment at the end of its useful life will be important remedy for increasing failure rates and potential outages in the future. Beyond the aging infrastructure issue, the transmission grid must also be upgraded and expanded to handle the increased energy flows and address the operating conditions that today's transmission grids are subjected to. High-voltage power electronic devices would allow more precise and rapid switching to improve system control and to help increase the level of power transfer that can be accommodated by the existing grid. Distributed energy technologies could also play a role in relieving certain power flow demands on the transmission and distribution networks as well as in improving reliability. While the new investment will certainly include some new transmission lines, it will also encompass new power delivery technologies: Flexible AC Transmission Systems (FACTS), reactive power management (including dynamic systems controls), super-conducting materials, micro-grid, etc.

Although major improvements have been made since 2003 blackouts, there is still a need for regulatory bodies to better define and enforce the standards for reliability. Examples like establishing Electric Reliability Organization (ERO) in North America (presently planned for 2007) represent a step in that direction.

Today's communication and computer technologies have produced a new revolution in the power industry, especially in the field of power system control where vertical integration is much improved. Computer based relays communicate not only with a center, but also with each other. This in turn facilitates the deployment of overall system-wide protection and control philosophy [6-8, [6-9]. With an information infrastructure, it is possible to tie all the monitoring, control and protection devices together through an information network. The key to a successful solution is fast detection, fast and

powerful control devices, high-speed reliable communication infrastructures, and smart algorithms, in other words Wide Area Monitoring, Protection and Control System (WAMPAC).

In summary, following measures should be taken to minimize potential for blackouts:

- Strengthen transmission network, through building lines and cables and distributed generation.
- Increase transmission power control capability by use of HVDC links and FACTS.
- Regulatory actions to assure coordination and enable efficient system planning, systematic reviews, permitting, and market operations.
- Employ new technologies to enable coordinated wide-area monitoring, protection, and control systems (WAMPAC) as cost-effective solutions.
- Continue research and developments on application of new technology such as energy storage, superconductivity, and micro-grids.

6.3 DESIGN VARIABLES FOR A DEFENSE PLAN

Since a defense plan is a set of coordinated system protection and control schemes, the design variables for a defense plan are similar as for a System Protection Scheme (SPS). **Figure 6.1** shows the general structure of a system protection scheme comprising of input facilities for electric and status variables, a decision process, and output action orders.

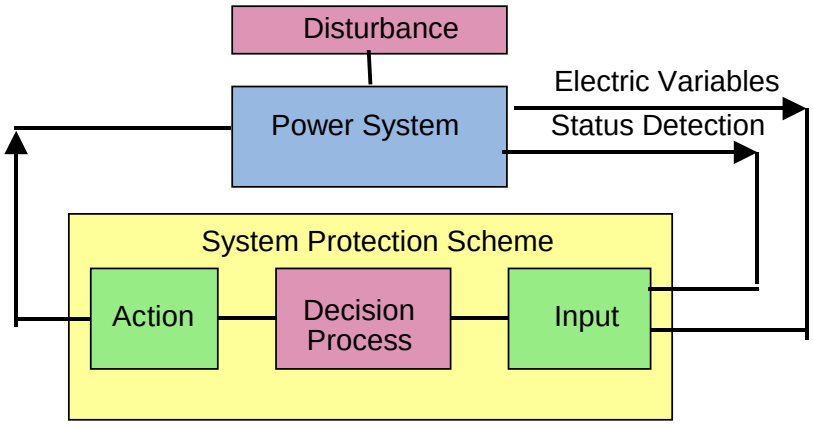


Figure 6.1 General structure of a system protection scheme

Typically, utilities rely on system protection schemes tailored to their particular grid. These are open-loop schemes aimed at providing stabilization against severe disturbances and highly stressed grid conditions. Designs are loosely categorized into:

- Event-based
- Parameter-based
- Response-based
- Combination of the above

In an event-based scheme, short circuit or outage events can be directly detected to initiate actions such as generator/load tripping, or VAR compensation. A parameter based scheme is based on a significant change in measured variables t initiate actions. Most of the schemes implemented in practice are being triggered by combination of events and parameters. Those schemes initiate pre-planned, automatic, and corrective actions based on studies of pre-defined system contingencies for variety of conditions

In a response-based scheme, during disturbances, there is a close loop incorporated in the decision process to provide better response to actual system conditions. Response-based schemes may be less expensive because fewer sensors and communications paths may be needed.

6.3.1 Set of System Variables

Depending on the purpose of a defense plan, different quantities have to be measured or derived at different speed and accuracy levels (compare events shown in Chapter 3, Figure 3-1). Some remedial actions have to be effective within fractions of a second, e.g. against loss of synchronism. On the other hand, actions against thermal limitations or long-term voltage instability can be allowed to take longer time, in the area of seconds as opposed to milliseconds. There are basically two types of indicators of instability: those directly measured in the power system (such as voltage current, frequency, power flow, status values) and those indicators derived from the measurements.

A general set of variables is also achieved from a power system state calculation through the use of real-time state estimators running real-time contingency analysis. They need to be proven, accurate, with reliable telemetry and 90-95% convergence, and with availability of critical functions to 99.99% or better. A Supervisory and Data Acquisition (SCADA) based state estimation could be improved by using phasor measurement units (PMU). Results are based on complete observability by PMUs, from which any type of index can be derived. Also, faster than real-time simulations, based on the state calculation, may be possible.

In the list below, some examples are given for suitable inputs to a remedial action, for various applications. The variables can be either directly measured, or derived from the measurements by more or less complex algorithms. Refer to chapter 7 for details.

Directly Measured Basic Inputs

- Power System Voltages and Currents
- Control Signal
- Status

First level derived variables

Included in the first level derived variables are quantities based on measurement of one quantity, or arithmetic functions of the same type of quantities, such as:

- Time derivatives of the measured quantities
- Sum and difference of the same type of quantity
- Maximum, minimum, mean, RMS, etc., of a measured quantity
- Frequency, rate-of-change of frequency of AC quantities
- Phase angle, phase angle differences, etc., for AC phasors

Second level derived variables

Included in the second level derived variables are quantities based on measurements of several quantities, such as:

- Power and rate of change of power
- Impedance and rate of change of impedance
- Volts per Hertz (V/f) and dV/df
- Volt/power related quantities, e.g. dV/dP, dV/dQ

Complex variables

Included in complex variables are indices based on measurements from a larger area of the power system or from a state estimation (or PMU-based state calculation), such as:

- Minimum singular value for the load-flow Jacobian
- Load impedance compared to Thevenin impedance
- Severity indices for instability detection (both in time or frequency domains)

Based on the measured and derived variables, different algorithms can be designed for protection and emergency control.

6.3.2 System Measures

There is a rather limited amount of system measures that can be taken to prevent a hazardous system from going unstable. System measures for certain phenomena are shown below.

Actions to counteract angular instability include:

- Load shedding or load switching
- Generation rejection
- Fast valving
- HVDC support
- Braking resistors
- AVR boosting
- Shunt device switching
- FACTS stabilizing support
- Actions to counteract voltage instability are:
- Under-voltage load shedding
- Reactive power support
- HVDC support
- Gas turbine start up
- Tap-changer blocking
- Actions to counteract active power unbalance in the islanded system are:
- Under-frequency and or rate-of-change-of frequency load shedding (power deficiency)
- Generation tripping (power surplus)

Selection of SPS for mitigating extreme contingencies is described in Chapter 5.

6.3.3 Cost of and Interaction among Different Measures

The cost of different measures always has to be compared to the benefit for the power system, as well as to other measures and their benefit. Measures such as switching of shunt devices, start of gas turbines, and emergency power from HVDC links are preferable to last resort measures such as system separation and load shedding. Non-discriminative load shedding is normally the most costly as it includes customers. However, in very severe situations, there might not be enough time to wait for slower speed actions and fast measures are required.

Interruption costs are very different for different customers, and it varies also with respect to time and duration. Load shedding or load reduction based on contracts with customers that reduce their load on demand from the grid operator, is a very attractive solution. The problem might be that rather large individual loads are needed, and an alternative supply must be available for the customer. The most common example is probably large electrical heaters that can be switched to gas or oil fire, in case of high prices on electricity or network problems.

A well-coordinated defense plan design requires that all measures are coordinated to avoid worsening the disturbance and to allow for the most cost-effective way to arrest disturbance propagation.

For example, generator tripping needs to be coordinated with the rest of the system. Tripping generation too early, under low frequency conditions, before system load shedding has been fully utilized will further stress the system. Also, it is not advisable to trip a large number of generators simultaneously in order to avoid large frequency and angle oscillations. Furthermore, unnecessary generator tripping can be prevented by better coordination of generator protection with generator excitation control system, generator capability curves, and system frequency protection. Coordination among following elements is required:

- Loss-of-Field protection with AVR (automated voltage regulator) minimum excitation limiter (MEL) and Steady-State Stability Limits
- Over-excitation V/Hz protection with AVR over-excitation limiter (OEL)
- MEL and OEL with generator capability curve

Some other issues to consider: effects of low voltages on auxiliary system motors; impact of out-of-step swings; and use of Power System Stabilizers (PSS) to prevent instability.

Another example is related to preventing voltage collapse. Although active and reactive power support and voltage control are preferable, it may still be required to implement last resort under-voltage load shedding. In implementing under-voltage load shedding settings, reactive compensation availability and response need to be considered (e.g. impact of shunt capacitors and dynamic sources, such as SVCs and STATCOMs).

For angular instability problems, well-tuned power system stabilizers (PSS) are very efficient for small perturbations and normal network topology. In situations with significant loss of lines and wide angular excursions, more powerful measures are necessary, such as damping resistors, SVC, FACTS or TCSC devices. Again, effective last-resort measures to prevent further propagation of the disturbance are controlled system islanding and, finally, load shedding.

There are different ways to coordinate different measures, such as:

1) Identify the severity of the disturbance, in terms of deviation from nominal values for power system quantities. Then, select and adjust the measures to mitigate the disturbance.
2) "Closed-loop" process identifying priority of actions form the pre-defined list and evaluating the system response after each action. Continue to take actions from the list until the disturbance is controlled.
3) Combine the two processes above.

6.3.4 Advantages and Disadvantages of Distributed vs. Central Schemes

There are two opposing extreme philosophies in implementing a defense plan:

1) System scheme that requires communication links, sophisticated measurements, and centralized decision making
2) Scheme that relies on local measurements alone

The fully rely on the centralized approach; it would be required to add more intelligent applications to the control center (thereby increasing the number of "applications", i.e., software programs). With this trend, local devices would merely send data to the control center, and wait for the control center to determine the appropriate control actions. For this implementation, a time delay exists starting at the moment the data is collected and includes the time for traveling through the communications network, the time for the collection and processing at the control center, and finally the time for the decision to be communicated down to the local (substation) devices. This time delay is acceptable for normal day-to-day operation, but may be inadequate when the grid is in an emergency state for which correct decisions have to be carried out immediately. There is also an inherent problem to consider with the likelihood of a communications breakdown.

In conclusion, despite the fact that a defense plan addresses a system problem, there is a need for devices that use only local measurements. These devices are to be counted upon when other controls are not fast enough or cannot mitigate the aggravating situation. They also form the fallback position, or a safety net, for any global control/protection scheme when communication channels fail.

Complete decentralized control goes to the opposite extreme, all decisions are made locally based on local and system information received from either other local devices or from the central location. This is still an active area of research. Even if completely decentralized control works, it may take years for the proof of concept and acceptance by a utility industry.

Therefore, a combined approach based on scalability is recommended. Scalability means that the design must be modular to satisfy specific needs of the grid (local, regional or network-wide needs). The key to this approach is to extract as much intelligence as possible out of local devices, and where possible, allow the local devices to manage some of the tasks pertinent to the equipment being monitored. The practicality of this approach is that it allows a migration path for the users.

Improvements in communication and computer technology, as well as development of new algorithms to detect and prevent propagation of disturbances will influence how and where protection and control decisions are made. As communication system architecture has a major influence on a defense plan design, some of the issues related to centralized and decentralized schemes will be addressed in the next section.

6.3.5 Measurement and Communication System Architecture

Measurements are normally taken from the ordinary substation measurement equipment, such as CTs, VTs, position indicators and other transducers, and communicated, as measurements or binary signal. A system based on binary signals, such as "low voltage", "high power transfer", etc., where the measurement and evaluation is made locally and only the binary indicator is communicated, has much lower requirements on communication facilities and is normally much more robust, than systems where communication of measurement data is required.

One of the vital elements of a defense plan design is a reliable and secure communication. These devices are often required to send, receive, filter and process status and/or analog measurements. Some communication requirements/solutions include the following:

- Communication architecture to support redundancy and data integrity
- Sufficient bandwidth to meet the communication time constraints
- Communication system diagnostics/alarms
- The communication system architecture is normally either hub-based or ring based, see **Figures 6.2** and **6.3**.

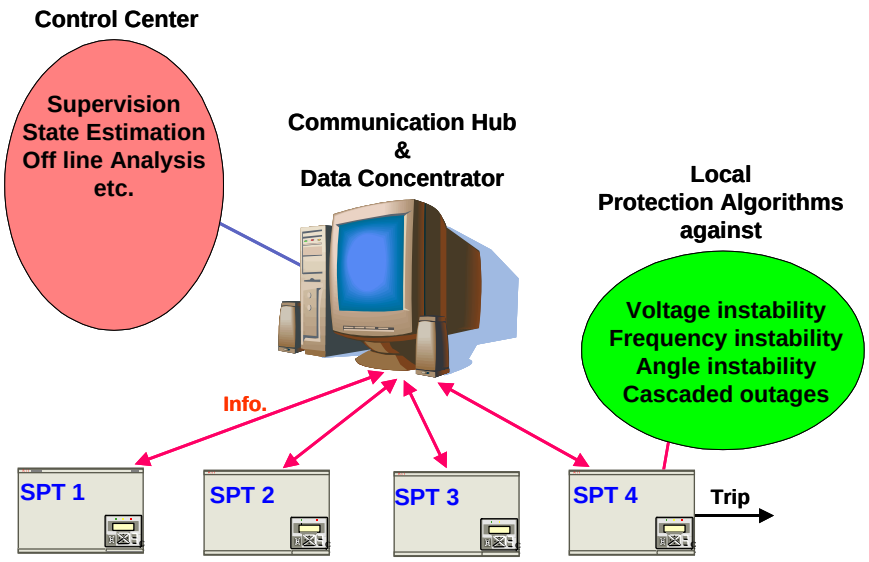


Figure 6.2 Hub-based communication architecture

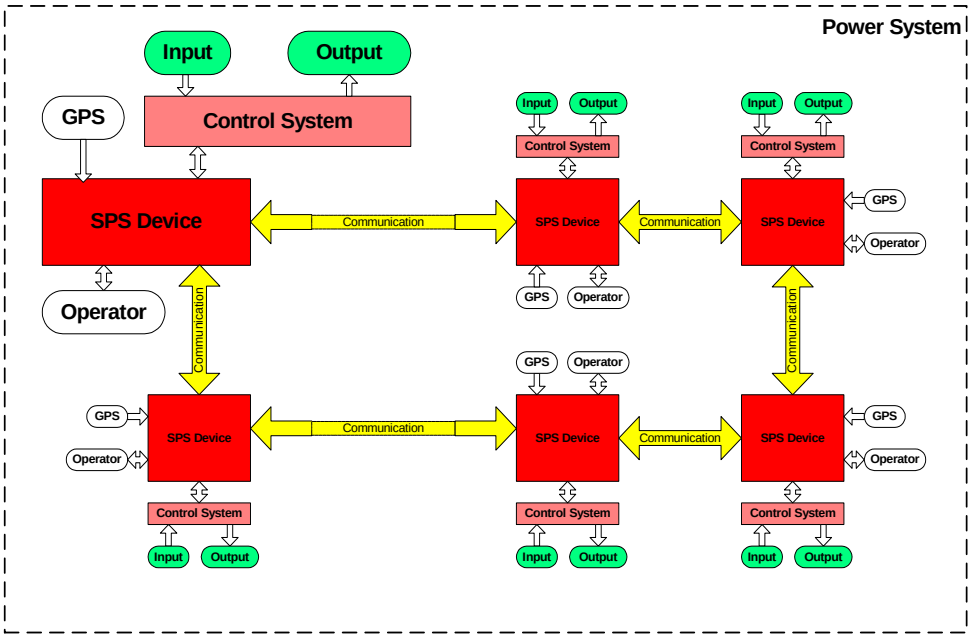


Figure 6.3 Ring-based communication architecture

In **Figure 6.2**, system protection terminals (SPTs) at different locations in the power system send their data to a hub protection center, which contains all the protection and emergency control algorithms. The protection center then sends out the trip and control orders. In order to avoid remote trip signals to be communicated in the network, the protection and control algorithms can be implemented in the substation, where the action is to be taken. In such a design the center is just a communication HUB, for exchange of measurements and data among the different SPTs.

A ring-based system is schematically shown in **Figure 6.3**. One arbitrary communication link can fail without any impact on the system functionality. Control Centers play important role in for coordination, manual arming capability, and communication.

For large systems hub and ring based systems might be too complex. A multi-layer architecture might then be an attractive alternative, as depicted in **Figure 6.4**.

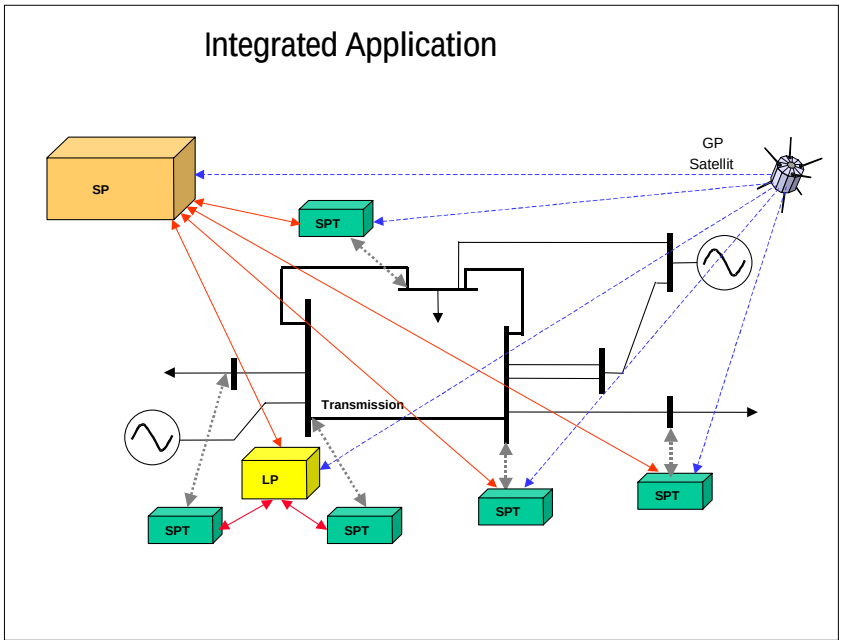


Figure 6.4 Multi-layered wide area protection architecture

The bottom layer and the basis of the multi-layered wide area protection system consists of system protection terminals (SPTs) or, in some cases, only phasor measurement units (PMUs). Groups of SPTs are integrated into the next layer, Local Protection Centers (LPCs). The top layer, System Protection Center (SPC) acts as the coordinator for LPCs. The extent and speed of disturbance would determine the types of calculations and information required to initiate actions. This three-layered architecture design may be achieved in incremental phases.

The initial objective is to develop the monitoring capability, e.g. Wide Area Measurement System (WAMS), with main purpose to improve post fault analysis, operator information, and state estimation. In the next phase, a WAMS could evolve into a Wide Area Measurement, Protection and Control (WAMPAC) system that would represent enhancement to SPSs. The conventional protection and control would still provide a fallback position, e.g. in case of a fast system protection breakdown. An alternative to the multi-layered system architecture can be so-called “flat architecture”, where SPTs are communicating with each other directly, using a ring communication structure, and acting as intelligent agents in a peer network.

6.4 DESIGN CRITERIA FOR A WELL COORDINATED OVERALL DEFENSE PLAN

System protection is a fast-detection, fast-response power system network security mechanism. It comprises of distributed, smart algorithms and electronic devices, which may need to communicate with one another, or with a central processor, over secure and reliable communication medium, and collectively react to unexpected incidents on the power grid. Even though incidents that can trigger a massive power blackout are very rare, a robust power grid without a defense plan is forced to operate conservatively all the time due to the fear of the unknowns, also known as contingencies. In the deregulated market, this conservative mentality translates into lost financial opportunity for the asset owners.

While system protection schemes have substantial advantages, there are certain concerns as well. As the existing transmission facilities may be more heavily utilized, there can be an increased exposure to potential criteria violations. The increased transmission system utilization and control schemes can also make it more difficult to schedule transmission outages and to operate the system. It is these reliability concerns that have led to the development of the additional guidelines concerning the implementation of a defense plan. The judgment will need to be used by system planners and operators in determining when the application of SPS will be acceptable. It is recognized that it is not possible

or desirable to have strict standards for the acceptability of the use of system protection schemes in all potential applications. Following design guidelines are recommended:

- When protecting the system from damage, remove the least amount of equipment from the transmission network
- Do not erroneously operate to cause outages of higher impact than originally designed for
- Scheme activation should not negatively impact transmission system operation
- Should allow for equipment maintenance
- Cascading transmission outages or system instability should not occur for failure of a single component, which would result in failure to operate when required
- The need for redundancy should be based on an evaluation of the system consequences for the failure of the system to operate, and the need to maintain overall system reliability

The implementation goal is to ensure that a defense plan will retain full functionality during the worst operating conditions for which a defense plan has been designed. Summary of criteria to assure proper implementation of a Defense Plan are listed below:

- Clearly understand the requirements and define functionality based on those requirements.
- Evaluate multiple solutions to find the proper balance among cost, performance, and risks.
- Define performance expected, including balance between reliability vs. security.
- Find proper balance between complexity vs. simplicity
- Dialog with all entities involved
- Define communication paths and specify reliability and availability of telecommunication system
- Plan for upgrades in the field.
- Define system topology, including HW, SW, and Logic
- Implement condition monitoring, including system diagnostics, communication diagnostics, and cyber security
- Coordinate with other schemes
- Consider operation and maintenance requirements, plans, and costs
- Develop a large scale test plan
- Field Commissioning Tests
- On-line test
- Periodic Testing
- Implement training for the staff using and being affected by this defense plan.

Next, some key design and implementation criteria will be described in more details.

6.4.1 Performance Based Specification

A defense plan is important for two main reasons. Firstly, it provides emergency protection and control, which acts as a safety net for operation of the power system. By limiting the consequences of disturbances and interruptions, it contributes to reducing the risk of operation. Secondly, it can be used as a proactive measure for increasing operating limits. For example, by implementing automatic schemes for generator tripping, load shedding, network separation, etc., capacity limits may be increased without security violations.

Developing a defense plan scheme requires a good knowledge of the chosen grid and a significant amount of engineering time to analyze "plausible" scenarios the scheme is to be exposed to and to specify what performance is expected from the scheme. Expected performance of the scheme is based on to the type and intended application.

6.4.1.1 Transmission System

A transfer limit placed on a given corridor is obtained from off-line simulations. Such limits are always on the conservative side because engineers take into account the outage of most critical equipment. Also, the exactness of such limits is often questionable because of many uncertainties in simulation analysis. Uncertainties include modeling and data errors, and differences between the simulated and the actual operating conditions. Simulations are usually performed off-line and are often performed several months before actual operation. The speed with which the protection/control devices or systems respond to disturbances is also taken into account in the simulation analysis.

A main task in the simulation analysis is the determination of power transfer corridor (PTC) limits. A PTC is defined as a set of circuits (transmission lines) or transformers separating two portions of the power system (closed interface), or a subset of circuits exposed to a substantial portion of the transmission exchange between two parts of the system (open interface).

In this context, the power flow on a PTC represents the net power flow from a sending end area to a receiving end area. At present, most utilities apply a deterministic (N-1) criterion as the main operational security criterion. The (N-1) is a simple, technical criterion which states that the system should be designed and operated in such a way that it is able to withstand any single contingency, e.g. outage of a line or generator, without resulting in unacceptable consequences. For some PTCs, a relaxed weather-dependent version of the N-1 criterion is applied.

The determination of PTC limits is an established part of operating procedures and the limits are generally determined from three different criteria:

- Thermal capacity limits (the steady state N-1 limit)
- Voltage constrained limits (dynamic or steady-state)
- Angle stability limit (transient stability or power oscillations)

In reality, these limits are functions of the state of the system (i.e. the load flow and network topology). Based on some loading criteria, the various limits may be as illustrated in **Figure 6.5**.

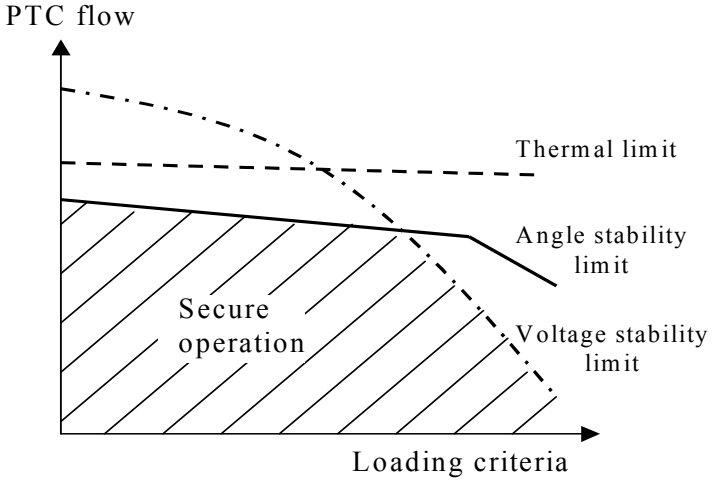


Figure 6.5 Typical Power-Transfer Corridor (PTC) limits

A typical situation is that the thermal capacity limit is fairly constant (when the network topology is unchanged), while the voltage stability limit is strongly dependent on system loading and reactive reserves. The angle stability limits may take different forms, but a loading limit will always exist. In some cases the operating limits will be determined by the voltage and angle stability constraints. On other interfaces or PTCs, the limits may be thermally constrained. In today's interconnected power

systems three phenomena mentioned above occur together. For example, overload cascading usually leads to low voltage and motor stalling (voltage collapse), as well as to angular instability.

A fundamental problem concerning the limits is that they are generally difficult to determine with sufficient accuracy and reliability, particularly for the exact on-line contingency that causes violation of those limits. This implies that limits are often set conservatively. By implementing a well-coordinated defense plan, it is possible to improve performance of the grid by better utilize power system margins without sacrificing reliability.

Performance based requirements for all three phenomena above, to resolve identified constraints are described below.

Thermal constraints:

- This is very much related to congestion management and handling of bottlenecks for efficient and secure operation. If a defense scheme is designed correctly, the transfer limits could be increased by considering following requirements:
- Estimate the impact of disturbance on the loading of the connection. Usually the post-disturbance loading can be tolerated for a time period before an action needs to be taken. During that time period, a defense plan must determine where generation should be adjusted (boosted or reduced) and possibly the types and amounts of load to shed.
- Enhance the existing overload protection with dynamic rating for the connection. Information (input) needed for dynamic rating includes non-electrical parameters such as wind speed, ambient temperature, line sag, etc.

The diagram below (**Figure 6.6**) can describe thermal damage to a transmission line qualitatively. This curve can be used to determine how fast the control action needs to be to prevent thermal damage. Usually, the time is not as critical as in the case of frequency instability or voltage instability (i.e., the time window is somewhat predictable, in the range of minutes).

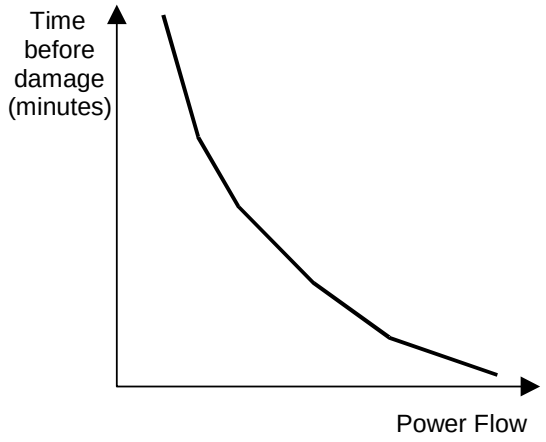


Figure 6.6 Relationship between thermal damage and power flow

"Overload cascading" normally moves slowly enough for operators to be effective. However, as today's systems are more heavily loaded (line starts out at a higher temperature and sag), it may outpace the operators so they loose the ability to properly intervene. One option is implementing overload protection on transmission lines, for example a thermal replica type that trips the line only at the verge of conductor damage. In addition, protection that can operate on high line loadings should be modeled in power flow contingency analysis studies.

Voltage-instability constraints

Design a defense plan to detect the closeness to voltage collapse fulfilling following requirements:

- Provide an early warning signal for the system operator. In this case, the subsequent control actions are up to the judgment of the operator.
- Perform automatic load shedding that should determine how much load to shed, where to shed, and how best to coordinate this measure with other measures (load tap-change blocking, capacitor switching, VC/STATCOM operation, etc.).

Angular instability constraints

If the system loses synchronism, a defense plan may detect an out-of-step condition and take actions based on performance requirements, such as:

- Speed and level of angle separation. For example, phasor measurement units (PMUs) could help provide early warning signs.
- Separate the system so the isolated areas have load and generation as balanced as possible to avoid load or generation tripping.
- After appropriate measures are taken, reconnect the system as soon as possible. For example, allow re-closing based on on-line conditions.

Example for a corridor

An example scheme for a corridor is illustrated in **Figure 6.7**. Two lines are loaded such that if one line fails, the remaining line is able to carry the full load. The system relies on a central control logic that supervises line status and transfer levels. Depending on whether the line is out of service, the central controller sends signals to generators on each side of the interconnection. Generation on the sending side can be immediately reduced to avoid overloading of the remaining line. Likewise, generation on the receiving side can be ordered to boost production (or shed load). The outcome is the utility can operate the tie lines at higher transfer levels, knowing that in an emergency, the control scheme operates and reduces the loading on the remaining line. High transfer levels imply a higher earning.

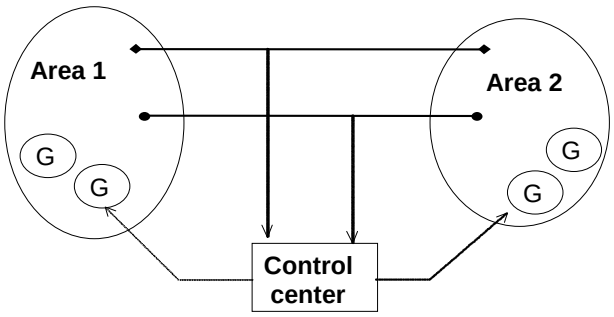


Figure 6.7 Representation of 2-area power system with SPS

6.4.1.2 Power Plant

Power plant owners set protection with protection of the plant as the highest priority. Power plants may trip needlessly during system upsets and islanding may be problematic. Islanding will impose some voltage and frequency excursions on plants. To achieve effective islanding, it needs to be coordinated with plant protection.

Some design criteria are addressed below:

- Problems like loss of excitation protection operating on the combination of high voltage and power swings should be avoided. Application of dual zone LOE protection is one option.

- Plant protection needs to be simulated in dynamic studies. Such simulation requires accurate load modeling, which in turn means modeling of induction motors and switch mode power supplies and the new discharge lighting that is replacing incandescent lamps in homes and businesses.
- Over-frequency in islands needs to be properly addressed. Over-speed protection and controls on generation can be unpredictable and should be studied. In general, islands with excess generation should not collapse as they often do. Plant over-speed controls and protection are rarely conducive to island survival.

In general, there is a need for a standard that outlines the intricacies of plant and grid protection and the tradeoffs to be achieved.

A related issue is plant design that allows the plant to ride through voltage and frequency excursions and tolerate failures within the plant. Most 500 MW combined cycle plants shut down completely for any in-plant problem that affects the steam or gas turbine portions of the plant. Modest additional expenditures that would allow continued operation at reduced power upon such an event might need to be made.

6.4.2 Reliability Requirements

The ultimate wide area system protection system would be a scheme that adapts to the changing conditions and provides a balance between the somewhat contradictory requirements on reliability:

- A scheme should always act when it is supposed to (i.e. dependability)
- A scheme never acts when it is not supposed to (i.e. security)
- A scheme should not act excessively (i.e. it should be able to shed the appropriate amount of load or generation in order to keep the system as much as possible intact.)

Implementing a scheme as described requires reliable and high-speed communications. The exact information about generators' status and output level need to also be tracked continually.

To assure a high level of reliability, separation of traditional protection and control devices from defense plan devices is strongly recommended. Separation of equipment location between conventional and defense plan devices is also recommended. Reasons for maintaining such separation include:

- Different functional requirements, and device set points
- Different maintenance and clearance requirements; set point changes are driven by different criteria and could have potential impact to other application
- Clear demarcation points exist between the two types of applications.
- Different maintenance and operating needs
- Potential confusion from operating and maintenance prospective
- Different failure response times between conventional protection and wide Area monitoring – Based on intended application and levels of redundancy
- Availability of the devices for routine automated system testing (isolation or unavailability of the wide area monitoring devices may not cause system limitations while may not be acceptable from the equipment protection prospective)
- Need for different test and isolation points
- Communication network, interfaces, and routing are different between defense plan devices and those used for conventional equipment protection

Ultimately, each application would need to be evaluated on a case-by-case basis. The complexity of the scheme, its purpose, space availability, and other factors may drive some of these decisions. Ultimately, the pluses and minuses of each option must be quantified in order to make the optimal

decision. It is recommended that the cost of the project be evaluated over its total life cycle (which includes ease of test and maintenance).

6.4.3 Operation and Maintenance Criteria to Assure Reliability and Security

System protection schemes are generally intended to operate for rare events, therefore, a well-defined operation and maintenance criteria and well-developed automated testing to verify inputs, logic, and output are critical in operating and maintaining the scheme when needed. The scheme needs to be maintained and upgraded due to the continually changing nature of the power grid. Therefore, equipment selection, application and implementation are a critical consideration. Equipment selection should consider provisions for adaptability of software and hardware to changing power system during the project life. Also, experience shows that catastrophes are usually not caused by outages of single equipment, but rather the result of a combination of unusual failures and circumstances.

Following operation and maintenance criteria are addressed to assure reliable and secure operation and maintenance of a scheme:

- Scheme purpose and overview
- Design criteria
- Logic
- Hardware (substation, transfer trip, auxiliary tripping, etc.)
- Redundancy
- Arming
- Detection
- Coordination with other protection and control schemes
- Telecommunication channels and path routing
- Actions Initiated
- Monitoring
- Commissioning, Maintenance, and Testing
- Performance and operational history
- Operating procedures for abnormal contingencies
- Partial loss of input data required for arming
- Total loss of input data required for arming
- Catalog Information

Above criteria should be addressed and fulfilled to deploy any scheme in a well-coordinated defense plan.

6.4.4 Redundancy Considerations

Redundant systems require more initial costs, but reduce costs during the life cycle of the systems. They increase operations and maintenance efficiency by minimizing downtime. Some of the drawbacks of redundant systems are in increased hardware. Depending on the application philosophy of primary and redundant applications being same or different hardware (component, additional training costs and need for more spare parts may also be considered as drawbacks. However, if product and type of hardware used are common to other protection and control applications, then added hardware and training are addressed from a system prospective. In general, the benefits over the life cycle outweigh the initial startup cost.

Some of the operation benefits of redundant systems are in:

- Safeguards against malfunctions in case an element in the chain fails to operate.
- Assurance that a faulty system will trip off-line even when one of the redundant devices fail.
- Reducing impact of measurement source failure. For example if voltage and frequency are computed from voltage source if source information is not correct.
- Minimizing inadequacy in the design of one of devices if different principle of operation is not repeated in the redundant (alternate) system.
- Redundant systems increase both reliability and security. They provide assurance for design flaws including:
- Failure in a power supply design
- Failure in the processor board
- Bad DSP
- Failure of a common operating element
- Failure or malfunction of software
- Supplier of parts for the protective device may change components and that would impact the overall package

In addition, redundant schemes safeguard against life cycle failures, such as aging of components (e.g.. electrolytic capacitor drying, transistor age failure mechanism).

In conclusion, as overall defense plan is very important system that has to be both secure and reliable, it is preferable to use redundant systems.

6.5 INTEGRATION OF A DEFENSE PLAN

In general every protection action, must be triggered by very specific criteria, event based or response based, and coordinated with other measures, that might be triggered by the same event, in order not to over- or under-react. Each SPS comprises of integrated and sometimes sequential or hierarchical, actions. Then, different SPS operating in the same area and forming a defense plan must be integrated. Furthermore, if required, various defense plans implemented in a region (e.g. WECC) should also be coordinated.

6.5.1 Coordination With Other Schemes and Measures

As already discussed in section 6.3.3, it is required to coordinate SPS with other SPSs and protection systems. There are many challenges to SPS applications in particular, as part of system planning and operating studies, that if not considered the scheme can inadvertently operate for an undesired condition.

For example, the rating of a system facility (e.g. transmission line, transformer, etc.) should not exceed the rating of the most limiting series element in the circuit or path of the facility, including terminal connections and associated equipment. In cases where protection systems and control settings constitute a loading limit on a facility, this limit should become the rating for that facility. Ratings of jointly owned facilities should be coordinated and provided on a consistent basis.

It is also important to perform “Open Loop Studies”. The open transmission loops may be difficult to identify. However, one can attempt to list and study those that could be identified. Over time, other open loop conditions could be studied as they are identified as critical. One of the challenges associated with performing advanced studies is identifying the pre-outage conditions to best represent overall system so that the study results could be used for a variety of contingencies that could not be predicted when the open loop condition actually occurs.

The sub-regions should evaluate the impact of open loop operation on their respective sub-regional paths. The potential factors for conducting emergency Operating Transfer Capacity (OTC) studies should include but not be limited to:

- The length of the outage
- Any abnormal conditions that may exist or were caused at the time of the open loop operation.
- Determination of whether the existing pre-defined islanding points are impacted
- The sub-regions should share the results of the studies with other sub-regions and coordinate overall impact

Another aspect to consider is the challenge associated with additional generation using the already congested grid. An SPS detects abnormal system conditions and take pre-planned, corrective action to provide acceptable system performance. In the context of new generation projects, the primary action of an SPS would be to detect a transmission outage or an overloaded transmission facility and then trip or run back generation output to avoid potential overloaded facilities or other criteria violations.

The alternatives to an SPS are pre-contingency generation curtailment or new transmission facilities. The primary reasons why an SPS might be selected over new transmission facilities are that an SPS can normally be implemented much more quickly and for a much lower cost. Due to these advantages, SPS is an alternative commonly proposed as a cost-effective method of integrating new generation into the grid while maintaining system reliability.

6.5.2 Power System Restoration

As it would not be possible to completely prevent blackouts, is it is important to put significant emphasis on effective and fast power system restoration after major disturbances. Returning equipment to service, followed by quick restoration of power to the users, is of paramount importance and can significantly minimize consequences of further outages. Power system restoration needs to be executed with well-defined procedures that require overall coordination within the restoring area, as well as with the neighboring electrical networks.

After the August 2003 blackout in North America, it took considerable time to restore generation. Some of the units did not have capabilities to be put in service immediately (black-start capabilities), and some units required longer time to be put online with full power (e.g. nuclear units due to security, and steam turbines due to allowable ramp-up rates). Although most of the cities during the Italian blackout in September 2003 were restored in five to nine hours it took more than a day to restore power to Detroit and New York. The slower pace for load restoration experienced in New York is due to the fact that the low voltage network loads in New York City and Manhattan area are part of a highly meshed Network system that affords a very high degree of reliability against localized outages. However, under blackout conditions, when a network is to be restored, the Network is isolated into 100 to 200 megawatt (MW) portions that need to be re-energized at a time, requiring a time-consuming and careful process so that the inrush does not provide a setback to the restoration effort.

Power system voltage, frequency oscillations, and the outage duration are critical factors in restoration. One contributing element to increased outage duration is the time it takes to identify the cause of an outage to be a system wide disturbance, recognizing the shortcoming leading to the disturbance, and the coordination process to determine the starting location. Hence, the importance of well defined and engineered information processing, to minimize preliminary outage investigation, and in order to allow time to focus on restoration process. The season and time of disturbance could also impact restoration process. In different seasons different types of load may be predominant. For example, load patterns on a hot summer day as opposed to a cold winter day. Outage restorations could also be prolonged if the effects of Cold Load Pickup or Hot Load Pickup are not carefully considered during system restoration [6-10].

Today's technology can be used to our advantage for a well-coordinated restoration plan. Some of the key elements for designing responsive restoration are:

- Well-defined procedures that require overall coordination within the restoring area, as well as with neighboring electric networks.
- Reliable and efficient restoration software tools that can significantly aid operators and area coordinators to execute operating procedures and to make proper decisions. This

tool is a part of the EMS/SCADA system that provides voltage, frequency, outage status, and other data.

- Regular training sessions to assure effectiveness of the process. The sessions should include practice drill scenarios that should incorporate any regional reliability or governmental policy requirements. For example, there may be a time delay requirement for load restoration after a bulk power system has returned to service, to allow the system to stabilize. There may also be critical loads, which must be given higher priority in restoration.

Automated restoration has not been widely used (usual implementation is by restoring loads switched off by under-frequency load shedding as the frequency recovers) to avoid unexpected worsening effects on the system. There is a potential in using new communication and measurement technologies for wider implementation of automated power system restoration to help operators speed up the process.

Designing the power system not considering the effects on restoration efforts may have detrimental effects on the speed of restoration. Restoration time and system security could be improved by planning of the generation mix and location considering not only market factors but incorporating value of faster restoration in the financial model.

6.6 TECHNOLOGIES SUPPORTING COORDINATION AND INTEGRATION

Evaluation alternatives should involve in-depth knowledge of the existing practices, operating constraints, and Regional, Provincial, or Governmental Reliability requirements, and cost effectiveness of the solutions. When the technology does not meet the functional requirements such as reliable out of step detection methods, load shedding, islanding, restoration, etc. in the best possible ways, then is to look for opportunities to develop solutions to fulfill the requirements. Another key component of technology evaluation is ability to upgrade equipment as system conditions change. Upgradeability should be evaluated from both a HW and SW perspective as power system configuration and/or flow patterns change over the project life.

Measurement and telecommunication technologies are key tools required to achieve coordination and integration of a defense plan. One of the most important functions of any coordinated defense scheme is the control of real time data flow within and between the control centers, substations and plants of the power system to be protected. To be implemented, this function requires a telecommunication infrastructure, considered as the backbone of the system protection scheme.

GPS-synchronization is the most common and reliable method to achieve coordination with respect to time. Based on the accurate time synchronization, phasors from AC quantities can be derived, from different parts of any power system, and used to from suitable criteria.

6.6.1 Synchronized Phasor Measurements

Phasor Measurement Unit (PMU) is a device for synchronized measurement of AC power flow is an indirect method of measuring and controlling the angle. Based on synchronized phasor measurements, more efficient state estimation can be performed. Based on fast and reliable state estimation a variety of system stability indices can be derived and monitored on-line to the system operator. Different (faster than real-time) stability programs for a number of contingencies can then be run to evaluate risks and margins.

Figure 6.8 shows the principle way of deriving the phasor from an AC-quantity. The phasor is a complex variable and can be expressed either as magnitude and phase angle or as real and imaginary part. A sinusoidal AC quantity is plotted as function of time in the lower diagram. The starting time (t=0) is set by absolute time reference and defines the phase angle θ. Differences between phase-angles are then independent of the starting time.

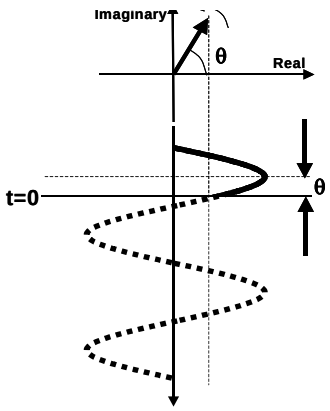


Figure 6.8 Phasor definition

By synchronizing the sampling processes for different signals - which may be hundreds of km apart - it is possible to put their phasors in the same phasor diagram, as shown in **Figure 6.9**. The voltages U1 and U2 are measured in two different substations, with time-synchronized measurements. The instantaneous values of the voltages can therefore be plotted in the same time-diagram, as well as their phasors.

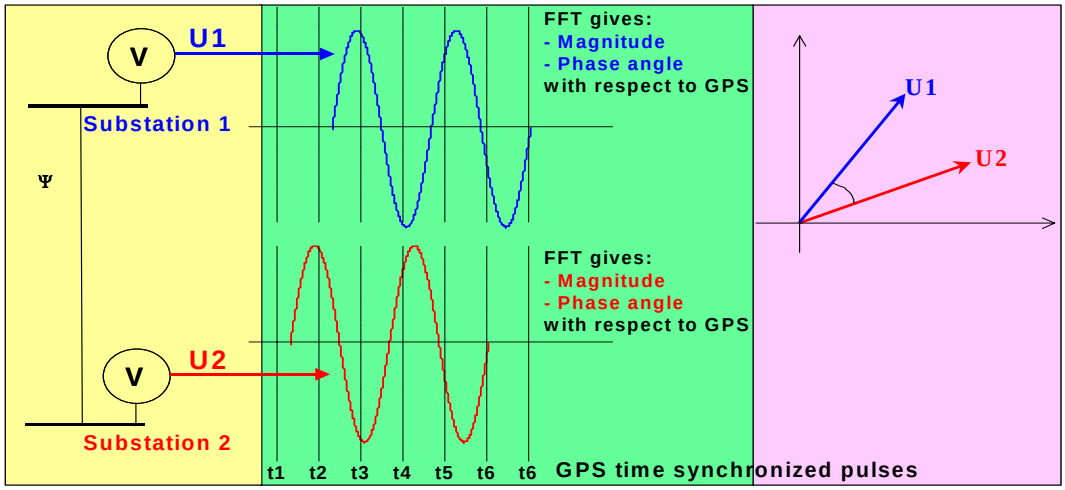


Figure 6.9 Synchronized phasor measurements in different substations

With a number of PMUs in a power system, powerful supervision, monitoring, and control systems can be designed. **Figure 6.10** shows a possible design for such a system. Wide-area schemes based on PMUs are well suited to track the power system dynamics and to react in a coordinated and optimized way [6-11]. As a prerequisite, PMUs must be placed on selected power system busses to provide the observability needed by a given application.

As a general rule, complete system observability will require that around one third of the busses be instrumented. Several PMUs placing techniques have been documented in the recent years to do so [6-12] - [6-15]. Complete observability is needed when full system state estimation is an objective as for the conventional EMS state estimator. Long-term voltage stability applications will also require complete observation of the load flows for deriving the voltage stability margins of a whole system. On the other end, voltage instability detections are often applied to specific heavy loaded regions of a power system thus reducing the number of required PMUs. Observability requirements may also be less demanding where geographic observability based on representative pilot phasors is appropriate. Angular and frequency instability schemes are good candidates for such pilot phasors usage. In this case, one PMU (or the average of a few PMUs) will provide the dynamic behavior of a given area. Such an approach is considerably reducing the number of phasor measuring instruments as well as the associated communication facilities.

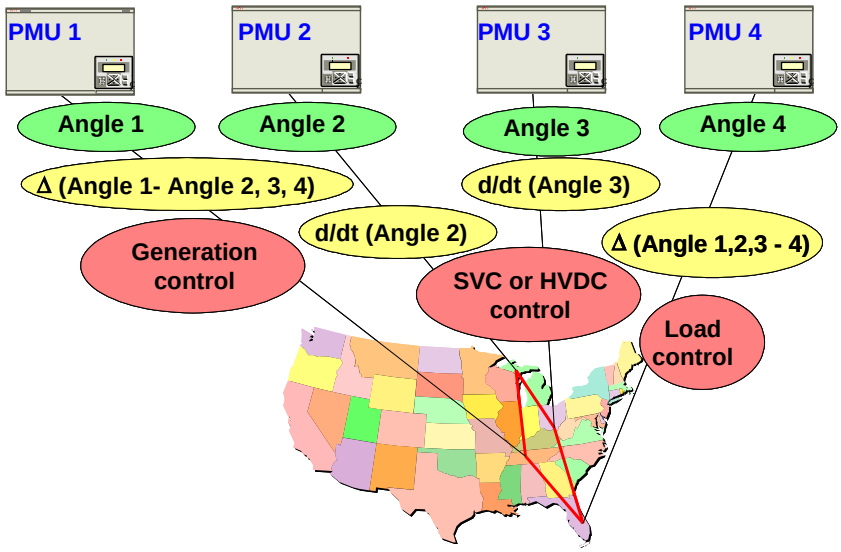


Figure 6.10 Interconnected PMUs for stability control

6.6.1.1 Measuring performance

PMUs accuracy requirements depend on type of applications. The 0.02-degree accuracy of commercial PMUs comes from the use of GPS signal for synchronization and it is not due to any specific application requirement. The time synchronization, required for most power system applications for angle difference information, vary between 10 and 50 microseconds depending on the application.

Data acquisition and signal processing must be accurate and fast enough to meet the requirements of the protection and control loops during steady state as well as disturbed (post contingencies) conditions. Sub- and hyper-synchronous phenomena must therefore be adequately filtered.

PMUs measuring performance is another important issue. Data acquisition and signal processing must be accurate and fast enough to meet the requirements of the protection and control loops during steady state as well as disturbed (post contingencies) conditions. Sub- and hyper-synchronous phenomena must therefore be adequately filtered.

PMUs and communication delays form another important aspect of wide-area protection systems. These delays indicate the viability of a particular communication medium since large communication delays amount to slower protection and controller actions.

PMUs and communication delays mainly comprise of:

Fix delay Tf : *Voltage (PTs) and current (CTs) transducers, analog and digital filtering, DFT window, signal processing, data concentrators, multiplexers*

Propagation delay Tp : *Propagation delay of the link (type of medium and physical distance)*

Data transmission delay Td : *Amount of data to transmit / data rate*

Tf depends on the transducers' accuracy and a typical value for *Tf* is 75 μs. Propagation and data transmission delays are dependant on the communication medium. Propagation *Tp* delays for fiber-optic cables, power lines or telephone lines are typically 25 μs while for LEO satellites they may be as high as 200 μs. Data transmission delays are obtained by dividing the length of the PMU data frame by the communication link data rate.

The IEEE C37.118 "Synchrophasor for Power Systems" standard specifies the data format for the PMUs. The performance of the PMU for off-nominal frequency components, timing errors, and system harmonics need to be examined and accounted for based on the type of application.

Three types of frames are defined within the IEEE C37.118:

- The data frame - Provides information for the phasor data and the state of the digital inputs.
- The header - An ASCII file that contains identification about the PMU, data source, algorithms and the analog filters used
- The configuration frame – A binary file that contains PMU identification code, number of phasors, nominal line frequency and the transmission period of the phasors.

The normal operation of the PMU requires only the transmission of the data frame, the header and configuration frames being only transmitted at equipment startup or upon request.

The data frame length for a typical PMU (12 phasors and 10 digital inputs) is around 680 bits, the header frame 200 bits and the configuration frame 2800 bits. For a worst-case scenario, where the two last frames are regularly transmitted together with the data frame, the *Td* would be around 110 μs on a 33.6 Kbps telephone line channel. The total delay *Tf + Tp + Td* is therefore approximately 210 μs. For fiber optic cables, the data transmission delay is negligible and the total delay is therefore close to 100 μs.

6.6.1.2 Effect of transformer errors on PMUs

The 0.02-degree accuracy given to the PMU by the GPS signals is usually not achievable in practice due mostly to the magnitude and phase errors caused by the instrument transformers used to obtain the signal from the power system. The magnetizing current drawn by the transformer's core and the current drawn by the burden produce an impedance drop across the instrument transformers that results in a magnitude and phase error in the secondary signal compared to that of an ideal transformer. Industry standards set classes for instrument transformers based on the allowed limits in the phase and magnitude errors of the secondary signal.

Testing of the instrument transformers prior to installation can be performed to determine a more accurate phase and magnitude error of each individual transformer that will allow the use of correction factors to reduce the error in the measurements. Unfortunately for installed transformers testing is not possible and the only error information available is obtained from the transformer class limits as set by the existing IEEE and IEC standards.

6.6.2 Telecommunication Infrastructure

One of the vital elements of SPS or RAS design is a reliable and secure communication infrastructure for data exchange amongst monitoring and controlling devices.

Real time data exchanges are used for collecting system state information and for issuing and coordinating control and protection actions. Real time requirements in terms of data type, data throughput, response time are dependent on the nature of the defense functions themselves. For example, angular stability phenomena are imposing stringent requirements in terms of response time and data exchange while voltage stability applications are slower in their dynamics and require lower transfer rates and longer response times.

The telecommunication infrastructure must be designed to fit the various applications supported by the defense plan. In this infrastructure, the communication links will be using different technologies depending on the required performances.

6.6.2.1 Telecommunication technologies:

Many different telecommunication technologies are being used by electrical utilities for monitoring, controlling and protecting their systems. This section will briefly present the available technologies and their main characteristics.

These technologies may be divided in the following categories:

- Pilot wire
- Power line carrier
- Basic telephone lines
- Leased lines
- Microwave radio
- Optical fibers
- Satellite communications

Pilot wire

Pilot wire uses a twisted pair of copper wire in a telephone type cable to directly connect the terminals of a protected line. The communication is either made by DC signaling or voice frequency signaling (by audio tones with frequencies from 200 Hz to 3000 Hz). Pilot wire is mainly used for blocking or tripping type of protection on transmission lines up to 10 miles in length.

Power line carrier

Power line carrier used to operate in on-off mode by transmitting radio frequency signals in the 10 to 500 kHz band over transmission lines. The overhead lines present a low loss media for high frequency carrier. New developments in this field enabled this communication technology to offer data rates in the range of 4 Mbps over medium and low voltage lines. It can be used for wide-area measurement and protection and substation networking. Propagation delays are considerably less than those of pilot circuits.

Basic telephone lines

Standard 2-wire analog telephone lines are a very economical way to transfer data to communicate with remote locations in situations where only occasional data transfers are required. Data rates for modems are typically 56 Kbps or less so that this medium is not suited for transferring large amounts of data. Dial up delay for setting up a call is also an inherent limitation of this technology.

Leased lines

Leased lines are dedicated communication channels carrying data over telephone circuits that have been conditioned for reducing attenuation, envelope delay distortion and noise. Telephone switches are bypassed and the modems are permanently connected to the line. Point to point and multipoint configurations are available. Two wire lines are for half duplex. Four wire circuits are also available to provide full-duplex communication.

Leased lines are either using analog or digital communication. While analog circuit transfer rates will generally be limited to 56 Kbps, digital circuits may rate up to 1.5 Mbps. However, digital communication equipments are significantly more expensive then analog systems.

Microwave radio

Many power systems infrastructures have built their own networks by using high capacity microwave radio systems. These microwave systems can transmit data anywhere from 1.5 Mbps (24 voice lines in the North American Digital Hierarchy) or 2 Mbps (30 voice lines in the European Digital Hierarchy) to hundreds of Mbps (thousand of voice channels) depending on the type of radio equipment used. Owning its own facilities makes the utility control its destiny by maintaining high levels of reliability.

Microwave system requires line of site transmission and often requires tall towers to allow for effective communication. The cost of such a microwave system can be quite high considering the cost of high capacity radio equipment and towers.

Optical fiber

The optical technology has the capability of operating at very high data rates and is suitable for a wide variety of applications. Fiber optic systems can transfer data at a rate of 1.5 Mbps/2Mbps to almost 10 Gbps (100 000 voice channels). The fiber optic cable is quite expensive to install but its enormous capacity makes it possible to utilities to share capacity with other parties.

Two types of cable are generally used, the optical ground wire (OPGW) or the all-dielectric self-supporting (ADSS). The OPGW is a static protection wire containing one or more steel tubes that hold optical fiber and are installed in place of a standard static protection wire on transmission or sub-transmission routes. The **ADSS** contains no metal members and can be installed in the power–space of a distribution route. The fibers are either single mode or multimode. The single mode is the most expensive but provides the highest capacity.

SONET (Synchronous optical network) is the American National Standards Institute standard for synchronous data transmission on optical media. Its international equivalent is synchronous digital hierarchy (SDH). Together, they ensure standards so that digital networks can interconnect internationally and that existing conventional transmission systems can take advantage of optical media through tributary attachments. SONET defines a technology for carrying many signals of different capacities through a synchronous, flexible, optical hierarchy.

Satellite communications*:* Satellites, including GEOs (Geosynchronous Earth Orbit satellites), MEOs (Middle Earth Orbit satellites) and LEOs (Low Earth Orbit satellites) can be utilized for power system communications because of their high reliability and their wide area coverage. The data transfer time delay can be up to 250 ms depending on the distance between the satellites to the surface of the earth. A communication satellite can be described as a microwave relay station. It is used to link two or more ground-based microwave transmitter/receivers, known as earth or ground stations. The satellite receives transmissions on one frequency band (uplink), amplifies the signal and transmits it on another frequency (downlink).

6.6.2.2 Advantages and disadvantages of different telecommunication technologies

A typical utility telecommunication network will make use of a combination of these technologies. Advantages and disadvantages are summarized in **Table 6.1**.

Technology	*Advantages*	*Disadvantages*
Pilot wire	*- Simple, reliable, widely used* *- Low cost*	*- High sensitivity to induced voltages* *Basic signaling functions* *- Short distance* *- Propagation delays*
Power line carrier communication	*- Robust, reliable, economic. High data rates* *- Low loss medium* *- Small propagation delays*	*- Frequency congestion* *- Subject to disturbances during faults in the power lines*
Basic telephone	*- Economical* *- Off the shelf equipment available* *- Line sharing arrangements (voice and data)*	*- Suitable for occasional data transfers* *- Time required for setting up a connection* *- Limited data rates*
Analog leased lines	*- Continuous access* *- Conditioned circuits : low noise, low distortion*	*- Limited data rates (56 Kbps)* *- Priced on a per-month distance sensitive basis*
Digital leased lines	*- Much higher data rates (1.5/2 Mbps) than analog.* *- Greater flexibility, sharing of applications*	*- More expensive equipment*
Microwave radio	*- High capacity (1.5 to hundreds of Mbps)* *- Sharing of multiple applications*	*- High cost of ownership* *- Line of site transmission*
Optical fiber	*- Most versatile technology* *- Extremely high data rates (1.5 Mbps to 10 Gbps)* *- Wide variety of applications* *- Electrically isolated medium* *- Small delays*	*- Higher initial installation costs* *- Overall life cycle benefits are greater* *- Requires care in termination and splicing*
Satellite	*- High data rates* *- Wide area coverage*	*- Large propagation delays (less for LEOs)* *- High cost for permanent connections and / or high bandwidth*

Table 6.1 Telecommunication technologies

6.6.2.3 Telecommunication protocols

A telecommunication protocol is a collection of rules governing the interactions between communicating entities. In a communication system, these entities are processes residing at the nodes of the network. For the electrical utility industry, protocols will support communication within control centers, within substations, between control centers and substations and also for the exchange of trade information.

Protocols are either proprietary or standard. Historically, proprietary protocols were developed because of the lack of standards. In this context, only devices from the same vendor were compatible. Consequently, the need for standardized communication between protection and control devices became obvious in order for utilities to be able to choose several suppliers within an IT infrastructure. Today, well-designed open protocols are available and they provide the following key advantages:

- Open system connectivity
- Supplier independence (interoperability of IEDs)
- More reliable products at optimized costs
- Risk management
- Freely available knowledge and specifications

IEC 60870-5, DNP3.0, Profibus, Modbus, have been extensively used. IEC 61850 is an industry standard protocol to be implemented more often in the near future. All these standards are described in more detail in Appendix 6A.

6.7 CONCLUSIONS AND FUTURE IMPROVEMENTS

As there are no perfect solutions for preventing blackouts, a number of different measures must be implemented to minimize the impact of future disturbances. This chapter emphasizes the need for the design and deployment of a well-defined and coordinated overall plan utilizing wide-area protection and control schemes.

The technological infrastructure for designing a defense plan is already available, in the form of broadband communication networks and high precision real-time monitoring and control devices, such as phasor measurement units, FACTS actuators, etc. This facilitates the emergence of a system-wide protection and control philosophy based on implementation of a well-coordinated defense plan against blackouts.

The actions of existing wide-area protection schemes are either event-based (i.e. certain contingencies act as triggers) or alarm-based (i.e. initiated when certain monitored quantities are out of their allowed ranges). Further improvement can be accomplished by implementing new wide-area defense systems, which can adapt to constantly changing system conditions. Such systems can initiate actions as simple as a transfer trip or as complicated as calculations based on system analysis. The common denominator is information sharing across the network, with the objective being to increase the security of the protection system without degrading its dependability.

New technologies mean that coordinated wide-area defense systems can be cost-effective solutions. Computer relays communicate not only with the control centre, but also with each other. The implementation of an advanced wide-area defense system requires a significant improvement over the existing decentralized systems. Decentralized subsystems will have to utilize advanced algorithms [6-16, [6-17] to make local decisions based on local measurements and/or selected remote information. With a fully developed information interchange and communications infrastructure, it will be possible to link all of the monitoring, control, and protection devices together. The key to a successful solution is rapid detection, fast and powerful control devices, communication systems, and smart algorithms, or in other words, a true Wide-Area Defense System.

6.8 REFERENCES

[6-1] D. Novosel, M. Begovic, V. Madani "Shedding Lights on Blackouts," Power&Energy, Jan/Feb 2004.

[6-2] "Wide Area Protection and Emergency Control", Working Group C-6, System Protection Subcommittee, IEEE PES Power System Relaying Committee, January 2003.

[6-3] S.H. Horowitz and A.G. Phadke, "Boosting Immunity to Blackouts", Power & Energy Magazine, September/October 2003.

[6-4] K. Uhlen et al., "A Probabilistic Security Criterion for Determination of Power Transfer Limits in a Deregulated Environment", 38th Cigre Session 2000, Paper 38-106, Paris, 2000.

[6-5] W. H. Quaintance et al., "Raising Energy Transfer in Corridors Constrained by Voltage Instability – Statnett Case", IEEE PES Summer Meeting 2000.

[6-6] K. Uhlen et al., "Raising Stability Limits in the Nordic Power Transmission System", Proceedings of the 14th Power System Computation Conference (PSCC'02). Sevilla, Spain, 24-28 June 2002.

[6-7] V Madani et al., "Remedial Action Schemes Application and Implementation Requirements", Western Electricity Coordinating Council, October 25, 2001.

[6-8] D. Novosel et al., "Practical Protection and Control Strategies During Large Power-System Disturbances", Proceedings of IEEE 1996 T&D Conference, Sept. 1996, Los Angeles.

[6-9] V. Madani, D. Novosel, A. Apostolov, S. Corsi, "Innovative Solutions for Preventing Wide-Area Disturbance Propagation", International Institute for Research and Education in Power Systems (IREP) Symposium, Cortina d'Ampezzo, Italy, August 2004.

[6-10] V. Madani, J. Law, C. Finn, R. Mansfield, "Deterministic Model for Cold Load Pickup", IEEE Midwest Power Symposium, October 1985.

[6-11] V. Madani "Western Interconnection Experience With Phasor Measurements", IEEE PES Power system Conference and Exposition (PSCE), October 2006.

[6-12] Cho Ki-Seon, Shin Jong-Rin, Ho Hyun Seung, "Optimal Placement of Phasor Measurement Units with GPS Receivers", Power Engineering Society Winter Meeting, 2001 IEEE, Volume: 1 , 28 Jan.-1 Feb. 2001.

[6-13] T.L. Baldwin, L. Mili, M.B Boisen Jr., R. Adapa, "Power System Observability with Minimal Phasor Measurement Placement", IEEE Transactions on Power Systems, Volume 8, Issue 2, May 1993.

[6-14] R.F. Nuqui, A.G. Phadke, "Phasor Measurement Unit Placement Based on Incomplete Observability", Power Engineering Society Summer Meeting, 2002 IEEE, Volume 2, 21-25 July 2002.

[6-15] Kamwa, R. Grondin, "PMU Configuration for System Dynamic Performance Measurement in Large Multi-Area Power Systems", IEEE Transactions on Power Systems, Volume 17, Issue 2, May 2002.

[6-16] D. Julian et al., "Quantifying Proximity to Voltage Collapse Using Voltage Instability Predictor", IEEE Power Engineering Summer Meeting, July 2000.

[6-17] K. Vu, M. Begovic, D. Novosel and M. Saha, "Use of Local Measurements to Estimate Voltage-Stability Margin", Power Industry Computer Applications Conference (PICA), May 1997.

APPENDIX 6.1: IEC-60870-5 PROTOCOL

IEC 60870-5 is successfully used in thousands of installation worldwide. It specifies the transmission protocols for tele-control equipment and systems with coded bit serial data transmission for monitoring and controlling geographically widespread processes. In the electrical power distribution and electricity applications, it is typically used for communication between central control system and substations (RTUs). It is optimized for applications that require short response times in relatively low-speed networks. The IEC 60870-5 specifies master-slave protocol and offer powerful functional enhancements for SCADA systems. Its two main characteristics are the report by exception and time stamping mechanisms. The IEC 60870-5 protocol is generally used for either multiple point-to-point star configuration, star, bus multi-point party-line configuration, or multi-point ring configuration.

DNP, Distributed Network Protocol

The Distributed Network Protocol is an open, public and non-proprietary protocol based on IEC 60870-5 to work within a variety of networks. DNP Version 3.0 was originally designed based on three layers of the OSI seven-layer model: application layer, data link layer and physical layer. The application layer is object-based with objects provided for most generic data formats. The data link layer provides for several methods of retrieving data such as polling for classes and object variations. The physical layer defines a simple RS-232 or RS-485 interface and an Ethernet interface. It was designed for master slave operation such as RTUs and subordinate IEDs over point-to-point links or multi-drop. It can also be implemented in any SCADA system for communications between substation computers, RTUs (Remote Terminal Unit) , IEDs and master stations; over serial or LAN-based systems. DNP is suitable for application in the entire SCADA/EMS environment.

Profibus

This protocol is intended for automation applications that are close to the process and makes simple bus interfaces with real-time behavior possible. This standard allows field automation components of different manufacturers to be interconnected in a distributed system and guarantees reliable communication. Such a system is called an "open system". In addition the Profibus protocol makes possible the easy integration into hierarchically higher automation systems (Manufacturing Automation Protocol, MAP). Thus the interconnection expense is minimized.

Modbus

A master-slave protocol that is popular with industrial users as well as in substations. It issues simple Read/Write commands to addresses inside an IED. Modbus is an application layer messaging protocol positioned at level 7 of the OSI model. It provides client-server communication between devices connected on different types of buses or networks.

IEC 61850, a new standard protocol

More recently, experts from North America and Europe worked on the definition of a new modern and flexible protocol, the IEC 61850, whose objective is to provide a communication system that supports interoperability between the functions to be performed in a substation but residing in equipment (physical devices) from different suppliers. Functional requirements have to be met independently of substation size and operational conditions. The functions of substation automation system are control and supervision, as well as protection and monitoring of the primary equipment and of the grid. Other functions are related to the system itself e.g. supervision of the communication.

In North America, the EPRI UCA (Utility Communication Architecture) project has taken up the cause of interoperable multi-vendor substation communications and control systems, developing the detailed specifications and sponsoring or coordinating demonstration projects. In Europe, the IEC has embarked on a parallel standards project 61850 for data communications systems for substation and protection. The two development teams have committed to develop compatible standards in which the UCA specification is a subset of the more general IEC standards group. This has lead to a single standard communications design approach for all future equipment from around the world. Even though the standard has been derived within the context of the substation environment, it may also be used for:

- Information exchange within the substation
- Substation to substation information exchange

- Substation to control center information exchange
- Distributed automation communication
- Metering communications

IEC 61850 is already being supported by many manufacturers and tested by many utilities. It will certainly become a major protocol in the design of future defense plans.

The UCA and the IEC standards both offer not-to-distant opportunities for synchronized global Ethernet broadcasting with sufficient and reliable bandwidth needed for information exchange within wide area monitoring schemes.

7 DEFENSE PLAN: ENGINEERING, DEVELOPMENT AND IMPLEMENTATION

7.1 INTRODUCTION

Chapter 6 (Figure 6.1) shows the overall structure of a Special Protection System (SPS)[4]: comprising input facilities and status variables, a decision process, and output action orders. Chapter 7 focuses on the architecture and engineering aspects, the application methodology, understanding the complexities and challenges of implementation, telecommunication and bandwidth considerations, various aspects of installation and commission testing, training tools and operational documentations, the use of training simulators and drill scenarios for operator response and system restoration practices, and overall system test plans for routine scheme testing. Various application methodologies using different hardware and non-homogeneous communication media are also presented.

7.2 SYSTEM PARAMETERS

The purpose (intent) of the SPS, RAS, or wide-area protection and control system determines the monitoring quantities and identifies the design limits for which the scheme is expected to function. Many power system values such as flow, voltage profile, and equipment status can be obtained either through dedicated monitoring or for less throughput time sensitive applications, may be derived from the Energy Management Systems (EMS) computations. However, parameters such as conductor rating, frequency response rate, ambient temperature, etc. may need to be identified separately when the information cannot be achieved by power system state calculation.

7.3 EQUIPMENT SPECIFICATION

Below, is a sample listing of input variables for a typical wide-area monitoring, protection and control (WAMPC), SIPS, or remedial action scheme. These variables maybe used for different applications. The variables can be either directly measured, or derived from the measurements by more or less complex algorithms.

Measurement Inputs

Power System Voltages

- Voltage – synchronized to local measurements in the same substation
- Voltage – Wide area synchronized
- Voltage phasors, i.e. magnitude and phase angle

Power System Currents

- Current – synchronized to local measurements in the same substation
- Current – Wide area synchronized
- Current phasors, i.e. magnitude and phase angle

Power System Frequency

- Frequency Measurements

Polarity Reversal

- Impacts telemetry computations and Arming levels - Examples: Substitute breaker for double bus single breaker applications or Main / Aux. bus configuration when a flow may change polarity as a result of switching.

Last Valid State

- For example, telemetry data during loss of communication channel

Control Signals

- Continuous
  - Generator / Synchronous Condenser AVR
  - Generator PSS (Power System Stabilizer)
  - Generator Governor
  - HVDC converters, SVC, FACTS, TCSC, D-VAR, etc., controllers

[4] Also referred to as System Integrity Protection Schemes (SISP)

- Binary
  - Increase/Decrease, according to pre-decided steps
    - Transformer tap-changer
    - Tie-line transfer
    - Reactive power compensation
  - Trip/Close: Circuit-breaker (line disconnect, generator rejection, load shedding, etc.)
  - Relay protection trip order

Status

- Circuit-breaker position
- Tap-changer position
- Generator field current limiter activated
- Generator armature current limiter activated
- Predefined thresholds reached
- Various alarm signals
- Relay protection start signals
- Disturbance recorder start signals

Arming

- Levels
- Nomograms
- Thresholds
- Methods
  - Automatic / Dynamic
  - Manual

In addition to the system requirements, there are hardware specifications for consideration. Based on the scheme complexity, these requirements could be quite extensive and apply both to the substation devices as well as central controller(s) as applicable.

1. Hardware, Basic Design, Application, and Construction

- Front panel interface
- Rating for the CT, PT, Inputs, Outputs Levels
- Continuous and momentary ratings
  - Types of inputs (grouped, individual isolated) – When grouped with a common, how many inputs are grouped together?
  - Methods to receive commands and latching outputs
  - Types of logic and physical outputs
  - Number of logic gates, latches, timers, etc.
- Adaptability to existing configurations - Digital network may not be available at every station
- Forward looking equipment capability – Do not have to change substation device when system requirements change.

2. User logic development tool

- Process speed, throughput time of the device

3. Communications Package

- User settable communication bit error detector
  - Display to view the lost packet – CRC error check viewable
- Retain last value option
  - Topography – point-to-point, multipoint
  - Analog telemetry using messaging network flooding
    - Analog value rate of update and communication
    - Comparison with use of transducer (12 bit resolution, 1 bit for polarity and 11 bits for magnitude)
    - Considerations to minimize potential impact to overall performance due to encryption technology used.
    - Any requirements if switched networks are used

4. **Other Telemetry Measurement Considerations:**

- Digitized vs. Analog and Accuracy – See Appendix 7.1
- Summing networks when summation of load in a given site is of interest
- Ability to override

5. Architecture (Ethernet Application)

- Telemetry Accuracy
- Transmission Speed
- Protocols supported (Modbus, DNP, etc.)
- IEC61850
- Number of user accessible ports for each of the supported protocols
- values

6. Management of messaging (software tools for tracking as it pertains to the substation device)

7 Logic development tools (Analog and status)

- Show demo for how to build a small logic
- Show demo of any on-line and off-line logic troubleshooting tools available

8. Recording and data storage requirements

- Quick restoration after a system event
- Automatic Event Analysis
- Provide event driven maintenance
- Time synchronization
- Types of records with appropriate sampling rate ranges and record length:
  - High-speed and Low-speed abnormal system conditions
- Waveform recording and sampling rates
  - Load profiles
  - Methods to reset
  - Automatic Reset
  - Sequence Count

9. Software Tools

- Availability of the tools as standard package vs. optional item
- Bit Mapping, Logic development, and logic event playback tools
- Identify feature available off-line and those requiring communication with the device
- Automatic event collection from multiple systems - Method event summary is presented (for example, is trigger point highlighted) and sorted amongst multiple events (from same device)

The selection of various equipment, identification of monitoring points, types of alarms and priority classification, various contingencies associated with equipment abnormal conditions, types and availability of real time data, considerations for various categories of inputs and output tests, development of the test scenarios, coupled by provisions for automated testing make such schemes very complex. Furthermore, wide area protection schemes may involve many different entities with different background and practices.

Therefore, it is critical to develop test plans for various stages of implementation, as modifications occur impacting parts of the wide-area schemes, as well as for routine maintenance.

7.3.1 Regulatory Compliance Requirements and Measurements

Within the North America, North American Electric Reliability Council (NERC) has established standards for the SPS (SIPS) or RAS functions. NERC requires that each Regional Council whose members use or are planning to use SIPSs shall have a documented review process to ensure that they comply with national and regional criteria and guides. For example, in the US, SIPSs should comply with the NERC Reliability Standards.

NERC Reliability Standards (Protection and Control section) identify purpose of SIPS:

- To protect against possible cascading outages - The goal of implementation of SIPS is to ensure that the system will retain full functionality during the worst operating conditions for which the SPS was designed
- NERC defines Cascading [7-1] as uncontrolled successive loss of system elements triggered by an incident at any location. Cascading results in widespread electric service interruption, which cannot be restrained from sequentially spreading beyond an area predetermined by appropriate studies.
- When protecting the system from damage, these protection systems should be designed to remove the least amount of equipment from the transmission network
- Should not erroneously operate o cause outages of higher impact than originally designed for.
- Operation should not negatively impact transmission system
- Similar to Protection and Control standards
- Designed to allow equipment maintenance
- A SIPS shall be designed so that cascading transmission outages or system instability do not occur for failure of a single component, of a SIPS, which would result in failure of the SIPS to operate when required
- Reliability Standards also identify redundancy requirements:
- The need for redundancy in SIPS should be based on an evaluation of the system consequences for the failure of the SPS to operate, and the need to maintain overall system reliability

7.3.2 Review Criteria

Some parts of the world, schemes are reviewed by independent groups of experts familiar with SIPS or WAPC schemes. For example, NERC has overview policies for review of SIPS applications and

requires that each Regional Council with NERC to establish and document SIPS applications and coordination with other protection and controls.

The criteria for review of the schemes should be identified within the region. Western Electricity Coordinating Council (WECC) is one of the NERC regions. The WECC compliance standards (based on WECC criteria) [7-2, [7-3] list the following types of schemes should be reviewed by an independent committee.

Impact to Reliability:

- Schemes for which failure would result in bulk transmission system performance in a neighboring utility outside the limits of the performance requirements;
- Schemes for which failure may result in unacceptable bulk transmission system performance within the scheme owner's system may be reviewed at the request of the owner of the scheme or as deemed necessary by other Regional technical committees;

Before the scheme is initially put into service to identify how to handle emergency situations;

- Before significant modifications or extensions are made;
- If modification involves new system planning studies;
- When new input or output locations are to be added;
- When a major component or system architecture change is required;
- If an owner is not sure whether a change is significant;

In the event of scheme failure;

- Any accidental or unintended operation that do not meet expected performance levels, or when a failure or false operation causes voltage collapse or cascading;
- The failure is considered credible until the owners of the facilities have demonstrated that the cause of the failure has been corrected and it is no longer credible.

Every five years, the review will consist of receipt of confirmation from the scheme owner of no significant modifications or failures of the scheme. The design of existing schemes will not be subject to further review if there have not been significant modifications or failures.

NERC also has reliability standards and measures for bulk power systems. Parts of these standards relate to reliability, maintenance, and coordination of various types of protective schemes that may impact the power system balance operation [7-4]

7.4 TELECOMMUNICATION REQUIREMENTS

7.4.1 Communication Design and Availability Considerations

When designing a RAS or defense plan, the overall communications system performance including circuit or path quality in terms of availability are key factors. Also, critical is employing a concept to allow the availability to be measured in order to minimize downtimes and improve performance. Some typical measures are listed in parts of the North America. For example, availability of 99.95% is listed as a consideration in WECC [7-2, [7-5].

Telecommunication reliability information should be the average overall percentage, and not point-to-point information.

7.4.2 Use of Wire and Point of Entrance to The Substation

Another factor in design of the communication circuits is the provisions for the appropriate high voltage entrance protection when wire is used.

7.4.3 Use of Ethernet

When using non-deterministic communication systems used (such as Ethernet), the performance of systems should be carefully examined to make sure the scheme is not affected due to frequent maintenance (for example, weekly upgrade patches for cyber security enhancements) or during a

crucial moment when the scheme is being relied upon. Concepts such as V-LAN allow a direct or managed use of Ethernet.

If SIPS or RAS performance is dependent upon successful operation through a non-deterministic communications system or path, then the project team will need to identify how timing and latency issues will be addressed and verified. For example, timing and latency planning or management and verification for initial commissioning and in the event of network modifications or additions.

7.4.4 Communication Design and Ownership

Use of graphical displays or diagrams for each telecom path used in the defense schemes is extremely helpful. The diagrams should reflect the ownership of the circuit paths, and segments between different systems and the maintenance responsibility. Maintenance agreements and response commitments should be clear, for the respective network administrators of each of the systems, when multiple private systems are involved.

During initial stages of engineering, it is helpful to describe and list telecommunications media and electronic equipment (e.g.., microwave radio, fiber optic cable, multiplex node, power line carrier, wire pair, etc.) including redundancy employed in each telecom path. For each of the paths and segments of the RAS, identify the type of telecom equipment employed. For example, whether analog or digital licensed microwave radio, unlicensed spread spectrum radio, fiber optic SONET node, etc. are applied,

Common facilities used for components of defense plans telecommunication path and segment should be examined. There may be common mode elements that are not specifically excluded from redundancy by the local government or a reliability council. For example, in WECC critical communication circuit design guideline provides a list of possible common mode elements that may be considered in engineering (e.g. towers, generators, batteries), [7-5]. Identify paths or segments routed through common equipment chassis such as Digital Cross-connect System, SONET node, or router. Identify physical media carried or supported by the same structure, such as a transmission line tower, pole structure, or duct bank. Discuss outside plant and inside plant routing diversity.

When public network is used, sufficient and easily accessible documentation about monitoring and maintenance agreements including repair response, details of availability, and how possible change of ownership (of the network carrier) are addressed would be useful. When the public network is changing ownership in part of the defense scheme, the impacted portion (company where the affected scheme is operated from) should also notify the neighboring systems, or control areas as appropriate.

For redundant schemes, documentation about the extent of redundancy employed would be very useful for future reference, maintenance and troubleshooting.

7.5 BREAKER FAILURE INITIATION AND APPLICATION

When designing a defense plan that involves many substations and breaker terminals, it is possible that not all exiting breakers part of the tripping, or shedding, are equipped with multiple independent trip coils. Therefore, parts of the overall scheme may rely on use of breaker failure.

Application of breaker failure for WAPC type schemes should be viewed as both the consequence for a breaker that fails to open as well as the system impact if breaker failure operation in a given station during an action called by the WAPC. Since the WAPC schemes are designed to perform during system disturbances, a breaker may be exposed to very high currents during interruption for a disturbance or system swing, and not initiating breaker failure may cause significant equipment damage.

Some of the application and setting considerations for breaker failure include:

- Installation of a dedicated breaker failure for RAS or WAPC (independent of the breaker failure for equipment protection; e.g. line protection).
- Incorporating the logic for breaker failure initiation into the RAS or WAPC device. For example, the breaker failure initiation (contact closure) based on the WAPC system may not need to be as fast as breaker failure initiation for fault clearing. Conversely, line fault clearing and associated breaker failure activation may be slower than breaker failure initiation due to a RAS or WAPC scheme operation.
- In the case of multi-function devices, share the breaker failure device for normal breaker failure function as well as for the RAS or WAPC by programming different elements,

and set points. A note of caution; design should provide flexibility such that maintenance can be performed on the breaker failure device while keeping the overall intent of the defense plan in service.

7.6 TYPES OF TESTS WHEN FOR IMPLEMENTING A DEFENSE OR REMEDIAL ACTION SCHEME

The ultimate success of the implementation solution depends on a proper testing plan. Each application would need to be evaluated on a case-by-case basis. The complexity of the scheme, its purpose, space availability, and other factors may drive some of the decisions associated with the architecture for the scheme applied and the levels of tests to be performed. A proper test plan should include:

- Lab testing for proof of concept of the initial architecture plans and subsequent major changes such as overall performance requirements.
- Field-testing
- Study validation
- Commissioning Testing
- Automatic and manual periodic testing
- Detailed test plans for scheduled system wide testing
- Intelligent or Automatic Maintenance Testing of the entire scheme

7.7 LAB TESTING - OVERALL CONCEPT

Prior to the implementation of a design concept, lab testing is practiced to prove the concept. Lab testing is designed to validate the overall scheme in a controlled environment. Lab tests permit controlled inputs from numerous sources with frequent checks of the output at every stage of the testing process. The lab tests ensure that the desired results are accomplished in the lab environment in contrast to costly and time-consuming field debugging.

For example, in a group of three SPS devices, a lab test could be simulated to check wide-area communications (fiber / copper, Ethernet), average message delivery and return time, unreturned messages count and CRC failure count (under simulated noise conditions), and back-up communication switching timings. **Figure 7.1** shows a lab set-up for a redundant WAPC scheme as system A and System B where systems “A” and “B” substation devices are not the same style.

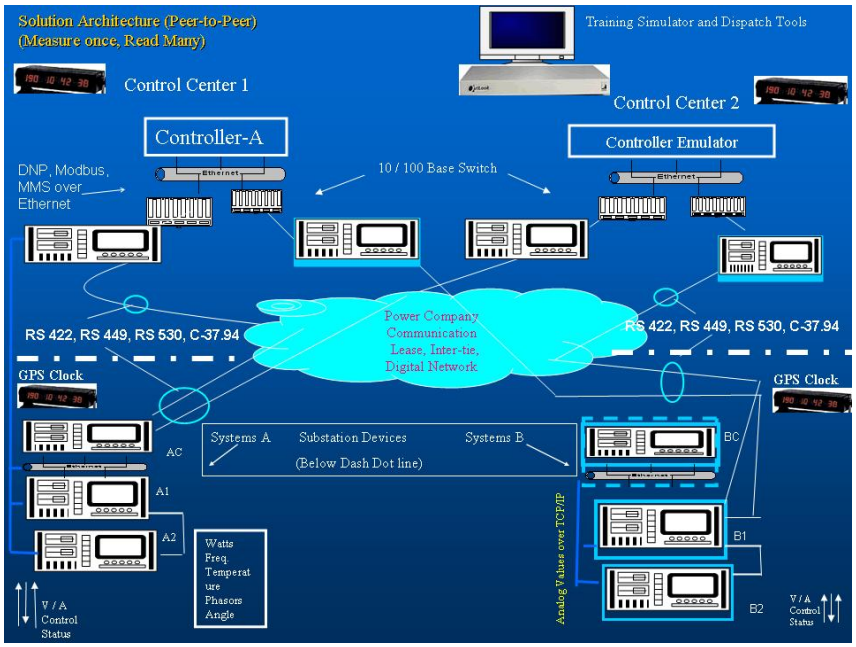


Figure 7.1 – Example of proof-of-concept Test Set-up for a Redundant Scheme

In **Figure 7.1**, the central controllers are not at the same location. For proof of concept, only one controller is available. In case of System "A", communication to the central locations is managed through the "AC" chassis. In System "B", communication to central locations is through the "B1" chassis, with chassis "BC" providing a local function such as a data concentrator.

7.8 FIELD COMMISSIONING TESTS

Field commissioning tests should be carried out to check the performance of the special protection scheme against the real world abnormal system conditions. The telemetry data and the dynamics of various power system configurations such as breaker close and bypass contacts, changing the selectivity of the current transformer inputs, the total trip timing over the implemented communications between devices and the central control station, and the possible scenarios of unavailability of devices at the time of execution of a command signal in a given station all need to be tested. In general, every input point and every logic condition needs to be validated against expected results. Additionally, the effect of DC transients on line outage should be tested thoroughly in the field before placing the scheme into service.

It is a good practice to prepare a comprehensive list of tests and commissioning procedures. This document will help address multiple purposes. For example:

- Consistency in tests performed at different stations and by different project teams
- Investigations when a section of the scheme not works properly during performance testing or after scheme is in service.
- Identifies the types of tests performed prior to placing the scheme in service. As portions of the scheme are modified due to expansions at a substation, the list can serve as a roadmap for the new project team.

For schemes involving multiple systems, the various components are tested similarly amongst participants.

7.9 SYSTEM PERFORMANCE TESTING

Proper implementation requires a well-defined and coordinated test plan for performance evaluation of the overall system during agreed upon maintenance intervals. The maintenance test plan, also referred to as functional system testing, should include inputs, outputs, communication, logic, and throughput

timing tests. The functional tests are generally not component level testing rather overall system testing. Some of the input tests may need to be done ahead of overall system testing, to the extent that the tests affect the overall performance.

The concept is to validate the overall performance of the scheme including the logic where applicable, to validate the overall throughput times against system modeling for different types of contingencies, and to verify scheme performance, as well as the inputs and out puts. Maintenance engineers should have a library of system-wide test cases.

For example, for each operating contingency, the tests should assure:

- *Proper detection by the under-voltage, under-frequency, or outage detection devices*
- *Successful communications to the central system controllers and proper identification of the inputs received*
- *Proper processing of information*
- *Execution of the needed action*
- *Completion of the action at the substation*
- *Validation of the throughput timing*
- *Verification of breaker failure schemes*
- *Verification of the block auto-reclosing*
- *Analysis of the sequence-of-event (SOE) information*
- *Use of state estimator to generate pre-outage conditions to restoration test scenarios*

The outcome of these tests should be reported back to engineering staff for coordination during planning, operation, and protection study intervals.

7.9.1 Design and Implementation Standards

The following definition of a system protection system comes from a NERC reliability standard [7-4].

"A system protection system (SPS) or remedial action scheme (RAS) is designed to detect abnormal system conditions and take pre-planned, corrective action (other than the isolation of faulted elements) to provide acceptable system performance". Note that this definition specifically excludes the performance of protective systems to detect faults or remove faulted elements. It is system oriented both in its inception and in its corrective action. Such action includes, among others, changes in demand (e.g. load shedding), changes in generation or system configuration to maintain system stability or integrity and specific actions to maintain or restore acceptable voltage levels. One design parameter that sets these schemes apart is the "arming" and "disarming" levels in response to system conditions. For example, a watchdog type of scheme may be required. Some SPSs are armed automatically by the system control center computers, while others require human operator action or approval, and some are armed all the time.

Figure 7.2 is a simplified representation of part of a defense plan or RAS where line undercurrent is used to detect line outages. For simplification, the one line does not show the details such as series compensation or the number of capacitor segments, line reactors, or the secondary side of the transmission transformers. Very often, the scheme entails monitoring the low and high side of transformers as well as monitoring the underlying system on the secondary side of the transmission transformers. Likewise, depending on the type of disturbance, actions may include bypass of the series capacitors, insertion of reactors, or insertion of mechanically switched shunt capacitors.

In **Figure 7.2** example, the redundancy for the undercurrent is at the remote substation and both ends send their respective information to the redundant controllers shown on **Figures 7.3** and **7.4**. Also, considerations are given in the design to allow proper isolation of the inputs, outputs at the substation and at the controller locations to facilitate troubleshooting or provide mechanisms for testing as appropriate.

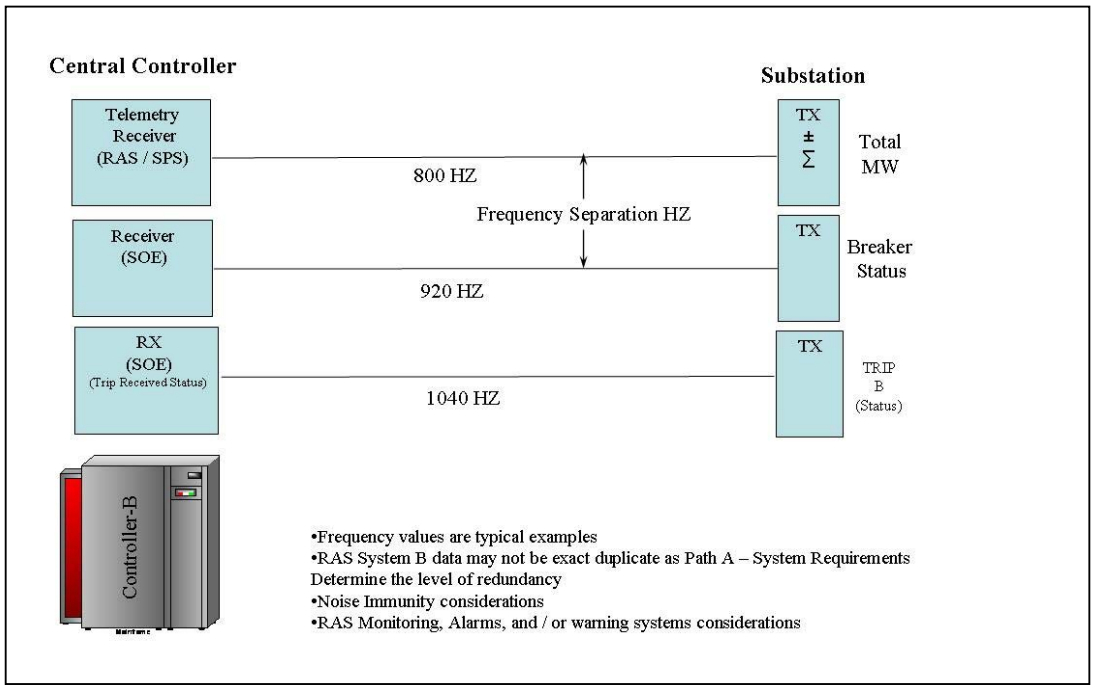


Figure 7.2 - Typical Line Monitoring Scheme

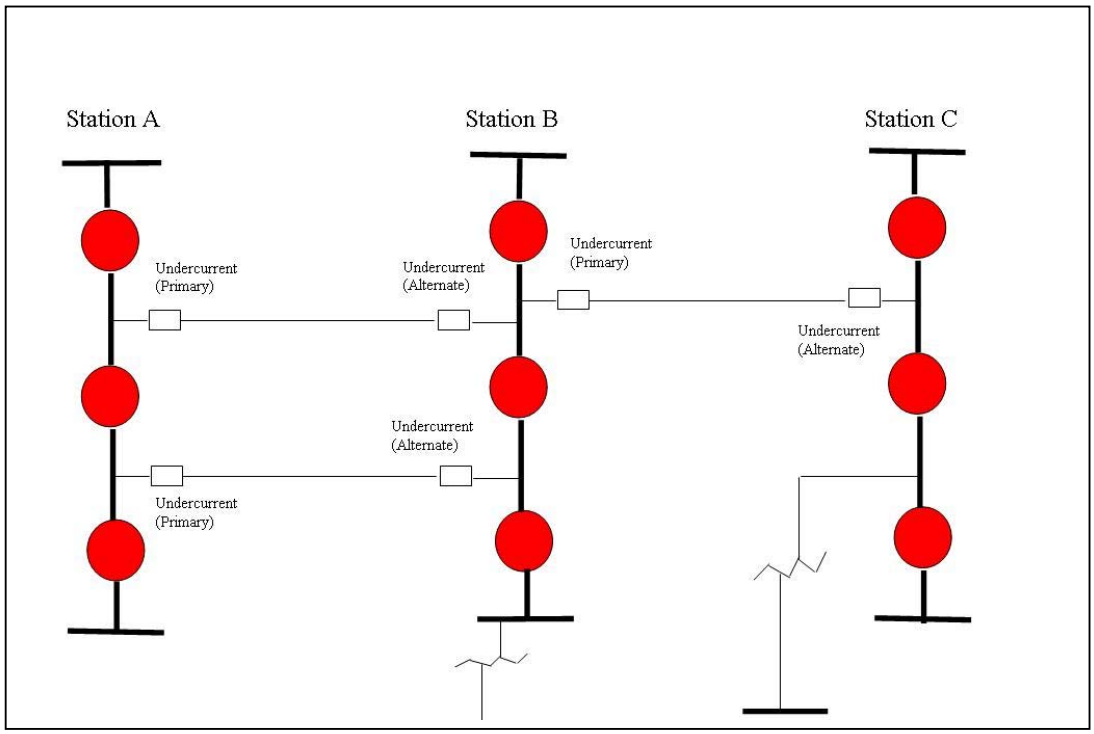


Figure 7.3 - Typical Telemetry and Status Points for One Path (e.g. Path A) of a Redundant System with Audio-Tone communication

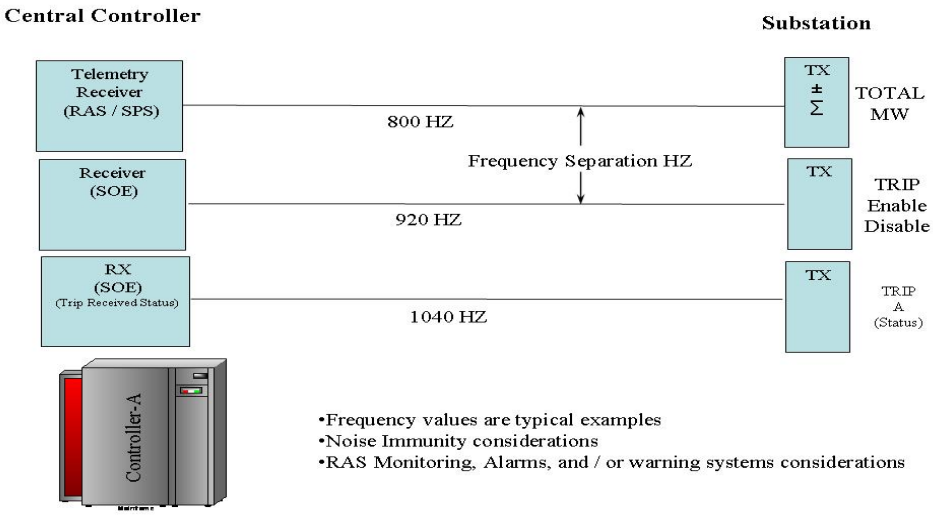


Figure 7.4 - Typical Telemetry and Status Points for Path B of a Redundant System with Audio-Tone communication

Figure 7.5 shows a typical architecture for a wide-area scheme. Depending on the intent of the scheme, several control areas or systems may be interconnected. Again, the test coordinator or coordinators need to have full knowledge of the intent of the scheme, isolation points, simulation scenarios, and restoration to normal procedures.

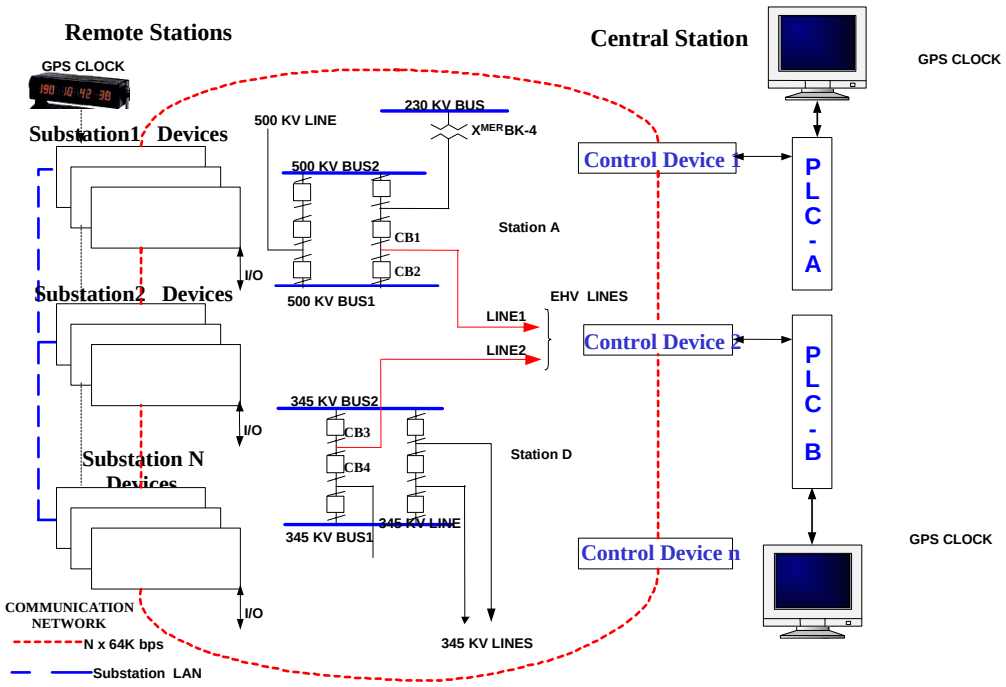


Figure 7.5 - Physical Architecture of a Redundant Wide-Area or RAS

7.10 VALIDATION TESTS THROUGH STATE ESTIMATION

A critical consideration in implementing wide area monitoring and control schemes is the development of automated test scenarios. Such test cases could be prepared based on the type and the intended application of the scheme, and should include provisions for ease of updating case studies as system conditions change.

Implementation of overall system performance tests, automated and intelligent system testing, needs a well developed test plans for such tests. These tests may require the scheme to be unavailable during tests while the redundant system continues to provide the safety net, RAS, or SPS function.

The overall system testing may include electrical supervisory provisions from a central dispatch for added security. Some key elements of test setup include:

- Test Units Connectivity to the Devices with communication interface for communicating with the Field Devices
- Supervisory Process (Dispatch Permission)
- Test Signal (Test person)
- Frequency, Voltage and other power system conditions that need to be simulated
- Outages (Input Test)
- Trips (Output Tests)
- Enable / Disable Functions of the field devices
- Automatic restoration enable / disable
- Functional Tests
- Overall Timing Results

Figure 7.6 shows an example of simulator system setup for testing of RAS controller A. Once overall performance tests for various scenarios are completed on one system, the simulator can be utilized for the redundant system (B) performance testing. Other test methods are possible. For example, once a particular scenario is completed on system A, the test coordinators repeat the test on system B to compare performance between the two systems and administer any corrective actions.

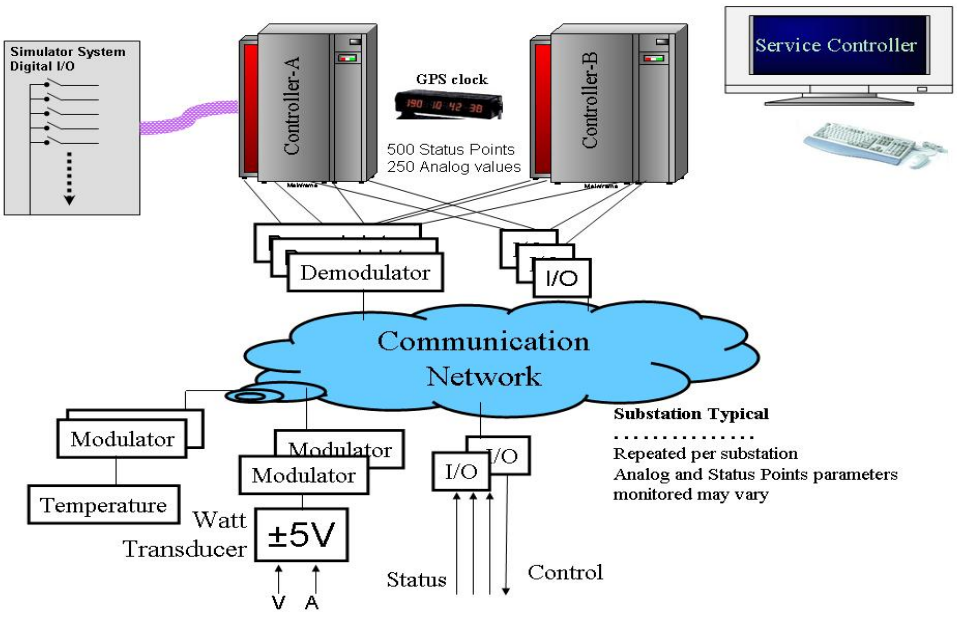


Figure 7.6 - Setup for Performance Testing of a Redundant Wide-Area, RAS, or SPS

The overall functionality of the SPSs should be validated against the system studies. The total throughput of the system during commissioning and scenario testing stages, should measure significantly less than the throughput time identified in systems studies to allow for system changes and in case other stringent contingencies are identified in the future.

It is advisable to create a detailed test plan as part of the overall implementation. A combination of the Logical Architecture, Logic Design, and the Physical Architecture could be used in preparation of the test plan.

For schemes that involve transmission constraints and stability limits, data from the state estimator can be used to determine different pre-outage flows within the power grid.

The pre-outage flows are loaded into the controller as pre-contingency conditions. The controller, or simulator portion of the controller, would then be programmed for various outage, underfrequency, and / or undervoltage status scenarios to perform overall system performance evaluation.

State Estimator data could also be used to develop case scenarios representing future flows and load patterns for further system performance evaluations or to make adjustments where necessary.

7.11 PERIODIC TESTING (INPUT/OUTPUT)

A proper test plan to simulate line outage on the monitored transmission/distribution lines in the respective substations and tripping of the lines should be conducted on a periodic basis to test the contingency plans and as a learning curve for the better understanding of the SPS application.

This test should be conducted without disabling any inputs. Only trip output contacts or auxiliary tripping devices are disabled opening (isolating) the trip or possibly the close path (in case of capacitor bypass or reactive insertion).

Technology advancement in communication and computers has provided opportunities to simplify implementation of wide-area protection and control systems. Computer based devices can

communicate power system information both with central controllers as well as with each other. This, in turn facilitates the deployment of overall system-wide protection and control schemes. With an information infrastructure, it is possible to connect all the monitoring, control and protection devices together through an information network.

Some key indicators to a successful solution are fast detection, fast and powerful control devices, high-speed reliable communication infrastructures, and smart algorithms.

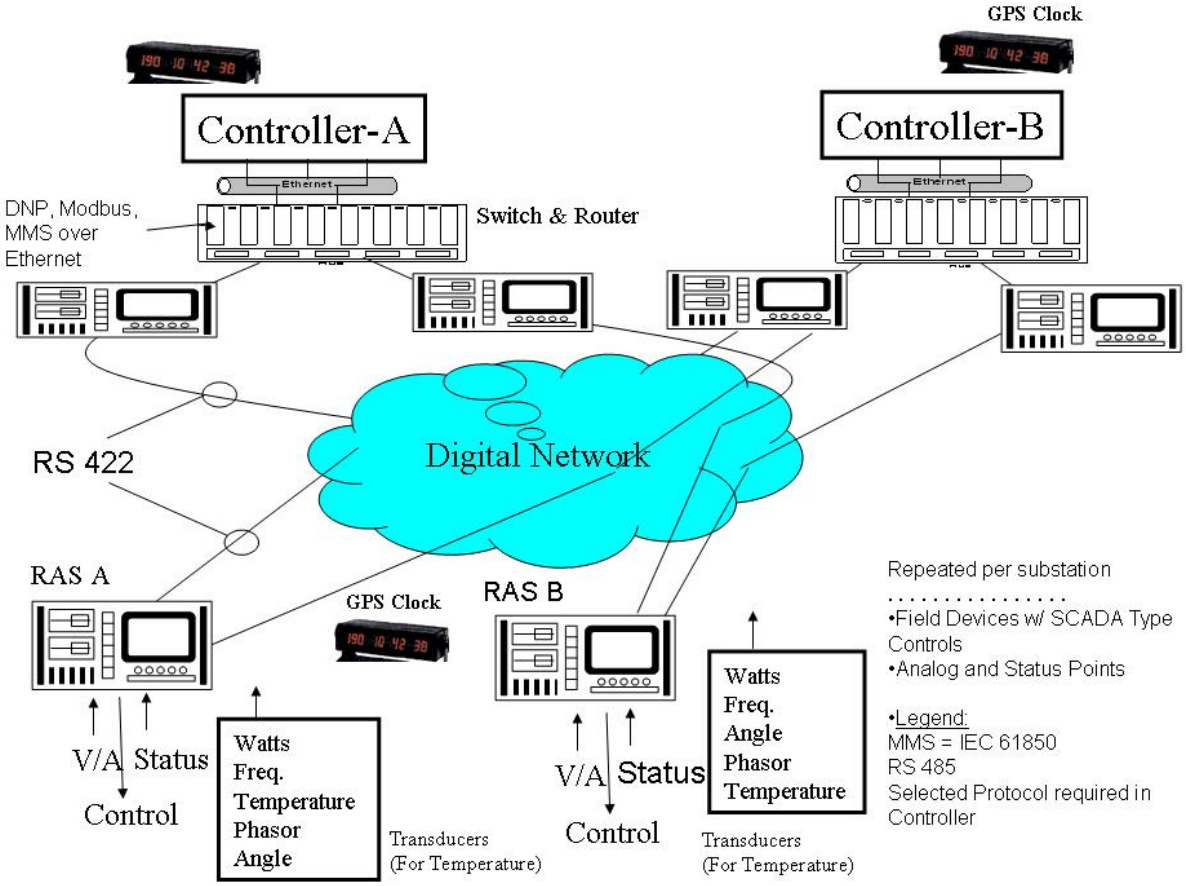


Figure 7.7 Redundant SPS or RAS System with Central Controllers at Different Physical Locations Using Peer-to-Peer Connectivity

Figure 7.8 shows the test setup for performing overall system testing (Design Validation). In this configuration network (Ethernet) use is limited to local stations, where test simulations are routed to the devices that communicate the test scenarios to the substation devices through digital network, peer-to-peer connections at DS0 (e.g. RS 422 at 64 or 128kbs) level.

In reality, open protocol (e.g. IEC-61850) could be used to perform the entire schemes if the scheme is designed the same way.

The key consideration in overall systematic testing is to verify as much of the hardware and software elements (design, application, programming, telecommunication, etc.) from the system that would be used when the scheme is in service and operational.

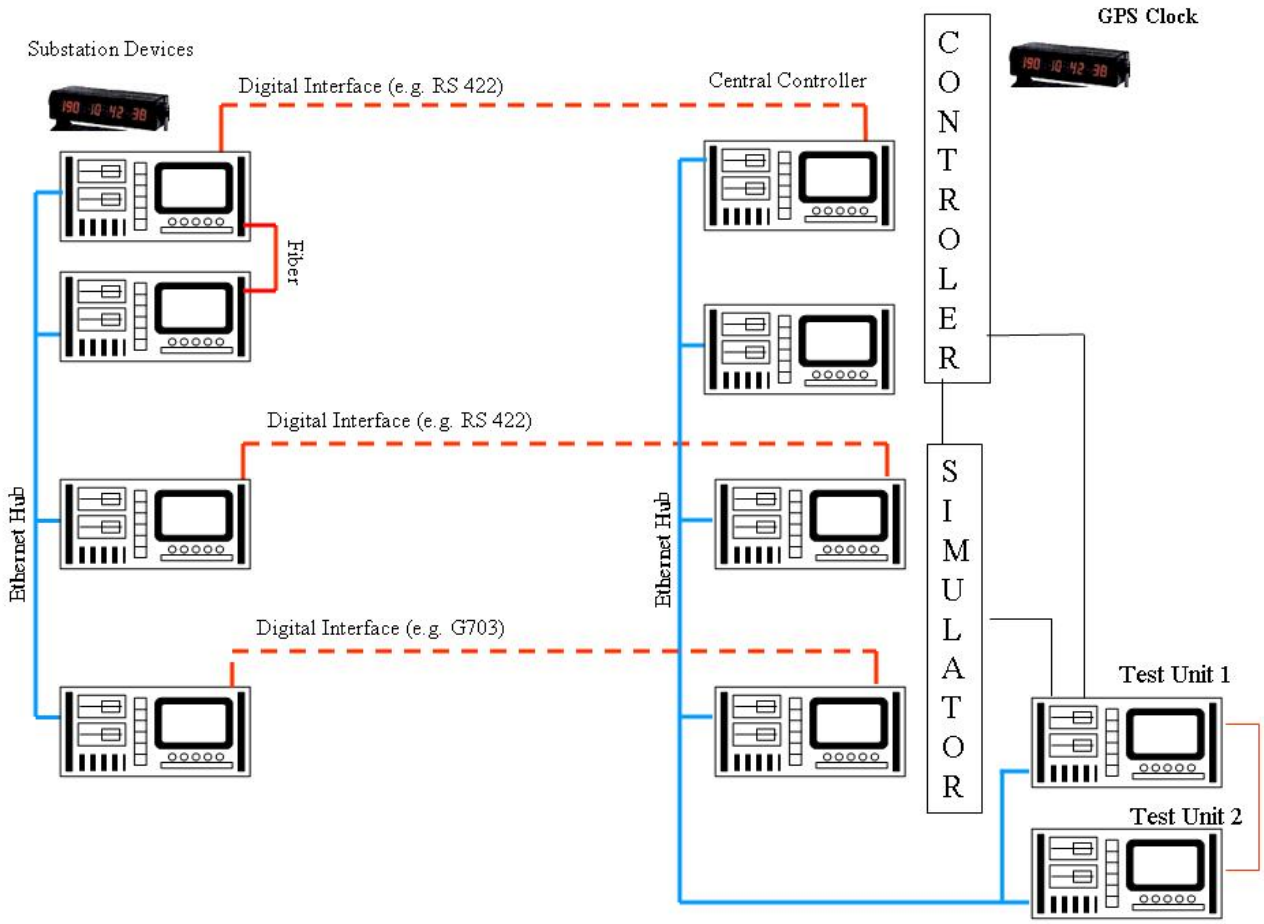


Figure 7.8 – Typical Test Setup for Overall Performance Testing and Throughput Timing Measurements - Test Units and Simulator Connected to the Controllers

7.12 ETHERNET BASED SCHEMES AND TESTING

High Speed Ethernet and latest protocol standards such as DNP and / or the IEC 61850 support a new generation of devices at the substation and at controller locations. **Figure 7.9** shows a combination of analog Ethernet and DS0, or peer-to-peer communication, for status and command purposes. The analog data may be updated at a rate of 4 times per second (250 milliseconds), and the digital status points are delayed only by the channel propagation time.

As there are concerns with network congestion and other factors, there are technologies such as V-LAN that provide a more direct communication channel for telemetry. Also, as these schemes require highly secure paths and are for mission critical applications, there are often discussions on whether a dedicated network is warranted. Some installed based systems in North America make use of a dedicated network as opposed to the system corporate network.

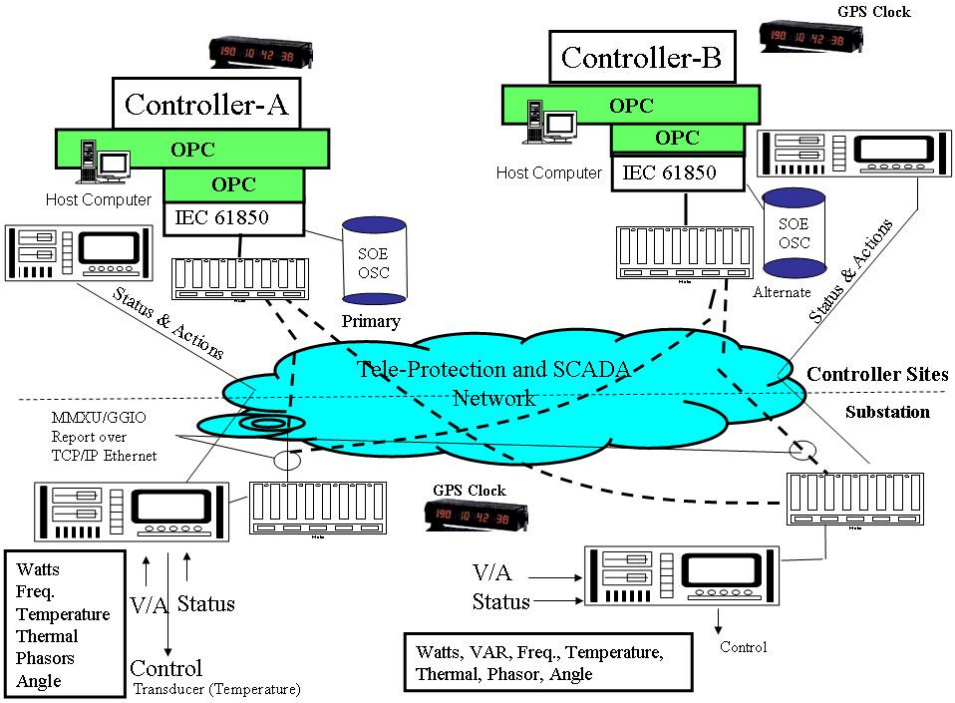


Figure 7.9 Ethernet Based Wide-Area Protection and Control Scheme
Refer to Appendix 7.2 for additional examples

7.13 PERSONNEL TRAINING

The successful design and implementation of a defense plan based on Special Protection Scheme is highly depending on both the expertise and the specific training of the engineering team involved with the project.

The following design aspects shall be duly covered by the expertise of the engineering team:

- Power system protection
- Power system SCADA
- Compliance with EMC requirements for HV plants
- Telecommunication media and electronic equipment
- Project management might also be an important subject where several agents are involved in the project (suppliers, contractors and different utilities).

In addition, the scope of supply shall include specific training modules for the engineering team, such as:

- Hardware application (CPU and interfaces)
- Communication package
- Logic development tools

Another important training module shall be provided in the scope of supply to cover the basic maintenance procedures.

7.14 CONCLUSIONS AND RECOMMENDATIONS

Chapters 6 and 7 provide a comprehensive review of the many considerations and elements of defense plans, from conceptual ideas to various components, including engineering, design, documentation, training and drill scenarios, to procedures for smart restoration and systematic maintenance tests. Various stages of implementation tests and overall performance tests are described, with examples that assist interested readers with recommendations for proper application and successful projects. Defense plans often address extreme contingencies, and therefore, they do not operate frequently. In light of this, systematic tests over the life cycle of the plan are required to maintain the knowledge that is necessary in order to make use of such schemes, and to accommodate continued system and scheme expansions when necessary.

Detailed step-by-step test procedures [7-2], [7-6] that help both field and central controller personnel during routine tests are also recommended. These test procedures are best developed during commissioning tests, while resources are located at various field locations and are able to verify the contents as well as the results.

The recommended frequency for overall system tests is every 12-18 months. Increased time intervals may seem attractive in terms of reducing maintenance costs, but the benefits of such tests over the life cycle outweigh the costs of frequent system tests. Not only do these tests provide performance evaluations as power systems expand and conditions change, but they are also excellent transitional opportunities for knowledge to be transferred to the new people who will become responsible for maintenance, operation, and investigative reports. These tests also provide good baseline knowledge in the event that the scheme requires modifications, upgrades or expansion. Today's technology allows automated scheduled system testing that minimizes resource time for tests while allowing the knowledge to be gained or transferred when such tests are built-in to the original architecture.

With respect to the systematic tests, one approach that is used by power transmission system professionals who are responsible for maintenance is to examine portions of the scheme that may have operated properly during the 4-6 months prior to the overall interval tests, and then determine whether postponement of testing on those portions that have operated successfully is warranted.

7.15 REFERENCES

[7-1] NERC Reliability Standards for the Bulk Electric Systems of North America, "www.nerc.com"

[7-2] V. Madani et al - WECC, Remedial Action Scheme Reliability Subcommittee; "*Information Required to Assess the Reliability of a RAS"*

[7-3] V. Madani, WECC "Remedial Action Schemes Application and Implementation Requirements & Performance Assessment Measures", October 2001

[7-4] NERC Reliability Standards, Protection and Control section.

[7-5] A. Badella et al - WECC, "Communications System Performance Guide for Protective Relaying Applications", 2006

[7-6] V. Madani, D. Novosel, A. Apostolov, S. Corsi "Innovative Solutions for Preventing Wide Area Disturbance Propagation", IEEE 2004 General Meeting, Blackouts Panel Session, Denver, June 2004

APPENDIX 7.1: DIGITIZED TELEMETRY AND ACCURACY CONSIDERATIONS

When using digitized power system parameters, resolution should be considered. Also, polarity (sign) may need to be considered depending on the type of telemetry monitored and the scheme design for the current transformer (CT) having polarity reversal capability such as in a double bus single breaker schemes when either of the busses can be used as transfer bus based on different switching configurations.

Examples of digitized resolution for 8 bits and 16bits are

8 bits [7 bits + sign] (1 out of 128)

16 bits [15 bits + sign] (1 out of 32,768)

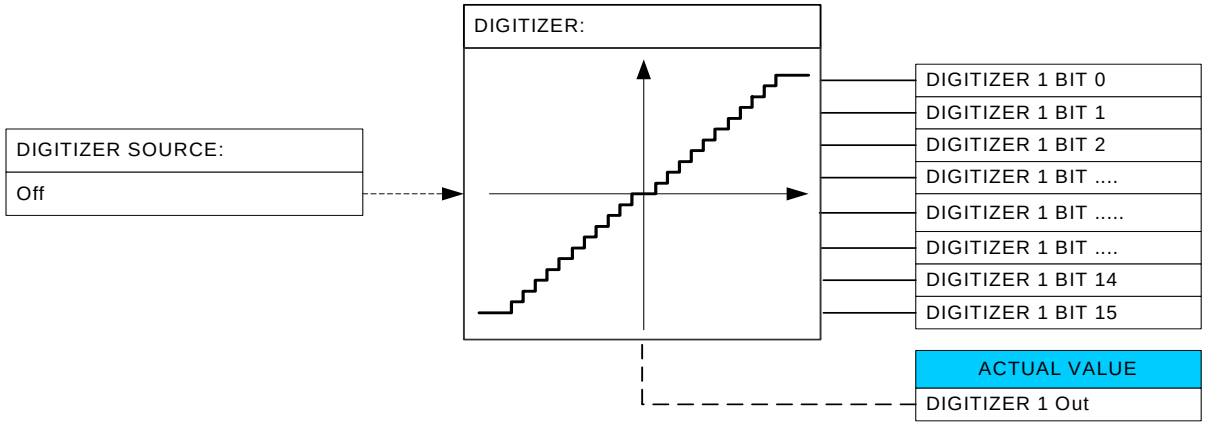


Figure A7.1 – Example of A/D and D/A - Digitization and Accuracy

APPENDIX 7.2: EXAMPLE OF OVERLOAD SPS APPLICATION AND TESTING

Figure A7.2 shows an overload scheme applied to meshed bulk power system. When a single line suddenly becomes unavailable during peak periods, the remaining line would become overloaded. The line outage detection scheme would detect the stressed system conditions and execute corrective actions. The corrective actions include balance of load and generation flows and may include automatic generation run back at the source side, and increasing generations and / or shedding loads & pumped storage generators at the remote end to balance the system before equipment are damaged.

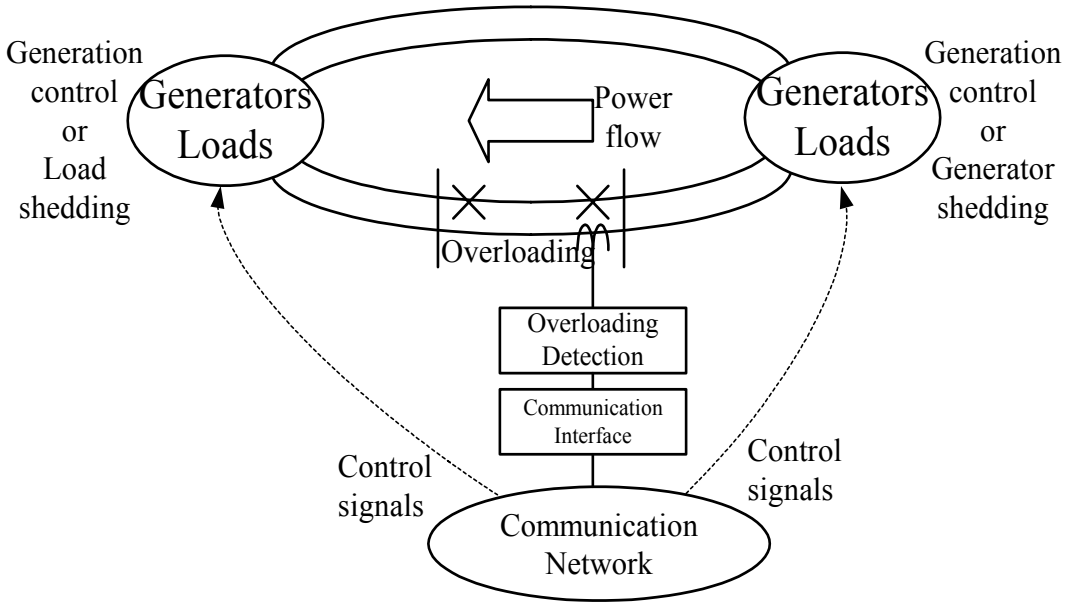


Figure A7.2 – Example of Overload Scheme

For adaptive load mitigation schemes, the system may be partially adjusted by initially activating pump load separation for example, followed by a second computation of system conditions before executing further actions. For such adaptive schemes, the corrective actions continue to be executed until the congestions are mitigated and system is relieved. More intelligent application like Optimal Power Flow (refer to Chapter 2) to the control center would be possible to calculate the amount of appropriate control actions.

The arming of such schemes will determine the mode of operation for the scheme and whether the system adjustments need to be immediate or the conditions support gradual balancing of load and generation.

Communication networks utilized may be a combination of audio-tone or digital connectivity so long at it meets the overall throughput requirements. The level of redundancy is based on the scheme criticality, the possibility for other mitigation measures such as operator ramp down reaction time, or the frequency for being in a condition that the scheme performance is depended on.

To test the overall performance of such schemes, the tests should include different modes of operation; i.e. adaptive or all at once actions. Tests should cover the overall performance for example as a result of communication loss.

8 FUTURE DIRECTIONS IN POWER SYSTEM DEFENSE STRATEGIES

8.1 FUTURE ENVIRONMENT

8.1.1 The Evolving Power Industry Environment

The North American power network may realistically be considered the largest machine in the world. Its transmission lines connect all the electric generation and distribution on the continent. But this network was developed over 100 years without a conscious awareness or analysis of the system-wide implications of its current evolution under the forces of deregulation, the digital economy, and interaction with other infrastructures. Only recently has the possibility of power delivery beyond neighboring areas become a key design and engineering consideration, yet the existing grid is being required to handle a growing volume and variety of long-distance bulk power transfers. Grid congestion and atypical power flows are increasing, while customer expectations of reliability are rising to meet the needs of a pervasively digital world.

The occurrence of several cascading failures in the past 40 years has helped focus attention on the need to understand the complex phenomena associated with the interconnected systems. Widespread outages and huge price spikes during the last several years have raised public concern about grid reliability at the national level. According to data from the North American Electric Reliability Council (NERC), outages from 1984 to the present affected nearly 700,000 customers annually, with smaller outages occurring much more frequently (affecting tens to hundreds of thousand of customers every few weeks or months), larger outages occurring every 2 to 9 years and affecting millions, and much larger outages affecting 7 million customers per decade along with major disasters and their corresponding cost (**Figure 8.1**). Some references concerning major blackouts in North America are provided in [8-1] to [8-5].

The effects of deregulation and economic factors and the impact of policies and human performance must be considered as well. The electric power grid was historically operated by separate utilities, each independent in its own control area and regulated by local bodies to deliver bulk power from generation to load areas reliably and economically. Power grids must work economically to:

- acquire power from low-cost producers and
- deliver power to the loads at the lowest cost.

Competition and deregulation have created multiple energy producers who must share the same regulated energy distribution network—such that this network now lacks the carrying capacity or safety margin to support the anticipated demand. In the U.S. electrical grid, investments in maintenance and R&D have continued to decline, as shown in **Figures 8.2** and **8.3**. Similar trends are also evident in long-term R&D investment in this and related areas. The U.S. Energy Policy Act of 2005 gives a self-regulating electric power organization, subject to review by the Federal Energy Regulatory Commission, the authority to enforce reliability rules and regulations and creates opportunities for R&D and investment opportunities to boost reliability.

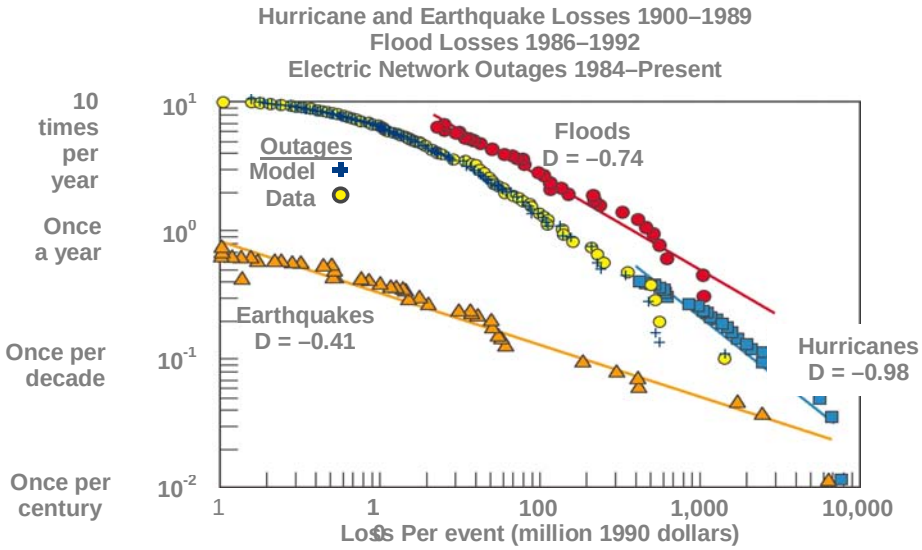


Figure 8.1. Frequency of occurrences vs. cost for the major U.S. Hurricanes, Earthquakes, Floods, and electric power outages and power law distribution

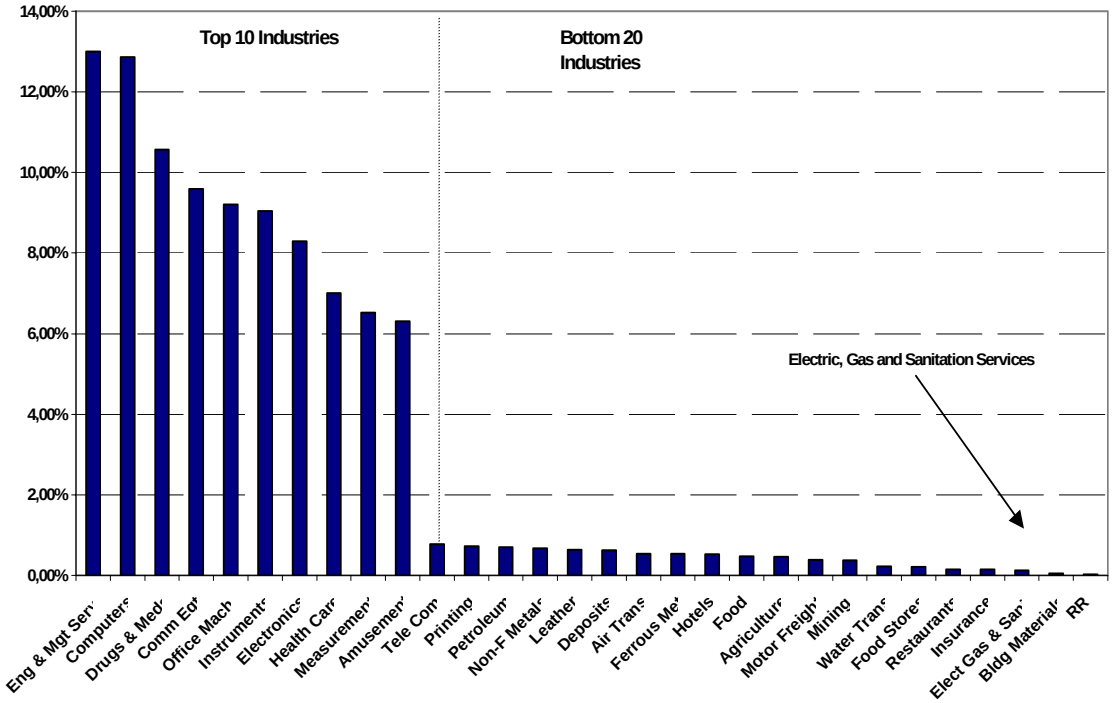


Figure 8.2. Declining infrastructure investment

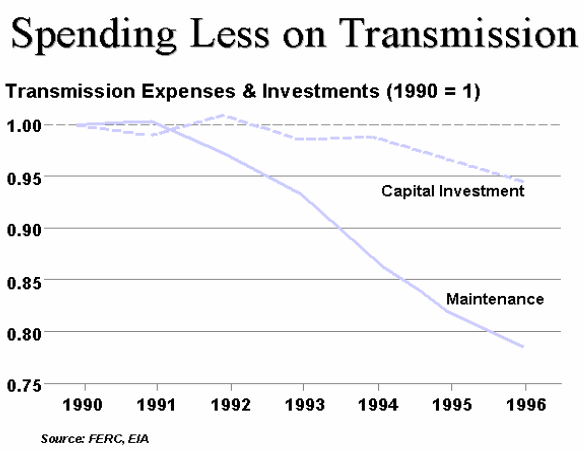


Figure 8.3. Percentage of industry R&D expenditures as a portion of net sales

The complex systems used to relieve bottlenecks and clear disturbances during periods of peak demand are now at greater risk to serious disruption and technological improvements for these systems are needed. A timely issue is merging of sensor-enabled databased models with derived models from first principles combined with online updating. How can robust controls and observers be developed that can use secure sensing to identify and build realistic models and appropriate responses? Will they be able to adapt, control, and mitigate disturbances to achieve their goals?

The recent California energy crisis in 2001–2004 is one of the most visible parts of a larger and growing energy crisis in the U.S., resulting from a decade of inadequate investments. The most basic problem in the California crisis was that declining investment in these infrastructure components led to a fundamental imbalance between growing demand for power and an almost stagnant supply. This imbalance had been in the making for years and is prevalent throughout the nation, as shown in **Figures 8.4-8.5** (Source: Western States Power Crises White Paper, EPRI, Summer 2001).

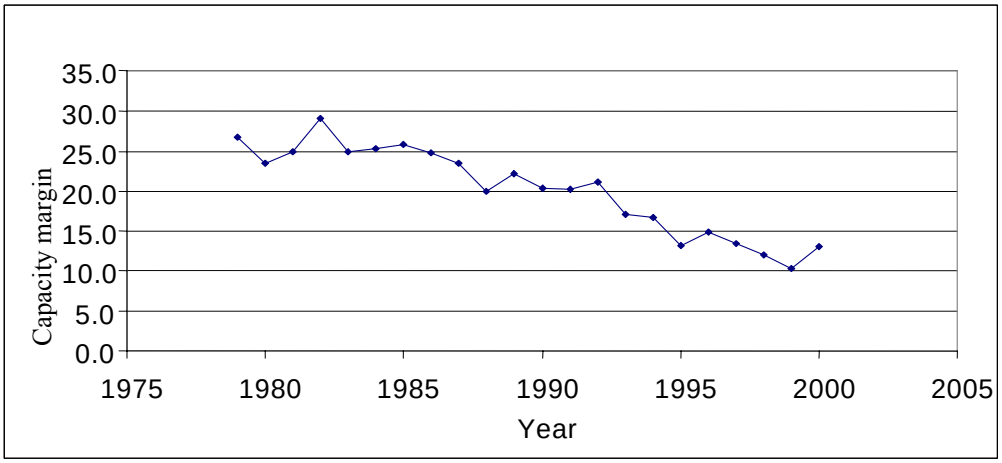
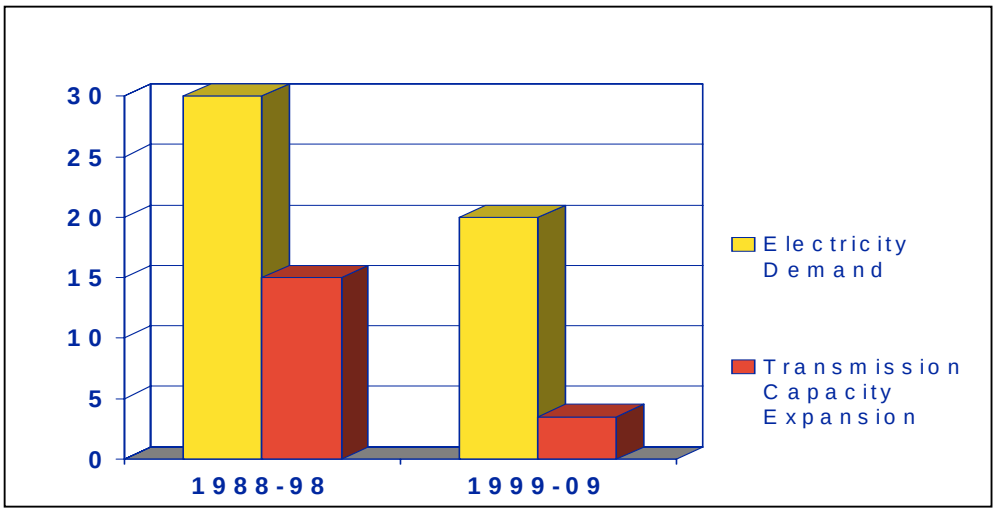


Figure 8.4: Generation Capacity Margin in North-America

Figure 8.5: Transmission additions in U.S.



8.1.2 Sources of Vulnerability

Power system generation, transmission and distribution infrastructures are designed to deal with all types of contingencies, including acts of nature, human errors, power or communication equipment failures and accidents. Fires, ice storms, windstorms, lightning strikes, geomagnetic storms are common causes for transmission outages. Mechanical problems are common causes for generator outages.

Newest threats are from intentional sabotage and malicious attacks. Terrorists may have plans to physically attack and damage transmission lines, substations and power plants. Computer hackers may breach the security of transmission grids, power plants and substation control systems. Simultaneous coordinated major outages at different substations that would have been considered impossible prior to 9/11 must now be considered as possible and credible events. This chapter addresses the next steps to increase the robustness, resilience and security of the energy infrastructure.

The philosophy of operating power systems has not changed fundamentally over the last 25 years. The same steady state Energy Management System (EMS) functions are performed today as were performed in the mid 1970s. These functions are now performed on low cost PCs instead of large multi-million dollar mainframe computers. New technological solutions are needed so that power systems can more robustly handle severe outages from both natural events and acts of terror. Power systems need to be designed to shut down more gracefully with minimal loss of load when severe contingencies occur, and customer service needs to be restored faster after major system outages.

Both the importance and difficulty of protecting power systems has long been recognized. In 1990, the Office of Technology Assessment (OTA) of the U.S. Congress issued a detailed report, *Physical Vulnerability of the Electric System to Natural Disasters and Sabotage*. The report documented the potential cost of widespread outages, estimating them to be in the range of $1-5/kWh of disrupted service, depending on the length of outage, the types of customers affected, and a variety of other factors. In the New York City outage of 1977, for example, damage from looting and arson alone totaled about $155 million – roughly half of the total cost.

During the decade since the OTA report, the situation has become even more complex. In addition to physical vulnerability, the increased susceptibility of power systems to disruptions in computer networks and communications systems must now be considered as well. Power system control has also become more centralized, in order to improve operating efficiency. However, terrorists might exploit such centralization to magnify the effects of a localized attack. In addition, many customers have also become more dependent on electronic systems that are sensitive to power disturbances. A 20-minute outage at an integrated circuit fabrication plant, for example, can cost $30 million.

Some of the complexities involved in protecting power systems and related infrastructures were identified by EPRI's *Electricity Infrastructure Security Assessment* in response to the 9/11 terrorist attacks. In particular, this assessment identified three different categories of threats:

Attacks *upon* the power system: In this case, the electricity infrastructure itself is the primary target with ripple effects, in terms of outages, extending into the customer base.

Attacks *by* the power system**:** Here the ultimate target is the population, using parts of the electricity infrastructure as a weapon. Power plant cooling towers, for example, could be used to disperse chemical or biological agents.

Attacks *through* the power system: Utility networks include multiple conduits for attacks on other infrastructures, including lines, underground cables and tunnels. An electromagnetic pulse, for example, could be coupled through the grid to damage both electricity and telecommunications networks.

Indeed, if infrastructure security is not assured, even maintaining current levels of productivity and service will be jeopardized. Conversely, as this chapter emphasizes, deploying some of the advanced technologies needed to enhance security will also have a positive effect on efforts to improve grid reliability and coordinate power system operations with those of other energy infrastructures.

In response to these challenges, national and international electric power systems need a comprehensive strategy to prepare for the diverse threats. Such a strategy should both increase protection of vital industry assets and ensure the public that they are well protected. We'll need to consider a number of actions in formulating an overall security strategy, including:

- Securing the grid from cascading damage;
- Pathways for environmental attack must be sealed off.
- Monitoring, sealing off and "sectionalizing" vulnerable conduits.
- Making critical controls and communications secure from penetration by hackers.
- Building greater intelligence into the grid to provide flexibility and adaptability, including automatic reconfiguration.
- Ongoing security assessments, including the use of game theory to study potential scenarios, will be needed to ensure that the power industry is prepared for the changing vulnerabilities.

8.2 FUTURE DEFENSE SYSTEMS

Advanced technology will necessarily play an important role in efforts to provide enhanced security because of the electricity infrastructure's unique attributes. Assuming that individual utilities are already undertaking prudent steps to improve physical security wherever possible, technology can make a vital contribution by enhancing the inherent resilience and flexibility of power systems to withstand natural disasters or attacks.

Electric Power Research Institute (EPRI), a non-profit energy research consortium organized for the benefit of utility members, their customers, and society at large, is responding to this need by launching an Infrastructure Security Initiative, a two-year program funded by the electric power industry to develop and apply key technologies that could greatly improve overall system security. For a related article, please see:

http://www.epri.com/journal/details.asp?doctype=features&id=381

From a broader viewpoint, a new mega-infrastructure is emerging from the convergence of energy (including the electric grid, water, oil and gas pipelines), telecommunications, transportation, Internet and electronic commerce. Furthermore, in the electric power industry and other critical infrastructures, new ways are being sought to improve network efficiency and eliminate congestion problems without seriously diminishing reliability and security.

In order for these challenges to be met, several Critical Capability Gaps need to be addressed:

Vulnerability assessment. The first priority among efforts to improve overall system security is to assess vulnerabilities and identify the most effective countermeasures. The probabilistic method

developed in this effort will also provide the basis for improved assessment of risks encountered during normal power system operations.

Adaptive islanding. Following major stresses due to extreme contingencies, initial reaction will focus on creating self-sufficient islands in the power grid, adapted to make best use of the network resources still available.

Secure communications. A wide-area, secure communications system is needed to replace the use of Internet for critical monitoring and control functions, in order to reduce vulnerabilities and improve availability of critical information for system recovery.

Strategic Power Infrastructure Defense (SPID) system. Following an event, SPID would analyze information about the status of the power system and secure communications system, and coordinate their use for adaptive islanding.

Self-healing grid. Once a stable configuration of grid islands had been established after an event, self-healing algorithms would gradually bring the power system back to its normal state as more resources become available. Application of these algorithms would also help optimize normal grid operations.

Intelligent Network Agents (INAs). Most sensing and control agents in a power system today simply respond to changing local conditions according to pre-programmed instructions. INAs would have decision-making capability, based on internal analysis of network-wide conditions. Once implemented, INA technology would facilitate adaptive islanding, SPID, and the self-healing grid.

8.2.1 Future Defense System Architectures

8.2.1.1 Strategic Power Infrastructure Defense

The vulnerabilities have highlighted a critical dilemma in how the power system of the future should evolve. Centralization of control over wide areas by entities such as Regional Transmission Organizations (RTOs) offers the promise of greatly increased efficiency and improved customer service, but dispersed local control may be more robust in the face of extreme events affecting power system infrastructures. This dilemma was recognized many years ago and the results of a multi-year research program indicate a way to increase both efficiency and resilience by combining top-down and bottom-up decision making into a new type of hierarchical communications and control architecture.

Called the Strategic Power Infrastructure Defense (SPID) [8-6, [8-7] system because of its ability to make large power systems more robust in the face of extreme contingencies, this new architecture can provide the basis for integrating a variety of advanced technologies into the present power system and thus enabling it to evolve. The SPID concept has grown out of the Complex Interactive Networks/Systems Initiative (CINSI) – a five-year, $30 million research program launched in 1999 and funded jointly by EPRI and the U.S. Department of Defense (through the Army Research Office). The initiative supports six research consortia, involving 26 universities, with each consortium addressing a separate aspect of the fundamental problem: how to improve the robustness, reliability, and efficiency of the nation's interdependent infrastructures for energy, communications, finance, and transportation. Two electric utilities, Exelon and Tennessee Valley Authority, are also participating directly in CINSI by providing staff expertise, data, test and demonstration sites, and management tools. The ambitious goal of this research is to avoid widespread network failures due to cascading of problems among the various infrastructures by enabling them to heal themselves automatically after a disturbance. This self-healing ability would also help optimize normal operations.

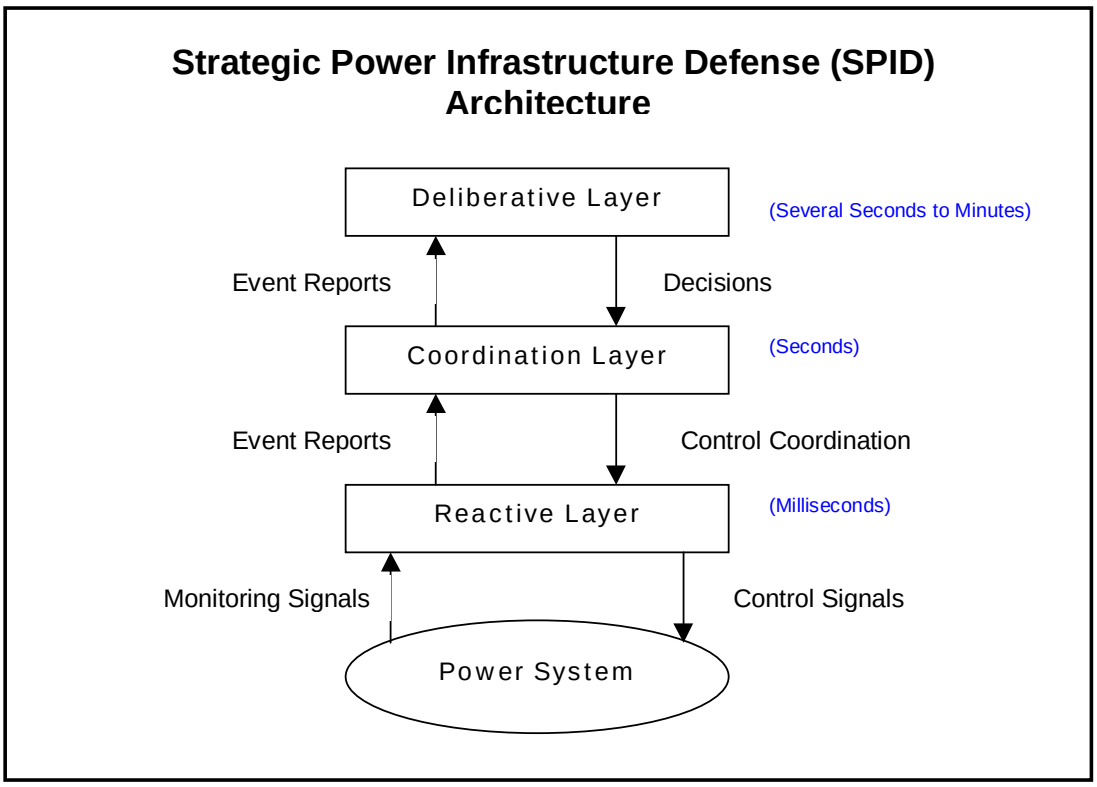


Figure 8.6: Strategic power infrastructure defense system architecture

As shown in **Figure 8.6**, the SPID architecture [8-6] is made of a three-layer, hierarchical control structure interacting with the power system. Each layer consists of numerous computerized "agents", some specialized for reacting quickly to changing conditions, others for analyzing conditions based on previous experience. These agents can communicate both horizontally and vertically, thus providing SPID with the crucial ability to make decisions on both local and system-wide levels.

The Reactive Layer is designed to handle immediate problems on the power system by following simple rules. A protection agent in this layer, for example, may receive a signal from power system monitors indicating a line fault and decide to activate a particular circuit breaker to isolate the fault. However, a reconfiguration agent in the Deliberative Layer may overrule this action and activate another circuit breaker, based on how the rest of the system would be affected. Meanwhile, agents in the Coordination Layer would be tracking system conditions, filtering alarms, and verifying actions taken.

During a major emergency, this powerful control scheme would enable intact portions of a power system to continue functioning under local control while planning ahead for eventual reconnection of islands and overall system stabilization. In addition, SPID would provide power systems with the ability to identify hidden failure modes not identified by present modeling techniques, to perform real-time vulnerability assessments using on-line information, and to substantially reduce vulnerability to cascading failures.

Prototype SPID software has been successfully tested on a 179-bus system model, demonstrating the feasibility of the three-layer architecture just discussed. Implementation of a SPID-based control system for a power network, however, will require developing a portfolio of new technologies and support systems. A wide-area measurement system (WAMS), for example, will be needed to provide synchronized phasor measurements (voltage and phase angle) from widely separated points in a network. Global positioning satellite technology has made possible the time stamps required to synchronize these measurements, but WAMS is also in the prototype demonstration stage.

A new generation of other sensors will need to be developed and deployed in order to provide accurate information on a variety of system conditions, through WAMS. Protecting such information will

require development of the secure communications system described earlier. Finally, the software needed to process the new information and carry out self-healing functions will have to be built into the microprocessors that form the physical basis of intelligent network agents. Once accomplished, this combination of elements will represent the most fundamental shift in the power system control concept since utility networks were originally designed more than a century ago.

8.2.1.2 Self-Healing Functions

When major disruptions occur on a power system today, the transmission network automatically responds by breaking into self-contained "islands," according to fixed procedures that have been established well in advance. Such procedures have not generally been updated since the onset of deregulation and will not be adequate for dealing with widely spread major events. Rather, a more flexible islanding method is needed that will minimize the overall impact of an event, taking into account the location and severity of damage, load status, and available generation. A major benefit of having this advanced islanding capability would be that power systems better withstand severe natural events, such as hurricanes.

As a first step, existing islanding schemes should be re-examined immediately for each of the three major North American interconnections, in order to develop an optimal number of pre-set islands for early deployment. Depending on the desired security level and the impact on market operation, each interconnection could be divided into a pre-set number of islands in a way that disturbances in one island are less likely to spread to other islands.

Next, full implementation of adaptive islanding will require development of fast pattern-recognition and diagnostic systems to rapidly determine the locations and nature of the initiating events. The ensuing amount of damage should also be estimated, coupled with analytical capabilities to separate the grid optimally into self-sustaining electric islands. Work would involve wide-area security monitoring, network topology estimation, and the use of wide-area measurement sensors. Adaptive load forecasting could also be used to dispatch distributed resources (DR) to help stabilize the power system in each island and to prepare for eventual reconnection of the islands.

Development of a self-healing grid capable of automatically anticipating and responding to power system disturbances while continually optimizing its own performance – will be critical for quick recovery from an event, as well as meeting the future electricity needs of an increasingly digital society. The proportion of the economy requiring digital quality power will grow rapidly during the next two decades. As a result, the electricity infrastructure will need to increase the mean time to failure of the entire supply chain to meet the reliability, security, and power quality demands of an increasingly digital society.

The ultimate goal of the self-healing grid is to provide automated capabilities that can anticipate many potential problems, reduce recovery time when unexpected disturbances actually occur, and enhance performance of normal operations. To reach this goal, three primary objectives need to be achieved:

- **Dynamically optimize the performance and robustness of the system.** Under normal operating conditions, an array of sensors will monitor the electrical characteristics of the system (voltage, current, frequency, harmonics, etc.) as well as the condition of critical components, such as transformers, feeders, circuit breakers, etc. State and topology estimation will be based on these real-time measurements. The system will constantly be tuning itself to achieve an optimal state based on predetermined optimality criteria, while constantly monitoring for potential problems that could lead to disturbances. When a potential problem is detected and identified, its severity and the resulting consequences will be assessed. Various corrective actions can then be identified, and computer simulations run to study the effectiveness of each action. Once the most effective response is determined, a situational analysis will be presented to the operator, who can then implement the corrective action very efficiently by taking advantage of the control system's automated features.
- **Quickly react to disturbances in such a way as to minimize impact.** When an unanticipated disturbance does occur on the system, it will be quickly detected and identified. An intelligent islanding scheme, for example, can be activated automatically to separate the system into self-sustaining parts to maintain electricity supply for customers according to specified priorities, and to prevent outages from spreading.

- **Effectively restore the system to a stable operating region after a disturbance.** Following the system's initial reaction to a disturbance, actions will be taken to move the system towards a stable, optimized operating state. To do so, the status and topology of the system need to be assessed in real time, allowing corrective actions to be identified and their effectiveness to be determined by look-ahead computer simulations. The most effective action can then be implemented automatically. When a stable operating state is achieved, the system will again start to self-optimize.

For the self-healing grid concept to be implemented, new software development must be supported in several areas:

Look-ahead simulation capability. Such a capability will require development of fast algorithms to propose alternative reconfigurations of the system, either in response to disturbances or as a step toward optimizing long-term system performance. Look-ahead simulation would be used to verify the feasibility and reliability of each configuration. Such simulation can take place in faster-than-real-time by drawing on approximate rules for system behavior (such as power-law dynamics) and by using simplified models of a particular power network.

Modeling and analysis. Understanding the true dynamics of a system will require development of new modeling techniques that can be used to analyze the dynamics of transmission and distribution networks and to halt disturbances quickly (in the order of milliseconds or faster). At the same time, system operators and planners will be able to change the resolution of the modeling in order to "zoom" in or out on particular areas of a network.

Optimization algorithms. Improved optimization and control theory will be needed, along with decision analysis to model hybrid (discrete/continuous) systems. New stability simulation capabilities should also be introduced as needed.

Automated Reconfiguration. Once predictions have been made about the effect of various potential reconfigurations of a power delivery system, the actual reconnections need to be carried out quickly and effectively. Achieving this goal will require automating many recovery operations that will make human intervention on both transmission and distribution systems more efficient.

Validation of Integrated Models with Real-Time Data: Once the fundamental capabilities of fast simulation and modeling have been successfully demonstrated using carefully chosen sets of test data, off-line tests will begin at control centers, using real-time data under field conditions. These data will be used to validate the models and to determine their ability to handle realistic problems. The validation process will incorporate the communications architecture already being developed as part of the self-healing grid concept.

8.2.1.3 Multi-Agent Systems

Electric power networks already use thousands of "agents" – in the sense of decision-making devices – to perform specific kinds of control functions. A protective relay on a transformer, for example, is an agent that can disconnect the transformer when a short circuit occurs on the line to which it is connected. This kind of operation is typical: The agent responds to changing local conditions, based on a pre-programmed set of instructions. Such simple agents, however, do not take full advantage of the computing power and communications options now readily available. At worst, this means that an agent's response to local conditions may actually impair overall system operations. Conversely, development of more sophisticated agents that can share information and make decisions based on a network-wide assessment could greatly improve the robustness of power systems. Specifically, such intelligent network agents (INAs) will form the backbone of SPID architecture and provide the vehicle for applying algorithms of the self-healing grid.

Creating a new generation of context-dependent INAs is one of the most complex tasks facing developers of the power system of the future. They must be simultaneously semi-autonomous and collaborative, modular but fully integrated, able to function in multiple modes, and capable of self-improvement based on experience. Although the goal is eventually to create an INA-on-a-chip, these agents currently exist only in simulation. Considerable progress has been made, however, in developing realistic test cases for these simulated agents, introducing new techniques for coordination and on-line context interpretation, and identifying ways to use the agents to help integrate physical network operations with real-time market functions.

Figure 8.7 is an illustration of the multi-agent system model of the Strategic Power Infrastructure Defense (SPID) system in Figure 6 [8-6]. Based on the three-layer structure (deliberative, coordination and reactive layers), each layer contains a number of agents. The deliberative layer includes agents performing vulnerability assessment, hidden failure monitoring, event identification, system reconfiguration and restoration and planning tasks. The reactive layer contains the fault isolation and frequency stability agents and the lower level protection and generation agents. The coordination layer agents are event/alarm filtering agents, model update agents and the command interpretation agents. Note that the "inhibition" signals may be determined by the deliberative layer and sent to the reactive layer to inhibit actions of the protection devices if the actions are considered to be harmful for the overall power grid performance.

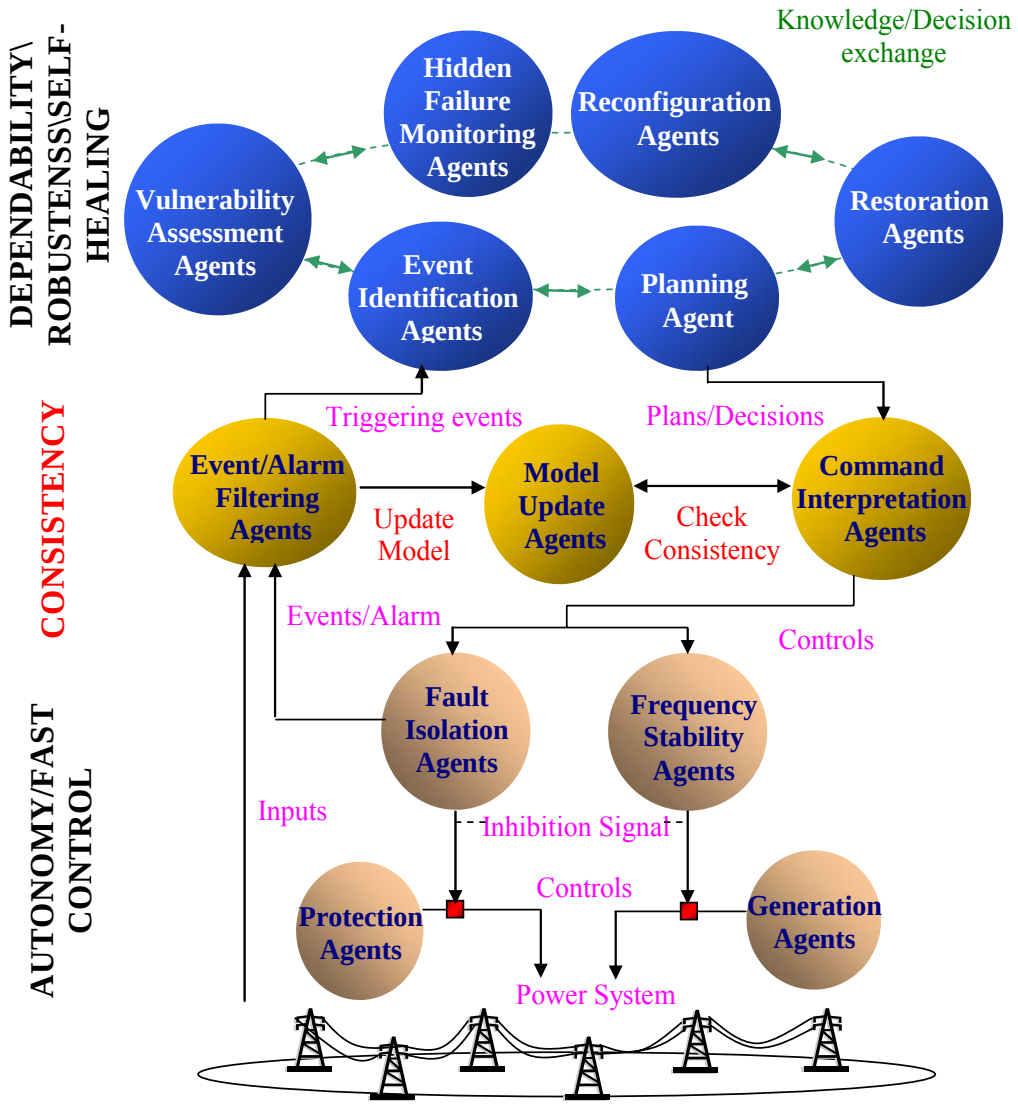


Figure 8.7: Multi-agent system model of the SPID system

8.2.2 Wide Area Information and Sensing

8.2.2.1 Wide Area Measurement Systems

Parallel to this effort will be enhancement and expansion of the Wide-Area Measurement System (WAMS), which uses satellite time stamping to coordinate data coming from sensors distributed over a large regional network. Specifically, fast simulation algorithms will be combined with pattern extraction techniques, such as data mining and cluster analysis, to provide better analysis of massive data sets and thus improve the ability to anticipate system failures. Eventually these capabilities will be incorporated into the INAs.

Because the fast-simulation techniques are based on statistical analysis of probable failure modes, rather than deterministic calculations involving discrete contingencies, the results can reveal the trade-offs involved in operating a power system beyond certain limits. Such knowledge will eventually help operators understand how best to respond when a system starts to get overloaded. Specifically, potential vulnerabilities can be revealed, for either dynamic operating conditions or physical areas of a grid, including protection devices.

Initially such analytical capabilities can be introduced by adding more local processing power at the substation level, where stand-alone computers and communications equipment would draw on data provided by the present generation of intelligent electronic devices (IEDs) and remote terminal units (RTUs). Eventually, however, advanced sensing, computing, and communications technology will need to be incorporated at the chip level in a new generation of INAs attached to critical equipment for improved system integration based on the SPID control architecture.

The main function supported by the WAMS will be the power system dynamic state estimation. Synchronized phasor measuring units (PMUs) will provide the voltage and current phasors and line status for estimating real time load flows and system topology. This function will be a key input for all three levels of the SPID architecture.

At the deliberative layer, the system state is needed for vulnerability assessment, system reconfiguration and restoration while at the coordination layer, it is used for updating the system model. At the reactive level, the system dynamic state is required for performing wide-area stability functions.

Angular and frequency stability would be taken in charge by stability agents. For such fast phenomena, PMUs derived pilot phasors might be used for computing instability indices and detecting loss of synchronism between coherent areas (angular instabilities) or under or over-frequency conditions (frequency instabilities) [8-7, [8-8, [8-9]. System state would also be required for predicting voltage instability conditions.

Typical preventive actions taken in charge by the reactive layer (generation and protection agents) are given below:

- Power plant : generator tripping, fast valving, braking resistor, excitation systems
- Transmission system: transmission line switching, shunt inductance or capacitance switching, dynamic reactive compensation, FACTS, HVDC converters, on load tap changers;
- Load: load shedding, load modulation (demand side management).

A functional infrastructure for interconnecting synchronous measuring units, with stability agents and generation – protection agents is shown in **Figure 8.8**.

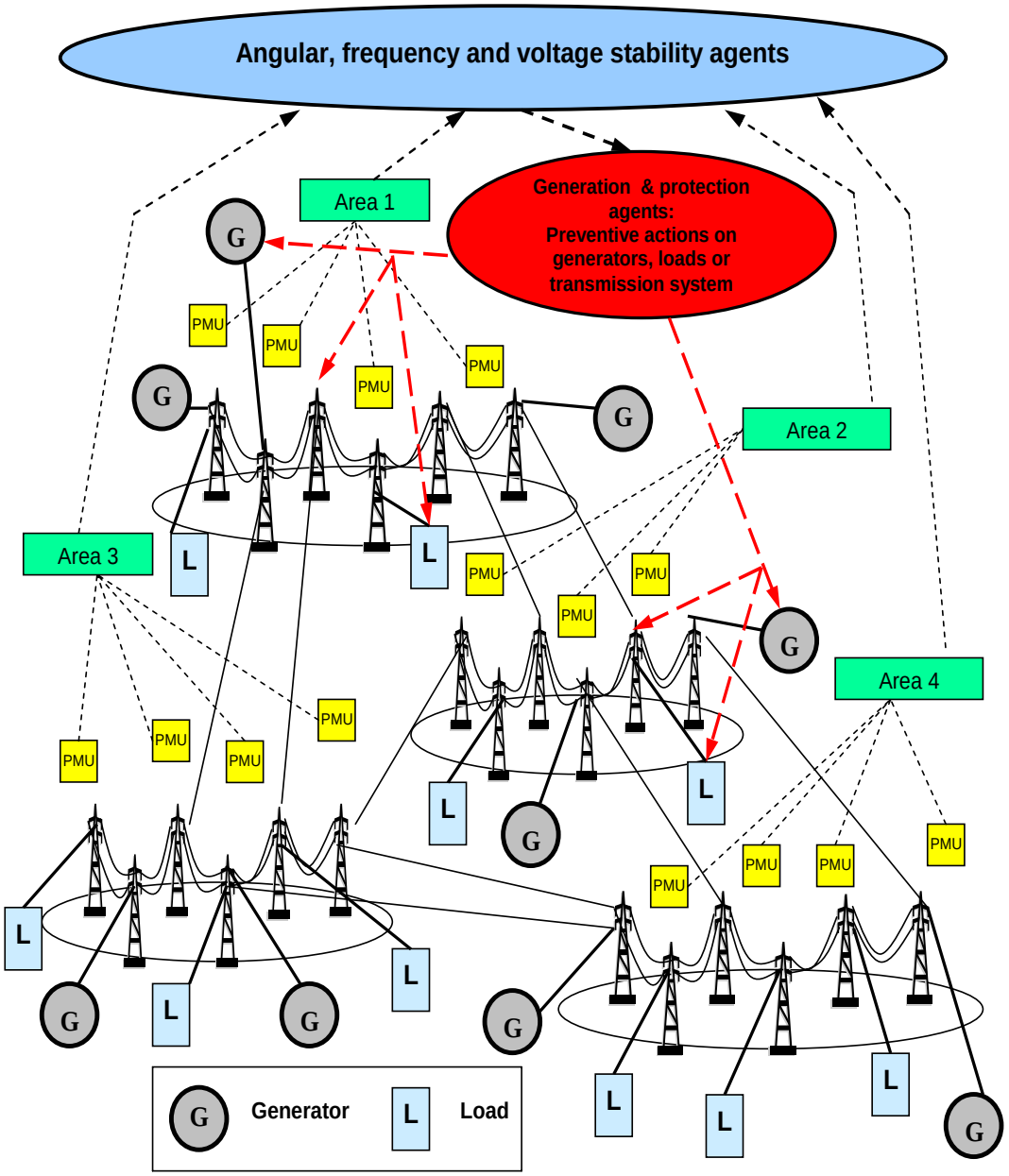


Figure 8.8: Wide-area Control and Protection System

Four areas are represented in Figure 8. Dotted lines represent communication links within the infrastructure. In each of the area, measurements coming from the PMUs (phasors and connectivity) are concentrated in an AMS (Area Measuring System) to generate the pilot phasor and the sub-system state. These data are communicated to stability agents for detection of potential instability conditions. When detected, preventive actions are communicated to generation and protection agents:

- to stabilize the system as an whole or
- to reconfigure the system in two or more islands

Information needed for predicting system reliability and wide-area control of power systems can be categorized into two groups: off-line and on-line. The transmission line characteristics, types of protective devices, and market rules can be off-line data because they do not change frequently.

On-line power system topology should be available. These data items are available at various substations or control centers. The substations and the proposed systems should be connected via Intranet and satellite communication. The group of on-line data includes information that frequently changes over time such as operating voltage, current, frequency, generation, and event/alarms. Most of current protection/measurement devices can send the data through dedicated communication networks to the control centers. Other types of on-line data to be considered are the environmental and market data. For instance, since temperature and humidity impacts power system operating conditions critically, the data should be updated regularly. The system can receive data from a meteorological data source through Internet and/or satellite. In a market environment, bidding data and power schedules between generations and loads are accessible through Internet/OASIS.

8.2.2.2 Communication Systems

As previously introduced in chapter 6 (paragraph 6.6.3), the power system currently uses several media for its protection, control, and information-sharing functions. The most common ones include: power line carrier (PLC), microwave, optical fibers, pilot wire and wireless communications.

PLC operates by transmitting radio frequency signals between 10 kHz to 490 kHz over the transmission lines. PLC with power output of order 150 W can be used up to 150 miles. Normally, PLC carries only one channel of 4 kHz bandwidth. The frequency range is limited by government regulations. The PLC is the most common communication media used in the U.S. for protection. However, it has some disadvantages such as its bandwidth limit and its subjectivity to lightening, switching surges, and network reconfiguration.

Microwave operates in the 150 MHz to 20 GHz frequency range. This bandwidth can carry a lot of communication channels for a variety of information. The disadvantage of the microwave is that the transmission length is limited to a line of sight path between antennas. Microwave is subject to atmospheric attenuation and distortion. The combined latency using modem plus analog microwave is around 100 milliseconds between two adjacent antennas.

Optical fibers are now considered the most reliable media of communication. A single fiber cable can carry up to 8000 channels. In addition to the capacity the fiber has no interference with other electric systems. The only disadvantage is the cost of the cable system and the cost of construction. Optical fiber communication has the smallest latency among all media.

Pilot wire is normally telephone wire either owned by utility companies or leased from telephone companies. This type of communication has a bandwidth up to 4 kHz. Overhead lines may experience interference from power lines while the underground is subject to damages for many obvious reasons.

Wireless is one of the modern methods of communication (security is a concern). Low orbit satellite communication system provides an option to transmit information covering a very large range. The delay and the cost of installation are the two main problems.

All of the above media may be using different communication networks such as circuit-switched networks, packet-switched networks, and cell-switched networks. In addition to the above layers, there is the electricity infrastructure itself that will make these functions work together. Distributed intelligence is the trend. Local, regional and global functions are implemented. Communication and protection performance requirements are indicated in **Tables 8.1**-**8.2**:

Table 8.1: Communication requirements

Power System Tasks	**Bandwidth Requirement**	**Current Response Time**
Load Shedding (Local Decision)	Low	Seconds
Adaptive Relaying (e.g., Blocking relay)	Low	Not Available
Hierarchical Data Acquisition and Transfer	High	Seconds (e.g., 2-12 sec. scan for RTUs)
Line / Bus Reconfiguration	Low	Minutes (manual)
Control Devices (e.g., FACTS, Transf, etc.)	Medium	Seconds (manual)
Fault Event Recorder Information	Medium	Minutes
Generator Control	Low	Seconds

Table 8.2: **Protection schemes & communication requirements**

Type of relay	Data Volume (kb/s)		**Latency**	
	Present	Future	Primary	Secondary (s)
Over current protection	160	2500	4-8	0.3-1
Differential protection	70	1100	4-8	0.3-1
Distance protection	140	2200	4-8	
Load shedding	370	4400	0.06-0.1 (s)	
Adaptive multi terminal	200	3300	4-8	0.3-1
Adaptive out of step	1100	13000	Depends on the disturbance	

8.2.2.3 Communication Security Issues

Control and monitoring systems inside control centers, power plants, and substations are generally proprietary, stand-alone systems not designed to be secure against cyber threats. Also, because of Internet's advantages in terms of productivity improvements and reduced costs, control systems are being networked without the technology to make them secure. As a result, Internet now represents the largest external threat to the security of critical control systems. Deregulation has also increased vulnerability to cyber threats because centralized control entities, such as ISOs and RTOs, mean that attacks can impact a larger area. In addition, when utilities divest their generation, they lose control of the cyber security in the generation units that are still electronically connected to their control centers. The growing complexity of the power system and its control and communications networks exacerbates these problems.

Technology developed for Internet applications, such as firewalls and intrusion detection systems, may not provide utility control systems with the required level of security. In particular, remote access

creates a high level of cyber vulnerability for control systems, because commonly available software enables users from remote locations to view and change any parameter of the system. Such software generally has minimal security (passwords at best), and leaving modems connected creates cyber vulnerabilities for the control systems. Energy markets also rely on Internet for much of their communications.

Although most organizations attempt to protect their business systems and control centers from cyber attacks, plant control systems and substations may not be adequately protected. It may therefore be possible to penetrate mission critical operations control systems through unsecured access points. Potential risks span the spectrum from having data stolen (industrial espionage) to total loss of power flow control or substantial physical damage (sabotage). Risks can occur not only during the initiation of events, but also during restart and restoration, by changing equipment set-points and emergency operating or restoration procedures.

A wide-area, secure communications system needs to be developed as an alternative to Internet for critical monitoring and control functions. Although computers are widely used for fast local control of equipment as well as to process large amounts of sensor data from the field, coordination between control centers is still based largely on telephone calls. As recent events have indicated, cell phone and land lines may be overwhelmed after a catastrophic event. In addition, the "reserve margin" of the public switched communication network in the U.S. is currently under 20%.

As a first step, information security provisions such as authorization, authentication, and encryption must be added to current communications protocols. To accomplish this, each protocol must be reexamined to determine the impact on performance of adding these security features. Eventually, however, a secure, private communications system must be adopted as an effective alternative to Internet–based systems. Advanced cyber security technologies are particularly needed for power system control and monitoring.

First, a comprehensive assessment should be performed to determine which communication technologies and security options are appropriate for utility operations, and where they should be implemented first. Utilities have unique requirements for communications performance – such as timing, redundancy, substation control and protection, equipment control and diagnostics, etc. – that must be preserved in spite of security constraints. In particular, security adds data "overhead" and timing delays that could disrupt real-time operations, so that issues of time and bandwidth will also have to be solved.

Next, a new private communications network must be designed from the ground up to provide required levels of security, including authorization, authentication, encryption, intrusion detection, redundancy. New networks must provide sufficient bandwidth and improved efficiency to provide real-time data to meet requirements of control center operations. These new networks should be based on the existing Utility Communications Architecture (UCA) to ensure widespread compatibility.

8.2.3 Failure Analysis

8.2.3.1 Hidden Failures of Protective Systems

In general, protective relays can fail in two ways: trip when it is not supposed to (not secure), and failure to trip when it is supposed to (not reliable). A hidden failure is not simply a failure of the protective system. This class of failures is not normally incorporated in the protective system design and setting. An example of a hidden failure is the transmitter of a relay. The transmitter failure may result in the inability for the delay to send a blocking signal to another relay. Since the blocking signal is not sent, the other relay may trip, leading to an unnecessary loss of line. The hidden failure may remain undetected until it is activated by a fault. Hidden failures may also lead to undesirable cascaded events that often cause widespread power outages [8-12]. Monitoring the hidden failures is the task of one of the agent in the Strategic Power Infrastructure Systems [8-6] illustrated in **Figure 8.7**.

8.2.3.2 Cascaded Events

The primary objective of a defense system is to prevent the events from cascading by taking protection and control actions in the early stage of the event scenario. Widespread power outages are often caused by cascaded events consisting of transmission line outages, generator trippings and relay malfunctions. An analysis of the August 10, 1996, outage in the western U.S. power grid indicates that the system becomes vulnerable as

- Lines are out of service for maintenance
- Cascaded line tripped due to cascaded events
- Loading on lines exceeded limits
- Reactive power problems developed
- 13 generators tripped as part of the cascaded events involving a hidden failure
- Islanding actions were taken

These problems of hidden failures, failures of EMS / SCADA / communication, incorrect diagnosis of the cascading events, inaccurate power system models, inadequate coordination of the under-frequency load shedding relays are causes of the widespread power outages.

8.2.3.3 Market Related Events

In a competitive power market environment, disturbances in the market can cause vulnerability of the power infrastructures. Examples of the market related scenarios are:

- A large number of transactions on the grid leading to uncertainties in the generation, load and power flow patterns
- Excessive price volatility that creates a high level of uncertainty in the supply and demand, causing vulnerable system conditions that are hard to predict during planning or operation
- Lack of economic incentives for expansion of the generation or transmission facilities to accommodate the load growth
- Gaming on the transmission grids leading to transmission congestion or vulnerable network operating conditions

Methods to handle the above market related scenarios and to avoid vulnerable operating condition of the power grid remain to be developed.

8.2.4 Vulnerability Assessment

Vulnerability assessment is an important aspect in our effort to avoid catastrophic failures due to cascaded events. Cascaded events can include component failures (e.g., line or generator outages), malfunctioning of protective devices (e.g., relay and/or breaker failures), human errors, and cyber or communication problems, etc. Despite the significant progress made over the past decades in the software and hardware simulation technologies, there is still a lack of tools that allow accurate simulations of catastrophic failures due to cascaded events.

There are excellent tools today for simulations of the power system behavior in the steady state, dynamic and transient conditions. Tools are also available for simulation of the protective devices. However, no tool at present would allow comprehensive and accurate simulations of the cascaded events that can span a wide range of operating conditions from normal and abnormal conditions to islanding and possibly a complete shutdown. Tools are also lacking for simulation of system restoration procedures from a blackout back to a normal condition. These tools will be very useful for planning and operation of the power grids. Planners can simulate cascaded events to determine the system vulnerability level with respect to the past or hypothesized major events. The tools will also allow simulations of the wide area protection and control methods to evaluate their effectiveness. These tools are also likely to provide decision support for planning of the system restoration process.

The proposed new simulation tools for cascaded events and catastrophic outages will require extensive models of the system components over a wide range of operating conditions. Since the duration of a scenario can last for a long period (e.g., hours), there will be new challenges in the efficiency of simulation techniques. Protective devices including hidden failures and breaker malfunctions will need to be modeled in the simulator. Operators' decisions play an important role in these events. The simulation environment should be able to allow these decisions to be implemented as the system conditions evolve during simulation.

There is a great need for vulnerability indices for the wide area power grids. The index is a measure of how likely a sequence of events can lead to a catastrophic outage of the power grid. Existing indices for power system security such as line overloads and voltage violations are designed for the traditional system security framework that is based on the N-1 or N-2 security concept. The proposed concept of vulnerability index should take into account the wide area protection and control functions that are intended to avoid catastrophic operating conditions. R&D is much needed in this area.

8.2.5 Risk Assessment

Risk Management is an important task for the protection of critical infrastructures. While risk generally cannot be eliminated, enhancing protection from known or potential threats can help reduce it. "Risk management is a systematic, analytical process to determine the likelihood that a threat will harm an asset or resource and to identify actions that reduce the risk and mitigate the consequences of an attack or event" [8-11]. The document [8-11] from National Infrastructure Protection Center provides a risk management model that not only assesses assets, threats, and vulnerabilities but also incorporates a continuous assessment feature. As described in [8-11], a risk management approach has several elements: assets assessment, threats assessment, vulnerabilities assessment, as well as countermeasures identification and continuous assessment. Reference [8-11] provides a simple equation for a quantified risk level, i.e.

$$\text{Risk} = \text{consequence} \times (\text{threat} \times \text{vulnerability})$$

where the "threat × vulnerability" segment represents the likelihood of the unwanted event occurring, and the "consequence" represents the damage due to the unwanted event.

Different types of critical infrastructures form a coupled system [8-12]. An important element to handle their interdependencies is the set of tools. A taxonomy of tools that define the research requirements for the next generation of tools has been developed [8-12]. This taxonomy provides an overview of tools necessary to conduct in depth analysis and characterization of threats, vulnerabilities, and interdependencies of critical infrastructure systems and their interactions. The tools are developed to handle consequence, vulnerability, threats, risk assessment, interdependency, simulation, and security.

8.2.6 System Reconfiguration

The recent events and major power outages have altered how the power industry views the security and safety of the power infrastructure. In addition to resolving the local and regional levels power disturbances and outages, the industry must begin to evaluate the possibility of the larger, more systemic impacts of cascaded events and possible sabotage activities. To minimize the potential damages caused by such radical events, the power infrastructure must be more intelligent and flexible, allowing coordinated operation and control measures to absorb the shock and minimize the impact. Therefore, new research problems need to be formulated. Once the damage is translated into its effects on the power grid components or subsystems, much of the existing techniques for power system analysis will be applicable.

Once the Risk Management shows a high risk level alert, for example, the risk index gives a high numerical risk rating, countermeasures should be taken to lower the overall risk to an acceptable level. One of the important efforts is to investigate the countermeasure options is constructing a *flexible grid configuration*. The proposed method is to create self-sufficient sub-networks in the power grid to make best use of available resources [8-13]. Assuming a stable grid of sub-networks is established, a self-healing strategy could be used to gradually bring the power system back to its normal state when risk rating goes back to the low level.

8.3 RECOMMENDATIONS AND CONCLUSIONS

8.3.1 Recommendations

Electric power infrastructures are facing great challenges that require significant R&D efforts [8-14]-[8-15]. Although development of a secure, reliable, robust power system represents a very ambitious goal that will not be fully achieved for several years, individual elements of such an advanced system can be integrated with the existing grid beginning almost immediately. Careful planning will be

required so that this type of phased integration provides maximum benefits at the earliest possible time. **Figure 8.9** gives a broad overview of how the power system of the future can evolve smoothly. Many of the steps involved could be accelerated, however, if sufficient funds were available.

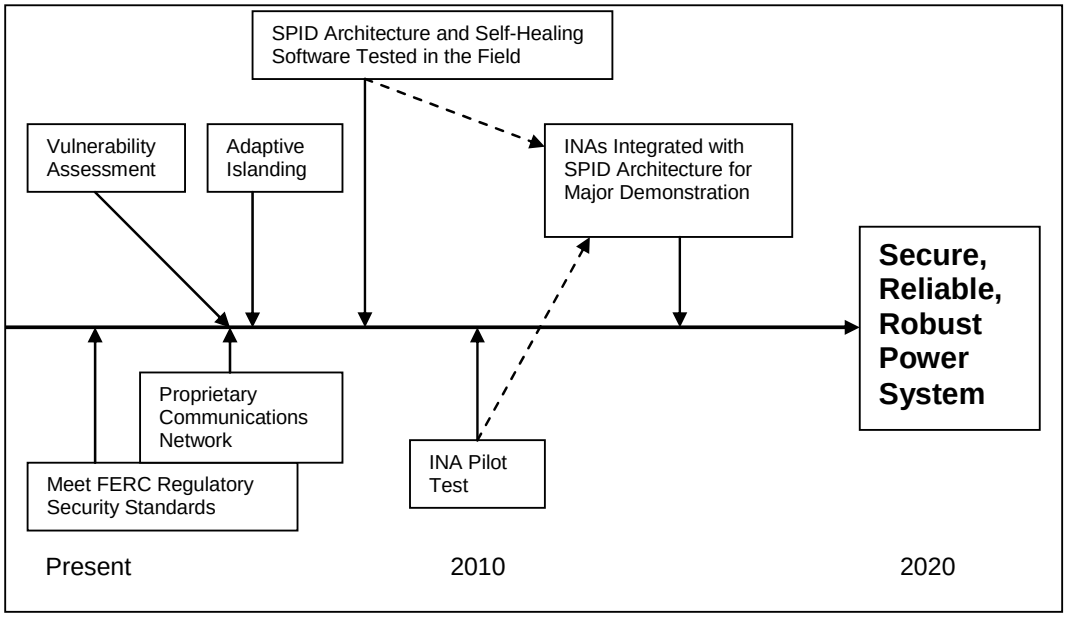


Figure 8.9: Timeline for development and deployment

As shown in the figure, major milestones include:

Meet FERC Regulatory Standards. New secure protocols for use with Internet-based information and control systems should be implemented immediately, together with other security standards set forth in Appendix G of FERC Notice of Proposed Rulemaking, Docket No. RM01-12-000. These include establishment of basic security programs at each utility, definition of security perimeters for physical and cyber systems, asset classification and control, access control to critical systems, procedures for critical system management, incident response procedures (including reports to the Electricity Sector – Information Sharing and Analysis Center), and contingency plans for business continuity.

Vulnerability Assessment: Basic tools for conducting a nationwide vulnerability assessment are currently being developed as part of the EPRI Infrastructure Security Initiative (ISI).

Proprietary Communications Network: ISI will develop an overall system design based on the Utility Communication Architecture, and a wide-area network could be pilot-tested.

Adaptive Islanding: New methods of screening and pattern extraction are needed to rapidly identify the consequences of various island configurations after a major disruption. Adaptive load forecasting, including dispatch of network resources in anticipation of island reconnection, are also needed. Both research areas are being pursued as part of the CEIDS Self-Healing Grid Initiative.

SPID Architecture and Self-Healing Software: Fast-simulation and modeling software (required to enable self-healing functions) are being developed by the CEIDS Self-Healing Grid Initiative, together with a detailed design of SPID architecture. The two could be tested together in the field using stand-alone computers and communications equipment at the substation level.

INA Pilot Test: Incorporation of self-healing software and associated sensors and communications capability into microprocessors in order to create an INA-on-a chip could be ready for pilot field-testing in 2006–2007.

INA Integration with SPID Architecture: Depending on results of the INA pilot test, integration of microprocessor-based INAs might be demonstrated on a major regional grid by 2015.

Secure, Reliable, Robust Power System: Full implementation of the power system of the 21st century, capable of self-healing and self-optimization, could be achieved by 2020.

8.3.2 Conclusions

Any complex dynamic infrastructure system typically has many layers and decision-making units and is vulnerable to various types of disturbances. Effective, intelligent, distributed control is required that would enable parts of the network to remain operational, and even to automatically reconfigure, in the event of local failures or threats of failure. In any situation subject to rapid changes, completely centralized control requires multiple, high-data-rate, two-way, communication links, a powerful central computing facility, and an elaborate operations control center. But all of these are susceptible to disruption at the very time when they are most needed (i.e., when the system is stressed by extreme stresses such as natural disasters or unusually high demand). Management of disturbances in all such networks and the prevention of cascading effects throughout and between networks require a basic understanding of the true system dynamics, as well as effective distributed control functions that will enable parts of the networks to remain operational, or even to automatically reconfigure themselves.

When failures occur at various locations in such a network, the system breaks into isolated "islands", each of which must then fend for itself. With the intelligence distributed and the components acting as independent agents, those in each island have the ability to reorganize themselves and to make efficient use of whatever local resources remain to them in ways that are consistent with the established global objective of minimizing the impact on the overall network. Local controllers will guide the isolated areas to operate independently, while preparing them to rejoin the network, without creating unacceptable local conditions either during or after the transition. A network of local controllers can act as a parallel, distributed computer, communicating via microwaves, optical cables, or the power lines themselves, and intelligently limiting their messages to only the information that is required to achieve global optimization and to facilitate recovery after failure.

Although the immediate and critical goal is to avoid widespread network failure, the longer-term vision is to enable adaptive and robust infrastructures. From a broader perspective, science and technology help to expand the upper bounds of our quality of life. During the past ten thousand years, fundamental understandings gained through scientific discovery, and facilitated by innovative technologies, have provided humans with the tools to ascend from savagery to civilization. Engineers have played a central role in shaping our world and building everlasting "monuments of our civilization" through science and technology. The key challenge before us is to recognize the lasting monuments that we are building right now for future generations.

The following was expressed in the July 2001 issue of *Wired* magazine: "The best minds in electricity R&D have a plan: Every node in the power network of the future will be awake, responsive, adaptive, price-smart, eco-sensitive, real-time, flexible, humming, and interconnected with everything else."

Achieving this vision and sustaining infrastructure reliability, robustness, and efficiency are critical long-term issues that require strategic investments in research and development. Given economic, societal, and quality-of-life issues, as well as the ever-increasing interactions and interdependencies among infrastructures, this objective offers exciting scientific and technological challenges.

8.4 REFERENCES

[8-1] G. S. Vassell, "Northeast Blackout of 1965," *IEEE Power Engineering Review*, Volume: 11, Issue: 1, January 1991, pp. 4-8.

[8-2] "The Con Edison Power Failure of July 13 and 14, 1977 (1978, June)", Available: http://chnm.gmu.edu/blackout/archive/a_1977.html.

[8-3] C. W. Taylor and D. C. Erickson, "Recording and Analyzing the July 2 Cascading Outage [Western USA Power System]," *IEEE Computer Applications in Power*, Jan. 1997, pp. 26-30.

[8-4] D. N. Kosterev, C. W. Taylor, and W. A. Mittelstadt, "Model Validation for the August 10, 1996 WSCC System Outage," *IEEE Transactions on Power Systems,* Aug. 1999, pp. 967-979.

[8-5] "The US Blackout Timeline", *Power Engineer*, Volume: 17, Issue: 5, Oct.-Nov. 2003.

[8-6] C. C. Liu, J. Jung, G. T. Heydt, V. Vittal, and A. G. Phadke, "Conceptual Design of the Strategic Power Infrastructure Defense (SPID) System," *IEEE Control System Magazine*, Aug. 2000, pp. 40-52.

[8-7] Juhwan Jung, George Karady, James McCalley, Gerald Heydt, Chen-Ching Liu, Arun Phadke, Vijay Vittal, "Wide Area Protection and Control Using a Strategic Power Infrastructure Defense System", CIGRÉ 39th. Session, August 2002

[8-8] I. Kamwa, R. Grondin, "PMU Configuration for System Dynamic Performance Measurement in Large Multi-Area Power Systems," *IEEE Trans. on Power Systems*, May 2002, pp.285-394.

[8-9] I. Kamwa, R. Grondin, A. Henniche, G. Trudel, L. Riverin, "Rapid Stability Assessment of Extreme Contingencies Based on Wide-Area Severity Indices," CIGRE/IEEE Symposium on Quality and Security of Electric Power Delivery Systems, Montréal, Canada, Oct. 7-10, 2003.

[8-10] D. C. Elizondo, J. de La Ree, A. G. Phadke, and S. Horowitz, "Hidden Failures in Protection Systems and Their Impact on Wide Area Disturbances," IEEE Power Engineering Society Winter Meeting 2001, Vol. 2, pp. 710-714.

[8-11] National Infrastructure Protection Center, "Risk Management: An Essential Guide to Protecting Critical Assets," Nov. 2002, Available:

http://www.in.gov/ctasc/whatsnew/risk_management 11-02.pdf.

[8-12] S. R. Trost, "Tools for 21st Century Infrastructure Protection," Workshop on protecting and assuring critical national infrastructure: setting the research and policy agenda, Palo Alto, CA July 21-22, 1997.

[8-13] H. Li, G. Rosenwald, J. Jung, and C. C. Liu, "Strategic Power Infrastructure Defense," *Proceedings of the IEEE*, May 2005, pp. 918-933 (Guest Editor: M. Amin).

[8-14] M. Amin, "Evolving Energy Enterprise – Grand Challenges: Possible Roads Ahead and Challenges for R&D," IEEE Power Engineering Society Summer Meeting, 2002, pp. 1705-1707.

[8-15] M. Amin, "Modernizing the National Electric Power Grid," Workshop on Modernizing the National Electric Power Grid, co-sponsored by NSF, Entergy, EPRI and Department of Energy, Nov. 18-19, 2002, New Orleans, LA

CONCLUSION

In general, even though a power system is planned and designed to withstand any credible contingency, it can also be affected by more severe disturbances than those for which it was conceived, and this can lead to a partial or total frequency and/or voltage collapse. The Task Force C2.02.24 position is that more effort must be directed at enhancing the ability of the bulk power system to withstand extreme contingencies, which are usually initiated by multiple faults but which may also be initiated by single faults associated with multiple or successive disconnections of transmission components.

Recent blackouts in a number of countries have demonstrated the need for defense plans to respond to extreme contingencies. The philosophy behind protection against extreme contingencies is that a system-wide power failure must not be the consequence of a situation that could reasonably have been avoided. The primary objective is therefore to preserve the integrity of the power system by using automatic schemes that are simple, reliable and safe for the system, and that provide the widest possible coverage against all possible extreme contingencies, bearing in mind at all times that simplicity should prevail over selectivity in determining the scope of the actions to be carried out. Achieving this objective would limit the number of consumers who experience service interruptions, and at the same time maintain a viable level of system operation.

In addition to the existing "event-based" control, there is also a need for "response-based" actions. The concept of Wide-Area Defense offers better detection and control strategies, which lead to better management of disturbances and significant opportunities for higher power transfers and operating economies. The continuing improvement of analytical tools and study procedures for the various types of disturbances discussed in this document, along with developments in enabling technologies for monitoring and control, offer great opportunities for designing advanced protection schemes by using system-wide information together with distributed local intelligence and by communicating selected information between separate locations to counteract the propagation of major disturbances.

However, it is also crucial to have system restoration plans on hand for all types of contingencies, and the emergency power supplies at system control centers and telecommunications stations must be efficiently maintained so that they can be used in the event of a major system outage.

This report provides a comprehensive look at the many considerations and factors that should guide the development of defense plans. From conceptual ideas to various components, including engineering, design, documentation, operational training and maintenance, the report proposes ways to implement these schemes securely. However, defense plans address extreme contingencies and therefore do not operate frequently. In light of this, systematic tests over the life cycle of the plan are needed to maintain the necessary know-how and to accommodate continued system and scheme expansions when necessary.

For many years, the industry has been implementing this concept in several parts of the world, but the cost and operational complexity of these schemes has prevented us from reaping the full benefits. However, today's technologies enable coordinated Wide-Area Defense Systems to be cost-effective solutions. Computer relays communicate not only with the control centre, but with each other. The implementation of an advanced Wide-Area Defense System requires a significant improvement of the existing decentralized subsystems. Decentralized subsystems will have to utilize advanced algorithms to make local decisions based on local measurements and/or selected remote information. With a fully developed information interchange and communication infrastructure, it will be possible to link all of the monitoring, control and protection devices together. The key to a successful solution is rapid detection, fast and powerful control devices and efficient and reliable communications systems, and smart algorithms, or in other words, a true Wide-Area Defense System.

Electric power infrastructures are facing great challenges that require significant R&D efforts. Although the development of a secure, reliable, robust power system represents a very ambitious goal that will not be fully achieved for several years, individual elements of such an advanced system have been and can be incorporated into the existing grid.

As expressed in the July 2001 issue of *Wired* magazine: "The best minds in electricity R&D have a plan: Every node in the power network of the future will be awake, responsive, adaptive, price-smart, eco-sensitive, real-time, flexible, humming, and interconnected with everything else."

Achieving this vision and sustaining infrastructure reliability, robustness, and efficiency are critical long-term issues that require strategic investments in research and development. Given economic, societal, and quality-of-life issues, as well as the ever-increasing interactions and interdependencies among infrastructures, this objective offers exciting scientific and technological challenges.