# Emergency control and its strategies

L. Wehenkel
University of Liège - Department of Electrical Engineering
Institut Montefiore, Sart-Tilman B28, B-4000 Liège, Belgium

Email: Louis.Wehenkel@ulg.ac.be Web: http://www.montefiore.ulg.ac.be/∼lwh/

**Keywords:** emergency control, security control, automatic learning, voltage stability, transient stability, probabilistic methods.

## ABSTRACT

The objective of this paper is to discuss research trends in the context of power system emergency control. First, different possible strategies are discussed for the design of emergency control schemes. Then some new research directions are presented. The paper does not restrict its scope to a particular type of stability problem. Rather, it aims at providing a global view of emergency control and discusses the potential impact of new approaches.

## 1 INTRODUCTION

Power system security is more and more in conflict with economic and environmental requirements. Security control aims at making decisions in different time horizons so as to prevent the system to experience undesired situations, and in particular to avoid large catastrophic outages. Traditionally, security control has been divided in two main categories : preventive and emergency control (EC).

In preventive security control, the objective is to prepare the system when it is still in normal operation, so as to make it capable of facing future (uncertain) events in a satisfactory way. In emergency control, the disturbing events have already occurred, and thus the objective becomes to control the dynamics of the system in such a way that consequences are minimized.

Thus, the main differences between preventive and emergency control are as follows.

- Types of preventive control actions : generation rescheduling; network switching; reactive compensation; sometimes, load curtailment.
- Types of emergency control actions : direct or indirect load shedding; generation shedding; shunt capacitor or reactor switching; network splitting.
- Frequency of control actions : very frequent in preventive control and rather infrequent in emergency control.
- Instantaneous cost of individual control actions : rather low in preventive control; very high in emergency control.
- Total (integrated) cost of control actions : potentially very high in preventive control, low in emergency control (as far as emergencies remain very rare events).
- Time available for decision making : quite long in preventive control; may be very short in emergency control.
- Complexity of possible control operations : may be high in preventive control; must be simple in emergency control to be applicable in real-time.
- Uncertainty : in preventive control, the state of the system is well known but disturbances are uncertain; in emergency control, the disturbance is certain, but the state of the system is often only partially known; in both cases, dynamic behavior is uncertain.
- Open versus closed loop : preventive control is generally of the open loop feed-forward type; emergency control may be closed loop, and hence more robust w.r.t. uncertainties.
- Coordination among different control objectives : is possible in principle in preventive control; is much more difficult in emergency control.
- Strategy : preventive control is generally designed to handle the most likely events; emergency control is specially useful if it can handle also very unlikely events/situations.

In the past, many utilities have relied on preventive control in order to maintain system security at an acceptable level. In other words, while there are many emergency control schemes installed in reality, the objective in the past has been to prevent these schemes as much as possible from operating, by imposing rather high objectives to preventive security control. As to any rule, there are exceptions : for example controlled generation shedding has been used extensively in North America to handle transient stability problems; in the same way, corrective control has been used in many systems as an alternative to preventive control in the context of thermal overload mitigation. We will come back to these aspects in the main part of the paper.

Today, it seems that the pressure is to increase trading and competition in the power system field. This means that preventive security control will be (if it is not already) looked at as being an impediment to competition. Hence, in the future there will be strong incentives to rely less on preventive control and more often on emergency control. The objective of this paper is therefore to analyse the role of emergency control from a global perspective and to discuss new approaches and techniques which may help to improve power system emergency control plans. Rather than trying to provide a survey of existing work (which may be found e.g. in [13]) we try to provide a critical overview of the problem and of the solutions proposed by different research schools.

The paper is organized in the following way. In section 2, we start by discussing in a general setting what are the main issues to be addressed in the context of emergency control, starting with broad strategic decisions and ending with implementation concerns. Section 3 briefly reviews existing emergency control schemes and Section 4 discusses the main technological changes which are presently observed or will be in the near future, both in the context of hardware and software. Section 5 reviews research work presently carried out which may offer solutions to new and old problems. Finally, the last section summarizes the overview. Notice that we do not try to stick to any conventional way of looking at the problem, nor do we try to provide an exhaustive survey of existing work in emergency control. However, we will provide some additional references for further reading, where appropriate.

## 2 ASPECTS OF SECURITY CONTROL

Here we attempt to define what security control is all about, in a general way. Security control is decision making at different levels of detail and in different time frames. It starts in (national or international) regulation bodies which define security criteria and auditing principles, and ends by paying back customers who have suffered economic loss due to insecurity. Let us briefly enumerate the steps as they appear in logical sequence.

**Security standards.** The explicit definition of security standards is needed in order to set targets for security control. Clearly, security standards will depend on the role played by the electric energy system in the overall economy, as well as on political choices. The standards definition must comprise the specification of the desired levels of reliability, of the means associated to reach the stated objectives, the rules for allocating resulting costs and the auditing mechanism used for verification. Generally, at this level it is also decided which entities (private or public) are technically in charge of meeting the security standards.

**Research.** Research basically aims at understanding how electric power systems behave, in order to provide predictive models which may be used at the different levels of decision making. Today, the trend in research is clearly towards exploiting information technology (computation, database management, communications), which provides means for improved modeling and security control. Let us notice that since the electric power system is essentially stochastic, modeling should address both physical and probabilistic aspects.

**Long term investment.** Formerly, in the integrated framework, investment decisions were generally taken in a coordinated way, combining expansion of generation and transmission subsystems in an optimal way. Today, in order to favor competition, in most systems the investment of generation is a matter of independent decision making based mainly on business opportunities. Hence, the transmission system investment must follow in order to maintain desired levels of security. Building new lines is for the time being almost impossible in most developed countries, thus investment might probably focus on improving power system monitoring and control, by exploiting modern communication possibilities and power electronics.

**Maintenance planning.** Decision making aims at choosing maintenance plans in such a way that availability is maximized in periods where higher traffic on the system is expected. Again, since the generation subsystem is operated independently by a certain number of agents, there will be increased needs for probability methods in order to manage uncertainties. Also, in order to reduce uncertainties it will be necessary to be more reactive, in order to adapt maintenance plans smoothly as information becomes available.

**Transaction planning.** In short term (one day ahead, typically) transaction planning, the system structure is essentially fixed and the objective is to arbitrate among conflicting transactions without discrimination and while ensuring system security.

**Operation.** In the control room, the operator receives real-time information which is used in order to coordinate the scheduled transactions, while reacting to unforeseen events (disturbances, outages, unexpected behavior…). Part of the operators' job will be to handle 'slow' emergencies, e.g. related to thermal overload problems or slow voltage collapses.

**Emergency control.** In this category we focus on automatic control actions such as generation tripping, load-shedding, controlled islanding…We will further elaborate on this in the remaining part of the paper.

**Restorative control.** This aims at re-energizing the system after an event which has led to partial or total blackout. Efficient restorative control is necessary in order to minimize outage costs. Clearly, strategies for restorative control need to be coordinated with emergency control schemes.

**Post-mortem analysis.** Generally, after a major blackout it is necessary to find out the main causes and to evaluate the outage costs incurred by the users of the transmission system. Post-mortem analysis will be easier if the appropriate information has been stored during the disturbance and is made readily available to the analysts.

**Financial compensation.** After a major event, it is generally the case that some users should be paid for the economic losses they have incurred due to the consequences of the outage on their business. The inputs to these decisions are the results of post-mortem analysis, contractual agreements (possibly) and the rules for compensation defined in the security standards.

### 2.1 The objective of security control

Now we focus on the actual system control aspects, which concern preventive mode security control, emergency mode security control and restorative control. In the present section we start by formulating the security control problem from a theoretical point of view, which is both global and probabilistic.

#### 2.1.1 Two types of costs for security control

Whenever a (preventive, emergency or restorative) control action is taken, it will essentially imply two types of "instantaneous" costs : the *direct cost* of the control action and the *indirect cost* which models the impact of the control operation on the expected outage cost.[1] For example, if the control action is to increase some reserve, the direct cost is the price of the additional reserve which must be purchased; the effect on the indirect cost could be measured by the resulting reduction of the expected outage cost.

Thus, typically the two cost components will vary in opposite direction (when the direct cost increases the indirect cost should decrease), and the purpose of instantaneous decision making would be to choose the best tradeoff, i.e. the control action maximizing the overall *instantaneous benefit* (e.g. in dollars per unit of time).

Now, since control actions are to some extent irreversible, it is not sufficient in principle to consider only their instantaneous impact. Also, some control actions have infinite instantaneous costs (consider, for example, generator start-up costs) and hence they can be justified only with a dynamic calculation accounting for expected future benefits.

Combining these considerations, we summarize by stating that the primary objective of security control is to tradeoff various control actions possible (given the present state of the system, its control resources, and its expected future), so as to minimize the overall expected present and future costs. Since the power system is stochastic and dynamic in nature, from a theoretical point of view security control is therefore actually a "stochastic dynamic programming" problem.

#### 2.1.2 Modeling outage costs

It is well known that modeling of outage costs is a very difficult problem, mainly for two reasons : (i) the incurred costs depend strongly on the type of customers, and the duration and geographic extent of an outage will affect individual costs in a nonlinear fashion; (ii) the duration and geographic extent of an outage is very difficult to predict given the multiple uncertainties which will play a role (how the system behaves in abnormal modes, how the operator will react during the restoration process...).

We believe however, that it is becoming highly urgent to develop methodologies to evaluate expected outage costs, in order to be able to arbitrate correctly among preventive and emergency control actions and also in order to justify investment in emergency control plans of existing and future power systems.

#### 2.1.3 Uncertainties

Where come the uncertainties from ? Well, according to Murphy's laws[2] everything which is related to the future is uncertain.

More specifically, in preventive security control uncertainties are mainly of two kinds : external events (random processes like weather conditions, tree growing, human actions, market chaos...) and internal system reactions (failures of protections, unexpected load behavior,...).

In emergency control, the main uncertainty concerning external triggering events disappears in part at least, as well as the slower processes such as market trends and operator actions. The other uncertainties, concerning internal behavior will remain in place.

In the restoration phase, the operator is faced with a system in a very unusual situation, and often the way the system will react to his control actions is very difficult to predict.

### 2.2 On the need for decomposition

The global security control problem viewed as a stochastic dynamic programming problem is essentially intractable, for several reasons. For one, there are many control variables which may act in different time scales. In addition, as was already mentioned, the explicit tradeoff between direct and indirect costs is not yet feasible because we still do not have an agreed methodology to determine expected outage costs. Let us consider the practical ways to decompose this problem into more tractable subproblems.

#### 2.2.1 Decomposition by costs

The first level of decomposition which is today carried out concerns the tradeoff between direct and indirect costs. Decomposition by costs consists in replacing the evaluation of indirect costs (i.e. expected outage costs) by an a priori choice of deterministic security criteria.

For example, in most utilities it is decided a priori that preventive control actions should minimize direct costs *under some constraints* which are chosen so as to indirectly limit the long run expected value of indirect costs. These constraints are typically of the $n-1$ type: any preventive state is declared as acceptable from the viewpoint of the indirect costs, if it meets a certain number of constraints with respect to a certain number of postulated contingencies and with respect to a reference model (i.e. the uncertainties concerning the power system behavior are not taken into account explicitly).

The main advantage of this approach is to free the engineer from considerations about probabilistic models, since now the original problem of stochastic dynamic programming is translated into (i.e. approximated by) a deterministic dynamic optimization problem. In the context of real-time (control room) decision making, the latter problem is generally in turn approximated by a static optimal control problem.

Clearly, while this approach has the "tremendous" advantage of feasibility, it makes sense only as far as the constraints, contingency lists and models are chosen so as to reflect correctly the indirect costs. Of course, the deterministic approach is unable to take into account variations in time of probabilities of external disturbances (e.g. due to changing weather conditions) and hence intrinsically suboptimal. Furthermore, we believe that in the future indirect costs might fluctuate significantly due to trading, in a similar fashion as energy prices fluctuate in an open market structure. Hence, there will be pressure to define security constraints in a more flexible way so as to reflect correctly the actual indirect costs.

[1] The indirect cost term is also referred to as the *risk* term or expected severity in the litterature on probabilistic security assessment [6].

[2] By the time of writing this paper, it is still uncertain whether Kirchhoff's laws will be abolished or not, but we are pretty sure that Murphy's laws will survive for a period of time.

Notice that the decomposition by costs also results in the decomposition between preventive and emergency control by associating different sets of constraints to the two subproblems. Typically, preventive control uses constraints defined using the more likely contingencies whereas emergency control is supposed to cover unexpected events.

### 2.2.2 Physical decomposition

As was said in the introduction, the power system is a complex highly nonlinear system. Hence, it is both necessary and possible to decompose problems in various ways. In security control, and more specifically in emergency control, the decomposition can be appropriately made both in space and in time.

**Decomposition in time.** Starting with fast and ending with slow phenomena we enumerate the following subproblems.

**Fast transient behavior.** Loss of synchronism (as well as very fast voltage collapses) need very fast emergency control schemes to be avoided, with triggering delays reduced to a fraction of a second.

**Fast collapses.** Fast voltage or frequency collapses may evolve with time constants of a few seconds.

**Undamped oscillations.** Undamped oscillations may take longer time to build up, between tens of seconds to some minutes.

**Slow collapses.** Particularly, OLTC[3] driven voltage collapse takes typically a few minutes.

**Cascading trippings.** Overloaded line trippings are typically slow enough to allow operator intervention.

Although the above decomposition is classical, it is well known also that there are interactions among the different phenomena. For example, slower phenomena may induce faster ones, or fast control actions may lead to situations where slow control actions become necessary. On the other hand, the structure of a given power system may result in some phenomena being more likely to happen than others : for example, fast breaker tripping has resulted in strongly reducing the probability of loss of synchronism in many systems; however, change in generation patterns may result in new system oscillation modes which had disappeared in many modern power systems thanks to the installation of PSSs[4].

**Decomposition in space.** Some of the above problems have global impact and hence are difficult to further decompose.

Some others (e.g. voltage collapse problems) are inherently local and are easier to decompose in a geographic manner.

However, due to the nonlinear behavior the interactions among phenomena may be sensitive to the way the system is operating. In particular, the geographic extent of the phenomena will depend significantly on the generation patterns, and clearly generation patterns are becoming more uncertain in the future. Hence, we believe that the geographical decomposition has to be re-examined from time to time, and emergency control schemes should be designed in such a way that they can be reconfigured if needed.

[3]OLTC: on-load tap-changers
[4]PSS: power system stabilizer

## 2.3 Implementation concerns

### 2.3.1 Coordination

Decomposition calls for coordination : among different control areas and among control subsystems responsible for different physical subproblems.

On the other hand, it is important to feedback appropriate economic signals to the external part of the power system (generation companies, load aggregators, and large industrial customers) so as to allocate resources in a globally optimal fashion. An appropriate mechanism for feeding such signals back could be provided by flexible transmission charges and contracts for financial compensation of controlled outages.

### 2.3.2 Monitoring

An important part of security control is monitoring the state of the system, recording the various events which appear and metering non-deserved energy at different locations in the system. This information is necessary both in order to take the appropriate decisions in real-time and to carry out the appropriate post-mortem analysis so as to settle for financial compensation and auditing.

Clearly not all the information has to transit in real-time through fast communication channels. However, in order to exploit the information it is necessary to use precise enough and globally synchronised time stamps. The real-time monitoring system should also be designed in a client/server architecture which would allow flexible enough reconfiguration possibilities in the future, as new needs become apparent.

### 2.3.3 Redundancy and closed loop operation

In order to reach a certain level of reliability, the critical parts of the emergency control plan should be duplicated and open loop control should be avoided to the extent possible (which is not always the case).

Closed loop control is in principle more robust with respect to uncertainties, as far as it is using reliable and fast enough communication channels together with appropriate and accurate enough real-time measurements.

The geographical and physical decompositions of emergency control schemes often introduces some natural redundancy into the system : for example if a coordinated global defense plan fails, local devices may still act on in order to mitigate consequences.

### 2.3.4 Local versus centralized schemes

Local schemes are generally preferred because they are intrinsically more robust and less expensive to implement. Also, in some cases the transmission delays would prevent a centralized scheme from operating correctly.

On the other hand, when possible, centralized schemes may be more effective since they would base control actions on a better picture of the system and may exploit a larger set of candidate control actions. They may therefore reduce direct and indirect costs, at the price of more expensive equipment and smaller reliability.

Given the fact that in many actual power systems, existing emergency devices are mainly local devices distributed thoughout the system, it is suggested that centralized schemes may be added on top in order to make better use of the existing devices. The centralized schemes could be used in two different modes: *adaptive mode* where they would be used in order to adapt parameters of the local controllers (say delays and thresholds); *coordination mode* where they would be used in order to handle situations which need coordination (e.g. synchronization) between local controllers.

## 3 EXISTING EC SCHEMES

In order to fix ideas, we will give in this section a very brief overview of existing emergency control schemes, without aiming at being exhaustive. We suggest to consider references [13, 7, 27] for a more in depth analysis of present practices and trends.

### 3.1 Different philosophies

There are mainly to different types of schemes: open loop and closed loop systems.

#### 3.1.1 Open loop

These systems are mainly event driven, in the following sense: in preventive mode (on-line or off-line), simulations are carried out in order to predict how the system would behave under some contingencies and to determine whether and how an emergency control action could solve the problem. Once the emergency control action and the conditions under which it should be applied have been determined, relays are armed in an appropriate way. The relays triggering is then based on the reception of a signal from standard protections. Normally, the scheme acts in an "all or nothing" fashion and results in tripping some generators or loads from the system.

The advantages of the scheme are speed, reliability and predictability, which are essentially of the same order than classical relaying and protections. This is the reason why this scheme may be used to handle both fast phenomena and likely contingencies (see below).

#### 3.1.2 Closed loop

Closed loop systems are based on real-time measurements, sometimes they use specially designed communication channels and measurement devices in order to operate in a sufficiently reliable and fast way.

During the design stage, the appropriate signals and control logics are determined, and in real-time the system will act continuously according to the logic and values of real-time measurements. For example, in a simple under-frequency load shedding scheme, the measurement is local frequency and the scheme will trip a certain percentage of load each time the frequency drops below a certain threshold for a certain duration of time. After the system has acted, it is automatically rearmed, which allows further control actions to be applied if the result is not satisfactory.

The difficulty with such closed loop schemes are the following: (i) for some phenomena it may be difficult to obtain predictive enough real-time measurements; (ii) it is difficult to predict under which conditions the emergency control system will trigger, since this may depend strongly on the disturbances and on the way the system reacts (which are both uncertain). On the other hand, the main advantage, inherent from the closed loop nature, is precisely robustness with respect to uncertainties.

### 3.2 Transient stability

Transient (angle) instability emergency control schemes mainly depend on the structure of the power system and on the type of generation equipment used. For example, for thermal generators fast-valving may be efficient based on real-time measures of accelerations and speeds, while for hydro-generation tripping may be very effective due to the fact that hydro-generation may be restarted quickly and because the discrete nature of this control action is often compensated by the smaller size of individual generators.

One of the most sophisticated systems presently in place is the system used by Electricité de France [32]. It consists basically of three subsystems:

**Generation control:** transient excitation boosting and fast-valving in thermal power plants based on acceleration and rotor speed, in order to prevent loss of synchronism.

**Local islanding:** out-of-step relay based tripping of lines, using local measurements.

**Coordinated defense plan:** centralized special protection scheme using synchronized phase measurements, coordinating line tripping to isolate a large area loosing synchronism with load shedding in the remaining system to compensate for the loss of power in tie lines.

It is worth mentioning that in this scheme all three levels are of the closed loop type. They are supposed to act only in very abnormal situations.

Another type of scheme, of the open loop type is the generation shedding system used in North-America mainly in hydro-plants [31]. In this scheme, the tripping of a certain number of generators in specific power plants is associated to the tripping of some line in the EHV transmission system. Usually, the determination of control actions and arming conditions are made off-line in the study environment. On-line, in preventive mode, the system is armed or not, depending on state estimator results (e.g. power flow levels in lines) and in real-time only relay signals are used.

Finally, let us mention also the TSC (transient stability control) system developed by Chubu Electric Power Company [21], in Japan. This system combines on-line preventive mode transient stability evaluation to determine the optimal location of generators to be shed for different contingencies, with real-time event driven (i.e. open loop) generator shedding.

### 3.3 Voltage stability

In contrast to transient angle instability which is always a fast and system wide phenomenon, voltage stability problems may be more or less local and of variable speed.

Fast or "short-term" voltage instability problems may appear within seconds after a contingency and are generally driven by loads which have small recovery times (examples are industrial induction motors and power electronics driven devices). In this case, under-voltage load shedding is an attractive concept which may be implemented using existing technology and local devices [30].

Slower "long-term' voltage instability phenomena are usually related to tap changer driven dynamics. In this case, a natural control action is to prevent the tap changers from restoring the voltage at the load side. Usually, tap changer blocking devices use as signal EHV voltages with thresholds and delays appropriately set on the basis of simulations. Given the fact that EHV voltage are not necessarily the best indicators of voltage collapse, and given the fact that thresholds on these latter may be variable, other signals such as reactive reserves might be preferable.

Notice that in the case of slower voltage instabilities, the objective of automatic emergency control may be reduced to slow down the phenomena enough to allow manual (operator driven) control to take place in time. Operator control may result in load shedding or start-up of fast local generation if available. Another possible automatic control action which may be used in order to mitigate slower voltage collapse is secondary voltage control, comprizing coordinated changes in reactive generation of synchronous machines and static var compensators as well as switching of reactive compensation (capacitors or reactors). Also, because the phenomena are essentially quasi static, this type of emergency control scheme may be centralized and implemented through regional control center SCADA[5] systems.

### 3.4 Frequency collapse

In a large interconnected system, frequency collapse is generally the result of islanding and thus appears in practice only when other problems have already occurred (e.g. loss of synchronism or cascading losses of lines). On the other hand, in a smaller isolated system frequency collapse would be the result of loss of generation above the primary reserve. Normally both events are very unlikely to happen or at least highly unpredictable. Hence, event driven emergency control is not very appropriate.

Thus, typically emergency control is based on real-time measurements of frequency and its derivative [15]. A notable exception is the coordinated defense plan of the EDF system, where islanding of an area exporting a large amount of power is synchronised with load shedding in the external part of the system [32].

### 3.5 Thermal overloads

Upon the inception of abnormal contingencies, thermal overloads may occur in the EHV system. The time constants depend on the type of equipment and the importance of the overload : lines may support overloads during several minutes (depending on weather conditions) while transformers will generally trip after a few seconds.

In general, overload tripping starts slowly but it may induce quickly accelerating cascading events. Once the cascades of overloaded line tripping starts, it is generally very difficult to stop it, in particular because it may induce voltage collapses and result in undervoltage trippings of machines. So, the main difficulty is to reduce quickly enough the power flows in the overloaded lines so as to prevent it from tripping and induce cascades.

Often, the slower emergencies are handled by direct operator intervention (e.g. by shedding load or generation), but in some cases automatic emergency control devices have also been implemented in order to avoid cascading trippings.

### 3.6 Synthesis

The preceding brief overview of existing strategies and systems for emergency control aimed at highlighting the diversity of problems and approaches, and the fact that although there is a logical approach to decompose the problem, its solution is made difficult due to interactions and uncertainties. Among the main uncertainties which interfere with emergency control let us mention load behavior and the unreliability of independent generation's solidarity, which may be expected in the future.

Also, the complexity of the protection systems installed in modern power systems results in a certain brittleness of the overall system. For example, when examining the large blackouts which have occurred in the past, it is generally the case that among the underlying causes one finds unexpected behavior of some protection devices, either due to internal failure or due to mis-tuned parameters.

### 3.7 Further reading

In addition to the already mentioned references we suggest the following publications on existing emergency control systems [3, 28, 2, 8, 11, 1, 25].

## 4 TECHNOLOGICAL OPPORTUNITIES

In this section we will briefly discuss the main technological factors which may influence how emergency control will be tackled in the future : modeling, probabilistic approaches, computing power, direct control methods, communications and measurement techniques.

Some of these possibilities will be illustrated explicitly in the last section of the paper.

**Measurement devices.** Low cost of hardware already makes it possible to improve significantly the real-time picture available to emergency control systems.

For example, synchronised phasor measurement devices have been installed throughout the WSCC system in order to record huge amounts of detailed and precise measurements in real-time. This information may be used in order to improve dynamic models and as input signals to emergency control schemes [5].

[5] SCADA: supervisory control and data acquisition

**Communications.** Cost of standard communications decreases and more significantly flexibility and speed increases very quickly. Most present communication systems used in power systems have been designed long ago in a static hierarchical way.

With today's technology it becomes possible to reconfigure communication servers and clients in real-time. For some of the emergency control problems, it would be possible to use Internet technology in the near future, which would allow for low cost highly flexible communication links between substations and control centers.[6]

**Power electronics.** Given the fact that transmission systems will be operated and planned independently from generation and load, the possibility to increase the flexibility of the transmission system through the use of power electronics may play an important role in the future.

Although the investment in FACTS[7] devices is not as fast as anticipated, we may foresee that in the future this technology will become more or less unavoidable.

**System theory methods.** Recent progress in system theory and simulation techniques makes it possible to exploit more realistic models in the design of emergency control schemes.

For example, on-line DSA[8] becomes slowly a reality. On-line DSA may be exploited in the future in the context of both preventive and emergency control.

**Computing hardware.** Low cost and ever increasing speed of computers makes the use of simulation easy. In most applications of security control there are huge opportunities for parallel computations provided that some additional tools are developed.

**Databases.** Database technology has evolved in the recent years so as to allow the storage and efficient retrieval of huge amounts of information in geographically distributed repositories.

The existence of such huge amounts of data accumulated through time in various fields has led to the development of a new field called "data mining" [19]. Data mining basically allows one to extract synthetic knowledge from large databases using statistical methods based on automatic learning.

In the context of emergency control, data mining could be used in order to improve models and make better use of existing simulation tools at the design stage [18]. This is further discussed below.

**Information theory.** Information theory was founded by Claude Shannon immediately after the second world war. Since then, it has been among the main responsibles for the progress in informatics and communications in this century. It provides the theoretical and practical tools to asses the value of information in decision making, to study the effect of uncertainties and the means to fight against random behavior of systems.

[6]This is not meant to replace but rather to supplement existing communications.

[7]FACTS: flexible AC transmission systems

[8]DSA: dynamic (voltage or transient stability) security assessment

In particular, information theory provides high level concepts in order to exploit probabilistic models and control stochastic systems. Among the recent developments in information theory we may mention efficient channel coding methods, automatic learning theory and application of information theory in game theory and to stock markets [9].

More specifically, we believe that the use of information theory in emergency control may allow one to identify appropriate measurements for emergency control schemes, and to evaluate the technical and financial benefit of introducing redundancy and adaptability in the existing defense plans.

Information theory is also at the basis of automatic learning techniques which will be further discussed in our practical context in the next section.

## 5 PRESENT RESEARCH DIRECTIONS

In this last section we will discuss some recent work which has been carried out at the University of Liège in the context of emergency control. We use this work in order to illustrate different philosophies, which we believe representative of work carried out by many teams. Unfortunately, during the writing of this paper, time was too short to collect more references of other related work. Hence, we appologize for not citing this work.

### 5.1 System theory based approaches

In this category we classify those approaches which are mainly based on the use of analytical models or on the exploitation of principles from system theory.

#### 5.1.1 Voltage collapse

We briefly summarize the philosophy behind the work reported by our colleagues in [17, 16].

**Optimal load shedding.** Reference [17] describes a method based on the use of a fast long-term voltage instability simulation tool called ASTRE. By its very nature, the tool focuses on long-term voltage instabilities, i.e. those driven by OLTC devices and possibly thermostatic loads.

The idea consists in using information gained from the simulation of an unstable system trajectory in order to:

- identify the instability mode, which is defined as the point in the load power space where the system crosses the bifurcation surface (i.e. the bounding surface of the region of existence of a stable operating point) together with the normal vector at this point;
- determine from the above information and from the point in the load power space characterizing the pre-disturbance load value (load demand), an appropriate direction of control in the load-power space. In practice, this takes on the form of a list of candidate buses ranked by decreasing efficiency of load shedding;
- determine the minimal amount of load to be shed at each bus, for a given delay of load shedding and taking

into account the optimal unconstrained control direction together with constraints (amount of interruptible load at each bus);

- the procedure is repeated for different delays in order to find the best delay in order to minimize the total amount of load shed.

In this procedure, the instability mode is thus obtained as a direct by-product of a single simulation. On the other hand, optimal values of amount of control and delays are obtained by an iterative procedure which relies on repetitive simulations, which are feasible thanks to the efficiency of the used simulation tool.

One of the interesting observations reported in the above reference [17] is the fact that the amount of load shed (i.e. the resulting outage cost) is strongly dependent on the delay used for deciding when to act. On one hand, load shedding should take place as late as possible in order to avoid undue action (in low voltage but stable cases) and allow other possible control actions to be taken (e.g. compensation switching, where available). On the other hand, it can be shown that beyond some point in time, the longer one wait to shed, the more one has to shed. This point in time may vary quite a lot with the disturbance. For severe disturbances it may be required to shed some load right after the disturbance (after electromechanical oscillations have died out).

On the other hand, it is well known that early detection of voltage instability is difficult, since it takes some time to observe that EHV voltages decrease. Also, the speed with which the system will go towards the bifurcation surface will depend in practice on the way the load responds to voltage drops. Hence clearly, delays and even instability modes may be difficult to asses given the fact that load models are highly uncertain.

**Design of emergency control devices.** In [16] the author suggests how to combine the above method with heuristic search (genetic algorithms are suggested by the author as a nice tool in this case), in order to tune parameters of a "postulated" control device so as to shed an optimal amount of load. The postulated control device is supposed to operate in closed loop; it may either be an existing scheme or one proposed by the design egineer during the overal design process.

The idea is to use the above method in order (i) to determine the amount of load to shed for a set of unstable scenarios; (ii) to use the simplified simulation tool ASTRE in order to check whether, for a given choice of the control device parameters, the system is stable or unstable.

The resulting control device tuning may require a very large number of simulations; however, since this task is carried out off-line and may be parallelized quite easily, we do not see any major difficulty in terms of computantional feasibility.

**Discussion.** One advantage of the above approach is its generality: it may be in principle used for any kind of control device structure (although the tuning may become overwhelming if the number of parameters to tune becomes very large). While focus above is on load shedding, the method may be extended to handle other control actions such as reactive compensation switching and fast generation start-up.

The above methodology shows how progress in dynamic simulation tools, may be used to select, in a more or less automatic way, parameters of controllers. It is hence representative of research carried out by different teams throughout the world. For exemple, reference [24] describes a similar idea to use time domain simulation and optimization in order to determine control parameters for a special stability control system against loss of synchronism. Other research work was carried out at CEPEL in the context of coordinated and robust tuning of power system stabilizers [29].

One main drawback of simulation based controller or protection tuning is related to modelling uncertainties and due to the fact that the simulations have to be carried out for a certain number of postulated contingencies. Of course, in principle the method may use a sufficiently broad range of simulation scenarios, including various load models so as to yield a sufficiently robust design. On the other hand, it would be interesting to be able to identify also the structure of the controller (which measurements to use, and how complex de set of rules should be). How to do this in a very general and flexible way is precisely the topic of section 5.2, which suggests that the simulation scenarios should be sampled using a properly desgned probabilistic model, and that the design and validation of controllers may be achieved using data mining tools and automatic learning to extract information from database of simulated scenarios. Automatic learning methods are able to identify the appropriate measurements and adapt the complexity of extracted rules to the information contained in the simulated scenarios (problem complexity and representativity of the data base).

#### 5.1.2 Loss of synchronism

Let us describe another research presently pursued at the University of Liège, in the context of transient angle instability emergency control [37].

Here the idea is to use real-time measurements of the dynamic state variables of the system in order to determine closed loop control actions. In the most simple scheme, the method's principle merely consists of using real-time measurements of "synchronous" machines' angles, speeds and accelerations, in order to predict whether the system is in the process of loosing synchronism or not. In order to predict instability the real-time measurements are combined using the SIME method [38], which identifies the mode of instability (critical cluster of machines) and provides indications on how much and which generation to shed. The overall system may be used in a closed loop fashion, which makes it robust with respect to modeling uncertainties and types of contingencies.

The main difficulty with the present scheme is related to telecommunication delays, which may reduce the speed of the control system to the extent that it becomes ineffective. On the other hand, the method in its present status is only able to handle control actions which act on the active power of generators. However, other controls such as SVC and generator voltage boosting, fast active power re-routing using FACTS and DC line modulation, dynamic breaking and SMES[9] should be considered also

[9] SMES: superconducting magnetic energy storage device

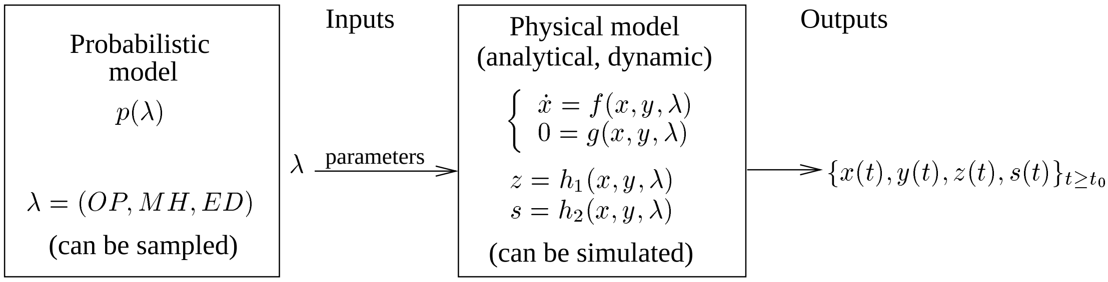


Figure 1: A priori information : probabilistic model and physical model

in the future.

Thus, further research is needed in order to determine appropriate strategies to implement this type of control in practice. Among the topics to be considered we mention the trade-off between local and centralized control, the combination with open loop control in case of very fast loss of synchronism and the design of other types of control actions.

### 5.2 Automatic learning approaches

Another research direction which is essentially complementary to the system theory type of methods described above, concerns the application of automatic learning to the design of emergency control devices. Automatic learning based approaches to emergency control rely on a general statistical framework, which has also been applied in the context of other power system problems, notably preventive security assessment. We will describe below the work carried out in collaboration between the University of Liège and Electricité de France [35], and at the end of this section we will mention other relevant work.

#### 5.2.1 Overall principle

The approach consists in two main steps : database generation using Monte-Carlo simulations of dynamic security scenarios, and database analysis using automatic learning [35]. Note that the Monte-Carlo approach is well suited to the intrinsically probabilistic nature of the problem (think about the random nature of external disturbances, failures of protection devices, mistuned settings…). On the other hand, automatic learning techniques are (by definition) designed so as to separate predictable information from the random component.

As sketched generically in Fig. 1, the Monte-Carlo simulations require two models : the probabilistic model (for random sampling), and the system dynamic model (for numerical simulation).

The probabilistic model (see Fig. 1) represents a priori knowledge about initial operating points (OP), external disturbances and inputs (ED) and other modeling parameters used in a dynamic simulation (MH). Notice that this scheme allows one to represent probabilities of failures of protection devices, ranges of possible model parameters of external systems or aggregated load areas…. All this information is symbolized by a parameter vector ($\lambda$ in Fig. 1) which defines a simulation scenario, and is fed later on into the physical model, in order to simulate the corresponding trajectory.

The design of the probabilistic model is generally the most difficult and at the same time the most important modeling step in this approach. The chosen probability distributions incorporate all prior knowledge as well as the definition of the range of conditions which the study aims to cover. In addition, the probability distributions may be biased in order to increase the probability of sampling those parts of the space which are interesting (e.g. close to the security boundary).

The dynamic model is as usual a set of differential and algebraic equations which define the analytical relationships among states, parameters, time, measurements (denoted by $z(t)$ in Fig. 1) and scenario severity indicators (denoted by $s(t)$ in Fig. 1). For instance, in the context of defense plan design, the candidate measurements would be all those variables which can be used as inputs by the emergency control scheme, whereas the indicators would denote the information which would be observed in case no control action is taken (e.g. expected outage cost). Thus in order to design a triggering rule, it is necessary in some way to predict the future values of the scenario severity $s$, given present and past values of measurements $z$. In general, $S$ and $Y$ are random variables (actually random processes). Thus, at some time $t$, a synthetic model is used to predict $S$ at some future time, $t' \geq t$, using the already observed values of measurements $\{z(\tau)\}_{\tau \leq t}$. This is suggested in Fig. 2, where the estimate is provided by the conditional expectation of this random variable given the already observed values of $Z$ (notation $\hat{s}(t') \approx E_{S|z}\{S|\{z(\tau\}_{\tau \leq t}\}$).

Such a prediction model provides normally only an approximation of this conditional expectation, which, because it can not be computed analytically in practice, must be estimated from a random sample of input/output pairs. Thus, as is suggested by Fig. 2, the design of such prediction models is carried out in the presented approach using automatic learning applied to random samples generated by Monte-Carlo simulations. As we will see, this requires, for each indicator variable which has to be predicted, the propper identification of relevant measurements (those parts of $y$ which carry indeed information about the future value of $z$) and the design of a synthetic model which will estimate severity as precisely as possible.

Notice that in practical applications (see also below), both $z$ and $s$ are vectors of variables which combine discrete (breaker status, relay trip…) and numerical information (voltage magnitudes, amount of load shedded, …).

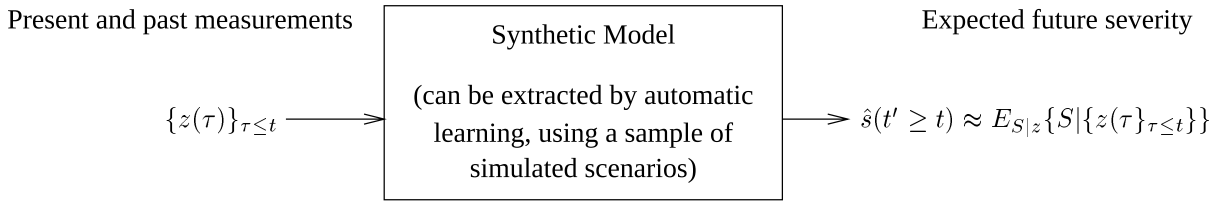


Figure 2: Information extracted by AL : expected value of future severity given past measurements

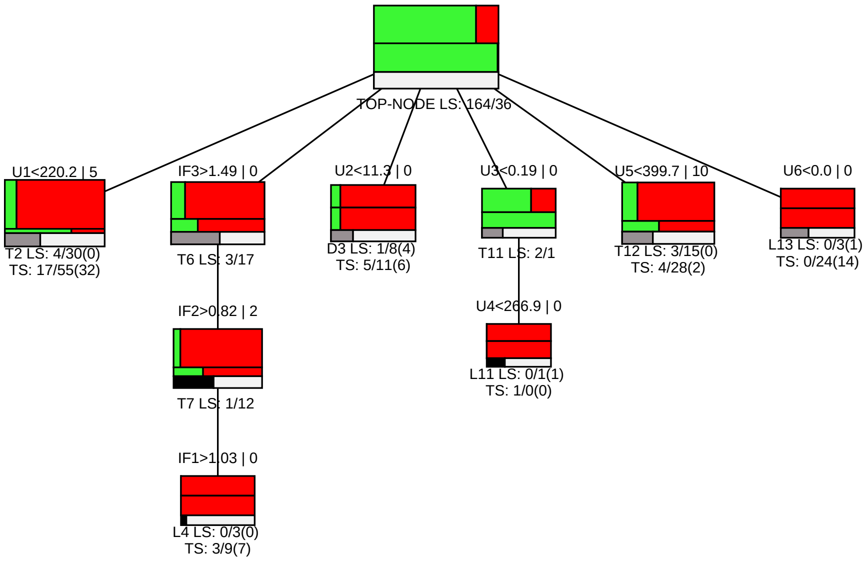


Figure 3: Voltage collapse prediction tree

### 5.2.2 Toolbox of AL methods

We will not provide any details about automatic learning methods per se (see for example [34]). Rather, we mention several complementary methods which can be used in practice. We will distinguish among supervised learning (which aims at building models able to predict some selected output variables on the basis of some particular input variables) and unsupervised learning (which aims at discovering similarities, in the form of groups of similar scenarios, or sets of correlated variables).

In the realm of supervised learning we mention the following methods:

- Decision and regression trees which are able to provide interpretable information, in particular identify relevant input variables for other methods (se also their recent extensions : fuzzy trees and temporal trees [4, 10]).

- Non-linear regression techniques, such as multilayer perceptrons and projection pursuit techniques, which essentially offer the possibility to model continuous input/ouput relationships in a very flexible way.

- Nearest neighbor or similarity based techniques, which offer the possibility to identify in a database scenarios similar to a given one.

In the realm of unsupervised learning we merely mention de classical K-means algorithm (which is used below), hierarchical agglomerative clustering (which may be used to analyse correlations among variables) and Kohonen feature maps (which offer some interesting interpretation capabilities) [34].

**Temporal decision trees.** Note that most of the variables used in the context of blackout analysis and emergency control design are of temporal nature. Thus the proper exploitation of this information may call for data mining methods specifically designed for temporal databases. There is presently a significant amount of research carried out in this context. In particular, we mention here the temporal tree induction method described in [10], which was specifically designed in order to achieve a good compromize between selectivity and anticipativity of detection. Figure 3 illustrates a temporal decision tree built with this method in the context of the study described below. This tree uses temporal input variables (voltage magnitudes and excitation currents of generators) in order to detect as anticipatively as possible a voltage collapse in some part of the system.

The tree detects voltage collapse by percolating scenarios downwards the tree. Along each arc of the tree a temporal test is installed (e.g. on the upper left arc the test is "U1 $< 220.5 \mid 5$", which means that the test becomes true as soon as the voltage at the 225kV bus1 has remained below the threshold of 220.5kV during at least 5 seconds). A scenario will reach a terminal node, in which case a voltage collapse is detected, only if all the tests leading towards that node eventually become true. Note that in such a temporal tree the tests leading to different terminal nodes are not mutually complementary and exclusive.

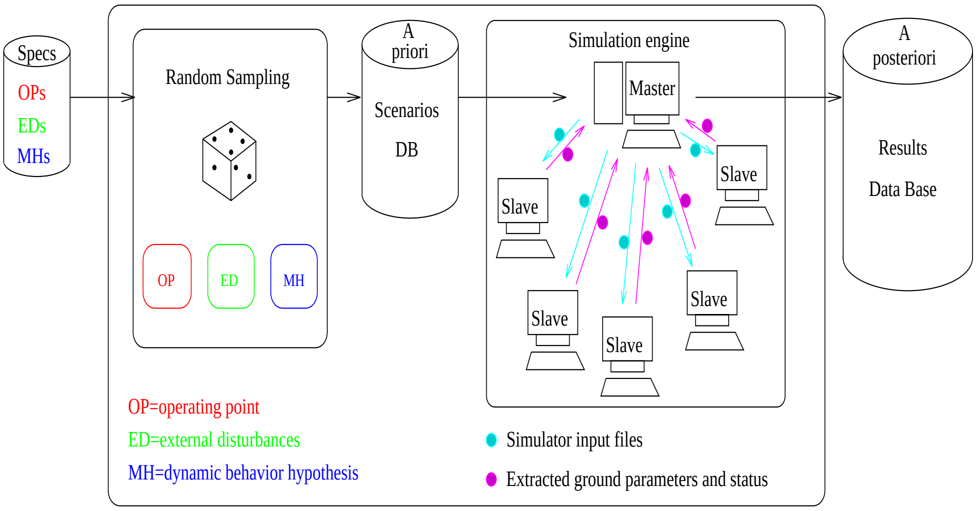


Figure 4: Parallel simulation of scenarios

Hence, a given scenario may never reach a terminal node (in this case it is considered stable). Otherwise, it might reach several terminal nodes, and it is detected as a voltage collapse as soon as it reaches one of these latter.

During the tree building, the method installs tests in a greedy fashion so as to detect as early as possible the truly unstable scenarios, while retaining at its internal nodes all (or a maximum number of) stable scenarios.

### 5.2.3 Summary

To sumarize, the overall approach proceeds as follows:

- Design of the probabilistic and physical models for the particular problem under consideration (expert judgment, statistical information. . . ).
- Random sampling of a certain number of simulation scenarios according to the probabilistic model and numerical simulation of these latter (this is achieved automatically, in parallel to speed up computations, and yields a database of simulation results : system trajectories in the most general case).
- Application of various automatic learning methods to extract information from the latter database, or some of its subsets (this step involves again expert judgment, and a toolbox of complementary automatic learning and information extraction methods, known as data mining toolbox).

### 5.2.4 Comments

Below we make some comments on the current status of the overall approach and provide some hints on research areas which have still to be explored.

**Database generation.** In order to reduce the number of required simulation scenarios, the Monte-Carlo sampling may artificially increase the probabilities of various types of failures, and sample only combinations of severe disturbances. In other words, the probabilistic model may be biased in order to sample predominantly those regions in the measurement space where the variance of the severity indicators is high. In the literature on Monte-Carlo simulations there are several well known variance reduction techniques which may be used for that purpose (see e.g. [26], and also the literature on optimal experiment design [12]).

However, the coupling of such techniques with automatic learning is more intricate and there is still much work to be done in this field (see also the literature on query based learning and reinforcement learning).

For the time being we used the approach by biasing the probability distributions in an ad hoc way, so as to concentrate the simulations in the regions where prior expertise tells us that most information can be gained. Note that without biasing the random sampling it would be necessary to generate huge amounts of scenarios in order to gather some interesting blackout situations. However, while biased probabilities were used for the random sampling, we keep track of the "actual" probabilities while generating the database so as to enable correct interpretation of the results.

**Numerical simulation tools.** In principle the approach can be used with any numerical simulation tool deemed sufficiently accurate for the problem under consideration.

Note however that in the context of defense plan design a rather detailed dynamic model should be used, able to simulate both slow and fast dynamics and various protective devices, so as to assess the performance of the system with good accuracy.

Thus, the database generation generally calls for parallel computations in order to be able to carry out several thousands of dynamic simulations with acceptable response times. In the study on the EHV system of Electricité de France sketched in the next section, 12 CPUs were thus used in parallel for the simulations (see Fig. 4).

**Flexibility w.r.t. prior assumptions.** The database analysis is an iterative "data mining" process. Experts use a data mining tool in order to find out the most frequent blackout modes, and to study relationships among different phenomena. The data mining tool comprises various graphical visualization modules able to show the information contained in the database, as well as a toolbox of automatic learning methods, already briefly discussed. Below we suggest different ways of using them in the context of the proposed approach.

Note that in traditional practice, in order to cope with the overall complexity of the problem, the experts use a divide-and-conquer approach, where the problem is **a priori** decomposed into simpler subproblems on a geographical and/or phenomena-wise base. If the system is undergoing changes this may be misleading, since expertise becomes more quickly obsolete and the "chance" of missing some potential risks is increased.

In the proposed approach, the principle is quite different. The problem is addressed a priori in a global way : the Monte-Carlo probabilistic model is designed in order to represent all reasonably possible causes of collapse (together with their relative probability) and the dynamic simulation model is designed so as to allow the study of both slow and fast phenomena. The geographical and phenomena-wise decomposition is carried out **a posteriori** by looking at the database of simulation results with the help of automatic learning. This allows one in principle to study interactions among various phenomena, if they happen, and to identify the most likely consequences in a more objective way.

However, during the database generation it is not necessary to restrict the amount of information which will be stored and available later for analysis. Actually, it is advisable to keep trace of all variables which could be used either as real-time measurements (inputs to emergency control device triggering criteria) or in order to define the scenario severity. The data mining tools offer the possibility to combine these variables in a very flexible way in order to build synthetic models. Note also that input and output variables may be either numerical continuous (analog states and measurements) or discrete events (fault occurrence, relay tripping, breaker opering/reclosure…).

**Managing large temporal databases.** While a couple of years ago, databases which could be handled by data mining tools were rather small (several tens of MBytes), today it is current practice to apply these tools to very large amounts of data (several hundred GBytes). Since mass storage and CPU power are cheaper and cheaper, there is strong incentive to keep a maximum amount of information from the simulations. Nevertheless, it may be necessary to filter and/or compress the raw outputs provided by the simulation engine.

For example, in the study on the French power system, the total amount of raw simulation results produced during the database generation was about 300 GBytes (sic). In order to bring storage requirements and processing times to an acceptable value, this information was reduced by a factor of about 200 by using appropriate data compression techniques.

### 5.2.5 Identification of collapse modes

Using illustrations from a real study, let us show how unsupervised learning methods may be used in order to find out the various modes of failure of the system. Note that these latter generally involve a combination of external faults with cascading line trippings (overloads), voltage collapse and loss of synchronism, intermingled with the action of various special stability controls already installed on the system.

The approach described was developed using a database generated for the French EHV system [35]. This database contains 1500 scenarios simulated for the study of the South-Eastern part of the French EHV system. The simulation model used about 11,000 state variables and represented in detail the dynamics of the European interconnection surrounding the study area. Each scenario was simulated during a long enough period (about 40-50 minutes) to observe cascading line tripping (overload relays) and their interactions with voltage and angle dynamics. All relevant special protection systems were modeled: coordinated defense plan, islanding schemes, low-voltage protections in substations, controlled generation tripping, under-frequency load-shedding, automatic tap-changer blocking schemes…

The objectives of the study were as follows:

- Identification of the main weaknesses of the system, without prior hypothesis on the dynamic profile of instabilities.
- Identification of (combinations) of disturbances capable of initiating a system collapse.
- For each threatening disturbance, identification of the final consequences and the dynamic profile of the collapse.

**Methodology.** During the study, a methododogy was developed in order to reach the above objective. It goes in 4 main steps:

- Definition of a notion of collapse severity.
  This measures the impact of the dynamics on consumption, generation and transmission in terms of how much equipement of each kind is tripped at a given stage of the scenario. All in all about 30 temporal variables were used in order to provide a picture of scenario severity with a good enough spatial resolution.
- Regrouping scenarios considering the final state (consequences).
  This regrouping was carried out using the K-means clustering algorithm and as attributes the former 30 attributes values at the end of the simulation period (final state severity).
- Subdividing each collapse group according to the dynamics (the main steps of the blackout).
- In depth analysis of each group, in order to characterize:
  - the nature (fast versus slow, voltage versus loss of synchronism, local versus wide area…) and localization of the collapse;
  - the initiating disturbances and main stages of the collapse (e.g. line fault, followed by overload tripping, followed by voltage collapse…);
  - the effect of protections and special control systems.

**Summary of results.** The above analysis resulted in a systematic study of the weak points of the study region. 33 patterns of collapse severity were identified, and 44 dangerous disturbance patterns.

Among the 1500 simulation scenarios, 700 were found to be stable, and the remaining 800 were divided in the following 5 main families

- local voltage collapse;
- regional voltage collapse;
- regional voltage collapse combined with local loss of synchronism;
- wide area voltage collapse combined with area mode loss of synchronism;
- local loss of synchronism.

The detailed analysis of the various collapse patterns allowed us to identify a certain number of reflex rules which could help operators to react in the appropriate way when a collapse starts to develop. This is indeed possible, due to the fact that among the dynamic patterns many start with a cascade of overloaded line trippings finally leading to the loss of a large area. This often leaves enough time for an operator to activate an already prepared load-shedding action which could relieve the overloads quickly enough to avoid the cascading trippings of lines and/or generators.

On the other hand, the database was also used in order to develop anticipative criteria to predict voltage collapse (see e.g. [10], and Fig. 3) in order to improve automatic tap-changer blocking schemes already in place on the system.

**Practical outcomes.** Let us briefly enumerate various practical possibilities which are offered by the presented methodology.

- Assessment of the efficiency of existing protection devices and defense plans (finding out how many adverse circumstances have to occur simultaneously to reach a large collapse).
- Improved understanding of possible interactions of the existing protection devices (are they helping each other, or rather fighting against each other) [14].
- Identification of the structural weaknesses of the system (which aspects of the existing defense plan should be improved in the future).
- Reflex rules for operators (a catalog of "situation / action" pairs which would help operators to recognize a dangerous situation and indicate them possible actions to avoid worse).
- Database of very stressed simulation scenarios of various kinds, which can be used in order to evaluate design options to improve the protection/defense plan.
- Study methodology which can be used again in the future to study other systems or monitor the safety level of the power system.

#### 5.2.6 Related work

In the context of emergency control, automatic learning based approaches have been applied by various research teams, and in particular in the context of out-of-step relaying. We mention the work [36] and [22, 23, 20, 33].

## 6 CONCLUSION

In this paper we have tried to provide a global view of the role of emergency control in modern power systems and various strategies to solve it. In particular, we have discussed two complementary research directions based respectively on system theory approaches and on automatic learning.

We believe that emergency control will become more and more important in the future. On the other hand, we are convinced that emergency control, and more generally security control, should take into account the uncertain and probabilistic nature of large scale power systems. Indeed, emergency control is supposed to opperate in very unusual situations which are not well understood and modeled in many cases, and it is supposed to handle the very unpredictible events which may endanger the operation of a power system.

Probabilistic methods allow one to build and use quantitative models of what we know and what we ignore about the power system and its environment. They allow one also in principle to identify the real risks by combining severities of consequences with probabilities of causes. We are convinced that probabilistic methods, if properly combined with system theory based simulation tools, can provide in the long term more objective and broadly accepted principles to arbitrate among preventive, emergency and restorative control options, and in each case to identify the control actions which would be the most effective in reducing the overall cost.

The combination of probabilistic models and system theory based methods may be achieved in the automatic learning based framework described in the last part of this paper. Its practical feasibility relies on the exploitation of many of the technological opportunities which have been described in earlier sections: parallel computations, database and data mining technology, and in the end information theory. It takes largely advantage of recent progress in the system theory based approaches such as those which have been mentioned in this paper.

**Acknowledgements**

The author would like to thank the input received while writing this paper from several colleagues of the University of Liège, as well as the research support received from Electricité de France in the context of the research carried out in collaboration.

## REFERENCES

[1] CIGRE WG 34.08. *Protection against voltage collapse*. Cigré bochure No. 148, 1998.

[2] M. Begovic and IEEE Potection Aids to Voltage Stability Working Group. Summary of "system protection and voltage stability". *IEEE Trans. on Power Systems*, 94-SM 432-5 PWRD, 1995.

[3] N. B. Bhatt. Field experience with momentary fast turbine valving and other special stability controls at AEP's rockport plant. *IEEE Trans. on Power Systems*, 11(1):155–161, 1996.

[4] X. Boyen and L. Wehenkel. Automatic induction of fuzzy decision trees and its application to power system security assessment. *Fuzzy sets and Systems*, 102:3–19, 1999.

[5] V. Centeno, J. De La Ree, A. G. Phadke, G. Michel, J. Murphy, and R. Burnett. Adaptive out-of-step realying using phasor measurement techniques. *IEEE Computer Applications in Power*, 6(4):12–17, 1993.

[6] TF 38.03.12 CIGRE, R. Marceau, and J. Endreyeni. Power system security assessment. *Electra*, November 1997.

[7] CIGRE TF 38.02.17 convened by C. W. Taylor. *Advanced angle stability controls*. CIGRE, 1999. To appear.

[8] C. Counan, M. Trotignon, E. Corradi, G. Bortini, M. Stubbe, and J. Deuse. Major incidents on the French electric system: potentiality and curative measures study. *IEEE Trans. on Power Systems*, 8(3):879–886, 1993.

[9] T. M. Cover and J. A. Thomas. *Elements of information theory*. Wiley, 1991.

[10] P. Geurts and L. Wehenkel. Early prediction of electric power system blackouts by temporal machine learning. In *Proc. of ECML-AAAI'98 Workshop on "AI Approaches to Time-series Analysis"*, Madison (Wisconsin), 1998.

[11] Y. Harmand, M. Trotignon, J. F. Lesigne, J. M. Tesseron, C. Lemaître, and F. Bourgin. Analyse d'un cas d'écroulement en tension et proposition d'une philosophie de parades fondées sur des horizons temporels différents. In *CIGRE Report 38/39-02, Paris*, August 1990.

[12] J. R. Koehler and A. B. Owen. Computer experiments. Technical report, Standford University - Department of Statistics, 1995. http://playfair.Stanford.EDU/reports/owen/.

[13] P. Kundur and G.K. Morison. Techniques for emergency control of power systems and their implementation. In *Proc. IFAC-CIGRE Symp. on Control of Power Plants and Power Systems*, pages 679–684, Beijing, 1997.

[14] C. Lebrevelec, P. Cholley, J.F. Quenet, and L. Wehenkel. A statistical analysis of the impact on security of a protection scheme on the French power system. In *Proc. of Powercom'98*, Beijing, Aug. 1998.

[15] M. Mandozzi, V. Menditto, G. Morescini, R. Marconato, and P. Scarpellini. Recent improvements of emergency control of ENEL power system in interconnected and isolated operation. *CIGRE report*, 39-302, 1992.

[16] C. Moors and T. Van Cutsem. Conception des systèmes de délestage de charge contre l'effondrement de tension. Private communication, in French, 1999.

[17] C. Moors and T. Van Cutsem. Determination of optimal load shedding against voltage instability. In *Proc. of PSCC99*, 1999.

[18] C. Olaru, P. Geurts, and L. Wehenkel. Data mining tools and applications in power system engineering. In *Proc. of PSCC99*, 1999.

[19] C. Olaru and L. Wehenkel. Data mining. *IEEE Computer Applications in Power*, July 1999.

[20] D. R. Ostojic and G. T. Heydt. Transient stability assessment by pattern recognition in the frequency domain. *IEEE Trans. on Power Syst.*, PWRS-6(1):231–237, 1991.

[21] H. Ota, Y. Kitayama, H. Ito, N. Fukushima, K. Morita, and Y. Kokai. Development of transient stability control system (TSC system) based on on-line stability calculation. *IEEE Trans. on Power Systems*, 1996.

[22] S. Rovnyak, S. Kretsinger, J. Thorp, and D. Brown. Decision trees for real-time transient stability prediction. *IEEE Trans. on Power Syst.*, 9(3):1417–1426, August 1994.

[23] S. Rovnyak, C. Taylor, and Y. Sheng. Decision trees using apparent resistance to detect impending loss of synchronism. Submitted for publication, 1999.

[24] S. M. Rovnyak, C. W. Taylor, and J. S. Thorp. Real-time transient stability prediction - possibilities for on-line automatic database generation and classifier training. In *Proc. of SIPOWER'95, IFAC Symp. on Control of Power Plants and Power Systems*, pages 247–254, December 1995.

[25] RRWG-WSCC. *Voltage stability criteria, undervoltage load shedding strategy, and reactive power reserve monitoring methodology*. Recative power reserve wokr group, Technical Studies Subcommittee, Western Systems Coordinating Council, 1998.

[26] Reuven Y. Rubinstein. *Simulation and the Monte-Carlo Method*. J. Wiley, 1981.

[27] J. R. Smith, G. Andersson, and C. W. Taylor. Annotated bibliography on power system stability control. *IEEE Trans. on Power Systems*, 11(2):794–800, 1996.

[28] M. Takahashi, K. Matsuzawa, M. Sato, K. Omata, and R. Tsukui. Fast generation shedding equipment based on the observation of swings of generators. *IEEE Trans. on Power Systems*, 3(2):439–446, 1988.

[29] G. N. Taranto, A. L. B. do Bomfim, D. M. Falcao, and N. Martins. Automated design of multiple damping controllers using genetic algorithms. *IEEE PES Winter Meeting*, 1999.

[30] C. W. Taylor. Concepts of undervoltage load shedding for voltage stability. *IEEE Trans. on Power Delivery*, 7(2):480–488, April 1992.

[31] C. W. Taylor. Special stability controls and applicable input signals: survey of western interconnected power system experience and applications with emphasis on improving the flexibility of DC transmission. In *Flexible AC Transmission Systems (FACTS 3) Conf.*, Baltimore, October 1994.

[32] M. Trotignon, C. Counan, F. Maury, J. F. Lesigne, F. Bourgin, J. M. Tesseron, and J. Boisseau. Plan de défense du réseau THT français contre les incidents généralisés : dispositions actuelles et perspectives d'évolution. In *CIGRE Report 39-306, Paris*, August 1992.

[33] T. Van Cutsem, L. Wehenkel, M. Pavella, B. Heilbronn, and M. Goubin. Decision trees for detecting emergency voltage conditions. In *Proc. of the 2nd Int. NSF Workshop on Bulk Power System Voltage Phenomena - Voltage Stability and Security, Deep Creek Lake, Ma*, pages 229–240, August 1991.

[34] L. Wehenkel. *Automatic learning techniques in power systems*. Kluwer Academic, Boston, 1998.

[35] L. Wehenkel, C. Lebrevelec, M. Trotignon, and J. Batut. Probabilistic design of power-system special stability controls. *Control Engineering Practice*, 7(2):183–194, 1999.

[36] K. Yabe. "Smart relay", optimization of discrimination rules for relay system. *Revue E*, (2-3):30–33, December 1996.

[37] Y. Zhang, L. Wehenkel, and M. Pavella. An approach to real-time transient stability emergency control. In *Proc. IFAC-CIGRE Symp. on Control of Power Plants and Power Systems*, pages 673–678, Beijing, 1997.

[38] Y. Zhang, L. Wehenkel, P. Rousseaux, and M. Pavella. SIME : A hybrid approach to fast transient stability assessment and contingency selection. *Int. J. of Elec. Power and Energy Syst.*, 19(3):195–205, 1997.