Electrical Power and Energy Systems 71 (2015) 151–159

Contents lists available at ScienceDirect

Electrical Power and Energy Systems

journal homepage: www.elsevier.com/locate/ijepes

Computational framework combining static and transient power system security evaluation using uncertainties

Amélia Yukie Takahata [a,b,1], Marcelos Groetaers dos Santos [a,c,1], Glauco Nery Taranto [b,2], Marcus Theodor Schilling [c,*]

[a] National Operator of the Electrical System (ONS), Rua Julio do Carmo 251, Cidade Nova, Rio de Janeiro, RJ, Brazil
[b] Federal University of Rio de Janeiro (COPPE/UFRJ), Dept of Electrical Engineering, Caixa Postal 68504, Ilha do Fundão, Rio de Janeiro, RJ, Brazil
[c] Fluminense Federal University (UFF), TCE/TEE/IC, Caixa Postal 33024 Leblon, CEP: 22440-970, Rio de Janeiro, RJ, Brazil

ARTICLE INFO

Article history:
Received 29 October 2014
Received in revised form 26 December 2014
Accepted 20 February 2015
Available online 17 March 2015

Keywords:
Computational tool
Probabilistic method
Reliability
Security
Uncertainty

ABSTRACT

This paper presents a simplified but effective procedure to represent power system uncertainties that allow the development of a computational tool to tackle the power system probabilistic security problem from both the small signal stability (SSS) perspective, and the transient stability (TRS) analysis perspective. A set of examples using the New England test-system is presented and discussed. Among the advantages of the suggested method, the following points are evident: (i) the ability to discriminate between the three types of uncertainties (scenarios, fault events, and noise types) that permeate power systems and that are relevant to the system security; (ii) the capacity to use existing traditional tools from both small signal dynamic analysis and transient stability analysis to adapt them easily to the well-established concept of probabilistic adequacy assessment, without resorting to abstruse and hard-to-implement theoretical techniques; (iii) the enormous advantage of usual availability for the required statistical data (no hard-to-collect data are required); and (iv) proposal of a conceptual procedure that renders a highly combinatorial problem amenable to current state-of-the-art hardware resources, within acceptable limits of computational burden. Important practical results that one may wish to highlight are related to the effective representation of noise uncertainties through a straightforward combination of weighted histograms, and the successful performance of the new *Apparent Stability Index – ASI*.

Introduction

According to [1], (*sic*) "the concept of uncertainty is just one category or type of the more general and broader concept of ignorance. It encompasses the ideas of *ambiguity* (the possibility of having multi-outcomes for processes or systems), *approximations* (a process that involves the use of vague semantics in language, approximate reasoning, and dealing with complexity by emphasizing relevance), and *likelihood* (defined by its components of randomness, statistical and modelling). The last subcategory (i.e. likelihood) can be understood in the context of chance, odds, and gambling, having aspects of randomness and sampling." Therefore, this is the subtype of uncertainty that is most commonly used in power systems reliability assessment, and therefore is the only one that will be discussed in this paper.

A broad overview of the literature covering the subject of both power systems adequacy and security, under the influence of probabilistic uncertainties, may be observed in [2,3], indicating that considerable maturity in this field has already been attained. Adequacy analysis considering the treatment of power system uncertainties under the realm of fuzzy variables has also been introduced [4–6], but the probabilistic approach still remains clearly dominant, even in more recent publications [7,8]. Probabilistic security analysis, despite recent advances [9], still lags behind adequacy analysis in useful applications for actual large scale power systems [10]. Several reasons could be mentioned to explain this situation, ranging from unavailability of data and computational tools to theoretical hurdles involving concepts, models, procedures and criteria for diagnosis. One remarkable difficulty related to probabilistic security analysis stems from the intrinsically combinatorial nature of the problem. It is well known that, if these problems are treated naïvely, combinatorial problems may easily render a so called trans-computational problem [11]. In

* Corresponding author. Tel.: +55 21 2274 1391.
E-mail addresses: amelia@ons.org.br (A.Y. Takahata), marcels@ons.org.br (M.G. dos Santos), tarang@coep.ufrj.br (G.N. Taranto), theodor1@netflash.com.br (M.T. Schilling).
[1] Tel.: +55 21 34449640, 21 34449814.
[2] Tel.: +55 21 25628615.

http://dx.doi.org/10.1016/j.ijepes.2015.02.042
0142-0615/

this situation even a fictitious ideal computer, working with a hypothetical lightning speed processing capability and unlimited memory and energy resources, would not provide a feasible solution.

This happens due to the Bremermann's limit, which was derived on the basis of quantum theory, and is expressed succinctly as, *sic* [1]: "no data processing systems, whether artificial or living, can process more than 1.36 E47 bits per second per gram of its mass". This statement is valid even when one considers a virtual Turing machine [12].

However, the practical treatment of a large-scale power system probabilistic security problem may be feasible if a set of simple artifices is recalled. Therefore, the objective of this paper is to present a simplified, but effective procedure to represent power system probabilistic uncertainties that allow the development of computational tools to tackle the power system probabilistic security problem, from both the small signal perspective, and the transient behaviour perspective. A conceptual framework is proposed and a set of examples is given and discussed.

Probabilistic small signal and transient stability analyses: previous approaches

Small signal stability (*SSS*) analysis has been performed in a deterministic and classical way, considering only unitary probabilities or certainties [13], or considering probabilistic state spaces. The probabilistic approach may be addressed with both analytical techniques [14–17], and numerical techniques [18–21] based on standard enumeration, Monte Carlo simulation, or even *ad-hoc* strategies such as the structured singular value theory (μ-analysis) [22,23].

Regarding probabilistic transient stability (*TRS*) analysis, earlier references appeared in the seventies [24,25]. Between 1978 and 1981, a series of seminal papers based on a new proposal were published [26–28], and were only interleaved by an alternative approach [29] in 1979. A new research avenue [30–32] exploring protection uncertainties and Monte Carlo simulation appeared later. Several authors also proposed joint formulations tackling, both the adequacy, and the security problem [33–41], simultaneously. A large set of publications dealing with several other aspects of probabilistic reliability, but also useful to transient stability, were also delivered, covering a plethora of new and diversified strategies, algorithms and concepts. Significant works have been developed and utilized based on arcane or original techniques such as the conditional probabilities [42], health analysis [43], bisection method [44], collocation method [45], Bayes classifier [46], cascading failure analysis [47], copula theory [48], cross-entropy methods [49], and bootstrap techniques [50]. Detailed comparisons between several methods have already been published [51] and research efforts in this area continue thriving [52–54]. Notwithstanding, despite the significant amount of literature, it seems that probabilistic security analysis has not yet gained large acceptance in the industry environment. The applications in actual large systems are seldom found [55]. However, it has been observed that stratifying power system uncertainties according to their type may help develop a quite simplified statistical approach amenable to the probabilistic security assessment, and may still render useful results.

Decoupled view of power systems uncertainties

A useful classification of power system uncertainties associated with power system states may encompass categories related to discrete and continuous/hybrid values, as shown in Table 1.

Table 1
Types of power systems uncertainties.

Discrete state uncertainties	Continuous/hybrid state uncertainties
Scenarios	Noise (small signals)
Fault events	Operational settings

Uncertainties related to *scenarios* (*S*) may be seen as those associated with long term stationary probabilities, calculated through standard statistical techniques. Scenarios are defined as necessarily countable, meaning that they are related to discrete random variables, and desirably with a "slow dynamics" (i.e., its occurrence should be sufficiently slow as to be possible, for practical purposes, to ascribe a probability value to it). For instance, in this paper, a time frame over one minute is selected as the limit for a given state to be ascribed the scenario type uncertainty. In this category, one may find, for instance, the existing grid possible discrete topology states (nodes and branches represented by stations, transmission lines, and transformers). Therefore, scenarios provide information regarding the probabilities of a given element to be in a given operational state, such as *in* or *out*, and are extensively used in traditional adequacy analysis. In this paper, the system topology uncertainties will only be circumscribed to single and double outages of transmission lines and transformers, but higher contingencies may be taken into account if the corresponding statistical data are available. For the sake of simplicity, detailed nodal topologies will not be modelled and each study will be conditioned to a given set of generators in operation. Load level probabilities will also be classified in the scenario category, because the approximate representation of the system load curve through three or four discrete load levels is usually accepted as reasonable. In the developed computational prototypes, up to five load levels can be considered. Hydrological profiles, and other countable uncertainties characterized by slow physical dynamics, may also fall into the scenario category. In this paper, up to five modes of inter-area tie flows representing uncertainties of different hydrological profiles will be considered. Therefore, modelling the uncertainty of a given specific scenario is relatively easy, because it is given by the product of probabilities for the existing elements in each scenario. For instance, let a hypothetical scenario be composed of a given grid topology (i.e., lines and transformers), a specific load level and a given generation dispatch representing one of the system accepted operational profiles. The product of the probability associated with the selected load level times the probability of the network topology times the probability of the chosen operational mode will render, in this case, the final scenario probability.

It is recognized that the automatic combinatorial generation of scenarios may be easy, but it has the drawback of eventually creating unacceptable or unrealistic probabilistic states from the standpoint of the actual stationary system. Disregarding those states would cause a loss of convexity (in this paper, the convexity concept is used in the sense that if unrealistic states are unaccounted for, summing up all of the remaining scenarios probabilities would result in a value less than one). An unviable state may be detectable if, for instance, no convergence is attained when a standard power flow solution is searched, or if a clearly unrealistic configuration is generated. In this paper, the unrealistic states are carefully avoided in the examples given, but when they occur in other situations, they may be counted separately, generating specific probabilistic indexes. Although the recovery of full convexity could be attempted, using skilfully selected repartition heuristics, this approach was not further investigated here.

Uncertainties related to *fault events (F)* are those associated with sudden severe disturbances, such as short-circuits, transient line outages, or any other sudden events, and with possible major