A rare-event approach to build security analysis tools for N-k (k>1) analyses

F. Fonteneau-Belmudes, D. Ernst, L. Wehenkel
University of Liège, Belgium

The usual approach for planning and operation of electric power transmission systems is based on the generally recognized N-1 criterion. However, the continual increase in complexity in power systems and especially the growing number of new interconnections may raise the question of whether this criterion is still sufficient, or even relevant.

For example, when considering the interconnected European transmission system, the probability that there is at least one transmission line disconnected for maintenance operations is rather high. The Transmission System Operators (TSOs) therefore need to be able to perform N-2, N-3 or even deeper security analyses, in order to make sure that it is possible to mitigate the corresponding contingencies while serving the electricity demand and respecting the operational constraints of the transmission network.

When running N-k (k>1) security analyses, a severe computational problem arises. Indeed, when k starts growing, the size of the set of potentially dangerous events becomes rapidly huge, and running a security analysis for every event to find the dangerous ones is often intractable.

Within the extremely large sets of events covered by the N-k context, we assume in this work that the number of dangerous N-k contingencies is very small with respect to the number of non-dangerous ones. Under this assumption, the problem of finding N-k dangerous events becomes equivalent to the problem of finding rare-events in combinatorial search spaces. This equivalence suggests that importance sampling techniques, which have been vastly successful for solving combinatorial problems, could also be used for efficiently identifying dangerous contingencies. With such techniques, it is possible to identify dangerous contingencies by running security analyses only for a small number of events.

In this work, we develop and validate an approach based on these importance sampling techniques for the fast identification of dangerous contingencies within the context of steady-state security analysis. This procedure has been evaluated on some non-trivial test systems, and the results show that it is indeed able to efficiently identify, among a large set of contingencies, the rare ones which are dangerous.