Consequence driven decomposition of large-scale power system security analysis

Florence Fonteneau-Belmudes[*], **Damien Ernst**[*], Christophe Druet[†], Patrick Panciatici[‡], Louis Wehenkel[*]

*University of Liège, Belgium - † ELIA (Belgian TSO) - ‡ RTE (French TSO)

2010 IREP Symposium, Buzios, Rio de Janeiro, Brazil, 1-6 August 2010

Power system security assessment

Power system security assessment = Identifying contingencies/scenarios that could lead to unacceptable operating conditions (dangerous contingencies) if no preventive actions were taken.

Problem may be approximated by running a security analysis for every element of a set of potentially dangerous contingencies.

Size of this set of potentially dangerous contingencies:

- grows with the size of the power system
- grows with increasing uncertainties about the future power injection patterns, load patterns and system topologies.

Question: What should you do when the size of the set becomes so large that you cannot screen every contingency one by one?

Traditional solutions:

- Increase the computational resources (note that the security analysis task can be easily parallelized).
- Use filtering techniques (= simplified conservative analysis techniques) to identify a subset of contingencies on which the full security analysis is carried out.

Shortcomings:

- Do not work in case of very large number of contingencies (say for example 10^{10}).
- Reliable and efficient filtering techniques are difficult to develop.

Our solution

A **generic** approach to identify dangerous contingencies by running a full security analysis for a number of contingencies greater that the number of dangerous ones but much smaller than the number of potentially dangerous contingencies.

Why generic? Work whatever the type of security analysis (e.g., static security, transient stability, voltage stability).

Come atop of existing security analysis tools and can be combined with any of them.

And no magic is necessary for the approach to work...

How does it work:

1. Draw at random a subset of contingencies C.
2. Run a security analysis for every element of C. Add the dangerous contingencies to the set DC.
3. Use the information collected from the security analyses to draw a new set C more likely to contain new dangerous contingencies.
4. If computational resources are exhausted output DC, else go back to 2.

3. Use the information collected from the security analyses to draw a new set C more likely to contain new dangerous contingencies.

Tools needed:

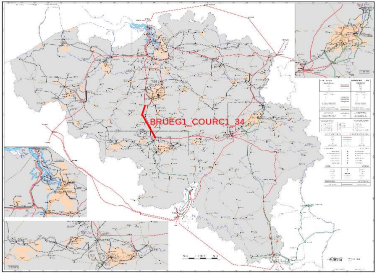
- A post-processor of the security analysis results to associate to a contingency a **severity index** (e.g., amount of load lost in the post-fault configuration).
- A method to embed the contingency space in a **compact metric space** where the severity indices vary in a “progressive way”.

Solution:

1. Identify among the contingencies already analyzed those with the highest severity index.
2. Identify among a family of sampling densities over the compact metric space, the one which is the most likely to generate the contingencies identified at Step 1.
3. Draw a new set C using the sampling density identified at Step 2.

Illustrative example

Test network:



Set of potentially dangerous contingencies: N-1 contigencies, loss of a transmission element, 634 elements.

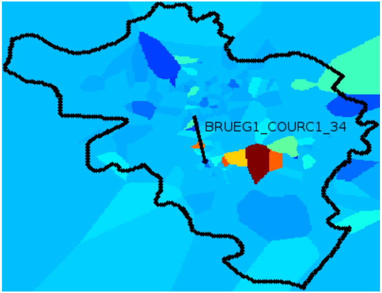
Available computational resources: 125 security analyses (load-flows) can be carried out.

What we want: To identify the 6 contingencies that cause an overload on a critical transmission line.

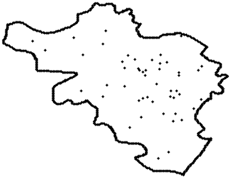
Tools needed:

- A post-processor of the security analysis results to associate to a contingency a **severity index** (e.g., amount of load lost in the post-fault configuration).
- A method to embed the contingency space in a **compact metric space** where the severity indices vary in a "progressive way".

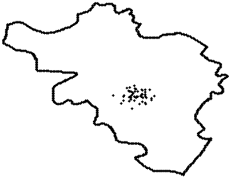
- **Severity index:** overload on the critical transmission line.
- **Compact metric space:** the plane is divided into surfaces corresponding to the contingencies according to their location on the geographical map.



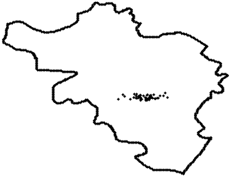
A typical run of the algorithm with multi-dimensional Gaussian sampling densities:



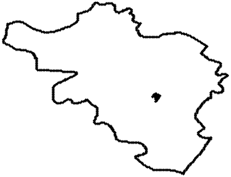
Iteration 1



Iteration 2



Iteration 3



Iteration 4

	Probability of finding at least *n* dangerous contingencies.	
n	Our approach	Monte Carlo
1	0.99	0.69
2	0.90	0.31
3	0.76	0.09
4	0.47	0.04
5	0.20	0
6	0.04	0

Comments:

- Results get even better with the decrease of the ratio:

$$\frac{\textit{number of dangerous contingencies}}{\textit{number of potentially dangerous contingencies}}$$

- Many improvements have already been brought to the basic version of the approach presented here.

Willing to know more...

"*Consequence driven decomposition of large-scale power system security analysis*". F. Fonteneau-Belmudes, D. Ernst, C. Druet, P. Panciatici and L. Wehenkel. In Proceedings of the 2010 IREP Symposium - Bulk Power Systems Dynamics and Control - VIII, Buzios, Rio de Janeiro, Brazil, 1-6 August 2010. (8 pages).

"*Pseudo-geographical representations of power system buses by multidimensional scaling*". F. Belmudes, D. Ernst and L. Wehenkel. In Proceedings of the 15th International Conference on Intelligent System Applications to Power Systems (ISAP 2009), Curitiba, Brazil, 8-12 November 2009. (6 pages).

"*A rare-event approach to build security analysis tools when $N - k$ ($k > 1$) analyses are needed (as they are in large-scale power systems)*". F. Belmudes, D. Ernst and L. Wehenkel. In Proceedings of the 2009 IEEE Bucharest Power Tech Conference, June 28th-July 2nd, Bucharest, Romania. (8 pages).

"*Cross-entropy based rare-event simulation for the identification of dangerous events in power systems*". F. Belmudes, D. Ernst and L. Wehenkel. In Proceedings of the 10th International Conference on Probabilistic Methods Applied to Power Systems (PMAPS-08), pages 1290-1295. Rincon, Puerto Rico, 25-29 May 2008.