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)

Florence Fonteneau-Belmudes, Damien Ernst, Louis Wehenkel

Department of Electrical Engineering and Computer Science
University of Liège, Belgium

PowerTech 2009 – July 2

1. Motivation for $N - k$ analyses

Does the $N - 1$ criterion scale to large interconnected networks?

- it was originally designed for small to middle size systems;

- in large interconnected networks, it is very likely that more than a single power element will be out of use at a specific instant.

⇒ More complex studies ($N - 2$, $N - 3$, ...) have to be performed.

2. Challenges faced

$N-k$ $(k>1)$ studies are combinatorial problems.

$\Rightarrow$ Analyzing individually all possible $N-k$ contingencies is intractable.

Example for a 1000 line electric network:

Type of analysis performed	Number of possible contingencies (loss of lines only)
$N-2$	10^6
$N-3$	10^9
$N-4$	10^{12}

3. Rarity assumption and formulation of the problem

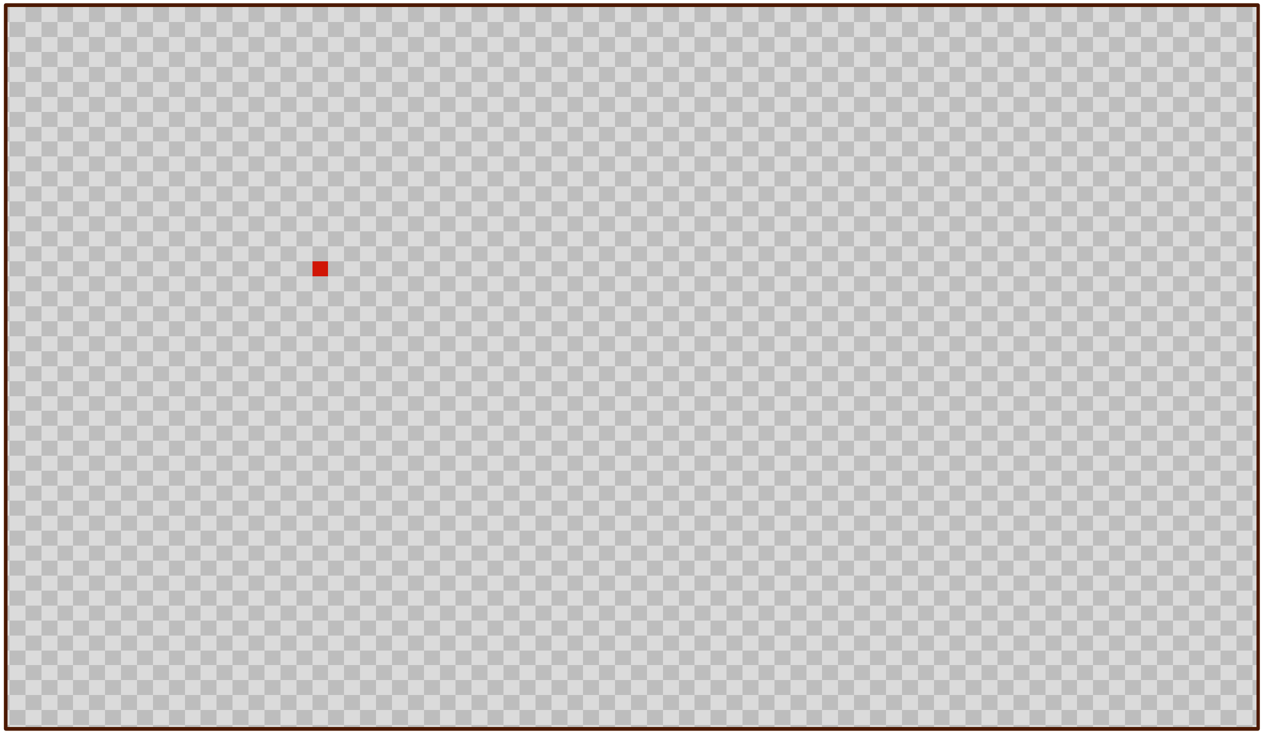
While the set of possible $N-k$ contingencies is extremely large, we assume that the dangerous contingencies are ***rare***.

- the problem of performing $N-k$ security studies can be formulated as a problem of **identification of rare-events in combinatorial search spaces**.

- we suggest to use importance sampling techniques to solve it.

4. Proposed procedure

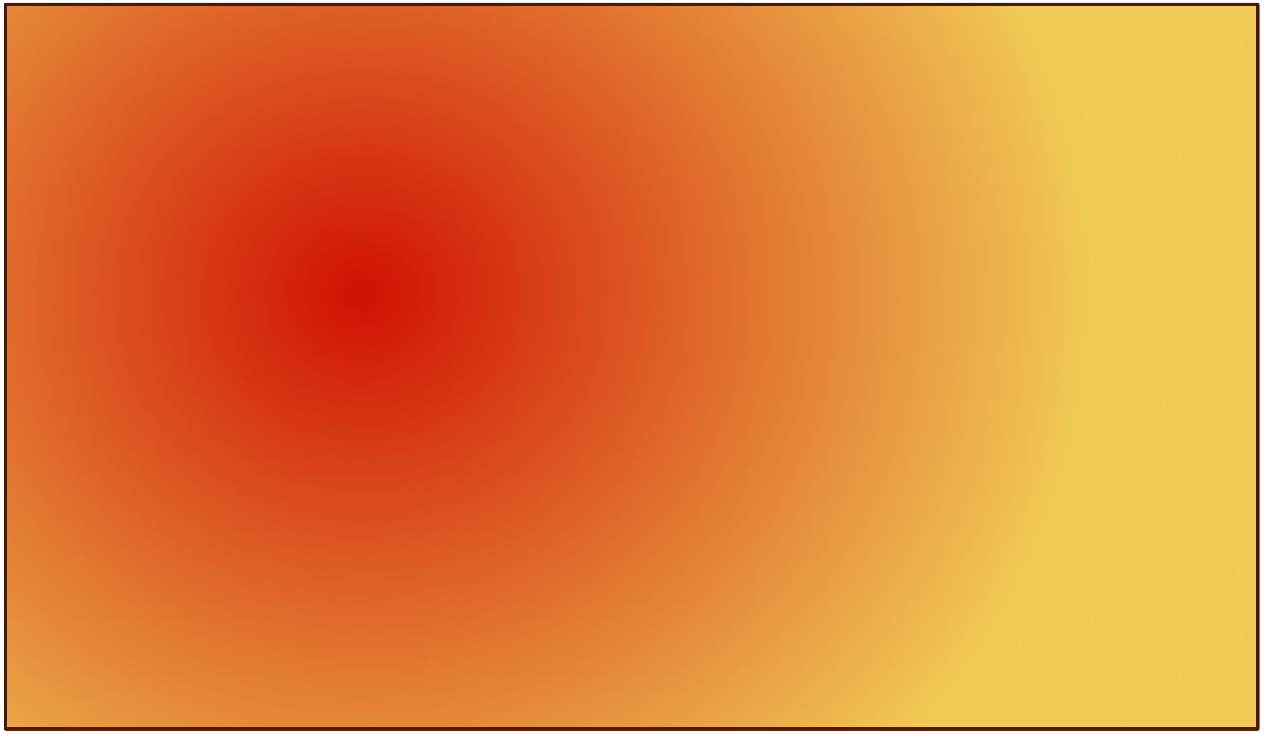
An iterative sampling framework to identify dangerous $N - k$ contingencies: illustration



Contingency space and contingency to identify

4. Proposed procedure

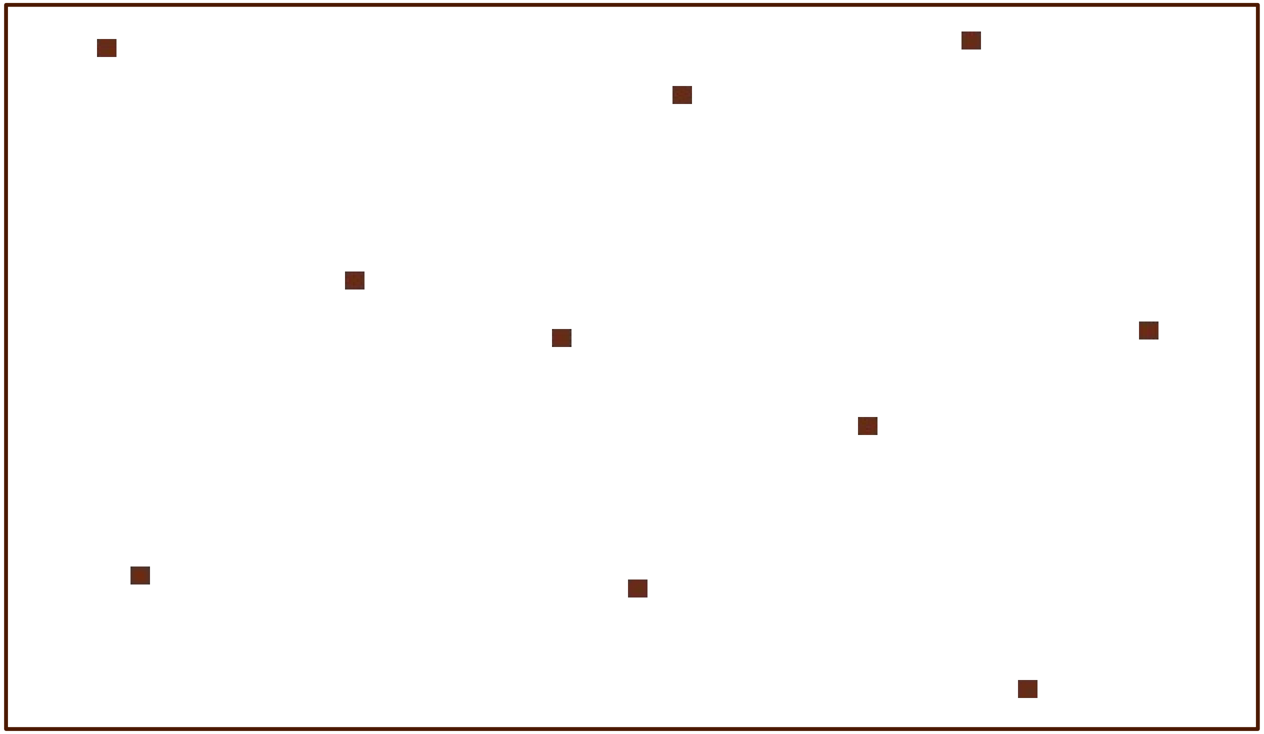
An iterative sampling framework to identify dangerous $N - k$ contingencies: illustration



Profile of the severity function

4. Proposed procedure

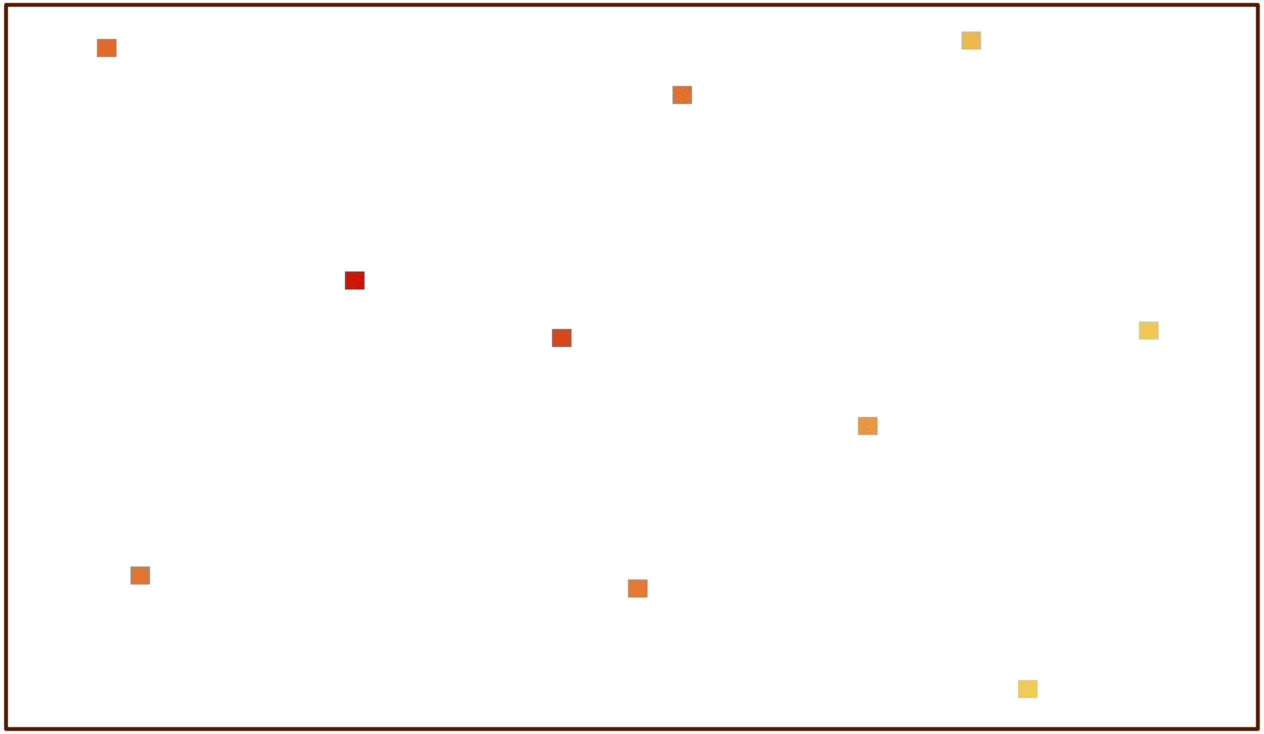
An iterative sampling framework to identify dangerous $N - k$ contingencies: illustration



First sample

4. Proposed procedure

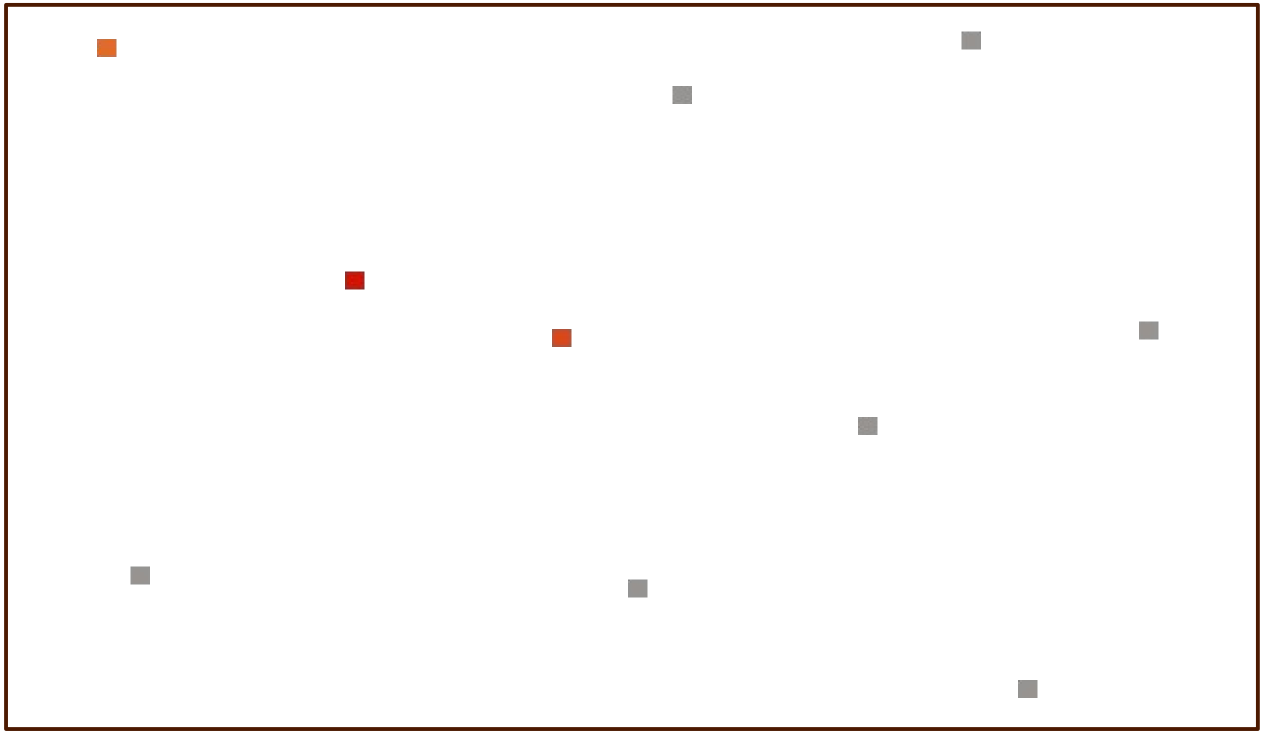
An iterative sampling framework to identify dangerous $N - k$ contingencies: illustration



Evaluation of the severity function

4. Proposed procedure

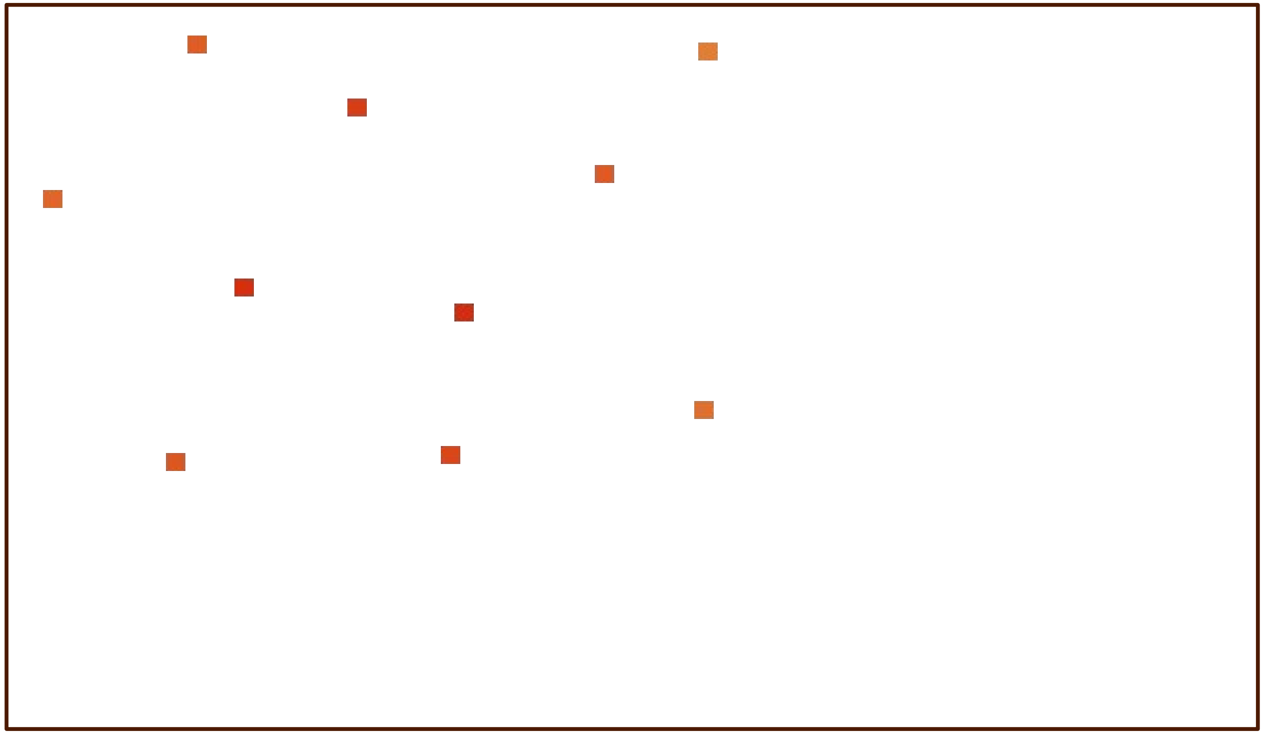
An iterative sampling framework to identify dangerous $N - k$ contingencies: illustration



Selection of the best elements

4. Proposed procedure

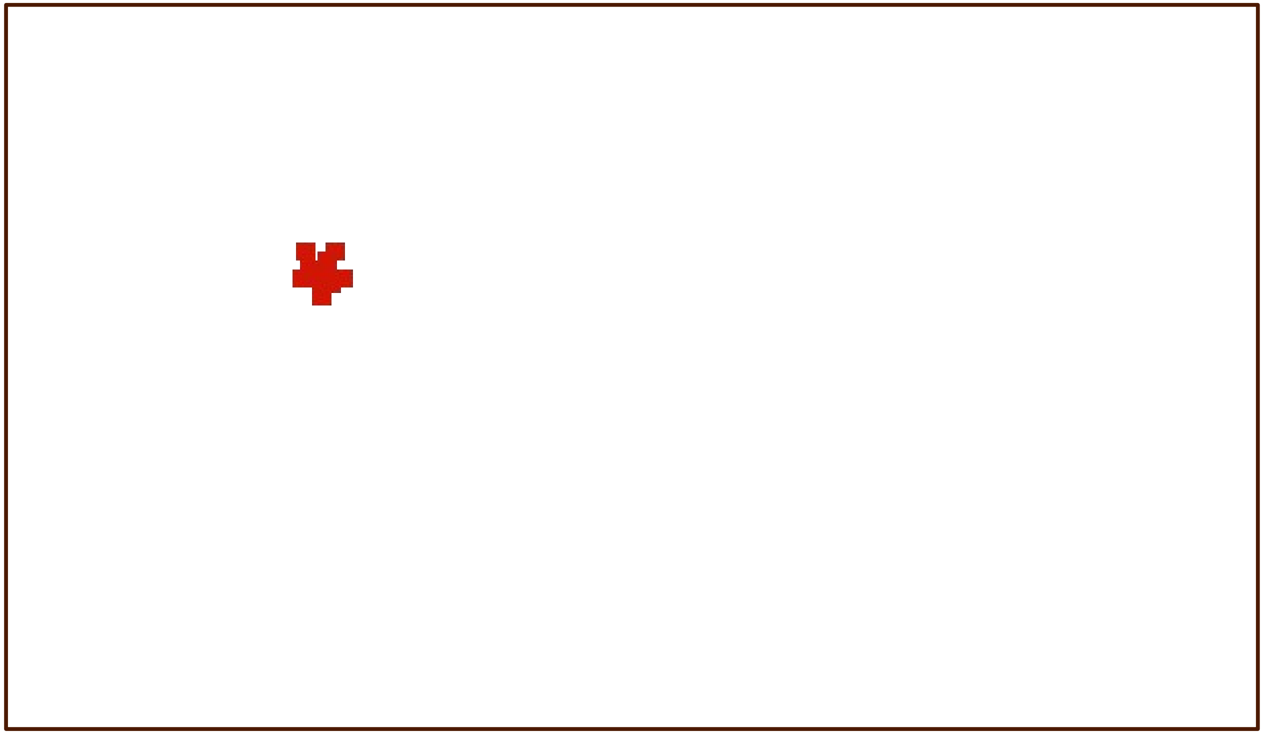
An iterative sampling framework to identify dangerous $N-k$ contingencies: illustration



Second iteration: generation of a new sample

4. Proposed procedure

An iterative sampling framework to identify dangerous $N-k$ contingencies: illustration



Final sample

4. Proposed procedure

Technical aspects

- ***definition of the severity function:***

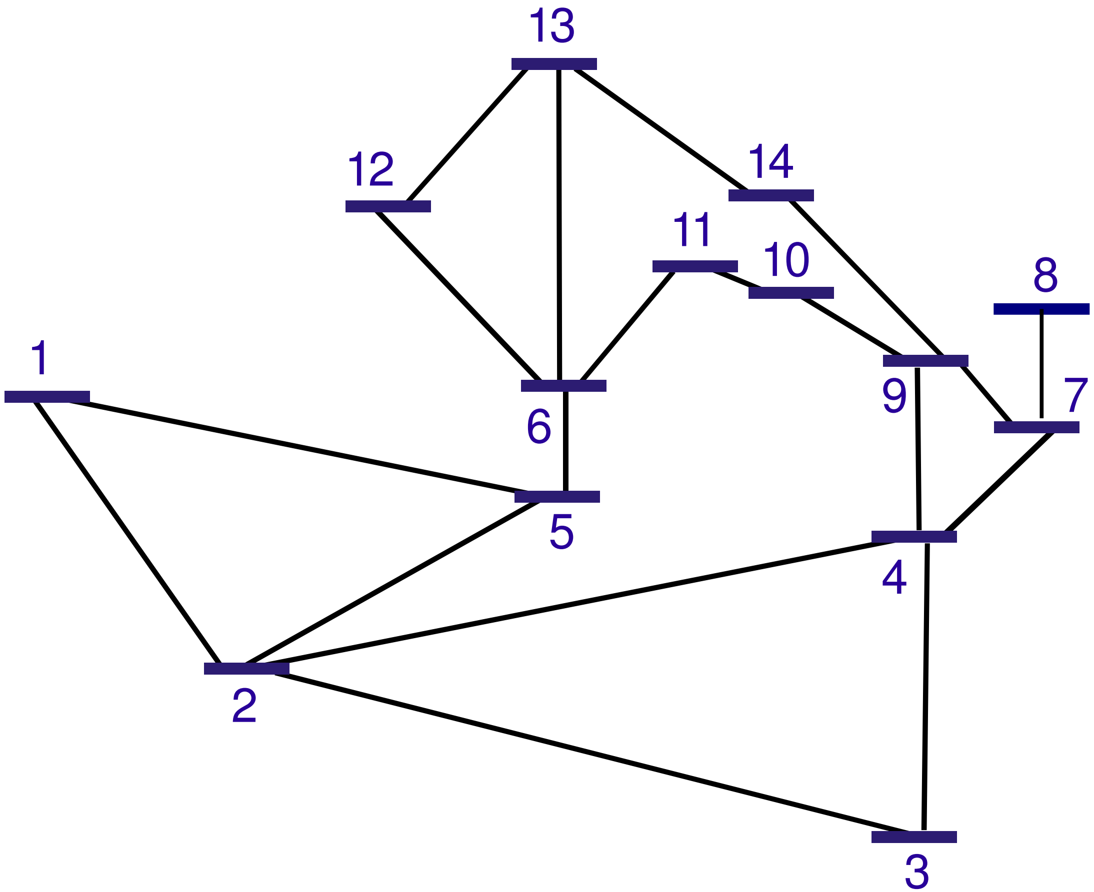
It should reflect how close a contingency drives the system to its stability limit.

- ***metrization of the contingency space:***

A metric has to be defined on the contingency space in order to represent contingencies as points in a low-dimensional space.

4. Proposed procedure

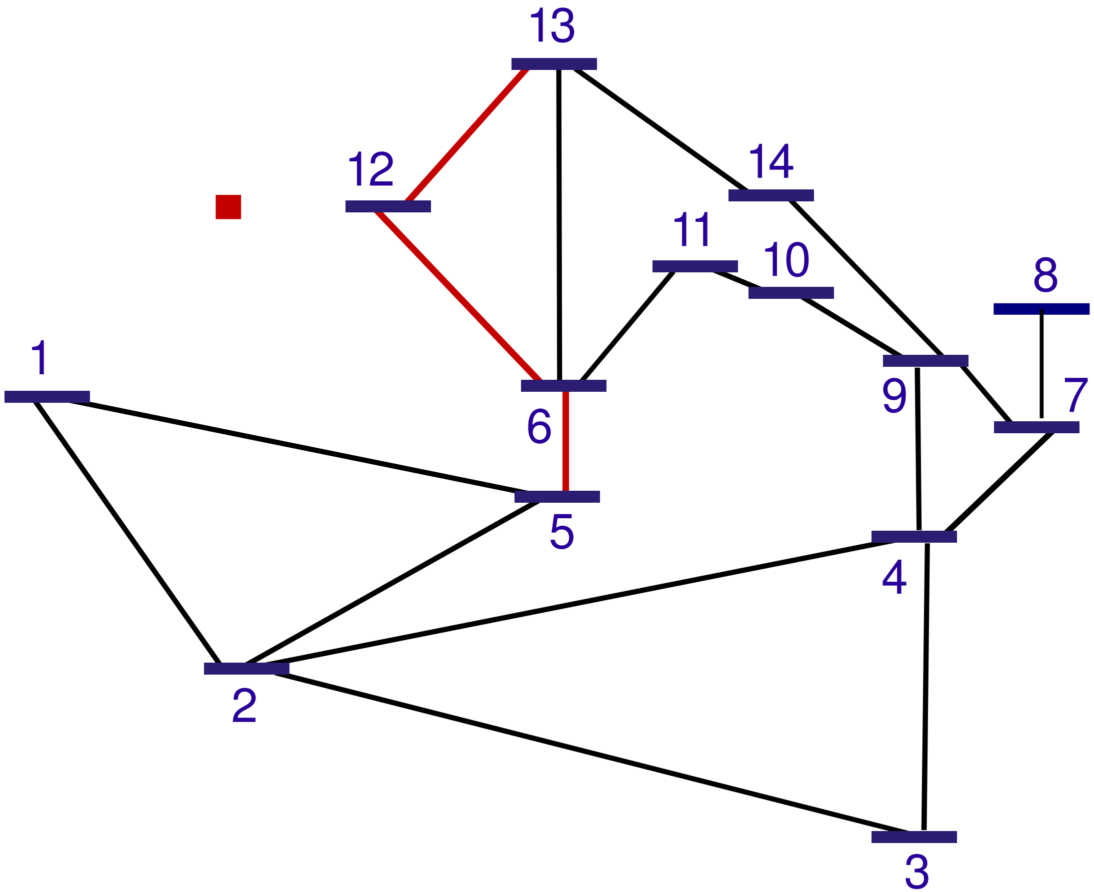
Technical aspects : metrization of the contingency space



Plot of the geographical map of the system (here: IEEE 14 bus system)

4. Proposed procedure

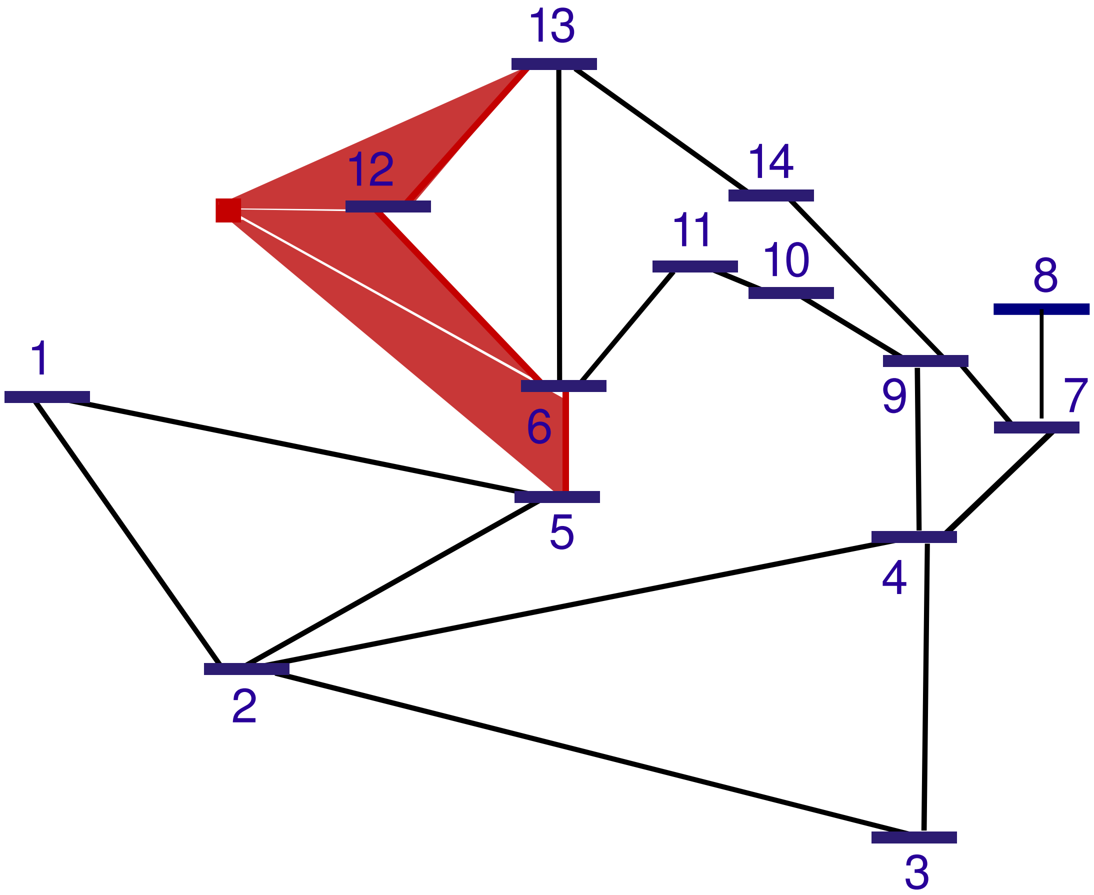
Technical aspects : metrization of the contingency space



Associating a contingency to each point of the space

4. Proposed procedure

Technical aspects : metrization of the contingency space



Associating a contingency to each point of the space

4. Proposed procedure

Technical aspects : metrization of the contingency space

➢ contingencies corresponding to points that are close to each other in the metrized space are expected to have similar effects on the security of the system.

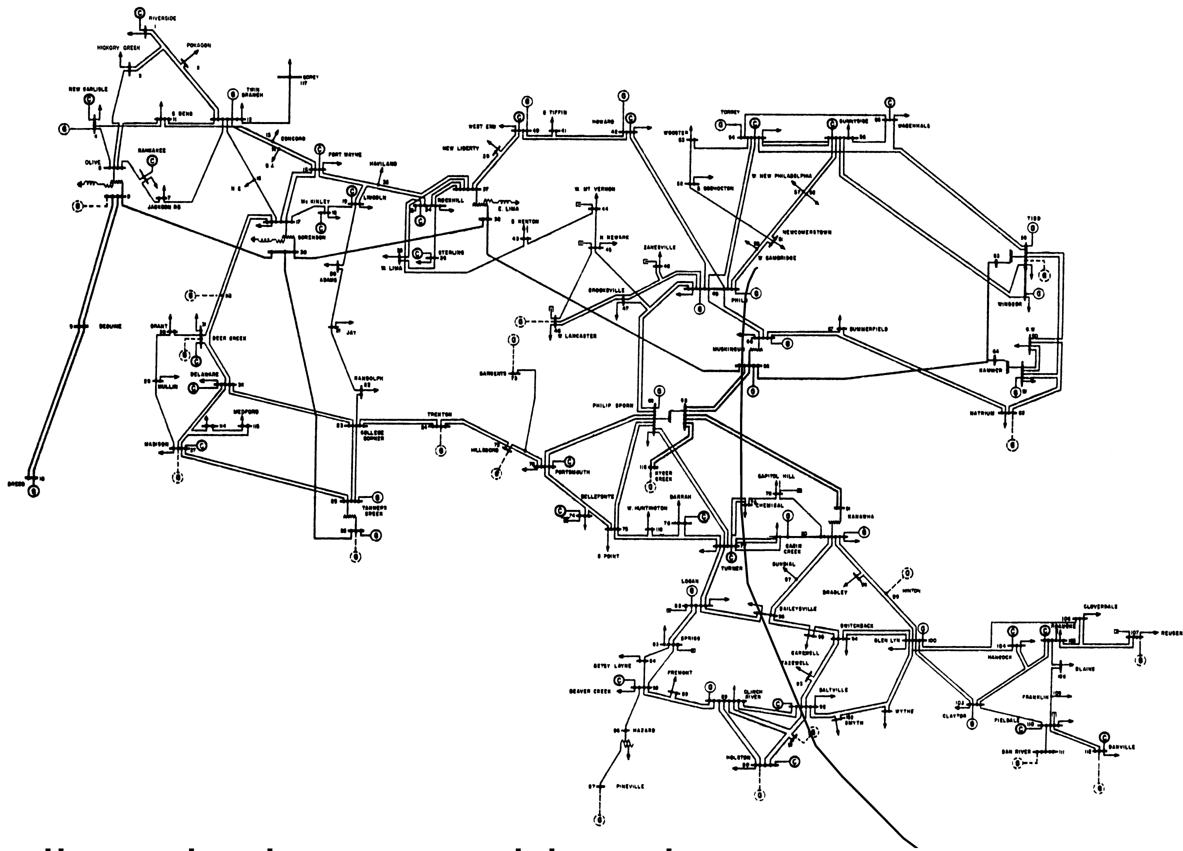
➢ the geographical representation of the network does not reflect accurately the reality of the system.

⇒ Representing the nodes according to their electrical distance is more relevant.

5. Results on the IEEE 118 bus test system for $N-3$ security analysis

Description of the problem

- IEEE 118 bus test system:



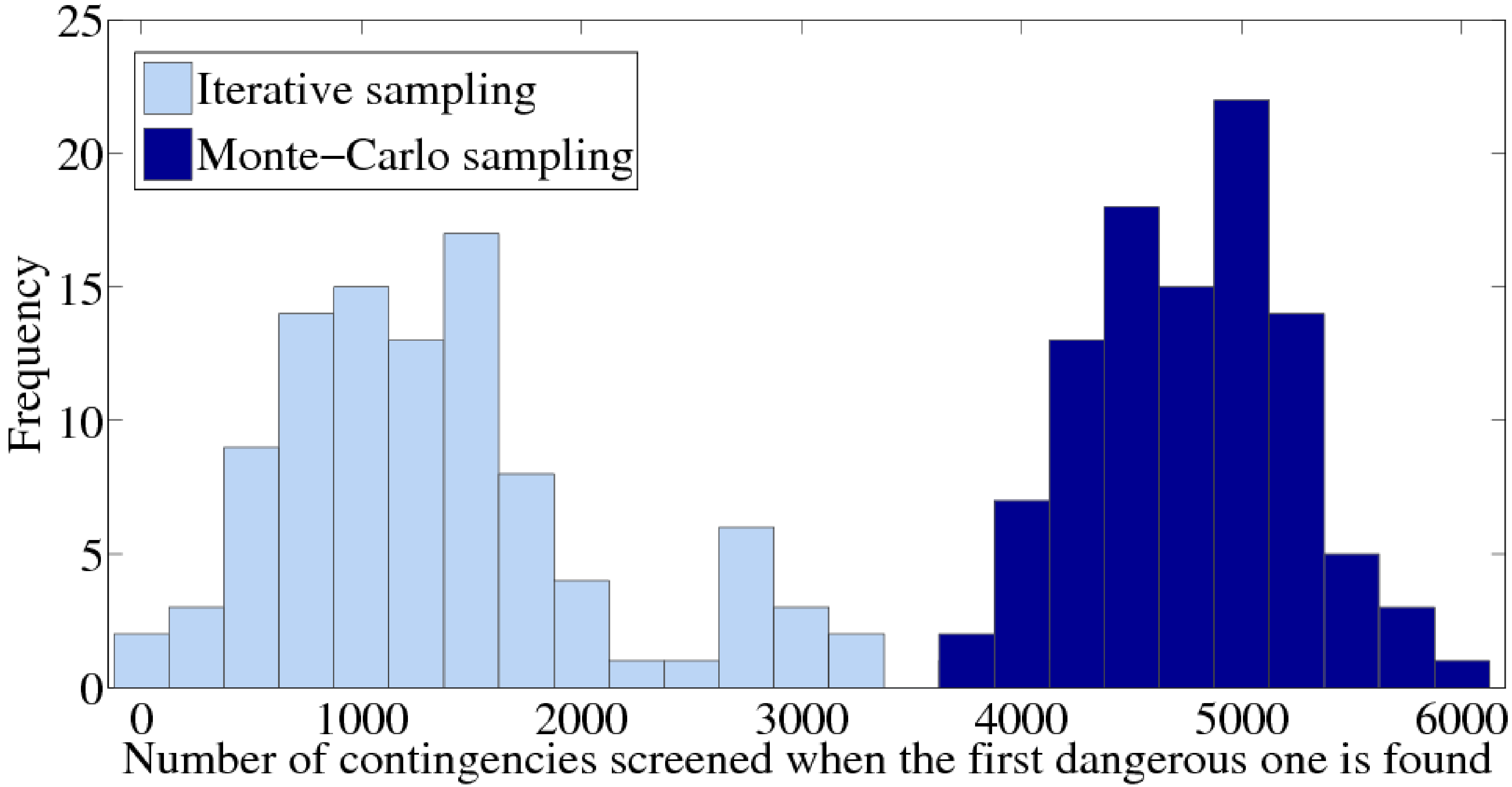
- $N-3$ security analysis, only line trippings considered.

- rate of dangerous contingencies: 2,1.10^{-4}

⇒ The rarity assumption is relevant.

5. Results on the IEEE 118 bus test system for $N-3$ security analysis

Speed at which one single contingency is identified



6. Conclusion

We have proposed a framework for efficiently performing $N - k$ security analyses without analyzing individually all the possible contingencies.

Prospects of extension of this framework:

- identification of potentially dangerous generation patterns, topic that gains in importance with the increasing penetration of renewable energies.