Contents

Chapter 1

Introduction

For many decades now, electricity has been a fundamental ingredient of private and industrial activities which means that any interruption of service can have massive consequences both from an economic and societal perspective. On the other hand, maintaining a highly reliable power system also comes at a cost. Thus, a balance between the costs of reliability and unreliability has to be found.

Risk assessment is the action of identifying (potential) events that can negatively impact the reliability of the power system. It is thus the first step towards risk management (balance between reliability and unreliability). And, it thus has an high impact on how the grid is operated. This is true for a wide range of timescales: from expansion planning (years ahead) to operational planning (15 minutes to days ahead). In the first case, it impacts what assets (lines, transformers, etc.) have to be built or upgraded. In the second case, it allows to define the operating limits of the system. With the introduction of complex and automatic remedial actions schemes, it also starts to have an impact on the real-time operation of the grid.

The reliability of a power system is often decomposed into adequacy and security. Consequently, risk assessment is also decomposed into adequacy and security assessments. ~~The~~ adequacy is the ability of the system to satisfy the consumers' demand and the system's operational constraints at any time, in the presence of scheduled and unscheduled outages of generation, transmission and distribution components or facilities. ~~The~~ security is the ability of the system to withstand disturbances arising from faults and unscheduled removal of equipment without further loss of facilities or cascading outages [1].

Si tu cites des définitions issues de normes, utilise des guillemets

1.1 Motivation

To reduce their greenhouse gases emissions, countries around the globe are installing more and more renewable energy sources in their grids. The weather-dependent nature of these sources (especially solar and wind) introduces additional complexity in the grid. Indeed, in the past, grids were designed to follow predictable and repetitive load patterns. Conventional generators (gas, nuclear, coal, etc.) would simply ramp up and down to follow the load. The grid could be considered to always be in a intermediate state between the state of peak load and the state of minimum load. Nowadays, power flow patterns are much more diverse as e.g. at a given moment, sun might be shining in the whole country, in part of the country or not at all. This diversity is further amplified by cross border exchanges that further decorrelate the energy sources.

In this context, the relevance of classical security assessment methodologies is decreasing. Indeed, security is often assessed based on one or a few "representative states" (typically at peak and minimum load). The assumption is that if the system is secure in those cases, then it is always secure. However, a higher diversity of power flow patterns means that a higher number of issues can threaten the power system security. This means that it will be more and more complex to derive a limited set of representative states that covers all possible threats. Also, in this approach, all threats are given the same "weight" while some threats might only occur in unlikely system configurations (e.g. at peak load with no renewable energy sources available).

Another challenge faced by power grids is the increasing importance of dynamic stability issues. This increase is caused by many factors including: reduced system inertia with the introduction of inverter-based generation, market liberalisation pushing the grid closer to its limits, increase of static limits through the use of dynamic line rating and better conductors, etc. Dynamic phenomena notably play an increasing role in cascading outages [2]. Cascading outages were previously mainly driven by thermal effects (line overloads, etc.) and would thus develop in a few hours, possibly ending in a fast collapse if the operators did not manage to stabilise the system. But cascades that are driven entirely by dynamic issues and that thus fully develop in seconds to minutes are becoming more common. This is especially true for large cascades that are already fast in the majority of cases[1].

The necessity to transition from deterministic security assessment methodologies (based on a worst-case scenario) to probabilistic methodologies (where different scenarios are weighted according to their probability) has been acknowledged in the industry and ~~the~~ literature. For example, the decision 07/2019 of the Agency for the Cooperation of Energy Regulators (ACER) of 19 June 2019 requires the European transmission system operators to develop a probabilistic approach for risk assessment of power systems by 2027. However, there is currently no convincing probabilistic methodology for the security assessment of transmission systems. Indeed, most of the literature focuses on slow cascading outages, and thus does not consider fast phenomena. Some research has however been done on probabilistic *dynamic* security assessment, but the developed methods require huge computational power and can thus only be applied on small-scale test systems.

1.2 Objectives

The objective of this thesis is thus to develop a dynamic probabilistic security assessment methodology that is efficient enough to be applied on a real-scale grid, and can give convincing recommendations on how to efficiently reduce the risk of cascading outages. This objective can be split in two sub-objectives. The first is to develop the general methodological framework. In order words, to develop a methodology to select the scenarios that have to be simulated and to estimate their probability. The second is to select appropriate models to be used in the aforementioned simulations. Similarly to the methodology, those models should be complex enough to give accurate results, yet simple enough to avoid issues of limited computational power, data availability, etc.

1.3 Approach

As power systems operate with a high level of reliability, there is limited historical data about their failures. This is especially true for large disturbances. Security assessment methodologies are thus naturally heavily based on simulations. Of course, lessons learned from past blackouts are very useful to identify the main drivers of cascading outages. Those lessons learned should thus have a high impact on the developed methodology (through the choice of scenarios to simulate) and the models used.

As power systems are evolving, some phenomena can grow in importance, and new phenomena can even appear. Lessons learned and expert knowledge thus have to be challenged and updated when necessary. The general approach used in this thesis to design both the security assessment methodology and the models is to start with complex methods/models to be used as a ground truth. And then, to simplify them as much as possible while keeping acceptable accuracy compared to this ground truth.

1.4 Expected contributions

The expected contributions of this thesis are listed below.

Methodology

- Identifying the threats that have an important contribution to the risk of cascading outages (and on the associated recommendations on how to reduce this risk), and the ones that can be neglected.

et les cas dans lesquels elles peuvent être négligées ?

[1] It is also worth nothing that even though large blackouts are rare, historical data shows that they contribute more to the risk that medium size blackouts [3, 4]. This is large blackouts tend to have higher restoration times and indirect costs (e.g. loss of critical infrastructure, civil disorders, etc.). Another reason is that blackout sizes have an heavy-tailed distribution [3, 4]. Large blackouts are thus less likely than smaller blackouts, but not much less likely.

- Showing that the proposed methodology can identify important threats that cannot be identified with static methodologies (methodologies that do not consider dynamic phenomena).

cette distinction entre méthodo dynamique et prise en compte de phénomènes dynamiques (potentiellement dans une méthodo (quasi-) statique) devrait p-ê être approfondie (au-delà de ce rapport)

- Increasing our understanding of power systems by highlighting interesting accident sequences and "near-misses".

↳ et des études de sensibilité associées?

Models

- Develop simple models of the ICT layer of power systems.
- Develop reduced load models from full distribution network models including the uncertainties from the full model.

1.5 Outline

Chapters 2 and 3 are introductory, while chapters 4, 5 and 6 are the main contributions of the thesis. Chapter 7 presents the next steps for the remaining of my thesis.

Chapter 2 gives first an overview the traditional approach to assess the security of power systems, as well as the most important causes of system insecurity. It also reviews the literature on probabilistic security assessment methods.

Chapter 3 gives and overview of the main protection systems used in power grids and their main failure modes. This is important as protections systems play a very important role in cascading outages.

Chapter 4 focuses on special protection schemes as they are becoming more common in power systems.

Chapter 5 discusses load models used in power system simulations. Currently used load models are indeed challenges by the increasing installed capacity of renewable energy sources in the distribution side.

Chapter 6 presents the proposed methodology and how it has been developed.

Chapter 7 concludes with perspectives for the remaining of my thesis.

1.6 Publications

Conferences: [5,6]

CYPRESS deliverables? ✓ (dans une catégorie séparée)

Chapter 2

Power system security

As mentioned in the introduction, security is the ability of a power system to withstand disturbances arising from faults and unscheduled removal of equipment without further loss of facilities or cascading outages [1]. Security is a complex problem, and many methodologies have been developed for the security assessment of power systems. Section 2.1 describe the "classical" (deterministic) security assessment methodology used by transmission system operators (TSOs) worldwide. Sections 2.2 then review different classes of probabilistic methodologies developed in the literature and discuss their limitations. As power system security is more and more threatened by dynamic phenomena, section 2.4 concludes this chapter with a review of the most important dynamic phenomena.

2.3 ?

2.1 Classical security assessment

In the classical methodology, a power system is deemed secure if it can withstand a set of "credible contingencies" without affecting customers nor violating security limits [7]. The set of credible contingencies is often based on the famous N-1 criterion, i.e. the power system should be able to withstand the loss of a single element (out of N)[1]. The possible loss of multiple elements due to a common mode failure (e.g. lines mounted on the same tower, lines connected to the same busbar) is a common addition to this list. The list definition varies from TSO to TSO and also on the considered time horizon (operation or planning). Also, during operational planning, the size of the list can vary depending on weather conditions. For example, the loss of multiple lines mounted on the same tower can be added to the list during a thunderstorm [7].

The definition of security limits also varies from TSO to TSO. Typically, security limits include a flat voltage profile (e.g. voltages at all buses between 0.95 and 1.05pu, this is to avoid disturbances for consumers and cascading outages), and the absence of overloads on all elements (to avoid cascading outages). Depending on the TSO, the security limits should be satisfied without the need for corrective actions (preventive approach) or after corrective actions have been implemented (corrective approach). In case (non-automated) corrective actions are used, it makes sense to define different security limits before and after the corrective actions are implemented (e.g. voltages between 0.9 and 1.1pu just after the disturbance, and between 0.95 and 1.05 after corrective actions).

A last important element of the classical security assessment methodology is the set of pre-contingency states of the system whose security will be assessed. Close to realtime operation, the pre-contingency state considered can simply be the current state of the system as estimated by the SCADA system. During planning, this is more complex as one should consider load and intermittent generation variability, possible generators and transmission elements unavailability, etc. The set of pre-contingency states (and credible contingencies) should be defined according to the following criteria [8].

- Credibility: the pre-contingency states should be reasonably likely to occur.
- Severity: the pre-contingency states considered should lead to the worst-case performance of the system for the considered contingencies.

[1] It should be noted that disconnections for maintenance are predictable and thus not considered to be contingencies. Disconnections for maintenance are thus already included in the N-0 situation.

- Representativity: the pre-contingency states and contingencies considered should cover the main weaknesses of the system and phenomena observed during past outages.

With the growing installed capacity of renewable but intermittent energy sources, it is becoming more difficult to choose a set of pre-contingency states and contingencies that satisfy the above criteria. Indeed, the variability of renewable energy sources greatly increases the number of possible pre-contingency system states. Consequently, the number of possible system issues also increases. There is thus an increasing risk of missing "worst-case scenarios". On the other hand, some issues might only appear during very specific system configurations. Designing the system around such issues would thus be uneconomical.

2.2 Probabilistic security assessment

Probabilistic methodologies are based on the concept of risk. The risk of a scenario is defined as the product of its probability (of occurrence) and its consequences. The consequences are usually expressed as energy (in MWh) not served or as the monetary cost of such energy not served[2]. Risk is thus expressed in MWh/y or €/y. Probabilistic approaches allow to have a cost-benefit analysis of the measures (investment in new assets, redispatch, etc.) used to secure the system. So, probabilistic methods should lead to more economical planning and operation of power grids. Another advantage of those methods is that, as opposed to deterministic methods, it is not necessary to know a priori the "worst-case" pre-contingency states and contingencies. When performing a probabilistic security assessment, one can use a larger set of states and contingencies. Then, the scenarios that contribute the most to the risk will naturally have a higher impact on the recommendations on how to secure the system. Disadvantages of probabilistic methods are however additional data requirements due to the necessity to estimate the probability of scenarios, and higher computation times due to the higher number of scenarios to simulate.

The necessity to transition from deterministic security assessment methodologies to probabilistic methodologies has been acknowledged in the industry and the literature. For example, the already-mentioned decision 07/2019 of the Agency for the Cooperation of Energy Regulators (ACER) of 19 June 2019 requires the European transmission system operators to develop a probabilistic approach for risk assessment of power systems by 2027. In the literature, research on probabilistic security assessment has been active for more than two decades. The remaining of this section reviews the state of the art of probabilistic security assessment methodologies and compares the main types of methodologies available.

Actually, a lot of different methodologies can be placed under the umbrella of probabilistic methodologies, but the number of uncertainties taken into account can vary greatly. The most straightforward probabilistic assessment method is the contingency enumeration method. It is similar to the deterministic method in that one will assess the security of a list of contingencies (usually larger than in a deterministic assessment, e.g. including N-2 events and loss of towers). The difference is that contingencies are associated with a probability. Also, instead of simply classifying contingencies as acceptable or unacceptable, the consequences are usually computed, but in a deterministic manner. Due to the relative simplicity of the methodology and similarity with the deterministic method, it is implemented in most commercial software tools[3] [8].

resp.

One industry-grade tool worth mentioning is ASSESS [12, 13] developed by RTE and National Grid (the French and British TSOs). It does not compute the consequences of contingencies (i.e. only classify them as acceptable or not), but it generally consider more uncertainties in the pre-contingencies states, and it has a toolbox of statistic and data mining tools that can be used to analyse the results. It is particularly useful to define operational limits by "drawing a line" between the acceptable and unacceptable pre-contingencies states.

A common mistake done when computing the probability of N-k events is to consider that it is equal to the product of the frequency of the k events. For example, ref. [8] says that if two lines have a failure rate of 1 in 20 years, then the double contingency failure rate is 1 in 400 years. This is however not true. The first way to understand why is to notice that the units do not match up. Indeed, the product of two frequencies should give a result in per squared years. A more intuitive way is to notice that the probability of two *independent* failures to occur exactly at the same time (or in an infinitesimal time interval) is zero (respectively infinitesimal). One should thus define the size of the time interval during which failures are considered to be simultaneous. More rigorously, the rate of occurrence of a double contingency (in per year) is the product of the failure rate of one of the two assets (in per year) with the (probability of) unavailability (unitless) of the second. The unavailability of an element is given by [refs]:

Tu prends le λ du 1er asset et le U du second ou l'inverse? Et tu as de toute façon encore une hyp. sur le comportement asymptotique de U. Mais c'est déjà mieux que de multiplier les λ!!!

$$U = \frac{\text{MTTR}}{\text{MTTF} + \text{MTTR}} \tag{2.1}$$

where the MTTR is the mean time to repair, and the MTTF is the mean time to failure of a component. Time to repairs can vary greatly in power systems. For example, when a line has to be opened after a single-phase fault, it is often possible to automatically reclose it after a second or a few dozens of seconds (depending on the scheme used). When it is not possible (e.g. stuck breaker or no automatic reclosure scheme installed), it might be necessary to send crew to reclose the line which can take a few hours. Repair times of large assets (transformers, towers, etc.) can be several weeks.

It is important to note however that after the failure of an element, operators will try to perform corrective actions to bring the system back to a (N-1) secure state. It is common practice to assume that operators are able to secure the system in 15 minutes [refs]. So two contingencies separated by more than 15 minutes are often referred to as N-1-1 contingencies instead of N-2 contingencies. To compute the rate of occurrence of N-k contingencies, one has thus to bound the time to repair by 15 minutes.

Double and higher order contingencies do not only occur due to the simultaneous occurrence of independent failures. Another important cause is the co-called hidden failures. A hidden failure is defined as a permanent defect that will cause a relay or a relay system to incorrectly and inappropriately remove a circuit element(s) as a direct consequence of another switching event [14]. Hidden failures are especially dangerous since they can cause high-order contingencies with a relatively high probability. For example, after a line fault, if one end of a line cannot be open, all lines that are connected to the same busbar or substation (depending on the cause of the failure, more details in chapter 3) will have to be disconnected to clear the fault. This causes a N-k contingency (with k in the order of 2 to 10) whose probability can be several order of magnitude higher than the probability of k independent failures. Also, as hidden failures usually cause the loss of adjacent elements, they tend to have higher consequences that the loss of independent lines that could be very far apart from each other. (équiv. à 2 événements N-1 indépendants

The importance of hidden failures is highlighted by the study of historical blackouts. For example, Ref. [3] observed that out of the 26 major unreliability events reviewed in a CIGRE (Conseil international des grands réseaux électriques) report[4] [15], 19 of them were triggered by losses of single transmission elements albeit that many of these events were exacerbated by other problems. Further analysis shows that 18 of the 26 events were caused or aggravated by hidden failures. The same observation can be made for smaller scale events. For example, the study of significant disturbances reported by the NERC [16] (North American Electric Reliability Corporation) in the period from 1984 to 1988 and summarised in [14] indicates that protective relays misoperations were involved, in one way or another, in 73.5% of disturbances[5].

Industry-grade tools only consider the uncertainties related to the initial state and initial contingencies. After the occurrence of a given contingency, the system is simulated in a fully deterministic manner. Those tools are thus unable to consider hidden failures as those manifest after the initial contingency[6].

Another limitation of modelling cascading outages in a deterministic manner is that cascading outages tend to have a "chaotic"[7] behaviour. This is because in a cascading outage, many elements are subject to abnormal conditions and thus likely to trip or misoperate. A good example of this is the tripping of lines caused by overload. When a line is overloaded, its temperature increases due to the Joule effect.

[2] It should be noted that the cost of energy not served is much larger than the cost of energy. For example, Ref. [9] estimated the cost of a one hour interruption of supply of a typical load to be around 20€/kWh. While the price of electricity on the bulk energy market is around 50€/MWh, so three order of magnitude lower.

[3] At the time of the writing of the CIGRE review [8] (2010), all tools used the quasi-steady-state (QSS) approximation (that will be described in section 2.2.1) to evaluate the consequences. Now, some tools (e.g. PSS/E [10] and DIgSILENT PowerFactory [11]) also allow to use dynamic simulations. Due to the simplicity of the method, it is possible to implement it with any tool that has basic scripting functionality.

[4] Most of these disturbances affected more than one million customers and led to at least 5 GW of unserved power

[5] This include both spontaneous operation of protections (without preceding event) and hidden failures. However, as power systems are designed to be N-1 secure, spontaneous operations should usually not have consequences.

[6] The hidden failures that occur just after the initiating event (e.g. failure to open a faulted line) could be modelled as part of the initiating events as done in [17, 18] ~~which is~~ discussed in section 2.2.2. This is however not possible for failures that occur later in the cascade. For those, it is necessary to have a probabilistic simulation of the evolution of the cascade.

[7] Not stricto sensu

It thus sag and can then enter in contact ~~in~~ with vegetation causing a short-circuit followed by a trip of the line. The line trip causes a redistribution of the power flows and can cause overloads in other lines which contribute to the propagation of the cascade. The redistribution could also resolve some overloads, stopping the cascade propagation. In a deterministic simulation, it is a common assumption to consider that when multiple lines are overloaded, the line with the most severe overload will trip first. In practice, slightly less overloaded lines could trip first due to different vegetation height, weather, etc. The trip of a different line can cause a very different redistribution of power flows that causes different lines to be overloaded in the next step of the cascade. The resulting cascade can thus be very different (in terms of size, geographical distribution, impacted elements, etc.) than the one simulated in a fully deterministic way. This difference is further amplified when we consider the competition between different cascading mechanisms.

These limitations of deterministic methods have fostered the development of probabilistic methodologies that are reviewed in the remaining of this section. Two main categories of probabilistic methodologies exist. The ones that use a static grid model (section 2.2.1) and the ones that use a dynamic grid model (section 2.2.2). These methods are quite different as they have to design around different limitations. The former have to introduce additional methods to approximate dynamic effects while the latter are limited by computation times. Additionally, section 2.2.3 reviews other types of methods that do not fall in the previous categories. ?

2.2.1 Methods with a static grid model

Methods based on a static grid model, often referred to as quasi-steady-state (QSS) methodologies typically follow the same procedure [19]. First, the system is initialised at the pre-contingency state, and the initiating contingencie(s) are triggered. Then, the post-contingency state is computed using a load flow algorithm. If some elements are subject to unacceptable conditions (e.g. overload, undervoltage, etc.), those elements are tripped or other remedial actions are implemented (e.g. under-voltage load shedding (UVLS), redispatch, etc.). After those disconnections/actions, the state of the system is recomputed. The process is repeated until no more elements are subject to unacceptable conditions or if a full blackout occurs.

The IEEE Working Group on understanding, prediction, mitigation and restoration of Cascading Failures (WGCF) classifies QSS methodologies according to five dimensions listed below [19]. It should be noted that some of these dimensions are themselves not one-dimensional.

- Pre-contingency states: most methodologies assess the risk of the system for a single pre-contingency state. The two most common extensions are the risk assessment over a given time period (e.g. one year, to consider e.g. seasonality of the load, maintenances, etc.), and inclusion of uncertainties (e.g. renewable generation). Uncertainties are generally treated used Monte Carlo (MC) methods. Ref. [20] reviews the most common probability distribution used to model different kind of uncertainties, as well as various methods used to overcome the limitations of basic Monte Carlo (e.g. sequential MC and Markov chain MC can be used to model dependencies between uncertain variables and time dependence, while importance sampling and quasi-MC can be used to increase the effectiveness of MC). It should be noted that pre-contingency sampling methods are roughly the same for methods with static and dynamic grid models. The paper thus reviews all of them.
- Degree of stochasticity: this includes both initiating and subsequent events.
  - Initiating events: in a deterministic approach, all N-k initiating events of a given order are considered, although a probability can be associated to each a posteriori. In a probabilistic approach, their probability is considered in the sampling process.
  - Subsequent events: in a deterministic approach, the evolution of the cascade is based purely on deterministic thresholds. For example, if a line is overloaded beyond a predefined limit, it is always disconnected[8]. This leads to a single possible evolution of the cascade for a given initiating event and pre-contingency state. In a probabilistic approach, elements are given a probability to trip when they are subject to violations (the probability can depend on the

Question terminologique: → quand il y a échantillonnage, on est dans une méthode de résolution stochastique d'une approche probabiliste ; si on prend en compte tous les N-k avec leurs probas respectives, c'est une résolution exacte d'une approche proba, mais pas vraiment une approche déterministe.

[8] In case of simultaneous (in the QSS sense) violations, either the element with the worst violation is disconnected, or all elements with violations are disconnected

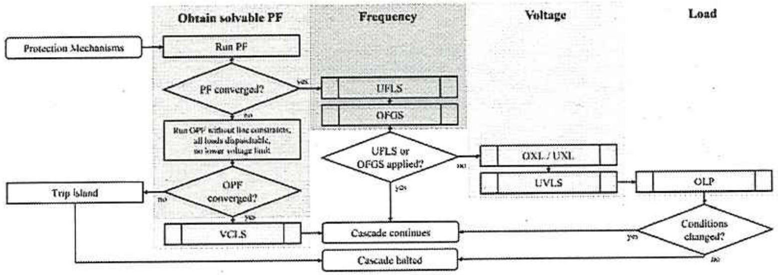

Figure 2.1: Flowchart of the AC-CFM methodology [21]. Abbreviations: PF: power flow, VCLS: voltage collapse load shedding, UFLS: under-frequency load shedding, OFGS: over-frequency generator shedding, OXL/UXL: over/under-excitation limiter, UVLS: under-voltage load shedding, OLP: overload protection

severity of the violation and other factors). For a given contingency and pre-contingency state, one thus obtains multiple cascading paths, each associated with a probability and specific consequences.

- Population of the contingency list: different methods can be used to generate the contingency list. The most common are contingency enumeration (consider all N-k contingencies up to a given order) and MC sampling. The contingency list can be reduced to the contingencies most likely to cause cascading failures by using screening methods.
- Power flow model: the pre-contingency state can be modelled either with an AC (full) or a DC (linearised) power flow. The DC model is faster but unable to account for voltage issues. Different methods can also be used to solve possible violations and non-convergence issues (of the AC load flow) in the post-contingency states. For example, an optimal power flow (OPF) will tend to model the actions that operators would use to solve the violations. The possible actions considered in the OPF can be load shedding, redispatch, topological actions, etc. Another possibility is to use models of protections such as UVLS, overcurrent protections of lines and transformers, etc. Some tools simply assume a total blackout in case of non-convergence of the load flow.
- Cascading mechanisms modelled: the tripping of overloaded elements is included in all methodologies. The disconnection of load and/of generators in case of unacceptable voltage is also commonly seen. Methodologies that consider hidden failures are a bit rarer[9]. Finally, dynamic cascading mechanisms (e.g. frequency, angle, and voltage stability issues) have to be modelled in a simplified way or using heuristics, and are considered by some methodologies.

In order to better illustrate QSS methodologies and the limitations in their modelling (especially dynamic issues), an example of QSS methodology is described and discussed. The example considered is the AC cascading failure model (AC-CFM) [21] that can be considered as one of the spiritual successors of the famous Manchester model [22]. This model follows a similar procedure to most QSS models, that is it initialises the system, triggers a initiating contingency, and then checks for violations and performs corrective actions until all violations are solved. However, as most QSS models, it differs by the corrective actions modelled. The steps that are taken to solve violations at a given step of the cascade are illustrated in Fig. 2.1 and discussed below.

(pas sûr de l'expression en anglais)

- Obtain a solvable power flow: as the AC-CFM uses an AC power flow, the power flow can fail to converge. This is often caused by lack of reactive power support that causes a voltage collapse. The modelling choice made for the AC-CFM is to use a OPF considering all load are dispatchable, and to minimise the load shedding necessary to obtain a converging load flow. In a dynamic simulation,

[9] Also, as will be discussed in chapter 3, dynamic grid models are required to model some hidden failures.

voltage collapses occur in a "smoother" manner as time is explicitly considered as a continuous variable. One can thus observe e.g. which loads are subject to undervoltages first and thus which UVLS relay actually triggers[10].

- Frequency: ~~the~~ AC-CFM models considers that if ? load-generation imbalances are ! less than a predefined threshold, the imbalance will be redistributed to the generators (that will increase or decrease their power to restore the imbalance) according to their participation factors. For larger imbalances, load or generation shedding[11] is necessary. In case of lack of generation, the load is reduced uniformly (although prioritisation can be implemented). In case of generation surplus, generating units are disconnected starting with the smallest ones as they tend to more easily lose synchronism. Also, the same imbalance threshold is used for all steps of the cascade. This is equivalent to assume that the frequency can be restored to its nominal value between each step. In a dynamic simulation, the evolution of the frequency is explicitly modelled. So, the maximum imbalance that does not cause load or generation shedding is the maximum imbalance that does not cause the frequency not to reach the threshold of under-frequency load shedding (UFLS, typically 49 Hz in a 50 Hz-system) or generator over-speed relays (typically 52.5 Hz). This maximum imbalance thus depends on the initial value of the frequency, the inertia of the system, potential synchronisation issues, etc. Also, for large imbalances, there is no guarantee that the balance can be restored before the frequency drops too low and generators are disconnected by their under-speed protections (typically at 47.5 Hz). This is especially true for systems with low inertia, for example, islands formed by the splitting of the original system, and/or systems with large penetration of (grid-following) renewable energy sources.
- Voltage: this block has two parts: the over/under-excitation limiters of generators, and UVLS.
  - OXL/UXL: in AC-CFM, generators that are over/under-excited are made into PQ buses, i.e. their reactive power output is considered equal to its limits. In a dynamic simulation, limiters would be modelled in a similar way. However, as over-excitation limiters protect the generators against excessive heating, a time-delay can be considered. It is also easier to consider the variation of reactive limits with the active power output.
  - UVLS: in AC-CFM, load is shed by block until voltages reach acceptable values. If multiple loads are subject to undervoltages, load is shed in all of them simultaneously. In a dynamic simulation, the order of triggering of UVLS relays will depend on the time evolution of voltages at individual load buses. UVLS at one bus can then alleviate or worsen voltage issues in neighbouring buses.
- Load: in AC-CFM, overloaded lines are tripped. If multiple lines are overloaded, they are all disconnected. In dynamic simulations, the order of tripping can be better modelled. Also, distance and out-of-step protections can be added in a dynamic model.

Additionally, the AC-CFM considers that frequency issues are solved first, followed by voltage issues, then overload issues. Again, in a dynamic simulation, the order and interactions between those issues can be better modelled. Finally, angle stability issues are not considered in AC-CFM.

The above discussion presented a particular QSS methodology with a given set of assumptions. However, for each of the cascading mechanisms, different assumptions could have been made. There is currently no consensus on the details of modelling required for QSS cascading failure simulation [19,24]. Also, the necessary level of detail is likely to be different systems and different operating conditions. Moreover, benchmarking has shown that different QSS methodologies lead to different results [19]. In particular, the distribution of cascading sizes and the critical elements differed depending on the methodology used. Finally, comparison between a QSS and a dynamic simulator has shown similar behaviour during the early stages of the cascade (slow phase), but different results for the later stages (fast phase) [25]. As purely fast cascades and dynamic issues are becoming more common [2], the use of dynamic models is expected to increase in the near future.

que veux tu dire ?

[10] Numerical stability issues can also occur in dynamic simulations but they tend to be rarer. To avoid those issues, one should be cautious of the models used (e.g. Ref. [23, p93-98] proposes to replace constant-power loads with restorative constant-impedance loads with a very short time constant). Protections tend to mitigate numerical issues as they disconnect elements are subject to severe conditions (e.g. distance protections disconnecting lines during voltage collapse).

what

[11] Generation shedding is most often called generator rejection, but the terminology of [21] is kept in this paragraph.

Outside of the field of cascading outage analysis, there has also been some concerns regarding static grid models. For example, RTE (the french TSO) is developing a tool called DynaFlow for steady-state computations using simplified time-domain simulation. Steady-states are usually computed with a power flow algorithm. Additional loops are added on top of this power flow to account for controls ~~used in~~ power systems (e.g. on-load tap changers, phase-shifter transformers, etc.). The order ~~of~~ which those loops are applied have an impact on the final state that is computed. This order was previously defined using heuristics and experience, but this was becoming complex with the increasing number of loops, especially for large systems. DynaFlow showed more accurate results and ease of use [26]. A similar tool called DynaWaltz was developed for long-term voltage stability. This tool replaced their previous QSS tool. DynaWaltz showed better accuracy than its predecessor while keeping similar computation times [27]. Note that both tools are deterministic.

in ?

2.2.2 Methods with a dynamic grid model

Methods based on a dynamic grid model methods, use time-domain simulations[12] to assess the consequences of a given scenario. Dynamic methods have been recognised as the most comprehensive and accurate methods for representing cascading outages [24,25,29]. The comprehensive aspect is maybe important to emphasise. Indeed, as illustrated in section 2.2.1, QSS methods need to introduce heuristics and/or simplifications to account for dynamic phenomena, and to estimate the order of occurrence of static issues. As dynamics methods use similar models than in classical dynamic stability assessment, the same largely accepted approximations can be reused (e.g. models of generators, exciters, etc.) which should help with the acceptance of dynamic security assessment methods by TSOs. The main difference between dynamic simulations for cascading outage simulations and stability assessment are that during cascading outages (i) the system is further from normal operation challenging the accuracy of the models, and (ii) protections (and their possible failure) play a much more significant role. Sensitivity studies are thus very important to control the first point. Chapter 3 is dedicated to the second.

The drawback of dynamic methods are significantly larger computation times[13] and data requirements. Compared to QSS methods, the additional necessary data is mainly linked to (i) the dynamic models of generators, loads, etc. and (ii) the models of protections. Data for the first point is generally available to TSOs as stability studies are performed routinely. However, it is important to have efficient data handling (e.g. automated transfer of data from stability tools to security assessment tools). The second point requires data regarding the failure rate of protections (that can be difficult to estimate) and the protection settings (that should be available but introduce additional data handling issues). Data requirements for dynamic security assessment is discussed in more details in section 6.3.1.

Multiple methods have been developed for probabilistic dynamic security assessment and are reviewed in the remaining of this section. In [23,29], random N-2 failures are simulated using a custom simulator. Protections are modelled, however, they are assumed to be perfectly reliable. Ref. [31] uses a similar methodology but uses the commercial simulator DIgSILENT PowerFactory.

Ref. [17,18] proposed a methodology based on event trees. An example of event tree is shown in Fig. 2.2. An event tree starts at a given initiating event (a permanent line fault in the left of the figure). The event tree then branches when subsequent events (typically protections against the initial event) are possible. Upward branches are usually associated with the occurrence of an event (e.g. protection operates successfully), and downward branches with non-occurrence of the event (e.g. protections fails to operate). The event tree thus generates a number of scenarios whose frequency and consequences can be estimated. In [17,18], the frequency is computed as the frequency of the initial event multiplied by the probability of the subsequent (non-)events. Fault trees can be used to model common-mode failures, they are presented in more details in dedicated literature, e.g. [32]. Consequences are estimated using dynamic simulations. The limitation of this method is that the event tree is built prior running the simulations. The analyst thus has to predict what protections will be activated. In practice, this is only

[12] In this thesis, time-domain simulations are implicitly assumed to use the root mean square (RMS) approximation. Dynamic methods are already strongly limited by computation time and thus cannot afford to use electromagnetic transient (EMT) simulations. Also, it is expected that the RMS approximation will remain adequate for most scenarios in the future [28].

[13] Classical offline dynamic security assessment (that takes into account uncertainty of the pre-contingency states but no uncertainty after the initiating event) of real-scale systems can already take one day in a high-performance computing (HPC) environment [30]. A probabilistic dynamic security assessment would require even more computational power. The magnitude of the increase depends on the range of uncertainties considered and the efficiency of the method.

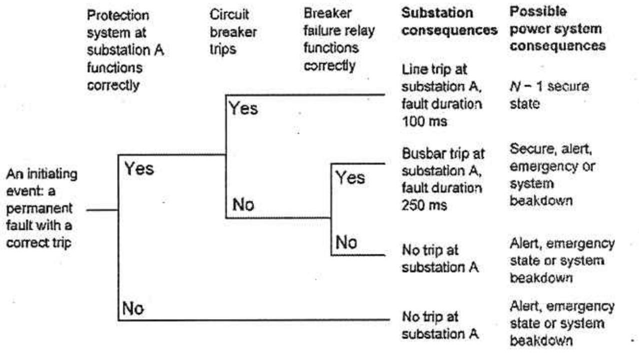
Protection system at substation A functions correctly
Circuit breaker trips
Breaker failure relay functions correctly
Substation consequences
Possible power system consequences
An initiating event: a permanent fault with a correct trip
Yes
Yes
No
Yes
No
No
Line trip at substation A, fault duration 100 ms
N − 1 secure state
Busbar trip at substation A, fault duration 250 ms
Secure, alert, emergency or system beakdown
No trip at substation A
Alert, emergency state or system beakdown
No trip at substation A
Alert, emergency state or system beakdown

Figure 2.2: A~~n~~ simplified example of event tree for a line short-circuit [18]

possible for the protections that isolate the fault (e.g. distance protections at both sides of the line). The use of event trees for security assessment of power systems is discussed in more details in section 6.1.1.

The Pacific Northwest National Laboratory (PNNL) developed a tool called Dynamic Contingency Analysis Tool (DCAT) for security assessment of power systems [33,34]. In this tool, after the initiating contingency, the evolution of the system is computed using dynamic simulation. Protections are modelled explicitly in the simulation, and when one protection activates, the simulation is stopped and the state of the system is saved. From this save, two simulations are run, one where the protection actually operates, and one where it fails to. The limitation of this method is that only missing protection~~s~~ operations are considered. Unwanted operations are not considered. Also, protections are considered perfectly accurate. The variable order of protection (due to e.g. measurement inaccuracies, incorrect settings, etc.) operations during a fast cascade is thus not considered. Finally, the reports did not show any example of application using the "protection misoperation" functionality. There was also no discussion on the impact on the computational burden of this feature.

An interesting feature of DCAT is that is uses both dynamic and QSS simulation~~s~~. Indeed, it uses dynamic simulations for the first 30 to 60 seconds after the initial contingency. If the system is deemed dynamically stable (i.e. if no event occurs during the last dozen of seconds of the dynamic simulation), then the tool ~~then~~ switches to (deterministic) QSS simulation. When an event occurs in the QSS simulation (e.g. a corrective action), the tools switches back to dynamic simulation.

Ref. [35] proposes the use of Dynamic Event Trees (DETs). DETs are an extension of event trees. In a DET, branchings are not predefined by the analyst but can occur at any time and any order. As time is a continuous variable, this means that a DET contains in principle an infinite number of scenarios. Numerical schemes are thus required to approximate those DETs. A more rigorous introduction to DETs is done in section 6.1.2. Ref. [35] proposed two numerical schemes. The first is skeleton-based MC. In this methodology, the first step is to build a so-called skeleton. This is done ~~with~~ in a similar way as in DCAT, i.e. the evolution of the system is simulated, and when a protection is triggered, the simulation branches. In one branch, the protection actually operates, and in the second it fails to. Upon this skeleton, additional branches are grafted at discrete time steps before and after the original branchings points. These additional branches take into account measurement and setting errors of the relays. The probability of each of these additional branches depends on the evolution of system variables in the skeleton. For example, if the variable monitored by the protection "hugs" the triggering threshold, the protection will be likely to trigger in a large time interval around its triggering time in the skeleton. On the other end, if the variable quickly goes beyond the threshold, the interval will be narrower. This methodology has been applied in [36]. The second method is MCDET. MCDET is a concatenation of MC and DDET (discrete DET, that can here be read as a synonym of skeleton). It was originally

Non! Les approches basées sur le squelette du DDET simulent tous les branchements liés à des seuils, puis y greffent les branchements se produisant au cours du temps.
Les DDET discrétisent les DET en fonction de la variable t.

proposed in the nuclear domain by [37]. In MCDET, continuous uncertainties (e.g. measurement errors) are handled by MC. Then, for each MC sample, a skeleton is built. This skeleton handles the discrete uncertainties (e.g. protection fails to operate). This method was however not fully implemented, and only preliminary results were presented [38].

DETs are more powerful than the previously mentioned methodologies as they can in principle account for any kind of uncertainties. However, they tend to be even more computationally expensive, and require more interactions with the simulator. They are thus used with custom simulators or simulators with powerful APIs.

It can be noted that, like DCAT, Ref. [35] uses both dynamic and QSS simulations but with a different approach. The approach is based on the observation that most cascades can be divided in two phases. In the first phase, the cascade is driven mainly by thermal effects (line overloads, etc.) and can last up to several hours (so-called slow phase). At some point, electromechanical phenomena become dominant and cascade ends is a fast collapse (so-called fast phase that last from several seconds to several minutes). Likewise, the methodology has two parts. In the first phase, the slow phase is simulated using a probabilistic QSS methodology. When a possible dynamic instability is detected, the method goes to the second phase. In the second phase, DETs are used as described above. As the QSS methodology generates a large number of similar scenarios, those scenarios are aggregated before being fed to the second phase.

2.2.3 Other methods

As previously mentioned, QSS methods have to make difficult modelling choices to consider dynamic phenomena and to model the order of occurrence of static issues. This lead some researchers to develop methods based on historical data. Indeed, historical data is by definition not dependent on modelling assumption. From historical data, one can observe what elements played critical roles in past cascades. Those elements are good candidates for upgrades or replacements. However, historical data alone does not allow to perform "what if" evaluation. For example, the benefits of a given upgrade cannot be estimated. This has led to the development of influence graphs models [39] that are tuned to match historical data. The most famous model of this category is the Oak Ridge-PSERC-Alaska (OPA) model [40]. The issue when building models from historical data is that this data consist mainly in small cascades as large blackouts are (hopefully) rare. However, as previously mentioned, large blackouts although rare have a very important contribution to the total risk (e.g. of load shedding) [3]. Moreover, large blackouts tend to be driven by different phenomena than small cascades. Indeed, large blackouts consist more and more often purely of a fast phase (driven by electromechanical phenomena), while small cascades always have an important slow phase (driven by thermal phenomena) [2].

techniques (?)

A lot of machine learning ~~have~~ have been developed for dynamic risk assessment and ~~have~~ are reviewed in [41]. However, those tools are only able to predict if a given scenario is stable or not (some tools are not purely dichotomic and can give a stability index or distance to stability indicator). They are thus unable to predict ~~to~~ the consequences of a given scenario. Moreover, those tools are deterministic. For a given pre-contingency state and contingency, they only give one output. They are thus unable to generate new scenarios as done in a DET.

2.3 Conclusion

Two main types of methods for probabilistic security assessment of power systems were reviewed. The first type of models uses the QSS approximation, i.e. it simulates the evolution of the power system using a sequence of steady-states. Those methods require a large number of assumptions in order to handle power flow convergence issues and to model dynamic issues and the order of activation of corrective actions. There is currently no consensus on what hypotheses are acceptable to make, and different QSS methodologies have shown to give different results [19]. Also, those methods are unable to accurately model fast cascading outages [25].

The second type of models is based on time-domain simulations. These methods are more accurate but require more computational power and input data. Out of the reviewed methodologies, DETs are the most powerful as they can in principle consider any type of uncertainty. However, they are even more computationally expensive than the other methods. Protections (and their potential failures) play a key role during cascading outages (especially fast cascading outages). They are thus naturally in a central position in all reviewed dynamic methods. However, only a few failure modes are considered in existing methodologies. This is discussed in more details in chapters 3 and 4. The issue of computation time is tackled in chapter 6.

2.4 Power system stability

Frequency, voltage, angle. (Others maybe later)

TODO: Models (generators, governors, loads, etc.) used? (comment of Michel Kinnaert at last meeting

Constant power load becomes restorative load with small time constant for convergence reasons.

TODO: Word spell check (check pdf to word tool)

Chapter 3

Power system protections

3.1 Basics

Horowitz book

- (CT/VT, breaker, basic working principles)
- (discrete fourier transform (DFT) but is not modelled in RMS tools)
- Distance protection
- Differential
- Overcurrent
- UFLS
- etc.
- Busbar arrangement, breaker failure protection

3.2 Protection performance during system disturbances

ENTSO-E defence plan

Say section not finished and give main ref ([42,43]) + bullet point of failures (ordered by importance)