ECOLE
POLYTECHNIQUE
DE BRUXELLES

Université libre de Bruxelles

IRCIRP - Formation doctorale en Sciences de l'ingénieur et technologie

Mid-term report

PhD student
Frédéric Sabot

Advisor
Pierre Henneaux

Co-supervisor
Pierre-Etienne Labeau

Supervisory committee
Michel Kinnaert
Johan Gyselinck
Jean-Michel Dricot

6th May 2024

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 comes at a cost. Thus, a balance between the costs of reliability and costs of unreliability has to be found.

Risk assessment is the first step towards risk management and thus has a high impact on how the grid is operated. It consists in identifying (potential) events that can negatively impact the reliability of the power system and potential solutions. Risk assessment outcomes impact risk management decisions in a wide range of timescales: from expansion planning (years ahead) to operational planning (15 minutes to days ahead). In the first case, risk assessment affects which assets (lines, transformers, etc.) have to be built or upgraded. In the second case, it helps 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 split into adequacy and security. Consequently, risk assessment is also split into adequacy and security assessments. 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". 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].

1.1 Motivation

To reduce their greenhouse gas emissions, countries around the globe are installing more and more renewable energy sources in their grids and their weather-dependent nature (especially for solar and wind) introduces additional complexity. 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. Similarly, power flows would usually be highest at peak load and minimum at low loads. Nowadays, power flow patterns are much more diverse as e.g., at a given moment, the sun might be shining in the whole country, in part of the country or not at all. This diversity is increased 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 power system security. This means it will be increasingly difficult 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 worst-case scenarios) to probabilistic methodologies (where different scenarios are weighted according to their probability) has been acknowledged in the industry and 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 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 to 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 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, then to simplify them as much as possible without significantly compromising on the accuracy of the results.

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.

[1] It is also worth noting 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 because 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 a 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).
- Increasing our understanding of power systems by highlighting interesting accident sequences and "near-misses". Indeed, sensitivity studies around those scenarios allow to identify elements for which a detailed modelling is useful.

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

This report can be split in three parts. The first (chapter 2) introduces power system security and reviews the state of the art. The second (chapters 3, 4 and 5) discusses the additional modelling requirements when performing probabilistic dynamic security assessment over deterministic dynamic security assessment. The third (chapter 6) develops a methodology for probabilistic dynamic security assessment.

Chapter 2 gives first an overview of 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 an overview of the main protection systems used in power grids and their main failure modes. This is important as protections system 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 challenged 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 List of publications

The following papers were published in conference proceedings.

- F. Sabot, P. Henneaux, I. S. Lamprianidou and P. N. Papadopoulos, 'Statistics-informed bounds for active distribution network equivalents subject to large disturbances', in *IEEE PES ISGT Europe 2023*, Oct. 2023. DOI: Toaddafterpublication
- F. Sabot, P.-E. Labeau and P. Henneaux, 'Handling protection-related uncertainties in simulations of fast cascading outages', in *IEEE PES ISGT Europe 2023*, Oct. 2023. DOI: Toaddafterpublication
- F. Sabot, P. Henneaux, P.-E. Labeau and J.-M. Dricot, 'Impact of the reliability of ICT systems on power systems with system integrity protection schemes', in *23ème congrès de Maîtrise des risques et de Sûreté de Fonctionnement (Lambda Mu 23)*, Paris Saclay, France, Oct. 2022. [Online]. Available: https://hal.archives-ouvertes.fr/hal-03876439
- F. Sabot, P. Henneaux and P.-E. Labeau, 'MCDET as a tool for probabilistic dynamic security assessment of transmission systems', in *2021 IEEE Madrid PowerTech*, Jun. 2021. DOI: 10.1109/PowerTech46648.2021.9494758

This thesis was performed in the framework of the CYPRESS[2] project. I had a significant contribution to the following deliverables.

[2] https://cypress-project.be/

- E. Karangelos, K. Thoelen, F. Faghihi *et al.*, *CYPRESS: Report D1.1 describing the selected performance metrics*, Jun. 2021. [Online]. Available: `https://cypress-project.be/images/nieuws/cypress_report_D11_executive_summary.pdf` (visited on 26/08/2022)
- A. Godfraind, F. Sabot, S. B. Mariem, V. Rossetto, P. Henneaux and Y. Vanaubel, 'CYPRESS: Report D1.3 describing the benchmarks', **Note:** Not yet published

TODO: Définition des ordres de contingences (N-1, N-k, N-1-1, etc.) = événement initiateur (arbitraire, ma définition) + proba et nombre à considérer
- N-1 (fréquence : 1e-1/y / contingences, nombre : 1000) : difficulté : échantillonnage efficace des conditions initiales (souvent 0 conséquences, mais risque non négligeable) - N-k (1e-4, 5000) : difficulté : moindre car va avoir plus souvent des conséquences importantes peu importe les conditions initiales - N-1-1 (1e-6 – 1e-7, 1000000) : difficulté : nécessaire d'avoir un screening / sélection des contingences - 2021 French-Iberic separation -> Focus sur les « interconnections » / common-mode (incendie) - Contribution au risque ? - Out of scope ? (Vu la séparation temporelle des contingences, on atteint potentiellement plus vite les limites statiques que dynamique) - Contingences continues / nuage noir / variabilité renouvelable (fréquence : ?, nombre : qq unes ?) : s'ajoute aux autres contingences - N-K (K » 1): résilience

TODO: Pour chaque chapitre, passer plus de temps sur l'intro et la structure

TODO: When writing, think about the "topic sentence, example, analysis/development, point, link to next paragraph" structure. (Can be flexible)

Operating in the Fog: Security Management Under Uncertainty

TODO: Curse of dimensionality / peel, example with hypersphere

TODO: Bien situer le contexte (vision planing mais opérationel envisable avec modifications), ce qui existe déjà, etc.

Chapter 2

Power system security

TODO: contingency types [11], future work: FMEA protection, missing vs unwanted trips., n-1-1 requires screening [12]

TODO: timescale decomposition, Eurostag and Dynaflow examples

TODO: QSS comparison on ccdf of total risk in log scale, but does not compare critical contingencies / recommendations given for risk reduction

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 describes the "traditional" (deterministic) security assessment methodology used by transmission system operators (TSOs) worldwide. Section 2.2 then reviews different classes of probabilistic methodologies developed in the literature and discusses their limitations. Section 2.3 concludes with a discussion of the limitations of state-of-the-art assessment methodologies.

2.1 Traditional security assessment

In the traditional methodology, a power system is deemed secure if it can withstand a set of "credible contingencies" without affecting customers nor violating security limits [13]. 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 [13].

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 traditional security assessment methodology is the set of pre-contingency states of the system whose security will be assessed. Close to real-time operation, the pre-contingency state considered can simply be the current state of the system as estimated by the

[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.

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 [14].

- 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.
- 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 [16]. 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] [14].

[2]It should be noted that the cost of energy not served is much larger than the cost of energy. For example, Ref. [15] 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 [14] (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 [17] and DIgSILENT PowerFactory [18]) 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.

One industry-grade tool worth mentioning is ASSESS [19], [20] developed by RTE and National Grid (i.e. the French and British TSOs respectively). 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.

TODO: ASSESS: add fig? and keywork data mining

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. [14] says that if two lines have a failure rate of 1 in 20 years, then the double contingency failure is rate 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:

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

TODO: Reformulate with $\lambda_1(1 - e^{-\lambda_2 T}) + \lambda_2(1 - e^{-\lambda_1 T})$ to be more clear and correct, ref Haarla book, p67

where the MTTR is the mean time to repair, and the MTTF is the mean time to failure of a component. Time to repair 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. If a second contingency occurs after corrective actions have been performed, this will be called a N-1-1 contingency. Corrective actions can typically be performed in 15 minutes. So the MTTR in eq. 2.1 should be replaced by $\max(\text{MTTR}, 15\text{ min})$.

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 [21]. 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 orders 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 than the loss of independent lines that could be very far apart from each other.

TODO: Mention Ian Dobson paper https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10054456, but (identified) critical lines might have more reliable protections (e.g. double differential (independent sets of relays), or even SIPS) than less critical ones (e.g. single distance protection with overcurrent backup). (Time resolution of data (1min) makes it difficult to differentiate between independent events and cascade. Actually, probably need some manual postprocessing to separate the two)
It turns out for two North American publicly available historical outage data sets that the three contingency motifs , , account for most of the probability of multiple line outages [32].
https://iandobson.ece.iastate.edu/PAPERS/dobsonchapter2SPRINGER24.pdf
[32] K. Zhou, I. Dobson, Z. Wang, The most frequent N-k line outages occur in motifs that can improve contingency selection, early access in IEEE Trans. Power Systems, 2023. doi: 10.1109/TPWRS.2023.3249825

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] [22], 19 of them were triggered by losses of single transmission elements albeit 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 [23] (North American Electric Reliability Corporation) in the period from 1984 to 1988 and summarised in [21] 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. It thus sags and can then enter in contact 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 cope with 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.

[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 [24], [25]. This 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

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 [26]. 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 [26]. 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 using Monte Carlo (MC) methods. Ref. [27] 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 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

[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

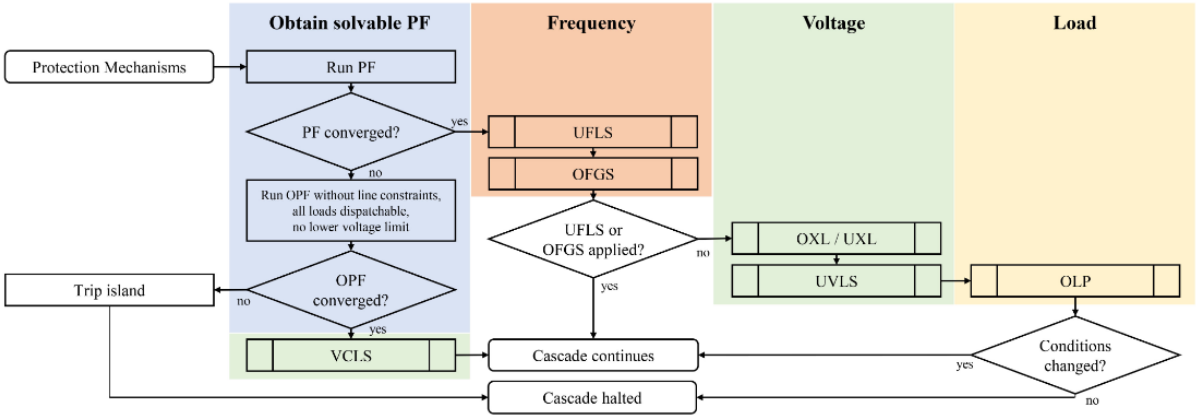


Figure 2.1: Flowchart of the AC-CFM methodology [28]. Abbreviations: PF: power flow, VCLS: voltage collapse load shedding, UFLS: under-frequency load shedding, OFGS: over-frequency generator shedding, OXL/UXL: over/under-excitation limiter, UVLS: under-voltage load shedding, OLP: overload protection

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) [28] that can be considered as one of the spiritual successors of the famous Manchester model [29]. 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.

TODO: Simplify figure to have less things to explain. In general, make text less dense.

- 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 an OPF considering all loads are dispatchable, and to minimise the load shedding necessary to obtain a converging load flow. In a dynamic simulation, 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: AC-CFM 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

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

[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. [30, p93-98] proposes to replace constant-power loads with restorative 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).

[11] Generation shedding is most often called generator rejection, but the terminology of [28] is kept in this paragraph.

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 [26], [31]. Also, the necessary level of detail is likely to be different for different systems and different operating conditions. Moreover, benchmarking has shown that different QSS methodologies lead to different results [26]. 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) [32]. 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.

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 or which those loops are applied has 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 [33]. 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 [34]. Note that both tools are deterministic.

2.2.2 Methods with a dynamic grid model

Methods based on a dynamic grid model 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 [31], [32], [37]. 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 dynamic methods use similar models than in traditional 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 is 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 is significantly larger computation times[13] and data requirements. Compared to QSS methods, the additional necessary data are 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 are discussed in more details in section 6.3.

Multiple methods have been developed for probabilistic dynamic security assessment and are reviewed in the remaining of this section. In [30], [37], random N-2 failures are simulated using a custom simulator. Protections are modelled; however, they are assumed to be perfectly reliable. Ref. [39] uses a similar methodology but uses the commercial simulator DIgSILENT PowerFactory.

Ref. [24], [25] 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 the 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 [24], [25], the frequency is computed as the frequency of the initial event multiplied by the probability of the subsequent (non-)events. To complement event trees, fault trees can be used to model common-mode failures, they are presented in more details in dedicated literature, e.g. [40]. 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 possible for the protections that isolate the fault (e.g. distance protections at both sides of the line and backups for these protections).

The Pacific Northwest National Laboratory (PNNL) developed a tool called Dynamic Contingency Analysis Tool (DCAT) for security assessment of power systems [41], [42]. 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 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

[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 [35], [36].

[13] Traditional 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 [38]. 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.

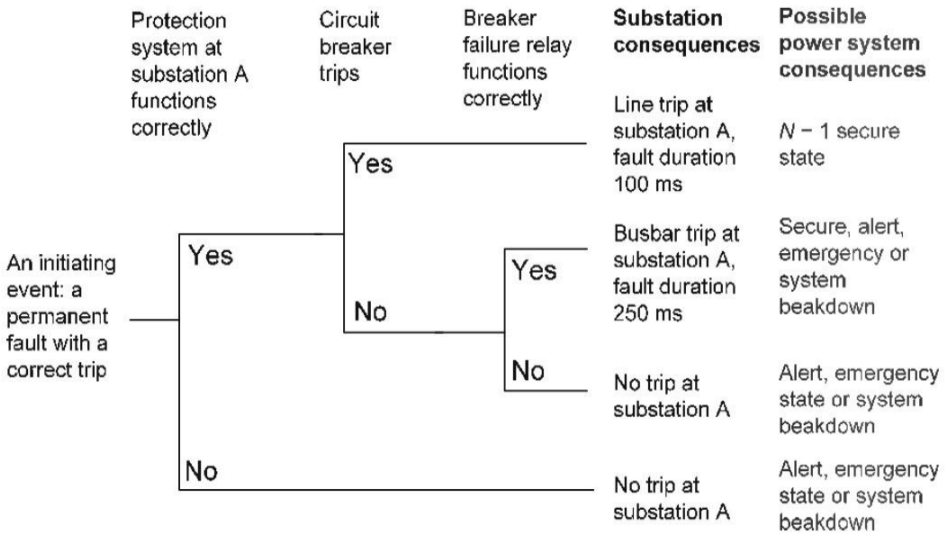


Figure 2.2: A simplified example of event tree for a line short-circuit [25]

on the impact on the computational burden of this feature.

An interesting feature of DCAT is that is uses both dynamic and QSS simulations. 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), 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. [43] 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. Ref. [43] 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 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 [44]. 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[14]). It was originally proposed in the nuclear domain by [45]. 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 [46].

TODO: Define correctly MCDET (no skeleton)

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. [43] uses both dynamic and QSS simulations but with a

[14]DDETs and MCDET are introduced more rigorously in section 6.1

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 led some researchers to develop methods based on historical data. Indeed, historical data are by definition not dependent on modelling assumptions. 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 [47] that are tuned to match historical data. The most famous model of this category is the Oak Ridge-PSERC-Alaska (OPA) model [48]. The issue when building models from historical data are that these 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].

A lot of machine learning techniques have been developed for dynamic risk assessment and are reviewed in [49]. 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 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 [26]. Also, those methods are unable to accurately model fast cascading outages [32].

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 chapter 3 and 4. The issue of computation time is tackled in chapter 6.

TODO: As apposed to nuclear, no failure (except if already present) during system evolution

TODO: Can generate initiating event contingency list from historical data instead of my "fault clearing event tree": https://arxiv.org/pdf/2209.02192.pdf (and add a few random N-2?, paper say 81% of N-2 are adjacent lines, and 19% remaining)

Chapter 3

Power system protections

[50]

As mentioned in the previous chapters, protections play a key role during cascading outages. Protections are usually designed to protect a given element against faults and abnormal conditions. The stability of the system as a whole plays a secondary (but still important) role in the design of protection systems. So, history has shown that even a protection operates "as designed", it can sometimes contribute to the propagation of a cascade and sometimes prevent its propagation [51]. Another point to consider is that, as the system operates in a (potentially very) degraded state during cascading outages, protection misoperations (either unwanted or missing trips) can become likely and impact the propagation of the cascade.

Section 3.1 briefly reminds the basic protection principles. Then, section 3.2 discusses the scope of considered protections in this thesis. Section 3.3 reviews the most important (from a system reliability perspective) protection misoperations that can occur during/due to cascading outages. And section 3.4 concludes with a list of the protection models considered in this thesis.

3.1 Power system protection basics

This section briefly introduces protections systems used in power systems. For a more complete overview, the reader is referred to textbooks on the subject. The book [52] has been used as a basis for this section.

3.1.1 Components

Protections systems usually consist of three main elements.

- Transducers (i.e. voltage transformers (VTs) and current transformers (CTs)) that reduce the magnitude of electrical quantities to values that are easier to work with (e.g. voltages from 400 kV to 110 V and currents from 1000 A to 1 A.).
- A relay that measures those electrical quantities and applies some predetermined logics to decide when to trip.
- A circuit breaker (CB) that disconnects the protected element. Note that for elements connected to more than one terminal (e.g. lines), a protection system (including transducers, a relay and a circuit breaker) is placed at each terminal.

3.1.2 Reliability, dependability and security

The reliability of protection systems is decomposed into two concepts: dependability and security. Dependability is the measure of certainty that a protection will operate for all faults for which they are designed to operate (e.g. always trip when there is a fault on the protected line). Security (of a protection system, not to be confused with security of a power system) is the measure of certainty that a protection will not operate for faults other than the ones for which it is designed (e.g. never trip for

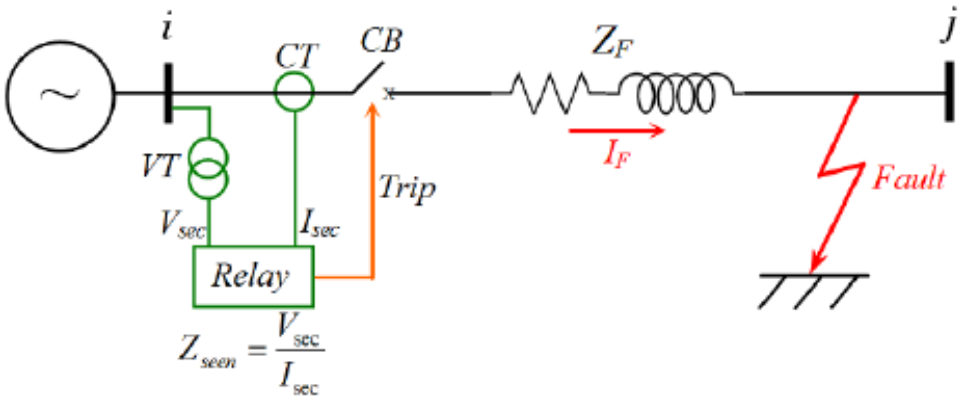


Figure 3.1: Basic schematic of distance protection [53]

faults on nearby lines). Most protection systems are designed for high-dependability. This is because allowing sustained (e.g. short-circuit) faults can cause important physical damage and even deaths. On the other hand, an isolated security issue (i.e. a protection incorrectly trips during normal operation) should have no consequences in a N-1 secure system. Security issues can however threaten the system stability when they occur following a fault or during a cascading outage. Balancing dependability and security is the most challenging aspect of protection system design.

3.1.3 Most common line protection schemes

The most common line protection schemes are reviewed below. Other types of elements (generators, transformers, etc.) can also use those schemes, but also other schemes. The latter are reviewed in the reference book.

- Distance protection: the working principle of distance protections is shown in figure 3.1. It is based on the fact that during a metallic short-circuit of a line, the ratio between the voltage and the current (called apparent impedance) measured by the relay is equal to the impedance of the portion of the line between the relay and the fault. If this measured impedance is smaller than the impedance of the entire line, it means that the fault is on the line and that the relay should open the line. In practice, uncertainties[1] imply that the presence of a fault can only be guaranteed when the apparent impedance is lower than 80 to 90% of the line impedance. Multiple "zones" are thus necessary to protect a line. The most common zones definition is as follows: Zone 1 protects 80-90% of the line and operates "instantaneously" (i.e. with no intentional time delay). Zone 2 protects 110-120% of the line (i.e. the full line with some margin) and operates with some time delay (e.g. 300 ms) to coordinate with the zone 1 of adjacent line(s). Together, zone 1 and zone 2 protect the full line. Using telecommunications, it is possible to have instantaneous operation for the full line. Additionally, a zone 3 is often used as a backup protection for the adjacent line(s). It thus covers the full line plus the longest adjacent line plus some margin. It operates with a larger time delay than zone 2 (e.g. 600 ms to 2 s). Distance protection is the main protection in transmission systems.

- Differential protection: the working principle is that the sum of ingoing and outgoing currents in a given protected zone should be equal to zero according to Kirchhoff's law. A sum that is (significantly) different from zero indicates the presence of a fault and the necessity to trip. Due to the geographical expansions of line (dozens to hundreds of kilometres), it is necessary to have communication between both ends of a line to use differential protections. Differential protection is thus mostly used for extra high-voltage (EHV) lines (400 kV in Europe).

- Overcurrent protection: as the name indicates overcurrent protection disconnect the protected line when it is subject to high currents. It can either be definite-time (trips when the current is higher

[1] Infeed from the other side of the fault, variation of line parameters due to variable sag, etc.

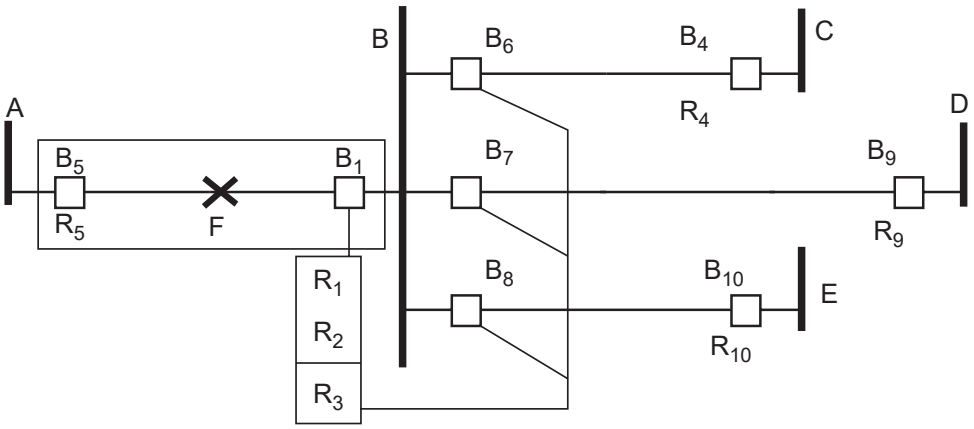


Figure 3.2: Duplicate primary, local backup, and remote backup protection [52]

than a threshold for a given duration) or inverse-time (trips faster for more severe overcurrents). Overcurrent protection is only used as backup protection in transmission systems.

3.1.4 Redundancy

As for all critical systems, redundancy is used to increase the reliability of protection systems. This is especially true at higher voltage levels where higher levels of redundancy are used. The example in Fig. 3.2 demonstrates the different kinds of backups used. In this example, there is a fault on line AB. The primary protection is the relay R_1 that sends a tripping signal to breaker B_1. R_2 is the duplicate primary protection. It can be identical to R_1 or use a different scheme. The transducers and battery power supply can also be duplicated. The breaker is usually not duplicated due to its higher cost. R_3 is the local backup or breaker failure protection. If R_1 or R_2 sends a tripping signal but B_1 does not open, it will send a trip signal to B_6, B_7 and B_8. Breaker failure protection operates with a larger time delay than the primary protection. R_4, R_9 and R_{10} act as remote backup protection. Remote backup protection is often performed by zone 3 relays.

Note: in its final version, this thesis will include a paragraph on substation configurations, the generic configuration(s) used in the test systems and statistical data on failure rates. More information on substation configurations can be found in [54]

3.2 Note on the protection models used in this thesis

The main objective of this thesis is to design a methodology for probabilistic dynamic security assessment of power systems. While probabilistic dynamic security assessment could be useful to help protection design, it is not the main objective as a satisfactory security assessment methodology has to be designed first. The protection models used in this thesis were thus chosen to satisfy two criteria. The models should lead to a relatively accurate estimation of the risk[2] and realistic cascading outage scenarios[3] such that (i) the added value of the method compared to QSS methodologies can be shown, (ii) variance reduction techniques used in the probabilistic methodology have similar performance than with more elaborated models. To explain the second criteria, it is necessary to briefly introduce probabilistic methods. Probabilistic methods often use Monte Carlo (MC) methods to handle uncertainties. The issue with basic MC is that, as power system are very reliable, most MC simulations lead to scenarios with no consequences which waste computational resources. Techniques that increase the likelihood of sampling more "interesting" scenarios (i.e. scenarios that contribute more to the total risk) are thus necessary. Those techniques can loosely be referred to as variance reduction techniques. The two criteria

[2]It should be noted that, even if using more complex models, the exact value of the risk (in MWh/y or €/y) is of low significance. What is important is to be able to compare the risk associated with different scenarios and to be able to identify actions that most effectively reduce the risk.

[3]The IEEE CFWG also recommends verifying that the methodology leads to cascading outage sizes that follow a power law [55]. The validation of the methodology is discussed in more details in chapter 6.

are quite abstract, but the main idea is to focus on protections that have the highest impact on the risk. This can be done through study of past cascading outages and experience.

It is difficult to obtain data regarding the exact protection design used by TSOs. Also, this data does not exist for academic test systems. It is thus necessary to use generic protection settings. If a TSO applies the methodology, they should have access to a database of protection settings. On the other hand, they initially might not have all protection models in their dynamic simulator, nor the interface necessary to automatically bring the protection settings to the simulator. They will thus likely also use the methodology with generic protection models. The methodology will then show what settings to modify to reduce the risk of cascading outages. It can then be a good exercise to compare those settings (obtained in a greenfield environment with a focus on system security) and the ones designed by protection engineers (in brownfield, with a focus on dependability, and with additional concerns regarding resistive faults, different types of fault, etc.).

3.3 Protection performance during system disturbances

As power system are drawn far from normal operation during cascading outages, protections are more likely to misoperate. Possible misoperations have been reported by the IEEE Power System Relaying and Control Committee (PSRC) in a report [51], its summary [56] and in previous works [57]. However, as mentioned above, only the misoperations that contributed most to the risk in previous blackouts are considered. The misoperations considered are more similar to the smaller list of misoperations given in [58, ch3] (that is itself based on [51], [56], [57]).

On top of those misoperations that are linked with the system degraded state, the possibility of a relay not operating simply because the relay (or its transducers, power supply or CB) is failed has to be considered.

Note: the final thesis will include more details on the misoperations that are not considered and the reasons for not considering them.

3.3.1 Distance protection

Distance protection misoperations are the most common type of misoperations. Zone 3 is the one that causes the most issues. This is because zone 3 has to overreach in order to provide backup for adjacent lines. During large disturbances, this zone is thus susceptible to trip even in the absence of fault. The three main causes for unwanted operations of zone 3 relays are listed below.

- High demand: higher line currents imply that the apparent impedance measured by relays decreases (if voltage is roughly constant). In some extreme cases, this can cause the apparent impedance to enter zone 3 or even zone 2. To avoid this issue, a load blinder must be used as shown in Fig. 3.3. According to NERC's (North American Electric Reliability Council) requirements, the distance protection must not trip for currents 1.5 times the maximum current line rating (considering dynamic line rating) at 85% of nominal voltage and for a power factor of 30 degrees [51]. Such a load blinder is thus used in our model.

- Power swings: large (potentially stable) power swings can cause distance relay to misoperate. To illustrate this, consider the following example. A test system consists of two synchronous generators connected by a single line. During a stable system swing, the angle difference between the two generators can be up to 180 degrees[4]. The voltage at the electrical centre of the network (here the middle of the line) is then 0 (sum of the voltages of the two generators assuming the magnitudes of the voltages are equal). From the relay point of view, this is equivalent to a metallic three-phase fault. The difference is that power swings develop on longer time scales than short-circuits. Relays can thus use a power swing blocking (PSB) function to distinguish between faults and swings. The model of PSB used in this thesis is still to be defined.

- Voltage instability: during voltage collapses, voltages decrease and loads tend to draw more current to partially maintain a constant power. For relays, this causes a reduction of the apparent impedance and potentially trips in zone 3 or zone 2. Similarly to power swing, the difference

[4] According to the basic equal area criterion model.

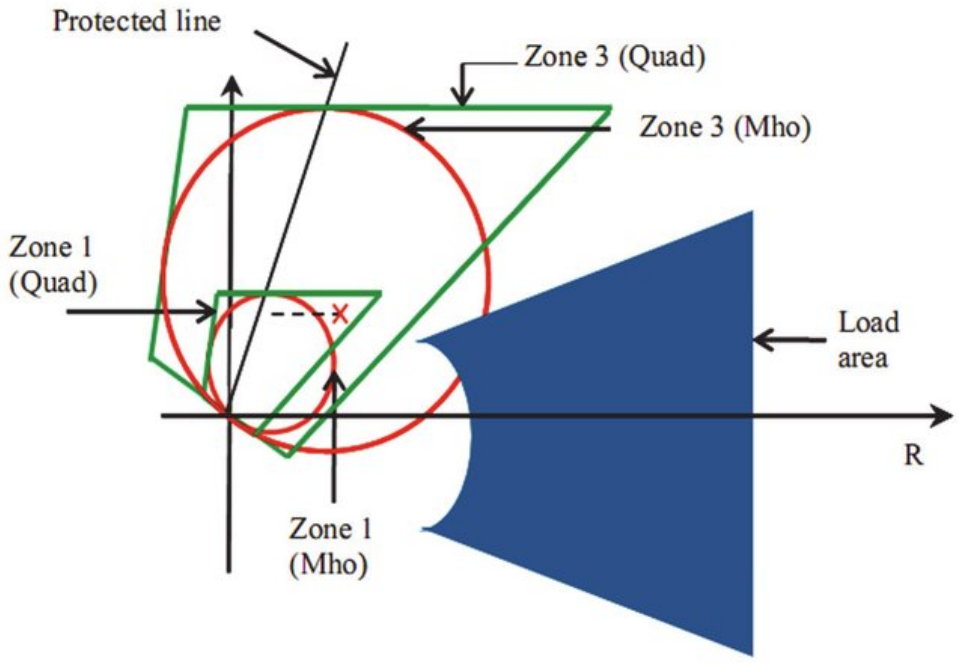


Figure 3.3: Load encroachment. The green zones are quadrilateral zones used by modern numerical relays. The red zones are mho characteristics mostly used by old electromechanical relays [59]

compared to actual fault is that voltage instabilities develop slower. However, there is no standard method to distinguish between voltage instabilities and power swings. PSB can thus be used for both. As PSBs typically reset after 2 s, the voltage collapse should be stopped faster to avoid tripping of distance relays. It should be noted that while tripping due to a voltage instability is usually unwanted, it can in some case limit the propagation of the cascade by isolating the zone where the voltage instability takes place.

Some other types of misoperations are given in [51] but not considered in this thesis. For example, currently installed numerical relays use methods like discrete Fourier transform (DFT) to evaluate phasor quantities (voltage and currents) used in the protection logics. This introduces inaccuracies during frequency deviations. However, those inaccuracies are relatively minor (up to 10% during very large frequency deviations) and affect all relays in the same way as the frequency is usually uniform in the whole system (or in a given island is the system is split). Those inaccuracies thus cannot significantly change the order of operations of protections. It is thus expected that neglecting this effect should not have a high impact on the possible cascading scenarios nor on their consequences.

Distance protection of multiterminal lines (lines with three or more connections) requires additional considerations. However, as academic test systems do not include such lines, those issues are not considered here.

3.3.2 Overcurrent protection

Line overcurrent protection is only ever used as a backup protection. It is thus expected to have little impact during cascading outages [51]. Ref. [51] mentions possible misoperation of the ground overcurrent element for untransposed lines (those lines are unbalanced and thus generate zero (and negative) sequence currents even when only positive sequence voltages are present). With numerical relays, it is however possible to solve this issue by restraining the ground element by a fraction (e.g. 10%) of the positive sequence current. This issue is thus not considered.

Overcurrent protection is sometimes installed on transformers to backup the differential protection and to protect the transformer against overcurrents (that reduce its lifetime). Typical settings for overcurrent protection of transformers is to trip for 130-200% of the transformer rating [58].

3.3.3 Differential protection

Due to its design, differential protection is mostly insensitive to system disturbances. The main reasons it is not the only type of protection used are the need for a communication medium (in the case of lines) and inability to act as a backup for elements outside of the protected zone. Some possible misoperations are given in [51] but are not considered here.

3.4 Summary of protection models used

The generic protection models used in this thesis are listed below. These models include the considerations given in section 3.3 as well as relatively standard protection models used in other (probabilistic or even deterministic) dynamic security assessment studies. Note that, by default, all protections that are said to operate instantaneously (or with no intentional time delay) are supposed to operate in 100 ms (this corresponds roughly to 20 ms for the relay to take the decision and 80 ms for the CB opening)[5].

3.4.1 Line protection

Lines are supposed to be protected by a distance and a differential relay. Actually, since no misoperations of differential relays are considered, differential relays are not explicitly modelled in the power system simulator. The differential protection only implies that faults will be cleared instantaneously for the whole line, not only the part that is covered by zone 1. Also, it reduces the likelihood of missing trip (discussed in more details in the final thesis, pilot distance protection will also be discussed).

Zone 1 protects 80% of the line and operates instantaneously. Zone 2 protects 120% of the line and operates with a 300 ms delay (including CB opening time[6]). Zone 3 setting is more complex due to infeed effects. It still has to be defined. Load encroachment of 150% of the maximum line current at 85% of the voltage with a 30 degrees power factor is also included. Finally, a PSB function is also added (exact model to be defined).

Since only three-phase faults are considered (due to the use of a RMS (root mean square) simulator), auto-reclosing of lines is not considered.

3.4.2 Generator protection

Generators must be protected against undervoltage (that cause degraded performance of auxiliaries), over- and underfrequency, overexcitation and out-of-step conditions. Thus the following protections are used:

- Undervoltage protection: this is especially critical for nuclear generators. For those an instantaneous undervoltage protection set at 0.9 pu is used. For other types of generators, a less strict protection can be used.

  TODO: `https://eepublicdownloads.entsoe.eu/clean-documents/pre2015/consultations/Network_Code_RfG/120626_-_NC_RfG_-_Requirements_in_the_context_of_present_practices.pdf` says requirement for all is 0.9 forever, 0.85 for 60ms (a bit country dependent).

- Under- and overfrequency: past blackouts (e.g. the 2003 Italy blackout) have shown that distributed generators tend to unexpectedly disconnect during frequency excursions. In this thesis, it is assumed that generators connected on the transmission side strictly follow ENTSO-E requirements for continental Europe [60]. So, instantaneous protection is used for frequencies outside of the range 47.5-51.5 Hz. According to [51], hydro units can operate in a large band of frequency. Generators connected to the distribution side are discussed in more details in chapter 5.

- Overexcitation: Volt-per-Hertz protection is used. The settings are still to be defined.

[5] The probability distribution of this time must still be defined

[6] To be confirmed.

- Out-of-step: a simple model of out-of-step protection is used. The generator trips instantaneously when the angle difference between the generator and the centre of mass of the system (or the island if the system is split) is larger than 180 degrees.

Under- and overexcitations limiters are also considered although they are not stricto sensu protections.

3.4.3 System protection

Undervoltage load shedding (UVLS) is not used by all TSOs and is thus not considered in this thesis. Underfrequency load shedding (UFLS) is used following ENTSO-E standards [61]. More precisely, UFLS instantaneously disconnects load by steps between 49 and 48 Hz. The number and size of steps are still to be defined.

Special protection schemes (SPSs) can also be considered. However, since they are designed to mitigate a specific weakness of a given system, it is not possible to define a generic model of a SPS. SPSs are discussed in chapter 4.

3.4.4 Transformer protection

An instantaneous overcurrent protection set at 150% of the rating of the transformer is used. No inverse-time protection is used. To be confirmed.

3.4.5 Protections on the distribution side

This is discussed in more details in chapter 5. Generator and motor protections are considered, but not line protections.

Chapter 4

Special protection schemes

This chapter is based on the following publication:

- F. Sabot, P. Henneaux, P.-E. Labeau and J.-M. Dricot, 'Impact of the reliability of ICT systems on power systems with system integrity protection schemes', in *23ème congrès de Maîtrise des risques et de Sûreté de Fonctionnement (Lambda Mu 23)*, Paris Saclay, France, Oct. 2022. [Online]. Available: `https://hal.archives-ouvertes.fr/hal-03876439`

As discussed previously, dynamic stability issues are becoming prevalent in many power systems due to various causes such as market liberalisation, intermittent energy sources, increase of static limits (thanks to better conductors and dynamic line rating), etc. There are three main general solutions to mitigate dynamic issues:

- Installation of new transmission infrastructure and upgrade of existing installations (lines, transformers, etc.): this solution is potentially the most effective but it has the drawback of high lead times (up to ten years) and costs. Also, due to public and regulatory pressure, TSOs have to give more and more justifications to choose this option.
- Redispatching: redispatch actions such as curtailment of renewable generation can also mitigate dynamic issues. However, these actions drive the system away from the economical optimum. These actions can be judged cost-prohibitive as they have to be performed each time a (plausible) disturbance threatens the stability of the system while the probability of the disturbance actually occurring can be very low. (Line switching is a low-cost redispatching action, but it cannot alleviate all issues on its own.)
- Special protection schemes (SPSs): SPSs are schemes that automatically perform corrective actions upon detection of a disturbance. These schemes lead to lower operating costs since corrective actions only have to be performed after a disturbance actually occurs. They are also significantly less expensive and quicker to install than transmission infrastructure. SPSs have to act quickly to be effective, usually in dozens of milliseconds to a few seconds. Possible actions that can be taken by a SPS include: generation rejection, turbine fast valving, braking resistor, fast unit start-up, governor setpoint change, load shedding, shunt switching, HVDC fast power change, on-load tap changer (OLTC) blocking, quick increase of synchronous condenser and FACTS voltage setpoint, and system splitting [62].

Case-specific solutions (e.g. fast frequency response to mitigate frequency instability, OLTC blocking to mitigate voltage instability, etc.) are also important but are too numerous to be discussed here. This chapter focuses on SPSs and in particular how to consider them in a probabilistic dynamic security assessment. In particular, section 4.1 discusses reliability considerations regarding SPSs and section 4.2 discusses the communication infrastructure necessary to use SPSs as well as potential threats linked to communications. Finally, section 4.3 concludes with perspectives of future work regarding SPSs.

In the literature, various definitions of SPSs exist. In this thesis, the following definitions are used. A system integrity protection scheme (SIPS) is a protection scheme whose primary objective is to protect the integrity of the whole power system. This contrasts with classical protection schemes whose primary

objective is to protect a given element against unacceptable conditions (including sustained faults). A SPS is any SIPS that is not a local under-frequency load shedding (UFLS) or under-voltage load shedding (UVLS) scheme. The term defence plan is also used in the literature. SIPSs are often the main elements of a defence plan, although other (slower) mitigation measures are also included [58], [62]. This term is however not used in the remaining of this thesis.

4.1 Reliability considerations

The integration of SPSs is usually done in two phases. In the first phase, the TSO designs a SPS to mitigate a specific problem in the system. This SPS requires data from only a few buses to detect this specific problem and has a small set of possible actions. In this phase, the SPS usually has a dedicated ICT infrastructure [63]. In the second phase, the TSO starts to rely on SPSs to mitigate various issues. In this case, a more scalable design consists of a centralised Control Centre (CC) that has access to measurements from most buses in the system. Then, a dedicated ICT infrastructure makes less sense. The SPS thus uses the existing ICT infrastructure used for traditional operations [64], [65]. Beyond scalability, an advantage of the second type of SPS is that they can make use of classical state estimation algorithms to compute the most likely state of the whole system even with partial information.

The reliability of the two types of SPSs has to be evaluated with different methodologies. The first type of SPS usually has a dedicated communication infrastructure and requires a limited number of remote measurements. The reliability of this kind of SPS can thus be modelled using standard reliability analysis such as reliability block diagrams and fault trees. An example of such an approach can be found in [66] and the references therein. It should however be noted that due to their relative low cost and critical nature, those SPSs are usually designed with a very high level of reliability (both selectivity and dependability). For example, the SPS presented in [63] determines the state of each line end using a 2-out-of-4 voting scheme. It also has two redundant communication infrastructures, and it has been extensively tested prior to installation. It might thus not be necessary to include the possible misoperation (nor unwanted nor missing operations) in a probabilistic security assessment. It can be considered in a more possibilistic approach, but this is out of scope of this thesis.

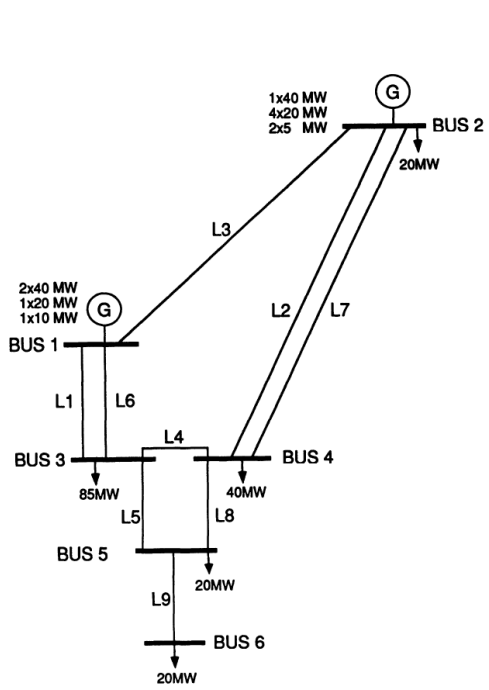
The reliability analysis of the second type of SPS can be decomposed into three parts: state estimation, communication and control actions. Estimating the state of the system requires to have a sufficiently large (and diverse) set of measurements. Observability analysis can be used to determine if a given set is appropriate. It should be noted that the (relatively recent) large-scale installation of phasor-measurement units (PMUs) implies that the random loss of a few measurements should have very limited impact on the state estimation performed by the SPS. It is thus mostly inadequate performance of the communication infrastructure that can potentially lead to poor state estimation. The performance of the communication infrastructure is discussed in section 4.2. Once the SPS has evaluated the state of the system, identified a disturbance and successfully sent a control action to one or several actuators, those actuators have to actually implement the corrective action. The performance of the actuators can again be evaluated using standard reliability methods (fault trees, etc.).

4.2 ICT infrastructure

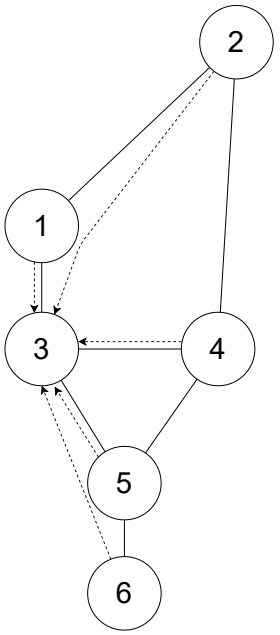
The first type of SPS has a very simple communication infrastructure and is thus no longer considered in the remaining of this chapter. Most of the literature on (the second type of) SPSs simulate the ICT infrastructure by simulating it with network[1] simulators such as ns-3, OMNeT++ or OPNET [67]. Some even use co-simulations, i.e. interface power system and network simulators and make them run together [68], [69]. Co-simulation is discussed in more details in appendix A. In this thesis however, it is preferred to use basic queuing theory. This approach allows to have an analytical formulation for the delays in the ICT system. It thus allows to have a better understanding of the system and to explore the impact of disturbances more easily.

So, queuing theory is introduced and used to size the ICT infrastructure in section 4.2.1. Then, it is used to study the impact of failures in section 4.2.2. A simple method to monitor the communication

[1] In this thesis, network is short for communication network, and grid is short for electrical grid.



(a) Physical part. Adapted from [72]



(b) Communication infrastructure. Plain lines represent communication links, and dashed arrows represent PMU traffic flows in normal operation

Figure 4.1: Cyber-physical Roy Billinton test system (RBTS)

performance in real-time is then proposed in section 4.2.3. Finally, the impact of different types of cyber-attacks is discussed in section 4.2.4.

4.2.1 Infrastructure sizing

The test case considered in this section is the Roy Billinton test system (shown in Fig. 4.1a) equipped with a centralised SPS. The SPS consists in PMUs that are installed at each bus and send measurements (voltage, current, frequency and possible breaker status) to a CC located near bus 3. The ICT infrastructure is shown in Fig. 4.1b. In real networks, phasor data concentrators (PDCs) are placed between the PMUs and the CC to aggregate the PMU traffic. This is is not the case here due to the small size of the system considered. The methods presented below can however easily be adapted to consider those PDCs.

It is necessary to have a communication infrastructure to link the PMUs to the CC. TSOs can either have their own infrastructure, this is e.g. the case in the UK [70, p110] and in Germany [71, p42] where optical ground wires (OPGWs) are installed on top of most transmission lines, or rent it from an Internet service provider (ISP). In the second case, the design of the infrastructure is outsourced to the ISP[2]. The focus is thus placed on the first case. However, ISPs use a similar methodology to what is described below. Also, for the sake of simplicity, it is assumed that a single OPGW is installed in parallel to every transmission line (including the double lines).

TSOs usually only use a fraction of the bandwidth provided by the OPGWs. They thus often choose to rent part of this bandwidth to ISPs [70, p110]. The traffic used for the SPS should however not be in competition with the ISPs' traffic. This is achieved using quality of service (QoS) mechanisms such as weighted fair queuing. These mechanisms allow to guarantee a given amount of bandwidth for the

[2]There is a tendency of operators of geographically-extended systems (e.g. railroads) to install fibre optic cables in parallel to their infrastructure and to sell them to ISPs. Part of the capacity of the cables is then rented back to the utility. There are two main causes to this trend. First, the bandwidth of modern cables often vastly exceeds the needs of utilities. Second, ISPs have more experience in managing communication infrastructures. A concern that this introduces is that critical communication infrastructures (electricity, railroad, etc.) get connected to the global internet. However, it has been shown many times that and "air gap" is not an effective cyber-security measure.

SPS. Below, queuing theory is used to determine the minimum bandwidth to reserve for the SPS to stay under a maximum delay.

The most common assumption in communication network traffic engineering is to consider that the distribution of arrivals is Poissonian [73]. In other words, it means that packets arrive with a constant mean rate and independently of the time elapsed since the last event. This assumption is very often valid in ISP networks due to the large number of independent inbound traffic sources[3]. Then, traffic load (or traffic intensity) of an element (router, firewall, etc.) is defined as:

$$\rho = \lambda/\mu \tag{4.1}$$

where λ is the arrival rate of packets in the element [packets/s], and μ is the processing rate of the element [packets/s]. Then, from the Poisson assumption, a well-known result from queuing theory [73] is that the average number of packets in the queue of the element is given by[4]:

$$N = \frac{\rho}{1-\rho} \tag{4.2}$$

We can then use Little's law [74] that states that the average queuing time t_q [s] spent by a packet in a system is given by:

$$t_q = N/\lambda \tag{4.3}$$

(Little's law is valid for any stationary system, e.g. a single queue or a complex network.) It is also interesting to decompose t_q into the waiting time t_w and the processing time $t_s = \frac{1}{\mu}$. For this, one can simply observe that when a packet arrives in a queue, it must wait for the average N packets already present to be processed. So,

$$t_w = N t_s \tag{4.4}$$

Eq. (4.3) and (4.4) imply that,

$$t_w = \frac{\rho}{1-\rho} t_s \tag{4.5}$$

and,

$$t_q = \frac{1}{1-\rho} t_s \tag{4.6}$$

Eq. (4.6) is plotted in Fig 4.2. This figure illustrates clearly the impact of congestion on delays. This figure shows that, in order to limit the waiting delay (and its derivative with respect to ρ), the network should be operated such that ρ is lower than 0.7 or even 0.5.

This methodology is now illustrated on the RBTS. For this, it is assumed that each PMU generates 120 kbps of traffic (packets of 300 bytes [75] sent at 50 Hz), that 300 kbps is reserved in each link for the SPS, and that packets are routed to the shortest path as shown in Fig. 4.1b. Also, the processing time of routers is assumed to be limited by the bandwidth of links, i.e. is equal to the packet size divided by the bandwidth, so 8 ms. The traffic in each link is simply the sum of all traffics going through this link[5]. From this traffic, one can compute the traffic intensity and the average queuing time as done in Table 4.1. Then, the average communication delay between a given PMU and the CC is simply given by the sum of the delays in the path between this PMU and the CC. Those delays are given in Table 4.2.

These delays can be compared with the maximum delay allowable for the SPS's actions. In this case, the SPS protects the system against angle stability issues by disconnecting a 20 MW generator at bus 2 when either line 2, 3 or 7 is lost. In [7], I showed that for this particular system, the generator should be disconnected at most 173 ms after the line loss. To determine the maximum communication delay that satisfy this constraint, the other (constant) delays have to be subtracted from those 173 ms. The processing times in the PMUs and CC is taken as 5 and 10 ms respectively [67]. A 20 ms worst-case delay due to the sampling rate of 50 Hz is also considered. The circuit breaker of the generator is supposed to open in 60 ms [76]. A constant 8 ms delay is considered for communication between the CC and

[3]The validity of this hypothesis in the communication network of an SPS is discussed later in this section.

[4]Assuming a steady-state system, infinite buffer size, and $\rho \leq 1$

[5]For routers where multiple PMU influxes are merged, a Poisson distribution of arrivals can still be assumed thanks to the additivity of the Poisson distribution. Thanks to this additivity property, queuing theory can easily be applied in large networks.

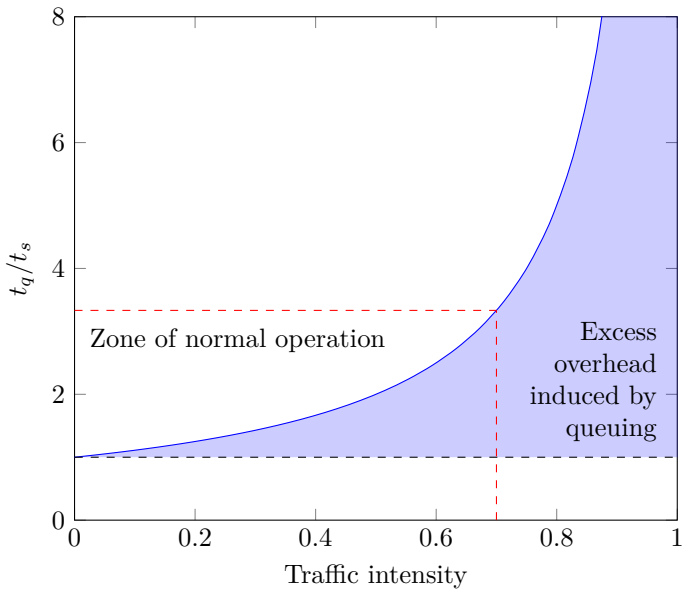


Figure 4.2: Communication delays as a function of congestion

Table 4.1: Computation of the average time spent by a packet in a given link for a reserved bandwidth of 300 kbps

Link	**Traffic**	ρ	N	t_q [ms]
2-1	120 kbps	0.4	0.67	13.3
1-3	240 kbps	0.8	4	40
4-3	120 kbps	0.4	0.67	13.3
5-3	240 kbps	0.8	4	40
6-5	120 kbps	0.4	0.67	13.3

Table 4.2: Average communication delays between each PMU and the CC

PMU #	t_q **(ms)**
1	40
2	53.3
4	13.3
5	40
6	53.3

the generator[6]. The propagation delays (1 ms per 200 km for a refractive index of the communication medium of 1.5) are neglected. There is thus 70 ms remaining for the communication delays between the PMUs and the CC. One can then verify than the average delays in Table 4.2 are lower than 70 ms. It is also possible to compute the probability of the delays being lower than 70 ms. This is however more complex, and discussed in traffic engineering textbooks [73].

The computations above have been made assuming a Poisson distribution of arrivals. The PMUs however send packets at a deterministic and constant rate. The developments above are still useful because the merging of several influxes in larger network tends to produce Poisson distributions. Also, the above method will very often lead to conservative results. In this particular case, simulations in ns-3 resulted in communications delays of 8 ms (the processing time in one router) for PMUs 1, 4 and 5, and 16 ms (twice the above value) for PMUs 2 and 6. Finally, due to the small amount of traffic needed by the SPS (and its critical nature), it is inexpensive to have large margins. This is true even for large networks. For example, even if all 2700 substations operated by the french TSO (mostly at 225 and 400 kV level) [77] send PMU packets (300 bytes [75]) at a sampling rate of 50 Hz, it only results in a total of 360 Mbps[7].

4.2.2 Impact of failure

The impact of cyber failures is studied differently if the ICT infrastructure is owned by the TSO or by an ISP. In the first case, the TSO can simply perform the same analysis as in section 4.2.1 but considering that some of the links are failed. For example, after a failure of link 3-4, traffic from the PMU 4 will be redirected through path 4-5, 3-5 which will increase the traffic intensity and queuing delays along this path. A higher bandwidth is thus necessary to stay under the target delay when considering possible failures. Additionally, if simultaneous failures of communication links and power lines are considered (due to a common mode failure), an additional delay has to be considered for the rerouting of the traffic.

In the second case, cyber failures will usually have a lower impact. This is because ICP's networks are usually more meshed than TSO's grids. For example, the core network of BT (formerly British Telecom) consists of 8 inner core nodes that are fully linked to each other, and 12 outer nodes that are each connected to at least 3 core nodes [78]. Also, in this case, it is the ISP and not the TSO that has to make sure the cyber failures have a limited impact on the performance of the ICT infrastructure. The service level agreement (SLA) should define to what level of reliability the ICT performance (i.e. availability and delays) should be guaranteed. Carrier-grade lines are often leased with a reliability level of 99.999% (i.e. 5 minutes of total downtime per year).

4.2.3 Monitoring ICT performance

Even if the ICT infrastructure has been appropriately sized (or if this the responsibility has been outsourced to an ISP), it is still useful to monitor its performance and to verify that the delays are under a given bound. Indeed, delays could increase following failures, bugs, attacks, increase of the traffic, etc. When high delays are detected, the SPS should arm schemes that are less time critical (e.g. disconnection additional generators or loads), or send an alarm to the operators such that they take preventive actions (e.g. reduction of the production at bus 2).

Monitoring the communication delays between the PMUs and the CC is direct since the packets sent by PMUs are precisely time-tagged (PMUs' clock are synchronised via GPS). For other communications (e.g. communication with the generator's circuit breaker), this generally is not possible. An alternative is to estimate communication delays from Round Trip Time (RTT) measurements. In other words, when the TSO sends a message to a given recipient, it measures the time that passed between sending the message and receiving the acknowledgement message from the recipient. Assuming a symmetric network, the one-way delay is half the RTT. Since the TSO might not always need to communicate with recipients, it is necessary to use so-called keep-alive messages to have a continuous monitoring of the RTT. RTT measurements are used very often in ICT networks. The RTT-based mechanism used by

[6]Queuing theory could also be used to compute this delay, however as messages from the CC to the generator travel in the opposite direction as messages from PMUs to the CC, they do not affect each other (assuming full duplex links).

[7]In the future, the size of the packets might increase slightly due to the transition to IPv6 (20 bytes), additional information regarding substation equipment being included in the PMU traffic (a few dozens of bytes), and longer cryptographic headers (a few dozens of bytes).

TCP as defined by the Internet Engineering Task Force standard [79] is presented below for illustration. There are similar mechanisms in other communication protocols such as RTP (Real-Time Protocol).

In TCP, when an application sends a messages, it expects to receive an acknowledgement from the recipient. If it does not receive one, it resends the message. The Retransmission TimeOut (RTO) is defined as the maximum time after which a sender considers that if it did not receive an acknowledgement signal, then its message was lost and must thus be resent. The RTO can thus be seen as an upper bound (with a good probability) of the RTT. As the RTT can vary in time (due to variability of the traffic, seasonal effects, attacks, etc.), a "smoothed" RTT is defined. Each time a new measurement R' of the RTT is made, the smoothed RTT is updated according to:

$$\text{SRTT} = (1 - \alpha) \times \text{SRTT} + \alpha \times \text{R'} \tag{4.7}$$

where α is a parameter often set to 0.125. To compute the RTO, a safety margin is added to the SRTT. This margin is higher when there are higher variations of the RTT. Mathematically, the variation of the RTT with is computed using,

$$\text{RTTVAR} = (1 - \beta) \times \text{RTTVAR} + \beta \times |\text{R'} - \text{SRTT}| \tag{4.8}$$

and the RTO as,

$$\text{RTO} = \text{SRTT} + 4 \times \text{RTTVAR} \tag{4.9}$$

The recommended value for β is 0.25.

4.2.4 Impact of traffic-based cyber-attacks

The impact of cyber-attacks is usually classified into three categories: confidentiality, integrity and availability. Loss of confidentiality has no direct impact on the power system. It must be addressed through the use of classical cryptography. Attacks on integrity (i.e. attacks that modify the data that is exchanged between different nodes) can cause wrong control actions either by directly injection/modifying control messages, or by modifying the measurements that are necessary to perform control actions. One advantage of using a state-estimation-based SPS is that it makes False Data Injection Attacks (FDIAs) more difficult. This is because the state estimator is based on a least square method. Measurements that have a high residual can thus be disregarded. This reduces the size of the set of possible successful attacks. There is a large body of literature on FDIAs (see e.g. the review papers [80], [81]). Specific cryptography techniques can also be used to protect integrity of the data (e.g. keyed hashing, authenticated encryption). The focus is thus placed on availability attacks in this section.

An example of availability attack is the Denial of Service (DoS) attack. In its most simple form, it is a volumetric attack that consists in exhausting computer resources by sending large amounts of redundant packets. More complex types of DoS attacks (e.g. reflector-based attacks) exist but they have the same overall effect. The effect can intuitively be seen as a shift to the right in Fig. 4.2. When small to medium amounts of traffic (compared to the available processing capacity of the system) are injected, it results in an increase of delays. When the total arrival rate is larger than the processing capacity of the system, then most packets are dropped; this is the most common case. QoS mechanisms can defend against DoS attacks, but they have to not only reserve bandwidth but also buffers. Other mitigation measures are discussed in dedicated literature.

The high amount of traffic caused by DoS attacks makes them easy to detect. They can thus often be mitigated automatically and relatively quickly. An attacker might thus prefer to use more "subtle" attacks to be less easily detected but still have an impact on the performance of the SPS. For example, if an attacker is able to take control of a router, he can then drop arbitrary packets instead of sending them to their original destination. This will have a different impact depending on the protocols that are used. The IEEE C37.118.2 standards recommends UDP (i.e. no retransmission of lost packets) for the traffic coming from PMUs and TCP (i.e. packets resent until an acknowledgement message is received) for the control traffic (from the CC) [75].

If the attacker is unable to decrypt the packets going through the router he hijacked, he might choose to simply drops half the packets he receives. Since UDP is used, it means that half the data will no longer reach the CC. For example, if the router 1 (from Fig. 4.1b) is attacked, then measurements from either bus 1 or 2 will be unavailable. In this case, we only one measurement is lost. The state estimation algorithm

can thus still compute the state of the whole system. However, in a real-scale system, individual routers (especially those near the CC) would see more measurements. It is thus possible to lose observability on part of the grid (standard methods for observability analysis can be used, e.g. [82]). Control messages on the other hand should never be completely missed, but they might need to be sent several times before being actually received. This introduce additional delays, and it would thus be useful to use a lower retransmission time than what is defined in [79].

If the attacker is able to decrypt the packets, he can cause more harm by dropping specific packets. The attacker could for example specifically drop disconnection messages that are sent to the generators. This basically renders the SPS out of service and a blackout could thus occur in case an action of the SPS is needed. The SPS considered here only has to operate for faults on lines 2, 3 and 7 (and only for some system configurations), so about once per year. The risk caused by such attacks is thus limited. For larger systems that heavily rely on SPS for many different types of faults (e.g. ref. [64] reported 4 operations of its SPS for the first 11 days of 2016), the risk would be higher. It is worth noting that the attacker does not necessarily need to decrypt the packets. A lot of information can be deduced from the non-encrypted headers of the packets (e.g. from the source, destination, and protocol used).

4.3 Perspectives

The probabilistic dynamic security assessment methodology presented in chapter 6 can theoretically be applied either in planning or in operation. However, computation time issues are more stringent in operation which requires additional considerations. A way to circumvent those issues could be to store the results of the security assessment (to be performed all year round). Then, during operation, results associated with similar operating conditions than the current conditions can be retrieved. A similar approach (although in a slightly different context) was proposed in [83]. This is however out of scope of this thesis.

Another perspective is to use a probabilistic security assessment to identify the threats that are more economically handled by a SPS and those that are too critical and require preventive actions (either redispatch or investments).

TODO: Add réunion Jean-Michel 3 Oct 22, MPLS sur le core network, datagramme sur le reste (donc perspectives sur le réseau distrib)

Chapter 5

Model of distribution grids

It has long been acknowledged that load models play have a critical influence on the results of dynamic simulations, especially on voltage stability [84]. Most utilities however use relatively (e.g. compared to generators) simple load models due to the difficulty to gather data on the loads connected to the distribution grid and their variable nature[1]. The most commonly used model is the ZIP load model (aggregation of a constant impedance, a constant current and a constant power load) and its derivatives [85].

The massive installation of distributed renewable energy sources (mostly wind and solar) in distribution grids challenges those load models. In particular interest in this thesis is the tendency of distributed generators to disconnect during wide-area disturbances. These disconnection had a high impact in historical blackouts. For example, the frequency collapse of Italy in 2003 was partly caused by the unexpected disconnection of 3400 MW of distributed generators while the frequency was still above 49 Hz [86, p115]. On the other hand, there are perspectives regarding the provision of ancillary services by distributed generators. Better modelling of those so-called active distribution networks (ADNs) is thus needed.

One way to accurately model the interactions between the transmission and distribution sides of a grid is to perform simulations on complete a transmission and distribution network as in [87][2]. However, this approach cannot be used in this thesis due to the high computational power requirements of probabilistic dynamic security assessment. Outside the scope of this thesis, this approach also has issues of confidentiality and data handling.

Reduced-order load models are thus necessary. Section 5.1 thus reviews load models used in the literatureand section 5.2 discusses perspectives.

5.1 Passive load models

Load models have seen renewed interest in the past decade due post-mortem reproduction of some blackouts being impossible with simple ZIP models [88, p11-12]. It was shown necessary to include at least a simple model of induction machines as in Fig. 5.1. The model of the induction machine can be either static (i.e. only include algebraic equations, so consider the slip s to be constant) or dynamic (i.e. differential-algebraic equations, so the slip varies with time as a function of the balance between the electromagnetic and load torques). More complex load models such as the WECC composite load model (CLM) have also been developed. The CLM is shown in Fig. 5.2. It consists in an on-load tap changer (OLTC), and equivalent feeder impedance, four different types of dynamic induction motor models, and electronic and a static (i.e. ZIP) load. It is being implemented in several time-domain simulators [89]. Various models whose complexity is between the ZIP and CLM models have also been developed and are reviewed by the CIGRE [88] and NERC [89] task forces on load modelling.

The models presented above however do not consider distributed energy sources. The simplest solution to this is to add one (or several) generic model(s) of renewable sources to the load model. However, estimating the parameters that give the most accurate representation of the system might be difficult,

[1] Both the total amount of load and shares of different types of loads (heaters, motors, lamps, etc.) vary with the time of day and the season.

[2] To limit the size of the studied system, it is of course necessary to only consider the medium voltage level of the distribution grids, not the low voltage level.

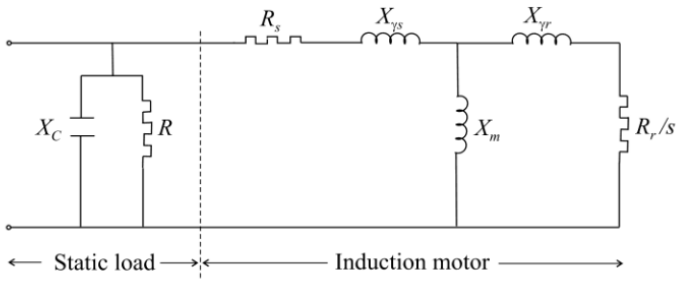


Figure 5.1: Constant impedance load in parallel with an induction motor [88]

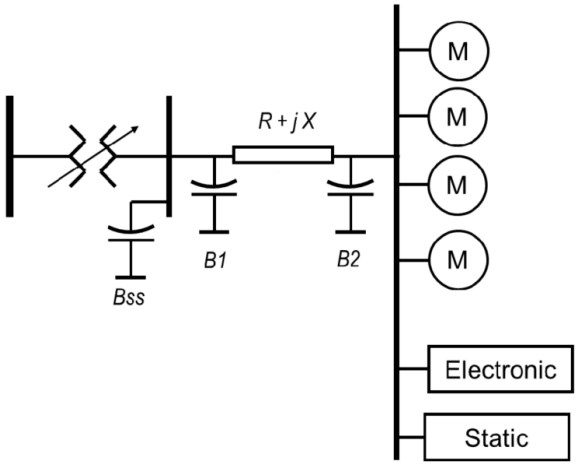


Figure 5.2: WECC composite load model [89]

especially since TSOs have little experience with ADNs compared to ZIP and motor load models. So, four main types of methods were developed in the literature to build ADNs models. They are listed below [90].

- Linear-based approaches: in these methods, the model of the full distribution network is first linearised. Then, different approaches (e.g. Hankel-norm approximation, modal approach, Krylov methods, etc.) allow to reduce the order of the linearised system. A theoretical bound on the error made by using the reduced-order model can be derived depending on the method used. These methods are however accurate only around a given operating point and are thus not appropriate to study large disturbances. These methods were originally developed to make reduced-order equivalents of neighbouring transmission systems. Indeed, TSOs mostly study the impact of disturbances originating in their own system. For moderately large disturbances, neighbouring TSOs are weakly affected, so a linearisation-based approach makes sense. Distribution systems however are much more dependant on their associated transmission system.

- Coherency-based approaches: synchronous generators that tend to swing together are grouped into an equivalent machine. The network around those machines is then also reduced. Like linear-based approaches, these methods were developed to model neighbour transmission systems. They are often not applicable to distribution systems as synchronous generators are rarely used there.

- Black-box approaches: in these methods, the model of a distribution system is an artificial neural network (ANN) that is trained to match the behaviour of the actual distribution system. These methods are quite popular since they do not require any information on the structure and components of the distribution grid. ANNs are thus most often matched to measurements of the behaviour of the distribution grid (often PMU measurements made at the point of common coupling (PCC) between the transmission and distribution grids). It is also possible to train ANNs

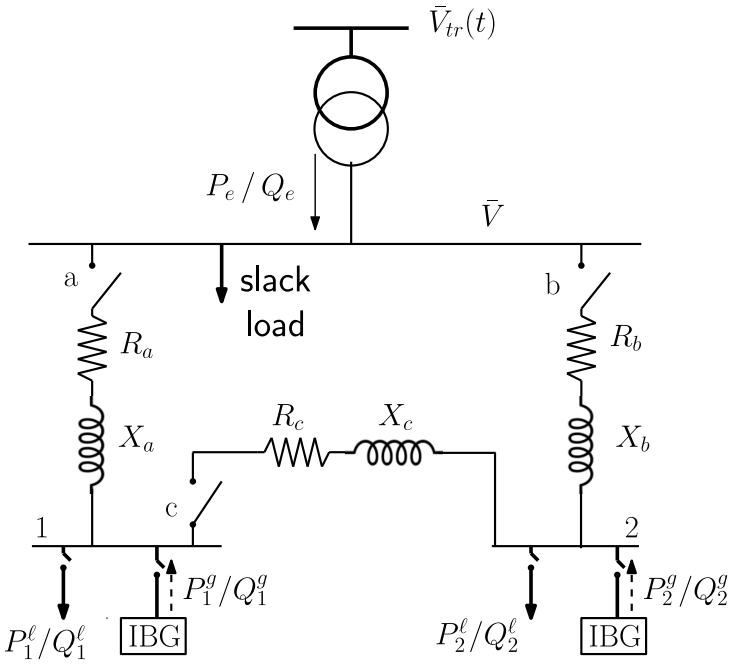


Figure 5.3: Possible grey-box equivalent topologies. Multiple topologies can be created from this scheme by changing the status of the switches [91]. IBG = Inverter-based generation

from simulations of the distribution grid, but grey-box approaches (described below) are often preferred when one has enough information on the distribution grid to simulate it. The main limitation of measurement-based approaches (and by extension black-box approaches) is that large disturbances are rare. It is possible to intentionally introduce disturbances to generate more data but those disturbances are usually kept small for obvious reasons (usually tap changes or capacitor switching). Training ANNs for those disturbances is thus often impossible.

- Grey-box approaches: grey-box approaches are similar to black-box approaches except that the model used is a physical model instead of an ANN. The model usually has at most a few buses and should have a similar structure than the real grid[3]. The advantage is thus that results are more comprehensive, but it is necessary to known the structure of the distribution grid. An example of grey-box model is shown in Fig. 5.3. Like black-box approaches, the parameters of the model are fitted to match the behaviour of the full model (e.g. in the least square sense). As it is not feasible to write the analytical formulation of the objective function (i.e. difference between behaviour of the grey-box and the real system), derivative-free optimisation methods (e.g. genetic algorithms, particle swarm optimisation) have to be used. The behaviour of the real system for a given operating point and disturbance can be obtained either from measurements or from simulations. As previously explained, only the simulation-based approach is appropriate when studying large disturbances[4].

As discussed above, only (simulation-based) grey-box approaches are suitable to study large disturbances. This is thus the type of approach chosen in this thesis. Most recent development on grey-box approaches have been made in the thesis of Gilles Chaspierre [91], [92]. His approach is thus used as a reference in this thesis. He also proposed a methodology to share the grey-box development between the TSO and DSOs to avoid confidentiality issues, and he discussed how to efficiently update the equivalent with varying operating conditions. Interestingly, he also proposed a control algorithm for a battery storage to be installed at the PCC to compensate for errors between the grey-box and the real system. Those elements are however not discussed further here.

[3]Taking the example shown in Fig. 5.3, if switches a and b are closed, and switch c is open, they grey-box model becomes two feeders in parallel. One feeder could represent a classical distribution system. The second, a large distribution-connected plant (with stricter connection requirements).

[4]When available, measurements should still be used to validate the equivalent and/or the full distribution model.

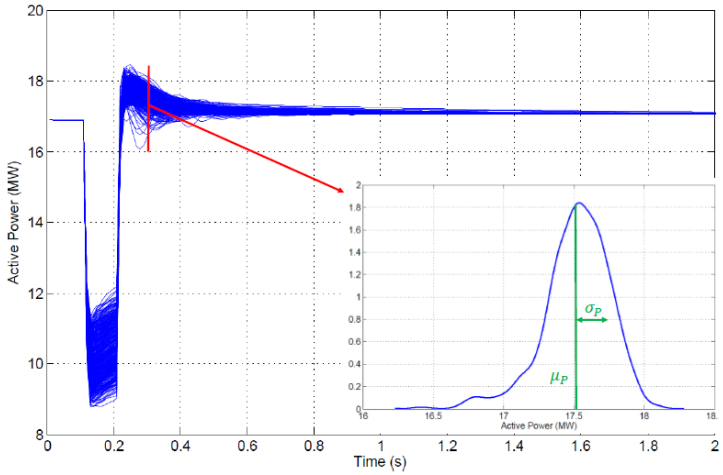


Figure 5.4: Average μ_P and standard deviation σ_P of the active power consumption of a distribution grid following a disturbance at t =0.3 s [91, p58]

5.2 Perspectives

The results in [91] were very satisfactory, so relatively little improvements can be performed[5]. Two main paths can be considered in this thesis. The first is the validation of grey-box models in large-scale studies. Indeed, in the literature, ADN equivalents (including grey-boxes, black-boxes, etc.) are validated in studies were only one distribution system is replaced by an equivalent (the others are simply considered to always behave as simple load models). In this thesis, studies will be performed by replacing all loads by equivalents. Additionally, as I study cascading outages, the models will be further challenged.

Another path to consider is the handling of model uncertainties. In [91], the complete model of the distribution system is simulated with random sets of parameters (e.g. parameters of the control loops of distributed generation, share of renewables, etc.) to account for uncertainties. From these simulations, one deduces the average (i.e. statistical expected) behaviour of the system as well its standard deviation. This is illustrated in the example in Fig. 5.4. The grey-box is then fitting to the average, and the objective function is a least square error weighted by the standard deviation for each point in time. In the rest of the literature, uncertainties are not considered (except measurement errors in measurement-based approaches). In this thesis, I might try to determine if using a single equivalent is appropriate, or if using multiple equivalents associated with different realisations of the uncertainties is necessary. Also, methods to propagate the uncertainties from the full model to the equivalent might be considered.

Finally, as this thesis is made in the framework of the CYPRESS project (presented in appendix A), the possibility to include cyber elements in the equivalents will be studied.

TODO: Fig of equivalent with average parameters vs. correct ones (in draft of ISGT paper), not fully accurate but already way better than simple load model

TODO: (fig 4 of CIGRE paper shows it would be best to cluster, but does not work for multiple disturbances)

[5] A more detailed discussion of potential improvement is done in section 7.2 of [91].

Chapter 6

Probabilistic dynamic security assessment

This chapter is partly based on the following publication:

- F. Sabot, P. Henneaux and P.-E. Labeau, 'MCDET as a tool for probabilistic dynamic security assessment of transmission systems', in *2021 IEEE Madrid PowerTech*, Jun. 2021. DOI: 10.1109/PowerTech46648.2021.9494758

TODO: Use the DPSA acronym. Potentially distinguish between DPSA and probabilistic DSA

TODO: Explain the choice of considered failure modes: EHV faults most likely to causes wide-area issues, EHV protected by diff+distance (in Elia) and talks for double diff, diff is a very good protection, cannot really be misconfigured and self-testing of relays (incl. more advanced stuff like Russian paper in CIGRE 2022 proceedings)

TODO: (D)PSA is more of a process than a methodology, refine the models/data by iteration

The objective of a probabilistic security assessment are to list the possible accident scenarios that can lead to unwanted consequences, to estimate the probability of these scenarios, and to estimate their consequences. Such assessment can be decomposed into two parts: (i) listing (or sampling) the possible pre-contingency states, and (ii) determining the possible post-contingency evolutions. As highlighted in the literature review (section 2.2), the second part is actually the hardest.

In a deterministic approach, only one post-contingency evolution is considered, because one assumes that all transmission equipment and protection systems operate as expected. The evolution is computed by simulation. Often, the protection systems are not explicitly modelled in the simulation. Their effect (e.g. fault clearing by opening a line) is predicted in advance and included in the simulator as part of the contingency. In a probabilistic approach, possible misoperations are considered which leads to multiple possible system evolutions. One way to handle those multiple possible evolutions is to use event trees as done in [24], [25]. Event trees are presented in section 2.2.2 and in Fig. 2.2. In the approach proposed in [24], [25], event trees are built prior running simulations. So, only events that can easily be predicted without simulations can be included[1]. Another limitation of event trees is that event are placed in a so-called event axis instead of a time axis. So, it is assumed that the timing of events does not influence the evolution of the system.

In theory, a skilled analyst can alleviate the above limitations. He can use his expertise and/or simulation results to identify events that can occur during the system evolution. Also, if the order and/or timing of events is of importance, he can add additional events to consider them (e.g. split "event A occurs" in "events A occurs before $t = 5$ s" and "event A occurs after $t = 5$ s). It can however be difficult to compute the probabilities associated with those events. Also, the analyst should try to only consider the most critical scenarios to avoid an explosion of the size of the tree. So, in practice, this requires a lot of effort from the analyst. So-called dynamic event trees (DETs) have thus been

[1] For example, if the initiating event is a line fault, the events that can easily be predicted are the triggering of the protections of this line, and their backup protections.

developed with the objective to move most of the burden of proof of correctness from the analyst to the methodology. DETs are introduced in section 6.1.

It should however first be noted while the above observations have mostly been made in the nuclear sector (wherefrom event trees originated) [93], they are even more relevant for power systems. There is two main reasons for this. First, there are significantly more initiating events to consider. Indeed, one should consider at least hundreds of possible (e.g. line) faults or even more depending on the size of the considered system (and the voltage level(s) considered). Also, for a given fault, multiple event trees should be built as the evolution of the system depends on the initial operating conditions. Second, a large number of events can occur after a disturbance, especially during fast cascading outages. Predicting those events as well as determining the importance of the timing and order of events might prove particularly complex.

Section 6.1 introduces DETs and reviews the literature on the subject. Section 6.2 discusses the proposed methodology. Section 6.3 discusses the data requirements for dynamic probabilistic security assessment, and section 6.4 presents the test cases used.

6.1 Dynamic reliability methods

Note: In the final thesis, this section will introduce more rigorously DETs and the different techniques that can be used to solve them. Also, "dynamic reliability" techniques (that include DETs) will be reviewed. In this report, only MCDET, the specific DET solving technique used in this work, is presented.

A DET follows the (time-dependant) evolution of the system after a given initiating event. This tree branches each time the system can transition to different states. For example, if the initiating event is a line fault, the DET will branch at the times when each of the circuit breakers (CBs) open. In that case, each branch is associated with a possible state of the CBs (i.e. both open, both closed or one open and one closed) and follows the evolution of the system in that given state. Additionally, because the operating time of the circuit breakers is not known with an infinite precision, branchings are made at each point in time were the breakers are likely to operate. If CB opening times are assumed to follow some continuous probabilistic distribution, there is theoretically an infinity of possible branching points to consider. Techniques are thus needed to solve them numerically.

It should be noted that contrarily to "static" event trees, branching points are not defined explicitly but via branching rules. For example, if the line is protected by distance protection scheme, the relays and CBs should be included in the model. Then, during the system evolution, when the apparent impedance seen by a relay goes below a (potentially uncertain) threshold, the relay send a tripping signal to the CB that either opens (after an uncertain amount of time) or fails to open. Branches are automatically created to follow the possible system evolutions (e.g. CB fail to open, CB opens 60 ms after receiving the signal, CB opens 80 ms after receiving the signal, etc.).

One of the available techniques is MCDET. MCDET is a concatenation of MC (Monte Carlo) and DDET (discrete DET). In MCDET, continuous uncertainties (e.g. threshold values, CB opening delays) are handled by MC and discrete uncertainties (e.g. CB fails to open) are handled by DDETs. DDETs are based upon the restriction of the possible branching points to discrete points in time. In other words, the system evolution after a disturbance is simulated, and at each time step branchings are created following aforementioned branching rules. The drawback of DDETs is the combinatorial explosion of the number of branches (that grows as the average number of branches created at each step to the power of the number of steps). To manage this explosion, it is necessary to introduce cutoffs (e.g. do not follow branches that have a probability lower than a threshold) and to increase the size of the time steps. It is however difficult to estimate how the size of the time steps and the cutoff thresholds affect the accuracy of the DET solving method. So, it is difficult to make a good compromise between accuracy and computation time.

In MCDET, a DDET is built for each (MC) sample of the continuous uncertainties. As only discrete uncertainties have to be handled by the DDETs, they can potentially be built completely (i.e. with no cutoffs and a very small time step). In this case, the accuracy of the DET solving technique depends only on the MC part. This is convenient as MC accuracy can be estimated easily with statistical methods.

6.2 Proposed methodology

As discussed in the previous section, the security assessment method used in this thesis is based on MCDET. An additional element has however to be added to the methodology to properly model the pre-disturbance state of the grid. Indeed, given a particular realisation of generator and transmission asset availabilities and load, system operators will try to dispatch power plants to minimise total costs while maintaining acceptable operating conditions (e.g. no overloads, acceptable voltages, etc.). The optimisation problem associated is called an optimal power flow (OPF). When potential (usually N-1) contingencies are considered, this is referred to as a security constrained (SC) OPF.

The methodology can thus be summarised as follow. First, generate a sample of the pre-contingency state (i.e. availability of assets, renewable production, etc.) and consolidate it by running a (SC)OPF program. Then, sample the remaining continuous uncertainties. Build a DDET to handle the discrete uncertainties. Repeat the above procedure until statistical convergence.

TODO: Simplified model of a few steps of slow cascade?

TODO: (Foot)note: sampling protection threshold before simulation implies "tabou" region [44].

6.3 Data requirements for dynamic probabilistic security assessment

Dynamic probabilistic security assessment requires a large amount of input data. The following paragraphs thus discuss the data needed to model the pre-disturbance state, the disturbances themselves, and the post-disturbance evolution.

6.3.1 Pre-disturbance state

The data required to model the pre-disturbance state of the grid is quite similar to the one used in deterministic dynamic security assessment (that is discussed e.g. in [38]). These data consist mainly of generation and load forecasts for the considered period. Planned maintenances are also often included. In a probabilistic assessment, the only additions could be unplanned maintenances and forecast errors. These are not considered in this thesis. Finally, the (SC)OPF also requires some data: running costs of generators (or at least a merit order) and static (current) limits.

6.3.2 Disturbances

In a probabilistic assessment, it is of course necessary to estimate the frequency of occurrence of disturbances. This requires historical statistics of past disturbances.

6.3.3 Post-disturbance evolution

Modelling the post-disturbance evolution of a system in a probabilistic assessment is generally more complex than in a deterministic one. This is because, in a probabilistic analysis, the system has to be simulated further away from normal operation (e.g. during cascading outages). For this, one should generally model the generators (including governors and voltage regulators), loads, transformers, etc. with the best (RMS) models available. If the accuracy of a model is deemed insufficient (e.g. difficulty to reproduce past disturbances, high sensitivity to input data, etc.), then better models have to be developed and/or better data have to be collected.

Additionally, since the system is simulated in degraded states, protections have to be modelled explicitly[2]. This requires to know what protections are installed in the system and what are their settings. Finally, to compute the frequency of scenarios, it is necessary to have an estimate of the probability of failure of protection systems. It is best to also have probability density functions (pdfs) of the protections thresholds[3] and operating times. Pdfs of all aforementioned parameters can also be used to refine the analysis and perform sensitivity studies.

[2] At least, the protections that are discussed in chapter 3.

[3] In order to model measurement and setting errors. The second point is particularly challenging.

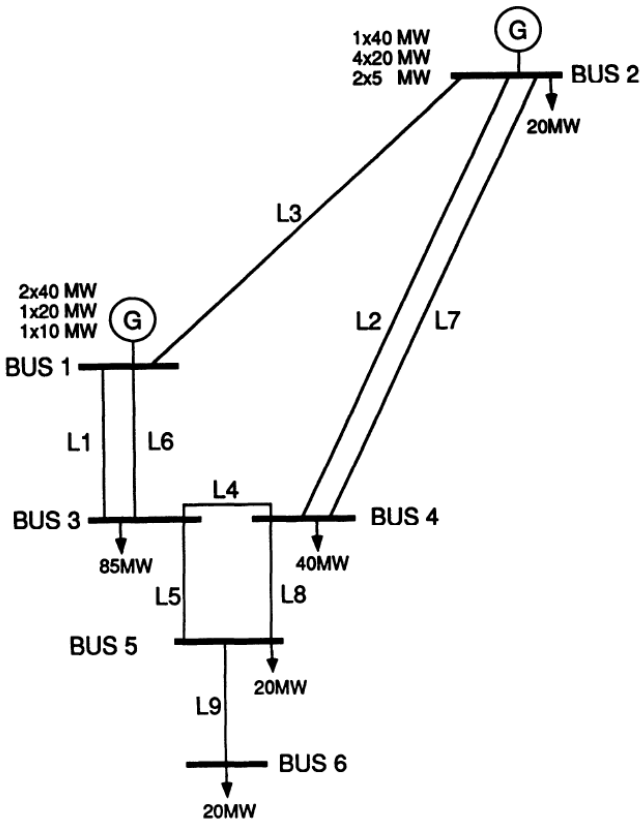


Figure 6.1: Roy Billinton test system. Adapted from [72]

TODO: 2-3 mots sur ce qu'Eurostag appèle le modèle electromec étendu (p117)

6.4 Test cases

The method proposed in this thesis will be applied on a variety of test cases. This report present two of them: the Roy Billinton test system (RBTS) and the three-area reliability test system (RTS). They are shown in Fig. 6.1 and 6.2 respectively. These systems were chosen because they include part of the necessary data (static data, load and generation profiles[4], economic data). Missing data include dynamic data (i.e. generator models) and protection data (types of protection installed, settings and reliability data). Another criterion in the choice of these systems is their size. The RBTS is a small (6-bus) system that can be used in simple case studies and for debugging. The RTS is a medium (73-bus) system that is large enough to represent cascading mechanisms found in larger grids, yet not to large which eases the interpretation of results, data handling and computational issues[5].

The following dynamic data have been added to those systems. Synchronous generators are represented with a seventh order model. For most generators, the excitation system is represented by an IEEET1 model, and the governor is represented with BPA GG (also known as WSCC type G) model as in [95]. A different model is however used for hydro units as they have a fundamentally different behaviour than other types of units. The model used is an GOVHYDRO1 model. Most parameters are taken from annex D of [96]. This annex contains typical data for different types of machines (hydro,

[4]The grid modernization laboratory consortium (GMLC) developed an updated version of the RTS. This version has a significant installed capacity of renewable generation. It also mapped the system to a geographical area such that meteorological data can be used to generate coherent generation forecasts.

[5]Finally, those systems were developed for research on reliability. Contrarily to other systems, parallel lines and parallel generators are not replaced with equivalent elements. This allows to more easily perform N-1 security analysis (double line failures are not accidentally considered as N-1 contingencies) and fill the missing data (generators have more realistic sizes, so typical parameters are easier to find).

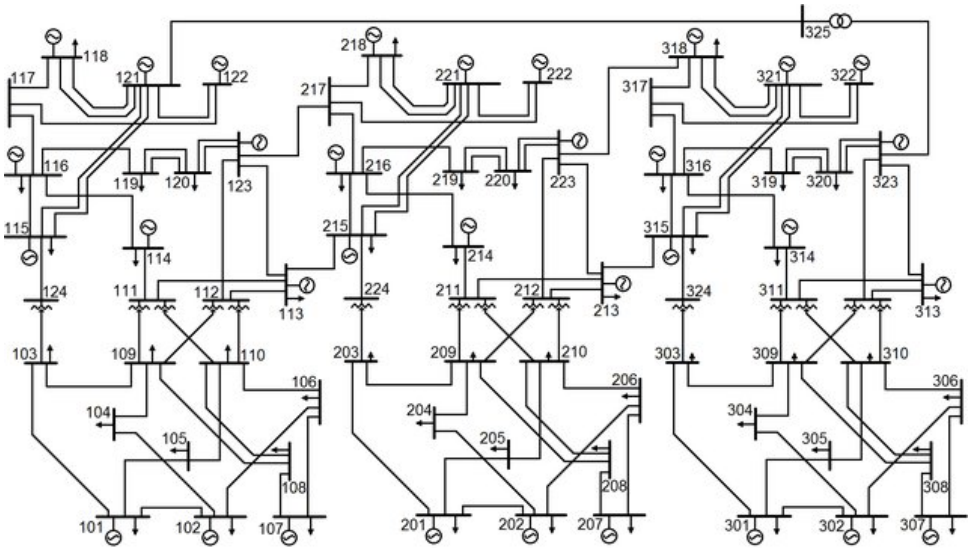


Figure 6.2: Reliability test system [94]

nuclear, coal, gas) and a wide range of rated powers (5 MW to 1.3 GW). So, for each generators of the test systems, parameters were taken from a machine in [96] that has the same type and that has the closest rated power. For hydro units, those parameters are completed with the ones in [97]. Models of wind and solar plants still have to be defined. However, WECC models or the generic inverted-connected generation model proposed in [91] will probably be used. Protection models are discussed in chapter 3.

TODO: Check this 7th order stuff if I have the time, or say "four winding model" model (one field winding, one d-axis damper winding and two q-axis damper windings) according to Dynawo terminology.

'Subsequent analysis is required to understand and mitigate high numbers of unsuccessful simulations'[38]

TODO: robustness analysis even if out of scope of "purely-probabilistic" assessment. E.g. redo analysis with all loads increases by 10% (but with lower statistical accuracy requirements)

Chapter 7

Perspectives

While it is of course expected that a probabilistic dynamic security assessment is more computationally expensive than a deterministic assessment, the difference will strongly depend on the effectiveness of the probabilistic methodology. Uncertainties in the pre-disturbance state of the system are already considered in a traditional dynamic security assessment [38]. So, the added computational effort of a dynamic probabilistic assessment is mainly in the modelling of the post-disturbance evolution. A notable contribution comes from the handling of uncertainties related to protections.

During a (fast) cascading outage, many protections trigger in a relatively short amount of time. Uncertainties in the timing of operations (modifying the order in which protections operate) and the possibility of protection failures can potentially lead to a very large number of scenarios to simulate for a given disturbance. However, it is not clear how many sample of protection timings will be required to correctly represent the possible system evolutions. Also, the risk associated with the many but low-probability possible protection failures is difficult to estimate a priori. The fact that protection failures might have a lower impact once the system has already passed a "point of no return" should also be studied.

The next step in my thesis is thus to provide some answers to the above questions. For this, the proposed methodology will be applied on the RTS (shown in Fig. 6.2). This test system is sufficiently large to represent cascading phenomena that occur in real-scale systems. But it is a priori small enough that the proposed methodology can be applied with manageable computation times. The use of a high-performance computing (HPC) environment and a more efficient simulator than in my previous work [8] will however be required. The results obtained should answer part of the above questions thus allowing to increase the effectiveness of the methodology (i.e. to reduce the computation time required to achieve the same risk assessment accuracy).

A dedicated sampling scheme might be developed in order to answer those questions. For example, the scheme could create more samples in scenarios where protection operations occur in quick succession.

From a practical point of view, it is necessary to implement the following elements:

- DET solving scheme: such a scheme has already been developed in my previous work [8]. It will be adapted to be more general and to work with Dynawo (the dynamic simulator used in this thesis) instead of PowerFactory. It will also be adapted for use in a HPC environment.
- (SC)OPF algorithm: this will be done using PowerModels.jl. It will thus be necessary to implement a PowerModels.jl to Dynawo parser. A Dynawo to PowerModels.jl parser has already been developed by a CYPRESS colleague.
- Add protection models to Dynawo.
- Implement the RTS in Dynawo.

7.1 Following steps

After completion of the above work, the following points will be studied.

- Risk assessment effectiveness: the effectiveness of the proposed methodology will be improved with the answers to the above questions, smart sampling schemes and more advanced DET techniques. In the best case scenario, the objective is to develop a methodology that can be applied for the planning of real transmission systems (with computation times lower than a week).
- Study the impact of load models and in particular, the impact of distribution-connected renewable energy sources and their low-voltage ride-through (LVRT) capabilities.
- Security assessment of future power systems: during the academic year 2022-2023, I will supervise a master thesis on the simulation of inverter-based generation (IBG)-dominated grids. The dynamics of those grids are mainly driven by grid-following and grid-forming converters that have very different behaviour from traditional synchronous generators. This is especially true during large disturbances during which the output current of the converters will more likely be at their maximal capacity.
- Security enhancements: risk assessment methodologies should ideally not be compared on the accuracy of risk estimation but on the recommendations they provide. So, during the last year of this thesis, methods to derive security enhancement recommendations from probabilistic risk assessment studies will be developed.
- The results obtained with the proposed method might be compared with results from QSS cascading methods in the literature.

7.2 Future work

The following points are out of scope of this thesis but are interesting future research tracks.

- Study of slow cascading mechanisms: slow cascading mechanisms still play a major role in some cascading outages, especially during the initial stages. For (usually small) cascades where only slow mechanism play a role, QSS methods available in the literature can be used. For cascades driven by both slow and fast mechanisms, it is more complex.
- Operator models: operators play an important role in the evolution of slow cascading outages. They are however either not consider or modelled with an OPF in QSS methods in the literature. Human errors (that have played important role in some past blackouts) should thus be considered.
- Use in real-time and operation: as discussed in section 4.3, the results of dynamic probabilistic security assessment could be stored for later use in system operation. Also, a SPS could be designed based on the results of the proposed method.

TODO: maintenances + maintanability of system (proba allow to push closer to operational limits, but check that still have some (long one-block) time to do maintenances

TODO: Look at Perspectives from 3.6 of "Stabilité et sauvegarde des réseaux électriques" (marc stubbe, jacques deuze (Tractebel) sous la direction de Michel Crappe (UMons)

TODO: to conclude, goal is not to compute a number (risk) as it is impossible to be perfectly accurate but to understand the system, cf nuclear PSA

(2006, Le projet PEGASE, https://orbi.uliege.be/bitstream/2268/9350/1/SRBE-Pegase.pdf)

Le besoin en simulation dynamique avancée

A l'heure actuelle, l'analyse de la sécu- rité repose généralement sur un modèle statique. Il apparait de plus en plus nécessaire, lorsque l'on se rapproche des limites de fonctionnement du système, de vérifier la qualité de la transition entre les états d'équilibre avant et après incident, mais aussi la stabilité du système, c'est-à-dire sa capacité à rejoindre l'état d'équilibre final. Le modèle dynamique est aussi indiqué pour une représentation précise des protections et automates qui répondent en fonction du comportement transitoire du réseau. Il est nécessaire pour déterminer les limites de stabilité du système telles que, par exemple, l'appa- rition d'oscillations interzonales résul- tant d'une augmentation du transit de puissance entre réseaux. Enfin, la simulation de tout scénario complexe pouvant mener au «black-

out» exige l'usage d'un modèle dyna- mique très détaillé. Par ailleurs, la simulation temporelle «Haute Fidélité» reste la seule voie pour acquérir une compréhension pro- fonde du comportement des grands sys- tèmes électriques. Elle apparait comme indispensable à la formation avancée des opérateurs des centres de conduite. Si le modèle mathématique du système électrique et de ses composants est en principe bien connu, sa mise en œuvre peut poser des problèmes majeurs résultant: – de la taille du modèle (jusqu'à 100.000 variables d'état, voire plus, pour le REI); – de la complexité du modèle (phéno- mènes appartenant à des échelles de temps très différentes, non-linéarités); – du temps de calcul ; – de la disponibilité des données. La taille du système est malheureuse- ment difficile à maîtriser car la modéli- sation doit être complète en (presque) toute circonstance, les différents phéno- mènes dynamiques étant généralement enchevêtrés. La gestion de la complexité implique des procédures rigoureuses de dévelop- pement des modèles de composants et leur validation. Le temps de calcul reste une barrière importante pour beaucoup d'applica- tions. Des développements algorith- miques et l'utilisation d'architectures informatiques spécialisées s'imposent. On notera enfin que la construction du modèle dynamique repose sur l'effort conjugué de toutes les parties pre- nantes: GRT, producteurs, constructeurs agissant de manière concertée pour une meilleure sécurité du système.

TODO: Parler d'EMT, besoin screening

References

[1] Power Systems Engineering Committee, 'Reliability indices for use in bulk power supply adequacy evaluation', *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-97, no. 4, pp. 1097–1103, 1978. DOI: 10.1109/TPAS.1978.354589.

[2] M. Noebels, I. Dobson and M. Panteli, 'Observed acceleration of cascading outages', *IEEE Transactions on Power Systems*, vol. 36, no. 4, pp. 3821–3824, 2021. DOI: 10.1109/TPWRS.2021.3071028.

[3] Vaiman, Bell, Chen *et al.*, 'Risk assessment of cascading outages: Methodologies and challenges', *IEEE Transactions on Power Systems*, vol. 27, no. 2, pp. 631–641, 2012. DOI: 10.1109/TPWRS.2011.2177868.

[4] B. A. Carreras, D. E. Newman and I. Dobson, 'North american blackout time series statistics and implications for blackout risk', *IEEE Transactions on Power Systems*, vol. 31, no. 6, pp. 4406–4414, 2016. DOI: 10.1109/TPWRS.2015.2510627.

[5] F. Sabot, P. Henneaux, I. S. Lamprianidou and P. N. Papadopoulos, 'Statistics-informed bounds for active distribution network equivalents subject to large disturbances', in *IEEE PES ISGT Europe 2023*, Oct. 2023. DOI: Toaddafterpublication.

[6] F. Sabot, P.-E. Labeau and P. Henneaux, 'Handling protection-related uncertainties in simulations of fast cascading outages', in *IEEE PES ISGT Europe 2023*, Oct. 2023. DOI: Toaddafterpublication.

[7] F. Sabot, P. Henneaux, P.-E. Labeau and J.-M. Dricot, 'Impact of the reliability of ICT systems on power systems with system integrity protection schemes', in *23ème congrès de Maîtrise des risques et de Sûreté de Fonctionnement (Lambda Mu 23)*, Paris Saclay, France, Oct. 2022. [Online]. Available: https://hal.archives-ouvertes.fr/hal-03876439.

[8] F. Sabot, P. Henneaux and P.-E. Labeau, 'MCDET as a tool for probabilistic dynamic security assessment of transmission systems', in *2021 IEEE Madrid PowerTech*, Jun. 2021. DOI: 10.1109/PowerTech46648.2021.9494758.

[9] E. Karangelos, K. Thoelen, F. Faghihi *et al.*, *CYPRESS: Report D1.1 describing the selected performance metrics*, Jun. 2021. [Online]. Available: https://cypress-project.be/images/nieuws/cypress_report_D11_executive_summary.pdf (visited on 26/08/2022).

[10] A. Godfraind, F. Sabot, S. B. Mariem, V. Rossetto, P. Henneaux and Y. Vanaubel, 'CYPRESS: Report D1.3 describing the benchmarks', **Note:** Not yet published.

[11] S. Robak, J. Machowski and K. Gryszpanowicz, 'Contingency selection for power system stability analysis', in *2017 18th International Scientific Conference on Electric Power Engineering (EPE)*, 2017. DOI: 10.1109/EPE.2017.7967241.

[12] P. Mitra, V. Vittal, B. Keel and J. Mistry, 'A systematic approach to n -1-1 analysis for power system security assessment', *IEEE Power and Energy Technology Systems Journal*, vol. 3, no. 2, pp. 71–80, 2016. DOI: 10.1109/JPETS.2016.2546282.

[13] ENTSO-E, 'Policy 3: Emergency operations', ENTSO-E, Tech. Rep., 2009. [Online]. Available: https://eepublicdownloads.entsoe.eu/clean-documents/pre2015/publications/entsoe/Operation_Handbook/Policy_3_final.pdf (visited on 25/07/2022).

[14] CIGRE Working Group C4.601, 'Review of the current status of tools and techniques for risk-based and probabilistic planning in power systems', CIGRE, Tech. Rep., Mar. 2010.

[15] P. Henneaux and D. S. Kirschen, 'Probabilistic security analysis of optimal transmission switching', *IEEE Transactions on Power Systems*, vol. 31, no. 1, pp. 508–517, 2016. DOI: 10.1109/TPWRS.2015.2409152.

[16] ACER, *Decision no 07/2019 of the agency for the cooperation of energy regulators of 19 june 2019 on all the TSOs' proposal for the methodology for coordinating operation security analysis*.

[17] Siemens, *PSS/E user manual version 33.4*, Mar. 2013.

[18] DIgSILENT, *PowerFactory 2019 - user manual*, Dec. 2018.

[19] RTE, *ASSESS, une plateforme d'analyse statistique et probabiliste des réeaux électriques*. [Online]. Available: https://www.yumpu.com/fr/document/view/49334695/rte-assess-fr-page-1 (visited on 28/07/2022).

[20] J.-P. Paul and K. Bell, 'A flexible and comprehensive approach to the assessment of large-scale power system security under uncertainty', *International Journal of Electrical Power & Energy Systems*, vol. 26, no. 4, pp. 265–272, 2004, 2002 Conference on Probabilistic Methods Applied to Power Systems, ISSN: 0142-0615. DOI: https://doi.org/10.1016/j.ijepes.2003.10.006.

[21] S. Tamronglak, S. H. Horowitz, A. G. Phadke and J. S. Thorp, 'Anatomy of power system blackouts: Preventive relaying strategies', *IEEE Transactions on Power Delivery*, vol. 11, no. 2, pp. 708–715, 1996.

[22] CIGRE Working Group C1.17, 'Planning to manage power interruption events', CIGRE, Tech. Rep., Oct. 2010. [Online]. Available: https://www.cigreaustralia.org.au/assets/Uploads/c1.17-planning-to-manage-power-interruption-events.pdf (visited on 08/06/2020).

[23] NERC, 'Disturbance reports', NERC, New Jersey, Tech. Rep., 1984–1988.

[24] L. Pottonen, 'A method for the probabilistic security analysis of transmission grids', Ph.D. dissertation, Helsinki University of Technology, Apr. 2005, ISBN: 951-22-7591-0.

[25] L. Haarla, M. Koskinen, R. Hirvonen and P.-E. Labeau, *Transmission grid security: A PSA approach*. London: Springer-Verlag, Jan. 2011, vol. 46. DOI: 10.1007/978-0-85729-145-5.

[26] P. Henneaux, E. Ciapessoni, D. Cirio *et al.*, 'Benchmarking quasi-steady state cascading outage analysis methodologies', in *2018 IEEE International Conference on Probabilistic Methods Applied to Power Systems (PMAPS)*, 2018, pp. 1–6. DOI: 10.1109/PMAPS.2018.8440212.

[27] K. N. Hasan, R. Preece and J. V. Milanović, 'Existing approaches and trends in uncertainty modelling and probabilistic stability analysis of power systems with renewable generation', *Renewable and Sustainable Energy Reviews*, vol. 101, pp. 168–180, 2019. DOI: https://doi.org/10.1016/j.rser.2018.10.027.

[28] M. Noebels, R. Preece and M. Panteli, 'Ac cascading failure model for resilience analysis in power networks', *IEEE Systems Journal*, vol. 16, no. 1, pp. 374–385, 2022. DOI: 10.1109/JSYST.2020.3037400.

[29] M. Rios, D. Kirschen, D. Jayaweera, D. Nedic and R. Allan, 'Value of security: Modeling time-dependent phenomena and weather conditions', *IEEE Transactions on Power Systems*, vol. 17, no. 3, pp. 543–548, 2002. DOI: 10.1109/TPWRS.2002.800872.

[30] J. Song, 'Dynamic modeling and mitigation of cascading failure in power systems', Ph.D. dissertation, Oregon State University, Mar. 2015.

[31] D. Yitian, P. Robin and P. Mathaios, 'Benefits and challenges of dynamic modelling of cascading failures in power systems', in *11th Bulk Power Systems Dynamics and Control Symposium (IREP 2022)*, Banff, Canada, Jul. 2020. [Online]. Available: https://arxiv.org/abs/2207.03389 (visited on 02/08/2022).

[32] E. Ciapessoni, D. Cirio and A. Pitto, 'Cascadings in large power systems: Benchmarking static vs. time domain simulation', in *2014 IEEE PES General Meeting - Conference & Exposition*, 2014. DOI: 10.1109/PESGM.2014.6939469.

[33] Q. Cossart, M. Chiaramello, A. Guironnet and P. Panciatici, 'A novel approach for the calculation of steady states in transmission systems using simplified time-domain simulation', in *2021 IEEE Madrid PowerTech*, 2021. DOI: 10.1109/PowerTech46648.2021.9494933.

[34] RTE, *DynaWaltz*. [Online]. Available: https://dynawo.github.io/about/dynawaltz (visited on 05/08/2022).

[35] J. Matevosyan, B. Badrzadeh, T. Prevost *et al.*, 'Grid-forming inverters: Are they the key for high renewable penetration?', *IEEE Power and Energy Magazine*, vol. 17, no. 6, pp. 89–98, 2019. DOI: 10.1109/MPE.2019.2933072.

[36] S. Ozgur Can, R. Thomas, P. Francesco Giacomo, A. Eros, C. G. Francisco Javier and B. Jef, 'Evolving power systems, addressing stability needs before it is too late', *ELECTRA*, no. 327, Apr. 2023.

[37] J. Song, E. Cotilla-Sanchez, G. Ghanavati and P. D. H. Hines, 'Dynamic modeling of cascading failure in power systems', *IEEE Transactions on Power Systems*, vol. 31, no. 3, pp. 2085–2095, 2016. DOI: 10.1109/TPWRS.2015.2439237.

[38] I. Konstantelos, G. Jamgotchian, S. H. Tindemans *et al.*, 'Implementation of a massively parallel dynamic security assessment platform for large-scale grids', *IEEE Transactions on Smart Grid*, vol. 8, no. 3, pp. 1417–1426, 2017. DOI: 10.1109/TSG.2016.2606888.

[39] Y. Dai, R. Preece and M. Panteli, 'Risk assessment of cascading failures in power systems with increasing wind penetration', *Electric Power Systems Research*, vol. 211, p. 108 392, 2022, ISSN: 0378-7796. DOI: https://doi.org/10.1016/j.epsr.2022.108392.

[40] D. F. Haasl, N. H. Roberts, W. E. Vesely and F. F. Goldberg, 'Fault tree handbook', Nuclear Regulatory Commission, Tech. Rep., Jan. 1981, **Note:** a US VPN is required to access the document because terrorists do not have access to this fancy technology. [Online]. Available: https://www.nrc.gov/docs/ML1007/ML100780465.pdf (visited on 04/08/2022).

[41] N. Samaan, J. Dagle, Y. Makarov *et al.*, 'Dynamic contingency analysis tool – phase 1', Pacific Northwest National Laboratory, Tech. Rep., Nov. 2015. [Online]. Available: https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-24843.pdf (visited on 04/08/2022).

[42] M. A. Elizondo, X. Fan, S. H. Davis *et al.*, 'Risk-based dynamic contingency analysis applied to Puerto Rico electric infrastructure', Pacific Northwest National Laboratory, Tech. Rep., May 2020. DOI: 10.2172/1771798. [Online]. Available: https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-29985.pdf (visited on 04/08/2022).

[43] P. Henneaux, P.-E. Labeau, J.-C. Maun and L. Haarla, 'A two-level probabilistic risk assessment of cascading outages', *IEEE Transactions on Power Systems*, vol. 31, no. 3, pp. 2393–2403, 2016. DOI: 10.1109/TPWRS.2015.2439214.

[44] F. Faghihi, P. Henneaux and P.-E. Labeau, 'Dynamic probabilistic risk analysis of the fast cascade phase of large disturbances in power system', in *11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012, PSAM11 ESREL 2012*, 2012, pp. 586–595.

[45] M. Kloos and J. Peschke, 'Mcdet: A probabilistic dynamics method combining monte carlo simulation with the discrete dynamic event tree approach', *Nuclear Science and Engineering*, vol. 153, no. 2, pp. 137–156, 2006. DOI: 10.13182/NSE06-A2601.

[46] P. Henneaux and J.-C. Maun, 'Numerical techniques for dynamic probabilistic risk assessment of cascading outages', IEEE PES General Meeting, 2016 (Boston, MA): Panel session entitled, "Cascading Outages – Dynamics, Protection, Validation and Data", 2016. [Online]. Available: http://site.ieee.org/pes-cascading/files/2016/07/8-Maun-CFWG-DynamicPRA.pdf (visited on 04/08/2022).

[47] P. Hines, I. Dobson and P. Rezaei, 'Cascading power outages propagate locally in an influence graph that is not the actual grid topology', *IEEE Transactions on Power Systems*, vol. 32, Aug. 2015. DOI: 10.1109/TPWRS.2016.2578259.

[48] B. A. Carreras, J. M. Reynolds-Barredo, I. Dobson and D. E. Newman, 'Validating the opa cascading blackout model on a 19402 bus transmission network with both mesh and tree structures', in *HICSS*, 2019.

[49] L. Duchesne, E. Karangelos and L. Wehenkel, 'Recent developments in machine learning for energy systems reliability management', *Proceedings of the IEEE*, vol. 108, no. 9, pp. 1656–1676, 2020. DOI: 10.1109/JPROC.2020.2988715.

[50] J. J. Bian, A. D. Slone and P. J. Tatro, 'Protection system misoperation analysis', in *2014 IEEE PES General Meeting | Conference & Exposition*, 2014. DOI: 10.1109/PESGM.2014.6939488.

[51] IEEE PSRC working group C12, 'Performance of relaying during wide-area stressed conditions', IEEE, Tech. Rep., May 2008. [Online]. Available: https://www.pes-psrc.org/kb/published/reports/Performance_of_Relaying_During_Stressed_Conditions.pdf (visited on 09/08/2022).

[52] S. H. Horowitz and P. G. Arun, *Power System Relaying*, Fourth. Wiley, 2014, ISBN: 978-1-118-66200-7.

[53] M. Amroune, M. Zellagui, T. Bouktir and A. Chaghi, 'Optimal placement of TCSC to improve voltage stability limit considering impacts on setting zones of distance protection relays', *ACTA Electrotehnica*, vol. 55, pp. 10–18, Jul. 2014.

[54] S. Horowitz and A. Phadke, 'Third zone revisited', *IEEE Transactions on Power Delivery*, vol. 21, no. 1, pp. 23–29, 2006. DOI: 10.1109/TPWRD.2005.860244.

[55] J. Bialek, E. Ciapessoni, D. Cirio *et al.*, 'Benchmarking and validation of cascading failure analysis tools', *IEEE Transactions on Power Systems*, vol. 31, no. 6, pp. 4887–4900, 2016. DOI: 10.1109/TPWRS.2016.2518660.

[56] D. Novosel, G. Bartok, G. Henneberg, P. Mysore, D. Tziouvaras and S. Ward, 'IEEE PSRC report on performance of relaying during wide-area stressed conditions', *IEEE Transactions on Power Delivery*, vol. 25, no. 1, pp. 3–16, 2010. DOI: 10.1109/TPWRD.2009.2035202.

[57] D. Tziouvaras, 'Relay performance during major system disturbances', in *2007 60th Annual Conference for Protective Relay Engineers*, 2007, pp. 251–270. DOI: 10.1109/CPRE.2007.359905.

[58] ENTSO-E "System protection and dynamics" subgroup, 'Technical background and recommendations for defence plans in the continental Europe synchronous area', ENTSO-E, Tech. Rep., Oct. 2010. [Online]. Available: https://eepublicdownloads.entsoe.eu/clean-documents/pre2015/publications/entsoe/RG_SOC_CE/RG_CE_ENTSO-E_Defence_Plan_final_2011_public_110131.pdf (visited on 09/08/2022).

[59] U. Patel, N. Chothani and P. Bhatt, 'Adaptive quadrilateral distance relaying scheme for fault impedance compensation', *Electrical, Control and Communication Engineering*, vol. 14, pp. 58–70, Jul. 2018. DOI: 10.2478/ecce-2018-0007.

[60] ENTSO-E, 'ENTSO-E network code for requirements for grid connection applicable to all generators', ENTSO-E, Tech. Rep., Mar. 2013. [Online]. Available: https://eepublicdownloads.entsoe.eu/clean-documents/pre2015/resources/RfG/130308_Final_Version_NC_RfG.pdf (visited on 10/08/2022).

[61] ENTSO-E, 'P5 – policy 5: Emergency operations', ENTSO-E, Tech. Rep., Sep. 2015. [Online]. Available: https://eepublicdownloads.entsoe.eu/clean-documents/Publications/SOC/Continental_Europe/oh/20150916_Policy_5_Approved_by_ENTSO-E_RG_CE_Plenary.pdf (visited on 10/08/2022).

[62] CIGRE Task Force C2.02.24, 'Defense plan against extreme contingencies', CIGRE, Tech. Rep. 316, Apr. 2007.

[63] R. Hanuise, M. Malichkar and E. Alcázar, 'Ensuring the stability of the Belgian grid with a special protection system', in *47th Annual Western Protective Relay Conference*, Virtual conference, 2020.

[64] D. Dolezilek and D. Rodas, 'Upgrading from a successful emergency control system to a wide-area monitoring, protection, automation, and control system for the country of Georgia power system', in *7th Annual Protection, Automation and Control World Conference*, 2016. [Online]. Available: https://cms-cdn.selinc.com/assets/Literature/Publications/Technical%20Papers/6760_UpgradingSuccessful_DD_20160429_Web2.pdf?v=20171206-212309 (visited on 17/08/2022).

[65] J. Malcón, R. R. Syed and S. K. Raghupathula, 'Implementing a country-wide modular remedial action scheme in Uruguay', in *3rd Annual PAC World Americas Conference*, Glasgow, Scotland, 2015.

[66] N. Liu, 'Reliability assessment of a system integrity protection scheme for transmission networks', Ph.D. dissertation, Department of Electrical & Electronic Engineering, University of Manchester, 2017.

[67] S. Canevese, E. Ciapessoni, D. Cirio, A. Pitto and M. Rapizza, 'Wide area system protection scheme design with an artificial intelligence approach considering communication constraints', in *2016 IEEE International Energy Conference (ENERGYCON)*, 2016. DOI: 10.1109/ENERGYCON.2016.7514080.

[68] W. Yu, Y. Xue, J. Luo, M. Ni, H. Tong and T. Huang, 'An UHV grid security and stability defense system: Considering the risk of power system communication', *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 491–500, 2016. DOI: 10.1109/TSG.2015.2392100.

[69] H. Lin, Y. Deng, S. Shukla, J. Thorp and L. Mili, 'Cyber security impacts on all-PMU state estimator – A case study on co-simulation platform GECO', in *2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*, Taiwan City, Taiwan, 2012. DOI: 10.1109/SmartGridComm.2012.6486049.

[70] U. Knight, *Power Systems in Emergencies: From Contingency Planning to Crisis Management*. Wiley, 2013, ISBN: 9780471490166. DOI: 10.1002/9781118878323.

[71] H. Georg, 'Co-simulation based performance evaluation of ICT infrastructures for smart grids', Ph.D. dissertation, Facultät für Elecktrotechnik und Informationtechnik, Techischen Universität Dortmund, 2015.

[72] R. Allan, R. Billinton, I. Sjarief, L. Goel and K. So, 'A reliability test system for educational purposes - basic distribution system data and results', *IEEE Transactions on Power Systems*, vol. 6, no. 2, pp. 813–820, 1991. DOI: 10.1109/59.76730.

[73] N. Mir, *Computer and Communication Networks*. Prentice Hall, 2015, Accessed on 2022.06.08, ISBN: 9780133814743. [Online]. Available: https://flylib.com/books/en/2.959.1.96/1/.

[74] J. D. Little, 'A proof for the queuing formula: $L = \lambda W$', *Operations research*, vol. 9, no. 3, pp. 383–387, 1961.

[75] 'IEEE standard for synchrophasor data transfer for power systems', *IEEE Std C37.118.2-2011 (Revision of IEEE Std C37.118-2005)*, pp. 1–53, 2011. DOI: 10.1109/IEEESTD.2011.6111222.

[76] National Grid, *Technical specifications 3.02.01: Circuit-breakers*, Accessed on 2022.06.08, 2018. [Online]. Available: https://www.nationalgrideso.com/document/33141/download (visited on 08/06/2022).

[77] RTE. 'Maintaining and making adjustments to the grid'. Accessed on 2022.06.08. (), [Online]. Available: https://www.rte-france.com/en/uninterrupted-flow-current/maintaining-and-making-to-the-grid.

[78] KITZ, *BT 21CN - network topology & technology*. [Online]. Available: https://kitz.co.uk/adsl/21cn_network.htm (visited on 18/08/2022).

[79] M. Sargent, J. Chu, D. V. Paxson and M. Allman, *Computing TCP's retransmission timer*, RFC 6298, Jun. 2011. DOI: 10.17487/RFC6298.

[80] G. Liang, J. Zhao, F. Luo, S. R. Weller and Z. Y. Dong, 'A review of false data injection attacks against modern power systems', *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1630–1638, 2017. DOI: 10.1109/TSG.2015.2495133.

[81] H. Zhang, B. Liu and H. Wu, 'Smart grid cyber-physical attack and defense: A review', *IEEE Access*, vol. 9, pp. 29 641–29 659, 2021. DOI: 10.1109/ACCESS.2021.3058628.

[82] A. Gómez-Expósito and A. Abur, 'Electric energy systems', in Florida: Taylor & Francis Group, LLC, 2009, ch. State estimation.

[83] C. Qiming, 'The probability, identification, and prevention of rare events in power systems', Ph.D. dissertation, Iowa State University, Jan. 2004. DOI: 10.31274/rtd-180813-9878.

[84] P. Kundur, N. Balu and M. Lauby, *Power System Stability and Control* (EPRI power system engineering series). McGraw-Hill Education, 1994, ISBN: 9780070359581.

[85] J. V. Milanovic, K. Yamashita, S. Martínez Villanueva, S. Z. Djokic and L. M. Korunović, 'International industry practice on power system load modeling', *IEEE Transactions on Power Systems*, vol. 28, no. 3, pp. 3038–3046, 2013. DOI: 10.1109/TPWRS.2012.2231969.

[86] UCTE, 'Final report of the investigation committee on the 28 Septembre 2003 blackout in Italy', UCTE, Tech. Rep., Apr. 2004. [Online]. Available: https://eepublicdownloads.entsoe.eu/clean-documents/pre2015/publications/ce/otherreports/20040427_UCTE_IC_Final_report.pdf (visited on 11/08/2022).

[87] P. Aristidou, G. Valverde and T. Van Cutsem, 'Contribution of distribution network control to voltage stability: A case study', *IEEE Transactions on Smart Grid*, vol. 8, no. 1, pp. 106–116, 2017. DOI: 10.1109/TSG.2015.2474815.

[88] CIGRE Working Group C4.605, 'Modelling and aggregation of loads in flexible power networks', CIGRE, Tech. Rep., Feb. 2014.

[89] NERC Load Modeling Task Force, 'Dynamic load modeling', NERC, Tech. Rep., Dec. 2016. [Online]. Available: https://www.nerc.com/comm/PC/LoadModelingTaskForceDL/Dynamic%20Load%20Modeling%20Tech%20Ref%202016-11-14%20-%20FINAL.PDF (visited on 12/08/2022).

[90] F. O. Resende, J. Matevosyan and J. V. Milanovic, 'Application of dynamic equivalence techniques to derive aggregated models of active distribution network cells and microgrids', in *2013 IEEE Grenoble Conference*, 2013, pp. 1–6. DOI: 10.1109/PTC.2013.6652356.

[91] G. Chaspierre, 'Reduced-order modelling of active distribution networks for large-disturbance simulations', Ph.D. dissertation, Université de Liège, Oct. 2020.

[92] G. Chaspierre, G. Denis, P. Panciatici and T. Van Cutsem, 'An active distribution network equivalent derived from large-disturbance simulations with uncertainty', *IEEE Transactions on Smart Grid*, vol. 11, no. 6, pp. 4749–4759, 2020. DOI: 10.1109/TSG.2020.2999114.

[93] P. Labeau, C. Smidts and S. Swaminathan, 'Dynamic reliability: Towards an integrated platform for probabilistic risk assessment', *Reliability Engineering & System Safety*, vol. 68, no. 3, pp. 219–254, 2000. DOI: https://doi.org/10.1016/S0951-8320(00)00017-X.

[94] P. Henneaux and D. Kirschen, 'Probabilistic security analysis of optimal transmission switching', *IEEE Transactions on Power Systems*, vol. 31, Mar. 2015. DOI: 10.1109/TPWRS.2015.2409152.

[95] P. Demetriou, M. Asprou, J. Quiros-Tortos and E. Kyriakides, 'Dynamic ieee test systems for transient analysis', *IEEE Systems Journal*, vol. 11, no. 4, pp. 2108–2117, 2017. DOI: 10.1109/JSYST.2015.2444893.

[96] V. Vittal, J. McCalley, P. Anderson and A. Fouad, *Power System Control and Stability* (IEEE Press Series on Power and Energy Systems). Wiley, 2019, ISBN: 9781119433712.

[97] E. Johansson, K. Uhlen, G. Kjølle and T. Toftevaag, 'Reliability evaluation of wide area monitoring applications and extreme contingencies', in *17th Power Systems Computation Conference, PSCC 2011*, Stockholm, Sweden, Jan. 2011.

Appendix A

Work performed in the framework of the CYPRESS project

Note: Due to time constraints, this chapter is basically empty. I however performed some work in the framework of the CYPRESS project which has not (yet) found a place in this thesis. This work also led to a publication attempt. This will be discussed in more details during the oral presentation.

A.1 CYPRESS project description

The energy transition leads towards smarter electric power systems taking the form of cyber-physical systems in which the electrical power grids are strongly interlinked with a growing number of information and communication systems. The project aims at developing novel knowledge, methods and tools needed to help ensuring the security of supply through the transmission grid, while accounting for the specific nature of cyber-threats and integrating them into a coherent probabilistic risk management approach.

A.2 Co-simulation

To be expanded.

TODO: Say co-simulation can be fast but require good implementation, stop and restart (e.g. PowerFactory) is too slow. Give some ideas of how I did it in Dynawo. Responsibility of the tool developers.