FMEA of a non-selective fault-clearing strategy for HVDC grids

G.D. Freitas[#], A. Bertinato[#], B. Raison[#]*, E. Niel[#†], O. Despouys[‡]

[#]SuperGrid Institute, Villeurbanne, France, guilherme.dantasdefreitas@supergrid-institute.com
*Univ. Grenoble Alpes, CNRS, Grenoble INP[**], G2Elab, F-38000 Grenoble, France
[#]Laboratoire AMPERE, INSA- Lyon, F-69621, Villeurbanne, France
‡Research and Development Dpt, RTE, F-92932 Paris la Défense, France

Keywords: FMEA, HVDC, MTDC, protection, risk.

Abstract

The Failure Mode Effect Analysis (FMEA) is a technique used to investigate failures in a process or component and to identify the resultant effects of these failures on system operations. In this paper it is explained how the FMEA can be used to define and assess the impact of the failure modes (FM) of a protection strategy for High Voltage Direct Current (HVDC) grids. The risk assessment of HVDC protection strategies is important because, despite of being very unlikely, the occurrence of failures during the fault clearing can cause impacts of great severity to the system. Equations for the likelihood and methods to measure the severity of FMs are discussed in the paper. A non-selective protection strategy is used to illustrate the method and the meaning of the risks assessed are discussed.

1 Introduction

High Voltage Direct Current (HVDC) grids are considered to be a promising solution for main problems faced by today bulk power system such as: lines congestion and the integration large amounts of renewable power. Among the challenges in the deployment of a HVDC meshed grid, there is the protection of these grids.

Several propositions for protection strategies for HVDC grids can already be found in literature [1]. Differences between these strategies range from the protection zone size up to the choice of fault suppression equipment. Publications on HVDC protection strategies usually contain only descriptions of actions and simulations of the primary sequence of the strategy. The analysis about what happens in case of failures during the fault clearing is poorly documented.

An investigation on the ways a protection strategy can fail not only exposes its weaknesses, allowing corrective actions to be taken, but also allows an evaluation on the performance of the protection strategy. Such analysis can therefore be useful to evaluate whether the protection strategy can be implemented for a certain case, or even to compare protection strategies.

A protection strategy is composed of several operations of protection equipment that might communicate or not. During the fault clearing process failures may happen, these failures can hamper, delay or have no effect on fault clearing process. The manner in which the steps of the protection strategy or protection equipment can fail are the failure modes of the protection strategy. These FM can be identified and evaluated using the FMEA.

Ideally, the FMEA should be initiated in the early stage of the design process. By doing so, several risks can be mitigated or reduced still in the conception phase. However, in this paper, the FMEA is used to analyze an already defined protection strategy for HVDC grids, and to evaluate the risk of its implementation.

As case study, the HVDC protection strategy using low-speed DC Circuit Breakers (DCCB) described in [2] was chosen. It is a non-selective fault clearing strategy which means that it prioritizes the fast suppression of the fault current over the selectivity. In another words, non-selective fault clearing strategies firstly suppress or reduce the fault current to then identify and isolate the faulty line.

By using FMEA relevant failure modes of the protection strategy are identified. The FMs have their impacts and likelihood estimated. Then, using these two values, the risk that the FM represent to the system can be assessed.

2 FMEA

The Failure Mode Effect Analysis is an analysis tool used to systematically investigate failures in a process or a component and identify the resulting effects on system operations. According to IEC 31010 [7], the FMEA is highly used and recommended for the performance of risk assessment. The same standard refers to risk assessment as the identification, analysis and evaluation of risks of a process or system.

The FMEA is used to reveal possible failures and to foresee the failure effects on the system as a whole. Regarding power grid protection strategies, the method represents a systematic analysis of the steps of the fault clearing in order to identify and evaluate the problems that might happen. For each step in the protection strategy, it must be investigated the possible manners it can fail. Some objectives of the FMEA are [4]:

- To identify in a process the potential failure modes;
- To evaluate the effects of each failure mode on the system;
- To estimate the risk associated with each failure mode;
- To provide information that allow understanding the capabilities and limitations of the process.

[**] Institute of Engineering Univ. Grenoble Alpes.

After the occurrence of a failure, an unwanted effect can be produced. The extent of these effects is indicated by the severity of the FM. The severity can be quantified or qualified in terms of system performance indicators or money loss, for example.

The likelihood of the failure modes is also of interest during the FMEA. According to ISO 31000 [5], likelihood can be defined as the chance that something might happen and it can be expressed either qualitatively or quantitatively. Accurate numbers for likelihood are difficult to find hence intervals are often used to categorize the likelihood of an event.

To ensure a systematic study, a table, referred in this paper as FMEA table, is used to organize the information about all considered FMs. In this table, the FMs are evaluated according to several criteria that vary depending on the application. Common assessments of FMs include severity, likelihood, impacts, causes, and detection methods. From these basic information, others indicators such as risk or risk priority number can be calculated and exposed on the table [4].

A weakness of the FMEA is that it is not suitable for revealing critical combinations of failures. However, for the application on protection strategies such limitation is not problem. As shown in [6], simple failures in HVDC protection strategies are estimated to be rare, so multiple failures are even more difficult to happen.

2.1 FMEA for HVDC grid protection strategies

In power system protection two main categories of failure modes are considered: failure to operate and undesired operation [7]. While the former indicates a missing operation when the protection equipment is needed, the latter relates to operations of the protection equipment under conditions it is not designed to react to. Similarly to [8], the FMs indicating failures to operate will be referred as *dependability failure modes*, and the FMs indicating an undesired operation will be referred as *security failure modes*.

Two security failures are mainly considered in power systems protection: spurious and sympathetic operation [7]. A spurious operation consists of an unwanted action of the protection equipment when there is no fault in the grid. And a sympathetic trip is when the protection operates unnecessarily after a fault in an adjacent zone.

A description of the protection strategy is required for the identification of the FMs. The more detailed the description is, the more detailed the FMEA can be. Descriptions with a clear division of the protection strategy in steps are particularly useful for the identification of the failure modes.

An initial approach to define the FMs is to consider a dependability and the two previously described security failures for each step of the protection strategy description. In AC protection systems, for example, these three FMs represent 95% of the protection systems misoperations [9] .

Once the failure modes are defined, their impact must be assessed. In power systems, there is a variety of impacts that can be considered in such analysis. For example, the impact can be based on grid's electrical or mechanical values such as bus voltage, lines overload [10] or mode damping [11]; it can also be monetized and addressed as a cost [12].

A way to describe an impact in power systems is by using the outage caused by the failure. Outages are specified by indicating the component (or amount of power) lost and the duration of the loss. Information about the outages caused by a FM can often be obtained by simply screening the grid topology and the protection strategy description.

The severity of the FMs is decided based on their impacts. When the impacts are specified quantitatively a function can be defined to establish the relationship between the impact and the severity [13]. The quantification of severity is not always possible and frequently a severity matrix is used to assign a risk to a FM. Table 1 is an example of a bidimensional severity matrix for impacts described in terms of DC grid components outage – component lost and duration of loss.

Table 1: Example of severity matrix for DC grid components outage.

Component lost	**Duration (ms)**		
	<100	100-500	>500
Line	Minor	Low	Low
1 Converter *	Low	Low	Medium
1 Converter **	Low	Medium	Medium
Entire grid *	Low	Medium	High
Entire grid **	Low	High	High

* DC side disconnection (STATCOM operation possible)
** AC side disconnection.

Concerning the likelihood of the failure modes, some assumptions commonly adopted for AC protection system reliability studies are, in this paper, considered to be valid also for DC protection [7]:

- The Mean Time To Failure (MTTF) of the protection components is much greater than the Mean Time To Repair (MTTR) of these components.
- The failure modes are independent and happen with a constant failure rate.

The likelihood of the FMs is calculated depending on the nature of the failure mode. For a dependability failure of equipment X, FM_{DX}, the likelihood can be calculated as:

$$\text{Likelihood}\,(FM_{DX}) = \alpha_X \times U_X \times \prod_{E \in S-\{X\}} (1 - U_E) \qquad (1)$$

where:

- α_X is the fault rate in the protection zone of equipment X;
- U_X is the unavailability of component X;
- S is the collection of all equipment required for the fault clearing.

It is possible to find the occurrence rate of spurious actions of some protection components; these rates can be used as the likelihood of spurious operation [8].

The likelihood of, FM_{SX}, a sympathetic operation of component X, can be calculated as:

$$\text{Likelihood}\,(FM_{SX}) = \sum_{l \in L} \lambda_l \times (1 - U_{Pl}) \times P(X|\tilde{l}) \qquad (2)$$

where:

- L is the collection of all protection zones adjacent to X;
- λ_l is the fault occurrence rate in the protection zone l;
- U_{Pl} is the unavailability of the protection equipment of the protection zone l;
- $\tilde{l}$ is the event of a successfully cleared fault in line l;
- $P(X|\tilde{l})$ is the probability of X operate given that $\tilde{l}$ happened.

The likelihood calculated using Equations (1) or (2) has the same unit as the failure rate. If the FMs are defined in terms of actions involving several protection equipment, the likelihood of the FM is calculated considering the failure of each component at a time.

Similarly to the severity, the likelihood of a FM can be divided into categories. The use of intervals for likelihood is common when reliability data is scarce or incomplete. The categories are defined such as they are relevant for the application case. In Table 2, an example of likelihood categories based on intervals of occurrence per year can be found.

Occ./year	Likelihood
>0,02	Regular
0,02-0,01	Probable
0,01-0,005	Occasional
0,005-0,002	Remote
<0,002	Unlikely

Table 2: Example of likelihood categories.

Once the severity and likelihood of a FM are known its risk can be evaluated. When quantities are used to express the likelihood and severity, the risk can also be calculated as a quantity [10]. However, if a qualitative analysis has been carried out, the use of a risk matrix is more suitable.

The risk matrix combines the categories of likelihood and severity to evaluate the risk of a FM. The risk matrix has the advantage of being readily adapted for application to any specific system [11].

Table 3 and Table 4 are examples of risk matrix for two different HVDC grids, System I and System II respectively. The tables are based on the categories of severity and likelihood found in Table 1 and Table 2. The risk in the matrices is divided into 5 categories: negligible, low, medium, high and unacceptable. The meaning of these categories is defined based on several criteria such as: grid code, money losses, quality or service, etc.

Likelihood	Severity			
	Minor	Low	Medium	High
Regular	Negligible	Medium	High	Unacceptable
Probable	Negligible	Low	High	Unacceptable
Occasional	Negligible	Low	Medium	Unacceptable
Remote	Negligible	Low	Medium	High
Unlikely	Negligible	Negligible	Medium	High

Table 3: Illustrative example of risk matrix for System I.

Likelihood	Severity			
	Minor	Low	Medium	High
Regular	Negligible	Low	Low	Medium
Probable	Negligible	Negligible	Low	Medium
Occasional	Negligible	Negligible	Negligible	Low
Remote	Negligible	Negligible	Negligible	Low
Unlikely	Negligible	Negligible	Negligible	Low

Table 4: Illustrative example of risk matrix for System II.

Therefore, the combination of likelihood and severity that specifies a certain level of risk can change depending on the criteria considered. Such flexibility in the definition of the risk can explain the differences between Table 3 and Table 4.

To expose all the relevant information about the FMs of HVDC grids protection strategies, this paper proposes a FMEA table organized into 6 columns:

- Failure Modes: all considered ways that a certain action of protection strategy can fail.
- Tag: each FM has an associated tag. The tag is used to ease the reference to the FMs.
- Impacts: in this column, it is described how the system is impacted by the specific FM.
- Severity: based on the impacts identified, this column will contain a qualitative or quantitative evaluation of the total impact of the FM.
- Likelihood: this column contains the value or category estimated for the FM's likelihood.
- Risk: the value or category of risk are assigned for the FMs in this column.

In Section 3, an example is shown to illustrate the use of the FMEA table and how to fill the above listed columns.

3 Case study

The bipolar HVDC chosen for the application case is the same as proposed in [1]. The grid topology and protection equipment are shown in Figure 1. Only pole-to-ground faults are considered in the assessment.

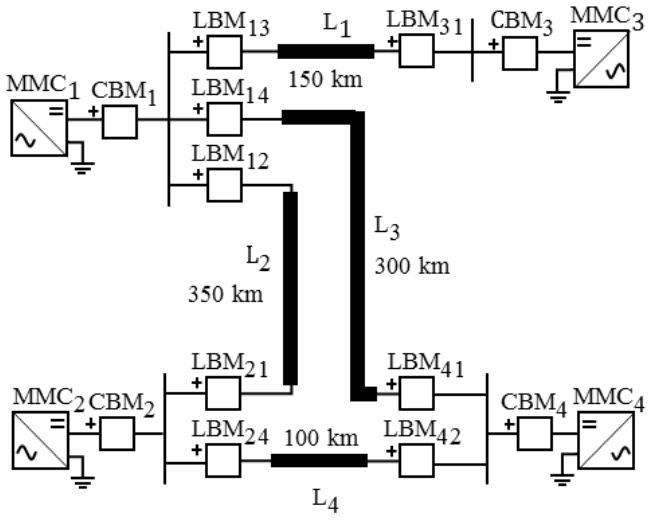

Figure 1: Case study grid architecture.

In Figure 1, the protection equipment is represented by the Line and Converter Breaking Modules – LBM and CBM respectively. LBMs and CBMs have the same components and they differ from each other mainly in their placement and function of their relays. The components of the Breaking Modules (BM) are shown on Figure 2.

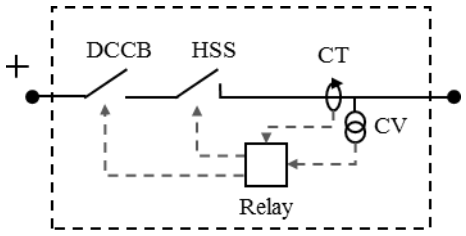

Figure 2: Breaking module.

The DC circuit breaker (DCCB) in Figure 2 is in series with a High Speed Switch (HSS), which differs from the DCCB as it has no DC current breaking capability (only AC current breaking capability). In Table 5, the time specifications for the components of the BM are found.

Component	Specification	Value
DCCB	Opening time	10-20 ms
	Reclosing delay	50 ms
HSS	Opening time	10 ms
Relay	Detection time	μs to ms
	Faulty line identification time	few ms
	Breaker failure detection	few ms

Table 5: Parameters considered for the components used in the protection strategy.

Regarding the protection strategy, the non-selective protection strategy based on low-speed DC circuit breakers described in [2] was chosen. A flowchart for the protection strategy is shown in Figure 3. The terms line and converter breakers found in the figure refer to the DCCBs at the line and converter breaking modules respectively.

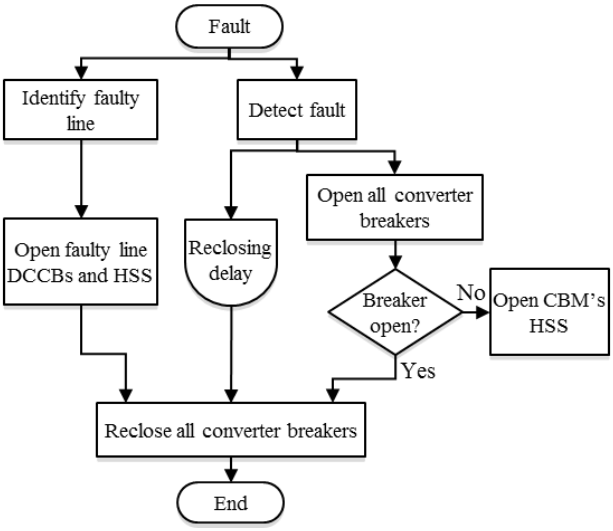

Figure 3: Flowchart of the protection strategy.

3.1 FMEA of case study

The protection strategy description is used in the definition of the failure modes. Only the primary sequence will be analyzed. Concerning dependability failure modes, a failure in operation of every action in Figure 3 is considered. For the sake of simplification, the only security failure considered is the spurious operation of the BMs. Therefore, for the protection strategy analyzed, the following failure modes are identified:

- Fail to detect;
- Fail to open converter breaker;
- Fail to identify the faulty line;
- Fail to isolate the faulty line;
- Spurious operation of CBM;
- Spurious operation of LBM.

The FM *failure to isolate the faulty line* express the opening failure of both the DCCB and HSS of the faulty line (Figure 3).

In the case study, the following hypotheses are considered for the FMs and protection equipment:

- In case of spurious trip of a breaker, the reclosing will be commanded right after its reclosing time has elapsed.
- If any component of the breaking module is unavailable, the entire BM is considered unavailable.
- If any component of the BM presents a security failure, it will lead to the opening of the BM's breaker.
- For the sake of simplification the detection and identification of the fault are considered to be based on local measurements.
- If after the detection the converter is not isolated by its CBM, its AC breaker will be tripped.
- If the converter DCCB recloses and the fault persists in the grid, it will open again and remain open for an undetermined amount of time.

As shown in Equation 1 the rate of fault occurrence in the cables of the case study grid is required. The failure rates of 480×10^{-6} and 880×10^{-6} failures/year/km were considered for the submarine and underground cables respectively [14].

Due to the low technological readiness level of HVDC grid protection equipment, some assumptions are made regarding the availability of these components. All protection equipment, with the exception of the DCCBs, are considered to have a reliability similar to their analogous in function and ratings on AC transmission. Regarding the DCCB, an unavailability of 0.0003 is considered [14].

Similarly to [8], the effect of setting errors, hidden failures, and failures on the dc power systems (batteries) are also considered as causes of breaking modules misoperation. Using the data found in [1] and [8], an unavailability of 0.0012 and a security failure rate of about 0.003 occurrences per year are considered for the BMs. No redundancy for the relay or measurement equipment (VT and CT) is considered.

The rate of occurrence of the FMs are found on Table 7. Equation (1) was used to find the occurrence rate for the dependability failure modes. For the security failure modes, the occurrence rate is determined by the multiplication of the security failure rate of the BMs by the number of BMs that can present the FM.

In Table 7, two failure rates were attributed to the FM named *spurious operation of LBM*. As it will be further explained, due to the asymmetric architecture of grid, this failure mode can lead to different impacts. Therefore, a distinction regarding the possible impacts of this failure mode was required. Also in Table 7, a tag is defined for the failure modes.

As explained in Section 2.1, the impact of the failure modes must be identified and several metrics can be used for such task. For the case study a definition of impact in terms of outages of DC grid's components is chosen. Table 8 presents the outages identified for the FM on Table 7. When the time is not specified, a duration longer than few seconds is assumed.

Failure mode	Tag	Occ./year
Fail to detect	FM1	0,0055
Fail to open converter breaker	FM2	0,0136
Fail to identify the faulty line	FM3	0,0027
Fail to open faulty line breaker	FM4	0,0068
Spurious operation of CBM	FM5	0,0224
Spurious operation of LBM	FM6.1	0,0112
	FM6.2	0,0336

Table 7: Occurrence rate estimated for the FMs.

Tag	Impact
FM1	AC side converter disconnection
FM2	DC side converter disconnection
FM3	DC side disconnection of all converters
FM4	DC side disconnection of all converters
FM5	DC side converter disconnection for 60-80 ms
FM6.1	DC side converter 3 disconnection for 60-80 ms
FM6.2	Loss of a line for 60-80 ms

Table 8: Outages identified for the different failure modes.

Once the severity function or table is defined, the severity of the FMs can be assigned. Taking the Table 1 for example, the severity assignment for the impacts can be accomplished by crossing the impacts identified on Table 8 with the outages severity shown in Table 1.

With the likelihood and severity of the FMs, their risk can be evaluated. As previously explained, the meaning of a level of risk depends on the criteria defined for the application. Taking as example Table 3 and Table 4, it can be noticed that the same failure mode can have different meanings for System I and System II.

Using Table 3 and Table 4 to define the risk of the FMs, the proposed FMEA table for the HVDC protection strategy proposed in the study case can be completed. In Table 6, the FMEA table has 2 columns for the risk: Risk I and Risk II. The former represents the risk of the FMs for System I (Table 3) and the latter for System II (Table 4).

Table 6: FMEA table for the case study considered.

Failure mode	Tag	Impact	Sev.	Likelihood	Risk I	Risk II
Fail to detect	FM1	AC side converter disconnection	Medium	Occasional	Medium	Negligible
Fail to open converter breaker	FM2	DC side converter disconnection	Medium	Probable	High	Low
Fail to identify the faulty line	FM3	DC side disconnection of all converters	High	Remote	High	Low
Fail to open faulty line breaker	FM4	DC side converter disconnection for 80-120 ms	Minor	Occasional	Negligible	Negligible
Spurious operation of CBM	FM5	DC side converter disconnection for 60-80 ms	Low	Regular	Medium	Low
Spurious operation of LBM	FM6.1	DC side MMC 3 disconnection for 60-80 ms	Low	Probable	Low	Negligible
	FM6.2	Loss of a line for 60-80 ms	Minor	Regular	Negligible	Negligible

No failure modes with unacceptable level of risk are found in Table 6. In case of a failure mode having an unacceptable risk level, actions for risk mitigation must be performed in order to reduce the likelihood or severity of such failure mode.

As shown in Table 6, according to the criteria considered, the failure modes with the higher risks are FM2 and FM3. Despite these two failure modes being classified in the same risk category, these two failure modes are in different categories of severity and likelihood. FM2 has a lower severity than FM3 but it is more likely to happen. Since the risk is directly related with these two values, from the point of view of risk to the system, FM2 and FM3 have a similar risk.

5 Conclusions

Despite of evaluating whether the successful performance of the protection strategy copes with the system requirements being important, the strategy must also fulfil certain requirements when it is not successful. Therefore, to have a deep understanding of the impact of the HVDC protection failures on the power system, an assessment of the protection misoperations is required.

A way to perform the Failure Mode Effect Analysis for HVDC grid protection strategies was presented in the paper. How to define possible failure modes were presented including equations for their likelihood.

The FMEA was used to identify and to evaluate the risks of the failure modes of a non-selective HVDC protection strategy for two specific systems. A qualitative approach was used in the case study; categories for likelihood, severity and risk were defined to evaluate the FMs. The results obtained in the analysis were organized in a FMEA table, which contains all relevant information for the analysis. Such table allows comparing the risk of failure modes by screening.

By using the information found in the table, the most hazardous failure modes can be identified. With the most relevant failure modes identified, risk reduction actions can be taken if needed, to reduce the severity or the likelihood of the failure modes until their level of risk is reduced to an acceptable level.

Finally, despite the FMEA being widely known methodology for risk assessment of processes, it is not yet the case for its application for HVDC grids. Therefore, further works on the subject will focus on refining the quantification of severity of failure modes and on how to define the criteria that should be considered during the categorization of risk, severity and likelihood.

Acknowledgment

The work was funded by Horizon 2020 PROMOTioN (Progress on Meshed HVDC Offshore Transmission Networks) project under Grant Agreement No. 691714.

References

[1] PROMOTioN, "D4.2 – Broad comparison of fault clearing strategies for DC grids," 2017. [Online]. Available: https://www.promotion-offshore.net/results/deliverables/. [Accessed: 17-Jul-2018].

[2] D. S. Loume, A. Bertinato, B. Raison, and B. Luscan, "A multi-vendor protection strategy for HVDC grids based on low-speed DC circuit breakers," presented at the 13th IET International Conference on AC and DC Power Transmission (ACDC 2017), Birmingham, UK, 2017.

[3] "IEC 31010:2009 - Risk management - Risk assessment techniques," International Electrotechnical Commission, 2009.

[4] IMCA, "Guidance on Failure Modes & Effects Analyses (FMEAs)," International Marine Contractors Association, Apr. 2002.

[5] "ISO 31000:2009 Risk management - Principles and guidelines," International Organization for Standardization, 2009.

[6] G. D. Freitas *et al.*, "Assessment methodology and performance indicators for HVDC grid protection strategies," presented at the 4th International Conference on Developments in Power System (DPSP 2018), Belfort, UK, 2018.

[7] V. V. Vadlamudi, O. I. Gjerde, and G. H. Kjølle, "The impact of protection systems on power system reliability," SINTEF Energi AS, 2014.

[8] E. O. Schweitzer, D. Whitehead, H. J. A. Ferrer, D. A. Tziouvaras, D. A. Costello, and D. S. Escobedo, "Line protection: Redundancy, reliability, and affordability," presented at the 64th Annual Conference for Protective Relay Engineers, 2011, pp. 1–24.

[9] NERC, "Misoperations Report," North American Electric Reliability Corporation, Jan. 2013.

[10] M. Ni, J. D. McCalley, V. Vittal, and T. Tayyib, "Online risk-based security assessment," *IEEE Trans. Power Syst.*, vol. 18, no. 1, pp. 258–265, Feb. 2003.

[11] R. Preece and J. V. Milanović, "Risk-Based Small-Disturbance Security Assessment of Power Systems," *IEEE Trans. Power Deliv.*, vol. 30, no. 2, pp. 590–598, Apr. 2015.

[12] V. Vittal, J. D. McCalley, V. V. Acker, W. Fu, and N. Abi-Samra, "Transient instability risk assessment," in *1999 IEEE Power Engineering Society Summer Meeting. Conference Proceedings (Cat. No.99CH36364)*, 1999, vol. 1, pp. 206–211 vol.1.

[13] K. N. Hasan, R. Preece, and J. V. Milanović, "The Influence of Load on Risk-Based Small-Disturbance Security Profile of a Power System," *IEEE Trans. Power Syst.*, vol. 33, no. 1, pp. 557–566, Jan. 2018.

[14] Sinclair Knight Merz, "Calculating target availability for HVDC interconnectors," Ofgem, Final report, Dec. 2012.