Risk-based DC Security Assessment for Future DC-Independent System Operator

F. Gonzalez-Longatt
Centre for Renewable Energy Systems Technology (CREST)
Loughborough University
Loughborough, UK
fglongatt@fglongatt.org

C. Carmona-Delgado,
J. Riquelme, M. Burgos
Escuela Superior de Ingenieros,
Universidad de Sevilla
Seville, Spain
cristinacarmonadelgado@gmail.com

J. L Rueda
Department of Electrical Sustainable Energy, Delft University of Technology, Mekelweg 4, 2628 CD
Delft, The Netherlands
j.l.ruedatorres@tudelft.nl

***Abstract*—The use of multi-terminal HVDC to integrate wind power coming from the North Sea opens de door for a new transmission system model, the DC-Independent System Operator (DC-ISO). DC-ISO will face highly stressed and varying conditions that requires new risk assessment tools to ensure security of supply. This paper proposes a novel risk-based static security assessment methodology named *risk-based DC security assessment* (RB-DCSA). It combines a probabilistic approach to include uncertainties and a fuzzy inference system to quantify the systemic and individual component risk associated with operational scenarios considering uncertainties. The proposed methodology is illustrated using a multi-terminal HVDC system where the variability of wind speed at the offshore wind is included.**

Keywords— Fuzy; Fuzzy Inference system; HVDC; multi-terminal HVDC; randomness; risk; security assessment; uncertainty; wind power

I. Introduction

The draft *Network Code on High Voltage Direct Current Connections and DC-connected Power Park Modules* promotes investments in infrastructure in a non-discriminatory way, fair access to the network for new entrants and transparency in the market. These conditions make possible the rise of a new transmission system model, the *DC-Independent System Operator* (DC-ISO). There are so many challenges to be faced by the futures DC-ISO, however the exclusive uses of HVDCs to facilitate cross-border bulk power transfers and the massive integration of offshore wind power coming from the North Sea, along with dynamically changing market, will entail facing increasing uncertainties in the transmission system operation. Hence, DC-transmission asset will be prone to be operated in more highly stressed and varying conditions, so *risk assessment tools* are crucial to ensure security of supply [1].

Assessing power system security in an environment massively populated by uncertainties is a complex and comprehensive task involving a multitude of factors, and dimensions. Several methodologies for security assessment have been developed over decades, each solving a specific part of the overall problem and there are different indicators in use to describe security [2]. Considerable effort has been devoted to the power system risk assessment using the probabilistic techniques [3], [4]. More recent, efforts to introduce online dynamic and static security assessment has been well documented in literature [5], [6]. Probabilistic techniques are often utilized in security assessment of HVDC system [7], however, there is a lack of development in terms of risk assessment of model *multi-terminal HVDC systems* (MTDC).

This paper proposes a novel *risk-based static security assessment* (RSSA) methodology named *risk-based DC Security Assessment* (RB-DCSA). It is used to quantify the risk associated with forecasted operational scenarios by considering the probability and severity of DC-voltage excursions, overload on cables and converter stations. The methodology provides an efficient risk assessment to a future *DC-Independent System Operator* (DC-ISO). It is based on indices (per individual component and system) which facilitate the decisions-making process in a time frame in which the decision is effective. The paper is organized as follows: Section II briefly defines the main considerations about DC-ISO and establishes the backgrounds about DC voltage and power control modes in MTDC with a brief discussion about probabilistic power flow. Section III focuses on the risk-based static security assessment proposed in this paper. Section IV presents on-line risk inference system strategy and Section V presents the proposed methodology. Section VI illustrates application examples on a representative test system of a future DC-ISO. Section VII concludes.

II. DC-Independent System Operator (DC-ISO)

One key element of the liberalization of electricity sector was separation of the control of the operation (and often the ownership) of the transmission system to ensure fair competition between generation companies requiring access to the monopoly transmission system. The United States of America has generally followed one model for achieving this – the creation of a stand-alone *independent system operator* (or ISO), later also known as a *regional transmission organization* (or RTO). The ISO has responsibility for controlling the access to and use of the transmission grid by competing generators and retailers. Europe has similar organizational categories to ISO, the European commission defines the term *transmission system operator* (TSO) as a company that is responsible for operating, maintaining and developing the transmission system for a *control area* and its interconnections. In England and Wales a different model for facilitating competition was followed, with the creation of the *National Grid Company*

(NGC). NGC is an *independent transmission system operator* (ITSO) which owns the transmission wires as well as controls their operation.

The introduction of HVDC grids brings with it major challenges, and opportunities. It has being recognized by ENTSO-E by creation of the most recent draft *Network Code on High Voltage Direct Current Connections and DC-connected Power Park Modules* [8]. It establishes rules for HVDC Systems and a common framework for connection agreements between network operators and all agents involved. *Network Code* established that any natural or legal entity is allowed to owning or developing a HVDC system. It opens the door to promote investments in infrastructure in a non-discriminatory way, fair access to the network for new entrants and transparency in the market -EU law 2009/72/EC.

The most popular European Model on transmission system is the *ownership unbundling* (OU) and using this clear-cut separation two possible scenarios on HVDC systems: (i) *DC-Independent System Operator (DC-ISO)*: a fully unbundled HVDC System Operators without the grid assets (still belonging to an integrated company) and (ii) *DC-Independent Transmission Operators (DC-ITO)*: a DC Transmission System Operator owning the assets and belonging to a vertically integrated company, with special rules to guarantee its independence. In this paper, DC-ISO is defined as *a private or public entity, and it to coordinates, controls and monitors the operation of the DC transmission system involving one or several power park modules and one or several TSOs*. DC-ISO is expected to perform the same functions as ISOs, but cover only the MTDC system.

A. DC Voltage and Power Control Modes in MTDC

There a are three main DC voltage control modes used on a VSC-HVDC terminal [9]: (i) *constant power mode*, (ii) *constant voltage mode* or (iii) *droop mode of control*. The DC voltage versus power characteristic curve those controllers are shown on Fig.

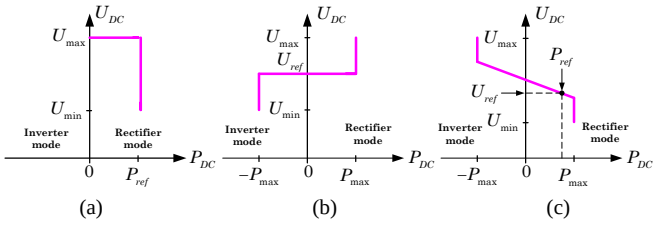


Figure 1. DC voltage versus power characteristics. (a). DC bus power controller (b). DC voltage regulator (c). DC voltage droop controller.

The DC voltage characteristics of *constant power control mode* is such that the power flow via the VSC-HVDC terminal (P_{DC}) remains constant and equal to the power reference (P_{ref}) regardless of the level of the DC voltage (U_{DC}), hence the vertical characteristic line in Fig. 1(a). *Constant DC voltage control mode* is such that VSC-HVDC voltage level (U_{DC}) remains constant and equal to the DC voltage reference (U_{ref}) regardless of the level of the power (P_{DC}). The DC characteristic curve of a constant DC voltage controller is horizontal line corresponding to the dc voltage reference (U_{ref}) depicted in Fig. 1(b).

DC voltage droop control can be seen as a combination of the two types of VSC-HVDC controls. It tries to control power to its reference level while at the same time contributing some balancing power. Since these two actions are somewhat contradicting (i.e., *power control* and *DC voltage control*) one action happens at the cost of steady state deviations for the other. DC voltage droop characteristic is shown in Fig. 1(c). The symbol R_{DC} refers to the *DC voltage response* and has the unit of MW/kV. The slope is often given in terms of the *DC droop constant* (ρ_{DC}), which is the ratio of change in *DC* bus voltage to the corresponding change in converter power both in per-units. It could also be defined as the change in DC voltage in per-unit that results in 100% change in converter power flow. The *DC voltage droop constant* (ρ_{DC}) and the DC voltage response (R_{DC}) are related to each other by:

$$\frac{P_{rated}}{U_{rated}\rho_{DC}} = R_{DC} \tag{1}$$

where P_{rated} and U_{rated} refer to rated power and rated DC voltage of the DC terminal, respectively. The relation between DC voltage and converter power at steady on a VSC-HVDC terminal using *DC voltage droop control* is given by:

$$U_{DC} = U_{ref} + \frac{1}{R_{DC}}\left(P_{ref} - P_{DC}\right) \tag{2}$$

It could be noted that the steady-state characteristics in constant power control mode and constant DC voltage control mode could be represented by DC voltage droop controllers with R_{DC} = 0 (i.e. ρ_{DC} = ∞), and R_{DC} = ∞ (ρ_{DC} = 0), respectively.

B. DC Voltage Steady-State including Uncertainties

The *Deterministic Power Flow* (DPF) is used to analyse and assess the planning and operating conditions of power system on a daily routine. DPF uses specific values of power generations and load demands of a selected network configuration to calculate system states and power flows [10].

The vector **P**, which refers to power flow into the DC grid via the dc terminals, is given by:

$$\mathbf{P} = K_{conv}\mathbf{U_{dc}} \otimes \left(\mathbf{Y}\mathbf{U_{dc}}\right) \tag{3}$$

where **Y** refers to the admittance matrix of the HVDC grid and the symbol ⊗ is entry-wise (point-to-point) matrix multiplication operator, also called *Hadamard product operator*. In Probabilistic Power Flow (PPF), uncertainties in the power system are modelled as random variables and the output of the power flow calculations are probabilistic distributions. The most widely used and straightforward numerical approach for the probabilistic power flow analysis is *Monte Carlo* (MC) method. This method substitutes a chosen number of values for the stochastic variables and parameters of the system model and performs a deterministic analysis for each value so that the same number of values are obtained in the results. In this paper, the selected approach is a probabilistic power flow based on MC simulation.

III. RISK-BASED STATIC SECURITY ASSESSMENT (RSSA)

Deterministic Security Assessment provides a simple rule for use in making this decision: optimize economy within hard constraints of the secure operational region. This approach achieved great success in the early power industry. The advantages are obvious, however, there are several drawback: *Not considering the likelihood of contingencies, ignoring the impact of non-restrictive incident, not giving the specific system risk indicators.* The increase number of uncertainties in modern power systems, i.e. market, stochastic generation and load, etc., imperatively requires more powerful security assessment tools. *Probabilistic reliability assessment* (PRA) is a systematic and comprehensive methodology to evaluate risks associated in power systems. *Risk* defined in IEEE Standard definitions as a measure of the probability and severity of undesired effects: "*product of probability and consequence*" [11]. *Risk theory* investigates the impact of credible contingency on system, and it uses *risk index* as a measure of the system's exposure to failure. It is also a leading indicator for security level which relates to robustness of the system to imminent disturbances. *Static security assessment* (SSA) is used to investigate if under post-disturbance steady-state conditions all components will operate within established limits. Next subsections presents the main theoretical aspects of the *risk-based static security assessment* (RSSA) used in this paper.

A. Risk Security Assessment

The basic relation for computing risk associated with an *operating condition X* at time period *t* (X_t) is given by the expected value of the *severity* (*Sev*) of the operating condition in the next time period (X_{t+1}):

$$Risk\left(Sev \mid X_t\right) = E\left(Sev\left(X_{t+1}\right) \mid X_t\right) \tag{4}$$

This expectation, applied to real power systems, is defined as the sum of the product of probability of any possible assumed credible system contingency (E_i) in the next time period and the *total risk* (or impact) associated with the specific contingency.

$$Risk\left(Sev \mid X_t\right) = \sum_{i}^{Ne} \Pr(E_i, X_{t+1} \mid X_t) \times Risk\left(Sev \mid E_i, X_{t+1}\right) \tag{5}$$

where N_e is the number of considered contingencies. In the context of a multi-infeed DC network, the DC voltage is the most important variable to ensure post-disturbance stable operation. For DC-voltage analysis, the specification of a contingency state (E_i) and the operating condition (X_t) allows the solution of the deterministic AC/DC power flow. The obtained post-disturbance steady-state conditions are included in a DC-voltage vector $\mathbf{U} = [U_1, \ldots, U_{Nb}]$, where the region of interest has N_b nodes. The total risk associated with the specific contingency is $Risk(Sev|E_i,X_{t+1})$ and it depends on the region of interest and also depends on the *violations of the security level considered*.

The *total systemic risk of DC-voltage violations* associated with the specific contingency (E_i) on the next time period is calculated according to:

$$Risk\left(Sev \mid E_i, X_{t+1}\right) = \sum_{k=1}^{N_b} Risk\left(Sev \mid E_i, U_k\right) \tag{6}$$

where $Risk(Sev|U_k)$ represents the probabilistic risk of DC-voltage violations for the *k*-th node. It is the expectation of the *component risk* over the uncertain DC voltages on *k*-th node.

$$Risk\left(Sev \mid U_k \mid E_i,\right) = \int \Pr\left(U_k\right) \times Sev\left(U_k\right) dU_k \tag{7}$$

$\Pr(U_k)$ is the probability of violations of the security level considered at the *k*-th node DC-voltage (U_k). This is obtained of the probabilistic power flow used to obtain the post-disturbance steady-state conditions considering the stochastic model of the considered input uncertainties (e.g. variability on wind speed, etc.). $Sev(U_k)$ is the *component severity* of the *k*-th node. Acceptability criteria of a DC-voltage level (**U**) must be defined, some criteria used to judge acceptability of system performance might be subjective. A *severity* function is assigned to the impact of the DC-voltage, *Sev*(**U**).

B. Total Systemic Risk Index (TSRI)

The *total systemic risk* related to *violations of the security level considered at DC-voltage* is calculated according to:

$$Risk\left(Sev \mid X_t\right) = \sum_{i}^{Ne} \Pr(E_i, X_{t+1} \mid X_t) \left(\sum_{k}^{Nb} Risk\left(Sev \mid E_i, U_k\right) \right) \tag{8}$$

where *TSRI* = $Risk(Sev|X_t)$. This is probabilistic security indicator that allows forecasting DC-voltage performance across all the DC network over time. The idea of this index is to provide the risk of system constraint violations, over or under DC-voltages, given a specified operating state.

C. Individual Risk Index (IRI)

The risk of violations of the security level considered at DC-voltage in a particular or individual component is named in this paper as *Individual Risk Index* (*IRI*). For instance the risk of DC-voltage violations, over or under DC-voltage, of the *k*-th node considering the a contingency state, E_i, is $IRI(U_k,E_i) = IRI_{Uk,i} = Risk(Sev|E_i,U_k)$, as show on (7).

The $IRI_{Uk,i}$ is calculated as a *severity function* that quantifies the consequence of the *i*-th contingency on DC-voltage and *k*-th node, which is weighted by the probability of the violation of the acceptability criteria.

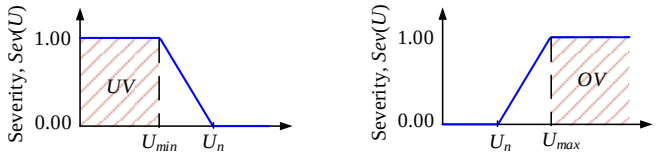
Severity provides a quantitative evaluation of what would happen to the power system in the specified condition in terms of impact, severity, consequence, or cost. Two extreme situations are especially risky in the context of a multi-infeed DC network: *under voltages* (*UV*) and *over voltages* (*OV*).

The severity function for under voltage is defined specific to each node, i.e. *k*-th node $Sev(U_k^{UV})$. The voltage magnitude of each node (U_k) determines the low-voltage severity of that bus following the function shown of Fig. 2(a) where U_{min} defines the minimum acceptable voltage and below that value the severity of under voltage is maximum (1.00). $Sev(U_k^{OV})$ represents over voltage severity function of the *k*-th node as represented on Fig. 2(b).

IV. Risk Inference System

A. Inference System

Security may be defined as the probability of the system's operating point remaining in a viable state space, given the probabilities of changes in the system (uncertainties defined by stochastic model of its randomness). The security assessments define if the system is in the normal state, determine whether the system is secure or considering uncertainties (i.e. contingencies). During system operation, the online determination of the security level is fundamental in order to take appropriate countermeasures, with the goal of bringing the system, if necessary, to a more secure operation condition. Security analysis and control have been implemented through a number of software packages in modern energy control centres [12].



(a) Under voltage Severity Function (b) Overvoltage Severity function

Figure 2. Typical severity applied in DC-voltage.

Increased uncertainties make more and more attractive the use of PRA, which has already been used by many utilities since 2001 and sufficient data is now available for the power industry to move toward wide-spread implementation of the methodology [13]. However, the most important drawbacks are the lack of "easy to use" and "comprehensive" PRA tools for systems operations and the speed of computation that make online PRA. This paper develops a novel online RSSA methodology. The *risk-based DC-voltage security assessment* (RB-VS) is used to quantify the risk associated with forecasted operational scenarios by considering the probability and severity of DC-voltage excursions, overload on cables and converter stations.

B. Fuzzy Risk Inference System (FRIS)

Future DC-ISO requires a power risk-based security assessment in order to get quantification of a security level associated with an existing or forecasted operating condition take decisions and that is where *fuzzy risk inference system* (*FRIS*) come in. The *FRIS* uses system that uses fuzzy set theory to map inputs to outputs dealing with reasoning that is approximate rather than fixed and exact.

The proposed *FRIS* produces a single final risk index combining the *fuzzy logic assessment* with the *risk security assessment*. A cascading *two-stage fuzzy inference system* (*2-stage FIS*) is used in order to obtain a composed risk index per contingency, named *contingency risk index CRI*. It defines system risk considering all violations (voltages and overload) of the security caused by the *i*-th contingency state in the system. The use of *FRIS* allows normalize risk indexes and combine them into a single one.

The procedure presented on Section V is used to calculate individual risk index (*IRI*) for the *i*-th contingency state for the following violations of the security: (i) under voltage $IRI(\mathbf{U}^{UV})$, overvoltage $IRI(\mathbf{U}^{OV})$, (ii) overload on cables $IRI(\mathbf{P}_{cable})$, and (iii) *overload on converter* $IRI(\mathbf{P}_{conv})$.

A severity function is defined for each violation of the security as shown on Fig. 3.

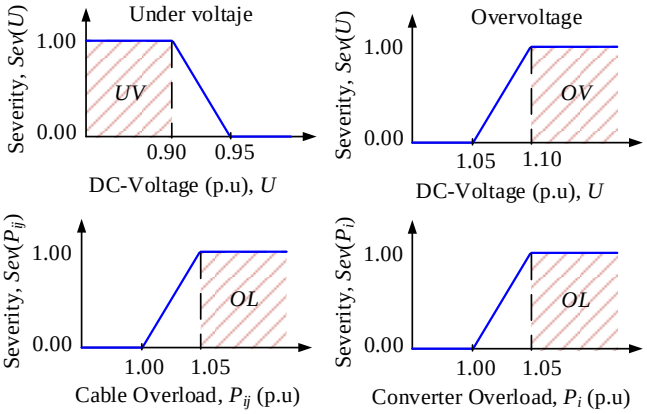


Figure 3. Severity functions of the four violations of the security considered.

U is the vector of DC voltages and superscript are used to indicates security violations considered by the *IRI*, under voltage (*UV*) and overvoltage (*OV*). Cable and converter overloads are included in $\mathbf{P}_{cable}$ and $\mathbf{P}_{conv}$ respectively. For instance, overvoltage voltage vector $\mathbf{U}^{OV}$ = [0 1 0 0 1], in used to represent overvoltage violations on node 2 and 5 of a 5 nodes DC-network.

Any security violation (voltage or overload) in only one element represents a risky situation, for this reason the most unfavourable *IRI* of the four considered security violation is used as input to the *FRIS*.

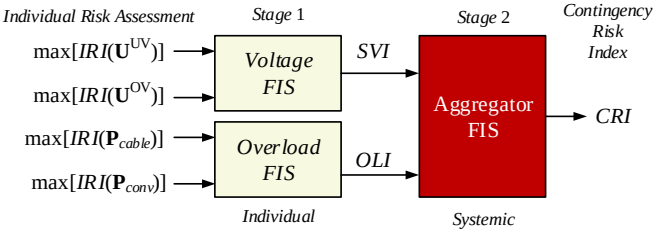


Figure 4. Proposed cascading two-stage FIS or *Fuzzy Risk Inference System* (FRIS).

The *Stage 1* of the *FRIS* includes two *FIS*: (i) *Voltage FIS* and (ii) *Overload FIS*. The consequence of the contingency state on the system voltage is represented through the *system voltage index* (*SVI*) and the consequence on the system overload through the *system overload index* (*OL*). Those indexes reflect risk related to the security limits violations in terms of the whole system. The outputs of all the *Stage 1 FIS* are subsequently compounded using *Stage 2 FIS*, which aggregates the effect of the voltage and overloads violations creating the *contingency risk index* (*CRI*). The *CRI* provides a unique risk index per contingency, $CRI \in [0,1]$, which can be used to rank contingencies per severity of the security violation and then decisions maybe taken. The *CRI* represents

the effect of violation of security level of the *i*-th contingency status. Now, the *total system risk index* (TSRI) of the risk of the whole power systems to all contingency statuses is calculated considering a convenient weigh of each risk with the probability of the contingency occurring. In this paper, of probability of any possible assumed credible system contingency (E_i) is assumed to be *Poisson distributed*:

$$Pr(E_i, X_{t+1} \mid X_t) = \left(1 - e^{-\lambda_t}\right) \cdot \exp\left(-\sum_{j \neq i} \lambda_t\right) \qquad (9)$$

where λ_t is the occurrence rate of contingency *t* per unit time. In this paper, converter and cable failure rates per year used are taken from [6].

Finally, the *Total Systemic Risk Index (TSRI)* consider the effect of all the contingencies in one single index as defined on (5):

$$TSRI = Risk\left(Sev \mid X_t\right) = \sum_{i}^{Ne} \Pr(E_i, X_{t+1} \mid X_t) \times CRI\left(E_i\right) \qquad (10)$$

FRIS is used to quantify, *SRI*, the total system risk associated with forecasted operational scenarios by considering the probability and severity for violations of the security related to: excursions on DC-voltage (under and over voltages), overload on cables and converter stations.

C. Fuzzy

The universe of discourse of the inputs and the output for the three FIS (*Voltage FIS*, *Overload FIS* and *Aggregator FIS*) has been partitioned into three linguistic values: *low*, *medium* and *high*, variables equally distributed along the interval [0, 1] and modelled in triangular fuzzy sets. Fig 5 shows the term set and membership functions for the inputs and the output (μ) of the as *FIS*.

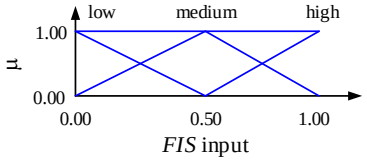


Figure 5. Term and membership function for inputs and output of *Voltage FIS*.

Table I shows the rule base of the specific *Voltage FIS* and Fig. 6 shows the two-dimensional curve that represents the mapping between input and output. Membership function, the rule base and the 2-D curve of *Overload FIS* and *Aggregator FIS* are not shown here for space limitation, however, follow similar to Voltage FIS.

TABLE I. RULE BASE OF VOLTAGE FIS

Rule	*Antecedents*		*Consequent*
No.	max[*IRI*($\mathbf{U}^{UV}$)]	max[*IRI*($\mathbf{U}^{OV}$)]	*SVI*
1	*low*	*low*	*low*
2	*low*	*medium*	*medium*
3	*low*	*high*	*high*
4	*medium*	*low*	*medium*
5	*medium*	*medium*	*medium*
6	*medium*	*high*	*high*
7	*high*	*low*	*high*
8	*high*	*medium*	*high*
9	*high*	*high*	*high*

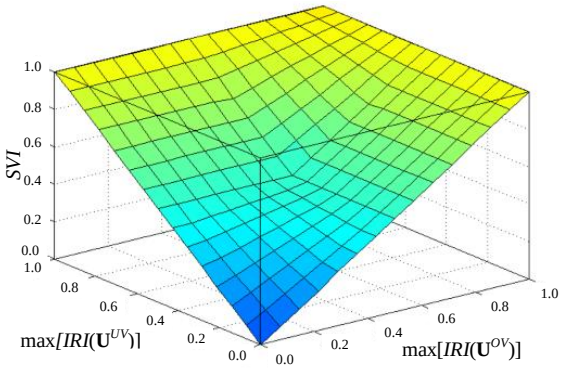


Figure 6. Two-dimensional curve that represents the mapping between input and output view of Voltage FIS.

V. METHODOLOGY OF RB-DCSA

The two previous Sections present a compressive explanation of individual aspects of the proposed risk-based security assessment of DC systems. This section summarizes the proposed methodology:

Step 1: Establish the stochastic description of the system's uncertainties using historical data or forecasted data where is available.

Step 2: Scenarios are generated to represent forecasted states of the power system. Pseudo-random numbers and the stochastic models of uncertainties are used to create the scenarios. Correlations between uncertainties can be considered and included during this process.

Step 3: Deterministic System Model Solution is used to calculate the steady-state conditions associated to each of the scenarios obtained previously. A sequential AC/DC power flow is used in this paper; it includes the main features of operation and control associated to converter stations [14].

Step 4: Post Simulation process includes the calculation of *probabilistic distribution function* (PDF) of the main variables of interest.

Step 5: Severity functions are assigned to measure the impact on the DC-voltage (under-voltage and overvoltage), cable's overload and converter's overload.

Step 6: The component risk and system risk are calculated. Equations (7) is used together with the severity function to calculate those risks (e.g. risk of DC overvoltage) (details in Section IV).

Step 7: A two-step fuzzy process is used to produce the risk associated with a forecasted operating condition. A two-stage fuzzy inference system is used to composes a fuzzy index making use of system risk at forecasted operating scenario and then a second fuzzy inference is used to impact of a specified contingency states (details Section V).

VI. SIMULATION AND RESULTS

In this Section, a multi-terminal VSC-HVDC text network is used to illustrate the methodology of risk-based security assessment. A MATLAB® R2014a [15] (version 8.3.0.532 64-

bit) program (m-file) has been developed for this specific propose. All simulations are performed using a PC based on Intel®, Core™ i7 CPU 2.5GHz, 16 GB RAM with Windows 8.1 64-bit operating system.

A. Test System

A 5-terminal, 345kV, VSC-HVDC network representative of the integration of offshore wind power coming from the North Sea is used for illustrative purposes [16] (see Fig. 7). All converter stations use symmetrical monopole topology using two different DC voltage control modes on the VSC-HVDC terminals: constant power control modes on the wind farm converter stations (WFC_i, i = 1, 2) and voltage droop control on the grid side converter stations (GSC_i, i = 1,… ,3), thus enabling *N*-1 security.

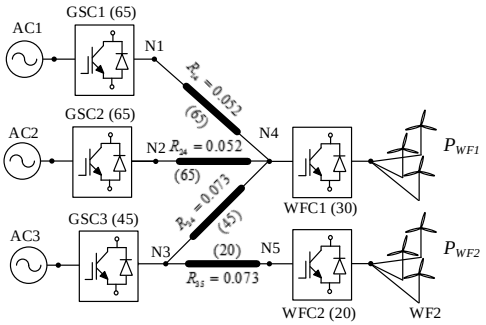


Figure 7. Five-terminal test network for power flow studies. R_{ij} defines the resistance between node *i* and *j* in Ohms. Values in parenthesis represent rated power in MW [16].

B. Uncertainties Modeling and Scenarios

The unique source of uncertainties in this paper is related to randomness of wind speed at the wind farm location. Fig. 8 shows the stochastic model used for the uncertainties, wind speed is modelled using a typical 2-parameter Weibull distribution and equivalent wind farm power production is calculated using sum of individual wind turbine power production. The power curve of *Senvion 6.2M* [17], 6,150 kW wind turbines are used in this paper.

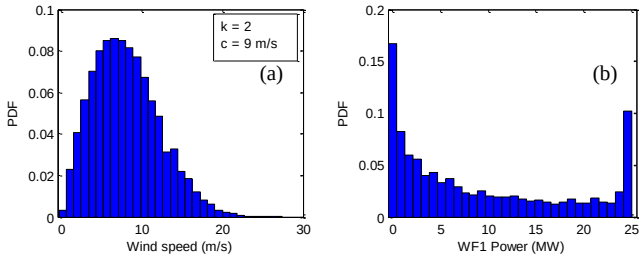


Figure 8. Probabilistic density function of (a) wind speed and (b) output power at WF1.

DC-ISO is expected to deal with contingencies in the DC side of the MTDC caused by: converter outage and cable outage. Table II summarize the simulation scenarios considered in this paper, starting from a pre-contingency state, and including an alphanumeric coding used for analyses interpretation. It must be noticed cable between N3 and N5, named Cable 3-5 is not include into simulation scenarios. This is because contingency on Cable 3-5 is equivalent to lose the WFC2 from the system point of view.

TABLE II. SUMMARY OF SIMULATION SCENARIOS INCLUDING CODING AND DETAILS

Scenario Code	*Equipment Outage*	*Details*
I	None	Base Case
IIA1	Converter	GSC1
IIA2		GSC2
IIA3		GSC3
IIB1		WFC1
IIB2		WFC2
III14	Cable	Cable 1-4
III24		Cable 2-4
III34		Cable 3-4

C. Post-Contingency Steady-state

Probabilistic power flow is used to calculate the probabilistic distribution function of **U**, $\mathbf{P}_{cable}$ $\mathbf{P}conv$. It is based on 10,000 Monte-Carlo simulations of the scenarios shown on Table II. Full results are not presented here for space limitation, but few results of *Scenario* I.A3, GSC3 outage, are presented for illustrative purposes. Fig. 8 shows the probability of overload Cable 4-2 (P_{45} > 65 MW) and over voltages (U_3 > 1.10 p.u) at N3.

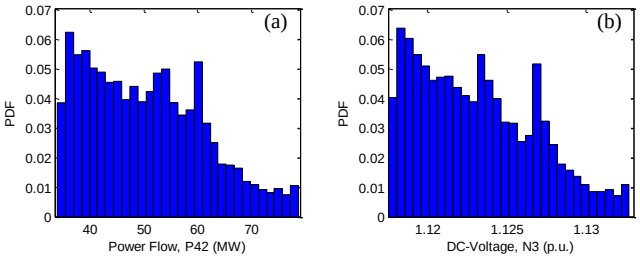


Fig. 1. Results of Scenario II.A3. Probabilistic density function: (a) power flow and (a) DC-voltage.

A. Individual Risk Index (IRI)

Severity functions as shown on Fig. 3 has been used to estimate the impact on the DC-voltage (under-voltage and overvoltage), cable's overload and converter's overload. Fig. 10 shows how the $IRI(\mathbf{U}^{OV})$ change depending on the contingency status, it can be noticed *Scenarios* II.A1, II.B1 and II.B2 exhibit not risk of overvoltage and II.A.3 is mots risky condition where all nodes exhibit the highest *IRI* of over voltages. All violations of the security has been calculated ($IRI(\mathbf{U}^{UV})$, $IRI(\mathbf{U}^{OV})$, $IRI(\mathbf{P}_{cable})$, $IRI(\mathbf{P}_{conv})$).

B. Risk-based Security Assessment

The two-step fuzzy process is used to produce the risk associated with the operating conditions. Inputs of the *Voltage FIS* and *Overload FIS* are depicted in Fig. 11. *IRI*s indicate under voltages are the most important concern on contingencies status related to cable outages (III14, III24, III34). Scenario IIA2 is the worst situation in terms of converter overloads and III24 is a risky situation for cable overloads. Now, the consequence of the set of contingency status, *Scenarios*, are evaluated from the systemic point of view, system voltage index (*SVI*) and system overload index

(*OLI*), a summary of those results are shown in Fig. 12.

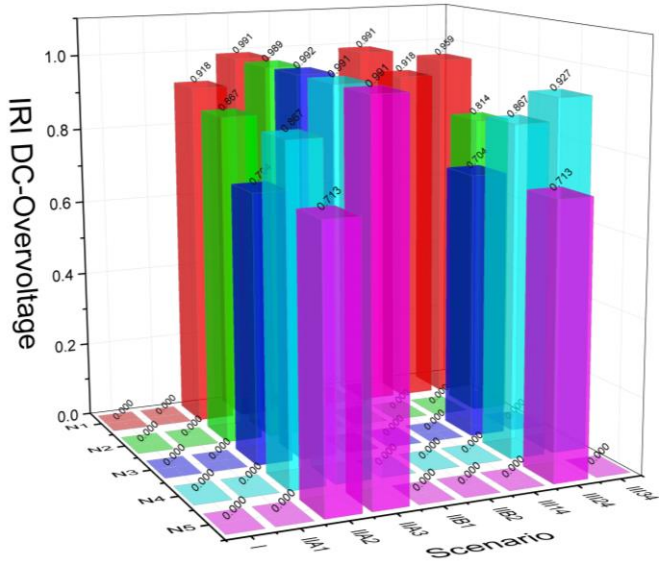


Fig. 2. Individual Risk Index of Overvoltage *IRI*($\mathbf{U}^{OV}$).

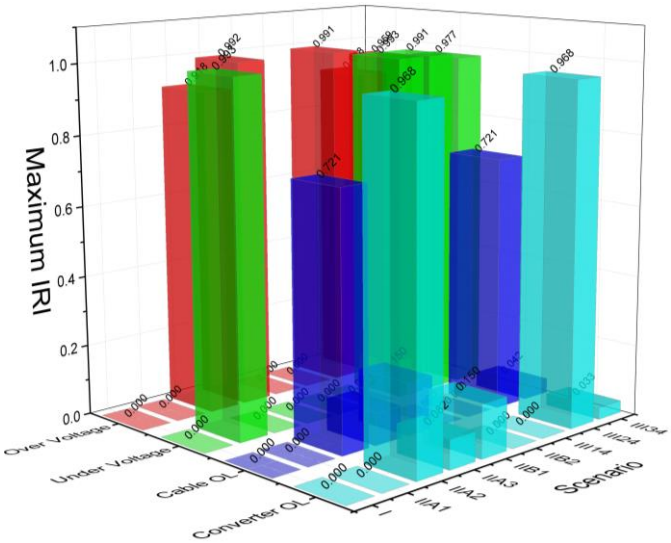


Fig. 3. Maximum Individual Risk Index per Scenario.

SVI is a lumped index and allows to indicate there is system voltage violation but it is not indicates if the violation is caused by a low or high voltage. Similar situation happens with *OLI*, where the violation cannot be identify by type of equipment: cable or converter. As expected, Scenario I, normal operation is a secure operation (*CRI* = 0), but surprisingly, Scenario IIB2 (WF2 outage) allows a safe operation. It is followed by Scenario IIB1 (WF1 outage) with *low risk systemic* (*CRI* < 0.33) caused by equipment overloads. The remaining Scenarios are considered to be condition of *high risk* (*CRI* > 0.66), mainly caused by violation of voltage security levels.

Finally, the *Total Systemic Risk Index* (TSRI) is calculated considering effect of all the contingencies considering the occurrence rate of contingency per year shown on Table III and IV. TSRI of 0.3313 is obtained and it is classified as *medium risk* (0.33 < *risk index* <0.66) condition based on the considered uncertainties. TSRI is an index looking after whole system considering the uncertainty coming from the randomness variability provided by the wind speed.

This is just an illustrative example and it is intended to show the use of the proposed methodology and shows the potential of those indexes as detect violation of system security.

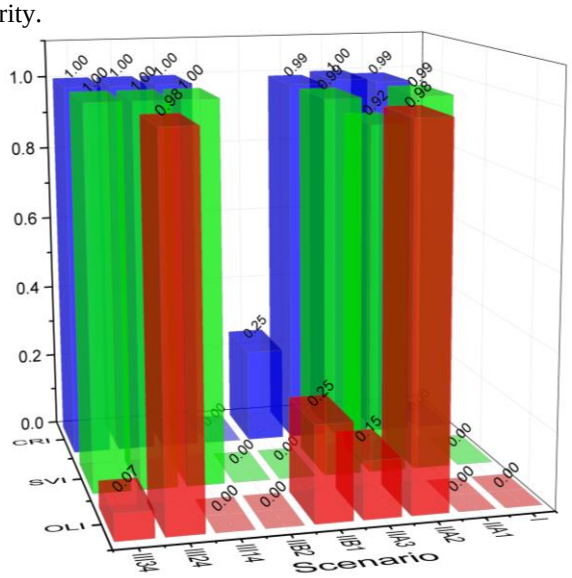


Fig. 4. Individual Risk Index of Overvoltage *IRI*($\mathbf{U}^{OV}$).

TABLE IIII. OCCURRENCE RATE OF CONTINGENCY

Equipment	*Failure rate (1/year)*
Converters	*0.12*
Cables (100 km)	*0.08*

TABLE IV. OCCURRENCE RATE OF CABLE CONTINGENCIES

Equipment	*Distance (100km)*	*Failure rate (1/year)*
Cable 1-4	*4.78*	*0.38*
Cable 2-4	*2.04*	*0.16*
Cable 3-4	*3.50*	*0.28*
Cable 3-5	*1.66*	*0.05*

II. CONCLUSIONS

This paper develops a novel risk-based static security assessment methodology named *risk-based security assessment* (RB-DCSA). This methodology is used to quantify the systemic and individual component risk associated with operational scenarios considering uncertainties. Proposed risk assessment considers the probability and severity of DC-voltage excursions, overload on cables and converter stations. Monte-Carlo simulations of AC/DC steady-state are used to define operational states considering the uncertainty and a two-step fuzzy process is used to produce the risk associated with the operating conditions. One advantage of the proposed FIS is to allow combine different types security conditions, and indexes inside the FIS allows identify, variables, equipment and locations of the security violations. The proposed methodology has been illustrated using a multi-terminal HVDC where uncertainties coming from the variability of the wind speed in two wind farms is included. Results shows the suitability of the proposed methodology to

identify total system risk, variables causing risky states (overload and voltage violations), type of security violation (over voltage, under voltage, overload), equipment or node where violation is found (node, converter cable) and also, the RB-DCSA allows contingency ranking. More evaluations must be performed to the methodology performance in order to extend it into on-line security assessment.

III. References

[1] F. Gonzalez-Longatt, "Frequency Control and Inertial Response Schemes for the Future Power Networks," in *Large Scale Renewable Power Generation*, J. Hossain and A. Mahmud, Eds., ed: Springer Singapore, 2014, pp. 193-231.

[2] J. D. McCalley, V. Vittal, and N. Abi-Samra, "An overview of risk based security assessment," in *Power Engineering Society Summer Meeting, 1999. IEEE*, 1999, pp. 173-178 vol.1.

[3] J. McCalley, S. Asgarpoor, L. Bertling, R. Billinion, H. Chao, J. Chen, *et al.*, "Probabilistic security assessment for power system operations," in *Power Engineering Society General Meeting, 2004. IEEE*, 2004, pp. 212-220 Vol.1.

[4] D. D. Le, A. Berizzi, C. Bovo, E. Ciapessoni, D. Cirio, A. Pitto, *et al.*, "A probabilistic approach to power system security assessment under uncertainty," in *Bulk Power System Dynamics and Control - IX Optimization, Security and Control of the Emerging Power Grid (IREP), 2013 IREP Symposium*, 2013, pp. 1-7.

[5] N. Ming, J. D. McCalley, V. Vittal, and T. Tayyib, "Online risk-based security assessment," *Power Systems, IEEE Transactions on*, vol. 18, pp. 258-265, 2003.

[6] S. Kai, S. Likhate, V. Vittal, V. S. Kolluri, and S. Mandal, "An Online Dynamic Security Assessment Scheme Using Phasor Measurements and Decision Trees," *Power Systems, IEEE Transactions on*, vol. 22, pp. 1935-1943, 2007.

[7] W. Chen, Q. Jiang, and Y. Cao, "Risk based vulnerability assessment for HVDC transmission system," in *Power Engineering Conference, 2005. IPEC 2005. The 7th International*, 2005, pp. 734-739 Vol. 2.

[8] ENTSO-E. (2014). *Continental Europe Operation Handbook*. Available: https://www.entsoe.eu/publications/system-operations-reports/operation-handbook/Pages/default.aspx

[9] T. M. Haileselassie and K. Uhlen, "Impact of DC Line Voltage Drops on Power Flow of MTDC Using Droop Control," *Power Systems, IEEE Transactions on*, vol. 27, pp. 1441-1449, 2012.

[10] P. Chen, Z. Chen, and B. Bak-Jensen, "Probabilistic load flow: A review," in *Electric Utility Deregulation and Restructuring and Power Technologies, 2008. DRPT 2008. Third International Conference on*, 2008, pp. 1586-1591.

[11] "IEEE 100 The Authoritative Dictionary of IEEE Standards Terms Seventh Edition," *IEEE Std 100-2000*, 2000.

[12] J. M. G. Alvarez and P. E. Mercado, "Online Inference of the Dynamic Security Level of Power Systems Using Fuzzy Techniques," *Power Systems, IEEE Transactions on*, vol. 22, pp. 717-726, 2007.

[13] Z. Pei, M. Liang, L. Hopkins, B. Fardanesh, P. C. Patro, J. Useldinger, *et al.*, "Utility application experience of Probabilistic Risk Assessment method," in *Power Systems Conference and Exposition, 2009. PSCE '09. IEEE/PES*, 2009, pp. 1-7.

[14] F. Gonzalez-Longatt, J. M. Roldan, and C. A. Charalambous, "Solution of ac/dc power flow on a multiterminal HVDC system: Illustrative case supergrid phase I," in *47th International Universities Power Engineering Conference (UPEC 2012)*, 2012, pp. 1-7.

[15] MATLAB, *version 8.3.0.532 (R2014a 64-bit)* Natick, Massachusetts: The MathWorks Inc., 2014.

[16] F. Gonzalez-Longatt. (2015). *Multi-Terminal HVDC Test Cases : 5-Node+2WF+3AC*. Available: http://www.fglongatt.org/Test_Systems/5-Node+2WF+3AC.html

[17] Servion. (2014). *The Senvion 6.XM Series*. Available: http://www.senvion.com/wind-energy-solutions/wind-turbines/6xm/