

Article

Investigating Various Severity Factor Behaviors for Operational Risk Assessment

Zunaira Nazir * and Math H. J. Bollen 

Department of Engineering Sciences and Mathematics, Luleå University of Technology, 93187 Skellefteå, Sweden
* Correspondence: zunaira.nazir@ltu.se

Abstract: Operational risk assessment is a stochastic approach to quantify the operational security of power systems. In this study, the interrelation between severity factor and operational risk, two important parameters in operational risk assessment, is analyzed. Four different definitions of severity factor, based on the results from network studies, are proposed and applied, resulting in different values for the operational risk indices. The behavior of these indices is analyzed under varying operating conditions and compared with the behavior of the severity factor for individual contingencies. This study confirms the importance of the severity factor definition and shows that multiple operational risk indices are required to obtain a clear picture of the operational security of a transmission system. One risk index may increase while another decreases.

Keywords: power system security; power risk analysis; operational risk assessment; contingency; severity factor; voltage collapse



Citation: Nazir, Z.; Bollen, M.H.J. Investigating Various Severity Factor Behaviors for Operational Risk Assessment. *Electricity* **2022**, *3*, 325–345. <https://doi.org/10.3390/electricity3030018>

Academic Editor: Angel Arcos-Vargas

Received: 27 June 2022

Accepted: 3 August 2022

Published: 5 August 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Ensuring transmission grid operational security and providing reliable power to distribution networks and large consumers is a fundamental task of the transmission system operator (TSO). In the past, stochastic approaches have been used for the reliability of the transmission system [1,2], mainly during long-term system planning. This subject is well covered in the scientific literature, including in a number of textbooks [3–5] and in a large number of papers, with [6–9] being some of the earlier most-cited ones and [10–13] some of the more recent papers. In [14], a stochastic programming approach is used to quantify the optimal level of reliability of a power system. In [15], a probabilistic time-dependent approach is used to quantify the reliability of a power system. In [16], the reliability of a power system is quantified through different performance indices; it is deduced that by moving from deterministic (N-1) to stochastic reliability criteria, the expected total cost will be reduced.

Such a stochastic approach is not deployed for operational security or for other short-term planning. Deterministic methods for operational security assessment consider all contingency events as equal, irrespective of their probability and their impact. Both different probabilities and different impacts can be included in the operational security assessment through the use of a stochastic method.

An operational risk technique was deployed by PJM in the early 1960s, using a unit commitment approach to assess the amount of spinning reserve at the generation side needed to cope with the loss of production units [17]. Over the years, there has been some further development of the methods, for several types of primary and secondary production reserves, including uncertainty in consumption and uncertainty in production from wind power [18–22] and market models [23,24]. Production reserves in the form of battery storage are included in [18].

The original method was extended to include the bulk transmission system in the 1970s [25–28]. One of the first realistic applications of the method was presented by Singh in 1988 [29]. Cascading failures are included in [30]. Reference [31] includes the risk of

instability due to single- and double-component failures. More detailed models, improved calculation methods, and applications are found in [32–34].

Stochastic-based operational risk assessment techniques can complement the various deterministic (N-1) methods [35,36] and will allow the TSO to include uncertainties in operational planning [37–39], whereas the (N-1) criterion only indicates whether the system is secure or not. Currently, TSOs deploy classical (N-1) deterministic criteria, which are occasionally insufficient, and which can create unnecessary barriers against new production and consumption. During periods with high and low component failure rates, this (N-1) criterion could lead to underestimation and overestimation, respectively. This (N-1) deterministic method does not allow any trade-off between operational risk and other risks.

The concept of operational risk assessment has been around for several decades; however, the practical implementation of it has not yet been achieved. Potential reasons behind this are that the (N-1) criterion works well and that there is a lack of experience of operational risk methods applied to realistic networks. Due to the integration of renewable energy resources into the grid, e.g., wind and solar, and to incorporate new types of uncertainties, the need for a stochastic method has increased. More advanced methods of operational risk assessment are required. There is a need to design a standardized set of severity factors so that the TSO can exchange information and results for different areas of the transmission system. This quantification can be used to manage the transmission system operation in a more effective way.

For instance, in [40], a stochastic approach is deployed to manage optimal power flow, which is further used to control the economic risk associated with system operation.

Within the operational risk assessment of transmission systems, most research is directed towards contingency ranking [41–43] and contingency filtration [44]. For instance, in [45], by deploying a “convolutional neural network”, contingency screening is done under the integration of renewable energy resources for high-probability contingency events. In [46], a fast-screening approach was used to extract the most influential contingencies.

Only a limited amount of research exists concerning the severity factor (SF) that quantifies the impact of an individual contingency and on the role of different SF definitions on the operational risk.

For instance, in [47], a severity evaluation is conducted in terms of thermal load, voltage instability, and loss of load, to reflect the impact of contingencies with the help of steady-state analysis. However, [47] does not highlight the importance of the severity factor in the transmission system security analysis. In [48], a distinction is made between online and offline security assessments and various alternatives of severity assessment are presented, including economic and control aspects. In [49], a severity factor definition is proposed to quantify the impact of a contingency in terms of voltage collapse. The method is used to estimate the expected future cost due to voltage instability. Overloading of transmission system components is another potential impact of a contingency. In [50], a severity factor is quantified in terms of the overloading risk of transmission lines. However, the risk is quantified on an annual basis. In [51], credibility theory is used for operational risk assessment under dual uncertainty; several risk indices are defined to quantify different impacts of contingencies: overload, overvoltage, and undervoltage. References [52,53] investigate online risk-based security assessment methods to make an online decision; various continuous and discrete severity factors are defined to quantify the impact of contingencies on voltage instability and overload. In [54], severity functions are proposed for overvoltage and undervoltage during a contingency. Despite the different definitions of severity factor in the literature, none of them explicitly mentions the significance of the severity factor in quantifying operational security, and limited work is directed towards the proposal of standardized severity factors.

This study investigates four different definitions of severity factor and how these definitions result in different operational risk behavior as a function of system loading. The main contributions of this paper are as follows:

- Four different severity factor definitions are proposed, quantifying four different impacts of a contingency on the transmission system: extreme loading; overvoltage; undervoltage; and voltage instability. A general formulation is given, and for three of the four definitions, a numerical threshold is proposed.
- The operational risk is calculated and analyzed for these four definitions, using a commonly used test system, the IEEE 39-Bus New England system, under varying operating conditions.
- The behavior of the severity factor for individual contingencies is compared with the behavior of the operational risk index for the system as a whole, for increasing system loading. It is shown that multiple definitions of severity factor, and thus of operational risk indices, are needed to obtain a complete picture of the operational security of a transmission system.

The rest of the paper is organized as follows: Section 2 discusses the approach used to quantify operational risk. The schematic procedural flow is debated in which the probability of contingency calculation through the component unavailability is mentioned. Section 2 also introduces the different severity factor definitions. Section 3 discusses the specific attributes and different alternatives to the severity factor and provides different mathematical definitions of severity factor. Section 4 discusses the system level operational risk behavior, for different technical severity factor definitions, under varying operating condition. Section 5 analyses the severity factor behavior of individual contingencies under varying operating conditions. Section 6 includes the discussion and recommendations resulting from this work.

2. Operational Risk Calculation

The operational risk assessment tool deployed in this study is a combination of contingency generation and the quantification of the impact for each contingency [55].

2.1. Operational Risk Procedural Flow

From the general definition (1) of operational risk, it follows that operational risk assessment consists of two steps:

1. The computation of probability of contingency, P_c .
2. The quantification of severity factor, $F_s(c)$.

$$R_{op} = \sum_{c=1}^{N_c} P_c \times F_s(c) \quad (1)$$

where R_{op} is the operational risk, P_c is the probability of contingency, $F_s(c)$ is the severity factor for that contingency, and N_c is the total number of contingencies. Figure 1 depicts the schematic procedural flow of operational risk assessment.

To calculate the severity factor, $F_s(c)$, network studies are required. For each contingency, several severity factors are calculated as discussed detailed in Section 3.

The component unavailability $Q(t)$ is computed from the failure rate and repair rate for the given lead time. After the computation of component unavailability, a contingency list is created and for each contingency on that list, the probability that the contingency could occur within the lead time is calculated. The computation of this probability is discussed in detail in Section 2.2.

After the calculation of probability of contingency P_c and the severity factor $F_s(c)$, for each contingency in the contingency list, the operational risk is computed and different operational risk indices are obtained, based on different definitions of the severity factor.

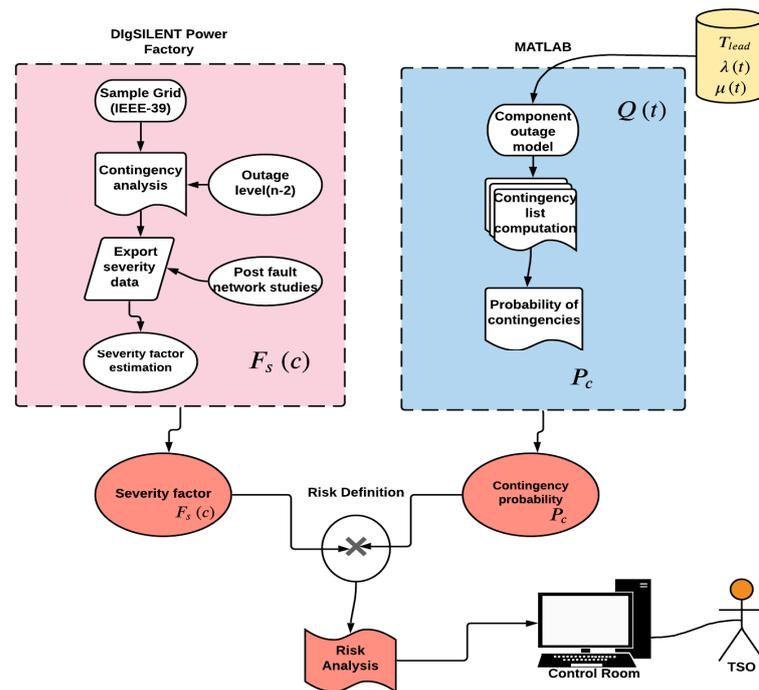


Figure 1. Schematic algorithm flow of operational risk assessment.

2.2. Probability of Contingency P_c

During operational risk assessment for contingency analysis, three main factors need to be considered. The first is the contingency definition in which the TSO will consider which component unavailability will be considered in the risk assessment. The second is the list of contingencies to be included in the calculation. This could be all contingencies up to a certain order, but it could also be based on other criteria. The third factor is the probability of the contingency cases in the list of contingencies. The right block in Figure 1 shows that the calculation of P_c consists of three steps, corresponding to these three things. After this, the probability of contingency is calculated.

1. Component Unavailability Model $Q(t)$

During the lead time, the component is either in operational or in non-operational mode as depicted in Figure 2. Two constant transition rates are assumed: μ and λ quantify repair and failure.

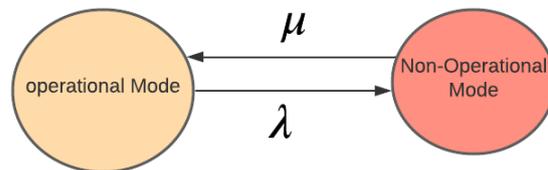


Figure 2. State space model of a repairable component.

At time $t = 0$, the component is in operational mode. That is the fundamental assumption made for operational risk assessment. When repair is possible during the lead time, the component unavailability model would be (2):

$$Q(t) = \frac{\lambda}{\lambda + \mu} \left(1 - e^{-(\lambda + \mu)t}\right) \tag{2}$$

Under a small lead-time assumption, $(\lambda + \mu)t \ll 1$, the exponential term would be approximated as in (3):

$$e^{-(\lambda + \mu)t} \approx 1 - (\lambda + \mu)t \tag{3}$$

which simplifies the component unavailability model in (4):

$$Q(t) = \frac{\lambda}{\lambda + \mu} [(\lambda + \mu)t] = \lambda t \quad (4)$$

2. Contingency Definition

After quantifying the component unavailability model for different components, for instance for component 1 and 2 in the network, the component unavailability model $Q_1(t)$ and $Q_2(t)$ is computed from (5) and (6), using (4) with $t = t_{lead}$:

$$Q_1(t) = \lambda_1 t_{lead} \quad (5)$$

$$Q_2(t) = \lambda_2 t_{lead} \quad (6)$$

After the computation of individual component unavailability, the probability of a contingency P_c is computed:

$$P_c = Q_1(t) \cdot Q_2(t) \quad (7)$$

To visualize the role of the severity factor in operational risk assessment, all (N-2) contingencies are considered in this study. For higher order contingencies, the probability computation Equation (7) would be different.

Equation (7) could be further simplified as Equation (8), which would also be different for higher order contingencies:

$$P_c = \lambda_1 \lambda_2 t_{lead}^2 \quad (8)$$

For the probability quantification of individual contingency cases simultaneously, only two component's unavailability is considered Equation (8), at the end of the lead time. The probability of contingency is calculated using a memoryless model.

2.3. Severity Factors $F_s(c)$

Different researchers quantify severity in different ways [56,57]. There is no standardized or commonly agreed way to define the severity factors. In this study, four different technical system-level severity factors are considered.

1. Severity factor for overvoltage.
2. Severity factor for undervoltage.
3. Severity factor for extreme loading.
4. Severity factor for system collapse.

2.4. Reliability and Operational Risk Indices

Quantifying the performance of the power system is not limited to operational risk assessment, where the severity factor and operational risk are used to quantify the (short-term operational) risk. Two types of indices are used to quantify the long-term reliability of the power system: those based on measurement, and those based on the prediction of the performance.

Some of the early work on indices based on the measurement of the performance of a transmission system was carried out by a CIGRE working group [58,59], continued by an IEEE working group [60], and resulting, among others, in IEEE Std. 1366 [61] and the recommendations by the Council of European Energy Regulators [61]. The indices originally used, based on measurements, have also found broad application as indices for the prediction of performance. In reliability assessments, the aim is to obtain predictive indices [62], where often the same notations (e.g., SAIFI and CAIDI) are used despite the different underlying definitions.

There are similarities and differences between reliability indices and operational risk indices. Consider, for example, the definition of "severity" for the interruption of a bulk-supply point, expressed as MW-minutes [58], later extended to "delivery point interruption severity" and "system interruption severity" [60]. For the latter two indices, the severity is

first added for all interruptions during one year and next averaged over all bulk supply points. For operational risk assessment, it is possible to use “severity” as a severity factor definition. However, it would not be the severity of an actual interruption, but the severity of a (possible) contingency. The operational risk is then obtained by adding over all contingencies, weighted by the probability of those contingencies occurring within a certain lead time.

2.5. Case Study

To perform second-order contingency analysis and conduct “post-fault network studies” to quantify the severity factor, “Power Factory” is used. In this study, to demonstrate the proposed idea, the “IEEE 39-Bus New England system” is used. It is also assumed that the failure rate for all of the components is in the range of 0.01 to 0.1 (failure per hour). The considered lead time is 10 h, which means that operational risk is quantified for the upcoming 10 h. For the contingency definition, all 34 transmission lines T_{T-L} , 12 transformers T_{Trf} , and 10 generators T_G are selected from the IEEE 39-Bus New England system. The total number of components T_C with a non-zero unavailability is 56.

In this study, for obtaining all contingency cases, the component outage order is not considered. Under this assumption, the number of contingency cases on the list is obtained using a combinational approach.

$$N_c = \binom{N_e}{O_c} \quad (9)$$

where N_e is the total number of components selected for the contingency analysis and O_c is the contingency order. In this case, with 56 components ($N_e = 56$) and second-order contingency analysis ($O_c = 2$), the total number of contingency cases in the contingency list would be 1540.

However, if the transmission system operator wants to consider the component outage order in the contingency case definition, then the permutation approach would be used for the contingency list and the total number of contingency cases in the lists would further increase, especially when higher-order contingencies are included. For second-order contingencies, it would be double the value according to Equation (9).

Specified thresholds are set for overvoltage, undervoltage, and overloading. By varying the generation loading level with equal proportions, different operating conditions are created. The base case is considered as the standard operating condition and is represented as (Std OC). When the generation loading level is increased by 10%, it is considered the second operating condition (2nd OC), and so on. Different types of severity factor and corresponding operational risk are calculated for up to 90% increments in the generation and loading of the network.

For the existence of the severity factor, three types of technical constraint thresholds are considered: undervoltage, overvoltage, and extreme loading. If, due to the contingency case, any component in the grid crosses this technical threshold, then the severity factor obtains a non-zero voltage. Detailed models of the different technical severity factors are discussed in Sections 3.3–3.6.

3. Designing of Technical Severity Factors and Their Thresholds

The severity factor $F_s(c)$ is used to quantify the impact of individual contingencies. Three types of severity factors (SF) can be defined using electric power system calculations.

3.1. Alternative Severity Factors

1. Technical severity factors, quantifying the impact of a contingency in terms of voltage, current, power, etc., in the transmission grid.
2. Economic severity factors, quantifying the contingency impact in terms of financial consequences for the grid owner and/or the customers.
3. Customer severity factors, quantifying the contingency impact on the customers, e.g., to quantify the number of customers affected by the contingency.

In this section, several technical severity factors are defined. Before quantifying the contingency impact, all severity factor definitions must meet specific criteria [63], as listed below.

3.2. Attributes of Severity Factor

A severity factor (SF) quantifies the contingency impact; each type of severity factor should have a specific attribute, independent of the contingency order.

- The SF should represent the consequences of a certain contingency.
- The SF should be understandable physically in the grid.
- The SF should be deterministic, and it should show the degree of violation.

The main conditions to be fulfilled by the transmission system during its operation can be summarized as follows:

- The voltage should be within a certain band.
- The current or loading of the equipment should be below a certain maximum permissible value.
- The system should be voltage-stable. The severity factor is calculated for steady-state analysis.

To quantify whether these conditions are fulfilled, four severity factors and their technical thresholds are defined in Sections 3.3–3.6, quantifying the extent of undervoltage, overvoltage, extreme loading, and voltage instability. The steady-state voltage instability is quantified through non-convergence contingency cases. In this study, the generators are modeled as PV nodes (constant active power and constant voltage, the latter to represent the automatic voltage regulator), and loads are modeled as PQ nodes (constant active and reactive power).

A severity factor is zero for a specific contingency when the corresponding condition is fulfilled everywhere in the grid. For undervoltage, overvoltage, and extreme loading, a numerical threshold is also defined.

3.3. Mathematical Formulation of Undervoltage Severity Factor $F_{UV}(c)$

This severity factor has a non-zero value when the contingency results in an undervoltage (i.e., the voltage drop crosses the defined threshold) for at least one of the busses in the transmission system.

The undervoltage severity factor, F_{UV} , is defined as follows:

$$F_{UV}(c) = 0, \text{ if } U(b, c) > U_{th-UV} \forall_b \quad (10)$$

$$F_{UV}(c) = \sum |(U(b, c)) - U_{base}(b)| \text{ if } \exists_b U(b, c) \leq U_{th-UV} \quad (11)$$

where c and b refer to the contingency and busbar under consideration, respectively; $U_{base}(b)$ is the voltage in the initial operation state and U_{th-UV} is the minimum acceptable voltage; and $(U(b, c))$ is the voltage due to the contingency c at bus b . The summation in (11) is done over all buses with voltage below the threshold. When the voltage during a contingency is above the undervoltage threshold at all buses, the severity factor is zero (10); otherwise, it is equal to the sum of the absolute values of the voltage change (11). The voltage change is the difference between the voltage during the contingency and the voltage before the contingency (the “base-case” voltage). The numerical threshold for undervoltage contingency is set to 0.95 p.u. of the nominal voltage.

$$U_{th-UV} = 0.95 \text{ p.u.} \quad (12)$$

3.4. Mathematical Formulation of Overvoltage Severity Factor $F_{OV}(c)$

The overvoltage severity factor, $F_{OV}(c)$, has a non-zero value when the contingency results in an overvoltage (i.e., the maximum voltage crosses the overvoltage threshold) for at least one bus. The overvoltage severity factor, $F_{OV}(c)$, is defined as in (13) and (14):

$$F_{OV}(c) = 0, \text{ if } U(b, c) < U_{th-ov} \forall b \quad (13)$$

$$F_{OV}(c) = \sum |(U(b, c)) - U_{base}(b)|, \text{ if } \exists_b U(b, c) \geq U_{th-ov} \quad (14)$$

where c and b refer to the contingency and busbar under consideration, respectively; $U_{base}(b)$ is the voltage in the initial operation state (before the contingency); and U_{th-ov} is the overvoltage threshold. ($U(b, c)$) is the voltage due to the contingency c at bus b ; the summation in (14) is done over all buses with voltage above the threshold. When the voltage during a contingency is below the overvoltage threshold at all buses, the severity factor is zero (13); otherwise, it is equal to the sum of the absolute value of the voltage changes (14). The voltage change is the difference between the voltage during the contingency and the voltage before the contingency (base-case voltage). The numerical threshold of overvoltage contingency is set to 1.05 p.u. of the nominal voltage.

$$U_{th-ov} = 1.05 \text{ p.u.} \quad (15)$$

If the voltage at any bus “ b ” during a contingency $U(b, c)$ is in the 0.95–1.05 p.u. range, then both overvoltage and undervoltage severity factors are equal to zero.

3.5. Mathematical Formulation of Extreme-Loading Severity Factor $F_{EL}(c)$

The extreme-loading severity factor, $F_{EL}(c)$, has a non-zero value when the contingency results in extreme loading for at least one of the components in the transmission system. The extreme-loading severity factor is defined as follows:

$$F_{EL}(c) = 0, \text{ if } (L(S), c) < L_{OL} \forall S \quad (16)$$

$$F_{EL}(c) = \sum |L(S)\%|, \text{ if } \exists_S (L(S), c) \geq L_{OL} \quad (17)$$

where L_{OL} is the extreme-loading threshold, S presents the components that face extreme loading, for instance transmission lines, cables, and transformers. $L(S)$ is the loading value at these components due to the contingency c . The severity factor $F_{EL}(c)$ is zero in (16) if the loading of the component is below the extreme-loading threshold; otherwise, the severity factor is the absolute sum of the loading at the transmission line and transformer in percentage (17). The threshold of extreme loading is set to 100% of the thermal rating of the line or transformer (18).

$$L_{OL} = 100\% \quad (18)$$

Although the limit in this case is taken equal to the thermal rating, there is no need to only consider this limit. There may be cases where a severity factor is more suitably based on exceeding, for example, 80% of the thermal rating; there may also be cases where, for example, 120% of the thermal rating is more appropriate, hence the use of the term “extreme loading” instead of “overloading”.

3.6. Mathematical Formulation of System Collapse Severity Factor $F_{SC}(c)$

The severity factor for system collapse has a non-zero value when contingency cases lead to the non-convergence of the load flow. The system collapse severity factor $F_{SC}(c)$ equals unity in (19) if contingency c does not converge the load flow (LF).

$$F_{SC}(c) = |1| \text{ if } ((c) \leftrightarrow \text{LF}) \quad (19)$$

$$F_{SC}(c) = 0 \text{ if } ((c) \leftrightarrow \text{LF}) \quad (20)$$

Otherwise, the severity factor $F_{5C}(c)$ for the convergent contingency case would be zero in (20). The main concern is that with non-convergence, there is no need to define a numerical threshold.

These non-convergent contingency cases are those cases that the transmission system operator does not want to occur during the lead time, as they could threaten the operational security of the grid.

4. System-Level Operational Risk Behavior under Varying Operating Conditions

To demonstrate the proposed methodology of operational risk assessment, the IEEE 39-Bus New England system is selected. This example network is used in the literature for different types of network studies [64,65]. The main voltage level of this network is 345 kV. Several operational conditions are defined, distinguished by their “generation load level” (GLL). The GLL is the percentage increase of all production and consumption, compared to the original values in the 39-bus system. Operational risk assessment is performed for GLL of 0%, 10%, . . . 90%. By performing contingency analysis, different operational risk indices are quantified by multiplying the probability of contingencies with the specified severity factor, defined in Section 3. Different operational risk indices are shown as a function of GLL. The analysis shows that an increase in one operational risk index may correspond to the decrease of another index. The decrease of a specific operational risk does not mean that the grid becomes more secure. This is illustrated through the interrelations between the different operational risk indices in Section 4.5. On the basis of one operational risk index, the TSO cannot declare that the power system is secure. To obtain a complete picture of the operational security, there is a need for multiple severity factor definitions and, correspondingly, multiple operational risk indices.

4.1. Operational Risk of Extreme Loading (OREL) Behavior under Varying Operating Conditions

This extreme-loading operational risk quantifies how much the transmission system can face the risk of extreme loading due to contingencies. Figure 3 shows the operational risk of extreme loading under different operating conditions, i.e., as a function of GLL. At standard operating conditions (GLL = 0), the overall operational risk of extreme loading (OREL) is 1497% $L(S)$. By increasing the GLL up to 40%, the overall operational risk of extreme loading increases. Higher power flows between generation and consumption will mean that more contingencies result in extreme loading, as depicted in Figure 3. For GLL at 50%, this increasing trend of OREL is broken. For 50% to 80% GLL, the OREL shows a decreasing trend.

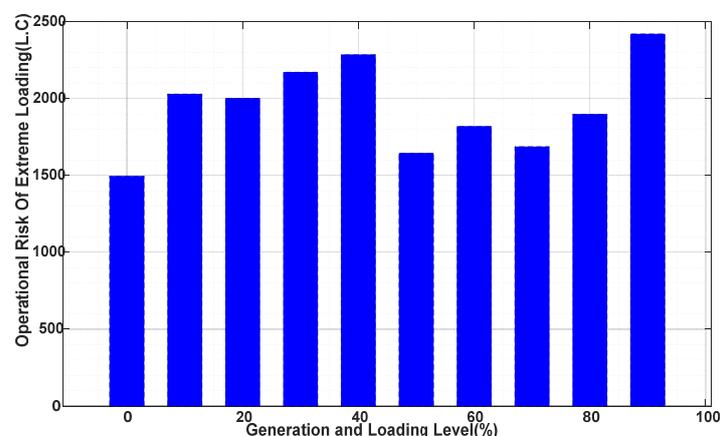


Figure 3. Operational risk of extreme loading as a function of GLL.

The reason for this decrease is that with increasing GLL, there will be more contingencies that result in system collapse (see Section 4.4). Some of the contingencies that contribute to the operational risk of extreme loading (OREL) at 40% GLL will result in non-

convergence of the load flow at 50% GLL. They will thus be contributing to the operational risk of system collapse. To obtain a complete picture of the operational risk, the TSO cannot rely on only one type of operational risk index. This is further discussed in Section 4.5 and in Section 5. System collapse is actually more threatening for the operational security of the power grid. A decreasing value for a specific operational risk index means that this specific risk is reduced, but it does not mean that the total risk to the transmission operation reduces. It is important to consider multiple SF definitions.

4.2. Operational Risk of Overvoltage (OROV) Behavior under Varying Operating Conditions

The operational risk of overvoltage (OROV) index quantifies the overvoltage risk for the transmission system. Figure 4 depicts the behavior of this operational risk under different operating conditions (i.e., for different GLL). Under standard operational conditions, the OROV is at its highest value, 2.066 p.u.; it decreases with increasing GLL, as depicted in Figure 4. The main decrease occurs when the GLL is between 10% and 40%. This decrease does not mean that the transmission system becomes more secure; however, it does mean that the risk of overvoltage is reduced. This is explained in Section 4.5, where the interrelations between the operational risk indexes are discussed.

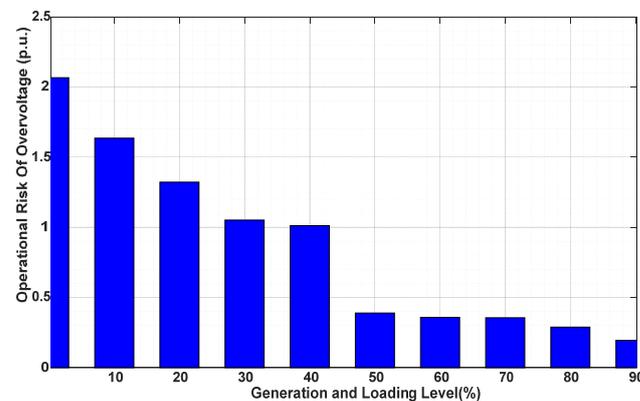


Figure 4. Operational risk of overvoltage as a function of GLL.

4.3. Operational Risk of Undervoltage (ORUV) Behavior under Varying Operating Conditions

The operational risk of undervoltage (ORUV) index quantifies the overall system undervoltage risk due to contingencies. Figure 5 depicts the ORUV behavior under varying GLL. At standard GLL, the ORUV is 17.72 p.u. The operational risk of undervoltage increases up to 70% GLL. Under further increments in the GLL, the ORUV decreases because many contingency events result in instability, in the same way as extreme loading (see Sections 4.1 and 4.5).

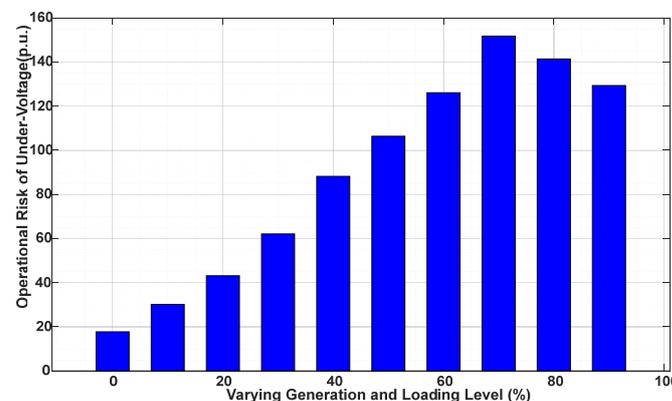


Figure 5. Operational risk of undervoltage as a function of GLL.

4.4. Operational Risk of System Collapse (ORSC) Behavior

The operational risk of system collapse (ORSC) quantifies the system's instability risk. In this study, instability is assumed to be equivalent to non-convergence of the load flow (see Section 3). Figure 6 depicts the ORSC behavior under varying GLL. Under standard operational conditions, the ORSC is 207.5% and it continuously increases with increasing GLL.

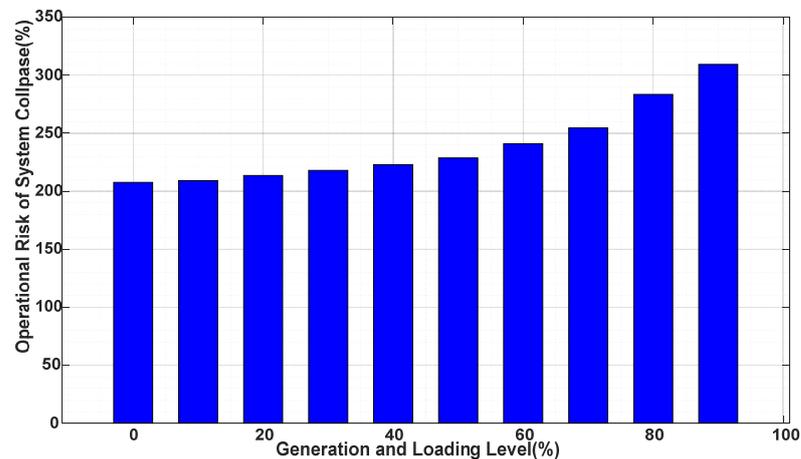


Figure 6. Operational risk of system collapse as a function of GLL.

4.5. Interrelation between Various System-Level Operational Risks

To make a comparison between the different operational risk indices, a “normalization” concept has been used in this study. Figure 7 depicts the different operational risk indices in one figure. The horizontal axis gives the different GLL values; the vertical axis presents a normalized value of the different operational risk indices, where the value for GLL = 0 is normalized to unity. By increasing the GLL, most operational risk indices increase, but irregularly. The decrease in OROV has been explained (see Section 4.2) from the increased power flows. The other operational risk indices initially increase. From 40% GLL, the OREL (“red curve”) decreases. The main reason behind this decrease is that many contingencies, especially those with high loadings, enter into the non-convergence mode, and consequentially, the ORSC increases. An example is shown in Table 1, where the contributions to OREL and ORSC are compared for several contingencies at 40% and 50% GLL. For the yellow-marked cells, the indicated contingency contributes to the indicated operational risk. At 40% GLL, the indicated contingency numbers (1389, 537, 414, 1121, 786, 536, 1331, and 861) converge, but show at least one component with extreme loading; because of that, they contribute to the operational risk of extreme loading. At 50% GLL, the same contingencies do not converge; they contribute to the operational risk of system collapse (ORSC), but no longer to the operational risk of extreme loading (OREL). Consequentially, through a comparison of contingencies for different operating conditions, the ways in which the contingencies move from OREL to ORSC with increasing GLL can be visualized.

The movement of these contingencies from OREL to ORSC explains why, in Figure 7, from 40% to 50%, OREL decreases and ORSC increases. The same applies to the OROV at 50% GLL, where many contingencies become the reason ORSC increases.

The operational risk of undervoltage (ORUV) (blue curve) reaches its highest value for 70% GLL. Table 2 shows that many of the contingencies that contribute to ORUV at 70% GLL enter into the system collapse mode at 80% GLL. Henceforth, the ORUV is higher at 70% GLL than the ORSC. At 80% GLL, the ORUV decreases and ORSC the increases compared to at 70% GLL.

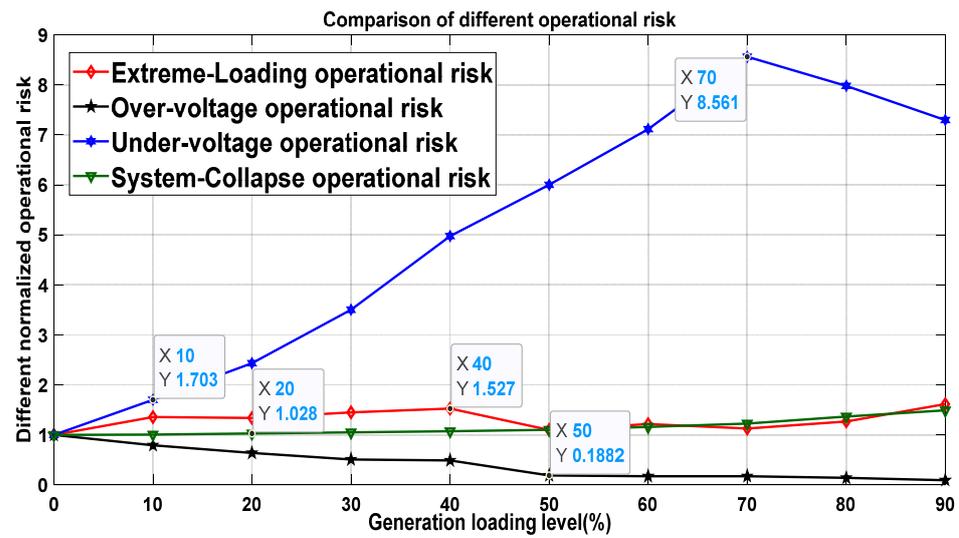


Figure 7. Interrelation between different operational risk definitions.

Table 1. OREL: Contingencies comparison under two operating conditions, where the yellow color indicates that these contingencies are contributing to the operational risk and the red color that they are not contributing.

40% GLL (5th OC)			50% GLL (6th OC)		
C_n	OREL	ORSC	C_n	OREL	ORSC
1389	✓	×	1389	×	✓
537	✓	×	537	×	✓
414	✓	×	414	×	✓
1121	✓	×	1121	×	✓
786	✓	×	786	×	✓
536	✓	×	536	×	✓
1331	✓	×	1331	×	✓
861	✓	×	861	×	✓

Table 2. ORUV: Contingency comparison under two operating conditions, where the yellow color indicates that these contingencies are contributing to the operational risk and the red color that they are not contributing.

70% GLL			80% GLL		
C_n	ORUV	ORSC	C_n	ORUV	ORSC
801	✓	×	801	×	✓
892	✓	×	892	×	✓
659	✓	×	659	×	✓
993	✓	×	993	×	✓
142	✓	×	142	×	✓
700	✓	×	700	×	✓
1170	✓	×	1170	×	✓

From this analysis and the number of contributing contingencies varying at the different operational conditions, it can be deduced that the various operational risks are interrelated. Consequentially, operational risk is multidimensional, and to completely describe the operational security of the grid, multiple severity factors are required on which basis more operational risk indices need to be quantified.

5. Further Analysis of Severity Factor Behavior under Varying Operating Conditions

To understand the behavior of operational risk indices with varying GLL, selected contingencies (C_N) are analyzed along with the probabilistic aspect of contingencies (P_c), and severity factor $F_s(c)$ under varying operating conditions. This analysis is aimed at ob-

taining additional insight into the different risks to which the operation of the transmission system is exposed.

5.1. Operational Risk of Extreme Loading Severity Factor F_{EL} Behavior

The total number of second-order contingencies in the selected network, i.e., the IEEE 39-Bus New England system, is 1540. For the OREL, the severity factor is quantified in terms of line and transformer loading that would occur due to the contingencies; there is no upper limit for the severity factor. As mentioned in Section 3.5, if a contingency results in extreme loading for multiple components, then the severity factor would be the sum of the loading values for those components.

Table 3 depicts the severity factor for extreme loading for several contingencies. Even under STD-GLL, several contingencies have a non-zero severity factor. For example, contingency 414 results in extreme loading across three components: line 13–14 between bus 13 and 14 experiences 205.4% loading, line 10–13 experiences 193.7% loading, and line 17–27 experiences 177.0% loading. The severity factor of contingency 414 is the sum of these loading values, i.e., 576.1%. With increasing GLL, the severity factors increase. For instance, at 10% GLL, contingency 2, SF increases by 10.56%, contingency 414 by 12.92%, and contingency 555 by 55.09%. However, for contingencies 377 and 537, the severity factor decreases. At the third operating condition (20% GLL) for contingency 2, SF increased by 22.07% and for contingency 414 by 27.43%, as compared to the STD-GLL, while contingency 555 enters into the non-convergence (N.C.) mode. All contingencies increase by a specific percentage compared to the previous operating condition and some enter into the non-convergence mode.

Table 3. Extreme loading severity factor behavior under varying operating conditions.

Contingency Probability	0.008	0.0631	0.0378	0.0841	0.042	0.0796	0.1055	0.0573	0.0615	0.1849	0.114
Contingency Number	2	137	377	414	446	537	555	950	952	1331	1356
Std OC	123%	238.90%	282.00%	576.10%	361.10%	244%	499%	383.10%	273.10%	254.90%	358.80%
10% (2nd OC)	136.40%	263.90%	159.50%	650.50%	407.70%	166%	773.90%	428.30%	302.80%	440.10%	N.C
20% (3rd OC)	150.10%	289.50%	341.40%	734.20%	460.80%	185%	N.C	477.50%	OV	494.30%	N.C
30% (4th OC)	164.40%	315.90%	372.20%	834.50%	526.60%	208.20%	N.C	533.50%	OV, UV	558.40%	N.C
40% (5th OC)	179.40%	343.20%	403.90%	987.80%	N.C	632.50%	N.C	OV, UV	OV, UV	650.20%	N.C
50% (6th OC)	204.80%	1661%	435.80%	N.C	N.C	N.C	N.C	870.10%	OV, UV	N.C	N.C
60% (7th OC)	369.50%	401.90%	471.10%	N.C	N.C	N.C	N.C	N.C	473.60%	N.C	N.C
70% (8th OC)	403.20%	434.30%	508.40%	N.C	N.C	N.C	N.C	N.C	517%	N.C	N.C
80% (9th OC)	443.10%	470.10%	548.50%	N.C	N.C	N.C	N.C	N.C	571.40%	N.C	N.C
90% (10th OC)	403.20%	434%	508.40%	N.C	N.C	N.C	N.C	N.C	517%	N.C	N.C

Legend	Low severity Factor	Medium Severity Factor	High Severity Factor	Non-convergent (N.C)
Contingency Number	Contingency Probability		Operating Condition	Contingency take part in undervoltage (UV) and overvoltage operational risk

From Table 3, it can also be noticed that with increasing GLL, any contingency can enter into the N.C. mode; its contribution moves from OREL to ORSC. For instance, contingency numbers 414 and 1331 enter into N.C. mode at the sixth operating condition (50% GLL), while contingency number 1356 enters into N.C. mode at the second operating condition (10% GLL) after a SF of only 358.78%. This concludes that there is no relation between a contingency entering N.C. mode and the SF for extreme loading. The quantitative analysis of extreme loading severity factors shows that the severity factors move from low values to medium, and then reach their peak value before entering into the N.C. mode. OREL behavior (Figure 3) is a replication of $F_{EL}(c)$ behavior; from STD-GLL to 40% GLL, the

contingencies’ severity factors increase, resulting in an increase of the OREL. From 50% GLL to 80% GLL, many contingencies enter into the N.C. mode; the result is that OREL decreases and ORSC increases. Some contingencies have zero contribution to both OREL and ORSC. These contingencies contribute to the operational risk for overvoltage (OV) and undervoltage (UV). For instance, contingency number 952 at 20%, 30%, 40%, and 50% GLL contributes neither to OREL nor to ORSC, but it does contribute to OROV and ORUV. At 60% GLL, the same contingency again contributes to OREL, and from 60% to 80% GLL, this severity factor increases. From 20% (third OC) to 50% GLL (sixth OC), contingency 952 does not create extreme loading situations across the components. Instead, it results in under or overvoltage at various buses. When the GLL is at 60%, the same contingency 952 results in extreme loading across components. The severity factor changes under the varying operating conditions, and from STD-GLL to 40% GLL, many contingencies contribute to the OREL. At 90% GLL, few contingencies with a high severity factor contribute. This reflection can be seen in Figure 3, which summarizes the OREL behavior.

5.2. Operational Risk of Undervoltage $F_{UV}(c)$ Severity Factor Behavior

The undervoltage severity factor is calculated as the sum of absolute voltage change over all nodes during a contingency. The threshold of undervoltage is set up to 0.95 p.u., as depicted in (11). For instance, at STD-GLL, contingency 891 (line 15–16 and generator G:03) creates undervoltage across many buses (32, 15, 12, 14, 13, 10, 11, 07, 08, 04, 05, 06) and the sum of the voltage change after the contingency is 1.65 p.u. Table 4 shows the severity factor for undervoltage for a number of contingencies. For analysis, only those contingencies are considered that show a high severity factor for undervoltage even in the STD-GLL. At first glance, the undervoltage severity factor increases for each contingency. This is illustrated in Table 4. The color variation (green to yellow to red) in each column represents the increase in severity factor. For instance, from STD-GLL to the second OC, where the GLL increases by 10%, for contingency number 891, SF increases by 14.78%; for contingency 1331, SF increases by 27.48%; and for contingency 1351, SF increases by 48.07%.

Table 4. Severity factor behavior of operational risk of undervoltage for varying operating conditions.

Contingency Probability	0.0567	0.1849	0.1002	0.103	0.1057	0.114	0.1223	0.1528	0.1094	0.1151
Contingency Number	891	1331	1351	1352	1353	1356	1359	1370	1405	1407
STD: OC	1.1642	1.3305	1.0372	0.9891	1.1097	1.6016	1.159	1.3767	1.1555	1.017
10%GLL (2nd OC)	1.3363	1.6962	1.5358	1.2538	1.6033	N.C	1.4345	2.3204	1.8285	2.7823
20%GLL (3rdOC)	1.557	2.0903	N.C	1.7328	N.C	N.C	1.848	3.7776	2.8812	N.C
30%GLL (4th OC)	1.8683	2.6369	N.C	N.C	N.C	N.C	2.3334	N.C	N.C	N.C
40%GLL (5th OC)	2.47	3.8621	N.C	N.C	N.C	N.C	3.387	N.C	N.C	N.C
50%GLL (6th OC)	N.C									
60%GLL (7th OC)	N.C									
70%GLL (8th OC)	N.C									
80%GLL (9th OC)	N.C									
90%GLL (10th OC)	N.C									

Legend	Low severity Factor	Medium Severity Factor	High Severity Factor	Non-convergent (N.C)
Contingency Number	Contingency Probability	Operating Condition		

Under transition from 10% GLL to 20% GLL, the SF for these contingencies increases. Some contribute to the ORSC. For instance, contingency 891 SF increases by 16.51%, and contingency 1331 SF increases by 23.23%. Contingencies 1351, 1353, and 1407 contribute to the operational risk system collapse. The SF for these contingencies reaches its peak value at 10% GLL. When GLL increases from 20% to 30%, contingency 891 SF increases by 19.993%; contingency 1331 SF increases by 26.14%; and contingency 1359 SF increases by 26.26%. Contingency 1370 and 1405 are at their peak value for 20% GLL; for 30% GLL,

they will enter into the non-convergence mode and contribute to the operational risk of system collapse. Similarly, when GLL increases from 30% to 40%, contingencies 891, 1331, and 1359 present their peak value of SF and increase by 32.20%, 46.46%, and 45.153%, respectively. Table 4 shows that some contingencies enter into non-convergence mode even at 10% GLL or 20% GLL, while some contingencies experience undervoltage before they take part in the operational risk of system collapse. It can be concluded that as the GLL increases from 0% to 90%, the contingencies' severity factor shows an increasing trend. It is also concluded that there is no relation between the loading level at which a contingency enters the non-convergence mode and the undervoltage severity factor for the base case.

5.3. Operational Risk of Overvoltage $F_{OV}(c)$ Severity Factor Behavior

Similar to the ORUV, the OROV (operational risk of overvoltage) severity factor is obtained as the sum of absolute voltage changes. As mentioned in Section 3.4 the overvoltage threshold is set to 1.05 p.u. For instance, at STD-GLL, when contingency 878 happens (line 15–16 and line 16–24), overvoltage occurs at buses 24, 23, 25, 22, 26, and 19, resulting in an overvoltage severity factor of 0.0658 p.u.

Table 5 shows the relevant SF for several contingencies; the SF decreases for most contingencies with increasing GLL. For instance, from STD-GLL to the 10% increment, the contingency 56 SF decreases by 1.322%, contingency 777 SF decreases by 6.44%, contingency 130 SF decreases by 8.1037%, and contingency 229 shows a decrease in SF of 64.825%. Some contingencies show an initial increase in SF, followed by a decrease or increasing GLL; examples are contingency 1015, 980, and 1190. During the increment from 10% GLL to 20% GLL, contingencies 56, 77, 130, 233, 878, and 1019 show a minor decrease in SF; contingency 229 shows a decrease of 37.98%.

Table 5. Overvoltage severity factor behavior under varying operating conditions.

Contingency Probability	0.05	0.0107	0.0569	0.0225	0.0236	0.0268	0.1402	0.1459	0.1204	0.073	0.0818	0.0924
Contingency Number	56	77	130	229	230	233	875	878	980	1015	1019	1190
STD (OC)	0.0605	0.0729	0.0617	0.0958	0.133	0.0631	0.0863	0.0658	0.0801	0.1017	0.0912	0.0752
10%GLL (2nd OC)	0.0597	0.0682	0.0567	0.0337	0.1196	0.0595	0.0859	0.0636	0.0849	0.1071	0.0867	0.079
20%GLL (3rd OC)	0.0583	0.0571	0.0518	0.0209	0.0374	0.0451	0.0813	0.0466	0.0852	0.1132	0.0884	0.0835
30%GLL (4th OC)	0.0563	0.0528	0.0522	0.0046	0.0276	0.0452	0.0279	0.044	0.0908	0.1201	0.0689	0.0893
40% GLL (5th OC)	0.0535	0.0417	0.0525	0.0039	0.0069	0.0453	0.0177	0.0438	0.0972	0.1278	0.0696	0.0957
50%GLL (6th OC)	4.80×10^{-2}	3.98×10^{-9}	8.02×10^{-10}	3.44×10^{-9}	0.0073	1.22×10^{-9}	0.0198	3.44×10^{-10}	0.0803	0.1371	0.0057	0.1124
60% GLL (7th OC)	2.47×10^{-2}	4.73×10^{-9}	2.14×10^{-9}	2.14×10^{-9}	2.14×10^{-9}	1.67×10^{-9}	2.14×10^{-9}	2.14×10^{-9}	5.99×10^{-2}	0.1462	1.49×10^{-8}	1.12×10^{-1}
70% GLL(8th OC)	1.96×10^{-2}	6.61×10^{-9}	6.78×10^{-9}	6.77×10^{-9}	6.79×10^{-9}	6.06×10^{-9}	6.79×10^{-9}	6.76×10^{-9}	6.27×10^{-2}	0.1571	2.58×10^{-8}	5.26×10^{-2}
80% GLL (9th OC)	1.43×10^{-8}	5.30×10^{-8}	2.13×10^{-8}	2.14×10^{-8}	2.13×10^{-8}	2.03×10^{-9}	N.C	2.13×10^{-8}	2.14×10^{-8}	N.C	4.12×10^{-8}	5.66×10^{-2}
90%GLL (10th OC)	6.57×10^{-8}	6.61×10^{-8}	6.60×10^{-8}	N.C	6.40×10^{-8}	6.44×10^{-9}	N.C	6.58×10^{-8}	6.61×10^{-8}	N.C	5.57×10^{-8}	6.13×10^{-2}

Legend	Low severity Factor	Medium Severity Factor	High Severity Factor	Non-convergent (N.C)
Contingency Number	Contingency Probability		Operating Condition	

With further increment in GLL, the overvoltage severity factor shows a decreasing trend for all contingencies except 1015.

5.4. Operational Risk of System Collapse Severity Factor $F_{SC}(c)$ Behavior

The severity factor for system collapse risk can only have a value of zero or one. The operational risk depends on the number of contingencies resulting in non-convergence of the load flow. Figure 8 shows that with increasing GLL, more contingencies enter into the non-convergence mode. Correspondingly, the operational risk of system collapse also increases.

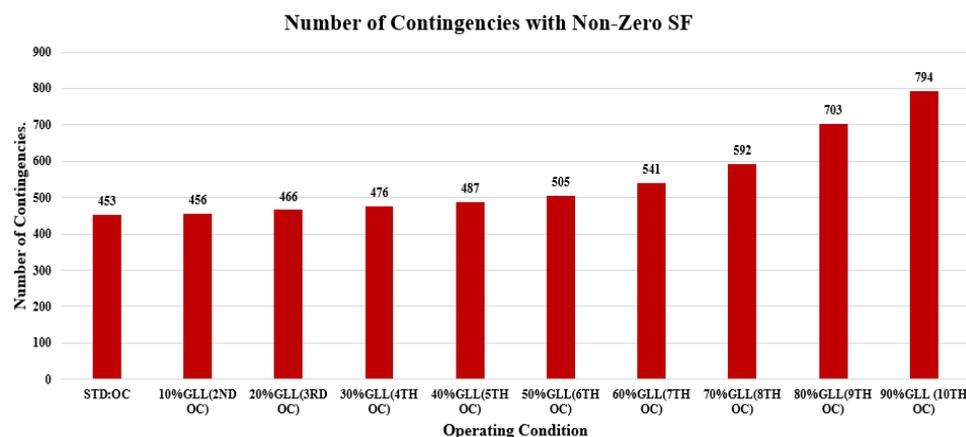


Figure 8. Severity factor in terms of number of non-convergence contingencies under different operating conditions.

6. Discussion

6.1. Technical Severity Factor

Definitions were presented in this paper for four different technical severity factors. Further studies are needed to evaluate the extent to which details in the definition, such as the choice of threshold level, affect the resulting operational risk. The value of the severity factor is also impacted by the details of the methods and models used, including the selection of contingencies (contingency ranking and filtration). Most applications of operational risk assessment require substantial simplifications to be made, leading to uncertainties in the resulting indices.

There are many possibilities in which the transmission system can become unstable, as, for example, shown in [66]. Assessing whether a contingency leads to instability requires a detailed system model and long computational times. This makes it difficult to include in an operational risk assessment.

In this study, Section 3.6, non-convergence of the load flow for a contingency case is used as a proxy for system instability.

This is not correct in all cases, but the method is fast and gives a reasonable indication of the system stability. However, it only covers voltage stability, and it includes numerical issues when the system is actually stable. Advanced network models are needed to avoid including numerical issues and to consider frequency instability, angular instability, and dynamic instability. Such advanced models require significantly more computational effort so that fewer contingencies can be included in the calculation of the operational risk. Further work is needed towards developing simplified and fast methods that can serve as a proxy for other types of instability, next to voltage instability, in operational risk assessment.

6.2. Customer Severity Factor

As mentioned in Section 3.1, the TSO can define three types of severity factor: technical, economic, and customer severity factors. In this study, only technical severity factors are considered, where the impact of contingency cases on the grid is quantified; this can be done, for example, in terms of transmission line and transformer overload or in terms of the overvoltage of buses.

With customer severity factor definitions, the contingency impact can be defined in terms of the number of customers without power or the duration of the power outage that results from the contingency case. The resulting severity factor definitions would be equivalent to those that form the basis for reliability indices such as SAIFI and SAIDI (system average interruption frequency/duration index), as defined in IEEE 1366 [67]. Further extension of the definitions, to obtain a more specific quantification of the impact of a contingency, should include, among others, the size of the customers (with possibly differ-

ent severity factor definitions for large and small customers); distinction between voluntary and enforced disconnection of the supply; the type of contract (including “guaranteed standards of service”); and the real impact on human comfort. The impact on human comfort, in particular, will require a substantial amount of further work; however, it would allow for a more relevant quantification of the potential impact of contingency cases.

6.3. Economic Severity Factor

When the contingency impact is quantified in economic terms for the power grid, for its customers, or for the TSO, this is referred to as an economic severity factor. Such an economic severity factor would, for example, include the costs for the customers due to interruptions, but also the costs that the TSO must make for starting local production units to mitigate overload and undervoltage. Even when the (N-1) criterion is used, an economic risk can be quantified through a severity factor that defines the costs the TSO has to make, for example, by starting expensive production, to ensure that the (N-1) criterion holds even after the occurrence of a contingency case. Such an application of a stochastic method for a system with deterministic operational security could be a way to enable the TSO to become familiar with ORA, without giving up the existing methods with which they have long experience.

For instance, in [68], the severity factor is defined as the minimum cost of generation and load shedding that must be incurred by the TSO due to the contingency occurrence. In [69], the researchers quantify the impact of transmission contingency cases in terms of bidding strategies to the electricity market.

In a completely different field, extensive research aims to quantify and manage the operational risk of investments in the banking sector. For instance, in [70], the authors use the copula approach to quantify the global risk. They quantify the frequency and severity of economic losses with the help of various marginal distribution functions. From this, they estimate the value at risk and the expected economic shortfall at different confidence levels. Similarly, in [71], a Bayesian approach is used to quantify the operational risk other than the credit and market risk. The latter are considered an internal risk of capital charge. For instance, if a TSO wants to deploy this approach for economic operational risk assessment of the grid, then the already planned cost (for power generation and fulfilling the load demand without any contingency) would be considered a regular cost. Due to a certain contingency case, the TSO will incur additional costs; to mitigate overloading, expensive generation has to be started to fulfil the security criteria. That additional cost would be considered an internal risk, as considered by the authors of [71]. In this way, the grid operator can quantify the extent of the economic risk associated with a specific operational state of the grid.

In a similar manner, the TSO can deploy the various techniques mentioned in [72] to quantify and manage the economic operational risk of the grid and can carry out the contingency planning in an economic risk-based way.

6.4. Standardization of Severity Factors

In this study, the operational risk of a transmission system is analyzed for different severity factor definitions. It is deduced that the severity factor plays a significant role in operational risk assessment; the resulting operational risk depends strongly on the considered severity factor. It is also concluded that to maintain or enhance the operational security of a power transmission system, the grid operator cannot rely on one type of operational risk index. There is a need to define multiple operational risk indices based on the different severity factor definitions to obtain a complete picture of the operational security.

From a mathematical point of view, many definitions of severity factor are possible and having formed enough experience, the results can be interpreted by a system operator. This includes guidelines on operational actions when different (operational risk) indices point in opposite directions.

However, the exchange of experience and benchmarking is difficult when different definitions are used. Consequently, it is important to define a number of standard severity factors that quantify the contingency impacts. There is no indication in the literature of any attempt to harmonize those definitions to come to a standard set of definitions. Next to the technical impacts, as considered in this paper, severity factor definitions are also needed for the economic and customer impacts. For customer impacts, severity factor definitions compatible with the reliability indices defined in IEEE Std. 1366 [73] should be used as a base.

6.5. Additional Further Work

Future research on operational risk assessment should include methods to present the detailed results of the operation risk assessment in such a way that it can easily be interpreted by the system operator.

It is also recommended to implement studies such as the one presented in this paper to a large number of existing or realistic transmission networks. An important result of such studies would be guidelines on what would be an acceptable risk level. Such acceptable levels may depend on the size of the network (line length, number of substations, amount of power transported, etc.) and on other risks against which the operational risks should be balanced.

Different acceptable risk levels would be needed for different severity factor definitions. Grid authoritative groups like NERC or ENTSO-E should take a leading role in coming with such guidelines.

Author Contributions: Conceptualization, Z.N.; methodology, Z.N.; formal analysis, Z.N. and M.H.J.B.; resources, M.H.J.B.; writing—original draft preparation, Z.N.; writing—review and editing, Z.N. and M.H.J.B.; visualization, Z.N.; supervision, M.H.J.B.; All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Billinton, R.; Bollinger, K.E. Transmission System Reliability Evaluation Using Markov Processes. *IEEE Trans. Power Appar. Syst.* **1968**, *PAS-87*, 538–547. [[CrossRef](#)]
2. Mallard, S.A.; Thomas, V.C. A Method for Calculating Transmission System Reliability. *IEEE Trans. Power Appar. Syst.* **1968**, *PAS-87*, 824–834. [[CrossRef](#)]
3. Billinton, R.; Allan, R.N. *Reliability Assessment of Large Electric Power Systems*; Springer Science & Business Media: Berlin/Heidelberg, Germany, 1988.
4. Billinton, R.; Allan, R. *Reliability Evaluation of Power Systems*; Springer Science & Business Media: Berlin/Heidelberg, Germany, 1996.
5. Endrenyi, J. *Reliability Modelling in Electric Power Systems*; Wiley: New York, NY, USA, 1978.
6. Choi, J.; Tran, T.T.; El-Keib, A.A.; Thomas, R.J.; Oh, H.; Billinton, R. A method for transmission system expansion planning considering probabilistic reliability criteria. *IEEE Trans. Power Syst.* **2005**, *20*, 1606–1615. [[CrossRef](#)]
7. Rei, A.M.; da Silva, A.M.L.; Jardim, J.; Mello, J.C.O. Static and dynamic aspects in bulk power system reliability evaluations. *IEEE Trans. Power Syst.* **2000**, *15*, 189–195. [[CrossRef](#)]
8. Billinton, R. Composite System Reliability Evaluation. *IEEE Trans. Power Appar. Syst.* **1969**, *PAS-88*, 276–281. [[CrossRef](#)]
9. Singh, C.; Mitra, J. Composite system reliability evaluation using state space pruning. *IEEE Trans. Power Syst.* **1997**, *12*, 471–479. [[CrossRef](#)]
10. Urgan, D.; Chanan, S. A Hybrid Monte Carlo Simulation and Multi Label Classification Method for Composite System Reliability Evaluation. *IEEE Trans. Power Syst.* **2019**, *34*, 908–917. [[CrossRef](#)]
11. Peng, L.; Hu, B.; Xie, K.; Tai, H.M.; Ashenayi, K. Analytical model for fast reliability evaluation of composite generation and transmission system based on sequential Monte Carlo simulation. *Int. J. Electr. Power Energy Syst.* **2019**, *109*, 548–557. [[CrossRef](#)]

12. Ramezanzadeh, S.P.; Mirzaie, M.; Shahabi, M. Reliability assessment of different HVDC transmission system configurations considering transmission lines capacity restrictions and the effect of load level. *Int. J. Electr. Power Energy Syst.* **2021**, *128*, 106754. [[CrossRef](#)]
13. Kamruzzaman, M.; Bhusal, N.; Benidris, M. A convolutional neural network-based approach to composite power system reliability evaluation. *Int. J. Electr. Power Energy Syst.* **2021**, *135*, 107468. [[CrossRef](#)]
14. Jun, Q.; Girgis, A. Optimization of power system reliability level by stochastic programming. *Electr. Power Syst. Res.* **1993**, *26*, 87–95.
15. Edimu, M.; Alvehag, K.; Gaunt, C.T.; Ronald, H. Analyzing the performance of a time-dependent probabilistic approaches for bulk network reliability assessment. *Electr. Power Syst. Res.* **2013**, *104*, 156–163. [[CrossRef](#)]
16. Heylen, E.; Ovaere, M.; Proost, S.; Deconink, G.; Hertem, D.V. A multi-dimensional analysis of reliability criteria: From deterministic $N - 1$ to a probabilistic approach. *Electr. Power Syst. Res.* **2018**, *167*, 290–300. [[CrossRef](#)]
17. Anstine, L.T.; Burke, R.E.; Casey, J.E.; Holgate, R.; John, R.S.; Stewart, H.G. Application of Probability Methods to the Determination of Spinning Reserve Requirements for the Pennsylvania-New Jersey-Maryland Interconnection. *IEEE Trans. Power Appar. Syst.* **1963**, *82*, 726–735. [[CrossRef](#)]
18. Wang, P.; Gao, Z.; Bertling, L. Operational Adequacy Studies of Power Systems With Wind Farms and Energy Storages. *IEEE Trans. Power Syst.* **2012**, *27*, 2377–2384. [[CrossRef](#)]
19. Janssen, A. Operating Considerations in Reliability of Modelling of Wind-Assisted Utility Systems. *Wind Eng.* **1982**, *6*, 193–205.
20. Vazquez, M.A.; Kirschen, D.S. Estimating the Spinning Reserve Requirements in Systems with Significant Wind Power Generation Penetration. *IEEE Trans. Power Syst.* **2009**, *24*, 114–124. [[CrossRef](#)]
21. Da Silva, A.M.L.L.; Sales, W.S.; Manso, L.A.D.F.; Billinton, R. Long-Term Probabilistic Evaluation of Operating Reserve Requirements With Renewable Sources. *IEEE Trans. Power Syst.* **2010**, *25*, 106–116. [[CrossRef](#)]
22. Billinton, R.; Karki, B.; Karki, R.; Ramakrishna, G. Unit Commitment Risk Analysis of Wind Integrated Power Systems. *IEEE Trans. Power Syst.* **2009**, *24*, 930–939. [[CrossRef](#)]
23. Bouffard, F.; Galiana, F.D. An electricity market with a probabilistic spinning reserve criterion. *IEEE Trans. Power Syst.* **2004**, *19*, 300–307. [[CrossRef](#)]
24. Zhou, Z.; Botterud, A. Dynamic Scheduling of Operating Reserves in Co-Optimized Electricity Markets with Wind Power. *IEEE Trans. Power Syst.* **2013**, *29*, 160–171. [[CrossRef](#)]
25. Patton, A. A probability method for bulk power system security assessment: I—basic concepts. *IEEE Trans. Power Appar. Syst.* **1972**, *PAS-91*, 54–61. [[CrossRef](#)]
26. Patton, A. A probability method for bulk power system security assessment: II—development of probability methods for normally operating components. *IEEE Trans. Power Appar. Syst.* **1972**, *PAS-91*, 2480–2485. [[CrossRef](#)]
27. Patton, A. A probability method for bulk power system security assessment: III—models for standby generators and field data collection and analysis. *IEEE Trans. Power Appar. Syst.* **1972**, *PAS-91*, 2486–2493. [[CrossRef](#)]
28. Patton, A. Assessment of the security of operating electric power systems using probability methods. *Proc. IEEE* **1974**, *62*, 892–901. [[CrossRef](#)]
29. Singh, C.; Patton, A.; Lago-Gonzalez, A.; Vojdani, A.; Gross, G.; Wu, F.; Balu, N. Operating considerations in reliability modeling of interconnected systems—an analytical approach. *IEEE Trans. Power Syst.* **1988**, *3*, 1119–1126. [[CrossRef](#)]
30. Da Silva, A.M.L.; Endrenyi, J.; Wang, L. Integrated treatment of adequacy and security in bulk power system reliability evaluations. *IEEE Trans. Power Syst.* **1993**, *8*, 275–285. [[CrossRef](#)]
31. Loparo, K.A.; Malek, F.A. A probabilistic approach to dynamic power system security. *IEEE Trans. Circuits Syst.* **1990**, *37*, 787–798. [[CrossRef](#)]
32. Khan, M.; Roy, B. Composite system spinning reserve assessment in interconnected systems. *IEEE Proc. Gener. Transm. Distrib.* **1995**, *142*, 305–309. [[CrossRef](#)]
33. Gooi, H.B.; Mendes, D.; Bell, K.; Kirschen, D.S.; Kirschen, D.S. Optimal scheduling of spinning reserve. *IEEE Trans. Power Syst.* **1999**, *14*, 1485–1492. [[CrossRef](#)]
34. Da Silva, A.L.; Alvarez, G. Operating reserve capacity requirements and pricing in deregulated markets using probabilistic techniques. *IET Gener. Transm. Distrib.* **2007**, *1*, 439–446. [[CrossRef](#)]
35. Zio, E. The future of risk assessment. *Reliab. Eng. Syst. Saf.* **2018**, *177*, 176–190. [[CrossRef](#)]
36. Li, W. *Risk Assessment of Power Systems Models, Methods and Applications*; John Wiley & Sons: New York, NY, USA, 2014.
37. Ciapessoni, E.; Cirio, D.; Kjølle, G.; Massucco, S.; Pitto, A.; Sforza, M. Probabilistic Risk-Based Security Assessment of Power Systems Considering Incumbent Threats and Uncertainties. *IEEE Trans. Smart Grid* **2016**, *7*, 2890–2903. [[CrossRef](#)]
38. Vefsnmo, H.; Kjølle, G.; Jakobsen, S.H.; Ciapessoni, E.; Cirio, D.; Pitto, A. Risk assessment tool for operation: From threat models to risk indicators. In Proceedings of the 2015 IEEE Eindhoven PowerTech, Eindhoven, The Netherlands, 29 June–2 July 2015.
39. Li, W.; Korczynski, J. Risk evaluation of transmission system operation modes: Concept, method and application. In Proceedings of the 2002 IEEE Power Engineering Society Winter Meeting Conference Proceedings (Cat. No.02CH37309), New York, NY, USA, 27–31 January 2002.
40. Perninge, M.; Söder, L. A Stochastic Control Approach to Manage Operational Risk in Power Systems. *IEEE Trans. Power Syst.* **2011**, *27*, 1021–1031. [[CrossRef](#)]

41. Jmii, H.; Meddeb, A.; Chebbi, S. Newton-Raphson Load Flow Method for Voltage Contingency Ranking. In Proceedings of the 2018 15th International Multi-Conference on Systems, Signals & Devices (SSD), Yasmine Hammamet, Tunisia, 19–22 March 2018.
42. Singh, S.N.; Srivastava, L.; Sharma, J. Fast voltage contingency screening and ranking using cascade neural network. *Electr. Power Syst. Res.* **2000**, *53*, 197–205. [[CrossRef](#)]
43. Pandit, M.; Srivastava, L.; Sharma, J. Cascade fuzzy neural network based voltage contingency screening and ranking. *Electr. Power Syst. Res.* **2003**, *67*, 143–152. [[CrossRef](#)]
44. Mikolinnas, T.A.; Wollenberg, B. An Advanced Contingency Selection Algorithm. *IEEE Trans. Power Appar. Syst.* **1981**, *PAS-100*, 608–617. [[CrossRef](#)]
45. Du, Y.; Li, F.; Li, J.; Zheng, T. Achieving 100x Acceleration for N-1 Contingency Screening With Uncertain Scenarios Using Deep Convolutional Neural Network. *IEEE Trans. Power Syst.* **2019**, *34*, 3303–3305. [[CrossRef](#)]
46. Kaplunovich, P.; Turitsyn, K. Fast and Reliable Screening of N-2 Contingencies. *IEEE Trans. Power Syst.* **2016**, *31*, 4243–4252. [[CrossRef](#)]
47. Almeida, S.A.B.d.; Pestana, R.; Barbosa, F.M. Integration of common cause faults in the operational probabilistic approach. In Proceedings of the 2010 IEEE 11th International Conference on Probabilistic Methods Applied to Power Systems, Singapore, 14–17 June 2010.
48. Bhuiyan, M.Z.A.; Anders, G.J.; Philhower, J.; Du, S. Review of static risk-based security assessment in power system. *IET Cyber-Phys. Syst. Theory Appl.* **2019**, *4*, 233–239. [[CrossRef](#)]
49. Wan, H.; McCalley, J.D.; Vittal, V. Risk Based Voltage Security Assessment. *IEEE Trans. Power Syst.* **2000**, *15*, 1247–1254. [[CrossRef](#)]
50. Dai, Y.; McCalley, J.D.; Samra, N.A.; Vittal, V. Annual Risk Assessment for Overload Security. *IEEE Trans. Power Syst.* **2001**, *16*, 616–623. [[CrossRef](#)]
51. Feng, Y.; Wu, W.; Zhang, B.; Li, W. Power System Operation Risk Assessment Using Credibility Theory. *IEEE Trans. Power Syst.* **2008**, *23*, 1309–1318. [[CrossRef](#)]
52. Ni, M.; McCalley, J.D.; Vittal, V.; Tayyib, T. Online Risk-Based Security Assessment. *IEEE Trans. Power Syst.* **2003**, *18*, 258–265. [[CrossRef](#)]
53. Ni, M.; McCalley, J.D.; Vittal, V.; Greene, S.; Ten, C.-W.; Ganugula, V.S.; Tayyib, T. Software Implementation of Online Risk-Based Security Assessment. *IEEE Trans. Power Syst.* **2003**, *18*, 1165–1172. [[CrossRef](#)]
54. Jong, M.D.; Papaefthymiou, G.; Palensky, P. A Framework for Incorporation of Infeed Uncertainty in Power System Risk-Based Security Assessment. *IEEE Trans. Power Syst.* **2017**, *33*, 613–621. [[CrossRef](#)]
55. Bollen, M.; Nazir, Z. Operational Risk Assessment—Time for a Smarter Look at Reliability for Power Transmission Systems. 2022. Available online: <https://smartgrid.ieee.org/bulletins/june-2022/operational-risk-assessment-time-for-a-smarter-look-at-reliability-for-power-transmission-systems> (accessed on 20 July 2022).
56. Liu, P.Q.; Li, H.-Q.; Du, Y.; Zeng, K. Risk assessment of power system security based on component importance and operation state. In Proceedings of the 2014 International Conference on Power System Technology, Chengdu, China, 20–22 October 2014.
57. Ciapessoni, E.; Cirio, D.; Grillo, S.; Massucco, S.; Pitto, A.; Silvestro, F. Operational Risk Assessment and control: A probabilistic approach. In Proceedings of the 2010 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT Europe), Gothenburg, Sweden, 11–13 October 2010.
58. Winter, W.H. Measuring and reporting overall reliability of bulk electricity systems. In Proceedings of the 1980 CIGRE Session, Paris, France, 27 August–4 September 1980. Paper No. 32-15.
59. Winter, W.H. Disturbance performance of bulk electricity systems. In Proceedings of the 1986 CIGRE Session, Paris, France, 27 August–4 September 1986. Paper No. 37/38/39-02.
60. Schneider, A.; Raksany, J.; Gunderson, R.; Fong, C.; Roy, B.; Neill, P.M.O.; Silverstein, B. Bulk system reliability-measurement and indices. *IEEE Trans. Power Syst.* **1989**, *4*, 829–835. [[CrossRef](#)]
61. 5th CEER Benchmarking Report on the Quality of Electricity Supply. 2005. Available online: <https://www.ceer.eu/documents/104400/-/-/0f8a1aca-9139-9bd4-e1f5-cdbdf10c4609> (accessed on 20 July 2022).
62. Allan, R. Power system reliability assessment—A conceptual and historical review. *Reliab. Eng. Syst. Saf.* **1994**, *46*, 3–13. [[CrossRef](#)]
63. Nazir, Z.; Bollen, M.H. Operational Risk Assessment of Transmission Systems: A review. *Int. J. Electr. Power Energy Syst.* **2022**. *submitted*.
64. Cupelli, M.; Cardet, C.D.; Monti, A. Voltage stability indices comparison on the IEEE-39 bus system using RTDS. In Proceedings of the 2012 IEEE International Conference on Power System Technology (POWERCON), Auckland, New Zealand, 30 October–2 November 2012.
65. Rahmouni, W.; Benaïssa, L. Transient stability analysis of the IEEE 39-bus power system using gear and block methods. In Proceedings of the 2017 5th International Conference on Electrical Engineering-Boumerdes (ICEE-B), Boumerdes, Algeria, 29–31 October 2017.
66. Kundur, P. *Power System Stability and Control*, Toronto; McGraw-Hill: New York, NY, USA, 2022.
67. IEEE. *1366-2012 IEEE Guide for Electric Power Distribution Reliability Indices*; IEEE Standard Association: Piscataway, NJ, USA, 2012.
68. Song, X.; Wang, Z.; Xin, H.; Gan, D. Risk-based dynamic security assessment under typhoon weather for power transmission system. In Proceedings of the 2013 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC), Hong Kong, China, 8–11 December 2013.

-
69. Pour, M.M.; Taheri, I.; Marzooni, M.H. Assessment of transmission outage Contingencies' effects on bidding strategies of electricity suppliers. *Int. J. Electr. Power Energy Syst.* **2020**, *120*, 106053.
 70. Valle, L.D.; Fantazzini, D.; Giudici, P. Copulae and Operational Risks. *Int. J. Risk Assess. Manag. Forthcom.* **2006**, *9*, 238–257.
 71. Giudici, P.; Bilotta, A. Modelling Operational Losses: A Bayesian Approach. *Qual. Reliab. Eng. Int.* **2004**, *20*, 407–417. [[CrossRef](#)]
 72. Jorion, P. *Value at Risk-The New Benchmark for Managing Financial Risk*, 3rd ed.; McGraw-Hill Professional: New York, NY, USA, 2007.
 73. IEEE. *P1366/D5-IEEE Draft Guide for Electric Power Distribution Reliability Indices*; IEEE: Piscataway, NJ, USA, 2022; pp. 1–40.