sustainability

MDPI

Article

A Preventive Control Approach for Power System Vulnerability Assessment and Predictive Stability Evaluation

Ersen Akdeniz [1,2,*] and Mustafa Bagriyanik [1]

[1] Department of Electrical Engineering, Istanbul Technical University, Istanbul 34469, Turkey
[2] Siemens Gamesa Renewable Enerji A.Ş, Izmir 35530, Turkey
* Correspondence: eakdeniz@itu.edu.tr

Abstract: Early detection of cascading failures phenomena is a vital process for the sustainable operation of power systems. Within the scope of this work, a preventive control approach implementing an algorithm for selecting critical contingencies by a dynamic vulnerability analysis and predictive stability evaluation is presented. The analysis was carried out using a decision tree with a multi-parameter knowledge base. After the occurrence of an initial contingency, probable future contingencies are foreseen according to several vulnerability perspectives created by an adaptive vulnerability search module. Then, for cases identified as critical, a secure operational system state is proposed through a vulnerability-based, security-constrained, optimal power flow algorithm. The modular structure of the proposed algorithm enables the evaluation of possible vulnerable scenarios and proposes a strategy to alleviate the technical and economic impacts due to prospective cascading failures. The presented optimization methodology was tested using the IEEE-39 bus test network and a benchmark was performed between the proposed approach and a time domain analysis software model (EMTP). The obtained results indicate the potential of analysis approach in evaluating low-risk but high-impact vulnerabilities in power systems.

Keywords: power system vulnerability assessment; preventive control; critical contingency selection; decision tree-based stability evaluation

Citation: Akdeniz, E.; Bagriyanik, M. A Preventive Control Approach for Power System Vulnerability Assessment and Predictive Stability Evaluation. *Sustainability* **2023**, *15*, 6691. https://doi.org/10.3390/su15086691

Academic Editors: Bo Yang, Zhijian Liu and Lin Jiang

Received: 23 March 2023
Revised: 11 April 2023
Accepted: 12 April 2023
Published: 15 April 2023

1. Introduction

Power system (PS) operation is a consumption–generation balancing act where operational costs aim to be minimized traditionally. In order to preserve the balance, system operators are obliged to take action in order to prevent cascading failures which might also lead to partial or total blackouts [1,2]. Thus, PS operators need to prepare emergency plans which requires a detailed analysis of their system including various aspects [3]. This phenomenon was also proven in recent blackout events, such as those in India and Turkey [4], where blackouts of whole electrical grids were caused due to operational failures, and the South Australian Transmission Grid failure which was due to insufficient analysis of vulnerabilities as a result of extreme weather conditions [5]. Any critical component failure may have negative impacts on system operational costs due to the ramp-up/down of generators or unserved energy penalties [6–9]. In practice, PS planners design the grid to be sufficient to cope with contingencies by allocating adequate reserves in generator production and transmission lines to provide a certain level of redundancy in case of pre-estimated critical contingencies [10,11]. However, as the system further expands from its original design, the implementation of additional reserves/capabilities is limited mostly by economic and environmental constraints, which weaken the hand of the PS operators (PSO) while keeping the system within the limits defined in power quality standards [12,13]. If a disturbance continues and required corrective action is not implemented, the system is expected to be drawn in an emergency state for which boundary limits are exceeded and as a result, the power system stability will be distorted [14–17]. Under these circumstances,

PSOs should take sufficient measures in order to maintain a secure operation, which might include load shedding and partial islanding as an alternative solution to prohibit a total blackout in the system [18–22].

In power system analysis, power flow optimization is known to be a critical topic attracting the attention of many researchers. Although several attempts have been made to model large-scale systems, none have proven to be completely successful [14,23]. The problem complexity arises not only from the problem size but also the complex non-linear dynamics of power systems. Most of the traditional OPF problems involve classical contingency constraints mainly relying on the electrical parameters of the system [17,18]. Steady-state security analysis is also a commonly used tool for determination of possible limit violations after credible outages [16,24]. However, as the grid complexity increases, the possible combinations of N-k contingencies drastically increase, which makes the analysis very time consuming, and makes real time analysis and online decision-making analysis almost unpractical [9,16]. Furthermore, as the cascading failure develops in a dynamic nature, steady state approximations become less reliable in predicting the behavior of the distorted system [25,26]. In such cases, transient stability analysis techniques and real-time transient models are implemented for obtaining a better system representation. However, as the dimension of the studied system enhances, implementation of time-domain analysis might become impractical due to grid complexity.

Most of the available work on contingency analysis studies uses exhaustive search and/or Monte Carlo simulation techniques to try and determine the worst contingencies [14,27,28]. For most of the N-2 contingency evaluation studies, electrically coupled pairs are generally used as a special case, such as after a line trip due to an initial fault, a neighboring or a parallel line dropping out of service due to overload, or a relay trip [17]. This type of approach provides a straightforward and reasonable way of determining the most probable contingencies in a classical manner. However, this approach might shadow contingencies due to new threats known as intentional attacks (cyber or physical) and adverse weather impacts.

Some recent studies [3,5,29] on power system vulnerability analysis are based mainly on topology and flow-based methods. Topology-based methods tend to be strongly dependent on grid topology, which sometimes does not discover the ongoing active phenomena inside. In flow-based approaches, energy balance equations and physical properties of the system are more important. However, as the system dimension expands, the solution complexity will also increase, which makes analysis inefficient. The techno-economic results of intentional attacks on transmission lines are demonstrated in [9], which indicates the necessity for PSOs to optimize their system to be resilient against such conditions. Critical equipment determination generally targets impacts due to single branch failure or randomly generated subsets. In [28], the proposed algorithm aims to select multiple contingency groups which can result in cascading failures. However, in these approaches there is a risk that the worst blackouts will not be detected and that high impact, small subsets will not be covered. In [7,8], the proposed methods are dependent on identifying over-limits and loss of loads but do not cover the complete process of disturbances. In [29], the impact of random line failures on grid vulnerability is studied, and it is concluded that small and large failures can induce similar performance loss in robustness. In [30], the overall vulnerability assessment of the power grid is made via structural and operative vulnerability indices defined for buses.

In our study, a different perspective of preventive control is presented by implementing a critical contingency selection algorithm through a dynamic vulnerability analysis module and a decision tree-based model stability evaluation with a multiple parameter knowledge base. In Section 2, the methodology of the solution approach is presented. In summary, for each critical scenario, an adaptive rescheduling and load shedding algorithm is used which considers operational and non-operational vulnerabilities for lines while bus loadings randomly changed within the $\pm$20% range. The secure system state is derived from the decision tree (DT) evaluation module using key performance indices as prediction parameters. Then, the critical point for the system where stability deteriorates is detected.

At this point, a corrective security-constrained and genetic algorithm-based optimal power flow (CSC-OPF) is implemented to determine the secure system settings via optimizing the generator active power output and load shedding if necessary. In Section 3, the developed methodology is tested using the IEEE-39 bus network and a benchmark is made between the proposed approach and time domain analysis software (EMTP) model for showing the effectiveness of the method in the determination of the stability deviation point for the tested contingency sequence. The details of the CSC-OPF algorithm and a sample result of the secure system state transfer cost calculation is presented for a specific contingency case. In Section 4, a brief discussion on findings and future work is presented.

2. Methodology

Within the scope of this study, a vulnerability analysis tool is developed enabling the user to define various operational scenarios for the selected test cases via the developed graphical user interface. Initially, a user can choose the test case for analysis with the required operational constraints and later can calculate the performance indices defined in Table 1. Then, the program provides the user individual (operational (OPI), intentional attack (TAI), adverse weather (AWI)) and total vulnerability indices (TVI) and related line rankings corresponding to their relevant vulnerability type. As a result, the vulnerability analysis program (VAP) selects the most credible contingency cases, thus narrowing the possible contingency subsets.

Table 1. Performance indicators used as DT predictors.

Contingency-Based PIs	**Severity-Based PIs**
$PI_{P_c} = \sum_{l=1}^{n_{line}} \frac{w_p}{2} \left(\frac{P_l}{P_{l,max}} \right)^{2N}$	$PI_{P_s} = \sum_{i=1}^{n_{line}} w_p \frac{P_{loading} - P_{lim}}{1 - P_{cri}}$
$PI_{Vb_c} = \sum_{i=1}^{n_{bus}} \frac{w_b}{2} \left(\frac{\lvert V_i - V_{bc} \rvert}{\lvert V_{max} - V_{min} \rvert} \right)^{2N}$	$PI_{Vb_s} = \sum_{i=1}^{n_{bus}} w_p \frac{1 - V_{b,i}}{V_{cri}}$
$PI_{Qg_c} = \sum_{i=1}^{n_{gen}} \frac{w_g}{2} \left(\frac{Q_{g,i}}{Q_{g,max}} \right)^{2N}$	$PI_{Qg_s} = \sum_{i=1}^{n_{gen}} w_g \left(\frac{Q_g}{Q_{g,max}} - Q_{g,lim} \right)^{2N}$
$PI_{Pg_c} = \sum_{i=1}^{n_{gen}} \frac{w_g}{2} \left(\frac{P_g}{P_{g,max}} \right)^{2N}$	$PI_{Pg_s} = \sum_{i=1}^{n_{gen}} w_g \left(\frac{P_g}{P_{g,max}} - P_{g,lim} \right)^{2N}$
$PI_{Ang_c} = \sum_{l=1}^{n_{line}} w_{ang} \frac{\lvert \Delta\theta_i \rvert}{90}$	$PI_{Ang_s} = \sum_{l=1}^{n_{line}} w_{ang} \frac{\lvert \Delta\theta_i - \theta_{lim} \rvert}{45}$
$PI_{LoL} = \sum_{l=1}^{n_{bus}} w_{LoL} \frac{P_{LoL}}{P_{L\_tot}}$; $PI_{LoG} = \sum_{l=1}^{n_{gen}} w_{LoG} \frac{P_{LoG}}{P_{L\_totG}}$; $PI_{IB} = w_{LoL} \sum_{l=1}^{n_{bus}} isl_{bus}$	
$OPI_{ctg} = \sum \left(PI_{P_C} + PI_{Vb_C} + PI_{Qg_C} + PI_{Ang_C} + PI_{LoL} + PI_{LoG} + PI_{IB} \right)$	$OPI_{sev} = \sum \left(PI_{P_S} + PI_{Vb_S} + PI_{Qg_S} + PI_{Ang_S} + PI_{LoL} + PI_{LoG} + PI_{IB} \right)$

After this selection, with the help of a decision tree-based security analysis module, the impact of each selected contingency on system stability is evaluated. According to the results obtained from the CSC-OPF module, the program tries to optimize the generator's active power settings to obtain the best fitness value defined by overall cost function. If system limit constraints are still violated, load shedding is implemented for transferring the system to a more secure state which enables convergence in PF. The cost of the system for current operational status and the cost of transfer to a more secure state is calculated via the secure transfer cost (STC) calculation module, and if a feasible result is obtained, secure system transfer conditions are applied by the decision support module.

2.1. Contingency Selection

In contingency selection, direct and indirect methods are widely used [4]. The contingency impacts defined in terms of performance indices (such as active/reactive power and voltage level variations) are regarded as direct methods [5]. However, some critical contingencies were reported because of natural calamities, malicious attacks, or maloperations [6,18–20]. Thus, in order to represent real system conditions a broader approach is needed. Our approach also considers non-technical parameters, which have previously been defined as non-operational performance indices [31,32]. With the help of the proposed vulnerability evaluation module, critical contingencies were selected according to the total vulnerability evaluation (TVE) module where operational and non-operational constraints are used in the determination of the most vulnerable points in terms of operational, adverse weather, and intentional attack considerations. Thus, instead of investigating all mathematically possible combinations, such as those made in a brute-force contingency analysis, a narrowed contingency subset was obtained using a fuzzy interference system which reduced the analysis time drastically. Then, for each credible contingency a fitness value for an objective function was evaluated, which aims to keep the load shed at minimum level while maintaining low bus voltage deviations and transmission system losses. After determining the optimal system configurations for each contingency from the reduced subset, the optimum generator set points, and if necessary, other relevant control actions such as load shedding, were determined. By doing so, the system will be able to be survive after the occurrence of any critical pre-defined contingency, thus preventing cascading failures and partial blackouts in the system.

2.2. Decision Tree-Based Security Analysis

Decision trees for classification are an effective artificial intelligence tool for solving high-dimensional classification problems [20]. The principal motivation is to form a predictive model of the system that covers all possible operational scenarios [25]. The complicated classification problems are converted to a set of inequality equations composed of pre-defined predictor parameters or their linear combinations [17,23].

During the training process of decision trees, a minimum of 10 times more than the number of degrees of freedom model is required to cover all possible contingencies and operational scenarios [33]. If the training set is large enough, the quality of the obtained results will be good (the details of training and dataset creation are presented in Section 2.5.2). In this module, base scenario and contingency scenarios are studied using prediction results described as secure or insecure where scenarios are obtained via loading variations under line outage conditions considering 2 consecutive losses in the same time frame. The predictors are derived from contingency- and severity-based performance indices. Their combinations and parameter details are given in Table 1 and the methodology is described in [34].

In this work, the MATLAB R2021a statistical and machine learning toolbox [35] was used for the creation of classification trees in order to interpret the relationship between the prediction variable and target variable values, which was system stability in our case. Classification trees are the foundation for other, similar machine learning algorithms implementing different applications of decision trees. Classification trees, which were described first in [34], are used as a decision tree analysis method. In this approach, decision trees are used where each node becomes a split point for a predictor variable. The final convergence of the test network under various operational conditions is used as a stability indicator, and performance indicators (PI) described in Table 1 are used as predictor variables.

2.3. Main Algorithm for Decision Support

The proposed decision support tool given in Figure 1 performs as follows:

- Topological system information (i.e., switch status, line/bus outages) and electrical parameters are obtained to determine the initial operating point (OP) of the system.

- The environmental and weather forecast-related information is obtained and assumed to be changing in accordance with different zones defined for the test network.
- With this initial information, a total vulnerability evaluation of the system, including operational, environmental, and adverse weather-related indices, is made in order to select the most vulnerable parts of the system [34]. The probable and possible risks are combined to provide a more comprehensive contingency analysis of the system under study.
- From each module located in the basic vulnerability module/evaluation (BVE), a stack based on TVR is formed for which the size is determined according to the system operation requirements set by TSO.
- From each stack, total vulnerability ranking (TVR) modules provide separate subsets of vulnerable lines.
- Then, a pre-check of system security and stability is made via the critical contingency check module considering load variations at time step ($\Delta t = \tau$). If any critical contingency which requires immediate action is detected, the base critical contingency check (Base C3) module for rescheduling is applied in order to shift the system to a more secure operating point (OP_0′). Otherwise, the system is kept around the initial operating point while updating results obtained from BVE.
- After occurrence of the initial contingency, the test system is transferred to a new operating state (if the system satisfies basic N-1 requirements, if not it is expected that the results from the BVE are transferred to a secure operating point) which is described as disturbed operating point-1 (OP_1).

Then, the proposed standard vulnerability evaluation module (SVE) determines an updated ranking for the operational constraints to detect the most vulnerable parts of the system according to operational/electrical parameters, and the first subset of operational performance ranking (OPR) is provided.

- Finally, a comprehensive check of system security and stability is made via the critical contingency check (C3) module while updating the information received from SVE and considering the load variation uncertainty. Similarly, if any critical contingency is detected from N-1 contingency scenarios for which the candidates are prepared by SVE, the rescheduling and load shed (RLS) algorithm first tries rescheduling the available generators. If the reserve generation capability is not enough, then the proposed algorithm sheds the load according to the selection methodology proposed in the next section.

2.4. C3-RLS Algorithm

The proposed critical contingency check module is a DT-based system security evaluation method. The knowledge base of the module produced by the scenario generation module for which the operator can easily define various system operating conditions including load variations and pre-outaged components.

The flow process for the C3-RLS module is described in Figure 2.

- The standard vulnerability evaluation module online monitors the system status and other weather- and intrusion-related information. As the system conditions change above the predefined limits, the output stacks of the related vulnerability ranking modules are updated automatically. Each module presents a separate critical line list accordingly.
- Then, all candidates are stacked in the critical contingency pool to be analyzed via the proposed decision tree stability (DTS) evaluation module. In the DTS module, a stability analysis is carried out for which details are presented in part 2.5. Initially, generator re-dispatch values are determined for the foreseen instability. If rescheduling is not enough, loads are shed according to the indices computed via the power flow contribution matrix. The optimal values are calculated via the corrective security-constrained AC optimal power flow (CSC-OPF) algorithm.

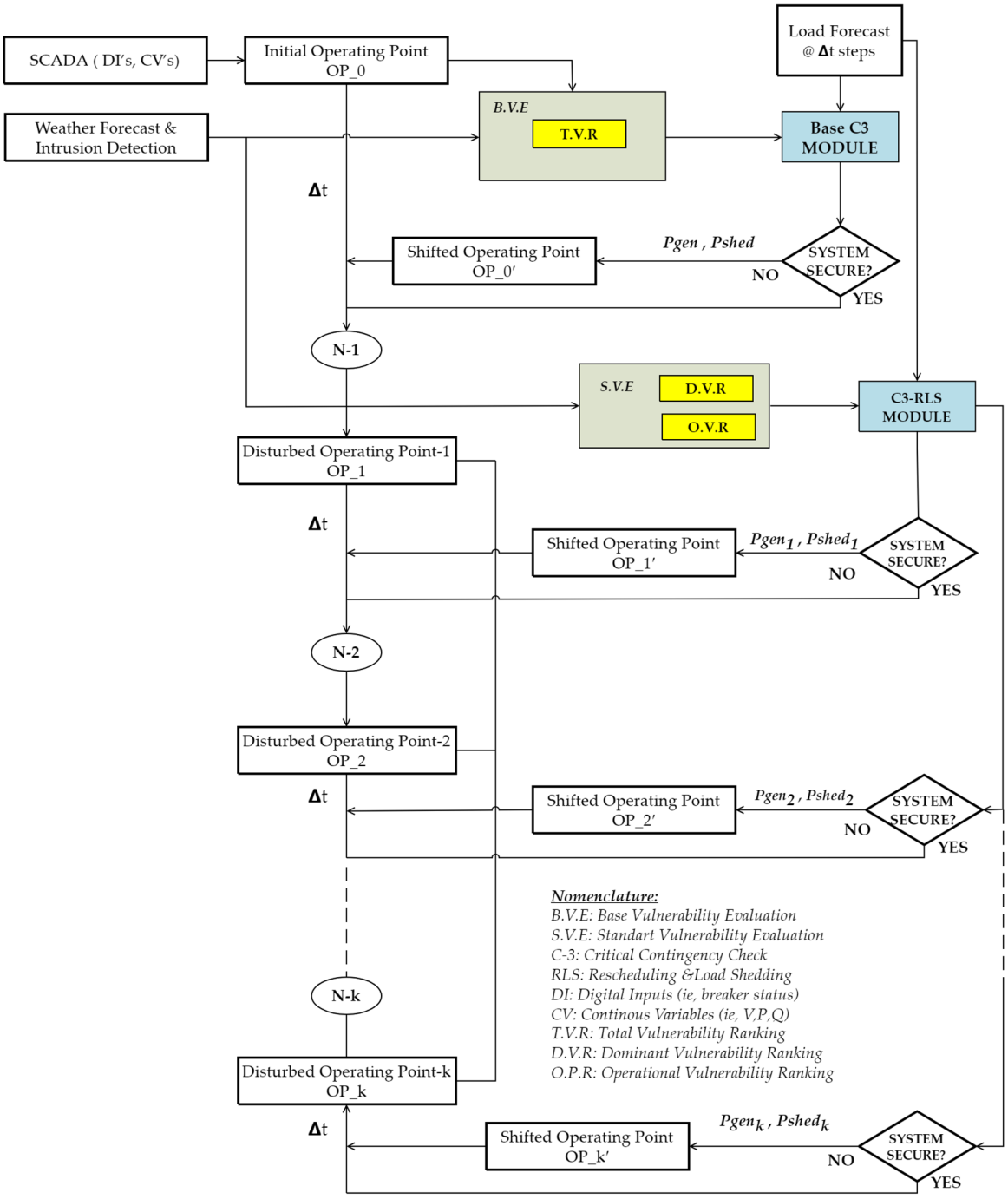

Figure 1. Proposed N-k contingency evaluation algorithm based on BVE, SVE, and C3-RLS modules.

In addition to operational costs based on generator active power, market prices related to the ramp up and down of generators, load shed, or unserved customer penalty costs are also foreseen in this module.

The knowledge-based decision support tool provides the best what-if operational scenarios and tries to optimize and transfer the electrical test system to a more secure state.

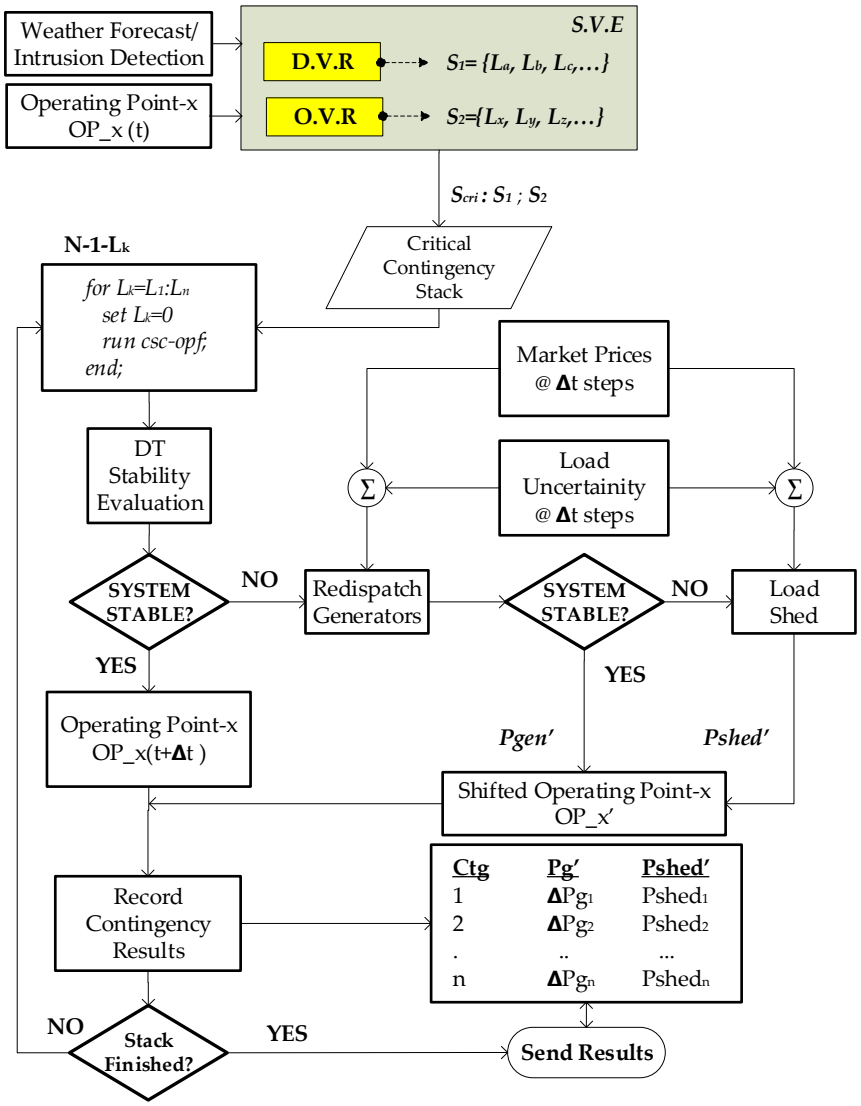

Figure 2. Proposed C3-RLS module flow chart.

2.4.1. Corrective Security-Constrained OPF Algorithm

The implemented corrective security-constrained optimal power flow (CSC-OPF) is based on an optimization approach using a genetic algorithm (GA) for finding the best combination of corrective actions and MATPOWER as power system equation solver. According to the objective function defined in (1), the GA implements an iterative search aiming minimize the costs for each system state change from u_0 to u_k due to the kth contingency:

$$\min_{u_0 \to u_k} \{f(u_k) + z(u_k)\} \tag{1}$$

$$z(u_k) = \left(w_{LoL} \times p_{LoL,k} + w_{Vb} \times \Delta V_{b,k} + w_{Vb_{ct},k} \times \Delta V_{b_{ct},k} + w_{P_L,k} \times \frac{P_{L,k}}{P_{L,0}} \right) \tag{2}$$

subject to:

$$g(x_0,\ u_0, y_0) = 0$$

$$h(x_0,\ u_0, y_0) \geq 0$$

$$g(x_k,\ u_k, y_k) = 0$$

$$h(x_k,\ u_k, y_k) \geq 0$$

$$|u_k - u_0| \leq \Delta u^{max}$$

where $f(u_k)$ is the system operating cost, $z(u_k)$, defined in (2), is the performance fitness function for the system state change, $g(x,u)$ represent equality constraints for power flow equations, and $h(x,u)$ includes system inequality constraints for which the details are described explicitly in [36].

2.4.2. Load Shed Selection

In case of generation inadequacy where the existing reserves cannot meet load demand requirements, a load shedding action is employed according to the protection strategy of the power system. The type of load (critical or uncritical) is one of the most common approaches in selection of the first group of loads to be separated from the system. If the power system operator has a bunch of loads to be selected, one of the proper shedding sequence methods is defined according to the load participation matrix [7]. For a pre-defined amount of load separation, those which alleviate branch flows the most are selected for decreasing the stress level of the transmission system. The quantity of the load shed is defined in (3) and (4):

$$\Delta P_{shed} = \alpha_{shed} \times \Delta V_{avg} \tag{3}$$

$$\Delta V_{avg} = \frac{1}{\tau} \int_{t_0}^{t_k} (V(t_k) - V(t_0))dt \tag{4}$$

where α_{shed} is the empirical factor relating the amount of load to be shed to the average voltage drop for the time frame of state change.

2.5. Knowledge Base and DT Rules Generation

2.5.1. Creation of Knowledge Base

With the help of the developed n-K contingency case generator tool given in Figure 3 and according to topological and pre-defined environmental configuration, datasets can be created by load scaling iterations for representing several variations in loadings for any IEEE test system whose data is available in MATPOWER. For each scenario the performance indices are calculated, and the convergence result of load-flow is defined as output flag (0/1) to be used in the DT analysis tool.

2.5.2. Decision Tree Formation

For the creation of the learning dataset to be used as a base input for DT, the performance indices defined in Table 1 were calculated for base (no contingency), N-1, and N-2 contingency cases under ±20% load changes for a 100-case per system configuration, which creates 108,200 cases for the IEEE-39 bus network available in MATPOWER 7.1 [37]. In order to create the optimal DT for security evaluation, the MATLAB statistical and machine learning toolbox was used. The obtained DT for each studied case is given in Figure 4 and the DT rules defining the security boundaries are presented in Table 2, respectively:

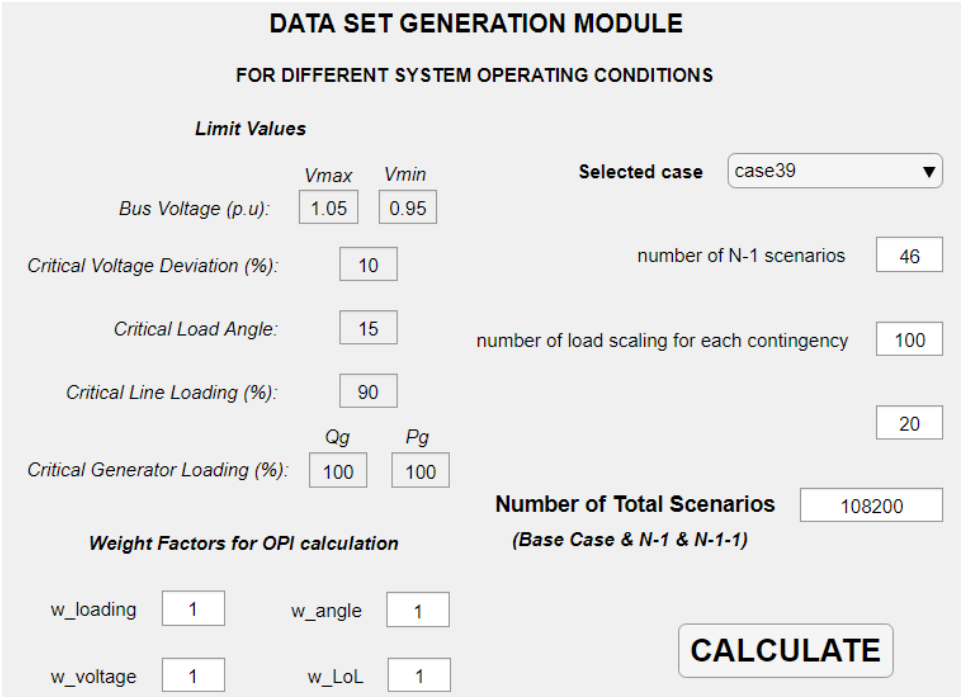

Figure 3. Dataset generation module developed in MATLAB-GUI.

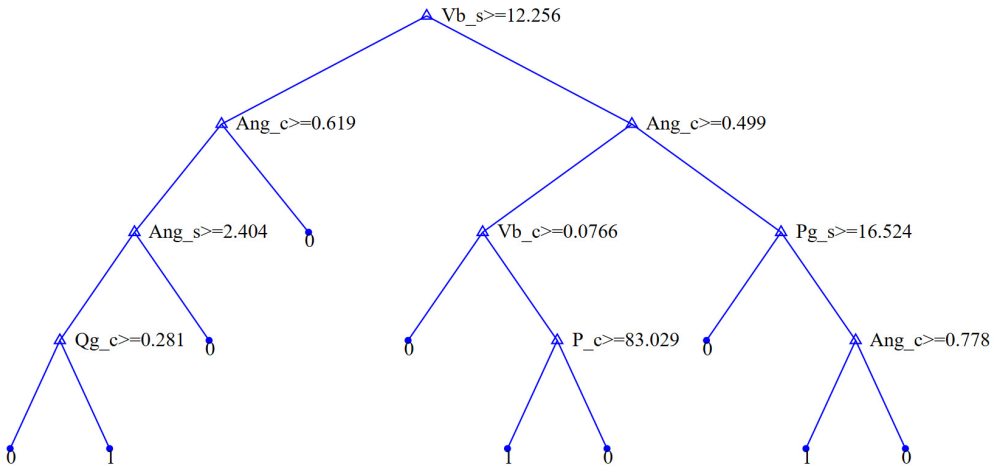

Figure 4. Classification tree for IEEE-39 security boundary definition (0: fail, 1: success).

2.6. Secure State Transfer Cost Calculation

For each selected contingency, the RLS module computes the proposed values for the generators, and if necessary, the loads to be shed. Defining the initial generator active power values as $P_{g,i}$, the proposed values are denoted as $P'_{g,i}$. The generic generation cost function given in (5) is as follows:

$$C_{gen} = a * P^2{}_{g,i} + b * P_{g,i} + c; \quad (5)$$

For which the relevant coefficients are defined in the MATPOWER case data file (i.e.; a = 0.01, b = 40, c = 0). The cost of the secure system transfer (C_{SST}) is defined as (6):

$$C_{SST} = C_{gen} * \sum_i^{n_g} Pg_i + C_{up} * \sum_i^{n_g} \Delta_{up} Pg_i + C_{down} * \sum_i^{n_g} \Delta_{down} Pg_i + C_{shed} * \sum P_{shed} \quad (6)$$

where C_{gen} is the base generation cost/MWh, C_{up} is the ramp-up cost/MWh, C_{down} is the ramp-down cost/MWh, and C_{shed} is the load shed penalty cost/MWh. The cost coefficients

were determined heuristically according to the generic market costs available in [38], which can be modified via the developed GUI of the CSC-OPF module as given in Figure 5. Operational unit costs are defined as multiples of the standard production cost (SPC) which is atually the average hourly production cost defined in terms of $/MWh.

Table 2. DT rules defining security boundary for IEEE-39.

Order	Rules	Result
1	Vb_s < 12.256 and Ang_c ≥ 0.619	INSECURE
2	Vb_s < 12.256 and Ang_c < 0.619 and Ang_s ≥ 2.404	INSECURE
3	Vb_s < 12.256 and Ang_c < 0.619 and Ang_s < 2.4 and Qg_c < 0.281	INSECURE
4	Vb_s < 12.256 and Ang_c < 0.619 and Ang_s < 2.4 and Qg_c ≥ 0.281	SECURE
5	Vb_s ≥ 12.256 and Ang_c < 0.499 and Vb_c < 0.0766	INSECURE
6	Vb_s ≥ 12.256 and Ang_c < 0.499 and Vb_c > 0.076 and P_c < 83.029	SECURE
7	Vb_s ≥ 12.256 and Ang_c < 0.499 and Vb_c > 0.076 and P_c > 83.029	INSECURE
8	Vb_s ≥ 12.256 and Ang_c > 0.499 and Pg_s < 16.524	INSECURE
9	Vb_s ≥ 12.256 and Ang_c > 0.499 and Pg_s ≥ 16.524 and Ang_c < 0.778	SECURE
10	Vb_s ≥ 12.256 and Ang_c > 0.499 and Pg_s ≥ 16.524 and Ang_c ≥ 0.778	INSECURE

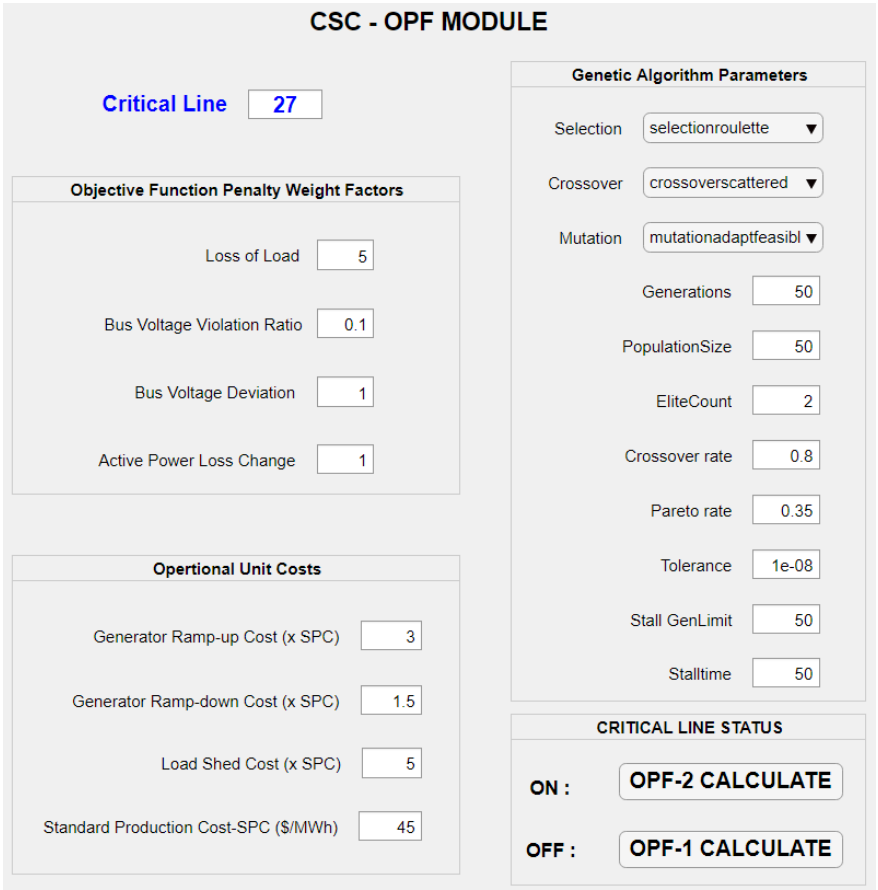

Figure 5. CSC-OPF module GUI.

3. Simulation and Results

The proposed analysis approach was tested on an IEEE-39 bus test network [11] for which implemented analysis tool developed in MATLAB. The system performance indices for IEEE-39 were calculated as given in Figure 6, in which OPI indicates operational performance impact indices, TAI indicates terrorist attack impact indices, AWI indicates the adverse weather impact indices, and TVI represents total vulnerability indices of the respective line outage obtained via fuzzy inference evaluation of three initially calculated indices for which the formulations are already defined in [34]. According to these rankings, the TSO analyst can choose the best-fitting vulnerability scenario that they would like to analyze depending on the specific vulnerability type. If they have no specific vulnerability interest they can choose the traditional analysis type, which is OPI-based analysis, or can choose all vulnerabilities included in a broader and possibilistic sense, which is TVI-based analysis.

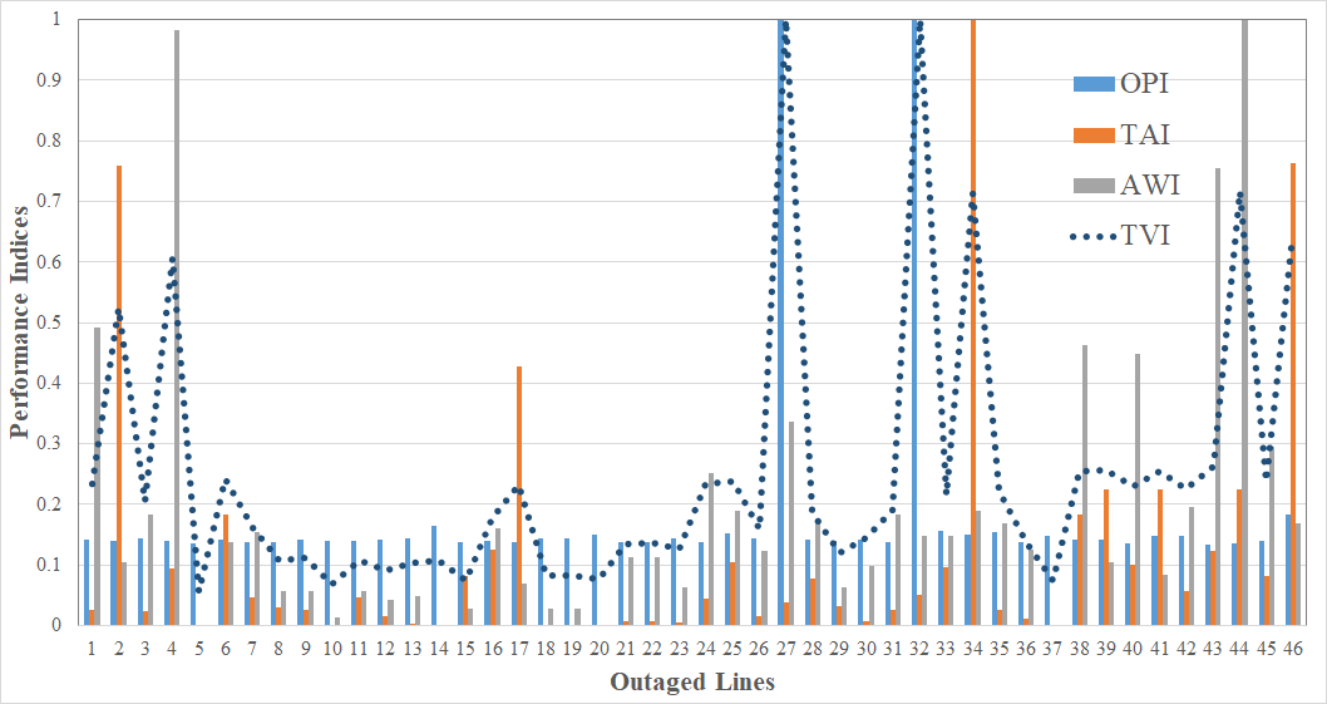

Figure 6. Performance indices distribution for IEEE-39 test network.

From the performance indices ranking, the total vulnerability ranking of 10 of the most critical lines is obtained. The contingency evaluation results for the IEEE-39 bus test system is obtained from the decision support module. The user interface is given in Figure 7 and the summary of the results is given in Table 3. This module enables the user to monitor two consecutive line outage contingencies at the same time.

3.1. Contingency Ranking and Stability Evaluation

In order to analyze higher N-k, where $k \geq 3$ the user can define these contingencies in the base case scenario definition, i.e., for analyzing k = 5, the base case conditions should be set to N-3 system conditions.

For the IEEE-39 test network, the selected operational performance indices-based contingencies, the obtained important PIs, and the loss of load (LoL) variations are given in Figure 8. It is observed that the IEEE-39 bus test system stability deteriorates after the N-4 contingency level. At this point, the specific contingency case must be benchmarked in a time domain analysis software to validate the critical contingency detection approach.

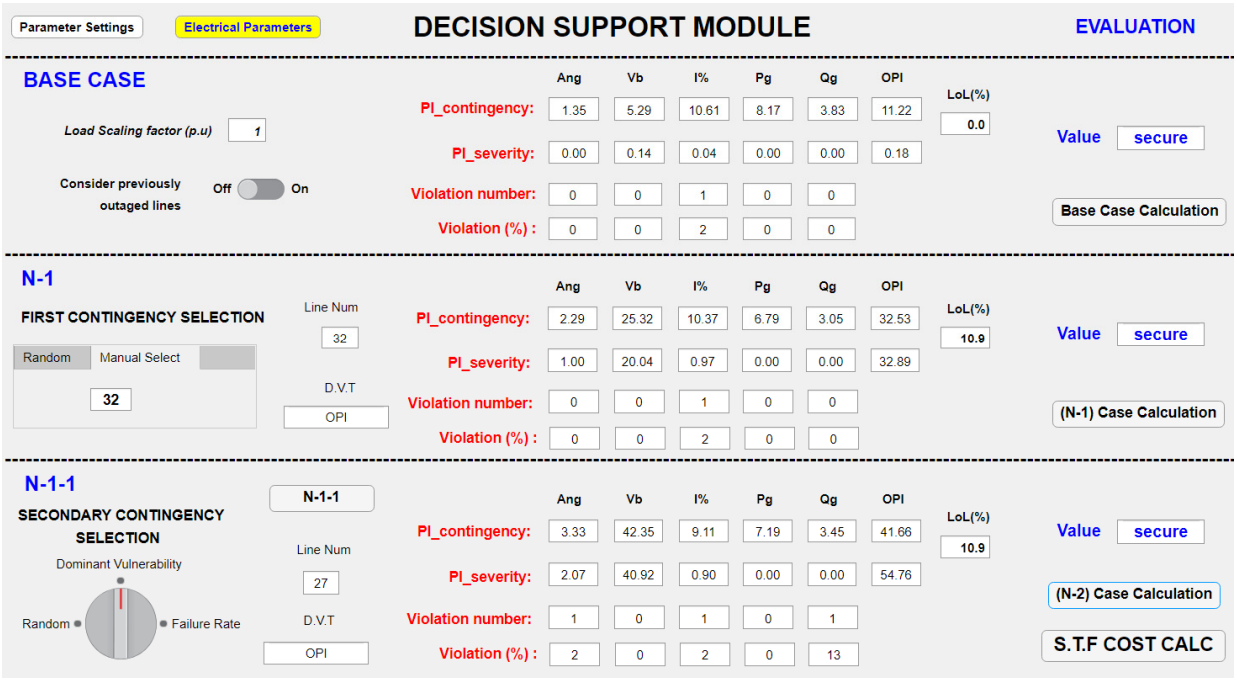

Figure 7. Decision support module GUI.

Table 3. Worst contingencies for IEEE-39 based on TVI ranking.

Order	Line ID	From–to Bus	DT Evaluation	Vulnerability Type	Isolated Bus Number
1	27	16–19	Insecure	OPI	4
2	32	19–20	Insecure	OPI	2
3	44	26–29	Secure	TAI	-
4	34	20–34	Insecure	TAI	1
5	46	28–29	Insecure	OPI	-
6	4	2–25	Insecure	AWI	-
7	2	1–39	Secure	TAI	-
8	43	26–28	Secure	AWI	-
9	39	23–36	Insecure	TAI	1
10	38	23–24	Secure	TAI	-

The foreseen cascading failure sequence was modeled in EMTP software [39] to obtain the dynamic behavior of the system based on generator active power outputs and rotational speeds. The connectivity diagram of the test model created within the developed interface with the most critical contingencies indicated in accordance with the dominant vulnerability types (OPI, AWI, TAI), as shown in Figure 9. For simulating the component outages, disconnectors are added to the relevant branches.

In order to simulate the consecutive cascading failure behavior, each component outage is assumed to occur at each 200 ms, respectively. The simulated behavior for the transient system model is modeled in an EMTP environment. Throughout the simulation, the active power output of the generators is given in Figure 10 and the rotational speed variation of the generators are presented in Figure 11.

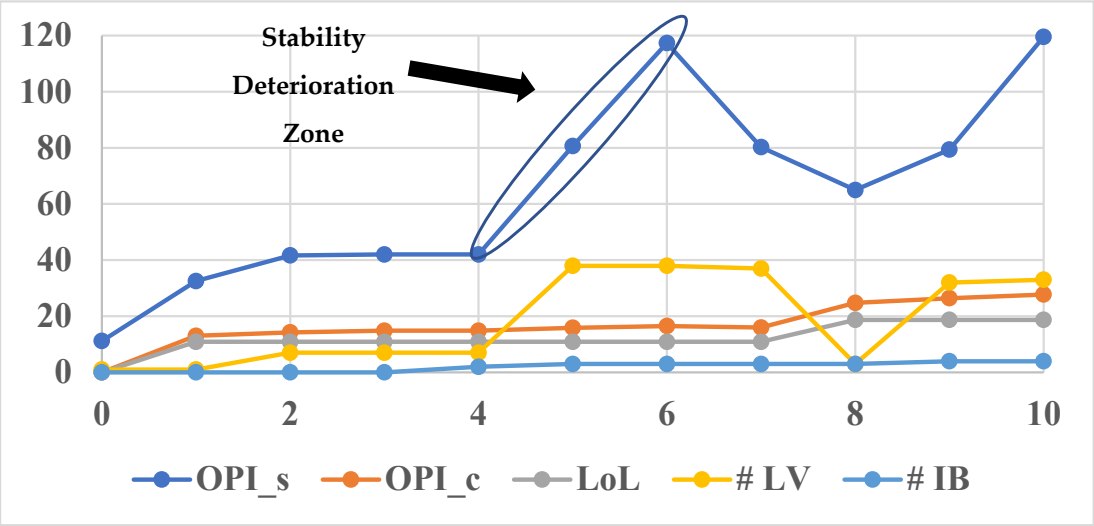

Figure 8. Performance indicators with respect to N-k contingencies (k = 1 to 10).

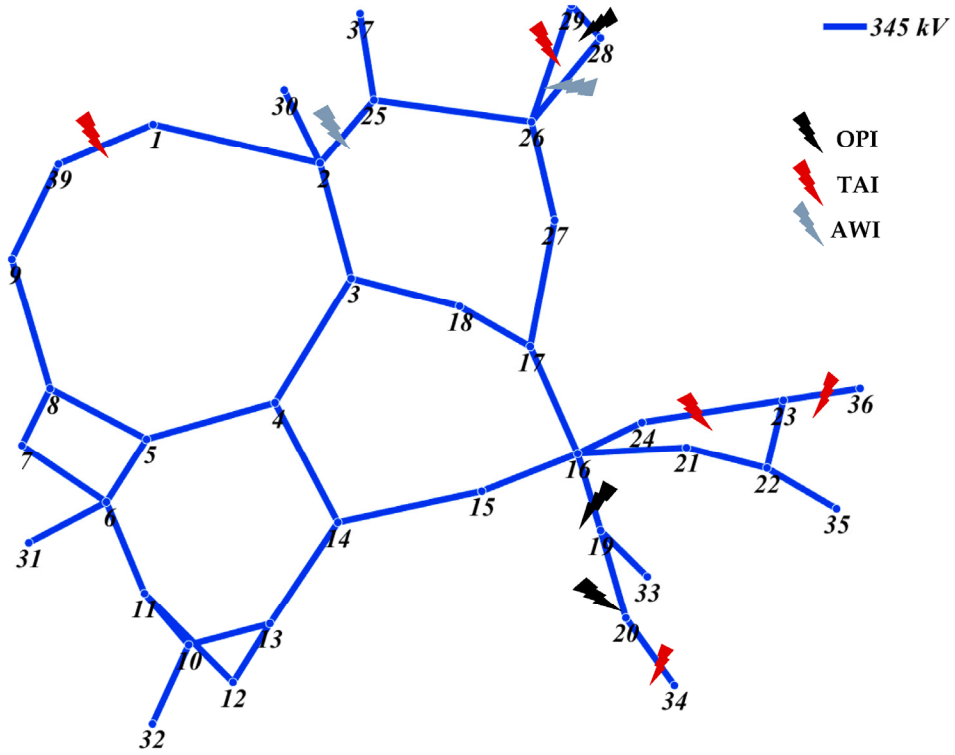

Figure 9. IEEE-39 bus system connectivity diagram indicating most vulnerable points according to OPI, AWI, and TAI indices.

As can be seen in Figure 9, the system stability starts to substantially deteriorate after the fourth (N-4) contingency, which corresponds to the 0.8 to 1.2 s interval zone shown in Figures 10 and 11. It is seen that after the sixth contingency, the severity related operational performance (OPI_s) and the number of limit violation indices (#LV) begin to change substantially. We can also observe slight changes in similar critical performance indicators, such as the related contingency operational performance (OPI_c), loss of load (LoL), and the number of isolated buses (#IB). It can be concluded that although the proposed algorithm is based on a steady state analysis tool where operational scenarios are defined in accordance with several N-k contingencies and load variations, by coupling it with decision tree

evaluation using performance indices as predictive parameters, the proposed algorithm predicts good results for the detection of instability. It is also worth noting that the critical point where the generator angles start to deviate from original values (around t = 1.2 s), as seen in Figure 11, coincides with the N-6 contingency case shown in Figure 9 where deterioration of stability is clear.

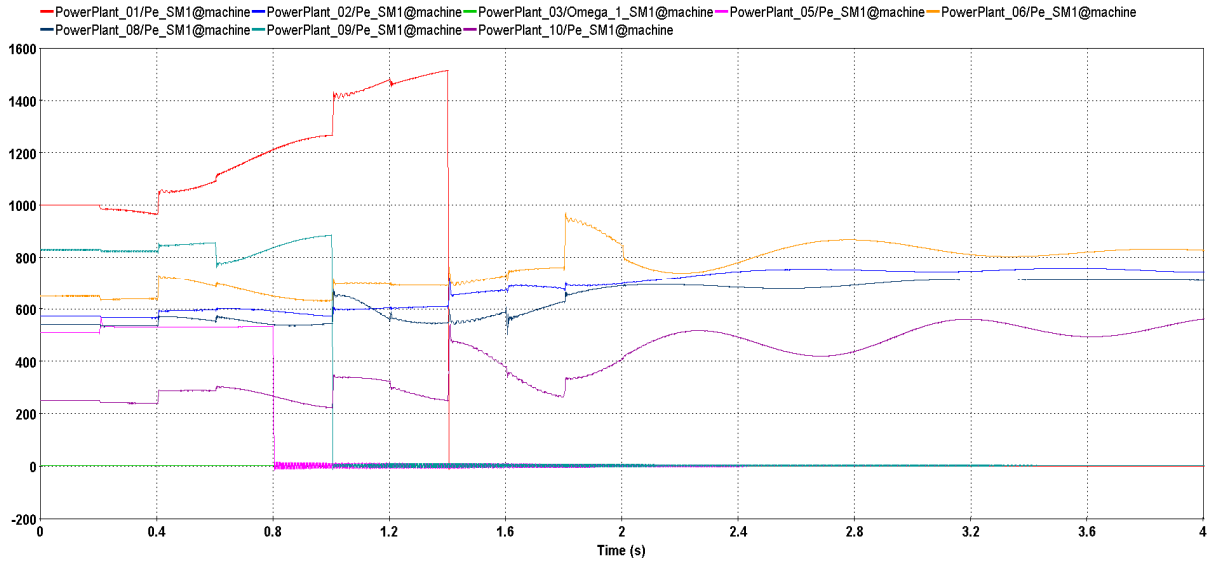

Figure 10. Active power variation of generators during foreseen cascaded failures.

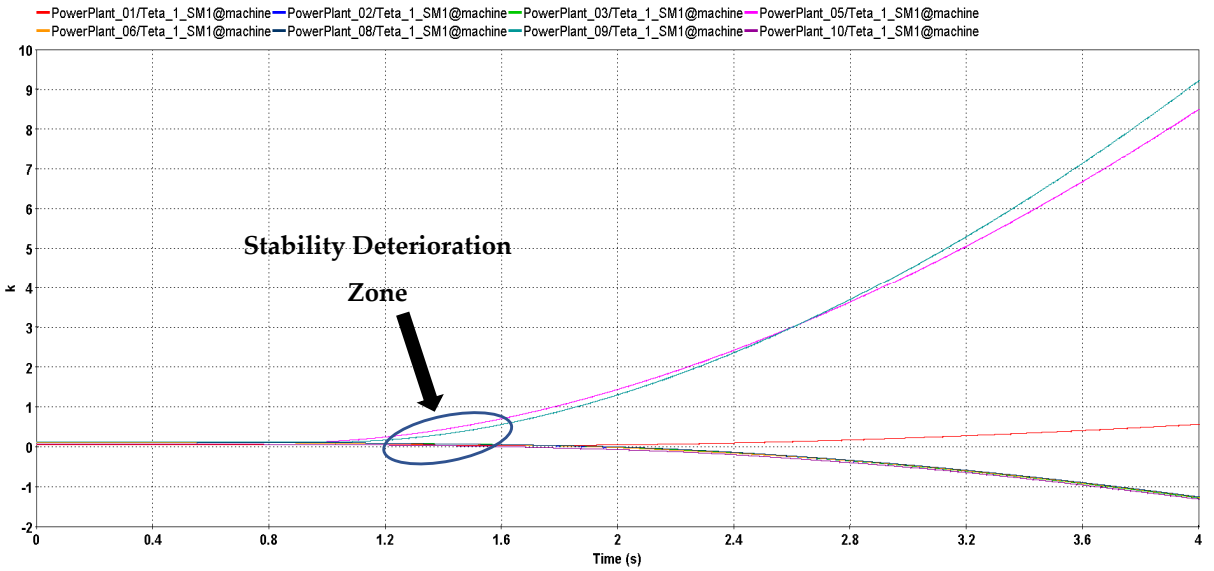

Figure 11. Generator rotational speed deviations during cascading failure.

3.2. Secure System State Transfer

For the N-k contingency analysis implemented according to the total vulnerability ranking, it was found that six contingencies resulted in an insecure state, and four of those also resulted in a bus isolated from the system. The line loadings and bus voltage deviations, being the most vulnerable cases, create a basis for improved constraints for the CSC-OPF problem. The genetic algorithm search aims to minimize the fitness objective applied to solve this corrective security-constrained OPF problem function, defined in Equation (1). Generator active power outputs are considered as main variables for optimization, which are represented as real numbers in the search space but are limited by the minimum and maximum limits of generators' active power. For candidate selection, the roulette

selection type was used and scattered crossover and adaptive mutation were applied to the candidates that formed the search space. The GA performance is very dependent on the predefined crossover (P_c) and mutation (P_m) probabilities. The GA performance for various crossover and mutation probabilities was tested for P_c = 0.6 to 0.9 and P_m = 0.001 to 0.01 and the ideal results, which have a faster convergence behavior, were obtained for the following algorithm parameters; N_{gen}: 50, N_{size}: 50, P_c: 0.8, and P_m: 0.01. As the system size is relatively small, it is observed that the proposed GA fitness function (defined in Equation (1)) reaches an almost optimum solution after the 30th generation. The mean and best possible solution candidates reached the same fitness value, as it can be seen from Figure 12.

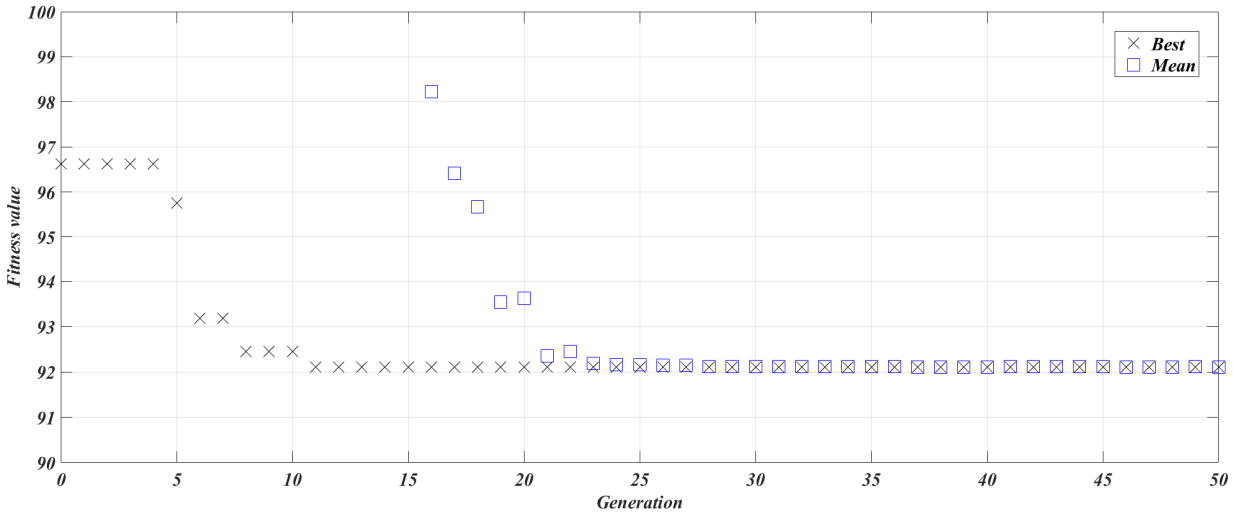

Figure 12. Convergence of VB-OPF algorithm for IEEE-39 bus test system.

As a numeric example, after the N-k contingency is selected, which includes outage of most vulnerable line (line-27/connecting buses 16 and 19), the CSC-OPF module calculates the new settings for generators as given in Table 4.

Table 4. New operational set points for generators after most credible contingency.

Gen-ID	P_{set}	P_{init}	P_{min}	P_{max}
1	667.48	250	0	1040
2	414.06	677.87	0	646
3	375.82	650	0	725
4	594.78	632	0	652
5	655.75	650	0	687
6	400.3	560	0	580
7	285.46	540	0	564
8	653.54	830	0	865
9	1040.9	1000	0	1100

Accordingly, the cost comparison of the systems when secure system transfer conditions are applied or not is shown in Figure 13. It is observed that by transferring the system to the proposed secure operating point using the CSC-OPF algorithm, although generation costs are slightly increased by avoiding the unserved energy (load shed) cost, the overall system operational cost is decreased by 20.4% for this specific contingency case.

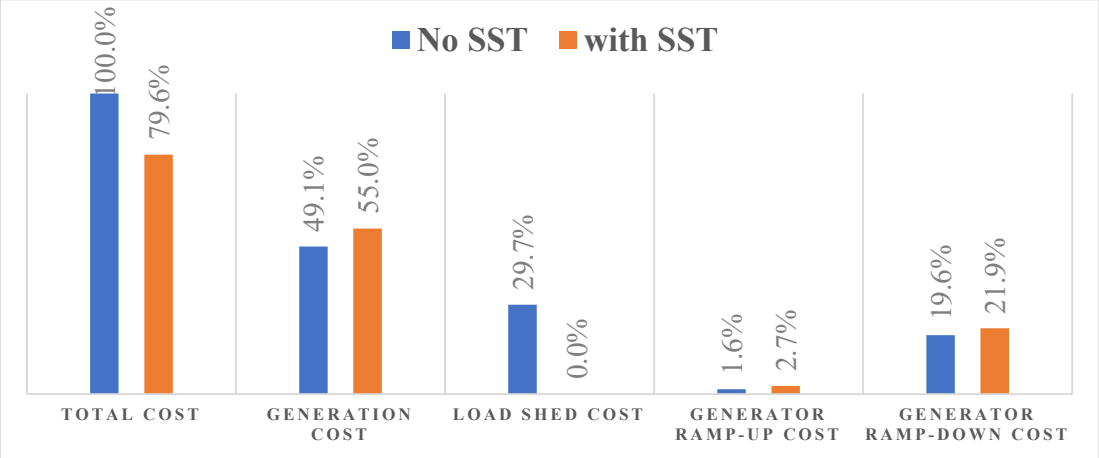

Figure 13. Cost comparison of SST operation with base (not applied) case in IEEE-39 network for the applied contingency scenario.

4. Results and Conclusions

In this study, a new preventive control approach is presented which implements critical contingency selection using a practical vulnerability search analysis and a decision tree-based stability evaluation module with a multi-variant parameter knowledge base. Using non-operational vulnerability indices, the proposed decision support system is expected to assist PSOs in making critical decisions for transferring the power system configuration to be resilient against the possible and probable contingencies which may lead to cascaded failures. By using the proposed methodology, the cascading failure withstand level of the system is expected to improve by transferring the system to a more secure operating point. In this study, it is also shown that although generator operational costs are slightly increased, the unserved energy costs due to load shedding can be alleviated, and as a result, more than 20% of the total system operation cost can be reduced in the specific contingency case. Furthermore, the validity of the stability deterioration detection approach was shown with the benchmark made using a commercial PSA software tool. Using this approach, we proposed a method that anticipates system stability during consecutive failures using the results obtained from steady state AC-OPF analysis, combined with decision trees, using presented performance indices iteratively. By implementing the proposed approach, users can understand several equipment outage scenarios based on vulnerability rankings, visualize the impacts of resulting outages, and estimate the operational cost of systems where a secure system transfer is considered or not.

The main contributions of this paper are as follows: (1) it introduces an approach for critical contingency selection considering operational and non-operational vulnerabilities jointly; (2) it studies a decision tree-based power system stability evaluation with a multi-parameter knowledge base where a corrective security-constrained and genetic algorithm-based OPF algorithm is used; and (3) it provides a contingency evaluation tool for system operators to quantify the impacts due to specific component outages arising from several vulnerabilities.

With the help of such knowledge-based decision support tools providing direct consolidated information from internal and external vulnerabilities, the load dispatch center's resilience capability is expected to be improved and PSOs will be capable of testing their disaster scenarios and understand the impacts of possible corrective maneuvers beforehand. In future work, the proposed algorithm will be tested on a more realistic network model with daily and seasonal load variations imposed.

Author Contributions: Methodology, E.A. and M.B.; Software, E.A.; Validation, E.A.; Investigation, E.A. and M.B.; Data curation, E.A.; Writing – original draft, E.A.; Writing – review & editing, M.B.; Supervision, M.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: No new data were created.

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

Nomenclature

Indices	
l	line index
i	bus index
g	generator index
Constants	
n_{line}	total number of lines
n_{bus}	total number of buses
n_{gen}	total number of generators
N	formulation parameter (i.e., 2)
w_P	overloading weight factor
w_b	bus voltage weight factor
w_g	generator active/reactive power weight factor
w_{ang}	angle weight factor weight factor
w_{Vb}	bus voltage deviation weight factor
$\boldsymbol{w_{LoL}}$	loss of load weight factor
$\boldsymbol{w_{LoG}}$	loss of generation weight factor
$w_{Vb,ct}$	bus voltage violation weight factor
w_{PLoss}	active power loss change weight factor
$P_{l\text{-}max}$	max active power of lth line
$P_{g,max}$	max. active power of ith generator
$Q_{g,max}$	max. reactive power of ith generator
ΔP_{shed}	amount of load shed
Variables	
P_l	active power of lth line
V_i	voltage level of ith bus
V_{bc}	base case voltage of ith bus
V_{min}	minimum voltage of ith bus
V_{max}	maximum voltage of ith bus
Q_g	reactive power of ith generator
P_g	active power of ith generator
ΔV_b	total bus voltage deviation in p.u
$\Delta V_{b\text{-}ct}$	number of bus voltage limit violation
isl_{bus}	total islanded bus number
$P_{L,0}$	base case power loss
$P_{L;k}$	k^{th} contingency case power loss
PI_P	active power performance index
PI_V	voltage performance index
PI_{Pg}	generator active power performance index
PI_{Qg}	generator reactive power performance index
PI_{Ang}	load angle performance index
PI_{LoL}	percentage of load shed p. index
PI_{LoG}	percentage of lost generation p. index
PI_{IB}	isolated bus number performance index
OPI_{ctg}	contingency based operational p.index
OPI_{sev}	severity based operational p.index
ΔV_{avg}	average voltage drop

References

1. Andersson, G.; Donalek, P.; Farmer, R.; Hatziargyriou, N.; Kamwa, I.; Kundur, P.; Martins, N.; Paserba, J.; Pourbeik, P.; Sanchez-Gasca, J.; et al. Causes of the 2003 major grid blackouts in North America and Europe, and recommended means to improve system dynamic performance. *IEEE Trans. Power Syst.* **2005**, *20*, 1922–1928. [CrossRef]
2. Gao, B.; Shi, L. Modeling an Attack-Mitigation Dynamic Game-Theoretic Scheme for Security Vulnerability Analysis in a Cyber-Physical Power System. *IEEE Access* **2020**, *8*, 30322–30331. [CrossRef]
3. Mohammadi, F.; Rashidzadeh, R. Impact of stealthy false data injection attacks on power flow of power transmission lines-A mathematical verification. *Int. J. Electr. Power Energy Syst.* **2022**, *142*, 108293. [CrossRef]
4. Abedi, A.; Gaudard, L.; Romerio, F. Power flow-based approaches to assess vulnerability, reliability, and contingency of the power systems: The benefits and limitations. *Reliab. Eng. Syst. Saf.* **2020**, *201*, 106961. [CrossRef]
5. Sperstad, I.B.; Kjølle, G.H.; Gjerde, O. A comprehensive framework for vulnerability analysis of extraordinary events in power systems. *Reliab. Eng. Syst. Saf.* **2020**, *196*, 106788. [CrossRef]
6. Mohammadi, F. Emerging Challenges in Smart Grid Cybersecurity Enhancement: A Review. *Energies* **2021**, *14*, 1380. [CrossRef]
7. Donde, V.; López, V.; Lesieutre, B.; Pinar, A.; Yang, C.; Meza, J. Severe multiple contingency screening in electric power systems. *IEEE Trans. Power Syst.* **2008**, *23*, 406–417. [CrossRef]
8. Rocco, C.M.; Ramirez-Marquez, J.E.; Salazar, D.E.; Yajure, C. Assessing the vulnerability of a power system through a multiple objective contingency screening approach. *IEEE Trans. Reliab.* **2011**, *60*, 394–403. [CrossRef]
9. Sadeghian, O.; Mohammadi-Ivatloo, B.; Mohammadi, F.; Abdul-Malek, Z. Protecting Power Transmission Systems against Intelligent Physical Attacks: A Critical Systematic Review. *Sustainability* **2022**, *14*, 12345. [CrossRef]
10. Tan, S.; Guerrero, J.M.; Xie, P.; Han, R.; Vasquez, J.C. Brief Survey on Attack Detection Methods for Cyber-Physical Systems. *IEEE Syst. J.* **2020**, *14*, 5329–5339. [CrossRef]
11. Nezamoddini, N.; Mousavian, S.; Erol-Kantarci, M. A risk optimization model for enhanced power grid resilience against physical attacks. *Electr. Power Syst. Res.* **2017**, *143*, 329–338. [CrossRef]
12. Li, Z.; Shahidehpour, M.; Alabdulwahab, A.; Abusorrah, A. Analyzing Locally Coordinated Cyber-Physical Attacks for Undetectable Line Outages. *IEEE Trans. Smart Grid* **2018**, *9*, 35–47. [CrossRef]
13. Bi, W.; Zhang, K.; Li, Y.; Yuan, K.; Wang, Y. Detection Scheme Against Cyber-Physical Attacks on Load Frequency Control Based on Dynamic Characteristics Analysis. *IEEE Syst. J.* **2019**, *13*, 2859–2868. [CrossRef]
14. Abedi, A.; Gaudard, L.; Romerio, F. Review of major approaches to analyze vulnerability in power system. *Reliab. Eng. Syst. Saf.* **2019**, *183*, 153–172. [CrossRef]
15. 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]
16. Fu, J.; Wang, L.; Hu, B.; Xie, K.; Chao, H.; Zhou, P. A Sequential Coordinated Attack Model for Cyber-Physical System Considering Cascading Failure and Load Redistribution. In Proceedings of the 2018 2nd IEEE Conference on Energy Internet and Energy System Integration (EI2), Beijing, China, 20–22 October 2018; pp. 1–6. [CrossRef]
17. Arroyo, J.M.; Fernández, F.J. Application of a genetic algorithm to n-K power system security assessment. *Int. J. Electr. Power Energy Syst.* **2013**, *49*, 114–121. [CrossRef]
18. Stott, B.; Jardim, J.; Alsac, O. DC power flow revisited. *IEEE Trans. Power Syst.* **2009**, *24*, 1290–1300. [CrossRef]
19. Liu, X.; Li, Z. Revealing the Impact of Multiple Solutions in DCOPF on the Risk Assessment of Line Cascading Failure in OPA Model. *IEEE Trans. Power Syst.* **2016**, *31*, 4159–4160. [CrossRef]
20. Yan, J.; Tang, Y.; He, H.; Sun, Y. Cascading Failure Analysis with DC Power Flow Model and Transient Stability Analysis. *IEEE Trans. Power Syst.* **2015**, *30*, 285–297. [CrossRef]
21. He, H.; Huang, S.; Liu, Y.; Zhang, T. A tri-level optimization model for power grid defense with the consideration of post-allocated DGs against coordinated cyber-physical attacks. *Int. J. Electr. Power Energy Syst.* **2021**, *130*, 106903. [CrossRef]
22. Rios, M.; Kirschen, D.; Jayaweera, D.; Nedic, D.; Allan, R. Value of security: Modeling time-dependent phenomena and weather conditions. *IEEE Trans. Power Syst.* **2002**, *17*, 543–548. [CrossRef]
23. Aliyana, E.; Aghamohammadia, M.; Kiab, M.; Heidaric, A.; Shafie-khahd, M.; Catalão, J.P.S. Decision tree analysis to identify harmful contingencies and estimate blackout indices for predicting system vulnerability. *Electr. Power Syst. Res.* **2020**, *178*, 106036. [CrossRef]
24. Liao, W.; Salinas, S.; Li, M.; Li, P.; Loparo, K.A. Cascading Failure Attacks in the Power System: A Stochastic Game Perspective. *IEEE Internet Things J.* **2017**, *4*, 2247–2259. [CrossRef]
25. Diao, R.; Vittal, V.; Sun, K.; Kolluri, S.; Mandal, S.; Galvan, F. Decision tree assisted controlled islanding for preventing cascading events. In Proceedings of the 2009 IEEE/PES Power Systems Conference and Exposition, Seattle, WA, USA, 15–18 March 2009; pp. 1–8. [CrossRef]
26. Zio, E.; Golea, L.R.; Rocco, S.C.M. Identifying groups of critical edges in a realistic electrical network by multi-objective genetic algorithms. *Reliab. Eng. Syst. Saf.* **2012**, *99*, 172–177. [CrossRef]
27. Cuadra, L.; Salcedo-Sanz, S.; Del Ser, J.; Jiménez-Fernández, S.; Geem, Z.W. A Critical Review of Robustness in Power Grids Using Complex Networks Concepts. *Energies* **2015**, *8*, 9211–9265. [CrossRef]

28. Henneaux, P.; Ciapessoni, E.; Cirio, D.; Cotilla-Sanchez, E.; Diao, R.; Dobson, I.; Gaikwad, A.; Miller, S.; Papic, M.; Pitto, A.; et al. Benchmarking quasi-steady state cascading outage analysis methodologies. In Proceedings of the 2018 IEEE International Conference on Probabilistic Methods Applied to Power Systems (PMAPS), Boise, ID, USA, 24–28 June 2018. [CrossRef]
29. Zeraati, M.; Aref, Z.; Latify, M.A. Vulnerability Analysis of Power Systems Under Physical Deliberate Attacks Considering Geographic-Cyber Interdependence of the Power System and Communication Network. *IEEE Syst. J.* **2018**, *12*, 3181–3190. [CrossRef]
30. Yan, J.; He, H.; Zhong, X.; Tang, Y. Q-Learning-Based Vulnerability Analysis of Smart Grid Against Sequential Topology Attacks. *IEEE Trans. Inf. Forensics Secur.* **2017**, *12*, 200–210. [CrossRef]
31. Rocchetta, R. Enhancing the resilience of critical infrastructures: Statistical analysis of power grid spectral clustering and post-contingency vulnerability metrics. *Renew. Sustain. Energy Rev.* **2022**, *159*, 112185. [CrossRef]
32. Du, H.; Lin, T.; Li, Q.; Fu, X.; Xu, X.; Cheng, J. Transmission expansion planning for power grids considering resilience enhancement. *Electr. Power Syst. Res.* **2022**, *211*, 108218. [CrossRef]
33. Breiman, L.; Friedman, J.; Olshen, R.A.; Stone, C.J. *Classification and Regression Trees*; Wadsworth: Belmont, CA, USA, 1984.
34. Akdeniz, E.; Bagriyanik, M. A knowledge based decision support algorithm for power transmission system vulnerability impact reduction. *Int. J. Electr. Power Energy Syst.* **2016**, *78*, 436–444. [CrossRef]
35. The MathWorks Inc. (2021a). Statistics and Machine Learning Toolbox Documentation, Natick, Massachusetts: The MathWorks Inc. Available online: https://www.mathworks.com/help/stats/index.html (accessed on 11 April 2023).
36. Zhu, J. *Optimization of Power System Operation*; IEEE Press Series on Power Engineering; John Wiley & Sons: Hoboken, NJ, USA, 2015.
37. Zimmerman, R.D.; Murillo-Sánchez, C.E.; Thomas, R.J. MATPOWER: Steady-State Operations, Planning, and Analysis Tools for Power Systems Research and Education. *IEEE Trans. Power Syst.* **2011**, *26*, 12–19. [CrossRef]
38. EPİAŞ Transparency Platform for Electricity Markets. Available online: https://seffaflik.epias.com.tr/transparency/piyasalar/gop/ptf.xhtml (accessed on 17 May 2021).
39. Electromagnetic Transients Program (EMTP®). Available online: https://www.emtp.com/ (accessed on 11 April 2023).