Power System Variables Selection in Static security Assessment for Binary-Class Support Vector Machine

Jignesh Borisagar
Gujarat Power Research and Development Cell,
Urja Vikas Nigam Limited,
Gandhinagar, India
jigneshborisagar05@gmail.com

Astik Dhandhia
Electrical Department,
Shantilal Shah Engineering College,
Bhavnagar, India
astikdhandhia@gmail.com

2024 29th International Conference on Automation and Computing (ICAC) | 979-8-3503-6088-2/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICAC61394.2024.10718805

***Abstract*— ensuring the accurate determination of operational decisions in current power system scenarios is paramount for guaranteeing power system reliability and security. Traditional power flow methods suffer from substantial drawbacks, including high memory demands and prolonged computation times, rendering them unsuitable for real-time static security assessments. As a result, alternative approaches are necessary to address these limitations and enable effective real-time monitoring and decision-making in power systems. Furthermore, the composite security index has been developed specifically to mitigate the masking issues inherent in performance indices that rely on line loadings and bus voltage deviations for security assessment. This enhancement grants the composite security index a heightened capability to differentiate between contingency cases characterized by closer violations. Consequently, the masking problem typically associated with traditional performance indices is effectively eliminated. Support Vector Machines (SVMs) are employed to tackle the binary-class classification problem in power system static security. The performance of the binary-class SVM classifier is contingent upon the selection of various power system variables, with optimal choices significantly enhancing classifier effectiveness. Sequential Forward Selection (SFS) is utilized to achieve optimal feature selection and minimize misclassification rates. Validation of this methodology is conducted using two IEEE standard test systems to validate its robustness and applicability.**

Keywords*— *Static Security Assessment, Artificial Intelligence, Feature Selection, Composite Security Index, Support Vector Machine

I. INTRODUCTION

The power system consists of three primary components: distribution, transmission, and generation. It is essential to ensure that consumers have a steady and adequate supply of electricity during the power system's operation. The deregulation of the electrical grid has heightened the importance of maintaining continuous power. Power system security refers to the system's ability to withstand critical contingencies without causing power outages for consumers [1]. A system achieves secure state when it operates within its acceptable range under normal and emergency conditions. Evaluating a system's steady-state behavior involves solving a series of algebraic equations, known as steady-state security assessment. This article specifically addresses static security assessments, focusing on three key components: power system control to ensure secure operation, contingency analysis, and power system monitoring [2]. Contingency analysis is the most challenging of these three components because it involves a series of time-consuming simulations. Power flow simulations are utilized in this process to determine the security of the power system. As a result, it may not be feasible for real-time applications in certain situations [3]. Thus, there is a necessity to develop novel and highly effective techniques to ensure the safe operation and control of large-scale power systems. The limitations of traditional approaches to security evaluation can be alleviated by employing pattern recognition (PR) methods. The pattern recognition method facilitates rapid power system security evaluation primarily through offline computation. A classification function is employed to swiftly assess system security; developed using training datasets generated offline. Static security assessment has been tackled using artificial intelligence techniques such as the Radial Basis Function Neural Network [4], Multi-layered feed forward network [5], Self-Organizing Feature Map [6], and Convolutional Neural Network (CNN) [7]-[9]. The effectiveness of the aforementioned approaches heavily relies on the particular problem context and does not encompass predicting future insecure states. Power system security is also addressed through hybrid approaches like Support Vector Regression with Teaching Learning-based Optimization [10] and Support Vector Machine (SVM) with Evolutionary Genetic Algorithm (GA) [11]. The outcomes of the aforementioned approaches largely hinge on the specific problem being addressed and typically do not forecast future insecure states. Therefore, in this context, the classification function is designed using Support Vector Machines (SVM). The Composite Security Index (CSI) incorporates hyper-ellipse concepts within the hyper-box to achieve a lower misclassification rate in security assessments. The masking issue will be addressed by employing the Composite Security Index (CSI). The power system variables used to generate patterns determine the performance of the intended function during both training and testing phases in the pattern recognition approach. Over the past forty years, researchers have utilized different sets of variables—such as bus voltages and angles, active and reactive power loads at buses, active and reactive generation at buses, and power flow in transmission lines—to construct input patterns for designing security functions. Researchers have selected subsets of the aforementioned variables to create patterns. It is crucial to investigate how different sets of variables influence static security assessments in pattern creation. The Sequential Forward Selection approach has been employed to reduce the dimensionality of patterns. Building upon the aforementioned research on static security evaluation of power systems, the following objectives have been defined for this study:

- Creating a composite security index to categorize patterns as either secure or insecure.
- Radial Basis Function (RBF) is applied in binary class support vector machines, while sequential forward selection serves as a method for optimal feature extraction.
- To employ an SVM-based binary class classifier for classifying static security assessment problems into secure and insecure levels using pattern recognition techniques.
- To assess how different power system variables affect the performance of a binary classifier constructed using a support vector machine as a pattern vector

The organization of the remaining sections in the paper is as follows: Section 2 presents the static security assessment utilizing the composite security index, while Section 3 discusses the static security assessment by pattern recognition. Section 4 presents the results and discussions for two IEEE test systems that demonstrate the usefulness of the proposed model for static security assessment, while Section 5 concludes the discussion.

II. Static Security Assessment Utilizing Composite Security Index

Static security pertains to the ability of a system to maintain operational integrity within a predefined region where constraints must not be breached. Moreover, in the rare event of a line or generator failure, any violations of boundaries must be confined within specified limits [2], [12-13]. A contingency is defined as the failure of any generator or transmission line within the power system. During a contingency event, a static security assessment evaluates any significant overloads on transmission lines or violations of bus voltage limits. Subsequently, critical contingencies are ranked and classified by the static security assessment (SSA) in descending order based on their primary adverse impact on system stability. The standard procedure for ranking and classifying contingencies involves calculating the performance index (PI) using load flow solutions. The masking issue significantly affects the approach to classifying and ranking contingencies [2], [14]. In [15], an enhanced methodology for computing the Composite Security Index (CSI) is introduced. This method employs a hyper-ellipse contained within a hyper-box, effectively eliminating the masking problem associated with conventional performance index (PI) calculations.

Formulation of Composite Security Index

The criteria outlined in (1) and (2) must be satisfied for power systems to operate normally.

$$\sum_{x=1}^{N_{Gen}} P_{Gx} = P_{TL} + P_l \tag{1}$$

$$\left.\begin{array}{l} P_{Gx}^{min} \le P_{Gx} \le P_{Gx}^{max}, x = 1,2,\dots,N_{Gen} \\ \left|V_y^{min}\right| \le \left|V_y\right| \le \left|V_y^{max}\right|, y = 1,2,\dots,N_{Bus} \\ P_{kl} \le P_{kl}^{max} \; for \; every \; branch, k-l \end{array}\right\} \tag{2}$$

After any outage, the satisfaction of constraints (1) and (2) verifies the "secure state" of the power system. Conversely, if any of these constraints are violated, the system is considered to be in an "insecure state." When determining the secure and insecure states of bus voltages, violations of both upper and lower limits are considered, whereas only upper limit violations are considered for transmission line loading. The system state is classified as secure or insecure based on the composite security index value, as outlined in the following section.

A. Bus Voltage Security Index

Set V_y^d ,$A_{V,y}^u$, $A_{V,y}^l$, $S_{V,y}^u$ and $S_{V,y}^l$ at bus y. And calculate $a_{(V,y)}^u$, $b_{(V,y)}^u$, $a_{(V,y)}^l$ and $b_{(V,y)}^l$.

$$\left.\begin{array}{l} a_{(v,y)}^u = \left[V_y - A_{V,y}^u\right]/\left(V_y^d\right); if \; V_y > A_{V,y}^u \\ a_{(V,y)}^l = \left[A_{V,y}^l - V_y\right]/\left(V_y^d\right); if \; V_y < A_{V,y}^l; \\ a_{(v,y)}^u = 0; if \; A_{v,y}^l \le V_y \le A_{v,y}^u \\ and \; y = 1,2,\dots,N_{Bus} \end{array}\right\} \tag{3}$$

$$\left.\begin{array}{l} b_{(v,y)}^u = \left[S_{V,y}^u - A_{V,y}^u\right]/\left(V_y^d\right) \\ b_{(V,y)}^l = \left[A_{V,y}^l - S_{V,y}^l\right]/\left(V_y^d\right) \\ and \; y = 1,2,\dots,N_{Bus} \end{array}\right\} \tag{4}$$

Using equations (3) and (4) from the hyper-ellipse formulation in [15], and setting $k = 1.0$, the security index for bus voltage can be expressed as shown in equation (5).

$$PI_{Vt} = \left[\sum_y \left(a_{(V,y)}^u / b_{(V,y)}^u\right)^{2k} + \sum_y \left(a_{(V,y)}^l / b_{(V,y)}^l\right)^{2k}\right]^{1/2k} \tag{5}$$

Classifying the power system state related to bus voltage security using equation (5) is straightforward, and it can be categorized as described in equation (6) below

$$\left.\begin{array}{l} PI_{Vt} = 0; Secure \\ PI_{Vt} \ge 1; Insecure \end{array}\right\} \tag{6}$$

B. Security Index for Transmission Line Power Flow

The line flow security index calculation considers only upper limits due to the focus on maximum limits of line power flow. In (7) and (8), set $A_{MW,z}$, $S_{MW,z}$ through z^{th} line.

$$c_{MW,z} = \left[|MW_z| - A_{MW,z}\right]/Base \; MVA \; if \; |MW_z| > A_{MW,z}$$

$$c_{MW,z} = 0 \; if \; \left|MW_z < A_{MW,z}\right| \; and \; z = 1,2,.,N_{line} \tag{7}$$

$$d_{MW,z} = \left[S_{MW,z} - A_{MW,z}\right]/Base \; MVA, \; z = 1,2,.,N_{line} \tag{8}$$

Calculate $c_{MW,z}$ and $d_{MW,z}$ for the z^{th} line. The power system state is assessed using the Line Power Flow Security Index, which is derived from equations (7) and (8). Its value can be computed using equation (10).

$$PI_{Po} = \left[\sum_z \left(c_{MW,z}/d_{MW,z}\right)\right]^{1/2k} \tag{9}$$

$$\left.\begin{array}{l} PI_{Po} = 0; Secure \\ PI_{Po} \ge 1; Insecure \end{array}\right\} \tag{10}$$

The composite security index, as defined in equation (11), is constructed by combining equations (5) and (9) and applying the hyper-ellipse methodology within the hyper-box framework. Contingency situations can be ranked in descending order based on their CSI values. CSI proves particularly beneficial in addressing masking and violation issues. According to (12), the CSI value can categorize the overall security status of the power system.

$$PI_C = \left[\sum_y \left(a^u_{(V,y)}/b^u_{(V,y)}\right)^{2k} + \sum_y \left(a^l_{(V,y)}/b^l_{(V,y)}\right)^{2k} + \sum_z \left(c_{MW,z}/d_{MW,z}\right)^{2k}\right]^{1/2k} \quad (11)$$

$$\left.\begin{array}{l} PI_C = 0; Secure \\ PI_C \geq 1; Insecure \end{array}\right\} \quad (12)$$

III. Static Security Assessment by Pattern Recognition

The system operator can effectively determine the static security of the system by referring to the two classes—secure and insecure—described here for static security assessment. The pattern recognition (PR) technique used in this approach reduces the burden on online computations since most simulation work is conducted offline. Offline simulations aim to generate a diverse set of operating scenarios, forming the foundation for developing the static security classifier. In online applications, this classifier directly facilitates quicker determination of static security. The data generation and pattern recognition methodology employed in this work for assessing power system static security are detailed in Figure 1.

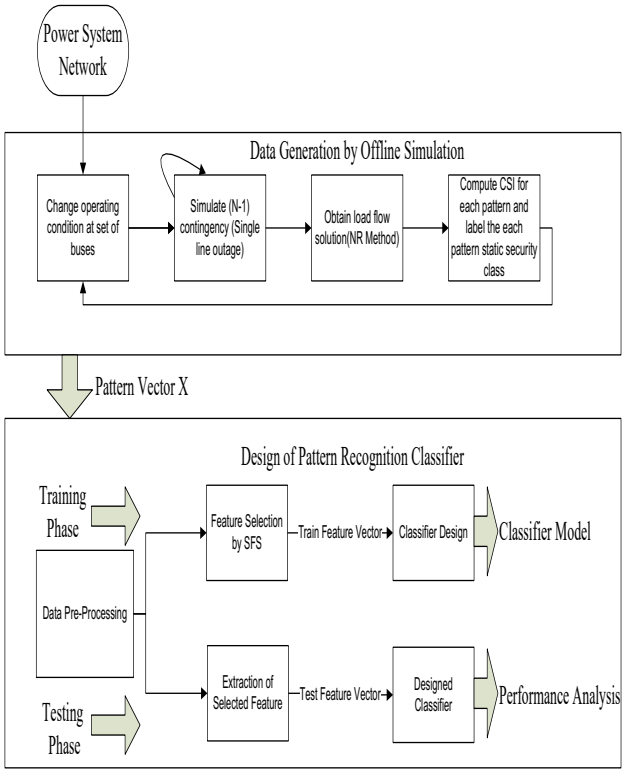

Fig.1 Steps followed in Data generation and PR approach for SSA

A. Generation of Patterns for Assessing the Static Security of Power Systems

Creating a comprehensive training set is often pivotal for ensuring the effectiveness of any pattern recognition approach. The training set should encompass a wide range of power system operating scenarios, including variations in active and reactive power loads at load buses, as well as contingency cases involving transmission lines and generators that could potentially impact the security of the power system. The offline data collected are referred to as "patterns" [16]. The range of load variations for both active and reactive power on these designated bus groups is set between 50% and 150% of their base case loadings. Moreover, the active power generation at generator buses is adjusted accordingly to meet the criteria specified in (1). Static security is significantly influenced by events such as generator or transmission line outages, as well as fluctuations in load. Specifically, each transmission line outage is implemented individually.

Selecting variables that comprehensively capture the characteristics of the power system is crucial. Hence, investigating how different sets of factors impact the power system in the current scenario is necessary. In this study, the influence of different sets of variables on the classifier's performance has been examined. These five sets are detailed in (13–17). Load flow analysis is conducted for each operational scenario, and a pattern is generated based on the values provided in (13–17). The determination of the power system state as secure or insecure will be based on the decision of the CSI, as described in (11).

$$X_1 = \{|V_y|, \delta_y\} \quad (13)$$

$$X_2 = \{|V_y|, \delta_y, Z\} \quad (14)$$

$$X_3 = \{|V_y|, \delta_y, P_{Gy}, Q_{Gy}, P_{Dy}, Q_{Dy}\} \quad (15)$$

$$X_4 = \{|V_y|, \delta_y, P_{Gy}, Q_{Gy}, P_{Dy}, Q_{Dy}, Z\} \quad (16)$$

$$X_5 = \{|V_y|, \delta_y, P_{Gy}, Q_{Gy}, P_{Dy}, Q_{Dy}, P_{kl}, Q_{kl}\} \quad (17)$$

A binary classification problem for static security assessment of a power system using pattern recognition has been introduced. SVM has been effectively employed to develop a binary classifier that categorizes the system into secure and insecure states. The composite security index enables the avoidance of masking issues and facilitates reliable differentiation between secure and insecure scenarios, even in cases where violations of power system limits occur in close proximity. The sequential forward selection technique reduces pattern size while enhancing classification accuracy. Through comparison of a binary classifier's performance using different sets of power system variables as patterns, it was found that including bus voltages, bus angles, and contingency numbers in the binary representation effectively encapsulated information about the power system's static security state.

B. Feature Selection

Each pattern comprises a large number of variables, as detailed in (13–17), which may increase in size relative to the system's scale. Feature selection, aimed at identifying a small subset of variables termed "features" from (13–17), proves beneficial in reducing the dimensionality of the original pattern vector. A set of variables like this is termed a feature vector, denoted as follows: $Y = \{y_1, y_2, .., y_k\}$. The variables in the feature vector are significantly fewer in number compared to those in the pattern vector. There is a possibility of losing some important variables during the process of selecting an optimal subset of features from the larger variable set. This potential loss could impact the accuracy of the classifier and potentially increase the misclassification rate. In this context, the feature selection process employs sequential forward selection (SFS), which

sequentially adds variables to the feature vector while minimizing the objective function. SFS starts with an empty set of features and iteratively adds variables one by one until the objective function ceases to be maximized.

C. Classifier Design using Multiclass Support Vector Machine

Sequential forward selection (SFS) is instrumental in extracting an optimal feature vector Y, which serves as input patterns for classifier construction. The classifier establishes boundaries that distinguish between secure and insecure classes. Unknown test patterns are employed to validate the classifier, developed using training patterns. Various techniques are utilized in classifier design, such as neural networks with backpropagation, K-nearest neighbor (KNN), and least squares [16]. While these techniques are computationally efficient, their lower classification accuracy may render them unsuitable for static security assessments.

Support Vector Machines (SVMs) are advanced learning algorithms that have shown impressive accuracy, particularly in complex systems, for solving classification problems. Let $A = \{m_i, n_i\}$ is a training set, where m_i the input vector is valued having $n-$ dimension and $n_i \in \{+1, -1\}$ represents a label for class determination of data instancen_i. The points closest to the generated hyperplane are known as Support Vectors (SVs). SVM aims to maximize the margin around these SVs. Through an iterative training process that minimizes the error function, SVM constructs this optimal hyperplane.

In this study, the security assessment of the power system categorizes classifications into two classes—secure and insecure. Each binary classifier is trained exclusively on data from its respective class. For the i^{th} and j^{th} classes in the training data, the function is resolved as optimization problem. The "Max-Wins voting" method is employed in this context for classification [17].

D. SVM Parameters selection

Support Vector Machines (SVMs) often benefit from using the Radial Basis Function (RBF) as a kernel mapping function [18]. This choice is recommended because the RBF kernel tends to result in lower misclassification rates, improved classification accuracy, and the ability to effectively capture non-linear relationships between selected features and class labels. The optimal values of (c, γ) are determined through v-fold cross-validation using Grid search. The best accuracy in cross-validation is achieved by selecting the optimal values of (c, γ) . The ranges$\{2^{-5}, 2^{-4}, \dots, 2^{14}, 2^{15}\}$ and $\{2^{-15}, 2^{-14}, \dots, 2^{4}, 2^{5}\}$ are chosen for c and γ, respectively.

In any pattern recognition problem related to power systems, achieving the highest classification accuracy of the classifier, as indicated in (19), is crucial for accurately estimating the power system state. Additionally, minimizing the misclassification rates for secure and insecure states, as described in (20) and (21), is equally important.

E. Performance evaluation terms

Classification Accuracy (CA)

$$CA\ (\%) = \frac{Total\ correctly\ classified\ patterns}{Total\ patterns\ in\ data\ set} \times 100 \qquad (19)$$

Secure Misclassification (SMC)

$$SMC(\%) = \frac{No.of\ secure\ cases\ classified\ as\ insecure}{Total\ number\ of\ insecure\ cases} \times 100 \quad (20)$$

Insecure Misclassification (SMC)

$$ISMC(\%) = \frac{No.of\ insecure\ cases\ classified\ as\ secure}{Total\ number\ of\ secure\ cases} \times 100 (21)$$

IV. Results and Discussions

This study focuses on power system static security assessment using a binary class support vector machine. IEEE standard test systems with 30 and 118 buses, covering both small and large system sizes, are employed to validate the findings obtained from the binary class SVM. Active and reactive power demands on specific buses are adjusted between 50% and 150% of their initial values. Each load modification scenario is accompanied by a single-line contingency case to generate more relevant patterns for static security evaluation. The minimum and maximum reactive power generation capacities of PV buses, along with their active power generation, are scaled proportionally to changes in load demand.

However, security assessments relying solely on the constraints outlined in (2) may encounter masking issues [14], [19]. To mitigate this challenge, the composite security index described by equation (11) and discussed in Section 2 of this study is utilized for evaluating static security. In the SVM binary classification problem, security states are categorized into secure and insecure classes. Alarm and security limits for all load buses are set at ±5% and ±7%, respectively, for voltages exceeding the nominal value of 1 per unit (pu).

The bus voltage should remain at the specified magnitude as long as the generator bus's reactive power stays within its upper and lower bounds. The alarm limit for transmission lines is set at 80% of their security limits. Table I outlines the details of the patterns created and how they were categorized into secure and insecure classes for the test systems under investigation.

TABLE I. Details of the Generated Pattern and its Classification into Secure and Insecure

	IEEE 30 Bus System	**IEEE 118 Bus System**
Total operating Cases	974 (818+156)	9791 (8723+1068)
Total Static Secure Cases (Training + Testing cases)	743 (613+129)	9080 (8092 +988)
Total Static insecure Cases (Training + Testing)	232 (205+27)	711 (631+80)

The total patterns are divided into two categories: 10% are allocated for testing and 90% for training. Careful feature selection using the sequential forward selection (SFS) approach results in improved misclassification rates and increased classification accuracy. The SFS approach is chosen in this study for its superior feature selection outcomes [20]. Table II presents the dimension reduction achieved for the test power systems under investigation using the SFS approach.

TABLE II. REDUCTION IN DIMENSION FOR THE IEEE 30 AND 118 BUS TEST SYSTEMS.

	IEEE 30 bus test system	IEEE 118 Bus Test System
Total No. of features	214	952
Features selected	09	60
% Dimension reduction achieved	4.21%	6.30%

Tables III and IV display the performance of the SVM-based multi-classifier for the IEEE 30-bus system and IEEE 118-bus system, respectively. The results in Tables III and IV demonstrate high accuracy levels in both training and testing phases, with minimal misclassification rates observed for the two test power systems.

It is observed that pattern X_2, as defined in (14), achieves higher classification accuracy during testing for both test power systems. The findings also showed that testing in a chosen pattern X_2 presented in (14), for both test power systems, resulting in the maximum accuracy. Furthermore, testing on a larger power system achieved 99.72% accuracy with the selected pattern X_2 specified in (14). The results indicate that pattern X_2presented in (14) consistently yielded the highest accuracy for both test power systems. The findings also indicated that in pattern X_2, there were two misclassifications in IEEE 30-bus system and three misclassifications in IEEE 118-bus system.

TABLE III. PERFORMANCE OF SVM-BASED BINARY CLASSIFIER FOR IEEE 30 BUS TEST SYSTEM

Selected Pattern Vector	Training sets	Testing Sets			Overall CA (%) (Training and Testing) (%)
	Samples CA (%)	Samples CA (%)	SMC (%)	ISMC (%)	
X_1 as in equation (13)	99.88% (817/818)	98.72% (154/156)	0 % (0/27)	1.55% (2/129)	99.69 % (971/974)
X_2 as in equation (14)	99.02% (810/818)	98.72% (154/156)	3.70 % (1/27)	0.7752% (1/129)	98.97 % (964/974)
X_3 as in equation (15)	99.75% (816/818)	98.72% (154/156)	3.70 % (1/27)	0.7752% (1/129)	99.59 % (970/974)
X_4 as in equation (16)	98.90 % (809/818)	98.08% (153/156)	3.70 % (1/27)	1.55% (2/129)	98.76 % (962/974)
X_5 as in equation (17)	99.88% (817/818)	98.72% (154/156)	3.70% (1/27)	0.7752 % (1/129)	99.69 % (971/974)

TABLE IV. PERFORMANCE OF SVM-BASED BINARY CLASSIFIER FOR IEEE 118 BUS TEST SYSTEM

Selected Pattern Vector	Training sets	Testing Sets			Overall CA (%) (Training andTesting) (%)
	Sample CA (%)	Sample CA (%)	SMC (%)	ISMC (%)	
X_1 as in equation (13)	99.84% (8709/8723)	99.53% (1063/1068)	1.25% (1/80)	0.405% (4/988)	99.81% (9772/9791)
X_2 as in equation (14)	99.90% (8714/8723)	99.72% (1065/1068)	2.5% (2/80)	0.101% (1/988)	99.88% (9779/9791)
X_3 as in equation (15)	99.78% (8704/8723)	99.53% (1063/1068)	2.5% (2/80)	0.304% (3/988)	99.75% (9767/9791)
X_4 as in equation (16)	99.87% (8712/8723)	99.62 % (1064/1068)	1.25% (1/80)	0.202% (2/988)	99.86% (9777/9791)
X_5 as in equation (17)	99.82% (8707/8723)	99.53% (1063/1068)	3.75% (3/80)	0.202% (2/988)	99.78% (9770/9791)

V. CONCLUSION

This paper introduces a binary class static security assessment of a power system using pattern recognition. By utilizing the composite security index, it addresses the masking issue and accurately distinguishes between secure and insecure scenarios even when violations of constraints occur in close proximity. SVM demonstrates effectiveness in creating a binary classifier that categorizes the system state into secure and insecure classes. Through efficient feature extraction aimed at enhancing classification accuracy and reducing misclassification rates, the sequential forward selection method substantially reduces pattern sizes. The performance of the binary classifier has been evaluated across various sets of power system variables, revealing that bus voltage, bus angle, and contingency number in binary form sufficiently encapsulate information about the power system's condition.

REFERENCES

[1] K. L. Morison, L.Wang, and P. Kundur, “Power system security assessment.” IEEE Power Energy Magazine vol. 2, issue 5, pp. 30–39, 2004.

[2] A.J. Wood, B.F. Wollenberg, and G.B. Sheble, “Power generation, operation, and control”, John Wiley & Sons, 2013.

[3] J. Srivani and K.S. Swarup, “Power system static security assessment and evaluation using external system equivalents”, International Journal of Electrical Power & Energy Systems, Vol. 30, Issue 2, pp.83–92, 2008.

[4] R. K. Misra and S.P. Singh, “Efficient ANN method for post-contingency status evaluation”, International Journal of Electrical Power & Energy Systems, Vol. 32, Issue 1, pp.54–62, 2010.

[5] L. Srivastava and S.N. Singh and J. Sharma, “A hybrid neural network model for fast voltage contingency screening and ranking”, International Journal of Electrical Power & Energy Systems, Vol. 22, No. 1, pp.35-42, 2000.

[6] D. Niebur and A.J. Germond, “Unsupervised neural net classification of power system static security states”, International Journal of Electrical Power & Energy Systems, Vol. 14, Issue 2-3, pp.233-242, 1992.

[7] M. Ramirez-Gonzalez, F. R. Segundo Sevilla, P. Korba, and R. Castellanos-Bustamante, “Convolutional neural nets with hyper parameter optimization and feature importance for power system static security assessment”, Electric power systems research, Vol. 211, 2022.

[8] M. Ramirez-Gonzalez, F. R. Segundo Sevilla and P. Korba, "Convolutional neural network based approach for static security assessment of power systems," 2021 World Automation Congress (WAC), Taipei, Taiwan, pp. 106-110, 2021.

[9] C. Lu, X. Ma, L. Li, Y. Lv and Y. Sun, "An online power system static security assessment method based on convolutional neural network", 2021 IEEE 5th Conference on Energy Internet and Energy System Integration (EI2), Taiyuan, China, pp.3127-3131, 2021.

[10] A. Dhandhia, and V. Pandya, “Contingency ranking in static security assessment using teaching learning based optimization enhanced support vector regression”, Materials today: Proceedings, Vol. 62, Issue 13, pp. 7174-7178, 2022.

[11] O.A. Alimi, K. Ouahada, A. M. Abu-Mahfouz, and S. Rimer, "Power system events classification using genetic algorithm based feature weighting technique for support vector machine", Heliyon Vol. 7, No. 1, 2021.

[12] M. Shahidehpour and Y. Wang, "Communication and control in electric power systems: applications of parallel and distributed processing", Wiley-IEEE, New Jersey, 2003.

[13] G.C. Ejebe, H.P.VanMeeteren and B.F. Wollenberg, "Fast contingency screening and evaluation for voltage security analysis", IEEE Transaction on Power Systems, Vol. 3, Issue 4, pp. 1582–1590, 1988.

[14] K. Nara, K.Tanaka, H. Kodama, R.R. Shoults, M.S.Chen, P. V. Olinda, and D. Bertagnolli, "On-line contingency selection for voltage security analysis", IEEE Transaction on Power Apparatus System, Vol. PAS-104, Issue 4, pp. 847–856, 1985.

[15] R.Sunitha, R.K. Sreerama and A.T. Mathew, "A composite security index for on-line steady-state security evaluation", Electric Power Components and Systems, Vol. 39, Issue 1, pp. 1-14,2011.

[16] C.K.Pang, F.S. Prabhakara, A.H. El-Abiad and A.J. Koivo, "Security evaluation in power systems using pattern recognition", IEEE Transactions on Power Apparatus and Systems, pp. 969–976, 1974.

[17] C. Hsu and C. Lin, "A comparison of methods for multiclass support vector machines", IEEE Transaction on Neural Networks, Vol. 13, Issue 2, pp. 415–425, 2002.

[18] J. Min and Y.C. Lee, "Bankruptcy prediction using support vector machine with optimal choice of kernel function parameters", Expert Systems with Applications, Vol. 28, Issue 4, pp. 603–614, 2005.

[19] R. Sunitha, R. Sreerama Kumar and A.T.Mathew "Online Static Security Assessment Module using Artificial Neural Network", IEEE transactions on power systems, Vol. 28, Issue 4, pp.4328-4335, 2013.

[20] S. Kalyani and K.S. Swarup, "Classification and Assessment of Power System Security Using Multiclass SVM" IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews) Vol. 41, Issue 5, pp. 753–758, 2011a.

NOMENCLATURE

P_{Gx}	Active power generation at generator bus x
P_{TL}	Total active load on buses
P_l	Total active power loss in the transmission line
P_{Gx}^{min}	Minimum active power generation at bus x
P_{Gx}^{max}	Maximum active power generation at bus x
N_{Gen}	Number of generators
N_{Bus}	Number of buses
$\lvert V_y^{min} \rvert$	Minimum bus voltage limit at bus y
$\lvert V_y^{max} \rvert$	Maximum bus voltage limit at bus y
$\lvert V_y \rvert$	Bus voltage at bus y
P_{kl}	Active power flow in the transmission line $k-l$
P_{kl}^{max}	Maximum active power flow limit in the transmission line $k-l$
V_y^{Des}	Desired bus voltage at bus y
$A_{v,y}^{u}$	Upper alarm bus voltage limit at bus y
$A_{v,y}^{l}$	Lower alarm bus voltage limit at bus y
$S_{v,y}^{u}$	Upper security bus voltage limit at bus y
$S_{v,y}^{l}$	Lower security bus voltage limit at bus y
$A_{MW,z}$	Active power alarm limit in transmission line z
$S_{MW,z}$	Thermal limit in transmission line z
δ_y	Bus angle at bus y
Q_{Gx}	Reactive power generation at bus x
P_{Dx}	Active power load at bus x
Q_{Dx}	Reactive power load at bus x
Q_{kl}	Reactive power flow in the transmission line $k-l$
Z	Contingency no. in binary