[1]Wael Abdullah Alsulami
[2]Sreerama Kumar Ramdas
[3]Muhyaddin Jamal Rawa

Artificial Neural Network based Fast and Accurate Static Security Assessment of 380 kV Saudi Power Grid

Journal of Electrical Systems

Abstract: - This paper proposes an artificial neural network (ANN) framework utilizing a multilayer feed-forward structure to evaluate the static security of a representative 380 kV Saudi transmission grid. The proposed model estimates a composite Static Security Index (SSI) that accounts for both line loading violations and bus voltage deviations. The ANN, designed with one hidden layer of ten neurons, receives normalized active and reactive power demands from load buses as inputs, while producing the SSI corresponding to each contingency as the output. Training is conducted using a back-propagation learning algorithm, where datasets are derived from Newton-Raphson load-flow simulations at various loading levels. Comparative analysis confirms that the proposed ANN approach matches the accuracy of the conventional NRLF-based evaluation while achieving substantially faster computation. The obtained performance suggests that the model can serve as an effective real-time decision-support tool for online contingency ranking and system security assessment in control centers.

Keywords: Power system security, Contingency selection, Saudi National Grid, Artificial neural network.

I. INTRODUCTION

Ensuring secure operation of an electrical power network requires rapid and precise evaluation of transmission line flows, overload detection, and monitoring of voltage magnitude deviations across buses. Previous research introduced contingency evaluation techniques based on the fast-decoupled load-flow method, demonstrating the ability to track voltage violations, line congestion, and overall network losses under different system states [1-4]. However, it is necessary to further reduce the computational overhead without affecting the accuracy. Conventional iterative power flow techniques are too slow for such on-line applications [5].

A multi-step adaptive regression technique [6] utilized for security assessment has shown reduced computation time. The Least Absolute Shrinkage and Selection Operator (LASSO) algorithm has been employed to estimate the security index for each power system operating stage by selecting the most influential features among bus voltages and line power flows. This approach improves computational efficiency by reducing the dimensionality of the input space while maintaining acceptable accuracy. However, despite its effectiveness in handling large datasets, LASSO may underperform when the system exhibits strong non-linearities, which motivates the exploration of non-linear models such as Artificial Neural Networks (ANNs) for enhanced accuracy in contingency ranking.

The degree of contingency is a crucial factor to consider while selecting the appropriate control mechanisms to preserve the integrity of system operations. Accordingly, the study has simulated the scenario and assessed the contingency selection process as a combinatorial optimization issue. The system's performance has been evaluated with a focus on accounting for double branch outages [7]. The obtained results confirm the method's capability to accurately recognize severe conditions.

The degree of deviation from security limits is quantified using several performance indices related to line loading and voltage magnitude variations during specific contingencies [8]. For the purpose of evaluating static security, conventional power flow and machine learning approaches have been compared. A number of machine learning approaches have been investigated in order to facilitate fast and reasonably accurate evaluation.

There is a masking issue with the majority of various performance indices based on bus voltage variations and line loadings used for security evaluation, thereby making it difficult to distinguish different contingency instances with comparable levels of violations. Ref. [9] has attempted to overcome these restrictions by developing a composite security index that uses a support vector machine (SVM) classifier to address the multi-class classification problem of power system security. The concept of a hyper ellipse enclosed within a hyper box has been utilized in this formulation.

[1] *Wael Abdullah Alsulami: King Abdulaziz University, Department of Electrical and Computer Engineering, Jeddah - 21589, Saudi Arabia
[2] King Abdulaziz University, Department of Electrical and Computer Engineering, Jeddah - 21589, Saudi Arabia
[3] King Abdulaziz University, Department of Electrical and Computer Engineering, Jeddah - 21589, Saudi Arabia

A Pattern recognition approach utilizing multi-class Support Vector Machine (SVM) technique has been proposed for static security evaluation in power systems has been proposed in recent research [10, 12]. The static security index is a numerical index that is calculated as the foundation for the multi-class SVM classifier architecture. The SVM classifier's simulation results have been compared with those of a Multilayer Perceptron network and the Least Squares Method [10]. In comparison to the other classifier approaches, the SVM classifier has been seen to provide higher accuracy with a lower rate of misclassification.

Ref. [11] proposes a fuzzy logic inference system fine-tuned with hybrid genetic-simulated annealing technique fast static security assessment of power systems. The research indicates that the proposed approach is a good candidate for the static security assessment under various operating scenarios.

The constraints of traditional power flow methodologies for power system security assessment can be overcome by using Artificial Neural Networks (ANNs) [13]. By utilizing the system data received through the continuous monitoring system in the control centers, ANN based models can be trained offline and thus can be effectively utilized for fast security assessment of power systems [14 - 17]. Several studies reported in the literature have focused on assessing and enhancing the security of the Saudi electrical network using artificial neural networks (ANNs) [18 - 22].

This paper investigates the feasibility of a multilayer feed forward ANN (MLFFNN) for the on-line static security assessment and contingency ranking of a typical 380 kV Saudi power grid. The system description and the composite security index utilized in the paper are given in Section two followed by the proposed ANN based approach security assessment in Section three, followed by the simulation results in Section four. Section five concludes the paper.

II. System Description and Seurity Assessment

The proposed ANN-based framework is evaluated using a representative 380 kV transmission system from the Saudi national grid, as shown in Fig. 1. This network comprises of 21 buses, three designated as generation buses and eighteen as load buses interconnected through 47 transmission lines. The system data is given in ref. [26] and base case Newton-Raphson load flow results are summarized in Tables A.1-A.3, which present the bus voltages, power generation and demand, and line power flows, respectively.

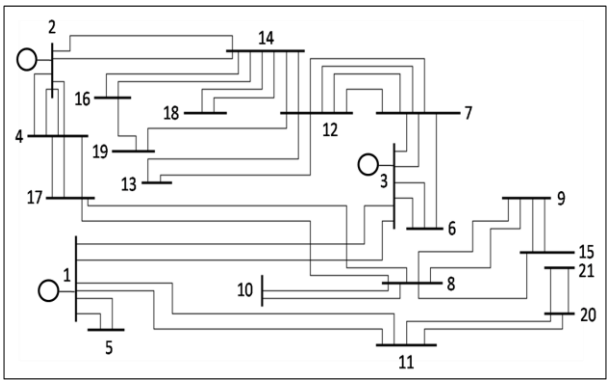

Fig. 1: Typical 380 kV Saudi Power Grid.

In a static security assessment algorithm, the base case load flow results are used as the benchmark. Corresponding to each contingency from the probable contingency list, load flow analysis is performed, and the respective static security in-dices are computed, based on which the operators can identify the critical contingencies in terms of line flow and bus voltage limit violations for further appropriate control actions.

To evaluate and rank the system contingencies, a composite Static Security Index (SSI) given is utilized. This index integrates two critical factors: deviations in line power flow beyond their rated thermal limits and voltage magnitude violations at load buses. The SSI is by

$$\mathrm{SSI} = \left(\frac{\mathrm{w}_1 \sum_{\mathrm{i}=1}^{\mathrm{N}_l+\mathrm{N}_t} \mathrm{LOI}_\mathrm{i} + \mathrm{w}_2 \sum_{\mathrm{i}=1}^{\mathrm{N}_\mathrm{b}} \mathrm{VDI}_\mathrm{i}}{100} \right)^{\frac{1}{4}} \quad (1)$$

Where w1 and w2 denote the respective weighting coefficients chosen based on the system under investigation. The Line Overload Index (LOI) quantifies the extent to which the real power flow in a transmission line exceeds its rated capacity and is given by:

$$LOI_l = \begin{cases} 0 & if\ P_{ij} \le P^{max} \\ \dfrac{P_{ij} - P_{ij}^{max}}{P_{ij}} & if\ P_{ij} > P^{max} \end{cases} \quad (2)$$

With S_{ij} being the real power flow in line i-j and S_{ij}^{max} its allowable limit. Meanwhile, the Voltage Deviation Index (VDI) measures the magnitude of voltage violations relative to permissible boundaries, defined as [26]:

$$VDI_K = \begin{cases} 0 & : \ |V^{max}| > |V_i| > |V^{min}| \\ \dfrac{-|V^{max}| + |V_i|}{|V^{max}|} & : \ |V^{max}| < |V_i| \\ \dfrac{-|V_i| + |V^{min}|}{|V^{min}|} & : \ |V^{min}| > |V_i| \end{cases} \quad (3)$$

where V_i is the actual voltage magnitude at bus i, and V^{min} and V^{max} correspond to its lower and upper operational limits, respectively.

The contingencies are classified into secure, marginally secure and insecure categories in the descending order of the value of security index determined for each of the contingencies as given in Table 1. Higher values of SSI imply lower security level of the power system at the prevailing operating condition.

Table 1. SSI Range and Security Condition

No	SSI Range	Security Condition
1	$0 < SSI \le 0.25$	Secure
2	$0.25 \le SSI < 0.35$	Marginally Secure
3	$SSI \ge 0.35$	Insecure

III. Proposed ANN Based Approach

Fig. 2 illustrates the configuration of the proposed multilayer feed-forward neural network (MLFFNN) developed for real-time static security evaluation of the Saudi 380 kV grid. The ANN has one hidden layer in addition to an input and an output layer. The input layer receives normalized real and reactive power values from the system's 18 load buses, forming a 36-neuron input vector, while the single output neuron provides the predicted Static Security Index (SSI) associated with a specific contingency. The hidden layer includes ten neurons that process weighted signals through sigmoid activation functions. Bias terms are included for both hidden and output layers, and all parameters are optimized via backpropagation to minimize prediction error.

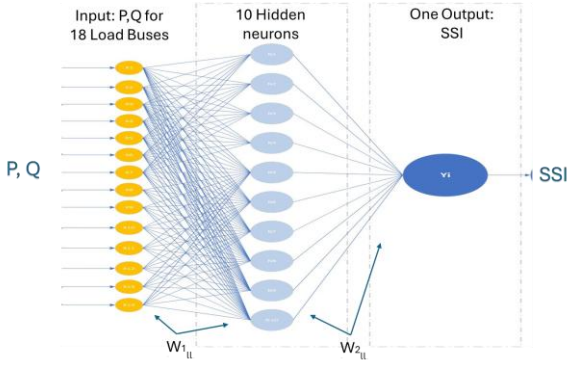

Fig. 2: Proposed ANN Architecture

Training data for the neural network are generated using Newton Raphson load flow simulations under multiple loading conditions for each considered contingency scenario. Each training instance comprised the normalized active and reactive power demands (P, Q) of all the load buses paired with its corresponding SSI value obtained from NRLF computations. The network parameters are optimized using the back-propagation algorithm, beginning with randomly initialized weight matrices derived through Xavier initialization to maintain gradient balance across layers [23, 24]. Throughout training, the mean squared error (MSE) between predicted and reference SSI values is iteratively minimized according to the following relation:

$$E_{mse} = \frac{1}{n}\sum_{i=0}^{i=n}(t_i - y_i)^2 \tag{4}$$

Where n indicates the number of trained models. At sample i, t_i represents the target, and y_i indicates Update of each weight w and bias b followed the standard learning rule:

$$\Delta w_{ij} = -\eta \frac{\partial E}{\partial w_{ij}} \quad , \quad \Delta b_j = -\eta \frac{\partial E}{\partial b_j} \tag{5}$$

IV. Simulation Results

The proposed ANN-based static security framework is applied to a representative 380 kV Saudi grid under twenty possible contingency scenarios given in Table 2. For each contingency, training sets are generated from Newton Raphson load flow simulations at multiple loading conditions. The network required a maximum of 97 epochs to achieve convergence, with mean squared error values below 10^{-3} across all cases. The performance of the proposed ANN based approach is assessed by comparing the SSI values predicted by the ANN with those obtained from the NRLF solution under various contingencies. Table 3 shows the contingency rank list obtained from the ANN model at the base case operating condition given in Appendix. The contingencies were are sorted in descending order of their severity according to their SSI values, which reflect the severity of the operating condition. As evident, contingency No. 13 representing the simultaneous outage of the two transmission lines connecting Bus 12 and Bus 14 is the most critical event, followed by contingencies 16 and 15. These cases exhibited significant limit violations, classifying them as insecure conditions. Meanwhile, scenarios 9, 1, and 5 are within the marginal security range, indicating stressed but operable conditions. The remaining contingencies are evaluated as secure, with SSI values well within the acceptable limits.

Table 2. SSI Range and Security Condition.

No.	Contingency
1	Outage ‖ Line 1 or Line 2 (between Bus 1 and Bus 2)
2	Outage ‖ Line 9 or Line 10 or Line 11 (between Bus 4 and Bus 17)
3	Outage ‖ Line 14 or Line 15 (between Bus 3 and Bus 7)
4	Outage ‖ Line 18 (between Bus 6 and Bus 7)
5	Outage ‖ Line 25 or Line 26 (between Bus 8 and Bus 17)
6	Outage ‖ Line 27 or Line 28 (between Bus 8 and Bus 10)
7	Outage ‖ Line 32 or Line 33 (between Bus 1 and Bus 11)
8	Outage ‖ Line 3 and Line 6 (between Buses 2-14 and 2-4)
9	Outage ‖ Line 5 and Line 7 (between Bus 2 and Bus 4)
10	Outage ‖ Line 8 and Line 9 (between Buses 2-4 and 4-17)
11	Outage ‖ Line 19 and Line 20 (between Bus 7 and Bus 12)
12	Outage ‖ Line 30 and Line 31 (between Bus 9 and Bus 15)
13	Outage ‖ Line 36 and Line 37 (between Bus 12 and Bus 14)
14	Outage ‖ Line 43 and Line 44 (between Bus 14 and Bus 16)
15	Outage ‖ Generation of Bus 2
16	Outage ‖ Generation of Bus 3
17	Outage ‖ Generation of Bus 7
18	Outage ‖ Generation of Bus 8
19	Outage ‖ Generation of Bus 10
20	Outage ‖ Generation of Bus 14

Table 3. Contingency Rank List: Comparison between ANN Approach and NRLF Approach

Contingency No.	SSI (ANN)	SSI (NRLF)	Percentage error (%)
13	0.744538156	0.744538156	0
16	0.340816821	0.340816821	0
15	0.332202787	0.332202787	0
9	0.316578401	0.316578401	0
1	0.308376000	0.308376000	0
5	0.350000000	0.298363926	0.173064065
10	0.287000000	0.293458591	0.022008526
12	0.293000000	0.292829201	0.000583272
17	0.287000000	0.287328730	0.00114409
11	0.283375587	0.283375587	0
4	0.182000000	0.279963361	0.349914934
14	0.276938433	0.276938433	0
8	0.266666000	0.266666287	1.08E-06
19	0.239000000	0.266045368	0.101656978
6	0.258100000	0.265158886	0.026621344
2	0.265048676	0.265048676	0
20	0.200000000	0.262740092	0.238791467
7	0.241842133	0.241842133	0
3	0.202311834	0.202311834	0
18	0.202311834	0.202311834	0

V. Conclusion

This research has proposed a multilayer feed-forward neural network (ANN) approach for performing on-line static security evaluation of the 380 kV Saudi transmission network. The adopted composite security index integrates both bus voltage and line-loading violations, providing a unified criterion for identifying and prioritizing critical contingencies. The network structure, featuring a single hidden layer of ten neurons, uses normalized active and reactive power demands as inputs and outputs the corresponding SSI. The preliminary investigations reveal that the proposed ANN based approach yields solution accuracy comparable to the conventional Newton-Raphson method while achieving significantly lower computation time. These advantages make the developed model a practical candidate for integration into control center applications supporting on-line grid security monitoring of Saudi National Power Grid.

References

[1] Tajdinian, M., Allahbakhshi, M., Mohammadpourfard, M., Mohammadi, B., Weng, Y., & Dong, Z. (2020). Probabilistic framework for transient stability contingency ranking of power grids with active distribution networks: application in post disturbance security assessment. IET Generation, Transmission & Distribution, 14(5), 719-727.

[2] Liyanarachchi, L., Hosseinzadeh, N., Mahmud, A., Gargoom, A., & Farahani, E. M. (2020, November). Contingency ranking selection using static security performance indices in future grids. In 2020 Australasian Universities Power Engineering Conference (AUPEC) (pp. 1-6). IEEE.

[3] Shrivastava, P., Sharma, A., & Channi, H. K. (2022, March). Static security assessment and contingency analysis for smart grid. In 2022 6th International Conference on Computing Methodologies and Communication (ICCMC) (pp. 119-125). IEEE..

[4] Mohammed, A. Q., & Alkhazraji, A. A. (2023). Multi Contingency Analysis In Power System Using Fast Decoupled Load Flow. Przeglad Elektrotechniczny, 2023(12).

[5] Nandini, P. S., Krishan, R., & Pullaguram, D. (2022, November). Static Security Assessment of Large Power Systems Under Contingency Cases. In 2022 IEEE 10th Power India International Conference (PIICON) (pp. 1-6). IEEE.

[6] Li, Y., Li, Y., & Sun, Y. (2018). Online static security assessment of power systems based on lasso algorithm. Applied Sciences, 8(9), 1442.

[7] da Silva, J. M., Costa, I., dos Santos, J. V. C., Barbosa, J. L. V., Braun, T., & Pessin, G. (2019). Toward a more reliable system for contingency selection in static security analysis of electric power systems. IEEE Systems Journal, 14(1), 1183-1194.

[8] Hailu, E. A., Nyakoe, G. N., & Muriithi, C. M. (2023). Techniques of power system static security assessment and improvement: A literature survey. Heliyon, 9(3).

[9] Dhandhia, A., Pandya, V., & Bhatt, P. (2020). Multi-class support vector machines for static security assessment of power system. Ain Shams Engineering Journal, 11(1), 57-65.

[10] Kalyani, S., & Swarup, K. S. (2012). Classification of static security status using multi-class support vector machines. The Journal of Engineering Research [TJER], 9(1), 21-30.

[11] Hailu, E. A., Nyakoe, G. N., & Muriithi, C. M. (2024). Data-driven approach to fuzzy inference system tuning for static security assessment of multi-area power systems with renewable energy. Ain Shams Engineering Journal, 15(2), 102369.

[12] Li, C., & Liu, Y. (2021). Online dynamic security assessment of wind integrated power system using SDAE with SVM ensemble boosting learner. International Journal of Electrical Power & Energy Systems, 125, 106429.

[13] Duan, R., Alrawi, O., Kasturi, R. P., Elder, R., Saltaformaggio, B., & Lee, W. (2020). Towards measuring supply chain attacks on package managers for interpreted languages. arXiv preprint arXiv:2002.01139.

[14] Peyghami, S., Palensky, P., & Blaabjerg, F. (2020). An overview on the reliability of modern power electronic based power systems. IEEE Open Journal of Power Electronics, 1, 34-50.

[15] Van Cutsem, T., Glavic, M., Rosehart, W., Canizares, C., Kanatas, M., Lima, Vournas, C. (2020). Test systems for voltage stability studies. IEEE Transactions on Power Systems, 35(5), 4078-4087.

[16] Allella, F., Chiodo, E., Giannuzzi, G. M., Lauria, D., & Mottola, F. (2020). On-line estimation assessment of power systems inertia with high penetration of renewable generation. IEEE access, 8, 62689-62697.

[17] Maihemuti, S., Wang, W., Wang, H., Wu, J., & Zhang, X. (2021). Dynamic security and stability region under different renewable energy permeability in IENGS system. IEEE Access, 9, 19800-19817.

[18] Alhelou, H. H., Golshan, M. E. H., Njenda, T. C., & Hatziargyriou, N. D. (2020). An overview of UFLS in conventional, modern, and future smart power systems: challenges and opportunities. Electric Power Systems Research, 179, 106054.

[19] Venzke, A., & Chatzivasileiadis, S. (2020). Verification of neural network behaviour: Formal guarantees for power system applications. IEEE Transactions on Smart Grid, 12(1), 383-397.

[20] Yin, L., Gao, Q., Zhao, L., Zhang, B., Wang, T., Li, S., & Liu, H. (2020). A review of machine learning for new generation smart dispatch in power systems. Engineering Applications of Artificial Intelligence, 88, 103372.

[21] Jiang, T., Zhang, R., Li, X., Chen, H., & Li, G. (2021). Integrated energy system security region: Concepts, methods, and implementations. Applied Energy, 283, 116124.

[22] Duchesne, L., Karangelos, E., & Wehenkel, L. (2020). Recent developments in machine learning for energy systems reliability management. Proceedings of the IEEE, 108(9), 1656-1676.

[23] Kalyani, S., & Swarup, K. S. (2013). Pattern analysis and classification for security evaluation in power networks. International Journal of Electrical Power & Energy Systems, 44(1), 547-560.

[24] Alimi, O. A., Ouahada, K., & Abu-Mahfouz, A. M. (2020). A review of machine learning approaches to power system security and stability. IEEE Access, 8, 113512-113531.

[25] "Static Security Assessment: A Case Study of the Saudi National Grid" (2024) European Journal of Engineering and Technology Research, 9(6), pp. 1–6. doi:10.24018/ejeng.2024.9.6.3199.

[26] Alsulami, W.A., Ramdas, S.K. and Rawa, M.J. (2024) Static Security Assessment: A case study of the saudi national grid, European Journal of Engineering and Technology Research, 9(6), pp. 1–6. doi:10.24018/ejeng.2024.9.6.3199.

APPENDIX

Table A1: Base Case Load Flow Solution – Bus Voltages

Bus No.	Voltage Mag. (pu)	Voltage Angle (degree)
1	1.010	0.000
2	1.010	-7.516
3	1.010	-0.132
4	1.007	-10.032
5	1.015	-0.303
6	1.014	-4.338
7	1.032	-9.477
8	0.991	-31.106
9	0.990	-31.837
10	0.990	-30.901
11	1.014	-1.894
12	1.035	-9.821
13	1.037	-10.218
14	1.040	-10.197
15	0.990	-32.249
16	1.040	-10.527
17	0.992	-18.106
18	1.041	-10.574
19	1.036	-10.429
20	1.015	-2.219
21	1.015	-2.712

Table A2: Base Case Load Flow Solution – Power Generation and Demand

Bus No.	Generation		Load	
	P_G (MW)	Q_G (MVAR)	P_D (MW)	Q_D (MVAR)
1	1721.48	3487	-	-
2	2500	3314	-	-
3	1200	3593	-	-
4	-	-	51.80	21.27
5	-	-	40.00	15.00

6	-	-	203.50	83.59
7	1000	1000	510.60	209.74
8	518	0	481.00	197.58
9	-	-	754.80	310.05
10	1200	449	714.84	293.63
11	-	-	888.00	364.76
12	-	-	725.20	297.89
13	-	-	518.00	212.78
14	746	154	740.00	303.97
15	-	-	888.00	364.76
16	-	-	592.00	243.17
17	-	-	148.00	60.79
18	-	-	425.50	174.78
19	-	-	592.00	243.17
20	-	-	370.00	151.98
21	-	-	148.00	60.79

Table A3: Base Case Load Flow Solution – Line Flows

Line		Load flow		
From bus	To bus	MW	MVar	MVA
1	3	710.28	-43.14	711.59
1	3	710.28	-43.14	711.59
1	5	32.017	-76.8	83.209
1	5	32.017	-76.8	83.209
1	11	879.84	-341.3	943.7
1	11	879.84	-341.3	943.7
2	4	524.31	-0.047	524.31
2	4	524.31	-0.047	524.31
2	4	524.31	-0.047	524.31
2	4	524.31	-0.047	524.31
2	14	201.38	-200.2	283.93
2	14	201.38	-200.2	283.93
3	6	582.89	-78.99	588.22
3	6	582.89	-78.99	588.22
3	7	727.29	-136.9	740.06
3	7	727.29	-136.9	740.06
4	17	682.05	25.402	682.52
4	17	682.05	25.402	682.52
4	17	682.05	25.402	682.52
6	7	906.92	-206.3	930.09
7	12	676.49	-437.8	805.79
7	12	676.49	-437.8	805.79

7	12	676.49	-437.8	805.79
7	12	676.49	-437.8	805.79
8	9	771.52	51.564	773.24
8	9	771.52	51.564	773.24
8	10	-153.19	-157.5	219.75
8	10	-153.19	-157.5	219.75
8	15	512.05	-187.8	545.4
8	17	-915.98	76.391	919.16
8	17	-915.98	76.391	919.16
9	15	299.22	-143.5	331.85
9	15	299.22	-143.5	331.85
11	20	323.84	-155.4	359.2
11	20	323.84	-155.4	359.2
12	13	323.89	-353.7	479.58
12	13	323.89	-353.7	479.58
12	14	360.48	-411.2	546.85
12	14	360.48	-411.2	546.85
12	19	792.17	-185.2	813.52
14	16	344.14	-103.8	359.46
14	16	344.14	-103.8	359.46
14	18	266	-214.8	341.87
14	18	266	-214.8	341.87
16	19	-51.852	-73.08	89.61
20	21	92.527	-43.97	102.44
20	21	92.527	-43.97	102.44