energies

MDPI

Article

Online Steady-State Security Awareness Using Cellular Computation Networks and Fuzzy Techniques

Lili Wu [1,*], Ganesh K. Venayagamoorthy [2,3,*] and Jinfeng Gao [1]

[1] School of Electrical Engineering, Zhengzhou University, Zhengzhou 450001, China; jfgao@zzu.edu.cn
[2] Real-Time Power and Intelligent Systems Laboratory, Holcombe Department of Electrical and Computer Engineering, Clemson University, Clemson, SC 29634, USA
[3] Eskom Centre of Excellence in HVDC Engineering, University of KwaZulu-Natal, Durban 4041, South Africa
* Correspondence: wuli1988@126.com (L.W.); gkumar@ieee.org (G.K.V.)

Abstract: Power system steady-state security relates to its robustness under a normal state as well as to withstanding foreseeable contingencies without interruption to customer service. In this study, a novel cellular computation network (CCN) and hierarchical cellular rule-based fuzzy system (HCRFS) based online situation awareness method regarding steady-state security was proposed. A CCN-based two-layer mechanism was applied for voltage and active power flow prediction. HCRFS block was applied after the CCN prediction block to generate the security level of the power system. The security status of the power system was visualized online through a geographic two-dimensional visualization mechanism for voltage magnitude and load flow. In order to test the performance of the proposed method, three types of neural networks were embedded in CCN cells successively to analyze the characteristics of the proposed methodology under white noise simulated small disturbance and single contingency. Results show that the proposed CCN and HCRFS combined situation awareness method could predict the system security of the power system with high accuracy under both small disturbance and contingencies.

Keywords: steady-state security assessment; situation awareness; cellular computational networks; load flow prediction; contingency; fuzzy system

Citation: Wu, L.; Venayagamoorthy, G.K.; Gao, J. Online Steady-State Security Awareness Using Cellular Computation Networks and Fuzzy Techniques. *Energies* **2021**, *14*, 148. https://doi.org/10.3390/en14010148

Received: 19 November 2020
Accepted: 22 December 2020
Published: 30 December 2020

1. Introduction

With the development of grid interconnection, the structure of modern power systems is expanding. It is constantly developing in the direction of high voltage, long distance, and large capacity, and becoming more complex. At the same time, the proliferation of highly permeable renewable energy sources, such as wind and solar energy, makes the electricity market impose loads on the grid in a more unpredictable, uncontrollable, and dynamic way. It is difficult to predict power grid information with an increasingly large geographic area and more dynamic load. Because of that, it is insurmountable for controllers to see the full picture of the power grid situation under a fault or contingency. Therefore, fast, accurate, and predictive estimation of the system security status has become a major concern for dispatchers.

Power system security estimation problems can be classified in dynamic security analysis and static security analysis [1]. At present, due to the long sampling time of supervisory control and data acquisition (SCADA) system, online security analysis is mainly conducted from the perspective of static security analysis, regarding voltage, current, active, and reactive power security, etc. However, the extensive deployment of a phasor measurement unit (PMU) provides a possible solution for fast online security situation awareness. Since dynamic security analysis is based on a steady-state initial value, a fast online updated static state can be used as an initial state of dynamic security analysis. Even static state tracking which is fast enough can be considered as a dynamic security analysis [2].

Various research studies have been conducted on steady-state security awareness using traditional methods. Literatures [3,4] have evaluated the voltage and load flow security using the situation awareness method. Xiao et al. [3] proposed a situation awareness method based on a static voltage security region of a large power system integrated with wind farms. Netto et al. [4] presented an efficient voltage security region construction tool using probabilistic reliability evaluation to solve a situational awareness problem. This probability-based voltage security assessment algorithm provides richer visual information about the system safety level and has the potential for real-time application. Sun et al. [5] proposed a steady-state operation situation awareness method based on the dynamic power flow method of the active distribution network to study the operation state of the power grid under time changes. The traditional methods can supply a fair result for the system situation, but most of them require the exact system model and are highly computational.

Wide applications of artificial intelligence (AI)-based power system security analysis reveal that AI technology is an effective tool for power systems model building, time saving during power flow computation, and online situation awareness. Fuzzy logic is an intelligent algorithm with natural rules which is closer to human thought than traditional logic systems. A particle swarm optimization combined K-means fuzzy algorithm was addressed in [6] for the power system security assessment. Both static and transient security could be classified as secure or insecure under given states and outages. The fuzzy logic clustering technique was adopted in [7] by Matos and so forth to evaluate global multi-contingency steady-state security. Literatures [8–10] proposed a fuzzy logic-based contingency ranking method instead of the conventional performance index approach to overcome the mask problems for power system static security analysis. Marannino et al. [10] proposed a neuro-fuzzy method for the voltage collapse risk classification. Halilčević et al. [11] used fuzzy membership functions of power system elements to estimate the system security level online. Later, Halilčević et al. [12] used the deterministic and fuzzy inference method to continuously estimate the security, adequacy, and reliability of power system current operation. Kalyani et al. [13] generated synchronized phasor measurements to construct a neuro-fuzzy network for online voltage security monitoring. Zhao et al. [14] proposed a hierarchical model for survival situation awareness using variable fuzzy set technology to estimate system survivability. Various applications of fuzzy logic-based power system security analysis reveal that fuzzy technology is a highly promising tool for translating the operator's linguistic experience to executable machine language which can make the operator aware of the security state of power networks. The use of the fuzzy set theory of variables improves the accuracy and objectivity of the evaluation results.

Besides fuzzy logic, other AI methods have been applied in literatures [15–19] regarding power system security awareness. Fan et al. [15] proposed a data-driven system voltage prediction model based on the generalized regression neural network to dig in-depth power system operation big data to enhance system situation awareness. Literature [16] proposed a real-time safety assessment tool based on PMU and a decision tree to estimate potential safety hazards after failure: Voltage amplitude fluctuation, temperature limit violation, voltage stability, and transient stability. Literature [17] formulated post-outage reactive power flow analysis as a nonlinear constrained optimization problem of a bounded network to be solved by the genetic algorithm (GA). Literature [18] assessed the static security of the power system using an enhanced radial basis function (RBF) neural network. Literature [19] proposed a novel steady-state contingency screening method combining the feed-forward neural network (FFNN) and the fast Fourier transform (FFT). The effectiveness of the AI methods has been verified through selected research cases and predetermined schemes. However, because of the time-consuming problem during online neural network training, the above AI-based methods are not suitable for online application.

CCN is a distributed scalable neural network architecture composed of a computing element (neural network or other) in each cell, which is suitable for describing complex nonlinear network systems whose actual model is not available, and learning its dynamic

characteristics in time and space [20]. As a distributed dynamic recurrent neural network, the CCN architecture has the advantage of high scalability, effective nonlinear modeling, and easy computation parallelized. The CCN has good performance in solving the problems of transient stability prediction [21], load flow inferencing [22], state estimation [23], dynamic state prediction [24], wide area measurement (WAM) [25], and situation awareness (SA) [26] using measurements from PMUs. In the previous research by the author [27,28], different kinds of neural network-based CCN were applied as an effective tool for power system state estimation. In literature [27], the multi-layer perceptron (MLP)-based CCN was applied to bus voltage prediction. MLP is a traditional neural network which is simple and easy to train. Even though it has not taken advantage of contextual information, the results are acceptable for voltage prediction. In literature [28], recurrent neural network (RNN)-based CCN was applied to state estimation. The results showed that the introduction of the CCN technique to the power system state prediction made it possible for online security analysis application, as the distribute structure of CCN could estimate the operation state with less time consumed. This paper proposed an online situation awareness method considering power system static security using echo state network (ESN)-based CCN and fuzzy logic. Different from MLP and other RNN neural networks which are hard to converge during the learning process, ESN is an effective tool for prediction even based on the simplest line regression training method. To validate the validity of the proposed ESN-based CCN method, MLP- and RNN-based CCN were also applied in this publication to compare with the results in literatures [27,28].

This paper is organized as follows. Section 2 introduces the design of the situation awareness system using the proposed method. The situation awareness was realized through 4 levels (perception level, comprehension level, projection level, and visualization level). Section 3 shows the perception and comprehension levels. In the design of the comprehension level, a two-layer CCN-based state prediction is proposed. Section 4 focuses on the projection level with the design of a hierarchical cellular rule-based fuzzy system (HCRFS)-based system security assessment. Section 5 shows system security visualization utilizing web-based computer language. Section 6 provides the discussion and results under small disturbance and contingency. Finally, Section 7 presents conclusions and suggests potentially promising future work in this field.

2. System Architecture

For modern intelligent power system, fast and accurate situational awareness is particularly important for power system security. When contingency occurs, it can provide an effective judgment basis for the operator in the control room the first time, and avoid wrong operation, missed operation, or delayed operation, which may lead to cascade failures, and even system blackout. The research of the power system situational awareness technology is still in its infancy. It mainly improves the power grid perception ability through information integration, overall control strengthening of power grid, system reliability enhancement, and operator misoperation decrease. Power system situation awareness is to accurately and effectively grasp power grid security situation through three levels: Perception, comprehension, and projection. This paper implemented a CCN and HCRFS combined online situation awareness method regarding power system steady-state security. The proposed situation awareness architecture is shown in Figure 1.

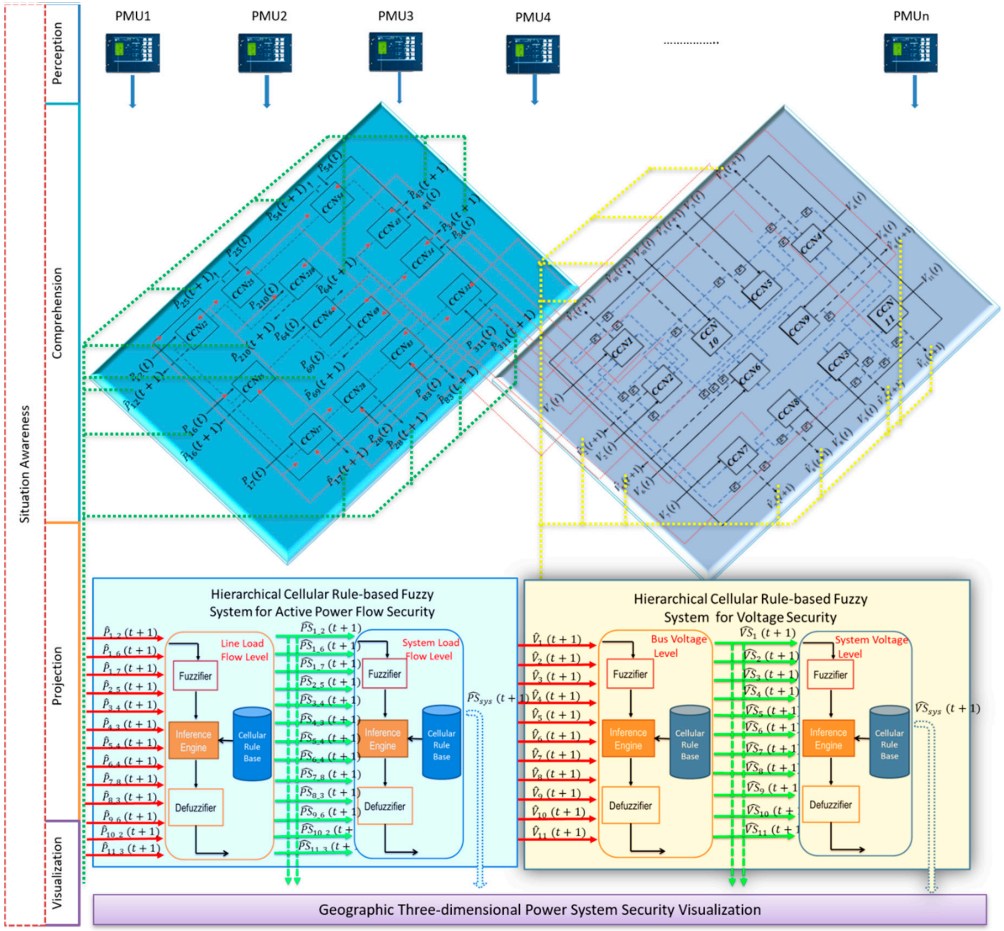


Figure 1. The cellular computation network (CCN)- and hierarchical cellular rule-based fuzzy system (HCRFS)-based power system security situation awareness.

Perception level: 12-bus power system model built in real-time digital simulation system (RTDS) benchmark to generate synchronized power system measurements from PMU.

Comprehension level: CCN-based two-layer online state prediction and estimation using PMU data.

Projection level: A HCRFS-based power system voltage and power security level assessment using prediction states.

Visualization level: A scheme to dynamically visualize the voltage and load flow situation in geographic environment is proposed using the forecasting system security levels.

As shown in Figure 1, in the perception process, PMUs were applied on a 12-bus power system to generate synchronized data. In the comprehension part, the voltage magnitude and load flow were predicted with a two-layer CCN-based mechanism using PMU data. In the projection step, the predicted voltage magnitude and active power were used to assess the power system security level using a HCRFS-based mechanism. Finally, buses and the system security level were displayed geographically two-dimensionally by the data visualization tools. The system architecture shown in Figure 1 is illustrated in detail in Sections 3–5.

3. Perception and Comprehension

The perception and comprehension levels of the proposed situation awareness technology regarding steady-state power system security are illustrated in this section.

3.1. PMU Based Data Generation of 12-Bus Benchmark (Perception)

As an early tentative study, a 12-bus power system was applied to test the steady-state power system security. The 12-bus power system model was built in a real-time digital simulation system (RTDS) benchmark. PMUs were deployed on each bus to generate synchronized power system measurements, like voltage magnitude, voltage angle, current magnitude, and current angle. Voltage violation and load overflow under contingency are common static security problems. In order to fully use the PMU data, the bus voltage and line current measurements were used to predict the bus voltage violation and load overflow.

The selected 12-bus power system had different types of generators and loads, and the network size was suitable for the initial CCN application. The 12-bus platform included 4 generators (Generator G_1 was connected to an infinity bus). The generators' and loads' active power capacity are shown in Table 1, while other details of the test power system can be seen in [29]. As shown in Table 2, there were 13 types of component contingencies in the 12-bus system: 8 transmission line contingencies, 2 transformer outages, and 3 generator trips.

Table 1. The 12-bus power system parameters.

Load/Gen. No.	Active Power/MW
Generator G_1 (infinity Bus)	289
Generator G_2	500
Generator G_3	300
Generator G_4	400
Load on Bus_2	280
Load on Bus_3	320
Load on Bus_4	320
Load on Bus_5	100
Load on Bus_6	440

Table 2. The 12-bus power system line information.

Line No.	From Bus	To Bus	Rating/MW
$Line_{1\_2}$	1	2	250
$Line_{1\_6}$	1	6	250
$Trans_{1\_7}$	1	7	1000
$Line_{2\_5}$	2	5	250
$Line_{3\_4\_1}$	3	4	250
$Line_{3\_4\_2}$	3	4	250
$Line_{4\_5}$	4	5	250
$Line_{4\_6}$	4	6	250
$Line_{7\_8}$	7	8	500
$Trans_{8\_3}$	8	3	1000
G_2	10	2	700
G_3	11	3	500
G_4	9	6	500

3.2. CCN-Based Two-Layer State Prediction (Comprehension)

In the comprehension process of the proposed situation awareness mechanism, a two-layer CCN-based method was proposed for state prediction. In Figure 1, the voltage magnitude of each bus is predicted with the top right CCN layer using PMU data, while the load flow of each transmission line is forecasted based on the top left CCN panel utilizing PMU data and the prediction from the voltage layer. ESN was applied in each cell of the two-layer CCN.

From Figure 1, regarding the voltage prediction layer, there were 11 buses that had been simulated, except the infinity bus of the 12-bus power system. ESN was implemented

in each cell representing each of the 11 buses. The relationship of each cell in CCN was a direct mapping of the connections of each bus of the test power system. In each cell, the one-step-ahead voltage magnitude prediction of the bus is defined as below:

$$\left|\widehat{V}_i(t+1)\right| = f\left\{|V_i(t)|,\ \theta_i(t),\ \left|\widehat{V_n}(t)\right|\right\} \tag{1}$$

where $|V_i(t)|$, $\theta_i(t)$ are the voltage, magnitude, and angle of bus i at time t. $\left|\widehat{V_n}(t)\right|$ is the one step delayed voltage prediction values of the neighbors that are connected to bus i.

In the load flow prediction layer, ESN was implemented in each cell representing each line. From Table 2, there are 13 lines in the 12-bus power system. The relationship of each cell in CCN was a direct mapping of the connections of each line of the test power system. In each cell, the predicted active load flow of line j is $\widehat{P}_j(t+1)$ which is shown in Equation (2).

$$\widehat{P}_j(t+1) = f\left\{\left|\widehat{V}_i(t)\right|,\ \theta_j(t), I_j(t)\right\} \tag{2}$$

where $\left|\widehat{V}_i(t)\right|$ is the time-delayed voltage prediction values of bus i generated from Equation (1). $\theta_j(t)$ is the current angle of line j at time t from PMUs. $I_j(t)$ is the line current magnitude at time t of line j.

3.3. The Online Learning of the ESN in Each Cell

ESN is one type of recurrent neural network which uses a dynamic reservoir to simulate the nonlinear relationship between the input and the output.

In an ESN with K inputs, N units in reservoir, and L outputs, the reservoir states are updated following the equation below:

$$X(i+1) = f_{res}\left(W_{in}U(i+1) + WX(i) + W_{fb}Y(i)\right) \tag{3}$$

where W_{in} is the weight between the input layer and reservoir units, W is the weight in the reservoir layer and the output layer, while W_{fb} is the feedback weight. f_{res} is the active function of the reservoir layer (usually the logistic sigmoid or the tanh function). $X(i)$ is the reservoir state, $U(i)$ is the K dimension input signal, and $Y(i)$ is the L dimension output signal. The output is obtained from Equation (4):

$$Y(i+1) = f_{out}(W_{out}(U(i+1), X(i+1), Y(i))) \tag{4}$$

where weights W_{out} is the readout weight matrix between the reservoir layer and f_{out} is the output activation function (typically the identity or a sigmoid).

In order to obtain the W_{out}, W_{in} and W were randomly initialized and Equations (3) and (4) were activated with input and output signals. After that, the W_{out} readout weights matrix could be trained by the line regression method in Equation (5) [30]:

$$W_{out} = (pinv(M) * T)^{Trans} \tag{5}$$

where M is $[(U(i+1),\ X(i+1),\ Y(i)]$ and $pinv(M)$ is the pseudo-inverse of M. T is the inverted of the output active function $fout^{-1}(Y(i+1))$. $Trans$ is transpose.

The online training of ESN using Equations (3)–(5) in each cell of the CCN is shown in Figure 2. In Figure 2, there are two modes (training mode and prediction mode) in each cell of the two-layer CCN model. For example, in the voltage prediction layer, the prediction mode worked for continuous voltage prediction using updating weights $W_{out}(k+1)$. The training mode, which was a mirror reflection of the ESN structure in the prediction mode, was activated if the mean square error (MSE) was larger than the expected tolerance. Each ESN/cell was trained with the line regression method in Equation (5) using a dynamic database which was updated with prediction data and target value.

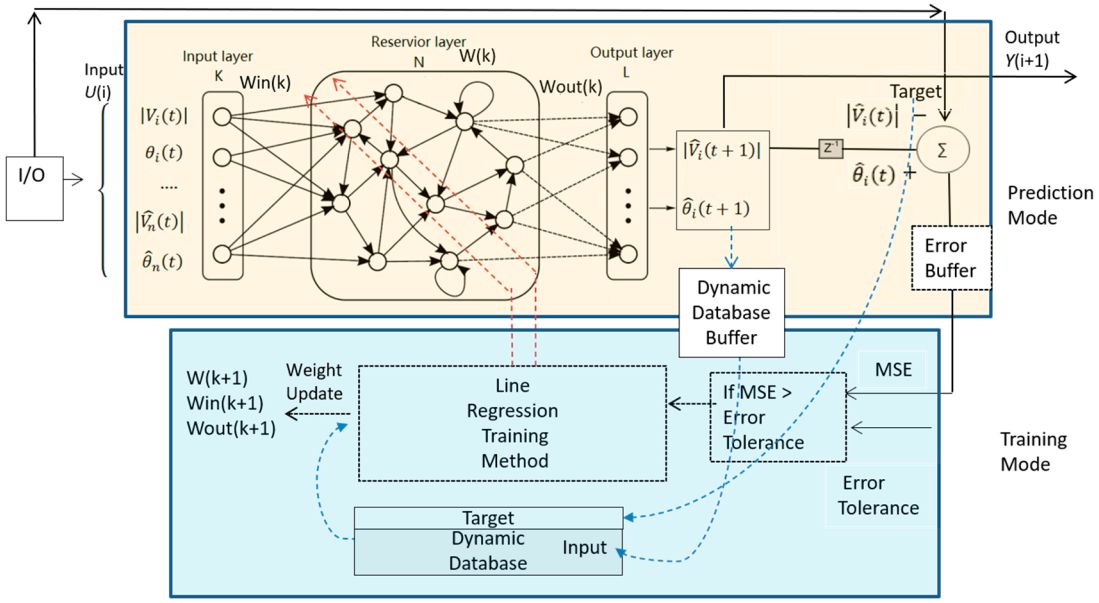


Figure 2. The online training of the echo state network (ESN) in each cell.

In the training mode of Figure 2, the fitness function is the MSE between the prediction value and real value of all the k training data points. The MSE is an effective measurement for forecasting the error of a prediction method in statistics.

$$MSE = \frac{1}{k}\sum_{i=1}^{k}|Act_i - Pred_i|^2 \tag{6}$$

It is defined as the mean of the square of the error between the actual value and prediction value. Where Act_i is the actual value and $Pred_i$ is the prediction value, and k is the number of the data points.

4. Projection

This section shows the projection process which was developed using an HCRFS-based power system security-level classification. The predicted voltage magnitude and active power from the comprehension part were used to assess the power system security level here.

4.1. Voltage Security Assessment

The voltage may violate beyond its limitation under disturbances such as load variations. A definition of voltage collapse, instability, and security introduced by IEEE [31] concluding the power system voltage stability may be threatened in the presence of a variety of single or multiple contingencies. Real-time voltage fluctuation can be performed using the security index [32] below:

$$Index_v(t) = \sum_{i=1}^{p}\omega_i.(\Delta|V_i(t)|)^m \tag{7}$$

where $\Delta|V_i(t)| = |V_i(t)| - |V_{li}|$, $\Delta|V_i(t)|$ is the voltage magnitude violation at time t. $|V_i(t)|$ is voltage magnitude of load bus i at time t. $|V_{li}|$ is the voltage magnitude limit of load bus i. p is the load bus number. ω is weight factor and m is exponent factor.

4.2. Active Power Flow Security Assessment

A possible way to express the real-time security level of overload is the power security index:

$$Index_{MW}(t) = \sum_{j=1}^{k} \gamma_j . \left(R_j(t)\right)^n \tag{8}$$

where $R_j(t) = \left(P_j(t)\right)/P_{lj}$, $R_j(t)$ is the active power overload ratio at time t. $P_j(t)$ is the branch j load at time t, and P_{lj} is the overload limit. k is the number of branches. γ is weight factor and n is exponent factor.

The above Equations (7) and (8) denote that the voltage magnitude violation $\Delta|Vi\ (t)|$ and active power rating ratio $R_j(t)$ are potential variables to formulize system security indices. The proposed HCRFS-based security assessment was performed via the predicted voltage magnitude violation $\Delta\left|\widehat{V}_i(t+1)\right|$ and active power rating ratio $\widehat{R}_j(t+1)$.

4.3. HCRFS Based System Security Assessment

From Figure 1, the voltage security assessment was designed via predicted voltage magnitude $\Delta\left|\widehat{V}_i(t+1)\right|$. Meanwhile, load flow security analysis was realized with an active power rating ratio, $\widehat{R}_j(t+1)$. The fuzzy controller transformed the expert knowledge into an automatic control strategy through fuzzification, inference engine, rule base, and defuzzification structure mode. In each designed HCRFS, there were two layers. The first layer was a single bus or line security assessment; meanwhile, the second layer was system level security analysis.

From the HCRFS for voltage security in Figure 1, it is clear that the input was $\Delta\left|\widehat{V}_i(t+1)\right|$, which was the predicted voltage magnitude violation of 11 buses, and the output was the system voltage security level $\widehat{VS}_{sys}(t+1)$. The proposed HCRFS fuzzy index for voltage security was performed by:

$$\widehat{VS}_i(t+1) = fuzzy\left(\Delta\left|\widehat{V}_i(t+1)\right|\right) \tag{9}$$

$$\widehat{VS}_{sys}(t+1) = fuzzy\left(\widehat{VS}_i(t+1)\right) \tag{10}$$

$$\Delta\left|\widehat{V}_i(t+1)\right| = \left|\widehat{V}_i(t+1)\right| - |V_{li}| (i = 1, 2 \ldots .11) \tag{11}$$

where $\widehat{VS}_i(t+1)$ is the voltage security assessment of bus i. $\left|\widehat{V}_i(t+1)\right|$ is the first step ahead predicted voltage magnitude of bus i from CCN which is shown in Equation (1). $|V_{li}|$ is the voltage magnitude limit of load bus i.

The proposed HCRFS-based overload security assessment which is shown in the left bottom panel of Figure 1 can be formulized below:

$$\widehat{PS}_j(t+1) = fuzzy\left(\widehat{R}_j(t+1)\right) \tag{12}$$

$$\widehat{PS}_{sys}(t+1) = fuzzy\left(\widehat{PS}_j(t+1)\right) \tag{13}$$

$$\widehat{R}_j(t+1) = \frac{\widehat{P}_j(t+1)}{P_{lj}} (j = 1, 2 \ldots, 13) \tag{14}$$

where $\widehat{PS}_{sys}(t+1)$ is the fuzzy index for system load flow security. $\widehat{PS}_j(t+1)$ shows the load security level of line j. $\widehat{R}_j(t+1)$ is the predictive active power rating ratio. $\widehat{P}_j(t+1)$ is the predicted active load flow of line j from CCN which is shown in Equation (2). P_{lj} is the active power rating.

4.4. Cellular Based Rule Base of HCRFS Block

The fuzzy implication of the first layer in the HCRFS was a multi-input–multi-output (MIMO) system:

Rule i: If a_1 is A_{1i} ... and a_r is A_{ri}, then b_1 is B_{1i} ... , and bn is B_{ni}.

where *i* is the number of rules, *r* is the input number and *n* is the output number.

The fuzzy implication of the second layer in the HCRFS follows multi-input–single -output (MISO) systems:

Rule j: if x_1 is A_{1j} ... , and x_r is A_{rj}, then y is C_j.

where *i* is the number of rules, *r* is the input number.

In the 12-bus power system, ideally to classify the power system states "Secure", "Alert", or "Emergency", it requires abundant combinations of input levels. Assume each of the 11 voltage inputs is classified by five levels (corresponding membership functions are NB, NM, Normal, PM, PB); this would mean 5^{11} = 48,828,125 voltage level combinations.

In order to overcome the rule explosion, an idea of the cellular-based rule base is inspired by the CCN structure. CCN is a cellular computational network consisting of a neural network in each cell that can be used to implement networked power systems. In the design of the voltage magnitude prediction layer, CCN was applied to implement the connection of the 11 buses. Each cell/bus of the CCN could be trained and used separately only considering the information of the nearest neighbors. Similarly, as the status of the system security had a tight relationship with contingency cases who may lead to voltage violation or overload, different types of contingencies were considered in developing rules process for the cellular concept based fuzzy system.

In the design of the cellular-based rule base, only the buses directedly connected to the contingency were considered. For example, if there was a line contingency between bus 1 and 2, only 2 primary buses (buses 1 and 2) were considered in the "IF" condition part, instead of all the inputs.

From Table 2, there are 13 outages. If the cellular-based fuzzy rules were applied for each outage using only 2 primary buses, the rule cases reduced to 5^2 = 25 voltage level combinations for each outage, and 13 outages meant 13 × 25 = 325 rules. Finally, it is more than 1 − (325 ÷ 48,828,125) = 1 − 0.00066% = 99.99% reduction in the number of rules.

5. Visualization

After the projection process, the buses and system security level were displayed geographically two-dimensionally using web-based computer language.

5.1. Bus Voltage and Line Load Flow Security Visualization

With the application of computer language, the security level of each element and the power system could be vividly displayed to the operation staff. As shown in Figure 1, all the predicted security information from the HCRFS block is displayed geographically two-dimensionally. The displayed information includes the voltage magnitude security level of each bus, the load flow security of each line, and the overall power system security level from the viewpoint of the whole power network.

The power system security states were characterized in three modes from the view of the power system operators, which were Secure, Alert, and Emergency:

- Secure: All the buses are in normal states, which means there is no alarm being presented and none of the contingency would cause overload or voltage violations;
- Alert: There is an alarm or contingency which needs the operator to pay attention;
- Emergency: It is indicated that a serious alarm appears, and the system is seriously insecure, or there is a contingency that may lead to system blackout which needs the operator to act immediately.

The voltage magnitude security of each bus was shown geographically above the position of each bus in the 12-bus power system as in below:

$$V_{security\ Level} = \begin{Bmatrix} Secure & Green\ Pie \\ Alert & Yellow\ Pie \\ Emergency & Red\ Pie \end{Bmatrix} \quad (15)$$

The positive "+" and negative "−" showed the voltage magnitude was above or below 1 pu. The diameter of the symbol increased with the rise of the security level to make it more noticeable.

The overload situation of each line was displayed in a circular arrow manner above that line using different colors.

$$P_{security\ Level} = \begin{Bmatrix} Secure & Green\ Circle \\ Alert & Yellow\ Circle \\ Emergency & Red\ Circle \end{Bmatrix} \quad (16)$$

5.2. Power System Security Level Visualization

The prediction of the power system security level from HCRFS was visualized in a meter to make it easy to read. Secure, Alert, and Emergency were labeled on the pane of the meter as a reference for the pointer to show the security level.

6. Results and Discussion

From Section 3, the voltage and active power flow prediction was carried out based on the two-layer CCN model. The power system steady-state security related to its robustness under the normal state, as well as to withstanding foreseeable contingencies without interruption to customer service. Thus, the CCN-based power system security analysis was done from two aspects: 1. Voltage and active power prediction with pseudorandom binary sequence (PRBS) signals on generators or load to simulate normal disturbance of the 12-bus power system; 2. voltage and active power prediction under single line outage to test the power system security in the event of unforeseen contingency. The details of the simulation cases are shown in Table 3. Case A is a training case with PRBS signals applied on generators G_2, G_3, G_4 to simulate the small noise and disturbance in the power system. The 0.5, 1, and 2 Hz PRBS signals were fluctuated positive and negative 15%, which were simulated voltage magnitude violations under the steady-state. Cases B to E were test cases.

Table 3. Simulation cases under different disturbances and outages.

Case No.	Disturbance Type
Case A	PRBS signals on G_2, G_3, G_4 (for batch training)
Case B	PRBS signals on loads of Bus_2, Bus_3, Bus_5, and $Line_{5\_4}$ outage
Case C	PRBS signals on load of Bus_2 and generator G_3
Case D	PRBS signals on loads of Bus_2, Bus_3, Bus_5, and $Line_{2\_5}$ tripped

In order to see the performance of ESN-based CCN, the MLP- and RNN-based CCN predictions [27,28] were applied in this paper for comparison. Different from the online learning of ESN, the weights of MLP/RNN-based CCN were generated from batch training using dynamic multi-swarm particle swarm optimization (DMSPSO) [33], and later applied to online prediction. Case A in Table 3 is the batch training data for MLP and RNN. In the batch training process, PRBS signals were applied on three generators to simulate the disturbance during actual system operation. The trained weights of MLP and RNN in each CCN cell were fixed and applied to online prediction in different scenarios. The parameter settings of the three kinds of neural networks are shown in Table 4. The stop

iteration numbers for batch training were 3000, but for online training, the stop criteria was MSE $< 1 \times 10^{-2}$.

Table 4. Parameter settings for different types of neural networks.

Neural Networks Type	Training Type	Training Method	Max Iter.	Search Range	Group Num.	Particle Num.
MLP	Batch training	DMPSO	3000	[−1.5 1.5]	4	3
RNN	Batch training	DMPSO	3000	−[2 2]	5	3
ESN	Online Training	Line regression	MSE $< 1 \times 10^{-2}$	[−2 2]	-	-

6.1. Voltage Prediction with PRBS Signals on Generators (Case A)

In Figure 3, 1 s ahead voltage prediction results under PRBS signals on generators G_2, G_3, and G_4 can be seen. The solid blue line indicates PMU measurements from the 12-bus RTDS model (real data), the green dot-dash line is voltage predictions from MLP, the black dashed line shows results of RNN, and the red dotted line indicates voltage prediction of ESN. The panels in Figure 3 include voltage prediction results for three generator buses (Bus_{G2}, Bus_{G3}, and Bus_{G4}) and three load buses (Bus_{L4}, Bus_{L5}, Bus_{L6}). The oscillations on the red dotted line within 0 to 200 ms of Figure 3 come from the initiation process of ESN online training. From comparison, all three kinds of neural networks can follow the voltage change trend with a slight time shift.

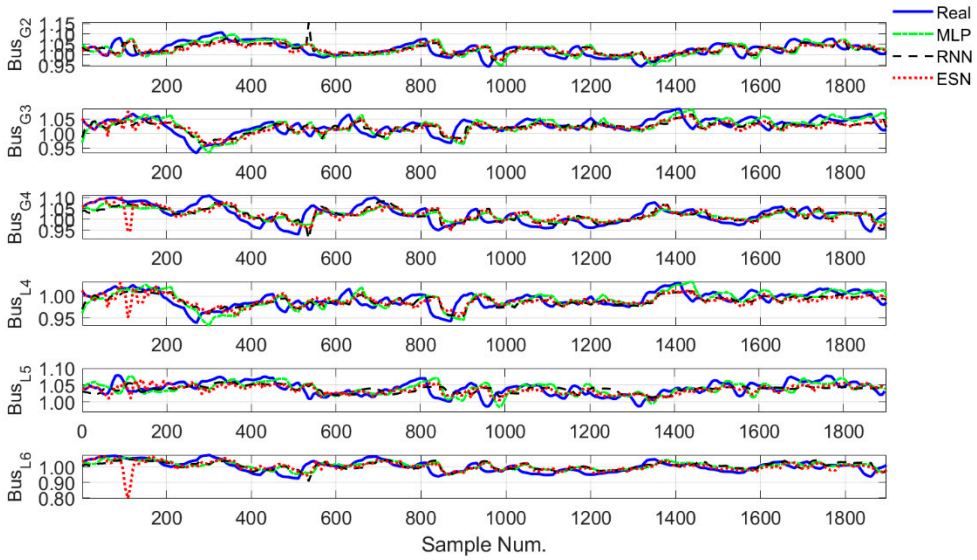


Figure 3. The 1 s voltage prediction near generator buses and load buses.

6.2. Voltage Prediction with PRBS Signals on Load Buses and Line Contingency (Case B)

Besides PRBS signals, transmission line contingency was also applied for several seconds and restored in this part for testing. Figure 4 shows voltage prediction results under PRBS signals on load buses (Bus_{L2}, Bus_{L3}, Bus_{L5}) and $Line_{5\_4}$ (which connected bus_4 and bus_5) outage. Because $Line_{5\_4}$ tripped, loads on bus_4 and bus_5 experienced slightly low voltage. As Bus_{L6} and Bus_{G4} were close to generators, the load on Bus_6 and generator on Bus_{G4} performed better with small oscillation when contingency occurred and disappeared. From Figure 4, the MLP- or RNN-based voltage prediction had a steady-state error, while the ESN prediction had the advantage of fast reaction and small overshoot when contingency occurred and was restored.

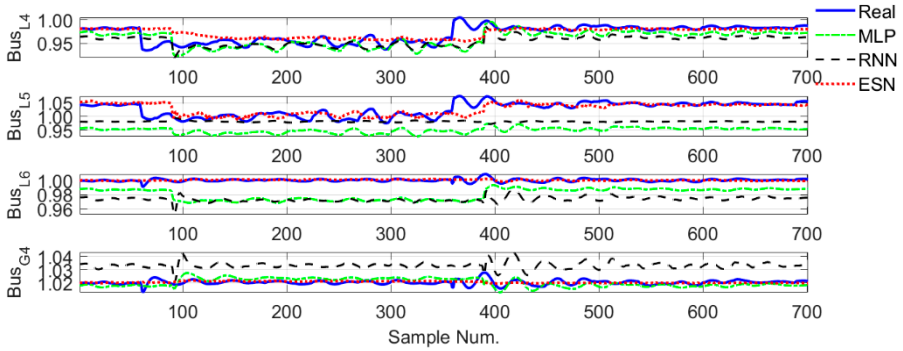


Figure 4. The 1 s voltage prediction on load buses and generator bus G_4 under pseudorandom binary sequence (PRBS) noise and $Line_{5\text{-}4}$ outage.

6.3. Load Flow Prediction with PRBS Signals on Generator and Load Buses(Case C)

A scheme with PRBS signals on load Bus_3 and generator G_2 was proposed here to see the performance of the active power prediction. In Figure 5, the performances of three kinds of neural networks were similar except for small differences. The MLP prediction performed better on peak values, while the online ESN method needed an adjusting time (simple 200 to simple 300) for initialization. The green dot-dash line in the $Line_{4\_3}$ panel looks like an average line in the horizontal direction. This phenomenon shows the MLP-based active power prediction cannot converge on Line $_{4\_3}$.

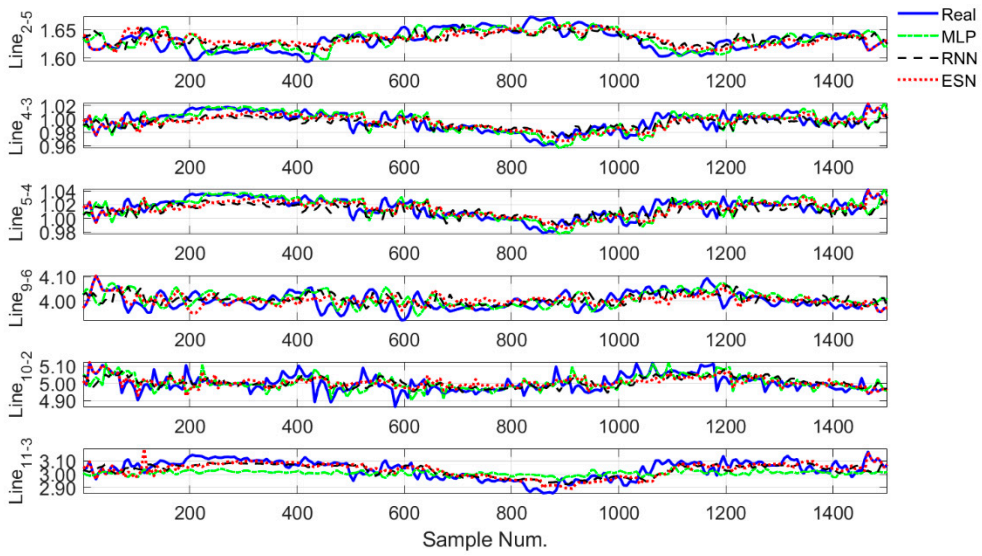


Figure 5. The 1 s load flow prediction of $Line_{2\text{-}5}$, $Line_{4\text{-}3}$, $Line_{5\text{-}4}$ (near load buses), $Line_{9\text{-}6}$, $Line_{10\text{-}2}$, and $Line_{11\text{-}3}$ (near gen. buses).

6.4. Load Flow Prediction with PRBS Signals on Load Buses and Line Contingency (Case D)

Figure 6 indicates the power flow change under load disturbance and $Line_{7\_8}$ break. The $Line_{1\_2}$ and $Line_{2\_5}$ undertook half of the loss led by the $Line_{7\_8}$ fault. The 1 s load flow forecast illustrated that the ESN method had excellent performance in line disconnection circumstances. From the comparison of all three methods, the online training ESN method overmatched the fixed weight RNN and MLP method as the online learning mechanism could update the weights of ESN in each cell timely, according to the situation change such as load noise of abrupt line off.

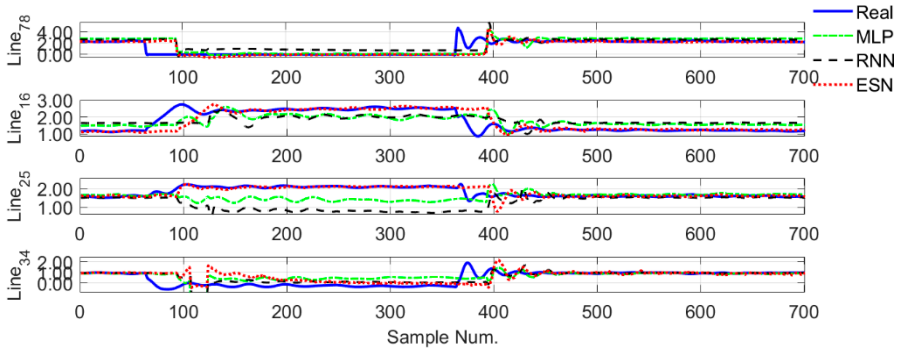


Figure 6. The 1 s ahead active power prediction on load Bus_3, Bus_4, Bus_5, and generator Bus_{G3} under PRBS signals on generators and $Line_{7\text{-}8}$ outage.

6.5. Performance Evaluation

As the performance of different neural networks was similar in Case A and Case C, the MSE errors between real values and predictions are shown in Table 5 for performance evaluation. It is reasonable that MLP/RNN performed better in Case A than ESN as Case A was a batch training case, while ESN needed initialization time for online training. But in Case C, ESN had better prediction results as the online training method could change the neural network weights with the situation change.

6.6. HCRFS based Power System Security Awareness

From Section 4, the two-layer HCRFS block could estimate the whole system security situation including component (bus and transmission line) security and system security. In the application of web-based computer visualization technology, the output voltage and load flow security level of the HCRFS could be vividly displayed to the operation staff in a visual manner. Figures 7–9 are the visualization results.

Figure 7 is the web-based graphic user interface under a normal operation state. The left graph is the component visualization (voltage security on each bus and load flow security on each line). The right meter is the corresponding system security display. From Figures 7–9, different colors indicate different security states of the system. It is defined in Equations (15) and (16) that green means the Secure state, orange shows the Alert state, while red indicates the Emergency state. The pie shapes represent the voltage security of each bus geographically. The circular arrows illustrate the load flow security level of each transmission line with various colors. Normally, the system is in the Secure state (Figure 7). The green pies on the buses and green circles on the lines show that the bus voltage and line load flow are all fluctuating within a secure range.

The security situation of the power system changes under disturbances, as shown in Figures 8 and 9. To highlight the main parts, Figures 8 and 9 remove style designs including title, background, and logo, zooming in on the geographic two-dimensional based component security and system security meter.

6.6.1. Bus Voltage and Line Load Flow Security Awareness under Small Disturbance

The visualization of each bus and transmission line under PRBS signals are shown in Figure 8a. Because of the disturbances (PRBS signals) on generators G_2, G_3, and G_4, there were some Alert states compared with the initial Secure states (Figure 7). In Figure 8, the yellow negative pies above the buses reveal that Bus_3, Bus_4, Bus_5, Bus_6, Bus_8, Bus_9, and Bus_{11} are slightly below the rated voltage. At the same time, yellow circles above the transmission $line_{1\_6}$, $line_{1\_7}$, $line_{7\_8}$, and $line_{8\_3}$ indicate slight overflow on those lines.

Table 5. Mean square error (MSE) between real values and predictions of different neural networks.

Neural Networks Type	Case A			Case C		
	Max. MSE	Min. MSE	Mean MSE	Max. MSE	Min. MSE	Mean MSE
MLP	9.5594×10^{-4}	8.7512×10^{-5}	5.2308×10^{-4}	0.0067	1.1533×10^{-4}	0.0015
RNN	0.0011	4.5032×10^{-5}	4.6935×10^{-4}	0.0047	1.1528×10^{-4}	0.0011
ESN	0.0012	4.7166×10^{-5}	5.2835×10^{-4}	0.005	8.7193×10^{-5}	9.9694×10^{-4}

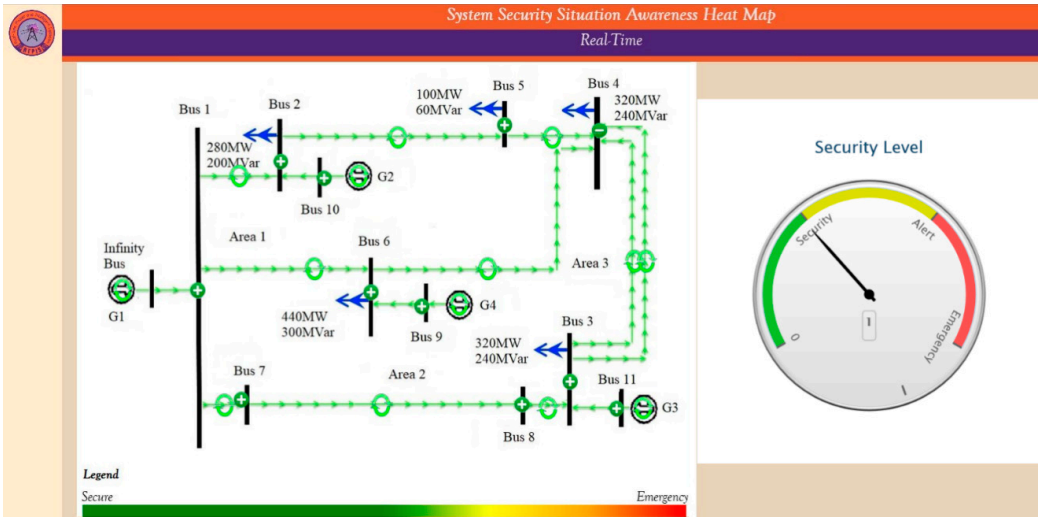
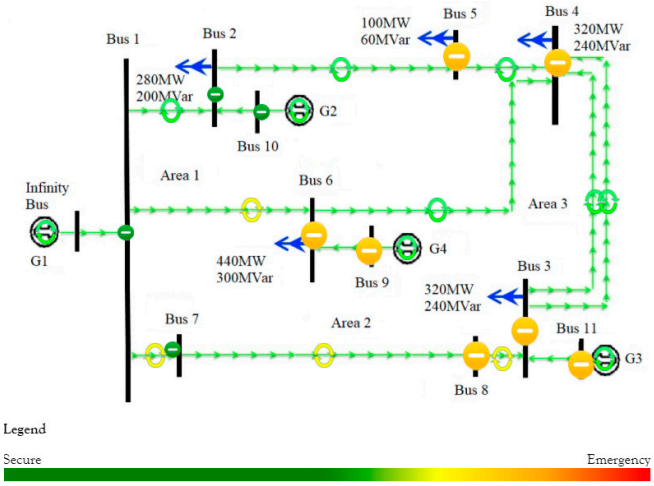
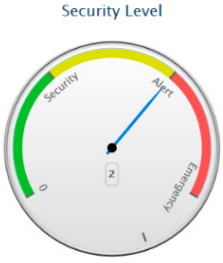


Figure 7. Graphic user interface of the situation awareness system (initial state).



(**a**)



(**b**)

Figure 8. Graphic user interface under PRBS signals disturbance. (**a**) The components' security awareness of the 12-bus power system, (**b**) The system security state.

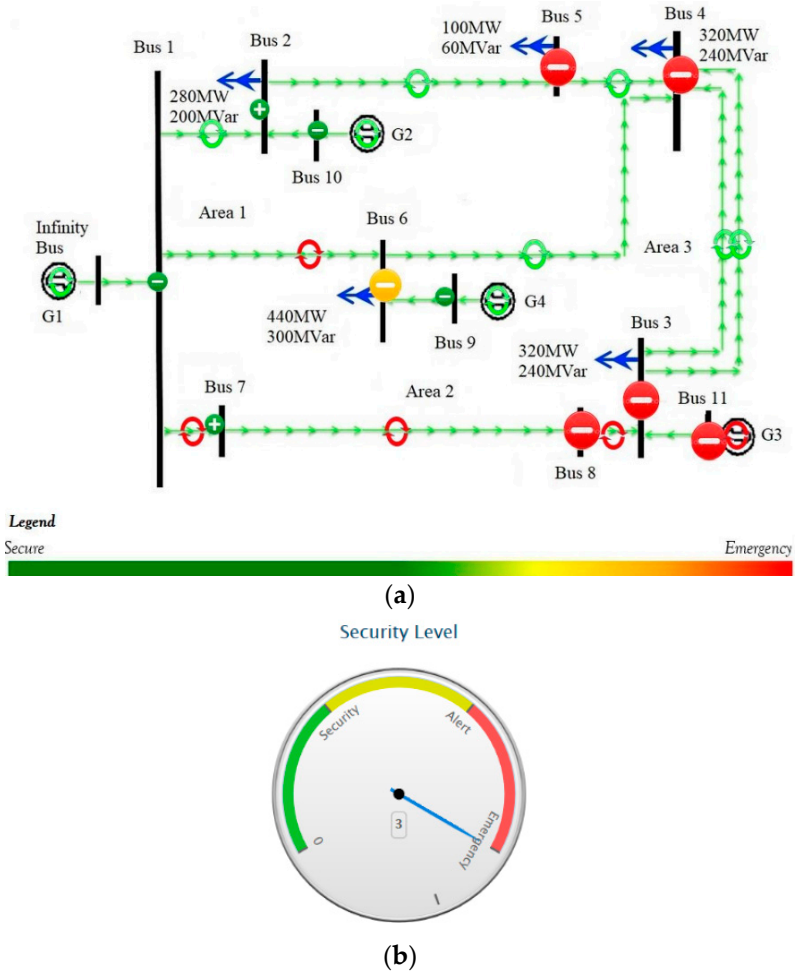


Figure 9. Graphic user interface state under PRBS signals and $line_{1\_2}$ contingency. (**a**) The components' security awareness of the 12-bus power system, (**b**) The system security state.

6.6.2. Bus Voltage and Line Load Flow Security Awareness under Small Disturbance and Line Contingency

Both PRBS signal and $Line_{1\_2}$ contingencies are applied in this simulation in Figure 9. Compared with the entire green in Figure 7, the 11 buses have 1 Alert state (yellow pie) and 5 Emergency states (red pie), while the 13 transmission lines have 5 Emergency states. Because $Line_{1\_2}$ is tripped, generator G_3 and transmission lines $Line_{1\_6}$, $Line_{1\_7}$, $Line_{8\_3}$, and $Line_{7\_8}$ are seriously overloaded (red circle). The five red pies show that because of the disturbance and $Line_{1\_2}$ contingency, the power system is instable, and Area 3 is in a serious sub-voltage situation.

6.6.3. Power System Security Level Visualization

The system security was defined in a meter considering all the buses' and transmission lines' secure state. The different states in the meters of Figures 7b, 8b and 9b were in accordance with the bus and line secure state from Figures 7a, 8a and 9a. The pointer in Figure 7b indicates that the system security level is Secure, which is consistent with the initial Secure state of the buses and transmission lines. Alert states on 7 buses and 4 lines in Figure 8a indicate that sub-voltage and overload appeared on the system. That is why the indicator points to Alert in Figure 8b at that time instant. The system security in Figure 9b is in Emergency level, corresponding to the 5 serious buses voltage violation and 5 severe lines' surcharge in Figure 9b.

7. Conclusions

This paper has presented how to implement power system security awareness using a CCN and HCRFS combined methodology. From the results presented, it can be seen that the ESN-based CCN bus voltage and line load flow prediction could estimate the state of the power system online better than MLP- and RNN-based CCNs, with a mean MSE lowered to 9.9694×10^{-4} under new events or contingency. The proposed HCRFS system reduces the number of rules in the rule-base dramatically by 99.99%. The two-dimensional visualizations could vividly display the bus voltage security levels, transmission line power flow security states, and the system security situation synchronously to the control room operator. The predicted security level could inform the system operator to react in advance to prevent a cascaded contingency and even a system blackout. Multiple results show that the proposed CCN and HCRFS combined visualization method could predict the security of the power system with acceptable accuracy under both small disturbance and line contingency. Future work includes: Improving the prediction accuracy, the dynamic security could be considered later, and parallel computing could be applied to improve the training efficiency. Furthermore, the proposed CCN and HCRFS combined system security level prediction and visualization technique can be applied to a 68-bus system to study the scalability of the proposed CCN- and HCRFS-based approach.

Author Contributions: All authors have contributed to the publication of this article. L.W. and G.K.V. worked together on the applications of cellular computational network (CCN) for the proposed study while first author was a visiting researcher at Clemson University in 2018 and 2019. L.W., G.K.V. and J.G. work together on proposed content of this paper; L.W. wrote the paper with guidance and advice from G.K.V. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by # 1312260 and Duke Energy Distinguished Professorship Endowment, the National Natural Science Foundation of China (61803343), Key R\&D and Promotion Project of Henan Province (202102210096, 202102210296), and Key Projects of Higher Education of Henan Province (19A120012).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: Lili Wu acknowledges the Real-Time Power and Intelligent Systems (RTPIS) Laboratory at Clemson University where she was a visiting researcher from January 2018 to December 2019. For the research study reported in this paper, Lili Wu acknowledges the contributions of RTPIS Lab and the research assistants including (i) Paranietharan Arunagirinathan for assisting with the power system model and its simulation on the real-time digital simulator and (ii) Iroshani Jayawardene for assisting with the visualization design and discussions on the cellular computational network.

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

References

1. Kundur, P.; Paserba, J.; Ajjarapu, V.; Andersson, G.; Bose, A.; Canizares, C.; Hatziargyriou, N.; Hill, D.; Stankovic, A.; Taylor, C.; et al. Definition and classification of power system stability. *IEEE Trans. Power Syst.* **2004**, *19*, 1387–1401. [CrossRef]
2. Debs, A.S.; Larson, R.E. A Dynamic Estimator for Tracking a Power System. *IEEE Trans. Power Appar. Syst.* **1970**, *89*, 1670–1678. [CrossRef]
3. Xiao, F.; Jiang, Z.-Q.; Ai, Q.; Hao, R. Situation awareness of power system based on static voltage security region. *J. Eng.* **2017**, *2017*, 2423–2427. [CrossRef]
4. Netto, N.A.R.L.; Borges, C.L.T. Enhancing the situational awareness of voltage security region via probabilistic reliability evaluation. *Int. Trans. Electr. Energy Syst.* **2020**, *30*, 1–15. [CrossRef]
5. Sun, C.; Liu, D.; Wang, Y. Operation Situational Awareness Based on Dynamic Power Flow for a Profound Analysis of Active Distribution Network. In Proceedings of the IET Conference Publications, Helsinki, Finland, 14–15 June 2016; pp. 2–5.
6. Kalyani, S.; Swarup, K.S. Particle swarm optimization based K-means clustering approach for security assessment in power systems. *Expert Syst. Appl.* **2011**, *38*, 10839–10846. [CrossRef]

7. Matos, M.A.; Hatziargyriou, N.D.; Lopes, J.A.P. Multicontingency steady state security evaluation using fuzzy clustering techniques. *IEEE Trans. Power Syst.* **2000**, *15*, 177–183. [CrossRef]
8. Krishnakumar, B.; Subaashini, M.; Kumar, E.G.; Arthi, R. Power flow based contingency analysis using fuzzy logic. *Procedia Eng.* **2012**, *38*, 3603–3613. [CrossRef]
9. Ozdemir, A.; Singh, C. Fuzzy Logic Based MW Contingency Ranking against Masking Problem. In Proceedings of the 2001 IEEE Power Engineering Society Winter Meeting, Columbus, OH, USA, 28 January–1 February 2001; pp. 504–509.
10. Marannino, P.; Berizzi, A.; Merlo, M.; Demartini, G. A rule-based fuzzy logic approach for the voltage collapse risk classification. *Proc. IEEE Power Eng. Soc. Transm. Distrib. Conf.* **2002**, *2*, 876–881. [CrossRef]
11. Halilčević, S.S.; Gubina, F.; Gubina, A.F. The uniform fuzzy index of power system security Suad. *Eur. Trans. Electr. Power* **2010**, *20*, 785–799. [CrossRef]
12. Halilčević, S.S.; Gubina, F.; Gubina, A.F. The composite fuzzy reliability index of power systems. *Eng. Appl. Artif. Intell.* **2011**, *24*, 1026–1034. [CrossRef]
13. Kalyani, S.; Swarup, K. Supervised fuzzy C-means clustering technique for security assessment and classification in power systems. *Int. J. Eng. Sci. Technol.* **2010**, *2*, 175–185. [CrossRef]
14. Zhao, J.; Zhou, Y.; Shuo, L. A Situation Awareness Model of System Survivability Based on Variable Fuzzy Set. *TELKOMNIKA Indones. J. Electr. Eng.* **2012**, *10*, 2239–2246. [CrossRef]
15. Fan, S.; Lin, J.; Zhang, T.; Dong, G.; Liu, X. Temporal and Spatial Distribution of Power System Voltage based on Generalized Regression Neural Network. *ISPEC* **2019**, 1891–1896. [CrossRef]
16. Diao, R.; Vittal, V.; Logic, N. Design of a real-time security assessment tool for situational awareness enhancement in modern power systems. *IEEE Trans. Power Syst.* **2010**, *25*, 957–965. [CrossRef]
17. Özdemir, A.; Lim, J.Y.; Singh, C. Post-outage reactive power flow calculations by genetic algorithms: Constrained optimization approach. *IEEE Trans. Power Syst.* **2005**, *20*, 1266–1272. [CrossRef]
18. Javan, D.S.; Mashhadi, H.R.; Rouhani, M. A fast static security assessment method based on radial basis function neural networks using enhanced clustering. *Int. J. Electr. Power Energy Syst.* **2013**, *44*, 988–996. [CrossRef]
19. Sidhu, T.S. Contingency screening for steady-state security analysis by using FFT and artificial neural networks. *IEEE Trans. Power Syst.* **2000**, *15*, 421–426. [CrossRef]
20. Luitel, B.; Venayagamoorthy, G.K. Cellular computational networks-A scalable architecture for learning the dynamics of large networked systems. *Neural Netw.* **2014**, *50*, 120–123. [CrossRef]
21. Wang, S.; Gao, W.; Meliopoulos, A.P.S. An alternative method for power system dynamic state estimation based on unscented transform. *IEEE Trans. Power Syst.* **2012**, *27*, 942–950. [CrossRef]
22. Hasala Dharmawardena, G.K.V. Cellular Computational Network for Distributed Power Flow Inferencing in Electric Distribution Systems. In Proceedings of the IJCNN, Budapest, Hungary, 14–19 July 2019; pp. 1–8.
23. Rahman, M.A.; Venayagamoorthy, G.K. Scalable Cellular Computational Network Based WLS State Estimator for Power Systems. In Proceedings of the 2015 Clemson University Power Systems Conference, Clemson, SC, USA, 10–13 March 2015.
24. Rahman, M.A.; Venayagamoorthy, G.K. Power System Distributed Dynamic State Prediction. In Proceedings of the 2016 IEEE Symposium Series on Computational Intelligence, Athens, Greece, 6–9 December 2016; pp. 1–6.
25. Balasubramaniam, K.; Luitel, B.; Venayagamoorthy, G.K. A scalable wide area monitoring system using cellular neural networks. *Proc. Int. Jt. Conf. Neural Netw.* **2012**, 10–15. [CrossRef]
26. Balasubramaniam, K.; Venayagamoorthy, G.K.; Watson, N. Cellular neural network based situational awareness system for power grids. *Proc. Int. Jt. Conf. Neural Netw.* **2013**. [CrossRef]
27. Wu, L.; Venayagamoorthy, G.K.; Harley, R.G.; Gao, J. Cellular Computational Networks Based Voltage Contingency Ranking Regarding Power System Security. In Proceedings of the Clemson University Power Systems Conference, Charleston, SC, USA, 4–7 September 2018.
28. Wu, L.; Venayagamoorthy, G.K.; Gao, J. Cellular Computational Networks for Distributed Prediction of Active Power Flow in Power Systems under Contingency. In Proceedings of the Proceedings of 2019 IEEE PES Innovative Smart Grid Technologies Europe, Bucharest, Romania, 29 September–2 October 2019; pp. 1–4.
29. Shan, J. A platform for validation of FACTS models. *IEEE Trans. POWER Deliv.* **2006**, *21*, 484–491. [CrossRef]
30. Jaeger, H. The "echo state" approach to analysing and training recurrent neural networks–with an Erratum note. *GMD* **2001**, *148*, 13.
31. IEEE. *IEEE Technical Report IEEE/PES Voltage Stability of Power Systems: Concepts, Analytical Tools, and Industry Experience*; IEEE: New York, NY, USA, 18 August 1990.
32. Stott, B.; Alsac, O.; Monticelli, A.J. Security Analysis and Optimization. *Proc. IEEE* **1987**, *75*, 1623–1644. [CrossRef]
33. Liang, J.J.; Suganthan, P.N. Dynamic Multi-Swarm Particle Swarm Optimizer. In Proceedings of the IEEE on Swarm Intelligence Symposium, Pasadena, CA, USA, 8–10 June 2005; pp. 124–129.