

# **Deep Learning**

## **Violation Detection in Power System Dynamic Security Assessment**

**Guilherme Mota**

Electrical Engineering Program

Instituto Alberto Luiz Coimbra de Pós-Graduação e Pesquisa de Engenharia  
Universidade Federal do Rio de Janeiro

08/12/2025

**1. What is DSA and why do we use it?**

**2. Data Extraction**

**3. Models and Results**

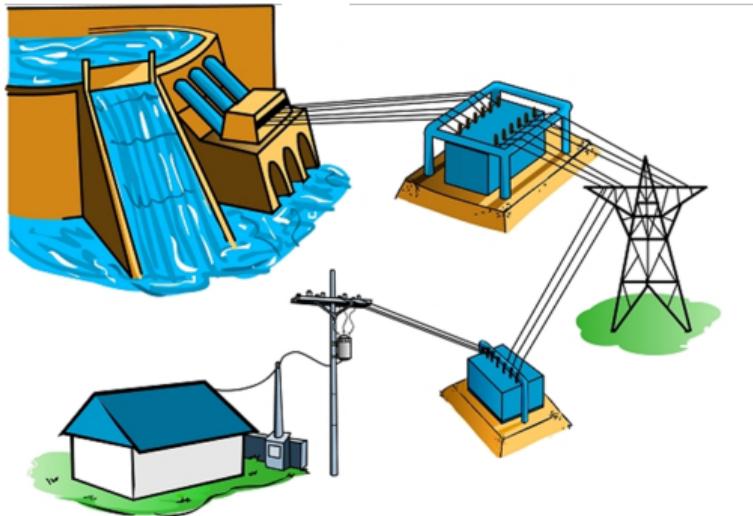
**4. Conclusions and Next Steps**

**5. References**

## **What is DSA and why do we use it?**

---

# Power System Operation



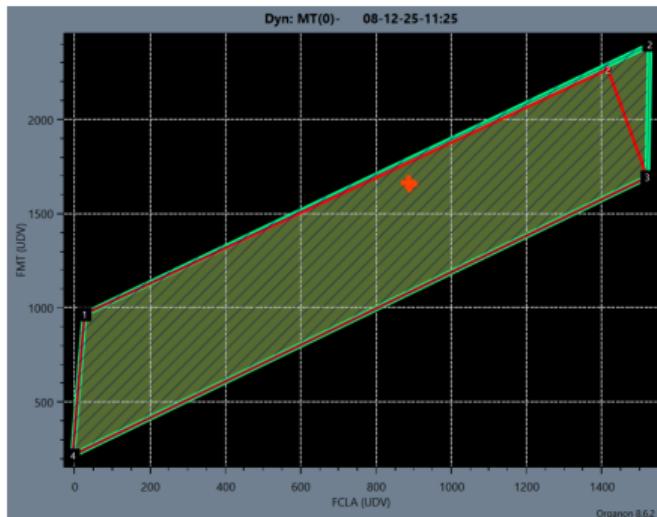
## Objective:

- ▷ Ensure a reliable supply of electricity to consumers while continuously balancing **cost efficiency** and **systemic security**

# Security Assessment

This assessment is performed online and offline through extensive simulations:

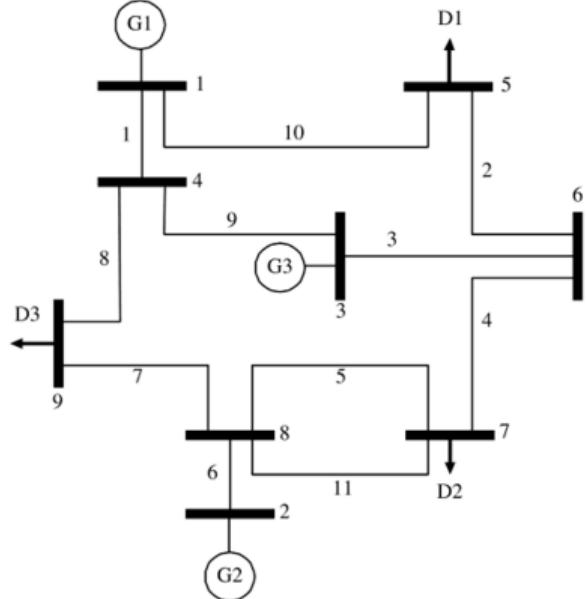
- ▷ Analytical tools are used to simulate the system's response to probable contingencies (problems)
- ▷ The simulations are time-consuming and computationally expensive
- ▷ **Motivation:** What if we could employ a model capable of identifying violations *before* running simulations?



# Literature Review

Deep learning approaches to DSA typically rely on benchmark test systems, using:

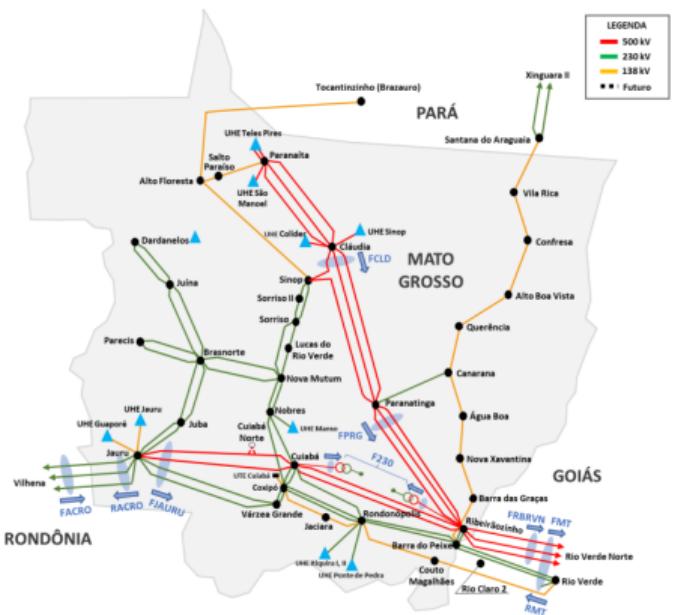
- ▷ **Features:** steady-state  $V\theta$ ,  $PQ$  power flow, and  $PQ$  load and generation
- ▷ **Label:** binary classification of security
- ▷ **Models:** CNN [1, 2, 3, 4], AE [5, 6], LSTM [7, 3] and GAN [8, 9]



## Data Extraction

---

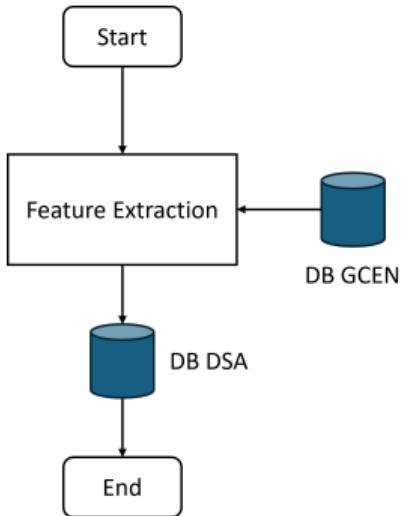
# Security Region of Mato Grosso (MT)



Extracted features from steady-state cases to construct DB DSA:

- ▷ Buses  $V\theta$
- ▷ Transmission lines MVA flow
- ▷ Transformers tap position
- ▷ Systemic fluxes (MW)
- ▷ Active power generation (MW)
- ▷ Aggregated  $PQ$  consumption, losses and exportation

# Feature Extraction and Data



Voltage and thermal violation labels were obtained from DB GCEN, based on online simulations performed in real-time

Within the merged dataset, we have:

- ▷ 322 features across approximately 10k instances
- ▷ Class imbalance ratios of 8 : 2 (voltage) 7 : 3 (thermal)

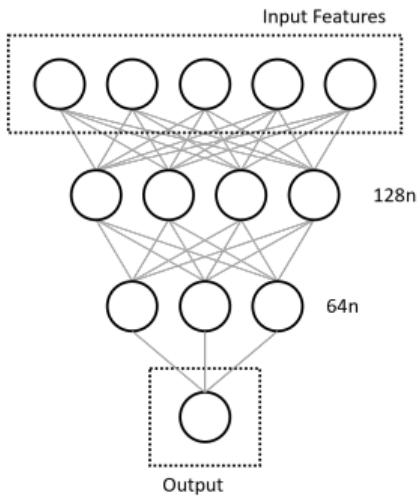
For model development, the following was adopted:

- ▷ Dataset split into 70% (TR), 15% (V) and 15% (TS)
- ▷ Accuracy, precision and recall were chosen as the figures of merit

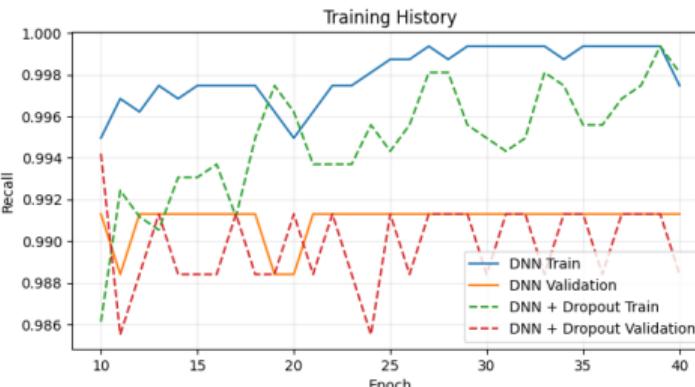
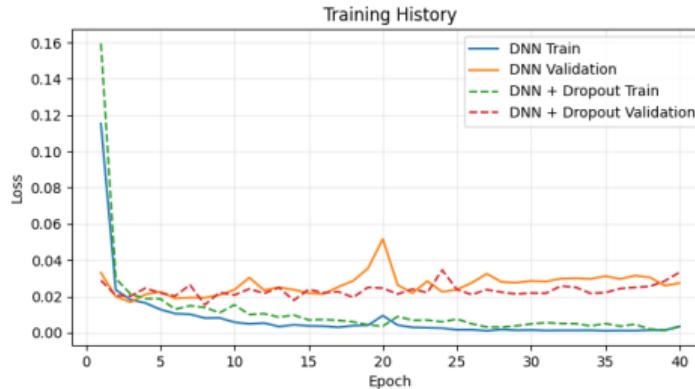
## Models and Results

---

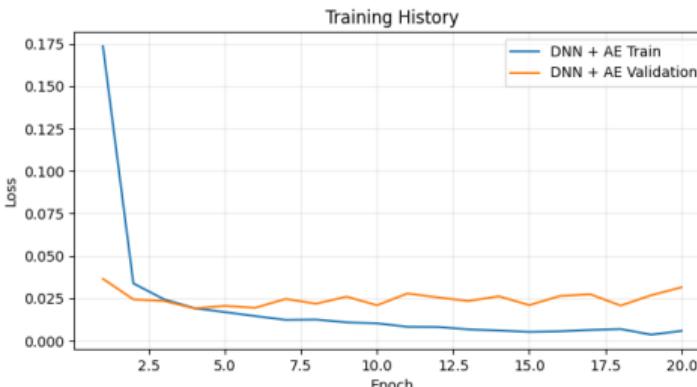
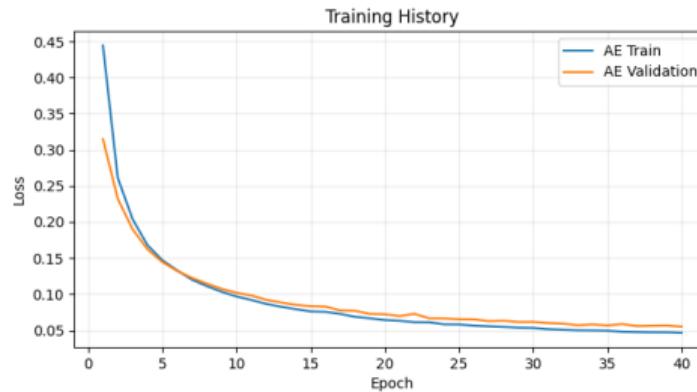
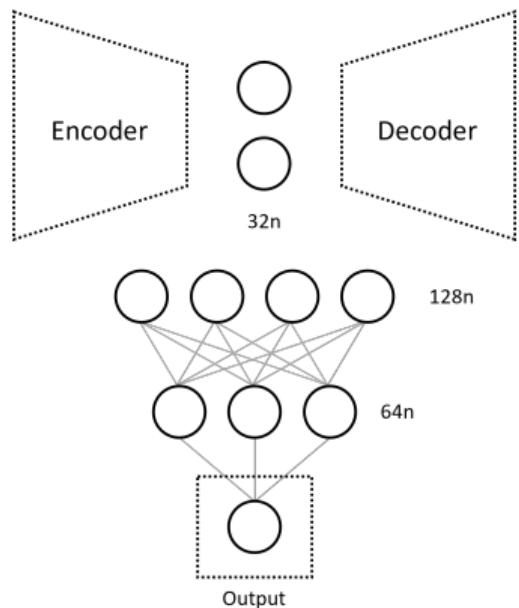
# Deep Neural Network



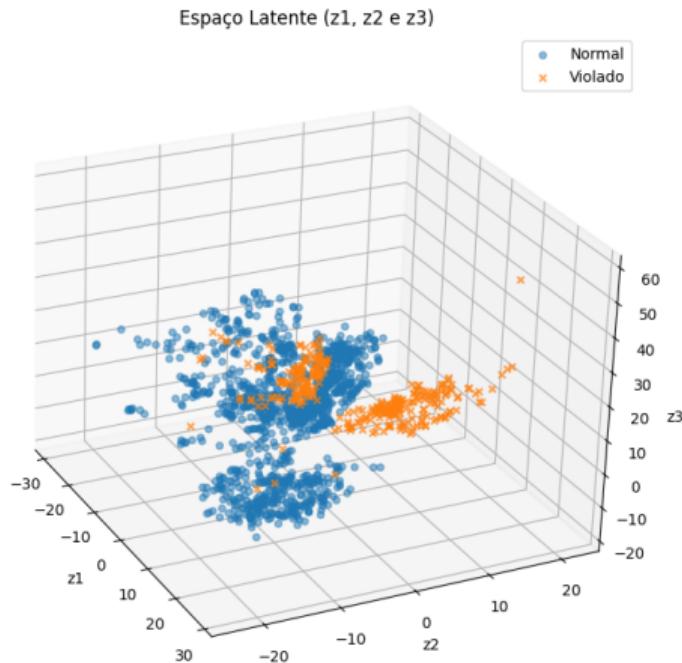
- ▷ ReLU activation between layers
- ▷ Optional insertion of Dropout regularization



# Deep Neural Network with Autoencoder



# Check Autoencoder Latent Space



AE with a 3-neuron layer to:

- ▷ Project data into a 3D latent space
- ▷ Visualize how the model organizes operating points based on learned representations

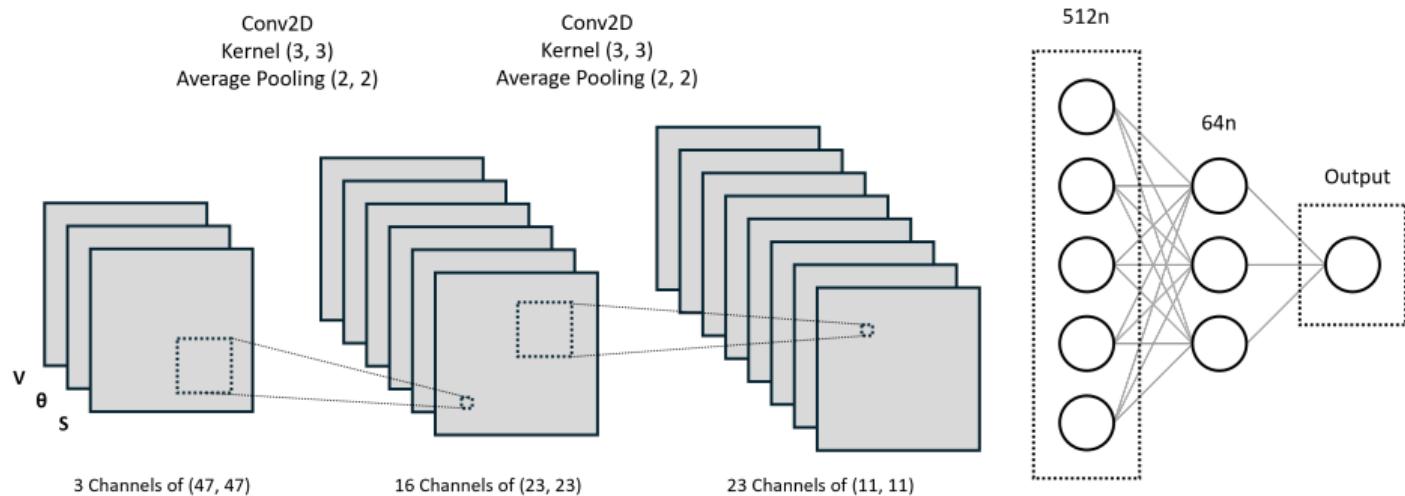
# Power Grid as Images

	Barra i	Barra j	
Barra i	$B_i$	$\dots$	$\Delta B_{ji}$
	$\vdots$	$\ddots$	$\vdots$
Barra j	$\Delta B_{ij}$	$\dots$	$B_j$
	$\dots$		$\ddots$

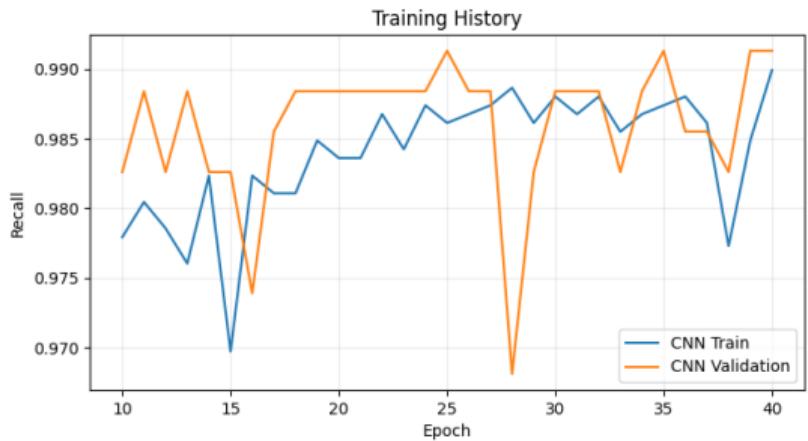
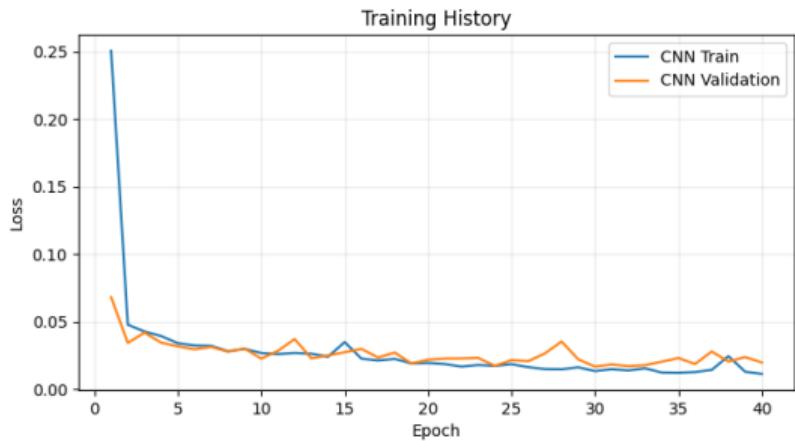
Represent the power system's meshed grid as matrix-based images:

- ▷ Each image has three channels: voltage magnitude ( $V$ ), voltage angle ( $\theta$ ), and apparent power flow ( $S$ )
- ▷ The grid topology becomes a spatial pattern, which enables the use of CNNs

# Convolutional Neural Network



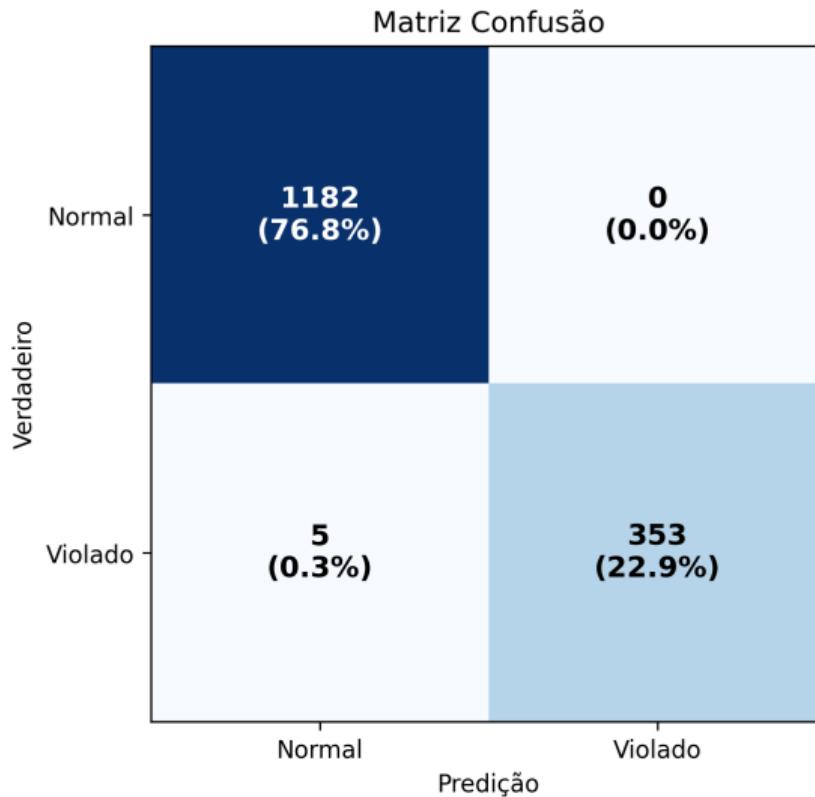
# Convolutional Neural Network



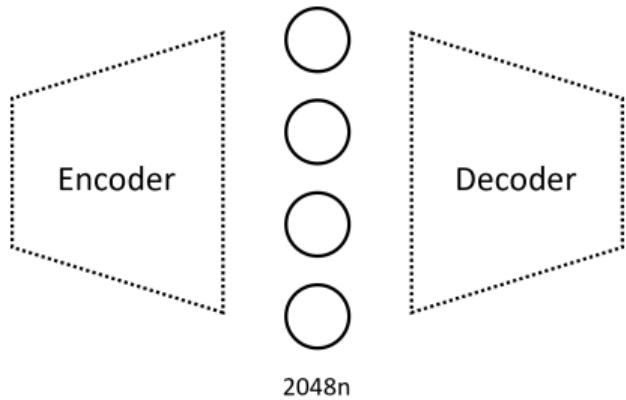
# Summary

<b>Model</b>	<b>Accuracy</b>	<b>Precision</b>	<b>Recall</b>
DNN	99.59% $\pm$ 0.17%	99.66% $\pm$ 0.75%	98.54% $\pm$ 0.16%
DNN with Dropout	99.65% $\pm$ 0.05%	99.89% $\pm$ 0.31%	98.60% $\pm$ 0.43%
DNN with AE	99.60% $\pm$ 0.20%	99.60% $\pm$ 0.60%	98.64% $\pm$ 0.32%
CNN	99.61% $\pm$ 0.10%	99.76% $\pm$ 0.16%	98.47% $\pm$ 0.55%

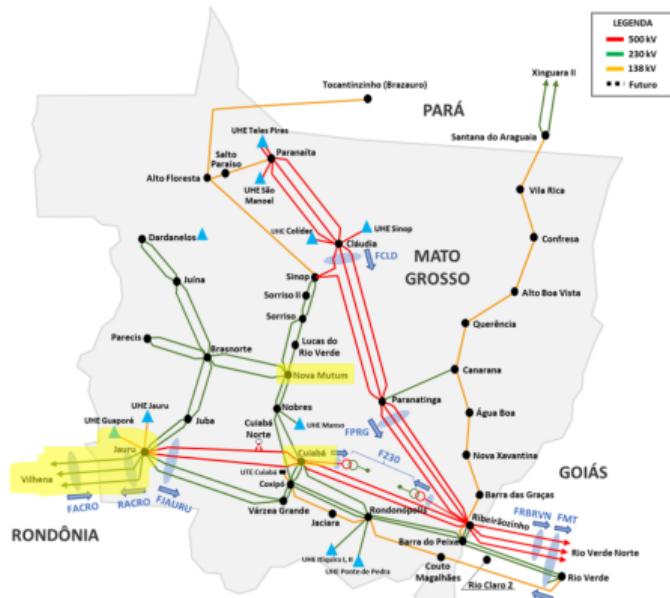
# Summary



# Evaluate Latent Impact with SAE



- ▷ Enforcing sparsity in the latent space through a KL regularization term
  - ▷ Identifying the latent neurons most frequently activated during violations
  - ▷ Assessing the impact on reconstruction



## **Conclusions and Next Steps**

---

# Conclusions and Next Steps

## Conclusions:

- ▷ The proposed models successfully predicted security violations in DSA using only local steady-state measurements
- ▷ This enables online estimation of security regions in a fraction of the simulation time, significantly accelerating preventive decision-making

## Next Steps:

- ▷ Integrate the proposed models with real-time measurements to enable online security assessment
- ▷ Extend the analysis to additional security regions

## References

---

# References I

- [1] M. Ramirez-Gonzalez, F. R. Segundo Sevilla, and P. Korba, “Convolutional neural network based approach for static security assessment of power systems,” in *2021 World Automation Congress (WAC)*, pp. 106–110, 2021.
- [2] J.-M. H. Arteaga, F. Hancharou, F. Thams, and S. Chatzivasileiadis, “Deep learning for power system security assessment,” in *2019 IEEE Milan PowerTech*, pp. 1–6, 2019.
- [3] G. Gong, N. K. Mahato, H. He, H. Wang, Y. Jin, and Y. Han, “Transient stability assessment of electric power system based on voltage phasor and cnn-lstm,” in *2020 IEEE/IAS Industrial and Commercial Power System Asia (ICPS Asia)*, pp. 443–448, 2020.

## References II

- [4] G. Justin, "A comparative analysis of machine learning methods for power system transient stability," in *2024 6th Global Power, Energy and Communication Conference (GPECOM)*, pp. 445–449, 2024.
- [5] T. Zhang, M. Sun, J. L. Cremer, N. Zhang, G. Strbac, and C. Kang, "A confidence-aware machine learning framework for dynamic security assessment," *IEEE Transactions on Power Systems*, vol. 36, no. 5, pp. 3907–3920, 2021.
- [6] M. Sun, I. Konstantelos, and G. Strbac, "A deep learning-based feature extraction framework for system security assessment," *IEEE Transactions on Smart Grid*, vol. 10, no. 5, pp. 5007–5020, 2019.

# References III

- [7] N. K. Mahato, J. Dong, C. Song, Z. Chen, N. Wang, H. Ma, and G. Gong, “Electric power system transient stability assessment based on bi-lstm attention mechanism,” in *2021 6th Asia Conference on Power and Electrical Engineering (ACPEE)*, pp. 777–782, 2021.
- [8] Q. Deng, C. Luo, Y. Wu, G. Li, X. Ling, Z. Liang, Y. Zeng, C. Qin, and J. Ren, “Data augmentation for dynamic security assessment based on hybrid model-data driven approach,” in *2025 IEEE International Conference on Power and Integrated Energy Systems (ICPIES)*, pp. 206–210, 2025.
- [9] C. Ren and Y. Xu, “A fully data-driven method based on generative adversarial networks for power system dynamic security assessment with missing data,” *IEEE Transactions on Power Systems*, vol. 34, no. 6, pp. 5044–5052, 2019.

**Thank you for your attention**

**Guilherme Mota**

Electrical Engineering Program  
Instituto Alberto Luiz Coimbra de Pós-Graduação e Pesquisa de Engenharia  
Universidade Federal do Rio de Janeiro

08/12/2025