AI-enabled Data-driven tools for Proactive Dynamic Security Analysis of Power Transmission Systems

Alfredo Vaccaro, FIEEE

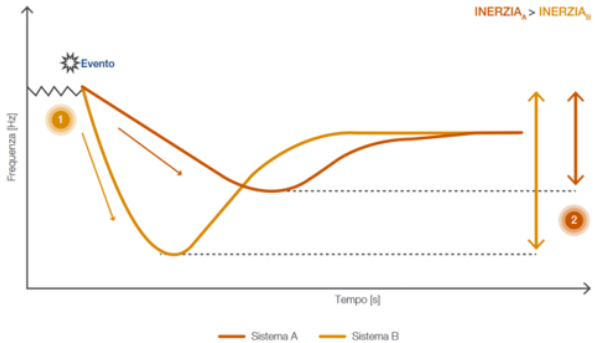
Chair of the Power System Research Group - University of Sannio - Benevento - Italy
Chair of the IEEE Power System Operation, Planning and Economics Committee - Technologies and Innovation SC

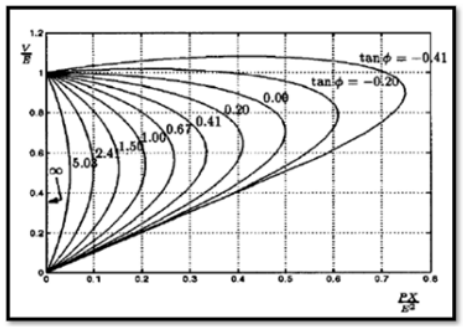
September 9, 2025

Motivations

Dercarbonized power systems features:

- de-commitment of large conventional synchronous generators;
- increasing deployment of inverter-based renewable units;
- continuous growth of energy-intensive loads (e.g. AI data-centers);
- increasing number of network interconnections;
- complex dynamics of the electricity markets.





Motivations

Dercarbonized power systems operation:

- drastic contraction of the flexibility resources for real-time balancing;
- abrupt reduction of the system inertia;
- sensible growth of complex operational uncertainties.

All these phenomena are raising the grid vulnerability to dynamic perturbations, pushing power systems to frequently operate under severe stressed conditions and closer to the stability margins.

Research Activities

Enhancing the Dynamic Security Assessment (DSA) tools by data-driven models is recognized as the most promising enabling technology to preemptive detect critical contingencies, and promptly identify preventive/corrective control actions.

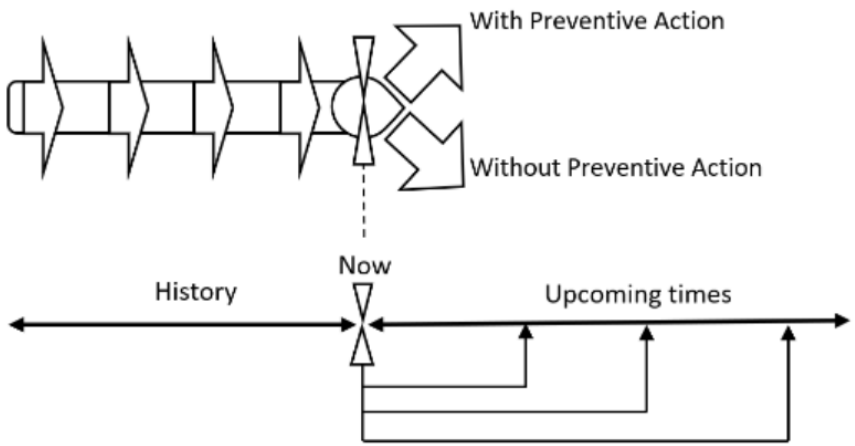
AI-based DSA

A wide spectrum of machine learning techniques has been recently proposed in the literature to surrogate the most time-consuming DSA functions by inferring from historical data-sets the hidden relationships between the state variables and the corresponding grid security state. These phasor data-driven DSA surrogates allows to:

- avoid the need for repetitively solving high-fidelity dynamic models;
- promptly detect critical patterns of the state variables triggering specific dynamic contingencies;
- enhancing the situational awareness of the DSA tools for TSOs.

Proactive DSA

Enhancing the DSA tools by proactivity functions, which allow predicting on multiple time horizons the power system vulnerability to critical dynamic contingencies.



Research Gaps

Open Problems

Deploying conventional phasor-based surrogate models for proactive DSA tools is not a viable solution due to:

- the difficulties in forecasting the bus voltage phasor profiles,
- the need to process a large number of input variables, which are characterized by complex statistical correlations.

These limitations could hinder the generalization capability of the proactive functions.

Figure 1: From Phasor-Based Analysis to Market Outcome-Oriented Approaches

Proposed Approach

Research Goals

Conceptualizing, developing and experimental testing of a phasor-data agnostic framework that leverages electricity market time-series for multi-step-ahead system security state classification.

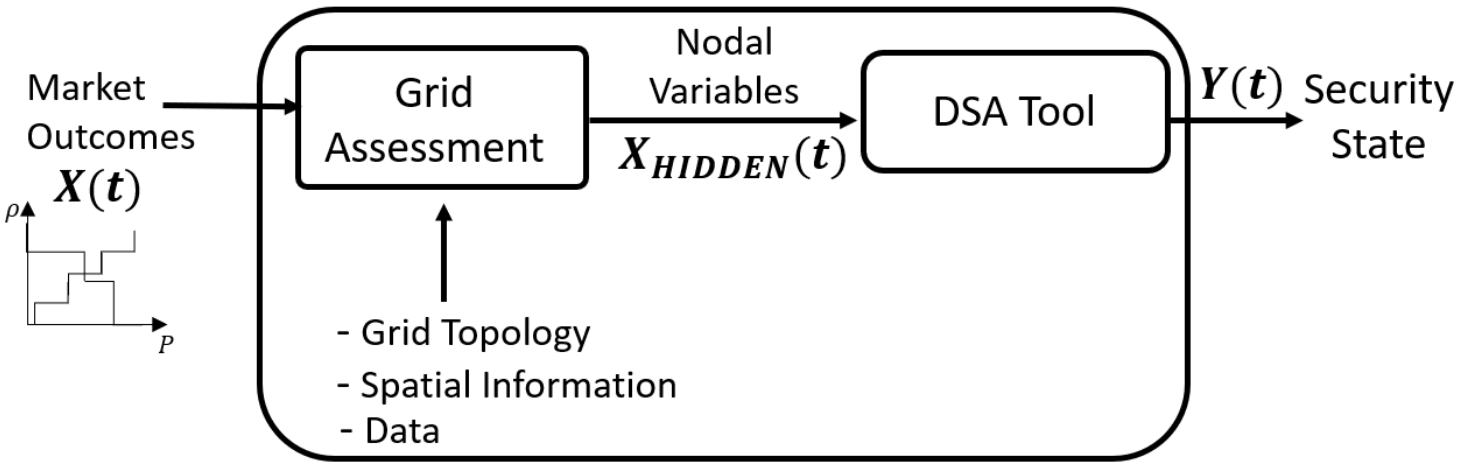


Figure 2: Scheme of the Proposed Methodology

Proposed Approach

Research Insights

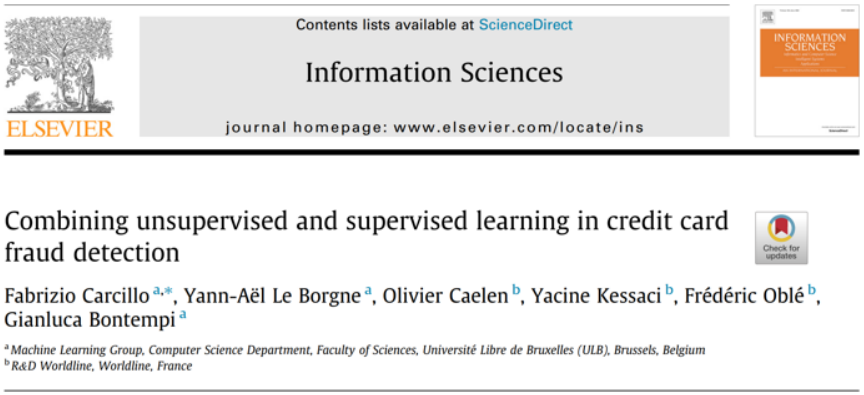
Knowledge discovery from electricity market time-series is expected to bring the following benefits to proactive DSA:

- they can be effectively predicted over several time frames;
- they are aggregated on a simplified equivalent power system;
- their evolution rules power system operation.

Expected Contributions

- Hybrid "best of both worlds" approach that enriches the supervised models with features derived from anomaly detection algorithms.
- Conceptualize a comprehensive, cost-sensitive analysis to guide model selection.

Enabling Methodologies



Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

Combining unsupervised and supervised learning in credit card fraud detection

Fabrizio Carcillo [a,*], Yann-Aël Le Borgne [a], Olivier Caelen [b], Yacine Kessaci [b], Frédéric Oblé [b], Gianluca Bontempi [a]

[a] Machine Learning Group, Computer Science Department, Faculty of Sciences, Université Libre de Bruxelles (ULB), Brussels, Belgium
[b] R&D Worldline, Worldline, France

2024 IEEE International Conference on Web Services (ICWS)

Assessing adversarial attacks in real-world fraud detection

Daniele Lunghi*, Alkis Simitsis†and Gianluca Bontempi§
Université Libre de Bruxelles, University of Athens, and Athena RC
Bruxelles, Belgium
*daniele.lunghi@ulb.be, daniele.lunghi@arc.gr
†alkis@athenarc.gr
§gianluca.bontempi@ulb.be

Smart Grids and Sustainable Energy (2025) 10:47
https://doi.org/10.1007/s40866-025-00276-y

RESEARCH

Enabling Methodologies for Discovering the Hidden Relationships Between the Electricity Market Outcomes and the Dynamic Power System Security

Silvia Iuliano[1] · Giorgio Maria Giannuzzi[2] · Francesco Del Pizzo[2] · Alfredo Vaccaro[1]

Received: 1 April 2025 / Accepted: 9 June 2025

Figure 3: Related Works

Problem Formulation

Mathematical Preliminaries

Let the dataset be denoted by $\mathcal{D} = \{(X_t, y_t)\}_{t=1}^{T}$, where T is the total number of observations. We have:

- $X_t \in \mathbb{R}^d$: a vector of d features (e.g., zonal load, power flows, generation levels).
- $y_t \in \{0, 1\}$: a binary label representing the system's security state at time t.

The core task is to predict the sequence of future security states $\{y_{t+1}, y_{t+2}, \ldots, y_{t+H}\}$.

To solve this problem we deploy two computing paradigms:

- Direct
- Indirect

Power System Research Group

Direct Forecasting Paradigm

Main insights

This approach involves training a single model for each forecast horizon $h \in \{1, \ldots, H\}$. We construct several distinct feature vectors for each time step t, all based on a lag window of size L.

- The most fundamental representation is the lagged feature vector, $\mathbf{x}_{t,\text{lag}}$. It captures **the direct temporal sequence** of the system's state variables, and we call it `Lagged`.

$$\mathbf{x}_{t,\text{lag}} = (X_{t-L+1}, X_{t-L+2}, \ldots, X_t) \in \mathbb{R}^{L \times d} \tag{1}$$

- A second approach, that we call `Stats`, is to create a statistical feature vector, $\mathbf{x}_{t,\text{stats}}$, which summarizes recent trends and volatility. It is constructed by applying a set of K statistical operators $\mathcal{S} = \{s_1, \ldots, s_K\}$ to a rolling window of recent data L for each of the d features. Let Ψ_{stats} be this transformation.

$$\mathbf{x}_{t,\text{stats}} = \Psi_{\text{stats}}(X_{t-W_s+1}, \ldots, X_t) \in \mathbb{R}^{d \times K} \tag{2}$$

Hybrid Computing Paradigm

Main insights

- A key **novelty** of this approach **is the integration of unsupervised learning into the supervised classification framework**, according to a **"best of both worlds"** approach.
- While supervised models excel at learning patterns from historical data, they may struggle with novel or unseen system states that precede an insecure event. Unsupervised anomaly detection, in contrast, is designed to identify such unusual patterns without relying on labels.

Hybrid Computing Paradigm

Unsupervised Anomaly Features

The following models are used to generate the anomaly scores:

- Principal Component Analysis;
- Isolation Forest:
- Gaussian Mixture Model;
- Elliptic Envelope;
- Local Outlier Factor;
- One-Class Support Vector Machines.

These models generate anomaly scores for the contemporary feature vectors. By feeding these scores as features into our supervised classifiers, we aim to build a more robust and adaptive security assessment tool.

Ensemble Methods

We evaluate several modeling approaches based on these feature vectors, as shown in Tab. 1.

- `BoB-concat`, where all distinct feature vectors are concatenated into a single, high-dimensional vector.

$$\mathbf{x}_{t,\text{merged}} = [\mathbf{x}_{t,\text{lag}} \parallel \mathbf{x}_{t,\text{stats}} \parallel \mathbf{x}_{t,\text{naive}} \parallel \mathbf{x}_{t,\text{event}} \parallel \mathbf{x}_{t,\text{anomaly}}] \quad (3)$$

$$\hat{y}_{t+h,\text{set}} = f_h^{\text{set}}(\mathbf{x}_{t,\text{merged}})$$

- `BoB-meta`, this is a two-level ensemble technique where a Level 1 meta-model, f_h^{meta}, learns to combine the predictions of the Level 0 base models.

$$\mathbf{z}_{t+h,\text{meta}} = [\hat{y}_{t+h,\text{lag}}, \hat{y}_{t+h,\text{stats}}, \hat{y}_{t+h,\text{naive}}, \hat{y}_{t+h,\text{event}}, \hat{y}_{t+h,\text{anomaly}}] \quad (4)$$

$$\hat{y}_{t+h} = f_h^{\text{meta}}(\mathbf{z}_{t+h,\text{meta}})$$

Indirect Forecasting Paradigm

Main insights

We investigate two distinct methods

- Indirect MIMO Strategy:

$$\hat{\mathbf{x}}_{t+h,\text{Ind-MIMO}} = g_h(\mathbf{x}_{t,\text{lag}}) \tag{5}$$

$$\hat{\mathbf{x}}_{t+h-1} = (X_{t-L+h}, \ldots, X_t, \hat{X}_{t+1}, \ldots, \hat{X}_{t+h-1}) \tag{6}$$

$$\hat{y}_{t+h} = c(\hat{\mathbf{x}}_{t+h-1}) \tag{7}$$

- Recursive Indirect Strategy: The forecast for step h is then generated by recursively applying the regressor:

$$\hat{X}_{t+h} = g_{\text{rec}}(\hat{\mathbf{x}}'_{t+h-1}) \tag{8}$$

Power System Research Group

Table 1: Summary of Forecasting Strategies and Feature Sets

Strategy	**Description**
Direct Paradigm Feature Sets	
`Lagged`	Raw temporal sequence of market variables
`Stats`	Statistical summaries of recent history
`Naive`	Historical sequence of security state labels
`Event`	Engineered features from event dynamics
`Anomaly`	Unsupervised anomaly scores of current state
Best of Both Worlds Methods	
`BoB-concat`	Concatenation of all feature sets
`BoB-meta`	Stacked ensemble of models on each set
Indirect Paradigm Strategies	
`Ind-MIMO`	Direct MIMO forecasting of features
`Ind-REC`	Recursive forecasting of features

Experimental Setup

The dataset consists of 51,998 rows, with 21 continuous features and 1 output variable. The number of zeroes (safe states) is 51,366, and the number of ones (contingencies) is 642.

Table 2: Features adopted in this study

Features	Type	N° Feats.
Power load	C	7
WP production	C	7
Inter-area PFs	C	7

Experimental Setup

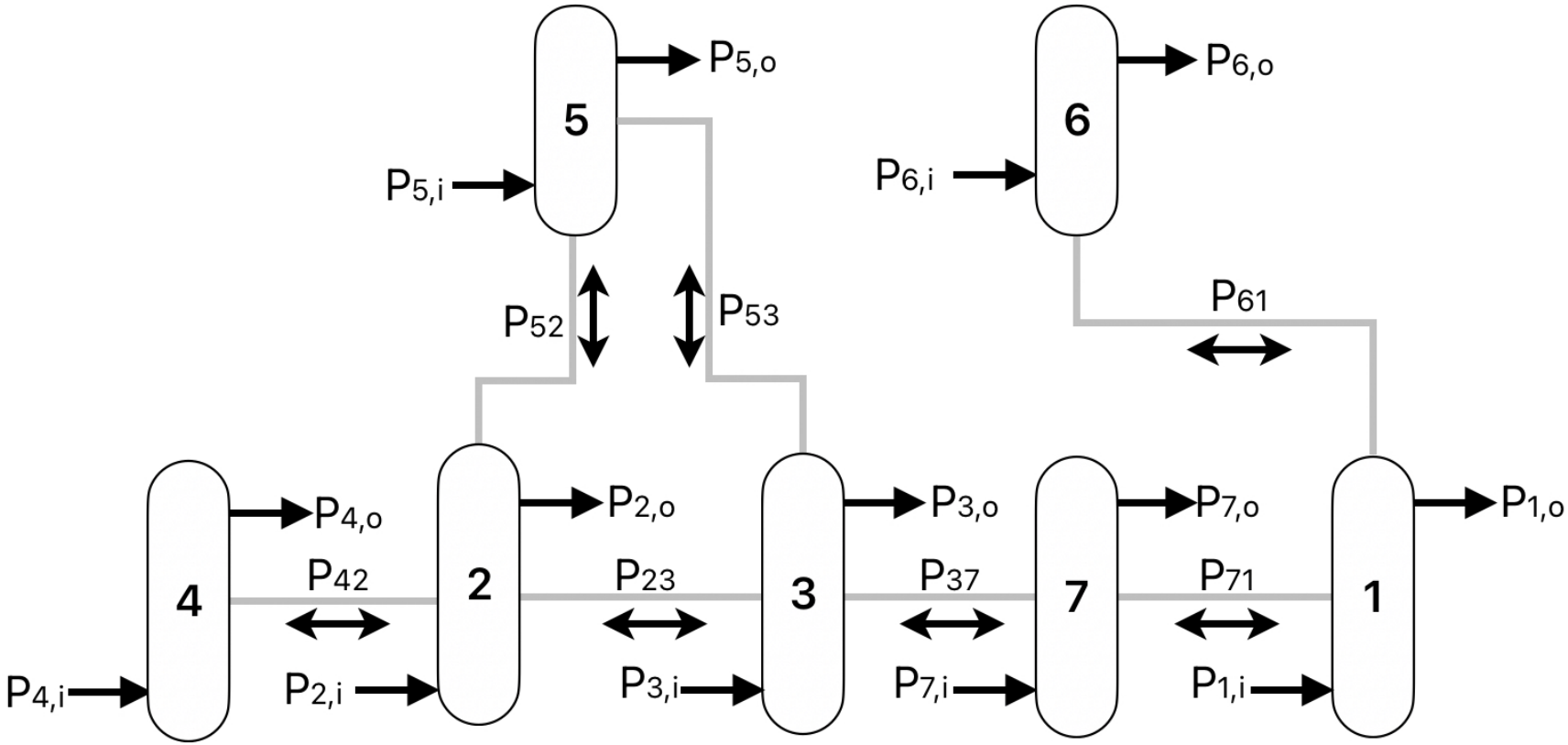


Figure 4: The power system used for settling the Italian Electricity Market

Experimental Setup

Metrics

- Matthews Correlation Coefficient (unbalanced datasets);
- Recall;
- Receiver Operating Characteristic - Area Under Curve (ROC AUC);
- Average Precision.

Cross Validation

- To ensure a robust evaluation and mitigate the risk of overfitting, we employ a time-series cross-validation scheme that respects the temporal ordering of the data.
- The choice of the number of folds (k) was critical due to the severe class imbalance in our dataset, where insecure states ($y = 1$) are rare events.

Results and Analysis

- We conducted a comparison of all proposed forecasting strategies across a 2.5-hour forecast horizon.
- Furthermore, a cost-sensitive analysis provides clear, actionable guidance on model selection for real-world deployment.

Results and Analysis

The Dominance and Decay of State Persistence:

- The most striking result is the exceptional short-term performance of the strategies that rely heavily on the recent history of security labels: `Naive` and `X_event`.
- At the one-step-ahead horizon (H=1), these models are the undisputed champions:
  - `Naive` model by using the least 20 binary labels, achieves an Average Precision of 0.500.
  - `X_event` model by using the least 20 binary labels, achieves an Average Precision of 0.514.
- This dramatically outperforms models based on market variables, confirming that the system state exhibits strong short-term persistence.

The Dominance and Decay of State Persistence:

- However, this simplistic approach proves brittle. As the forecast horizon extends to H=10, the performance of these models decays rapidly.

Table 3: Performance of Persistence-Based Models. Comparison at short (H=1) and long (H=10) horizons highlights their initial dominance and rapid performance decay.

Model	H	ROC AUC	Avg. Precision	F1-Score
`Naive`	1	0.923 ± 0.016	**0.500 ± 0.074**	**0.353 ± 0.033**
	10	0.748 ± 0.076	0.134 ± 0.052	0.201 ± 0.063
`X_event`	1	**0.934 ± 0.014**	**0.514 ± 0.107**	0.213 ± 0.097
	10	0.789 ± 0.056	0.120 ± 0.023	0.116 ± 0.042

Comparing Supervised and Unsupervised Feature Engineering

Robustness of Indirect and Ensemble Strategies

- The indirect strategies and the ensemble models were designed to be more robust over longer forecast horizons.
- The BoB-concat model, which concatenates all feature sets, emerged as a consistently strong performer.
- The results confirm that a combination of supervised and unsupervised learning yields a more robust and adaptive security assessment framework.
- This “best of both worlds” approach proved particularly effective in our ensemble models, especially over longer forecast horizons where simple state persistence fails.

Experimental Results

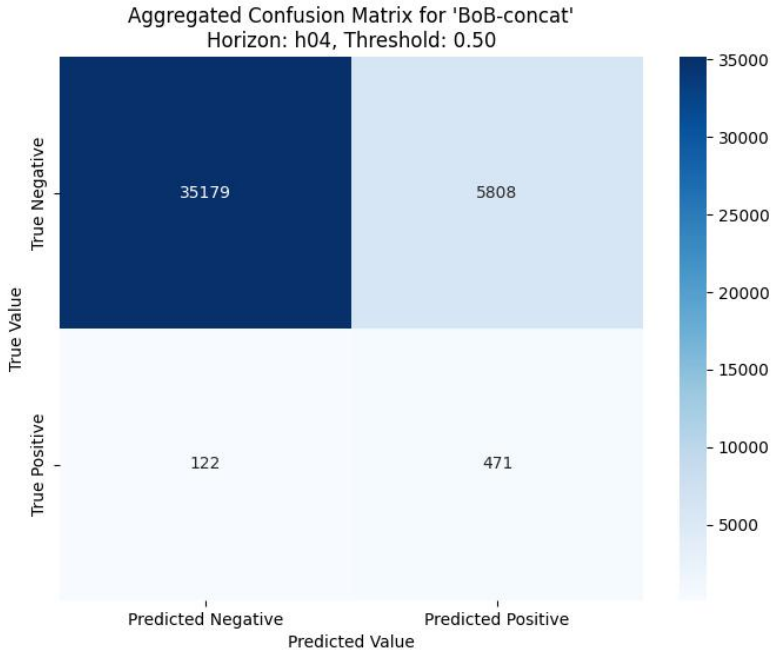


Figure 5: Confusion matrix which represents the performance of the most effective `BoB-concat` model in a multi-step prediction task, specifically at the fourth future time step (t+4)

Experimental Results

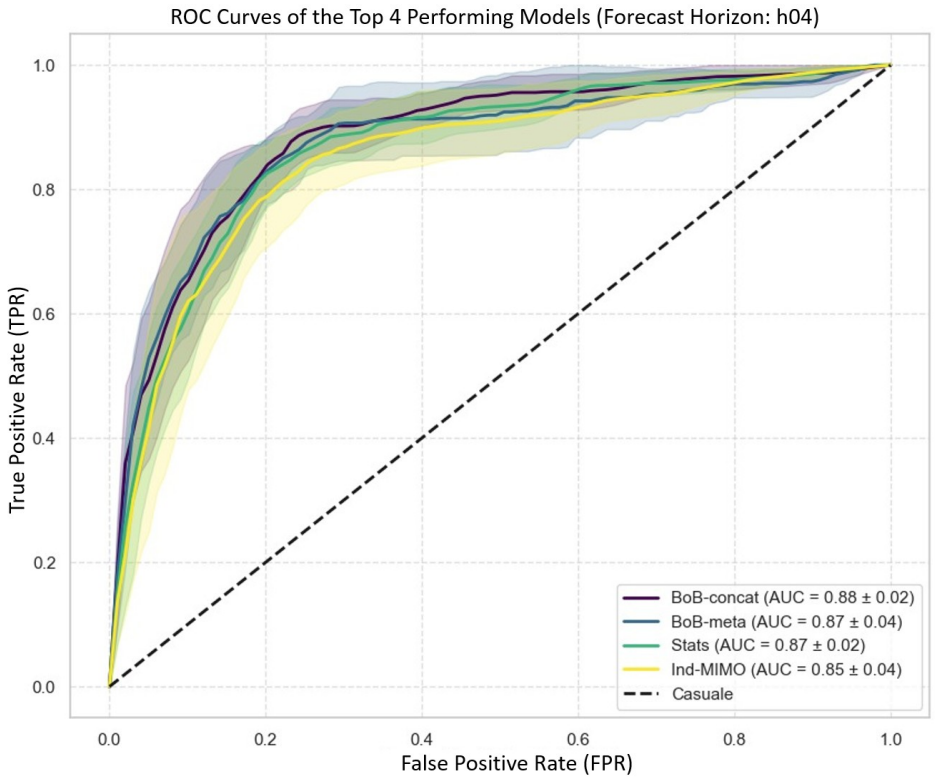


Figure 6: Receiver-operating characteristic (ROC) curves for the four top-performing models at time step t+4

Experimental Results

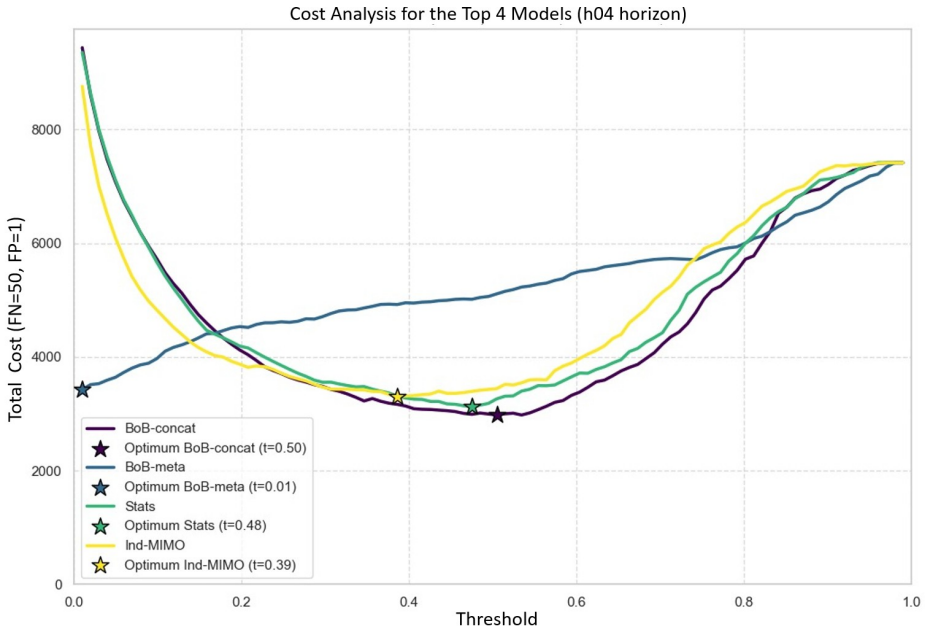


Figure 7: Cost Analysis for the top-performing 4 models at time step t+4

Conclusions

- We developed and validated a novel data-driven framework for the proactive dynamic security assessment by using market outcomes.
- The results confirm that a hybrid approach, which combines supervised learning with unsupervised anomaly detection, yields a more robust and adaptive security assessment.
- This fusion allows the system not only to learn from historical insecurity patterns but also to identify novel system deviations that may precede a critical event.

UNISANNIO PSRG Power System Research Group

Future works

Future research can further enhance model capabilities through several avenues, including:

- Exploiting Spatio-Temporal Dependencies (in progress);
- Multi-Modal Data Fusion;
- Enhancing Interpretability and Trust.

UNISANNIO PSRG Power System Research Group

Alfredo Vaccaro
University of Sannio
Benevento
Italy

vaccaro@unisannio.it

UNISANNIO PSRG
Power System Research Group