Machine Learning to Prevent Blackouts in Power Systems

Jochen Cremer
Delft University of Technology

Session: Application of Big Data and AI/ML in monitoring, operations, planning and protection

Credits

Federica Bellizio

Al-Amin Bugaje

Wangkun Xu

Dawei Qiu

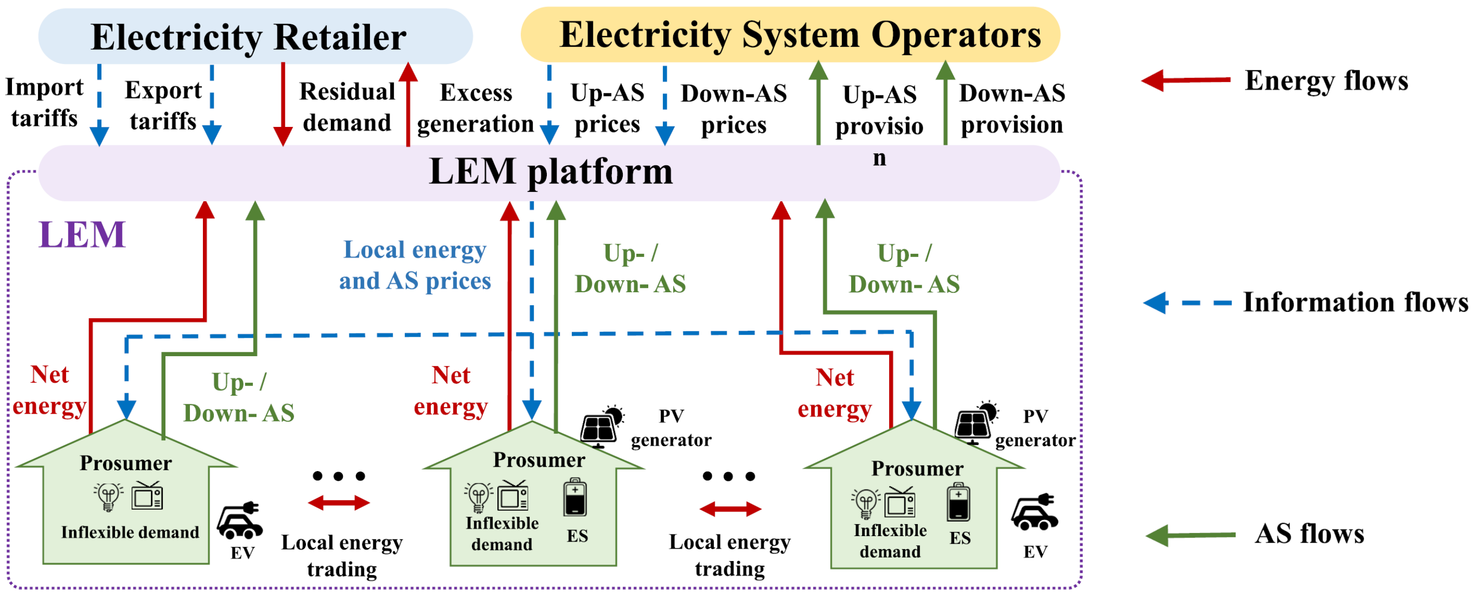
Yujian Ye

Dimitrios Papadaskalopoulos

Fei Teng

Goran Strbac

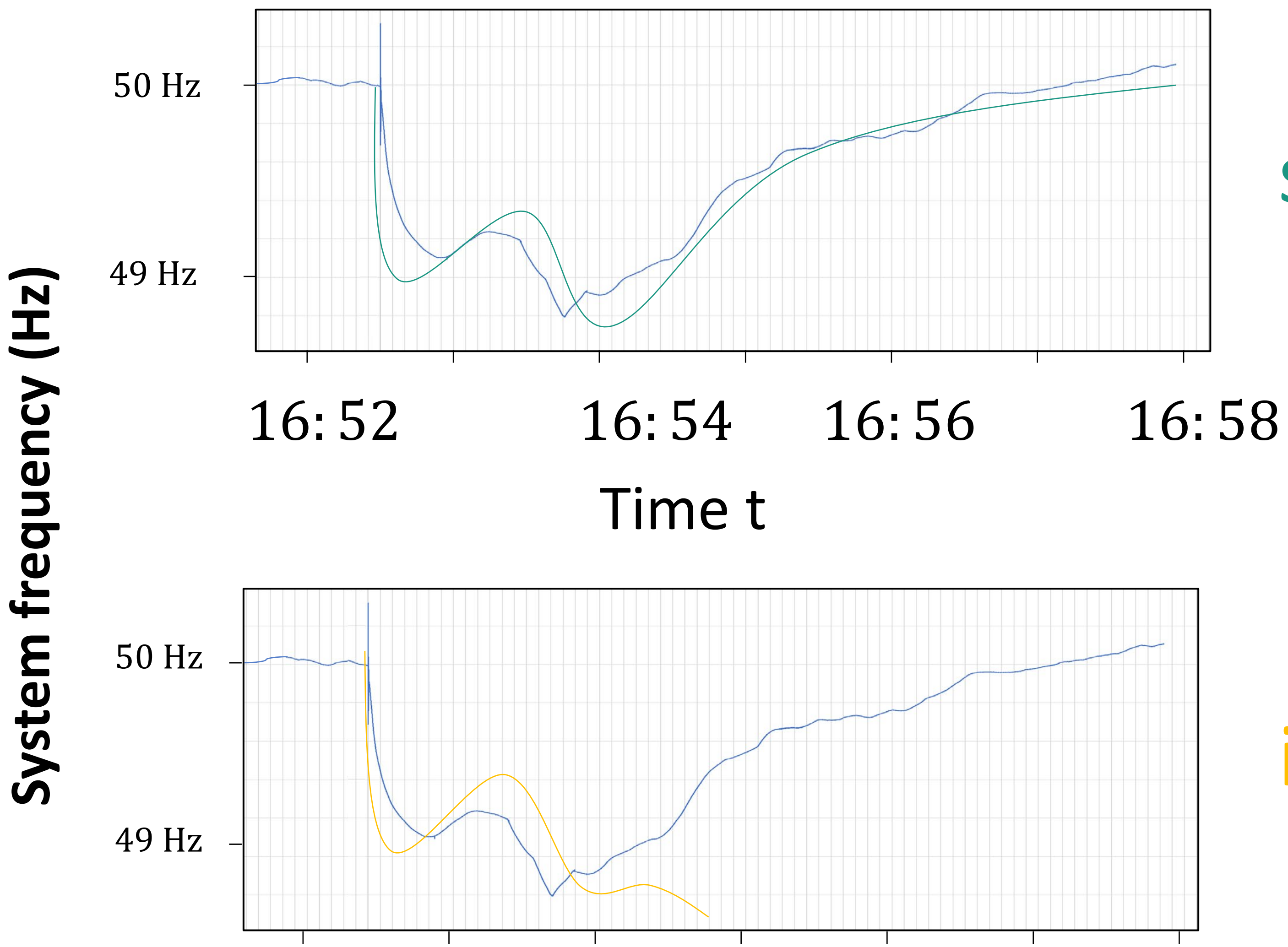
Cyber and physical risks for blackouts



1. How to support dynamic security?
2. How to reduce cyber-security risks?

- Federica Bellizio, Wangkun Xu, Dawei Qiu, Yujian Ye, Dimitrios Papadaskalopoulos, Jochen L. Cremer, Fei Teng, and Goran Strbac. "Transition to Digitalized Paradigms for Security Control and Decentralized Electricity Market." *Proceedings of the IEEE*, 2022,
- Federica Bellizio, Al-Amin Bugaje, Jochen L. Cremer, and Goran Strbac. “Verifying Machine Learning Conclusions for Securing Low Inertia Systems.” *Sustainable Energy, Grids and Networks*, 2022, *30*, 100656.

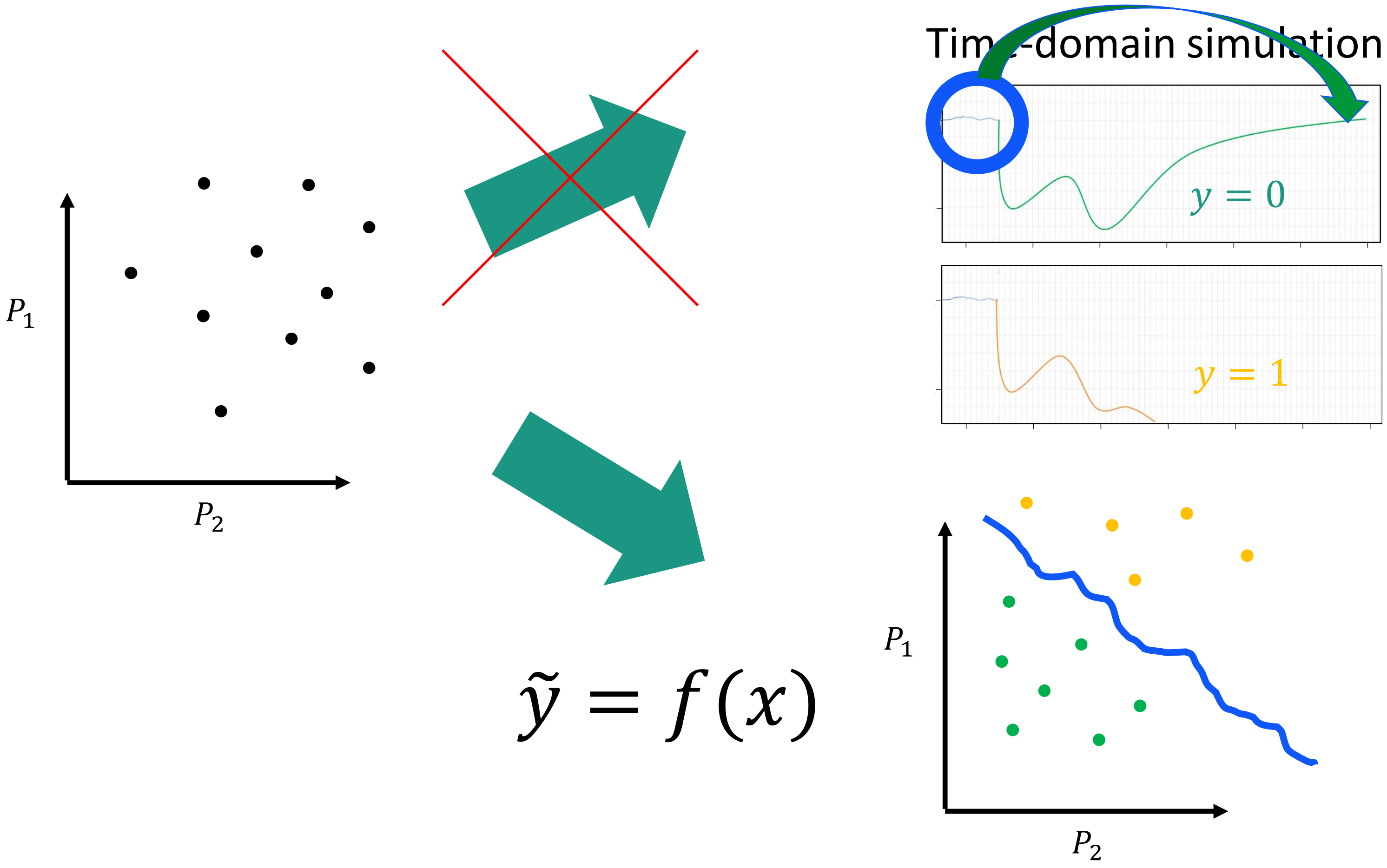
Real-time security in power systems



secure $y = 0$

insecure $y = 1$

Machine learning for real-time DSA

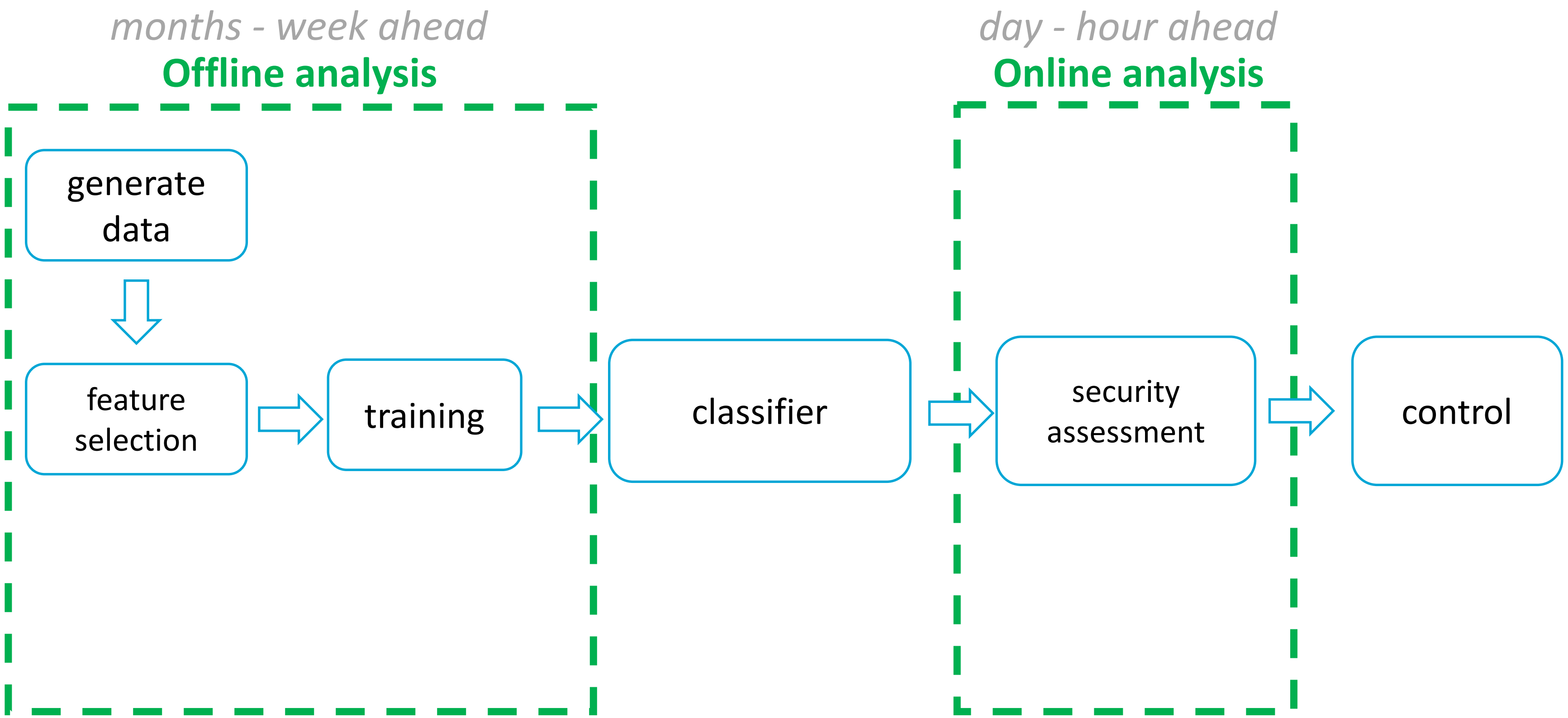


$$\tilde{y} = f(x)$$

How to train and use f?

L. Duchesne, E. Karangelos, and L. Wehenkel, “Recent developments in machine learning for energy systems reliability management, ”*Proceedings of the IEEE*, 2020.

ML-based prediction and control



F. Bellizio, A. A. B. Bugaje, J. L. Cremer, G. Strbac, “Verifying Machine Learning Conclusions for Securing Low Inertia Systems,” *Sustainable Energy, Grids and Networks*, 2022

Supervised learning approach

Operating condition $\boldsymbol{x}_k = [\boldsymbol{x}_k^L, \boldsymbol{x}_k^G, \boldsymbol{x}_k^V]$

Assessment $f_a : (\boldsymbol{x}, B) \rightarrow y_a = \begin{cases} 0 & \text{secure (negative)} \\ 1 & \text{insecure (positive)} \end{cases}$

Control $f_c : (\boldsymbol{x}^L, B) \rightarrow \boldsymbol{y}_c = (\boldsymbol{x}_{OPT}^G, \boldsymbol{x}_{OPT}^V)$

Supervised learning

The ML approach learns approximation functions

$\tilde{f}_a : (\boldsymbol{x}, B) \rightarrow \tilde{y}_a$

$\tilde{f}_c : (\boldsymbol{x}^L, B) \rightarrow \tilde{\boldsymbol{y}}_c = (\tilde{\boldsymbol{x}}_{OPT}^G, \tilde{\boldsymbol{x}}_{OPT}^V)$

such that

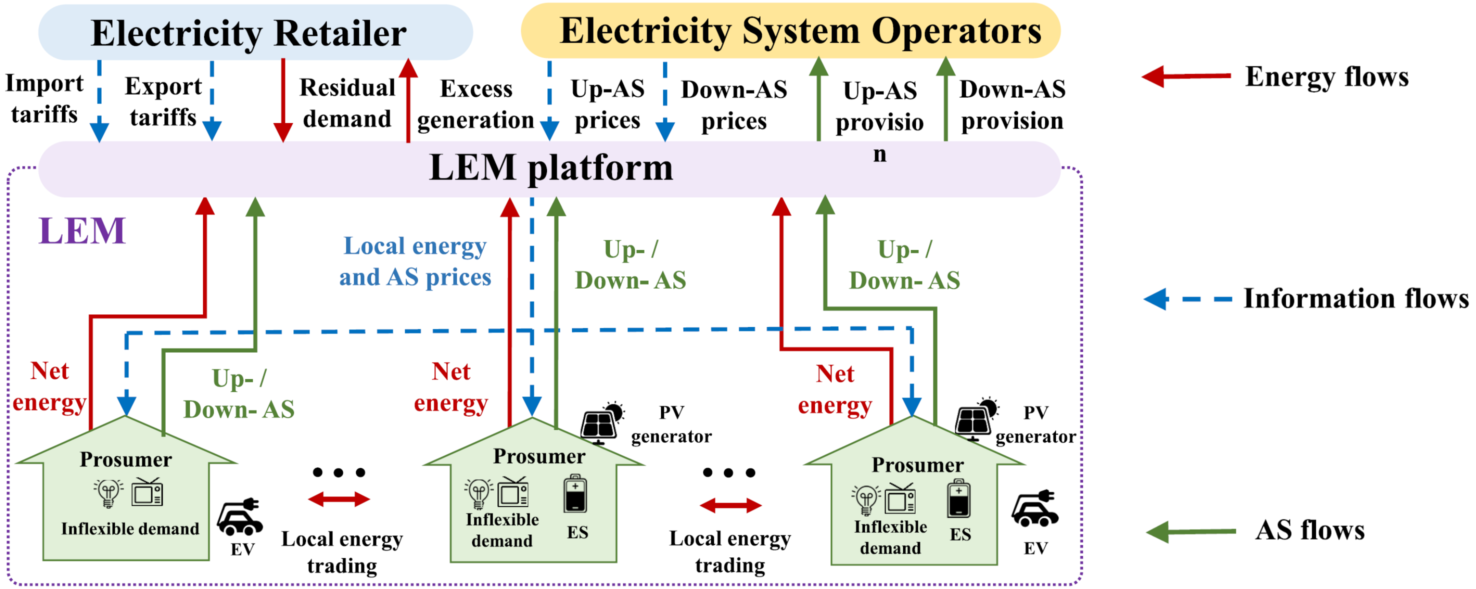
$\| y_a - \tilde{y}_a \|_p, \| \boldsymbol{y}_c - \tilde{\boldsymbol{y}}_c \|_p$ are minimised

Highly nonlinear -> difficult to find, evaluate in real-time

Requires a large training database to create many $(\boldsymbol{x}, B)$

Federica Bellizio, Wangkun Xu, Dawei Qiu, Yujian Ye, Dimitrios Papadaskalopoulos, Jochen L. Cremer, Fei Teng, and Goran Strbac. "Transition to Digitalized Paradigms for Security Control and Decentralized Electricity Market." *Proceedings of the IEEE*, 2022,

Cyber and physical risks for blackouts



1. How to support dynamic security?

2. How to reduce cyber-security risks?

- Federica Bellizio, Wangkun Xu, Dawei Qiu, Yujian Ye, Dimitrios Papadaskalopoulos, Jochen L. Cremer, Fei Teng, and Goran Strbac. "Transition to Digitalized Paradigms for Security Control and Decentralized Electricity Market." *Proceedings of the IEEE*, 2022,

- Federica Bellizio, Al-Amin Bugaje, Jochen L. Cremer, and Goran Strbac. “Verifying Machine Learning Conclusions for Securing Low Inertia Systems.” *Sustainable Energy, Grids and Networks*, 2022, *30*, 100656.

Cyber: False Data Injection (FDI) attacks on DSA

- Consider the power flow equations as $\mathrm{z} = \mathrm{h}(\mathrm{x}) + \mathrm{e}$. The state estimation:

$$\hat{\mathbf{x}} = \arg\min_{\mathbf{x}} \left\| \mathbf{R}^{-\frac{1}{2}} (\mathbf{z} - \mathbf{h}(\mathbf{x})) \right\|_2^2$$

- An FDI attack can be formulated by directly injecting on the estimated state:

$$\mathbf{a} = \mathbf{h}(\hat{\mathbf{x}} + \mathbf{c}) - \mathbf{h}(\hat{\mathbf{x}})$$

- This attack cannot be detected due to the unchanged residual

$$\begin{aligned} \gamma_a &= \left\| \mathbf{R}^{-\frac{1}{2}} (\mathbf{z}_a - \mathbf{h}(\hat{\mathbf{x}}_a)) \right\|_2^2 \\ &= \left\| \mathbf{R}^{-\frac{1}{2}} (\mathbf{z} + \mathbf{h}(\hat{\mathbf{x}} + \mathbf{c}) - \mathbf{h}(\hat{\mathbf{x}}) - \mathbf{h}(\hat{\mathbf{x}} + \mathbf{c})) \right\|_2^2 \\ &= \gamma \end{aligned}$$

Federica Bellizio, Wangkun Xu, Dawei Qiu, Yujian Ye, Dimitrios Papadaskalopoulos, Jochen L. Cremer, Fei Teng, and Goran Strbac. "Transition to Digitalized Paradigms for Security Control and Decentralized Electricity Market." *Proceedings of the IEEE*, 2022,

Defense on the attack

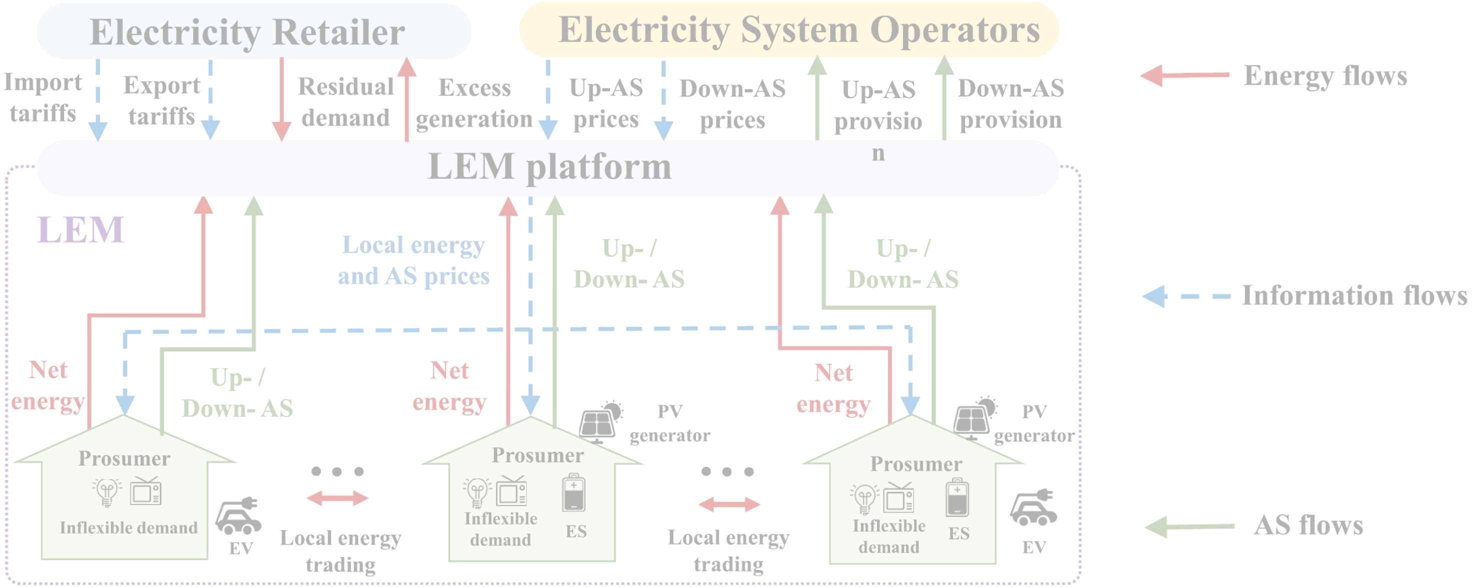
- **Moving target defence (MTD):** the system operator can proactively change the grid's parameter (e.g., reactance) so that the attacker cannot launch a perfect attack.

- Data-driven approach builds a detection model based on normal measurement. An attack alarm is raised if the residual is higher than the predefined threshold.

- A combined data-triggered MTD is proposed
  - High TPR and low FPR can be achieved

Federica Bellizio, Wangkun Xu, Dawei Qiu, Yujian Ye, Dimitrios Papadaskalopoulos, Jochen L. Cremer, Fei Teng, and Goran Strbac. "Transition to Digitalized Paradigms for Security Control and Decentralized Electricity Market." *Proceedings of the IEEE*, 2022,

Case studies



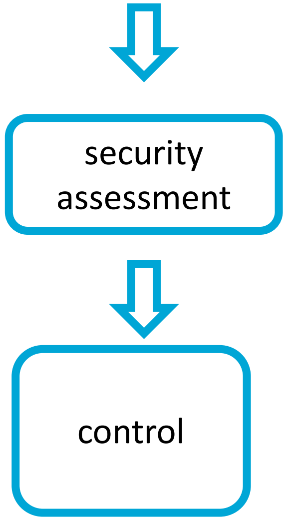
1. Support dynamic security
   A. in low-inertia systems
   B. with LEMs

2. Reduction of cyber-security risks

Federica Bellizio, Wangkun Xu, Dawei Qiu, Yujian Ye, Dimitrios Papadaskalopoulos, Jochen L. Cremer, Fei Teng, and Goran Strbac. "Transition to Digitalized Paradigms for Security Control and Decentralized Electricity Market." *Proceedings of the IEEE*, 2022,

Dynamic security with corrective LEM

IEEE 9 bus system, security of four control approaches, 25% wind power, Integral Square Generator Angle index (ISGA), $ISGA \leq 0.5$



Supervised learning

$$\tilde{f}_a : (\boldsymbol{x}, B) \Rightarrow \tilde{y}_a$$

$$\tilde{f}_c : (\boldsymbol{x}^L, B) \Rightarrow \tilde{\boldsymbol{y}}_c = (\tilde{\boldsymbol{x}}^G_{OPT}, \tilde{\boldsymbol{x}}^V_{OPT})$$

$$\tilde{f}_c : (\hat{x}_{a1}, B) \Rightarrow \tilde{\boldsymbol{y}}_c = (\tilde{\boldsymbol{x}}^G_{OPT}, \tilde{\boldsymbol{x}}^V_{OPT})$$

$$\tilde{f}_c : (\hat{x}_{a2}, B) \Rightarrow \tilde{\boldsymbol{y}}_c = (\tilde{\boldsymbol{x}}^G_{OPT}, \tilde{\boldsymbol{x}}^V_{OPT})$$

Approach	Insecure OCs
No control	928/1000
Centralised control with LEMs	95/1000
Attacked centralised corrective	204/1000
Attacked decentralised corrective	148/1000

Federica Bellizio, Wangkun Xu, Dawei Qiu, Yujian Ye, Dimitrios Papadaskalopoulos, Jochen L. Cremer, Fei Teng, and Goran Strbac. "Transition to Digitalized Paradigms for Security Control and Decentralized Electricity Market." *Proceedings of the IEEE*, 2022,

Reducing cyber-security risks

- **Issue:** Attacker launches FDI attacks on the voltage magnitude to mislead the security assessment.

- **Approach:** A combined data-triggered MTD

	Data-Driven Detector	Data-Triggered MTD
TPR	98.9%	97.5%
FPR	0.71%	0.12%

High TPR and low FPR

Federica Bellizio, Wangkun Xu, Dawei Qiu, Yujian Ye, Dimitrios Papadaskalopoulos, Jochen L. Cremer, Fei Teng, and Goran Strbac. "Transition to Digitalized Paradigms for Security Control and Decentralized Electricity Market." *Proceedings of the IEEE*, 2022,

Conclusions

- Neural networks can predict dynamic security using estimated operating conditions but require lots of training data **(limitation)**
- **Corrective control improves dynamic system security**
- Cyber-attacks **can make the system 2-times more dynamically** insecure
  - Centralised attacks are worse than decentralised attacks
  - Attacks on local measurements can influence prosumers

Contact & references

Speaker

Jochen Cremer
Assistant Professor IEPG, TU Delft, Netherlands
Web: https://www.tudelft.nl/ai/delft-ai-energy-lab
Email: j.l.cremer@tudelft.nl

Collaborators

Federica Bellizio

Al-Amin Bugaje

Wangkun Xu

Dawei Qiu

Yujian Ye

Dimitrios Papadaskalopoulos

Fei Teng

Goran Strbac

- Federica Bellizio, Wangkun Xu, Dawei Qiu, Yujian Ye, Dimitrios Papadaskalopoulos, Jochen L. Cremer, Fei Teng, and Goran Strbac. "Transition to Digitalized Paradigms for Security Control and Decentralized Electricity Market." Proceedings of the IEEE, 2022,
- Habib, Benjamin, Elvin Isufi, Ward van Breda, Arjen Jongepier, and Jochen L. Cremer. "Deep Statistical Solver for Distribution System State Estimation." IEEE Transactions on Power Systems, 2023.
- Federica Bellizio, Al-Amin Bugaje, Jochen L. Cremer, and Goran Strbac. “Verifying Machine Learning conclusions for securing Low Inertia systems.” Sustainable Energy, Grids and Networks, 2022, 30, 100656.
- Xie, H., Bellizio, F., Cremer, J.L. and Strbac, G., 2023. Regularised Learning with Selected Physics for Power System Dynamics. IEEE PES Belgrade Powertech, 2023.
- Veerakumar, N., Cremer, J. L., & Popov, M. (2023). Dynamic Incremental Learning for real-time disturbance event classification. International Journal of Electrical Power & Energy Systems, 148, 108988.
- Bellizio, Federica, Jochen L. Cremer, and Goran Strbac. "Transient Stable Corrective Control Using Neural Lyapunov Learning." IEEE Transactions on Power Systems, 2022.

Thank you!

Dynamic security in low-inertia systems

IEEE 14 bus system, transient stability, 40% renewable generation, data: 10.000 OCs, train/test = 70%/30%

feature selection

⇩

training classifier

⇩

security assessment

Features		Power generations	Power loads	Voltage angles	Voltage magnitudes
HI system	F1-score	65%	46%	43%	43%
	$I(X;Y)$	0.5	0.5	0.6	0.5
LI system	F1-score	99%	97%	93%	96%
	$I(X;Y)$	1.7	2.4	4.7	1.6

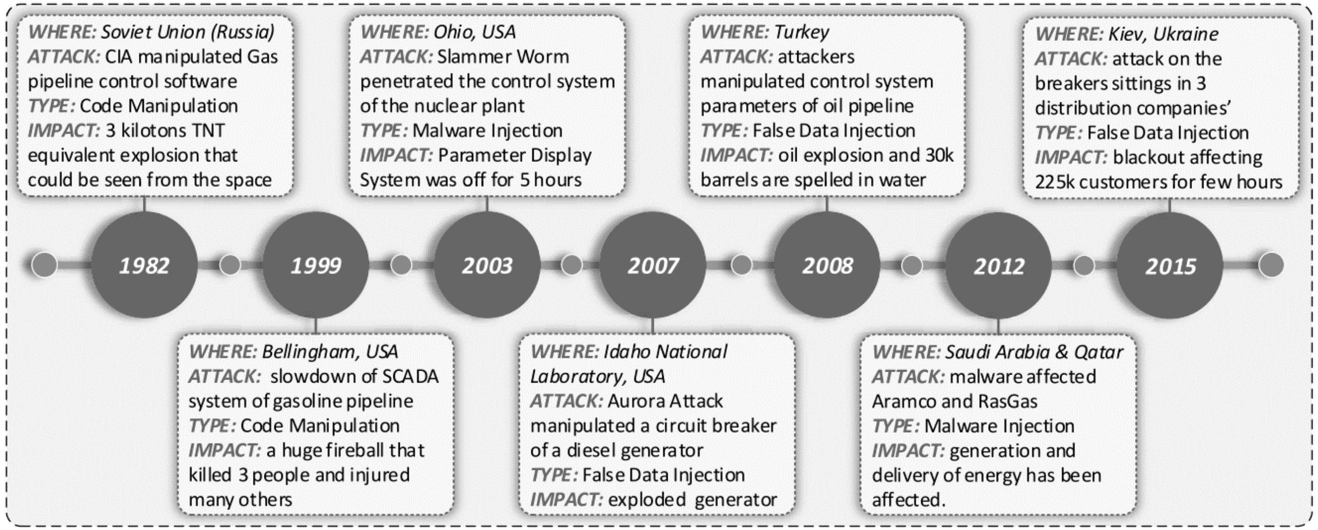
Model types	DT	SVM	XGBoost	ANN
HI system	59%	55%	63%	63%
LI system	99%	97%	99%	99%

Scores	$\frac{N^+}{N^+ + N^-}$	$I(X;Y)$	Accuracy	F1-score
HI system	0.7	2.1	75%	59%
LI system	0.2	10.4	98%	99%

F. Bellizio, A. A. B. Bugaje, J. L. Cremer, G. Strbac, "Verifying Machine Learning conclusions for securing Low Inertia systems," *Sustainable Energy, Grids and Networks*, 2022

Cyber security

- Advances in computation and communication have transformed the power system into a compound cyber-physical system (CPS).
- This new trend raises concerns about CPS vulnerability.



1. False data injection (FDI) attacks against dynamic security assessment
2. Attacks on the local energy market.

Source: Musleh, Ahmed S., Guo Chen, and Zhao Yang Dong. "A survey on the detection algorithms for false data injection attacks in smart grids." *IEEE Transactions on Smart Grid* 11.3 (2019): 2218-2234.