June 2023

NTNU

Kunnskap for en bedre verden

Cybersecurity and Digital Privacy Aspects of Smartgrids

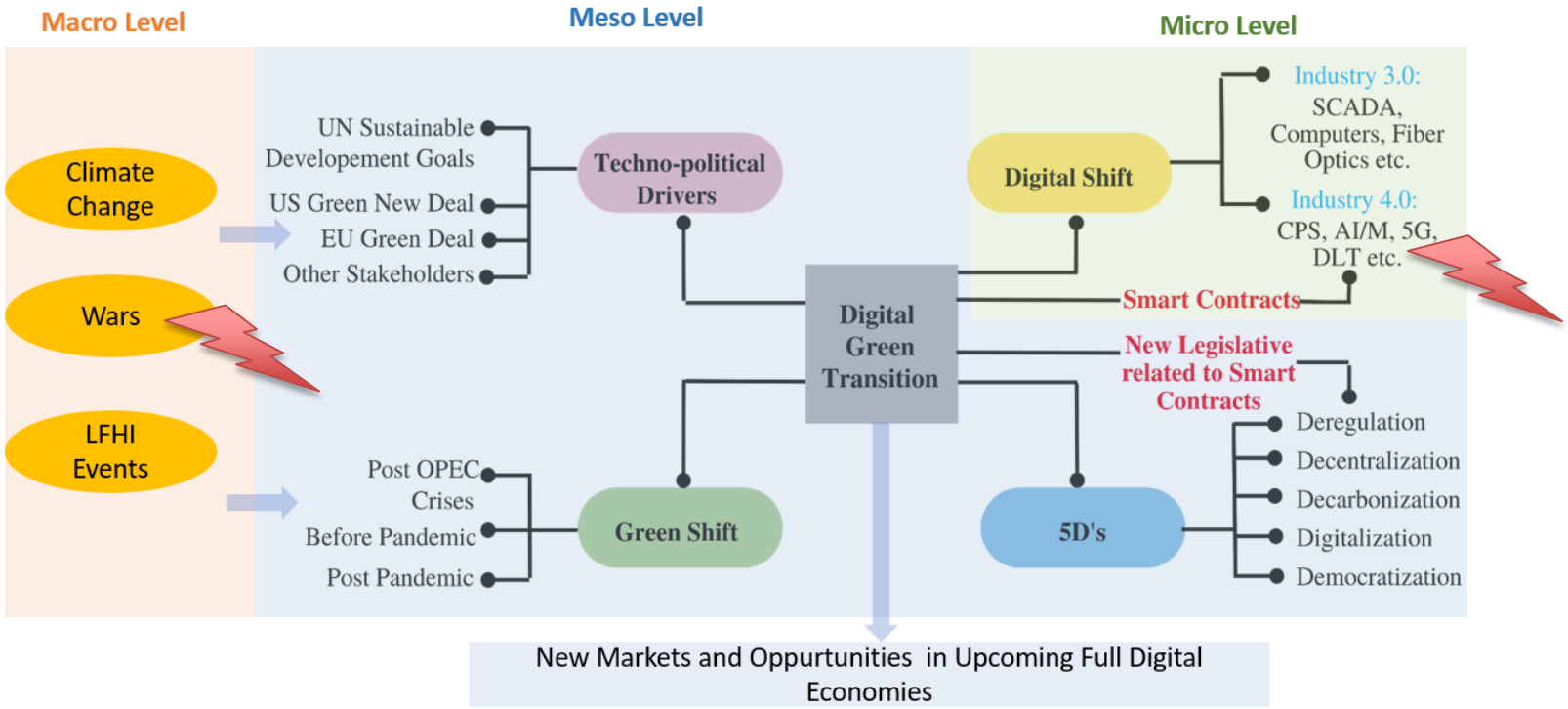
Associaate Professor Umit Cali
Department of Electrical Energy (DEE)

Agenda

- Cyber-physical-social Energy Systems and Energy Transition
- Foundations
  - AI
  - Cyberlaw
  - Smartgirds
- Digital Privacy in Energy Domain / Smartgrids
- Cybersecurity in Energy Domain / Smartgrids
- Conclusion and Outlook

Big Picture

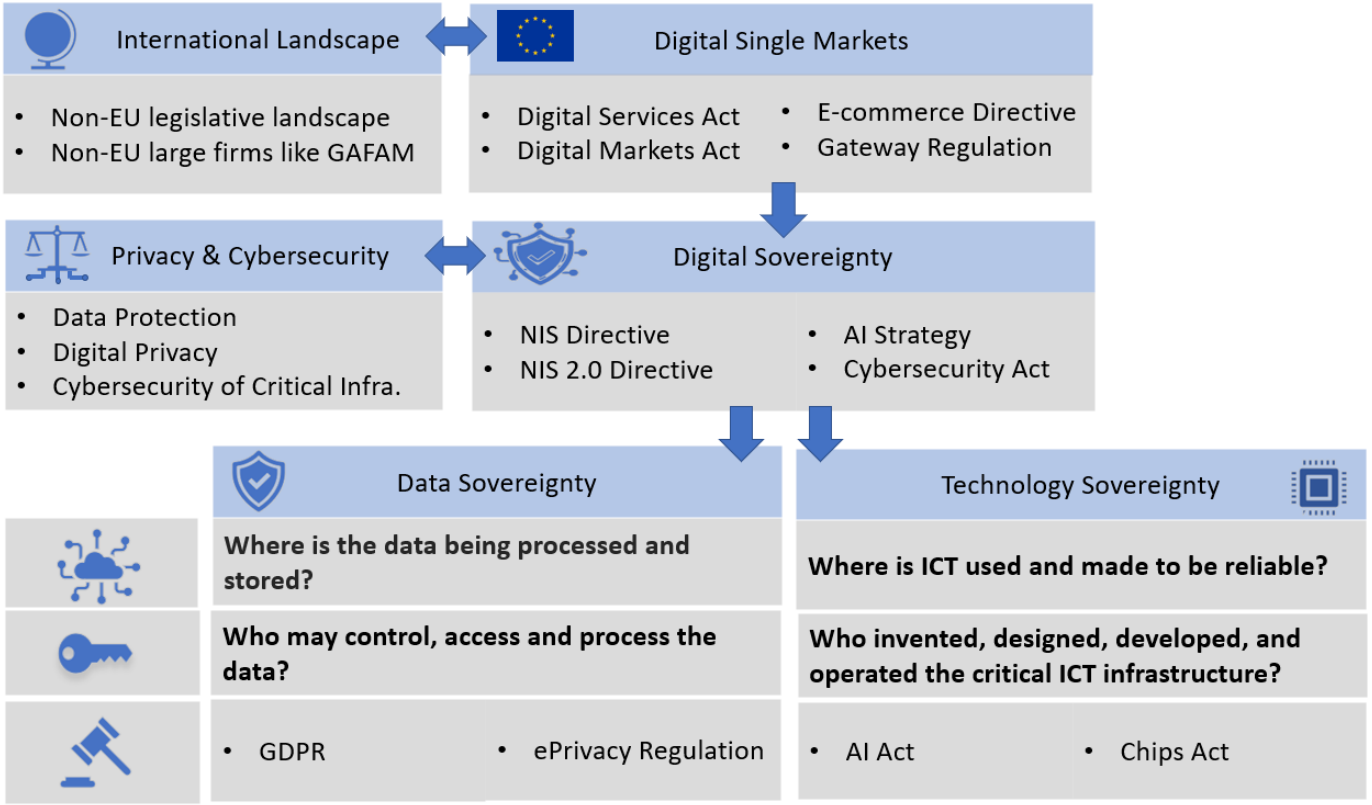
Global Landscape of Digital Green Shift



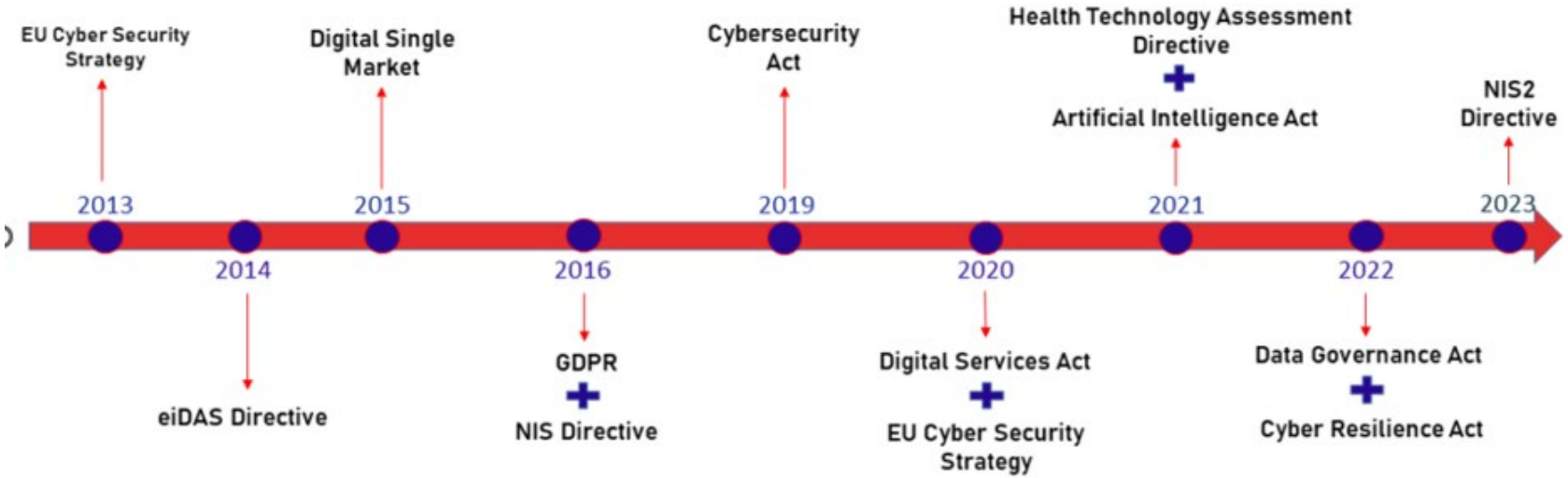
Source: **Cali** U., Kuzlu M., Pipattanasomporn M., Kempf J., Bai L. (2021) **Digitalization of Power Markets and Systems Using Energy Informatics**. Springer, Cham. https://doi.org/10.1007/978-3-030-83301-5_1

Cyberlaw

Cyberlaw Landscape

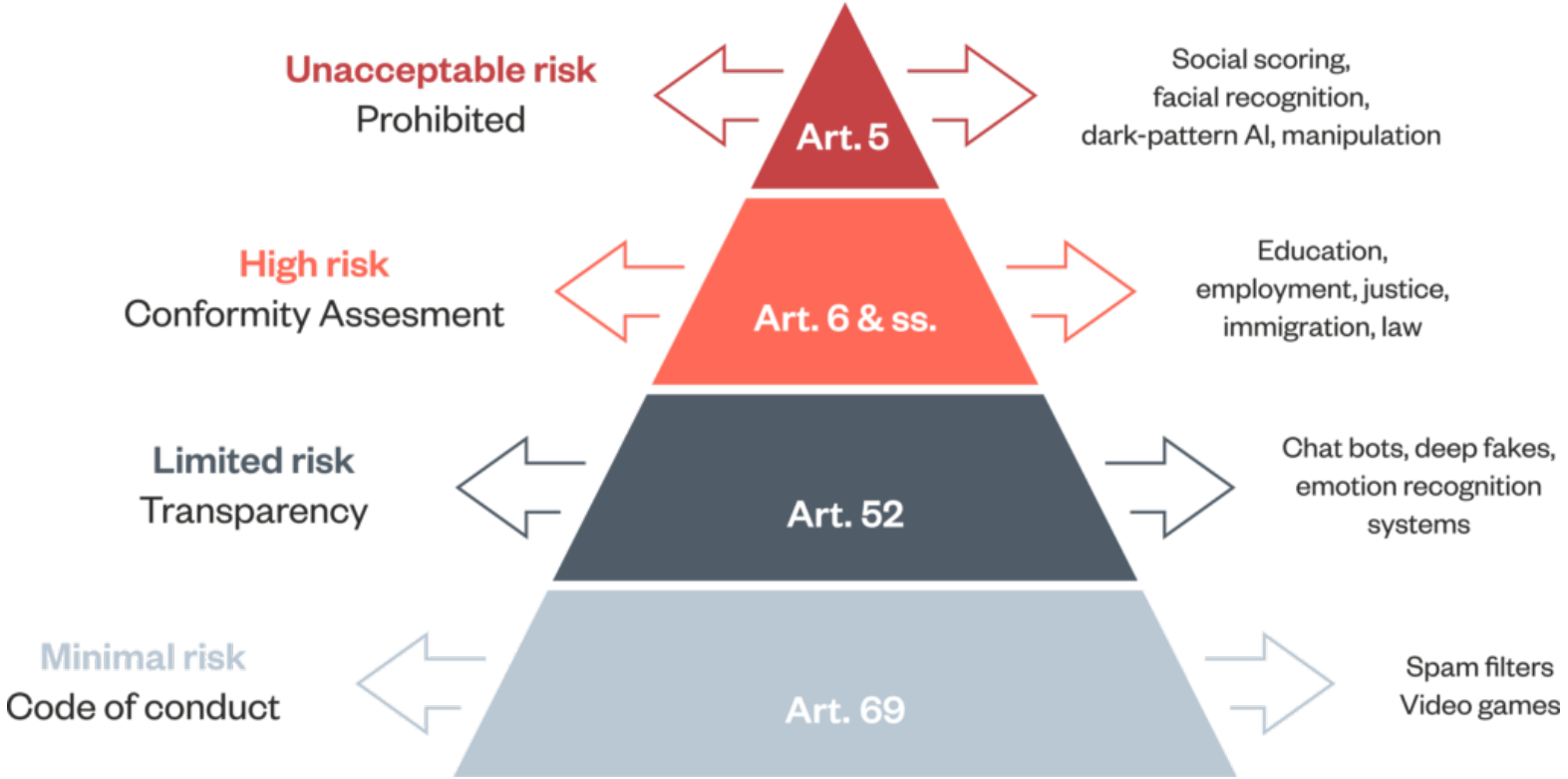


EU Cyberlaw and Policy Context



Source: headmind

AI Act Summary



Src:
adalovelaceinstitute

Network and Information Security Directive

DIFFERENCES BETWEEN NIS AND NIS2

NIS	NIS2	
	Expanded scope	
• Improvement of capabilities of EU Member States in the area of cybersecurity.	• Increasing the number of sectors covered by NIS.	• NIS2 adds new sectors to its scope. NIS2 classifies entities within its scope in two categories: (i) operators of essential services and (ii) important entities.
	Enhanced enforcement	
	• More measures regarding enforcement and supervision.	• Establishment of a minimum list of administrative sanctions. • Establishment of fines.
	Strengthening security requirements	
• Operators of Essential Services and Digital Service Providers must implement risk management practices and must notify significant incidents to the competent national authorities.	• Strengthened security requirements and a list of: (i) focused measures, including incident response and disclosure policies; and (ii) procedures, including, among other things, risk analysis, business continuity and crisis management, and human resource security.	• More stringent rules on supply chain security. • Two-stage approach to incident reporting.
	Cooperation	
• Increased cooperation at EU-level.	• Establishment of the European Cyber Crisis Liaison Organisation Network which supports the coordinated management of EU-wide cybersecurity incidents.	• Measures to increase trust. • Rules on information sharing between competent authorities. • Procedures in the event of a large-scale incident or crisis.

SECTORS COVERED

NIS	NIS 2
• Banking and financial market infrastructure • Digital infrastructure • Digital service providers • Energy • Healthcare • Transport • Water supply	Extended scope by adding new sectors. Service providers are classified into two categories: operators of essential services or important entities. • Digital services such as social networking services platforms and data centre services • Food • Manufacturing of certain critical products (such as pharmaceuticals, medical devices, chemicals) • Postal and courier services • Providers of public electronic communications networks or services • Public administration • Space • Waste water and waste management

Src: houthoff

Digital Privacy

Digital Privacy

What is Privacy? : According to Lillian BeVier : “Privacy is a chameleon-like word, used denotatively to designate a wide range of wildly disparate interests—from **confidentiality of personal information** to reproductive autonomy—and connotatively to generate goodwill on behalf of whatever interest is being asserted in its name.”

Three categories of Privacy:

- Individual
- Communication
- Information

Lillian R. BeVier, Information About Individuals in the Hands of Government: Some Reflections on Mechanisms for Privacy Protection, 4 WM. & MARY BILL RTS. J. 455, 458 (1995)

Digital Privacy

What is Digital Privacy?:

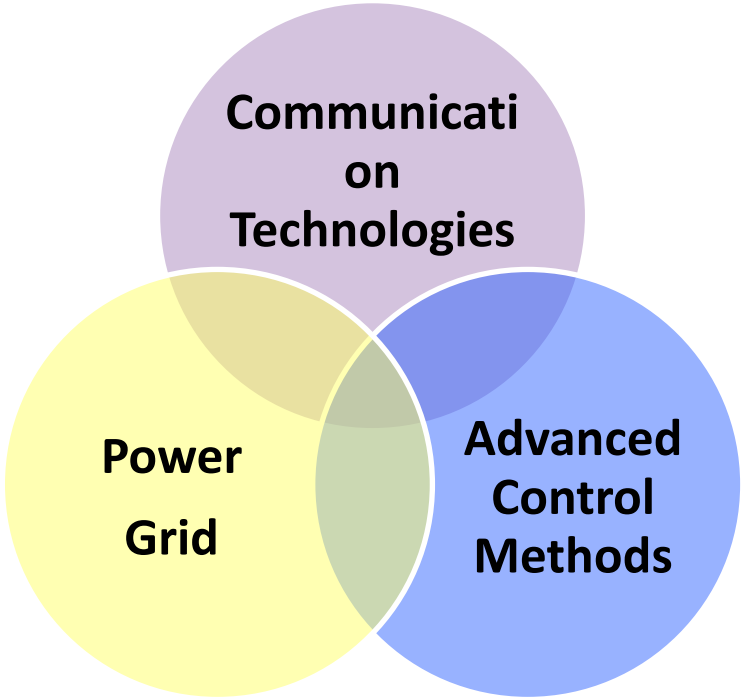
"**Digital privacy** is **an expectation of privacy** unless the user has given consent that includes an awareness of the risks associated with online services, and **individual control over the collection, distribution and retention of personal information**."

Robertson, L., & Muirhead, B. (2019, April). Unpacking the privacy paradox for education. In A. Visvizi, & M. D. Lytras (Eds.), *The international research & innovation forum: Technology, innovation, education, and their social impact* (pp. 27-36). Springer, Cham. https://doi.org/10.1007/978-3-030-30809-4_3

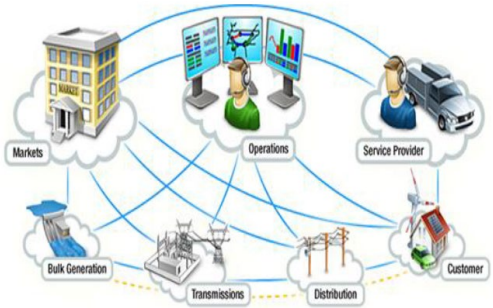
Foundations of AI and SGs

SmartGrid (SG)

Smartgrid is the next-generation electric power system with communication technologies and advanced control methods.



What is SG?



Source: http://smartgrid.ieee.org

Overall objective:

Smart/best/optimal utilization of all the available resources.

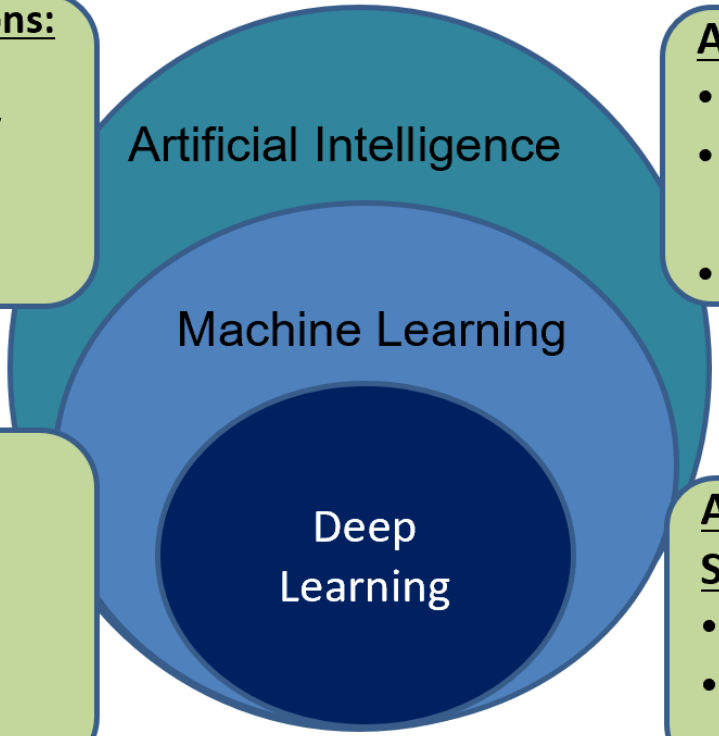
IEEE:

- Smartgrid is a large ‘System of Systems’, where each functional domain consists of three layers: (i) the power and energy layer, (ii) the communication layer, and (iii) the IT/computer layer.

- Layers (ii) and (iii) above are the enabling infrastructure that makes the existing power and energy infrastructure ‘smarter’

Artificial Intelligence and Energy Use Cases

AI for Power Grid operations:
- Smart grids
- Improved cyber security
- **Anomaly detection**
- Power system resilience

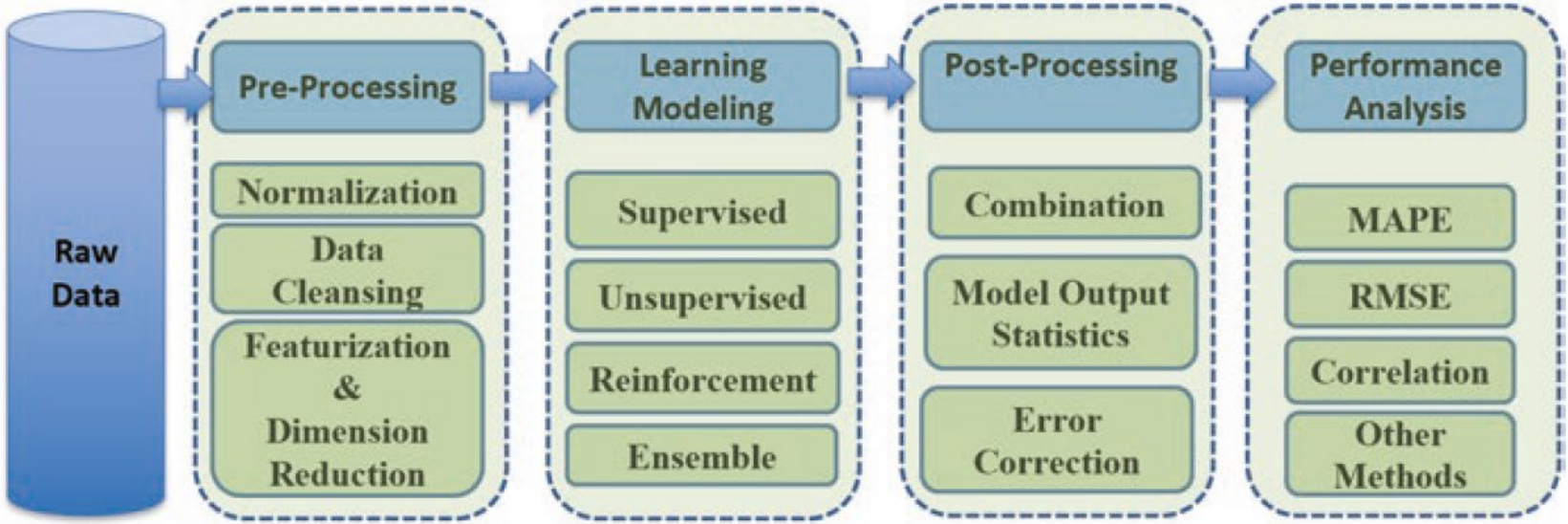


AI for Trading operations
- Load forecasting
- Electricity price forecasting
- Algorithmic trading

AI for Asset & Energy Management
- Predictive maintenance
- **Predictive (building) Energy Management Systems**

AI for Renewable Energy Sources
- **Wind power forecasting**
- Solar power forecasting
- Asset Lifecyle prediction

AI/ML General Process / Work Flow



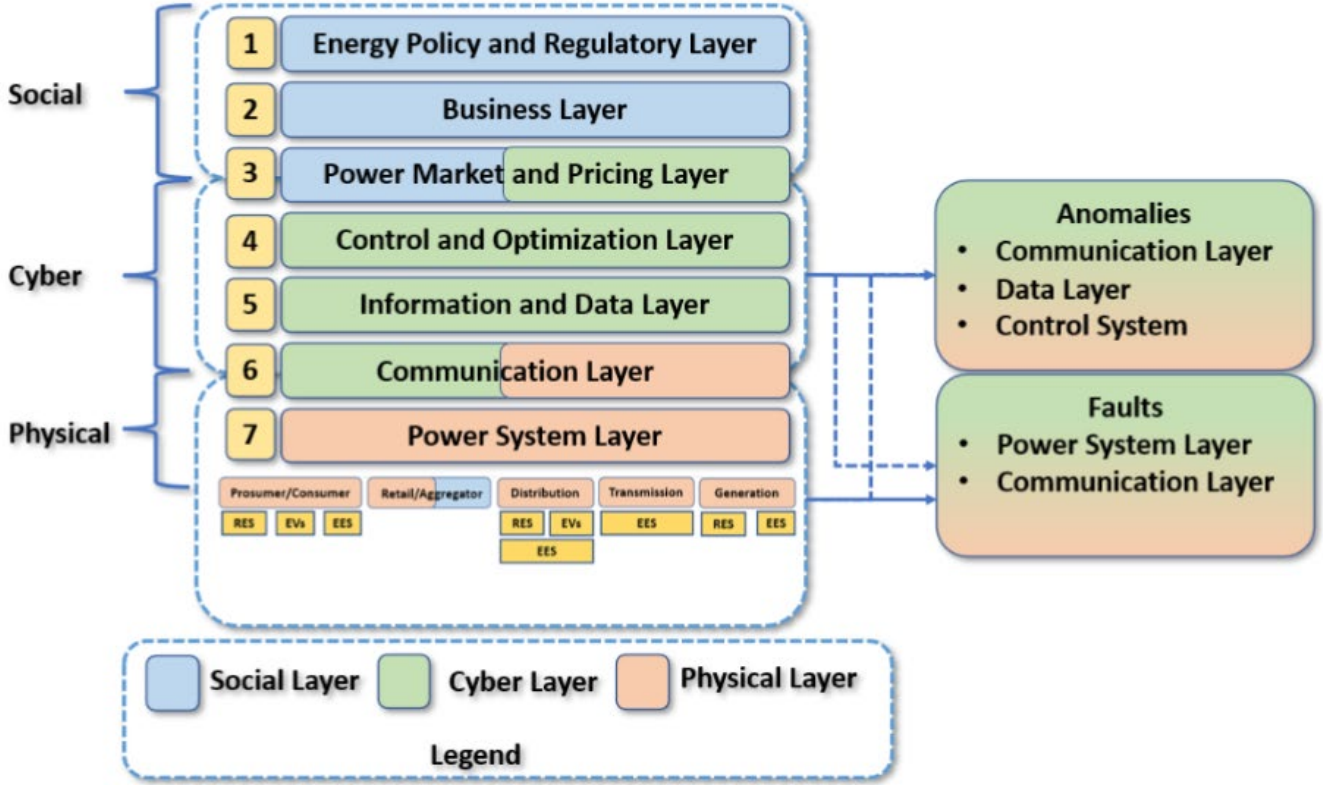
Grid Security using AI

Attack type	Algorithm	Data set
False data injection to PMU data [97]	SVE, perceptron, SVM, k-NN, SLR[a]	Synthetic data set
Denial of service (DoS), R2L, U2R, probe, and Normal class [98]	k-NN, NN, DT, random forest	KDD99 data set, NSLKDD
Energy fraud [99]	ANN	Synthetic data set
Stealthy false data injection [100]	SVM	Synthetic data set
False data injection to smart meter data [101]	DT and SVM	Private data set
False data injection to smart meter data [101, 102]	SVM	Private data set
False data injection to smart meter and sensor data [102]	SVM and KNN	Synthetic data set
False data injection to PMU data [102]	RBM[a]	Synthetic data set
Cyberattack to grid field devices such as RTUs[a], PLCs[a], PMUs[a], and IEDs[a] [103]	SVM	Synthetic data set
False data injection to the power flow data [104]	SVM, KNN, and ANN	Synthetic data set
False data injection to SCADA system [105]	CDBN[a]	Synthetic data set
False data injection to PMU data [106]	CDBN[a]	Synthetic data set

[a]Sparse logistic regression (SLR), restricted Boltzmann machine (RBM), remote terminal unit (RTU), programmable logic circuit (PLC), phasor measurement unit (PMU), intelligent electronic devices (IED), and conditional deep belief network (CBDN)

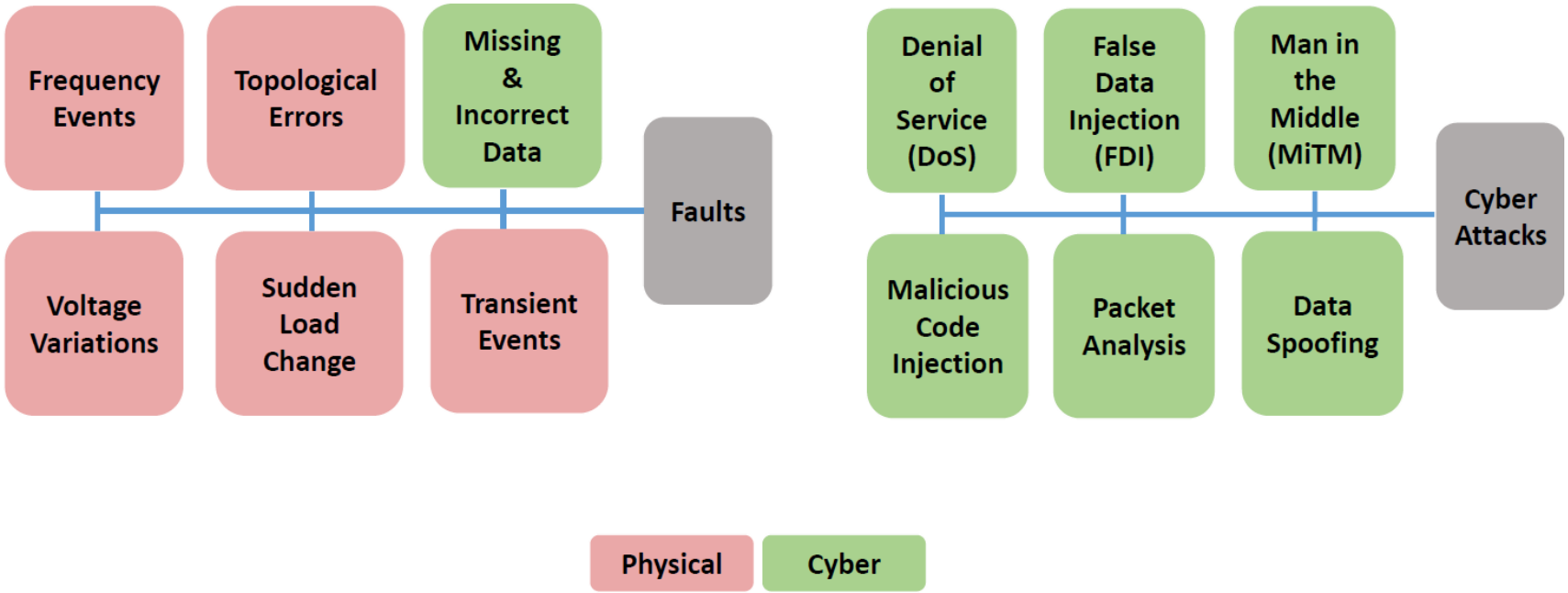
Source: **Cali** U., Kuzlu M., Pipattanasomporn M., Kempf J., Bai L. (2021) **Digitalization of Power Markets and Systems Using Energy Informatics**. Springer, Cham. https://doi.org/10.1007/978-3-030-83301-5_1

Technical Aspects: Anomaly Detection

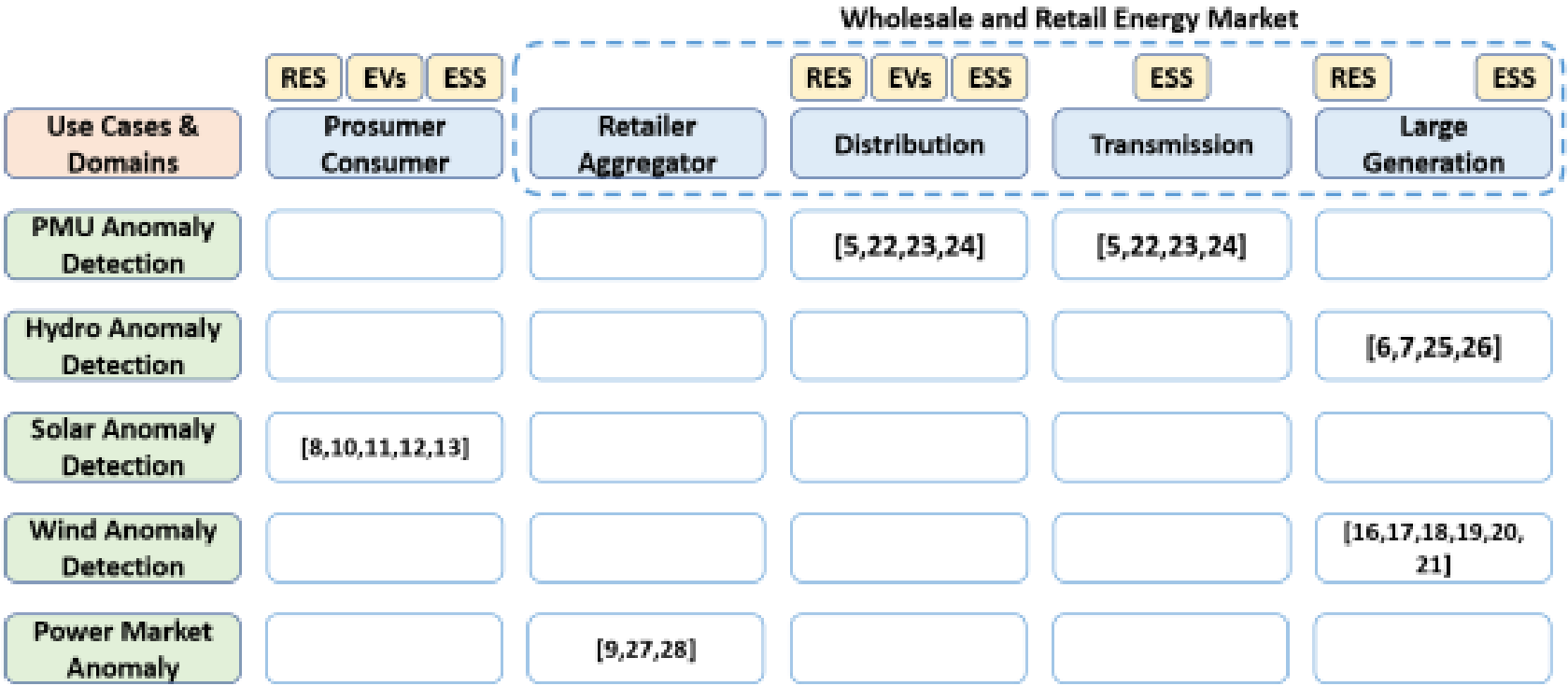


Source: **Cali** U., Kuzlu M., Pipattanasomporn M., Kempf J., Bai L. (2021) **Digitalization of Power Markets and Systems Using Energy Informatics**. Springer, Cham. https://doi.org/10.1007/978-3-030-83301-5_1

Technical Aspects: Anomaly Detection



Technical Aspects: Anomaly Detection



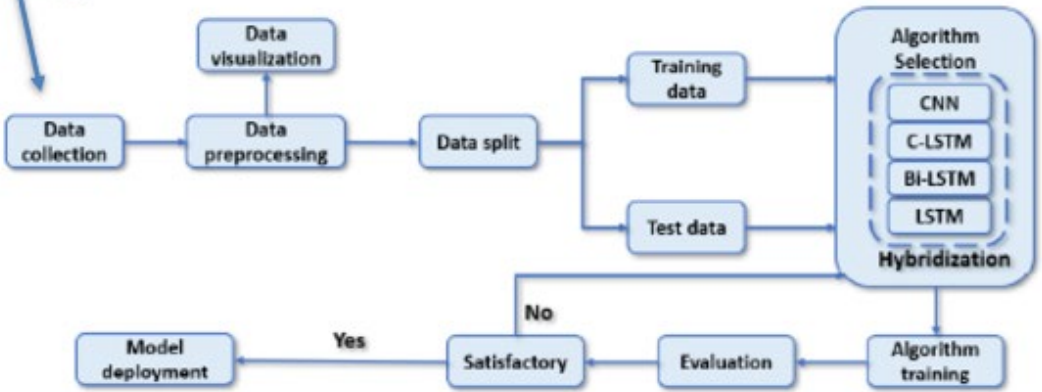
Technical Aspects: Anomaly Detection

Use Cases & Anomaly Types	Fault	Attack	Methods/Algorithms
Signal Processing, Statistics	[37,38]		Fast Fourier Transform
Physical: AI/ML	[39,40]		CNN,LSTM, Bi-LSTM, C-LSTM
False Data Injection (FDI)		[97,102,103,106]	SVM, k-NN, Sparce Logistic Regression (SLR), Conditional Deep Belief Network (CBDN)
Man in the Middle (MiTM)		[31,32]	Communication Layer
Other Attacks		[33,34,35]	Data and Communication Layer

Selected Use Cases

Technical Aspects: AI-based Anomaly Detection

PMUs



$$Precision = \frac{N_{TruePositives}}{N_{TruePositives} + N_{FalsePositives}}$$

$$Recall = \frac{N_{TruePositives}}{N_{TruePositives} + N_{FalseNegatives}}$$

$$F1 = 2 * \frac{Precision * Recall}{Precision + Recall}$$

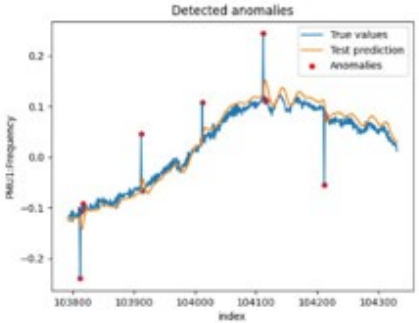
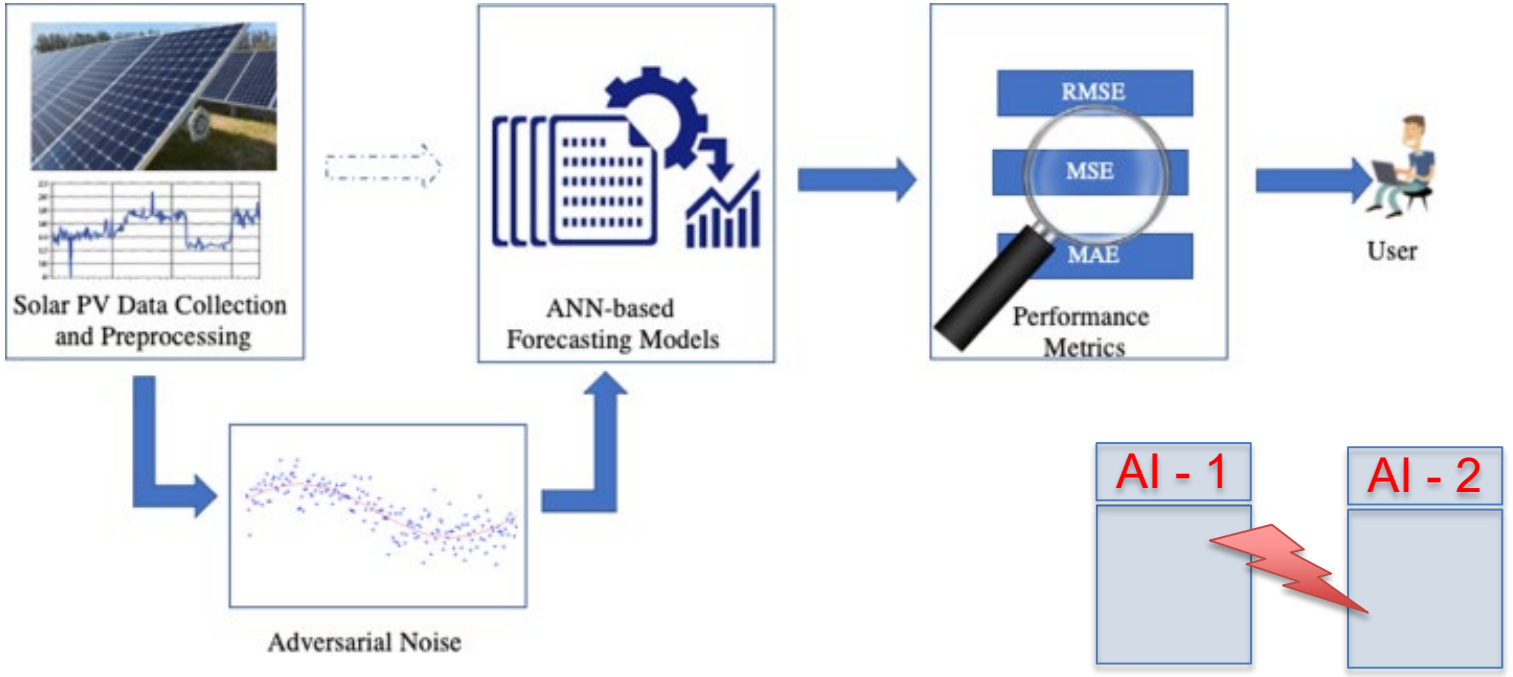


Figure 56: C-LSTM spike detection with noise filter.

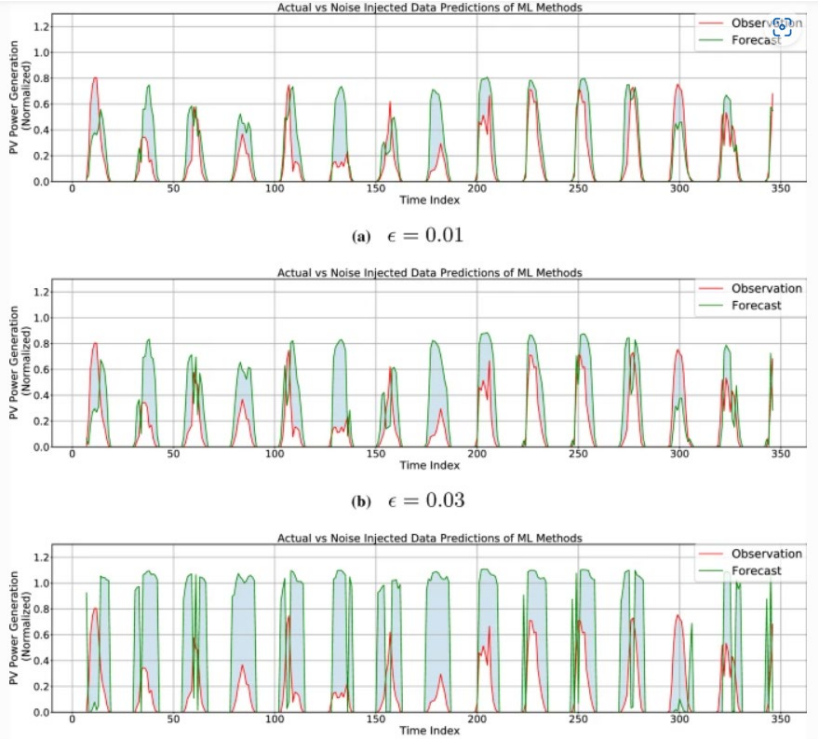
Regev, Yuval Abraham, Henrik Vassdal, Ugur Halden, Ferhat Ozgur Catak, and Umit Cali. "Hybrid AI-based Anomaly Detection Model using Phasor Measurement Unit Data." *arXiv e-prints* (2022): arXiv-2209.

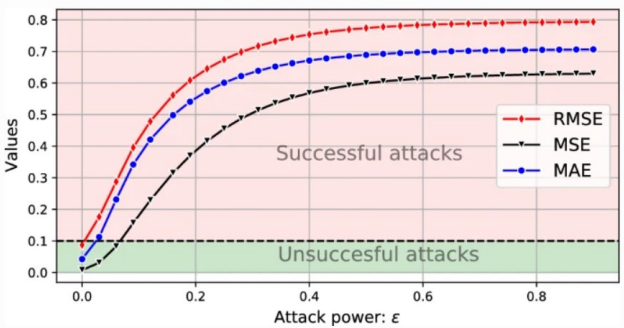
Cyber Risk to DER and Solar Forecasting Systems

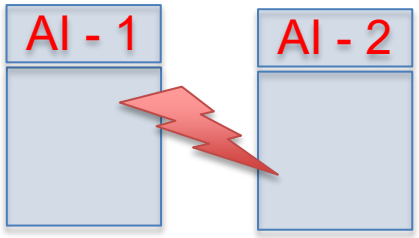


Kuzlu, M., Sarp, S., Catak, F.O., Umit Cali, "Analysis of deceptive data attacks with adversarial machine learning for solar photovoltaic power generation forecasting." *Electrical Engineering* (2022): 1-9.

Cyber Risk to DER and Solar Forecasting Systems



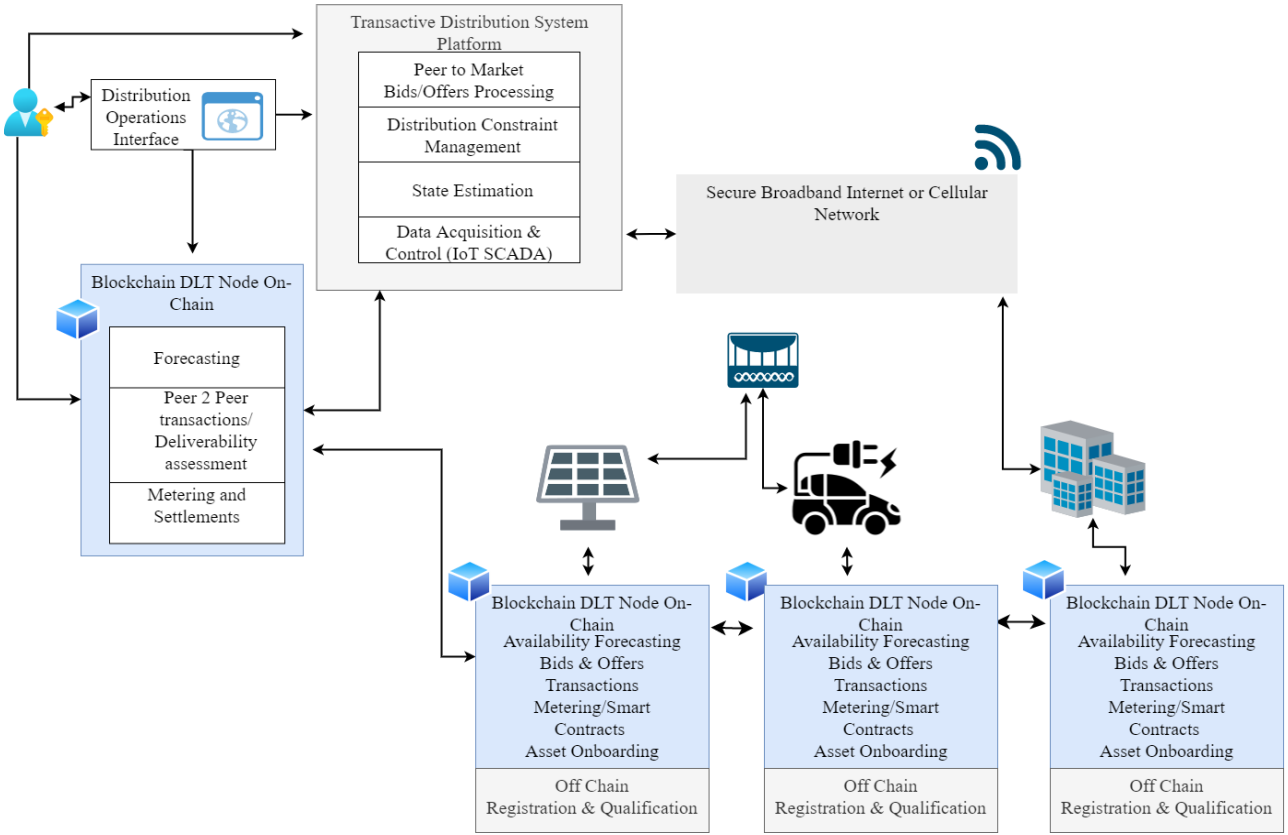




Kuzlu, M., Sarp, S., Catak, F.O., Umit Cali, "Analysis of deceptive data attacks with adversarial machine learning for solar photovoltaic power generation forecasting." *Electrical Engineering* (2022): 1-9.

DER and EV Use Case

Source: "**Standardization of the Distributed Ledger Technology Cybersecurity Stack for Power and Energy Applications**"; "Sri Nikhil Gupta Gourisetti, Umit Cali, Kim-Kwang Raymond Choo, Elizabeth Escobar, Christopher Gorog, Annabelle Lee, Claudio Lima, Michael Mylrea, Marco Pasetti, Farrokh Rahimi, Ramesh Reddi, and Abubakar Sadi Sani; **Sustainable Energy, Grids and Networks; Vol 28, December 2021**.

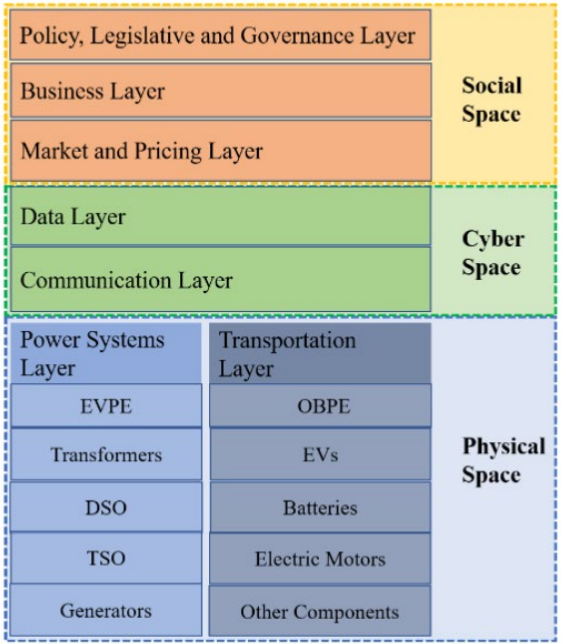


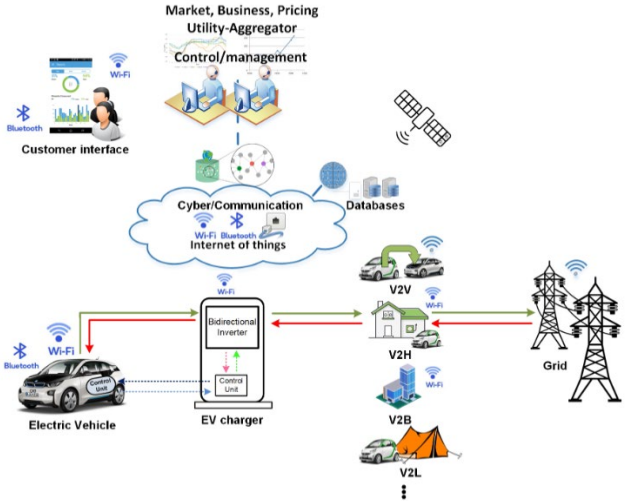
Cyber-Physical Security using AI and DLT

Cybersecurity and Digital Privacy Aspects of V2X in the EV Charging Structure

ABSTRACT

With the advancement of green energy technology and rising public and political acceptance, electric vehicles (EVs) have grown in popularity. Electric motors, batteries, and charging systems are considered major components of EVs. The electric power infrastructure has been designed to accommodate the needs of EVs, with an emphasis on bidirectional power flow to facilitate power exchange. Furthermore, the communication infrastructure has been enhanced to enable cars to communicate and exchange information with one another, also known as Vehicle-to-Everything (V2X) technology. V2X is positioned to become a bigger and smarter system in the future of transportation, thanks to upcoming digital technologies like as Artificial Intelligence (AI), Distributed Ledger Technology, and the Internet of Things. However, like with any technology that includes data collection and sharing, there are issues with digital privacy and cybersecurity. This paper addresses these concerns by creating a multi-layer Cyber-Physical-Social Systems (CPSS) architecture to investigate possible privacy and cybersecurity risks associated with V2X. Using the CPSS paradigm, this research explores the interaction of EV infrastructure as a very critical part of the V2X ecosystem, digital privacy, and cybersecurity concerns.



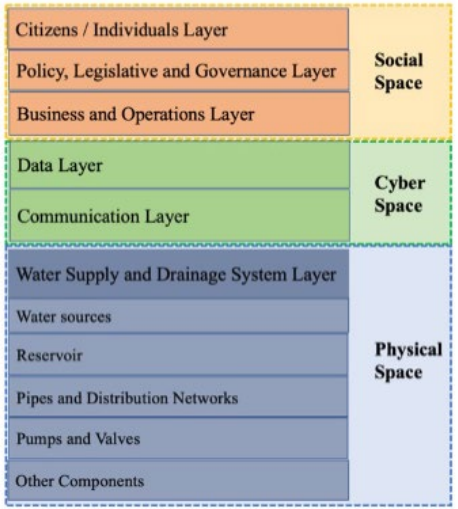


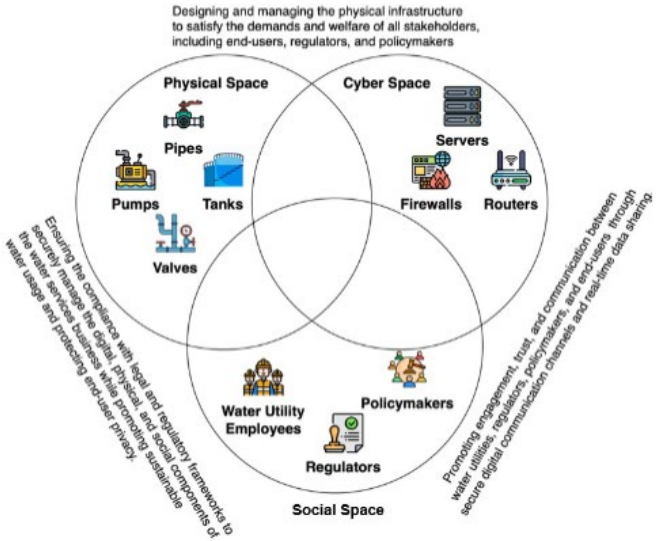
Umit Cali, Murat Kuzlu, Onur Elma, Osman Gazi Gucluturk, Ahmet Kilic, and Ferhat Ozgur Catak. 2023. Cybersecurity and Digital Privacy Aspects of V2X in the EV Charging Structure. In Proceedings of the 2023 European Interdisciplinary Cybersecurity Conference (EICC '23). Association for Computing Machinery, New York, NY, USA, 174–180. https://doi.org/10.1145/3590777.3591406

Cyber-Physical Security using AI and DLT

ABSTRACT

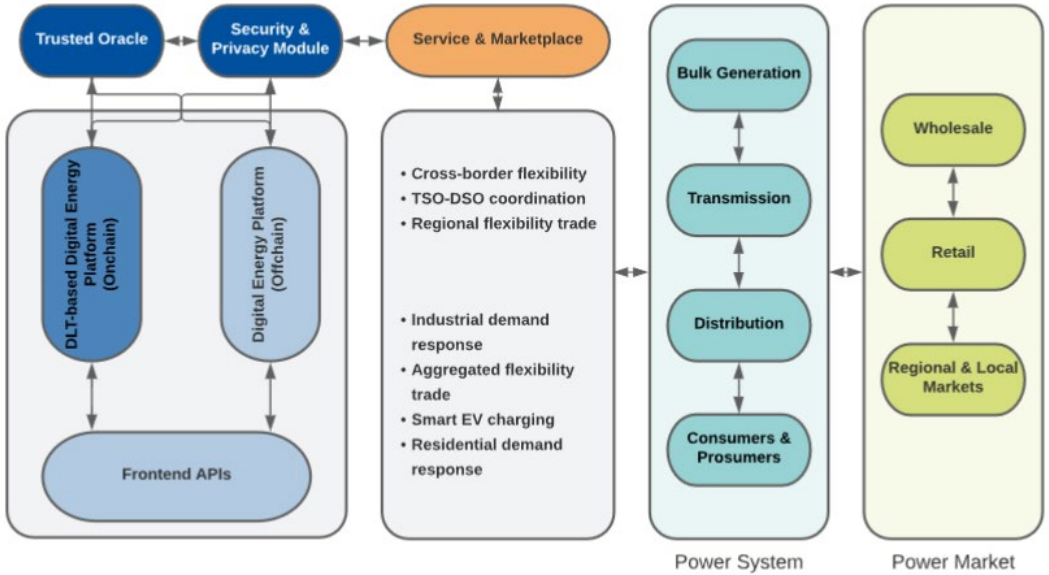
Water supply and drainage systems, which are categorized as critical infrastructure, serve a crucial role in preserving societal health and well-being. Since climate change effects, harsher regulations, population changes, and aging infrastructure pose problems for these systems, the industry is experiencing a digital transition to meet these concerns. This article addresses Cyber-Physical-Social Systems (CPSS) and its application to water distribution networks, combining cyber, physical, and social components for adaptive, responsive, and intelligent management. This paper's primary contributions include a review of recent security problems in the water industry, which emphasizes the necessity for stronger security measures. The article also examines how water distribution networks, as CPSS, fit into the interrelated realms of physical infrastructure, digital components, and stakeholder involvement, necessitating an all-encompassing system design and management strategy. In addition, the article investigates various cyber-physical attack scenarios, risk management methodologies, and the crucial role of integrated knowledge in mitigating these risks. In the context of increasing digitalization, the paper emphasizes the significance of taking into account both water infrastructure regulations under social space, such as the Water Framework Directive 2000/60/EC (WFD), and cyberspace-related legal and legislative standards, such as the Network and Information Systems (NIS) Directive, the General Data Protection Regulation (GDPR) and Cybersecurity Act. By tackling these difficulties and concentrating on privacy concerns, water utilities may contribute to the overall security and resiliency of vital infrastructure while assuring compliance with applicable legislation.





Umit Cali, Murat Kuzlu, Onur Elma, Osman Gazi Gucluturk, Ahmet Kilic, and Ferhat Ozgur Catak. 2023. Cybersecurity and Digital Privacy Aspects of V2X in the EV Charging Structure. In Proceedings of the 2023 European Interdisciplinary Cybersecurity Conferenc (EICC '23). Association for Computing Machinery, New York, NY, USA, 174–180. https://doi.org/10.1145/3590777.3591406

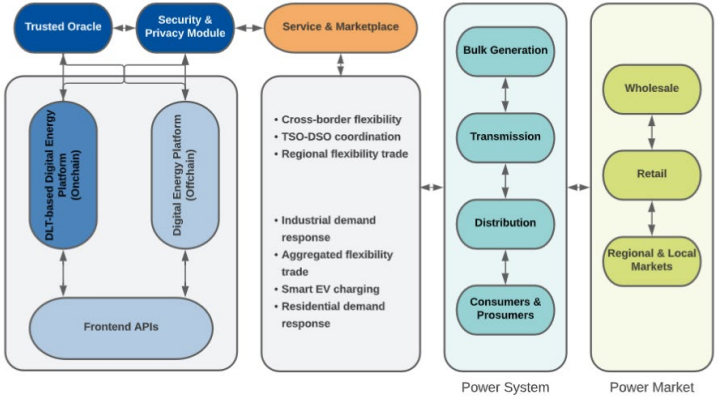
Designing the Next Gen Digital Energy Platforms



Digital Energy Platforms Considering Digital Privacy and Security by Design Principles

Umit Cali, Marthe Fogstad Dynge, Ahmed Idries, Sambeet Mishra, Ivanko Dmytro, Naser Hashemipour, and Murat Kuzlu. 2023. Digital Energy Platforms Considering Digital Privacy and Security by Design Principles. In Proceedings of the 2023 European Interdisciplinary Cybersecurity Conference (EICC '23). Association for Computing Machinery, New York, NY, USA, 167–173. https://doi.org/10.1145/3590777.3591405

Designing the Next Gen Digital Energy Platforms



Scale	Use Case	Technological Maturity [30]	Degree of Privacy Concern	Degree of Cybersecurity Concern
Cross-border	European Cross-Border Intraday (XBID) Solution	●●●●○	●○○○○	●●●●●
National	TSO-DSO coordination [31]	●●◐○○	●●○○○	●●●●●
Regional/	Regional flexibility trading (e.g. NODES)	●●●○○	●●○○○	●●●●○
Local	Industrial demand response reserves	●●●●◐	●●○○○	●●○○○
	Aggregators providing demand-side flexibility [32]	●●◐○○	●●●○○	●●○○○
	Smart charging EVs at commercial buildings and public places	●◐○○○	●●○○○	●●●○○
	Smart charging EVs at residential houses	●◐○○○	●●●●○	●●●○○
	Residential smart appliance demand-side flexibility [33]	●●○○○	●●●●●	●●●●○

Conlusion and Outlook

- COVID 19 levels accelerates the transition to Full Digital Economies
- Digital economies and markets are becoming open targets for cyber attacks
- Digital privacy and cybersecurity aspects are integral part of new energy systems
- Standards: There is no global standards yet
- Legislative and Political support is essential
- Creating technical guidelines on applying software cybersecurity standards
- Promoting collaboration and coordination across standards organizations' cybersecurity and AI technical committees to solve possible cybersecurity issues including trustworthiness and data quality.

VIELEN DANK FUER IHRE AUFMERKSAMKEIT!

THANKS FOR YOUR ATTENTION !

TAKK FOR OPPMERKSOMHETEN!

ILGINIZ ICIN TESEKKURLER !

umit.cali@ntnu.no