Emerging security and economic challenge within renewable energy communities: cost comparative analysis against cybersecurity issues in the evolving RECs scenario

Silvia Ricciuti, Simona Stoklin, Francesca Giuliano, Christian Mari, Massimiliano Zanchiello, Salvatore Manfredi

Fondazione Bruno Kessler, Università di Pisa, Politecnico di Milano, Università La Cattolica, Università di Perugia

sricciuti@fbk.eu, stoklin.simona@gmail.com, francesca.giuliano1@unicatt.it, christian.mari@polimi.it, smanfredi@fbk.eu, massimiliano.zanchiello@gmail.com

Padua, 28-30 November, 2024

8th AIEE Energy Symposium
Current and Future Challenges to Energy Security
– the energy crisis, the impact on the transition –

The Clean Energy for all Europeans Package

The Clean Energy Package has four Directives and four Regulations:

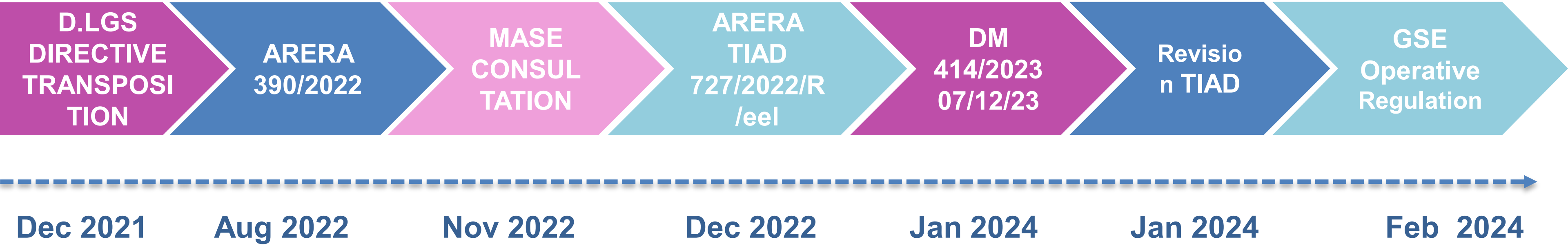
- *Energy Performance in Buildings [Directive (EU) 2018/844]*
- *Renewable Energy [Directive (EU) 2018/2001]*
- *Energy Efficiency [Directive (EU) 2018/2002]*
- *Governance of the Energy Union [Regulation (EU) 2018/1999]*
- *Electricity [Regulation (EU) 2019/943]*
- *Electricity [Directive (EU) 2019/944]*
- *Risk Preparedness [Regulation (EU) 2019/941]*
- *ACER [Regulation (EU) 2019/942]*

The Clean Energy for all Europeans Package

The Clean Energy Package has four Directives and four Regulations:

- *Energy Performance in Buildings Directive (EU) 2018/844*
- ***Renewable Energy Directive (EU) 2018/2001***
- *Energy Efficiency Directive (EU) 2018/2002*
- *Governance of the Energy Union Regulation (EU) 2018/1999*
- *Electricity Regulation (EU) 2019/943*
- *Electricity Directive (EU) 2019/944*
- *Risk Preparedness Regulation (EU) 2019/941*
- *ACER Regulation (EU) 2019/942*

Directive transposition in Italy



D.LGS DIRECTIVE TRANSPOSITION — Dec 2021

ARERA 390/2022 — Aug 2022

MASE CONSULTATION — Nov 2022

ARERA TIAD 727/2022/R/eel — Dec 2022

DM 414/2023 07/12/23 — Jan 2024

Revision TIAD — Jan 2024

GSE Operative Regulation — Feb 2024

Self-consumption configurations for sharing renewable energy:

- ***Renewable Energy Communities (RECs)***
- ***Jointly acting renewables self-consumers***
- ***Renewable self-consumers***

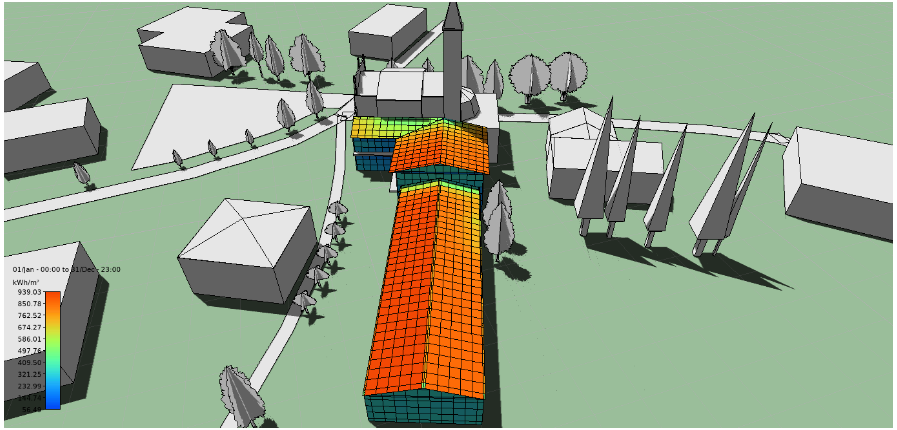
CACER
Self-consumption configurations
for renewable energy sharing

A new energy control strategy: Renewable Energy Communities (RECs)

Renewable Energy communities are entities with an autonomous legal form, members with free access, and a redefining territory underlying the primary electrical substation.

A **REC** has:

- ***Environmental Impact***
- ***Economic impact***
- ***Social impact***



	Bioenergy	Photovoltaic	Eolic	Hydro	Geothermal	Waste	Termic	Total
	MW	MW	MW	MW	MW	MW	MW	MW
Installed power on 2023	*4.100*	*24.200*	*11.700*	*22.800*	*900*	500	55.400	119.600

63.700

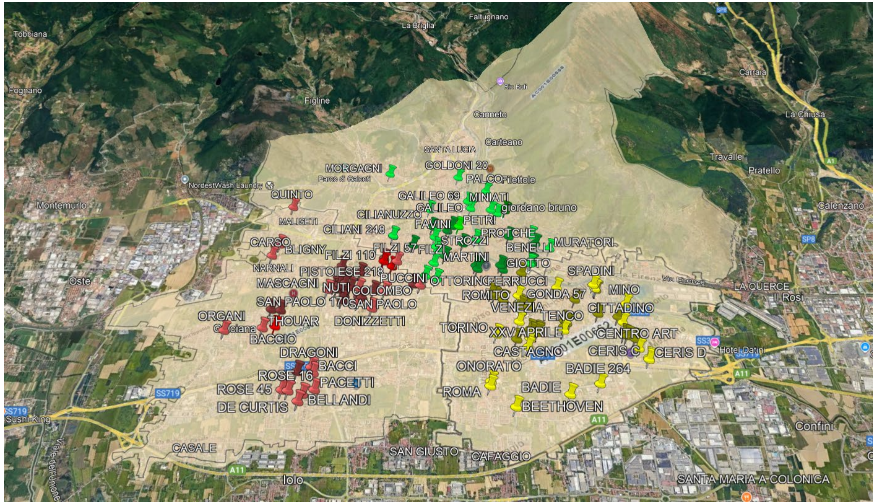
FER X		*50.000*	*16.500*	*630*	
CACER		*7.000*			
Energy Release		*5.500*			
Transizione 5.0		*1.000*			
On 2030	*4.100*	*87.700*	*28.200*	*23.430*	*900*

144.300

CACER 4,85%

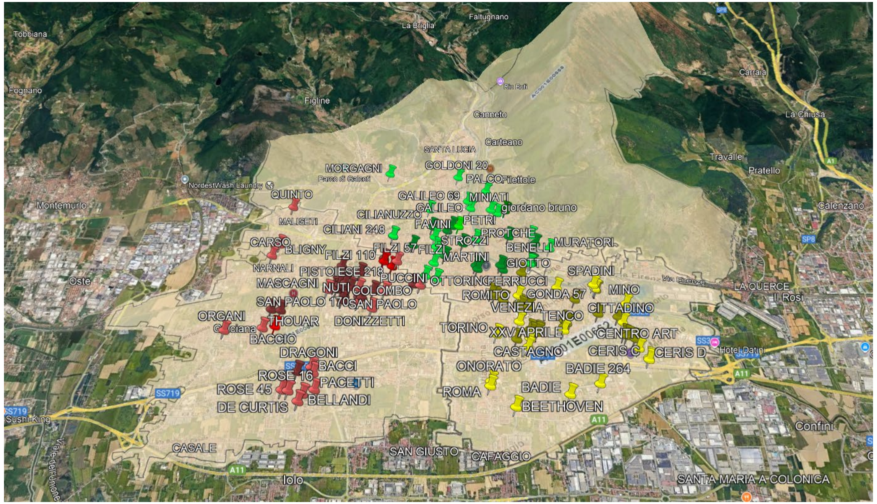
New energy control strategy & new challenges

- Process of establishment and settlement
- Legal representatives
- Common by-law
- Security & legal challenges
- Cybersecurity risks



New energy control strategy & new challenges

- *Process of establishment and settlement*
- *Legal representatives*
- *Common by-law*
- ***Security & legal challenges***
- ***Cybersecurity risks***



↓

REC more complex than other form of energy sharing

Legal Challenges

The legal challenges for a RECs are not only related to the decree 199/2021 implementing RED II, which governs RECs themselves, or to the sartorial choice regarding the legal status to be given to the REC. In fact, since optimizing the operation of the REC requires ***the adoption of building automation systems***, resulting in a ***larger cyber-attack surface***, it is essential to protect the systems from cyber threats.

Legal Challenges

Not only that, but since large volumes of data, including personal data, are managed in the RECs, the protection of the same must also ***be guaranteed according to the provisions of the applicable “privacy” legislation***, which includes the GDPR, the Privacy Code as novated by Decree 101/2018, and whatever else (Supervisory Authority Measures, etc.).

Cybersecurity Threats in RECs

In the case of RECs, in relation to the data managed, it is necessary to ensure the three CIA:

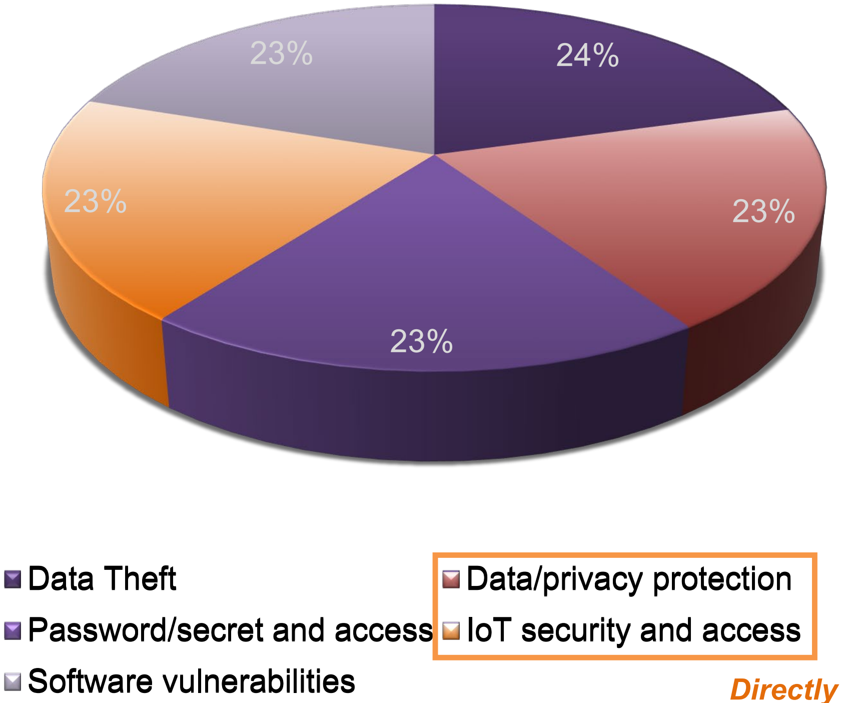
CONFIDENTIALITY **INTEGRITY** **AVAILABILITY**

Possible threats:

- Software threats of the smart grid (ransomware, malware)
- Phishing threats to the community members (Data breaches, theft of personal information
- Intentional threat from member of the community or physical security risks
- Energy system threat through flood of data traffics also called Distributed Denial of Service (DDoS)

Key Cybersecurity Concerns:

80% of organizations experienced an identity-related breach*



Directly involved with RECs

* 2024, Identity Security Threat Landscape Report

Prevention & Defence strategies

NIS2 directive:

- Risk analysis and cybersecurity policies for IT systems;
- Incident management;
- Operational continuity;
- Supply chain security
- Security in the acquisition, development, and maintenance of IT and network systems;
- Strategies and procedures for evaluating the effectiveness of cyber risk management measures;
- Basic digital hygiene practices and cybersecurity training;
- Policies and procedures regarding the use of encryption;
- Human resources security, access control strategies, and asset management (hardware, software, data);
- Use of multi-factor authentication or continuous authentication solutions.

Prevention & Defense strategies

To implement NIS2, organizations must start with a risk assessment to establish appropriate measures. This risk assessment should follow the ISO27005 standard methodology:

- Context Establishment
- Risk Identification
- Risk Analysis
- Risk Evaluation
- Risk Treatment
- Risk Acceptance
- Monitoring and Review

- Legal aspects of mandatory security assessment due to to privacy data potential issues
- Cost relevance that a security assessment of this kind can have

Risk mitigations

A possible risk mitigation strategy aims to reduce the impact and/or the probability of the occurrence of a potentially harmful event by reducing the attack surface:

- implementing secure software platforms for the management of energy communities (especially if such platforms are web-based);
- providing appropriate countermeasures against possible attacks on the LAN communication networks between various types of devices as well as the temporary unavailability of WAN communication networks that connect LANs or use cellular networks;
- securing the smart gateway that links control devices and the software platform, since it is typically an IoT device with low computational power and thus more easily attackable.
- Entrusting the implementation of a REC to specialized personnel for its security is also a risk mitigation measure.

RECs CF/Revenue

$$CF_{tot,cond}^{Y} = T_{inc,cond}^{Y} + T_{sold,cond}^{Y} + R_{cond}^{Y} - C_{man,cond}^{Y} - C_{gest,cond}^{Y} - C_{ass,cond}^{Y}$$

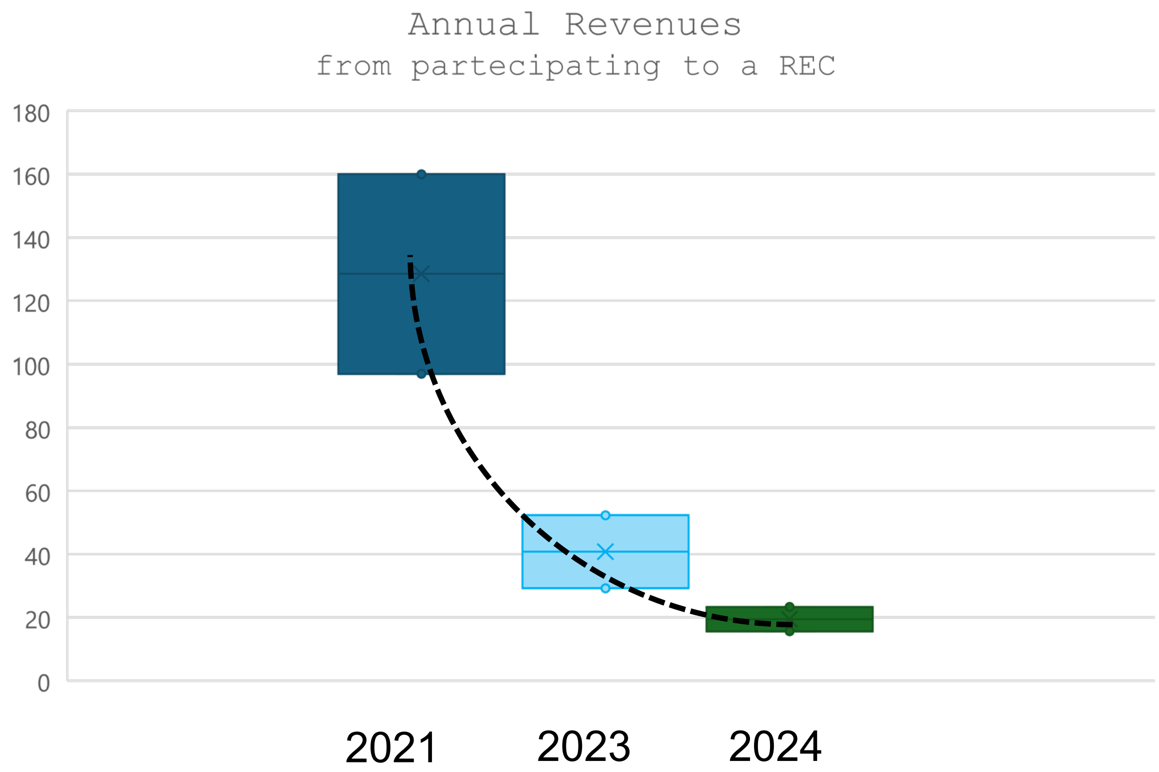
$C_{inv,cond}^{t=0}$ = $Cap_{PV} * C_{PV}$

$C_{man,cond}^{Y}$ =$MC_{PV}^{Y} * C_{pv}$

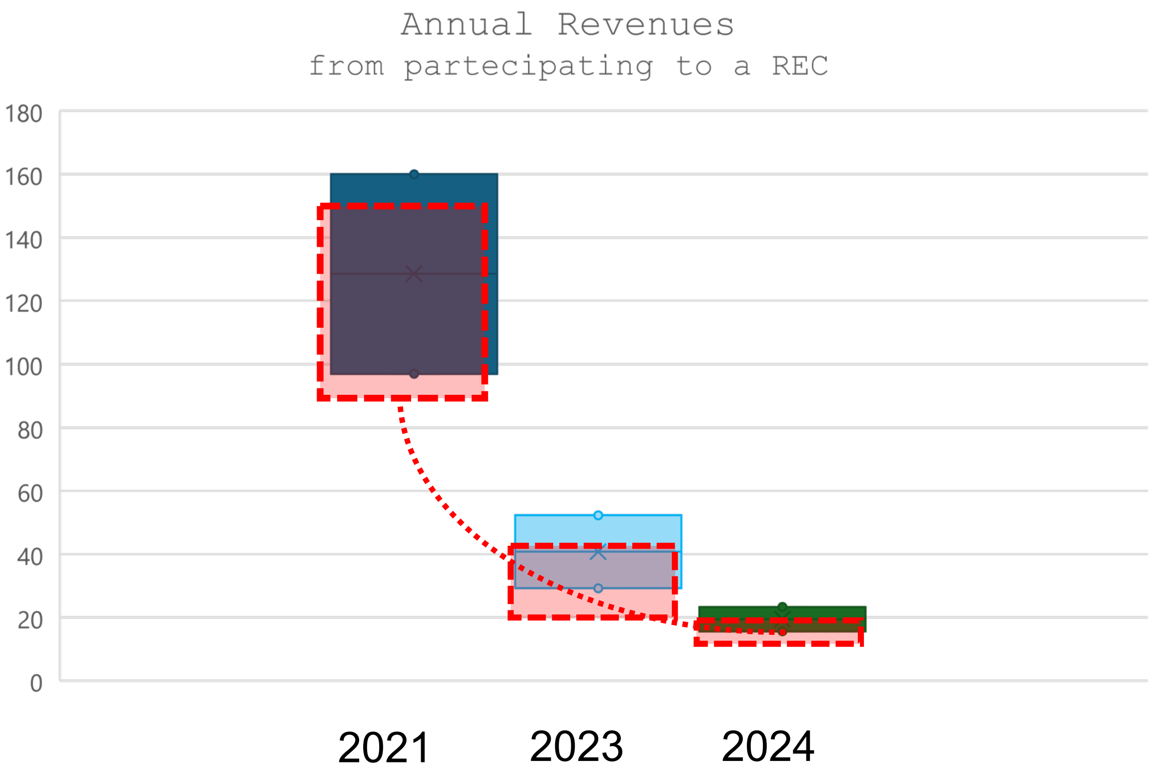
$C_{gest,cond}^{Y}$ = management costs and administrative costs

$C_{ass,cond}^{Y}$ = $AC_{PV} * C_{pv}$

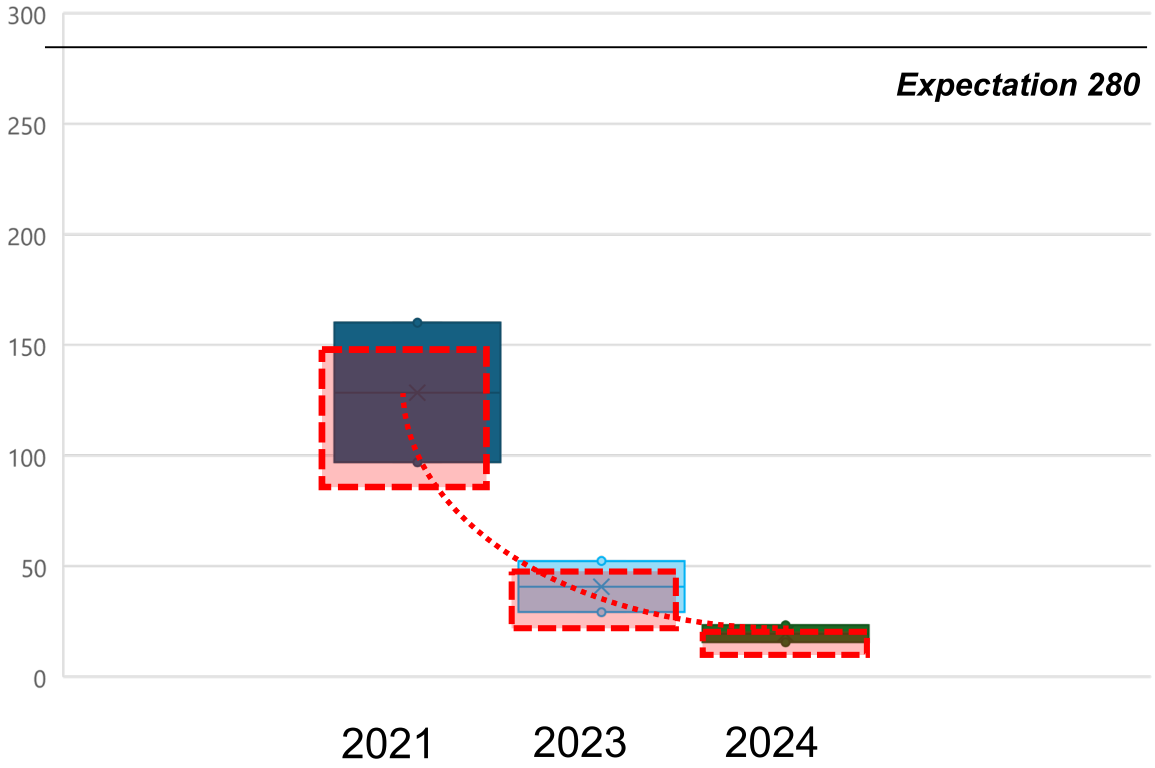
RECs CF/Revenue



vs Cybersecurity Costs



vs Cybersecurity Costs



Conclusions

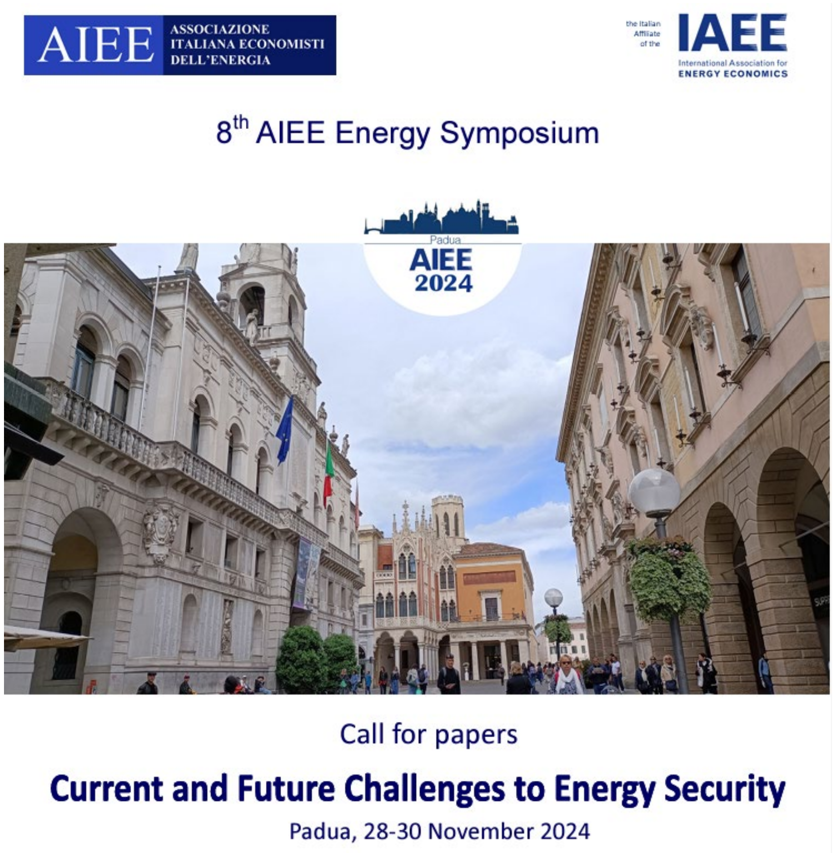
❑ Security and Legal Challenges are emerging with the growth of RECs

❑ Prevention and Defense Strategies must evolve to safeguard both digital and physical infrastructure. It requires additional investments that are not always easy for small/medium communities

❑ Legal Compliance and robust contracts are essential to avoid disputes and liabilities. Legal expertise can come at a significant cost.

❑ Step by step methodology to ensure a prompt intervention and mitigation of cyberattack

❑ But based on current forecasts, the economic revenues of RECs may not be able to support such kind of costs



AIEE ASSOCIAZIONE ITALIANA ECONOMISTI DELL'ENERGIA

the Italian Affiliate of the IAEE International Association for ENERGY ECONOMICS

8th AIEE Energy Symposium

Call for papers

Current and Future Challenges to Energy Security

Padua, 28-30 November 2024

Thank you!

Christian Mari, Silvia Ricciuti, Simona Stoklin,

Francesca Giuliano, Massimiliano Zanchiello

Salvatore Manfredi