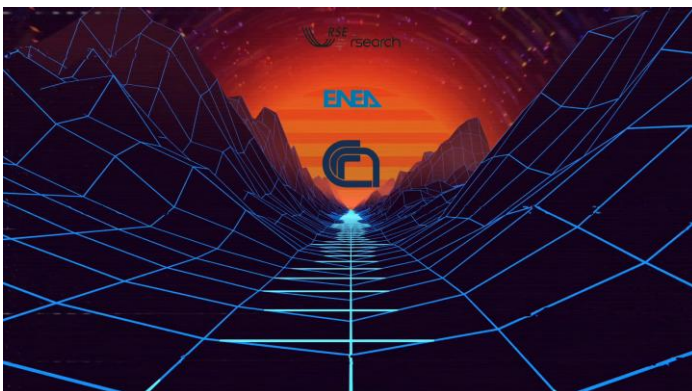


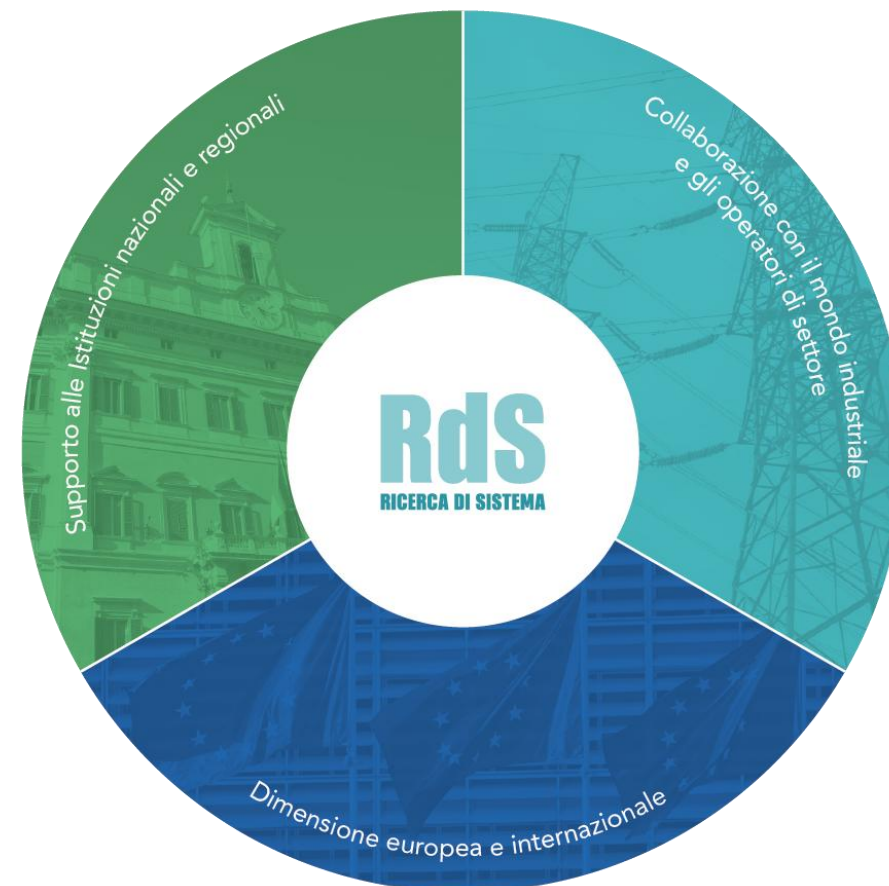
Integrated Project Cyber security of energy systems for the digital-energy transition



RSE S.p.A. - Energy System Research is a company indirectly controlled by the Ministry of Economy and Finance through its sole shareholder **GSE S.p.A.** RSE supports the Ministry of the Environment and the Energy Security (MASE) and the Regulatory Authority for Energy Networks Environment (ARERA).

Through the fund for the **System Research (RdS)**, it carries out **research activities**, with an **experimental and applied research approach**, on the entire **energy sector**, with a specific focus on **strategic projects (national and European)**, involving the centralized and local public administrations, the entire productive system in its broadest articulation, the associations of consumers and SME, in synergy with other research centers.

RSE represents **a connection between policy makers, the business community and citizens.**





Our company in a snapshot

TOTAL

staff in force

~380

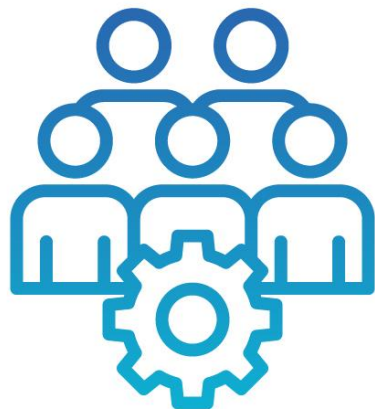


average age

46 years

average seniority

15 years



NEW HIRES FROM 2024 TO 2025

average age

32 years



LABORATORIES AND VENUES

laboratories

50+

RSE Milan

Via Rubattino, 54

RSE Rome

Via Maresciallo Pilsudski, 122/124

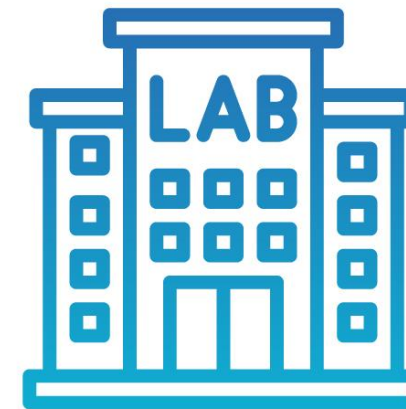
Via Antonio Bosio, 15

RSE Piacenza

Via Callegari

RSE Brugherio (MB)

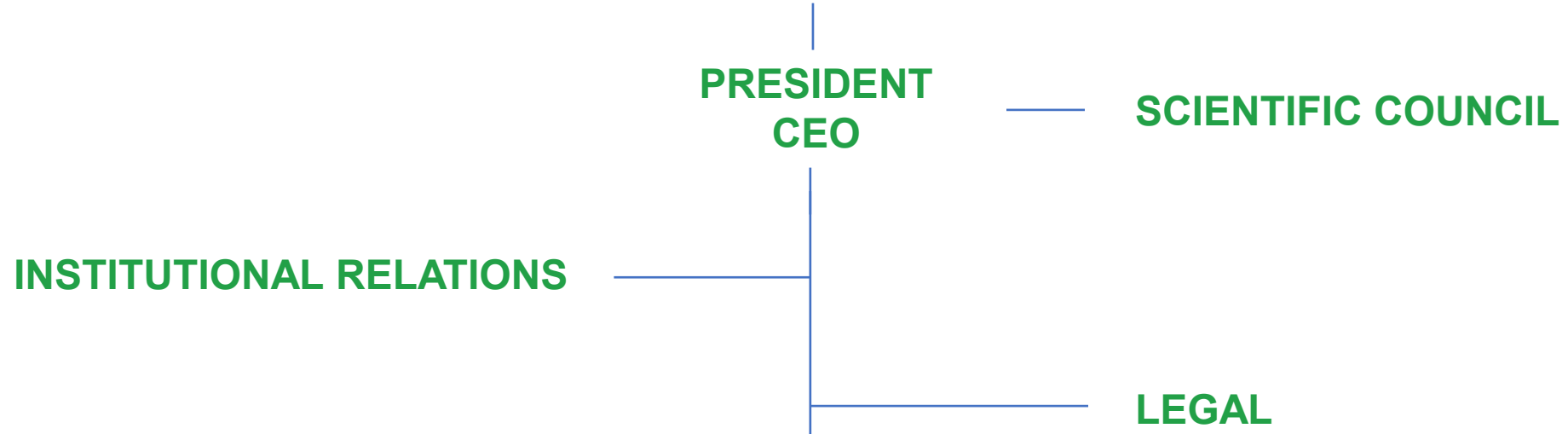
Via Matteotti, 105





Structure

BOARD OF DIRECTORS



DEPARTMENTS

EUT - Land and End-Use Energy Efficiency
SFE - Sustainable Development and Energy Sources
SSE - Energy Systems Development
TGM - Generation Technologies and Materials
TTD - Transmission and Distribution Technologies

CROSS SECTOR UNITS

ASI - Administration and Information Systems
HRM - Human Resources Management
SCV - Development, Communication and Enhancement
SQA - General and Technical Services, Quality and
Environment



RSE has been involved in more than **100 research projects** funded within various European supporting frameworks, and **coordinating** more than **20 projects**, and involving about **1000 partners**.

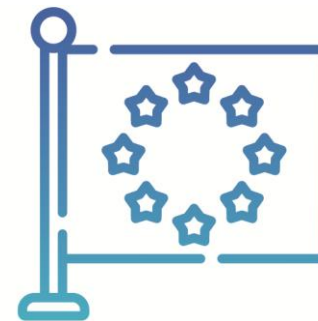
100
Projects

20
Projects led
as coordinator

1000
Partners

The **main goal** of the EU funded projects involvement is the **enhancement** and the **validation** of RSE knowledge and research capacity within an international environment, and the diffusion and further **enhancement of the Italian System Research (RdS) projects' results**.





RSE supports the **European Commission** pursuing the objectives of the energy transition, through the implementation of the *Clean Energy Transition Partnership (CETPartnership)*. RSE is involved in several *Technology Collaboration Programs* promoted by the IEA (International Energy Agency), coordinating the *ISGAN - International Smart Grid Action Network*.

RSE is active from the earliest stage in **Mission Innovation (MI)** and leads the *Green Powered Future Mission*.

- research plan for the national electricity system for the **three-year period 2025-2027**
- approved on 6 November 2024 by the Ministry of the Environment and Energy Security
- assignment of research activities to RSE, ENEA, CNR and distribution of resources carried out under Program Agreements
- RSE participates to the plan in 19 research areas, including 4 integrated projects, total RSE budget:143 ml EUR
- P2.1 Integrated Project Cyber security of energy systems for the digital-energy transition, coordinated by RSE, project budget 8,813 ml EUR



PROGETTI - RICERCA DI SISTEMA
2025

Progetto Integrato Cyber Security dei sistemi energetici per la transizione energetica-digitale

Il progetto integrato per la sicurezza informatica dei sistemi energetici assicura la protezione dei dati e dei processi digitali, in linea con il PNIEC 2030, la Direttiva NIS2, il Decreto Legislativo 138/2024 e le linee guida dell'Agenzia per la Cybersecurity Nazionale.

DECISORI INDUSTRIA RICERCA

#Controllo Generazione Distribuita
#Controllo Infrastrutture di Ricarica
#Cyber Anomaly Detection
#Cyber Attack Forecast #Cybersecurity
#Cybersecurity Assessment
#Cybersecurity Operation
#Cybersecurity Performance Testing
#Digitalizzazione #Intelligenza Artificiale
#IoT #Normativa #PNIEC #Resilienza
#Sistemi Cyber-Fisici
#Smart Energy Systems
#Transizione Energetica

Acronimo	Denominazione	Tipo Ente	Affidatario di riferimento
CNR	Consiglio Nazionale delle Ricerche	Affidatario	
RSE	Ricerca sul Sistema Energetico	Affidatario	
ENEA	Agenzia nazionale per le nuove tecnologie, l'energia e lo sviluppo economico sostenibile	Affidatario	
UNICA	Università della Calabria - Dipartimento di ingegneria informatica, modellistica, elettronica e sistemistica -DIMES	CoBeneficiario	CNR
DAFNE	Università degli Studi di Foggia - Dipartimento di Scienze Agrarie, Alimenti, Risorse Naturali e Ingegneria	CoBeneficiario	ENEA
ROMA3-DICITA	Università Roma Tre - Dipartimento di Ingegneria Civile, Informatica e delle Tecnologie Aeronautiche	CoBeneficiario	ENEA
UNIMO	Università del Molise- Dipartimento di Medicina e di Scienze della Salute "Vincenzo Tiberio"	CoBeneficiario	CNR
UNINA-DII	Università degli Studi di Napoli Federico II - DIPARTIMENTO DI INGEGNERIA INDUSTRIALE	CoBeneficiario	ENEA
UniPD-QTech	Padua Quantum Technologies Research Center	CoBeneficiario	ENEA
IMT	Scuola Alti Studi Lucca- IMT	CoBeneficiario	CNR
UNIGE	Università degli Studi di Genova - Dipartimento di Informatica, Bioingegneria, Robotica e Ingegneria dei Sistemi	CoBeneficiario	ENEA
UNIME	UNiversità di Messina - Dipartimento di Ingegneria	CoBeneficiario	CNR
UNIFI	Università di Firenze- Dipartimento di Matematica e Informatica 'Ulisse Dini'	CoBeneficiario	CNR
UniTN	UNITRENTO - Dipartimento di Ingegneria e Scienza dell'Informazione	CoBeneficiario	ENEA

DIGITALIZATION AND NETWORK EVOLUTION



- "To achieve the necessary developments in energy security... we cannot ignore the strengthening and **digitalization** of infrastructure."
- "The spread of **self-consumption** will naturally be favored by the diffusion of **digital technologies**, along with the **Internet of Things** and **greater accessibility to small- and medium-sized generation and storage systems**."
- "Digitalization will play a **cross-sectoral enabling role**, offering opportunities for acceleration across **the entire battery sector**. **Digital twins and big data analytics** will be crucial for the advancement of **battery management systems (BMS)**."
- "Achieving ambitious **decarbonization goals** requires, in addition to a **high degree of reliability, security, and flexibility** of the national energy system, its **substantial integration with digital technologies**, ensuring both **optimized management of renewable energy production** and the enabling of **greater electrification of consumption**."



- **Legislative Decree 2024/138**, Italian implementation of **European Directive NIS2 2022/2555** concerning measures for a high common level of cybersecurity in the Union



- **Cyber Resilience Act: European Regulation 2024/2847** concerning **horizontal cybersecurity requirements for products with digital elements**



- **Network Code on Cybersecurity: European Delegated Regulation 2024/1366** concerning sector-specific provisions for **cybersecurity aspects of cross-border electricity flows**

OB1 Ensure the **adequacy of cybersecurity technologies** in digital applications for energy control

- Energy applications that **interconnect energy operators and prosumers**
- Remote **control networks**
- Cyber **risks**
- **Telecommunication carrier** cybersecurity
- **Communication protocol** cybersecurity

OB2 Preserving the **resilience** of the electricity system from cyber attacks

- **Tools and technologies** to mitigate the vulnerability of energy networks
- Strategies, actions, and **protection schemes** to make them cyber-resilient

OB3 Leveraging **AI technologies** for energy services cybersecurity

- Tools and environments that leverage the potential of **AI to detect** new cybersecurity threats
- Tools and environments that **preserve** data and computational **privacy**
- Robust AI algorithms capable of resisting **generative and explainable** attacks

WP1

Cybersecurity technologies for new digital energy control applications

11 AL

WP2

Cybersecurity for more resilient **cyber-physical energy infrastructures**

15 AL

WP3

AI for cybersecurity and privacy of energy services

25 AL

WP4

Regulation, Standards and Dissemination

7 AL

WP1 – Cybersecurity technologies

- **Cryptographic schemes and algorithms** for cyber-immune control and automation systems, leveraging **security standards** and **resistant to quantum computer** attacks
- Digital **key management and certificates** for the cybersecurity of large-scale energy services
- **Compliance with cybersecurity standards** for **commercial** control and communication **devices** deployed in energy networks and microgrids
- **Quantum cryptography** in remote control communications and management of flexible energy resources
- Testing of smart grids with **fiber and air transmission channels** equipped with **quantum cybersecurity protection**
- Fiber and air communication **protocols for quantum cybersecure networks** in energy distribution
- Security, **trust, and privacy** in electric vehicles and their interaction with smart grids
- **Observatories** for cybersecurity governance and management

WP2 - Cybersecurity for more resilient cyber-physical energy infrastructures

- Digital models for the creation of **cybersecurity twins** for energy grid resilience assessments against cyber attacks
- **Cyber-power co-simulation**
- Digital twins of **multi-vector energy grid** components
- AI techniques for energy grid **intrusion detection**
- Cyber anomaly detection properties of **electrical protection devices** integrated into energy grids
- **Design and management strategies** for protecting energy systems from cyber risks
- Security, privacy, and trust for **energy communities**
- Trustless and post-quantum security for data collection and analysis for managing **Federated Smart Grids**
- Dynamic multi-criteria **risk assessment**; **dynamic system compliance** with cybersecurity **policies**

WP3 - AI for cybersecurity and privacy of energy services

- **GAN** techniques for dataset generation and intrusion detection algorithm evaluation
- **Quantum Machine Learning** for smart grids
- **Event and measurement analysis** for cyber attack detection on networks, microgrids, and energy applications, stream analytics architectures, systems for collecting, storing, and analyzing OT data flows
- **Intrusion detection** using **Artificial Intelligence techniques**, including generative adversarial networks and explainable AI, to improve attack prediction capabilities and automatic response to malicious actions
- AI methodologies and tools for **access control** and dependency analysis using formal methods
- **FDI detection** algorithms for resilience assessments
- Cyber threat **mitigation strategies** through automatic isolation of portions of communication networks
- **Privacy protection and data trust** in energy service meters and controllers
- **Blockchain** for energy smart grids on conventional architectures; **proof-of-work** using low-power, highly parallel devices
- **Cloud-native** smart grid security

Lab PCS-ResTest



Lab IoT



EV Charging Inf.



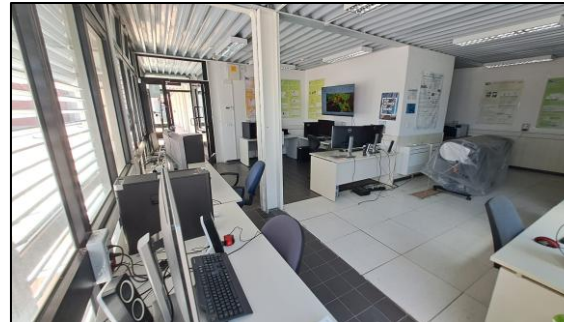
Test Facilities Milan & Piacenza



Electrical Nanogrid



Lab isense&Geomatics



Lab ICT – Cresco Infrastructure



Server Farm



EV Car



MV Grid Favignana Test Site



WP3
WP1
WP3
WP2
WP2
WP3
WP3
WP3

Agenda	Entity	Speaker
Integrated Project Cyber security of energy systems for the digital-energy transition	RSE	G. Dondossola
Securing the Power Grid: Strategic Methodologies and Technical Solutions	ENEA	M. Celino
An integrated framework for evaluating standard-based and quantum-safe cybersecurity solutions for electrical energy applications	RSE	M.G. Todeschini
Power Consumption Anomaly Detection Using Threat-Driven Data Injection	UniFI	T. Zoppi
Design of cybersecurity twins based on ICT-power co-simulation	RSE	R. Terruggia
Damn Vulnerable Infrastructure: are you ready for the next StuxNet	IMT-Lucca	G. Costa
AI-based techniques and tools for cybersecurity energy ranges	RSE	R. Terruggia
Attack scenarios to charging infrastructure communications	UniCA	L. Pisu
A method for smart grid intrusion detection through explainable deep learning	CNR	G. Ciaramella

Thank you for the attention

Progetto Integrato Cyber Security dei sistemi energetici per la transizione energetica-digitale - RSE

Giovanna Dondossola

Maria Valenti

Fabio Martinelli