After the RISEnergy Transnational Access, Users are required to submit a User Report. This should be done within 4 weeks after the Access is completed unless otherwise agreed. The User Report will be given to the User(s) by the WP2 leader. The report contains sections related to the work performed, the main results and observations that were achieved.

This document should be completed, signed, and sent by e-mail to risenergy@for.kit.edu.

Summary questionnaire for Users who have been granted Transnational Access (TA) under the RISEnergy project Horizon Europe TA scheme. More information on RISEnergy TA can be found in "General Rules" and in "Access Policy" which can be found on the RISEnergy webpage.

Please complete, sign, and send this form, together with the Cost claim by e-mail to risenergy@for.kit.edu with title: RISEnergy APPXXX - reports.

General information about the project	
Project title (as used in Application)	Cyber Attack Resilient Accelerated Protection Scheme
Project number (APPXXX) and acronym (max 15 characters)	APP203 and CARAPS
RISEnergy RI(s) accessed	TA25-ICCS-ESES-lab
Keywords (up to five, free text)	Smart grid, real-time digital simulator, cyber-attack, phasor measurement units, information and communication technologies.
Arrival date (in town where RI is located)	06.01.2026
Departure date (from town where RI is located)	24.01.2026
Starting date of Access (first day at RI)	07.01.2026
Finishing date of Access (last day at RI)	23.01.2026
Number of days not using the RI (during the above period)	04 days
Reason for not using RI those days (describe)	All Saturday and Sundays
Number of days using the RI	13 days
Number of Users granted Access (group size)	2 persons
Comments	None
User	

User group leader or sole applicant (user group member 1)	
First name	
Last name	
Affiliation / Employer	
Country of Employer	
E-mail	
User travelling to RI?	
Comments	
User group member 2	
First name	
Last name	
Affiliation / Employer	
Country of Employer	
E-mail	
User travelling to RI?	
Comments	

Access Summary Report - work performed and initial results

Brief description of the objectives of your project (up to 200 words)

[Please describe short the main objectives of your project]

The scope of this project is to enhance the security and reliability of the cyber-resilient accelerated protection scheme during various cyber threats. The project focuses on analysing the performance of various available communication assisted protection scheme, identifying the challenges and integrating cyber-security measures that can detect, respond to, and recover from potential cyber-attacks. Implementations will be done on a real-time experimentation environment, where the resilience, performance and effectiveness of the developed mechanism will be thoroughly tested and validated. The outcome will include a robust detection and resilient mechanism assisted accelerated protection scheme for cyber-attack conditions. This project focuses on integrating cybersecurity resilience into conventional protection techniques to maintain operational integrity, confidentiality, and availability during cyber events.

Objectives:

- To validate the cyber resilient scheme through the real-time system environment under various cyber-attack conditions.
- To analyse vulnerabilities in existing communication-based protection schemes under critical conditions.
- Developing the advance detection technique for several attacks such as delay attack, false data injection attack, packet drop attack, etc.

- Ensure fast and secure operation of method under fault conditions and prevent operation during cyber-attack. Ensure the trip signal is sent by the line current differential relay (LCDR) only when there is a real fault.
- To test the developed cyber-attack detection framework in real-time system.

Activities performed (up to 600 words)

[Please summarise the work carried you (steps taken, instrumentation used, techniques employed, data sources consulted etc.)]

The experimental set-up consists of software and hardware infrastructure, supporting offline and real-time simulations, such as hardware-in-the-loop testing along with the information and communication technologies (ICT). The power system model is simulated in RSCAD of the RTDS system. The analog signals from RTDS are used to transmit the current information measured by simulated current transformer (CT) to phasor measurement units (PMUs). The steps of the work performed at the ICCS-ESES laboratory is described below:

1. The modelling of power system (IEEE 9-bus system) is carried out in the RSCAD.
2. The transmission line designated for line differential protection testing is identified. All measurement devices, including current transformers (CTs) and potential transformers (PTs), are installed on the corresponding transmission line.
3. The current and voltage data are plotted and analysed within the 'Runtime' tab of RSCAD//RTDS.
4. All measurements are stored for subsequent offline logic formulation.
5. Additionally, the RTDS transmits current information to PMUs via analog output using wired connections.
6. The PMU is subsequently connected to an open phasor data concentrator (PDC) to facilitate data transmission via the IEEE C37.118-2005 communication protocol.
7. The network simulator (NetSim) software, installed on a client laptop, functions as an intruder to generate cyber-attack scenarios.
8. False data injection attacks (FDIAs), including scaling, ramp, pulse, and delay attacks, are simulated using NetSim during the transmission of information from the PMU to the open PDC.
9. All data from the RTDS and the open PDC have been collected by the users for subsequent analysis.
10. The entire hardware system is integrated into the local area network (LAN) using a TCP/IP-based architecture.

To show the step-by-step activities, the flow diagram is illustrated in Figure 1.

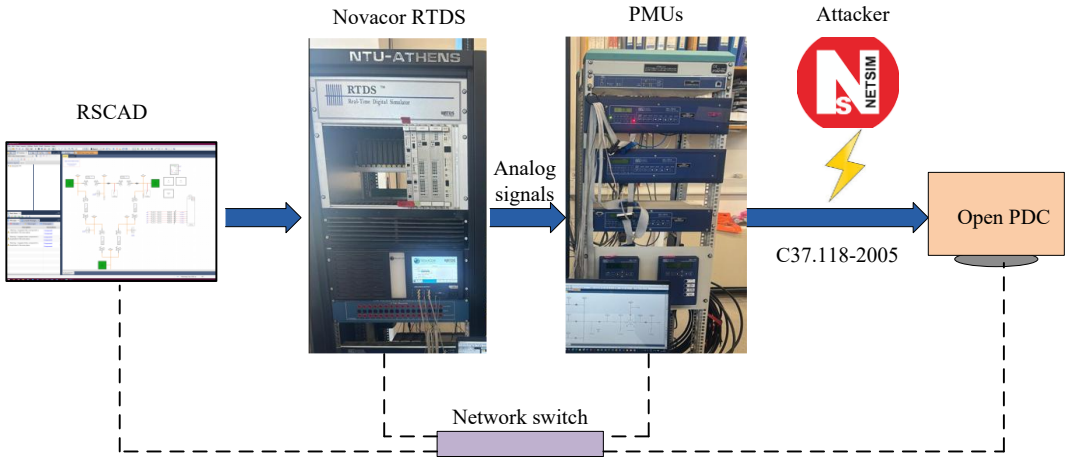

Figure. 1. Flow diagram of the real-time hardware system with RTDS.

The NetSim software is equipped with an integrated attack manipulator tool, through which various attacks such as incremental attack (scaling attack), decremental attack, ramp attack, pulse attack, random noise attack time synchronous attack and attacks of frequency can be implemented. Figure 2 shows the NetSim mimic used to implement the attacks. Through the manipulator interface, one can manipulate the magnitude of measurements for any desired values by entering the values in "Bias (%)" selection. Upon applying the bias, the resulting change in the measurement magnitude is immediately reflected in the OpenPDC visualization graphs, thereby enabling real-time observation of the attack impact.

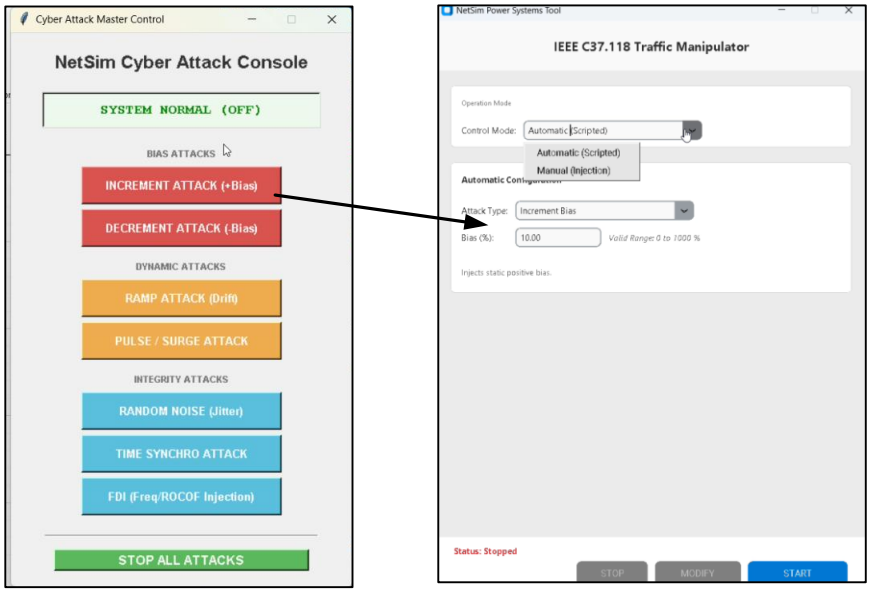

Figure 2. Mimic showing the types of attacks in NetSim software.

Scientific results (up to 800 words)

[Summarise the (initial) outcomes of your study at the RI(s).]

During the access to the ICCS-ESES lab. The users have build-up the simulation in RTDS which is shown in Figure 3.

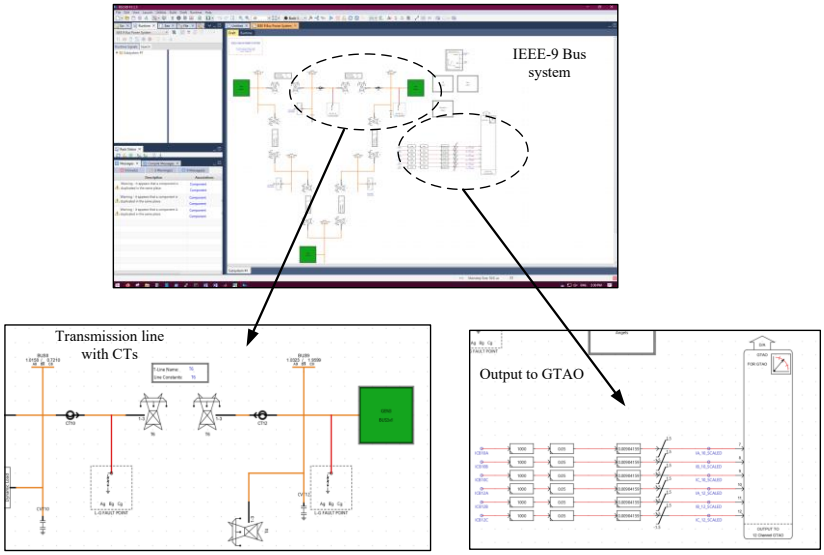

Figure 3. Simulation of system in RSCAD

The information from RTDS to PMU and then PMU to open PDC is recorded in "Graph Measurement" of open PDC. The recorded graph is shown in Figure 4. This value of currents are non-attacked values. It can also be said that these current values are before the attack.

Figure 4. Current waveforms in open PDC.

After the attack through the NetSim software, the current information is manipulated by an scaling attack with 10% increment of the current value. This attack is done on the current information transmitting from PMUs to open PDC. The attacked scenario is shown in Figure 5.

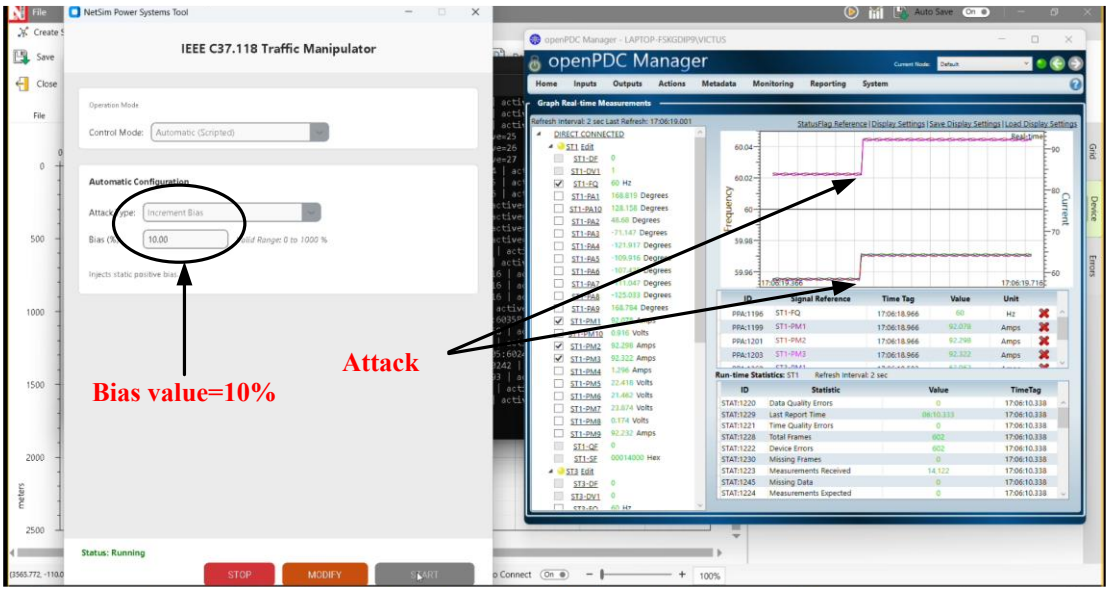

Figure 5. 10% incremental scaling attack on the current waveform.

Figure 6. shows the incremental attack with very less bias value of 1%. Since this value is hard to detect and is considered as normal operating value, it is very challenging for any intelligent electronic devices (IEDs) to detect this attack.

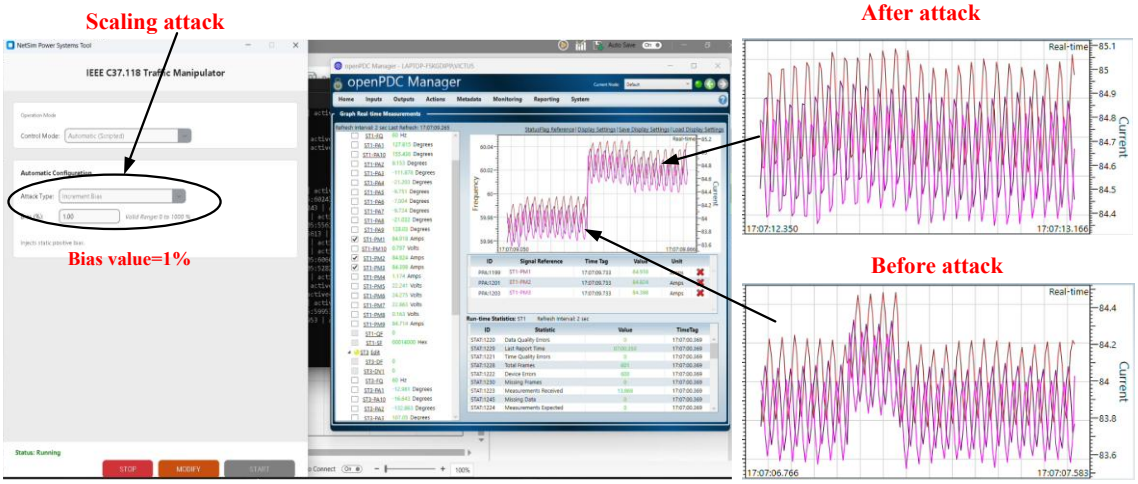

Figure 6. Incremental attack of bias value of 1% in the current waveform.

In addition to the scaling (incremental or decremental) attack, an attack strategy for ramp attack is also executed through NetSim. Figure 7, shows a ramp attack with the bias value of 0.05% on the current waveform.

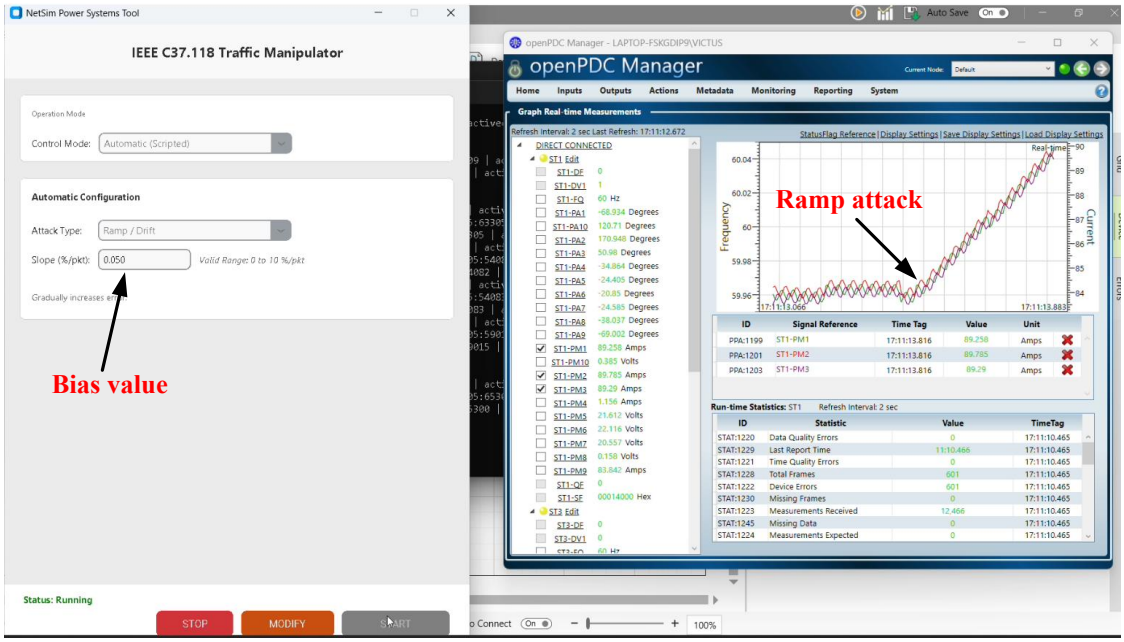

Figure 7. Ramp attack with 0.05%bias value.

Interpretation of the results (up to 400 words)

[Discuss the data obtained and describe the major scientific conclusions drawn.]

The experimental setup demonstrates attack scenarios within a real-time system and the real-time transmission of information from the PMU to the open PDC. This configuration provides a concise scenario for a wide area monitoring and protection system (WAMPS), illustrating the potential for attacks when information flows from the PMU to the central PDC.

Tests conducted in the ICCS-ESES laboratory using the complete hardware setup enabled the collection of real-time data from the real-time digital simulator (RTDS) and attack-related information from the open PDC. The collected dataset includes the records of healthy system operation, internal faults, and external fault scenarios, specifically considering line-to-ground (LG), line-to-line (LL), and three-phase (LLL) faults. All data are collected in CSV format. This dataset can be further utilized to develop attack detection algorithms in MATLAB or on microprocessor-based platforms, facilitating discrimination between compromised and fault-induced data.

Main achievements during the TA related work (up to 250 words)

[Describe the main achievements during your stay at the site(s), Outputs (results, publications, models, etc.), conclusions, next steps, potential impact]

Through this process, both the user and the Research Infrastructure (RI) provider acquired knowledge about cyber-attack scenarios in real-world systems. The key insights are as follows:

1. The communication process between the PMU and the open PDC.
2. The use of NetSim software to simulate cyber-attacks targeting measured data.
3. The transfer of information from the RTDS to MATLAB.
4. The transfer of information from the open PDC to the client system, which is subsequently used to develop an attack detection algorithm in MATLAB.

Data Management

[Describe the further usage and storage of project data. State where the data will be kept and name a person responsible for the data. Define data]

During the visit, the users have stored the data generated from RTDS on the computer provided by the RI provider. The stored information contains CSV files of the test results, ".rtfx" files corresponding to the simulation models, and all the supporting files for executing the models in RTDS. These data are subsequently used to perform offline tasks and post-processing works after the user returns to their home institution. All the data are transferred to a pen drive brough by the user. The original dataset is also available in the computer provided by the RI provider for their use.

Difficulties during the TA related work (up to 250 words)

[List problems and issues, you had, completing out your research project: Did you get access to all the necessary equipment, facilities, databases, etc.?
If not, please specify the problems that occurred and list equipment the was not working or accessible.]

During the visit to the ICCS-ESES laboratory, the users did not find any problems related to the test setup. All the necessary equipment were working well as per the discussion held before the lab visit.

Intended publications

[Explain where and how you expect to publish the outcomes of your project work. Include also anything already published (What and where?)]

Yes, the users are interested in preparing manuscripts based on the research conducted in the ICCS-ESES laboratory, with appropriate acknowledgment of the RISEnergy platform. This paper will be submitted to a reputable journal.

Expected impact

[The impact the expected results will have on current and future research or practice, public safety, European standardization, competitiveness, integration and cohesion and on sustainable growth. any follow on proposals, projects, collaborations, commercialisation]

The work will support in validating a cyber resilient protection framework capable of operating under various cyber-attacks and fault scenarios. This will enhance the understanding of the impact of cyber-attacks on substation automation system and developing mitigation solutions.
Moreover, the outcome of this research work aligns with the objectives of EU Network Code on Cybersecurity for the Electricity Sector [1]. This outcome will contribute to enhance cyber-resilience, improved monitoring, detection capabilities and support compliance with new regulatory requirements for the secure operation of critical electricity infrastructure.
The outcomes of this project will be submitted for publications in the reputed peer-reviewed journals. Furthermore, the project will serve as a foundation for future collaboration between National Institute of Technology, Raipur with ICCS-EES, NTUA, focusing on the development of impactful research projects and strengthening a strong international collaboration between the two universities, aiming to deliver sustainable solutions for smart grid systems.

[1]. New network code on cybersecurity for EU electricity sector - European Commission

Conclusions / additional comments
[Provide any other comments you might have on your work] The users successfully conducted the real-time experiments related to cyber-attack using real-time hardware setup such as RTDS, PMU and associated communication infrastructures. Various cyber-attack scenarios were effectively implemented using the NetSim software brought by the users, showcasing the realistic emulation of malicious data injection in the communication assisted measurements. The experimental results demonstrate the feasibility of the study to formulate the attack resilient schemes in the substation automation system.
Did you complete the European Commission User questionnaire https://ec.europa.eu/eusurvey/runner/RIsurveyUSERS?
☐ ✓ *Yes* ☐ *No*

Feedback – HSE, Ethics and Satisfaction

Please rate on a scale from 1 (excellent) to 5 (poor). Feel free to provide additional comments

	1 (excellent)	2	3 (neutral)	4	5 (poor)
Practical information on how to apply for Transnational Access and the overall application process	☐✓	☐	☐	☐	☐
Comment					
Information provided, once your project was accepted, on how to proceed	☐✓	☐	☐	☐	☐
Comment					

Support received at the site(s) regarding technical/scientific matters and logistics	Have you got sufficient support from the RI staff during the project? If not, please, specify the problems. ☐ ✓ *Yes* ☐ *No*
Please specify any problems	
RI extension / upgrades required	In your opinion, is the RI needed to be upgraded? If yes, please give an explanation. ☐ *Yes* ☐ ✓ *No*
Please specify	

Problems with local regulations	Have you had any problems with regulations of the visited RI owner (HSE, lab working hours, etc.)? If yes, please, specify ☐ *Yes* ☐ ✓ *No*
Please specify	
Health and safety issues	Did you encounter any health or safety issue during your research? Please provide details. ☐ *Yes* ☐ ✓ *No*
Please provide details	
Environment & Ethics	Did your research involve the use of elements that may cause harm to the environment, to animals or plants? Please provide details. ☐ *Yes* ☐ ✓ *No*
Please provide details	
Environment & Ethics	Did your research deal with endangered fauna and/or flora and/or protected areas? Please provide details. ☐ *Yes* ☐ ✓ *No*
Please provide details	
Environment & Ethics	Did your research involve the use of elements that may cause harm to humans, including research staff? Please provide details. ☐ *Yes* ☐ ✓ *No*
Please provide details	
Environment & Ethics – Dual use	Does your research have the potential for military applications? Please provide details. ☐ *Yes* ☐ ✓ *No*
Please provide details	
Environment & Ethics – Misuse	Does your research have the potential for malevolent /criminal/terrorist abuse? Please provide details. ☐ *Yes* ☐ ✓ *No*
Please provide details	
Environmental issues	Were any potentially dangerous substances (materials / gases etc.) released into the environment (atmosphere, water, or land)? Please provide details. ☐ *Yes* ☐ ✓ *No*

Please provide details	
Ethics issues	Are there any other ethics issues that should be taken into consideration? Please specify ☐ *Yes* ☐ ✓ *No*
Please provide details	

Overall impression of communication and interaction after finishing your TA and related work	1 (excellent)	2	3 (neutral)	4	5 (poor)
	☐✓	☐	☐	☐	☐

Comment
Suggestions for facilities not included in RISEnergy which you would use for your research
[Please provide suggestions for specific type of facilities missing (RI gaps) or measurement / experiments you would like to perform which can not be done on current RISEnergy facilities.] Not any.
Suggestions how RISEnergy can improve future TA programme, how to make the TA more impactful and how to enable the achievement of high TRL levels
[Your suggestions]

Feedback – Pro-active Innovation Support

Awareness	Did you know about the pro-active innovation support of RISEnergy? ☐ Yes ☐ No
[Please specify how you learned about the pro-active innovation support]	
Personal experience	Have you taken advantage of or benefited from the pro-active innovation support? ☐ Yes ☐ No
[*Please provide details]*	

Information/service provided by the pro-active innovation support?	1 (excellent)	2	3 (neutral)	4	5 (poor)
	☐	☐	☐	☐	☐

[*Please provide details]*

I declare that the above provided information and especially that information on the number of days visited the RI is correct.

☒ *I have read the RISEnergy privacy policy for participation in the RISEnergy TA and consent to participation and the associated data processing.*

Your full name:

Your signature: