European Research Infrastructure supporting Smart Grid and Smart Energy Systems Research, Technology Development, Validation and Roll Out – Second Edition

Project Acronym: **ERIGrid 2.0**

Project Number: **870620**

Technical Report Lab Access User Project

Adaptive protection for microgrids based on communication (PROOF)

Access Duration: 14/11/2021 to 10/12/2021

Funding Instrument:	Research and Innovation Action
Call:	H2020-INFRAIA-2019-1
Call Topic:	INFRAIA-01-2018-2019 Integrating Activities for Advanced Communities
Project Start:	1 April 2020
Project Duration:	54 months
User Group Leader:	Daniel Gutierrez Rojas (Lappeenranta University of Technology)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 870620.

Report Information

Document Administrative Information	
Project Acronym:	ERIGrid 2.0
Project Number:	870620
Access Project Number:	[113]
Access Project Acronym:	PROOF
Access Project Name:	Adaptive protection for microgrids based on communication
User Group Leader:	Daniel Gutierrez Rojas (Lappeenranta University of Technology)
Document Identifier:	ERIGrid2-Report-Lab-Access-User-Project-PROOF-draft-v1.0
Report Version:	v1.0
Contractual Date:	09/01/2022
Report Submission Date:	18/01/2022
Lead Author(s):	Daniel Gutierrez Rojas (LUT)]
Co-author(s):	Majid Hussain (LUT) and Iurii Demidov (LUT)
Keywords:	Microgrids, Adaptive protection, Cyber-security, European Union (EU), H2020, Project, ERIGrid 2.0, GA 870620
Status:	_x_ draft, __ final

Change Log

Date	Version	Author/Editor	Summary of Changes Made
18/01/2022	v1.0	Daniel Gutierrez Rojas (LUT), Majid Hussain (LUT), Iurii Demidov (LUT), Alkistis Kontou (ICCS-NTUA)	Draft report
14/02/2022	v1.1	Alkistis Kontou (ICCS-NTUA), Dimitris Lagos (ICCS-NTUA)	Hosting institute first review
9/03/2022	v1.2	Iurii Demidov (LUT), Daniel Gutierrez Rojas (LUT)	Revision according to feedback
8/04/2022	v1.3	Alkistis Kontou (ICCS-NTUA)	Hosting institute Final Check

Table of Contents

List of Figures

List of Abbreviations

LA	Lab Access
UP	User Project
DER	Distributed Energy Resources
IED	Intelligent Electronic Devices
ADN	Active Distribution System
DOCR	Directional Overcurrent Relays
MGCC	Microgrid Central Controller
CIGRE	Council on Large Electric Systems
LUT	Lappeenranta-Lahti University of Technology
ICCS	Institute of Communications and Computer Systems
IED	Intelligent Electronic Device
LAN	Local Area Network
RTDS	Real-Time Digital Simulator
NTUA	National Technical University of Athens

Executive Summary

The aim of this research was to contribute with decentralization of energy technologies by investigating technical aspects such as performance of new adaptive protection schemes, anomaly detection in microgrids and cyber-attacks. The research focused on simulation and test in a real-time environment a microgrid setup and run different topologies scenarios in which overcurrent protection will adapt according to the current state of the microgrid like open switches, high Distributed Energy Resources (DER) generation, low DER generation, etc. To do this, the switches and protective devices must communicate to each other.

During the research we explored 3 use cases connected to each other with the ultimate purpose of increasing security levels in microgrid, in the cyber-physical layers of energy systems. In the first, the Council on Large Electric Systems (CIGRE) low voltage benchmark microgrid was modeled on the RTDS and data was collected using a script generated for automatic fault reproduction and data collection into a .cvs file. The fault data was made by changed parameters such as fault resistance, fault point location and microgrid scenario. The main purpose of this use case was to use the collected data in further research for hard fault detection of fault in microgrids in presence of high fault resistance and low contribution of current from the DERs.

The second case purpose was to test a adaptive setting topology in the low voltage CIGRE benchmark. We had chosen 3 scenarios for the microgrid and collected the measurements needed to implement optimization in order to choose the adequate settings for a pair of relays that will maintain coordination and minimum operating constraints. By the use of a central management controller a logic implemented based on the state of the switches that determines the topology then it will send communication signals to the pair of relays to set accordingly to the state of the grid and therefore maintain microgrid protected from faults.

The third case was related to cyber security in microgrids. We divided this testing into two parts, in the first part simple diffential and overcurrent relay protection was tested. The test consisted on injecting GOOSE messages from a third party PC to the relays via Local Area Network (LAN) with the objective to overwrite the messages that the controller is sending. With this we managed to send fake settings to the relays making ineffective the ones being send by the controller. In the second part of this test, we placed a rasberry pi and by controlling remotely the sent again the fake settings to the low voltage CIGRE bechmark. We show how changing the setting under some scenarios, can trigger the protection and therefore open the microgrid switches under normal operation conditions.

1 Lab-Access User Project Information

1.1 Overview

User Project Title: Adaptive protection for microgrids based on communication

User Project Acronym: PROOF

Host Infrastructure: Institute of Communications and Computer Systems (ICCS)-National Technical University of Athens (NTUA)

Start date - End date: 14/11/2021 to 10/12/2021 User Group Member:

- Daniel Gutierrez Rojas, PhD Research Fellow, Lappeenranta-Lahti University of Technology (LUT) University, Finland
- Majid Hussain, PhD Research Fellow, LUT University, Finland
- Iurii Demidov, PhD Research Fellow, LUT University, Finland

1.2 Research Motivation, Objectives, and Scope

As the global population increases, the electricity demand also increases in a daily basis. Classical transmission systems are working at their limit, so they can deliver the amount of energy required. The current limitations associated with environmental licenses, economical funding, etc. to build new transmission lines or communications systems associated with power systems are leading to the need for installing generation much closer to the consumption nodes, making the power flow bidirectional and introducing a new entity, called prosumer (producer-consumer). Some research efforts have been focusing on using the prosumer capability of generating energy to bring economical and environmental benefits by centralized and decentralized energy management. This generation from DER contribute significantly to the reduction of green house gases, caused by traditional energy resources, and bring some electrical benefits to the electrical grid such as better voltage profile, enhanced reliability and security of supply.

Despite all the benefits, the introduction of DER to microgrids also impose some technical challenges, operational changes vary rapidly due to its low inertia of non-rotating elements and changes in weather conditions (wind and solar radiation) in hour basis, and in some cases, connecting and disconnecting intermittently along the bidirectional energy flow, after integration of DER to the grid. In terms of protection schemes for microgrids with DERs, to ensure safe operation, all variables of all elements must be monitored, and necessary changes must be made to the device protection settings, as operating conditions of the grid change (fault occurrence). Since conventional protection schemes that rely on large inertia and long transient periods are insufficient, adaptive schemes are necessary. The complexity of the cyber-physical system in adaptive protection presents challenges to control effectively their elements with intelligent algorithms, and any failure of the cyber domain might stress or even harm physical components. Microgrids that rely on central management controller, Intelligent Electronic Device (IED) communication need to keep the system updated of the actual state of the grid, to keep track of operating currents and voltages, and make proper fault detection to isolate accurately.

Based on the mentioned challenges, in this research work we investigate the full implementation and testing of an adaptive protection scheme on a benchmark microgrid. Furthermore, we test commercial equipment under a cyber-attack, so we can understand how these elements react to stress the cyber-physical domain and the overall impact on the electrical system and end consumer.

1.3 Structure of the Document

This document is organised as follows: Section 2, briefly outlines the state-of-the-art that provides the basis of the realised Lab Access (LA) User Project (UP). Section 3, briefly outlines the performed experiments whereas Section 4, summarises the results and conclusions. Potential open issues and suggestions for improvements are discussed in Section 5.

2 State-of-the-Art

The idea of adaptive protection was proposed in 1980’s, and its essence is promptly adjusting relay, also called as Intelligent Electronic Device (IED), settings in response to any changes in operating conditions. Literature shows that adaptive protection can extend the protect range while contributing to the security and stability. The cases of blackouts accompanied with the fault action of protection are so frequent that researchers have paid attention to the adaptive protection’s function in preventing them. Restricted by the communication systems with limited capabilities at that time, power system’s protection research before the 90’s has mainly focused on the protection of a single primary device based on the real-time information of the installed line of the power system. However, with the development of computer networks and communication technologies, it has become possible to implement the networked wide-area-information oriented adaptive protection (Gutierrez-Rojas, Nardelli, Mendes, & Popovski, 2021).

Some attempt efforts have already been made in solving protection problem of one single device including a line by means multi-agent system (MAS) techniques, but in a quite elementary way. To obtain adaptive relay settings, virtual real-time information of protected electric network is needed (Habib, Lashway, & Mohammed, 2018). Ensuring reliable protection is one of the primary challenges for distribution systems with increasing DER. Paired with computational intelligence and advanced system management capabilities, these systems are also referred to as Active Distribution System (ADN). ADNs have remote infeed from DER resulting in bidirectional power flow and, variable fault current levels and voltage profiles, which may cause blinding and/or sympathetic tripping for Directional Overcurrent Relays (DOCR) (Habib et al., 2018). It is suggested in (Ustun, Ozansoy, & Zayegh, 2011) that each time a fault is detected, these protection relays should communicate with a Microgrid Central Controller (MGCC) informing the commander about the fault event. The ‘commander’ then communicates back with the remote protection relay issuing a trip signal to that. This approach of communication during the presence of a fault is risky and a major point of criticism of the suggested strategy has been made. The work is noteworthy, but communication aspects are not adequately covered and there is a very limited discussion on how the communication of data would play a role in the proposed microgrid protection scheme.

Microgrid systems that use MGCC are very common but they are susceptible to cyber-attacks. These attacks can happen in both physical or cyber layer of the system and can impact part of the microgrid or as a whole. The malicious threats always aim where the impact of an attack might be greater, this means, controller is usually the target element as it can provide protective or power balance function to the rest elements of the microgrid.

Changes in the communication infrastructure of the distribution system and microgrid are also pertinent since the need for flexibility and cost-effective solutions is a priority. The research presented in the above sections have shown a standardized predominance of wired, centralized communication approaches for adaptive protection in microgrids. Recent studies show that there is not a specific trend in upgrade to newer systems for communication technology in practical and theoretical research (Beheshtaein, Cuzner, Savaghebi, & Guerrero, 2019).

3 Executed Tests and Experiments

3.1 Test Plan, Standards, Procedures, and Methodology

For this research multiple tasks had to be prepared beforehand. We implemented 3 use cases (described below) and the following activities were necessary to be carried out prior to testing:

- Choose low voltage CIGRE microgrid topology to work on the testing
- Previous simulation of the network scheme on a different software
- Preparation of algorithm for optimization of the setting and data processing
- Preparation algorithm for automatic collection of data (to be converted on different syn taxis)
- Preparation of communication hardware and code to replicate GOOSE messages

Those activities allowed a more fluent research work in laboratory as the team members didn't start to work on the tests from scratch.

The tesbed topology and the data flow connections can be seen in Fig. 1 and 2 . This topology was applied for all 3 use cases.

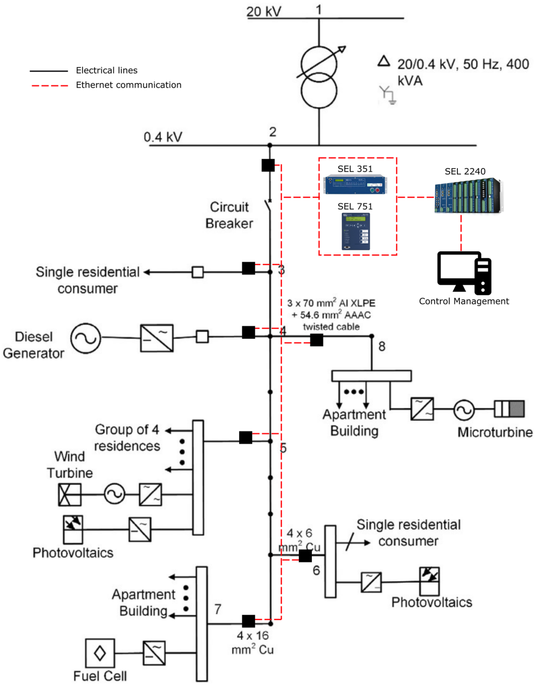

Figure 1: Topology and communication infrastructure

Use case 1:

In this use case we focused on collecting fault data from Real-Time Digital Simulator (RTDS) by using an algorithm that changed simulation parameters for every run and then collect the data. The simulation parameters concerned 5 different fault points, 7 different types of fault (AG,BG,CG,AB,BC,CA, ABC), 0.1-100 Ohms fault resistances in step of 5, and 3 microgrid scenarios. The scenarios chosen for this tests were Grid-connected (coupled to main grid and

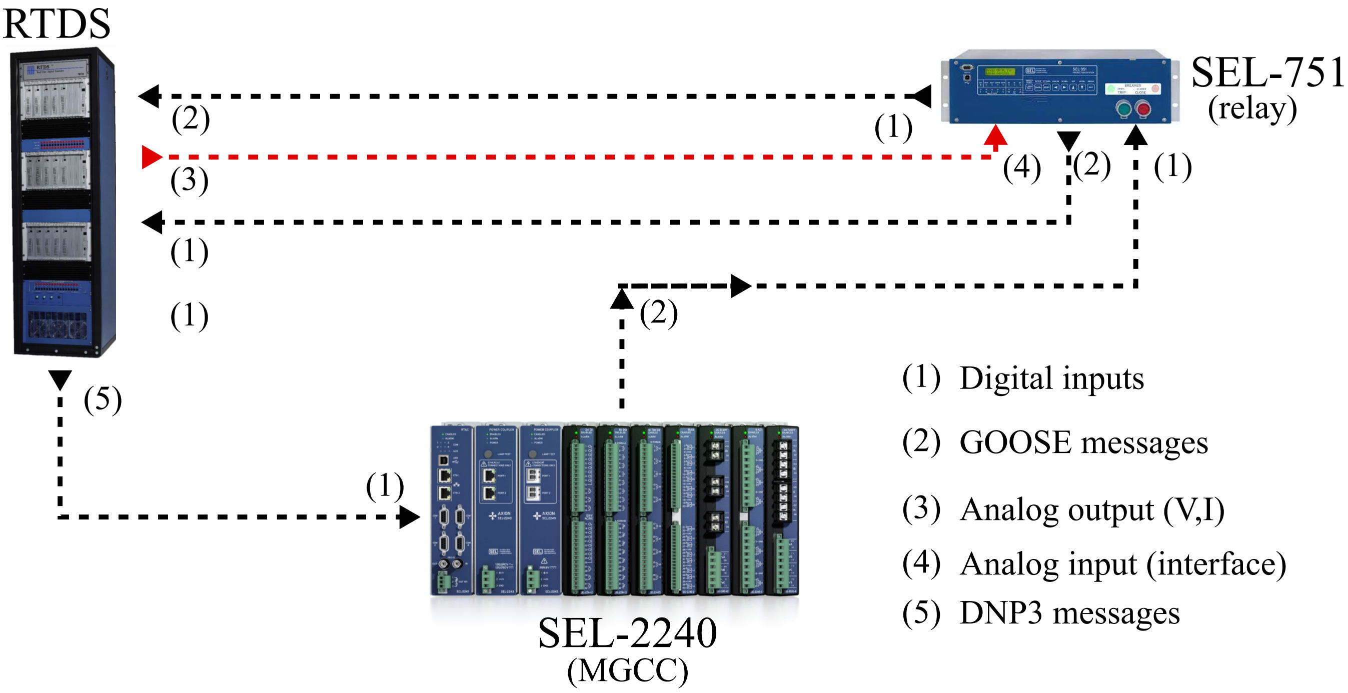

Figure 2: Communication schematic

all DER ON), Islanded (all DER ON), and Grid-connected (coupled to main grid and DER2 DER4 OFF). Data without fault but changing the parameters has been recorded. The low voltage CIGRE benchmark microgrid utilized for the uses cases can be seen in Fig. 3.

Use case 2:

In this use case, after the microgrid was implemented in the RTDS system, we selected the pair of relays that would have the biggest impact from one scenario to the other to test the adaptive methodology. We used swarm based algorithms for the optimization of the settings for each scenario, after collecting variables necessary under steady state operation in the microgrid.

Use case 3:

In this case the reliability of the communication link was tested in the cyber-domain by sending "false" GOOSE messages to the relays, replicating the commands from the MGCC. The replicated messages included different setting group option from the appropriate one, in order to change the settings to undesired protection schemes.

3.2 Test Set-up

During the experiments, as seen in Fig. 4 and 5, the following elements were utilized:

- RTDS
- SEL 751 (2)
- SEL 2240
- Raspberri pi
- LAN switch

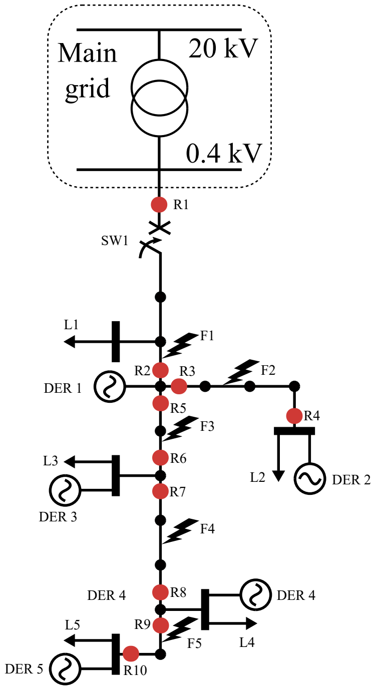

Figure 3: Low voltage CIGRE benchmark microgrid

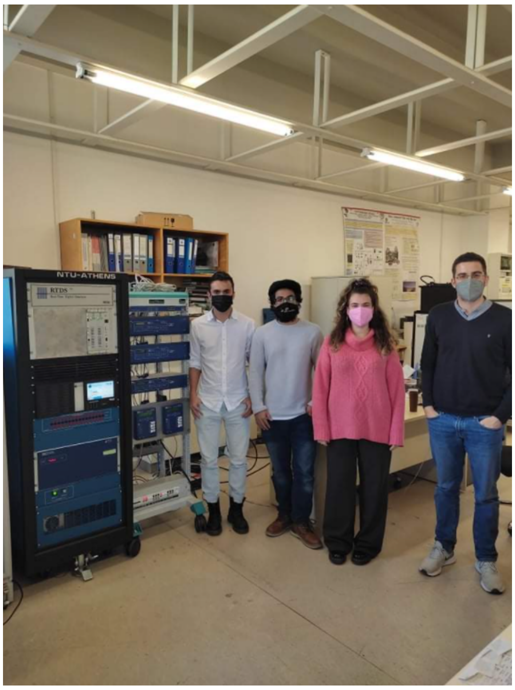

Figure 4: Project team and elements used during research

For the first use case test set up, we designed the low voltage CIGRE microgrid in the RTDS as three-phase diagram including all the control of variables and switches for change the parameters. At the same time, another member of the group was working on translating the automatic data collection algorithm into C++ as required by RTDS. Once the topology was designed, we ran different simulation scenarios as initial test, in order to adjust the energy balance in the microgrid when it was island mode.

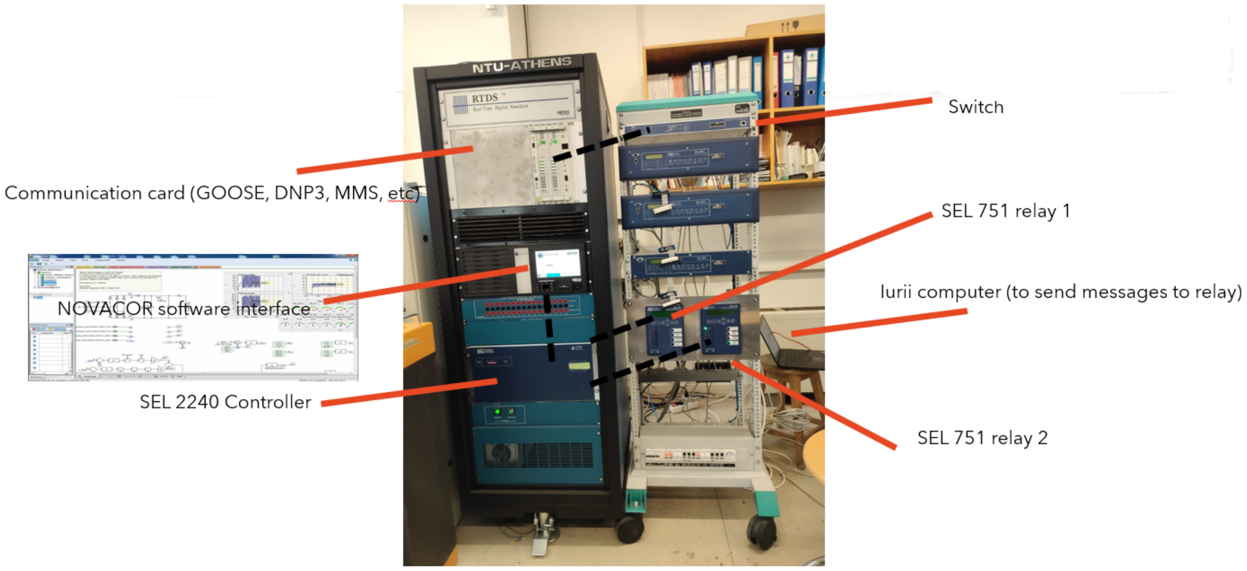
Switch
Communication card (GOOSE, DNP3, MMS, etc)
SEL 751 relay 1
NOVACOR software interface
Iurii computer (to send messages to relay)
SEL 2240 Controller
SEL 751 relay 2
NTU-ATHENS
RTDS

Figure 5: Project team and elements used during research

The second use case required some modifications in the topology on RSCAD software of RTDS, in order to match communication signals between the communication card and elements interfaces (controller and pair of relays). SEL softwares were utilized for the configuration of the communication scheme based on IEC 61850, in which the communication characteristics between the various elements were defined, and the appropriate configuration files were sent to the relay, for each microgrid scenario. Each setting group were constantly tested to obtain relay's tripping time and tripping coordination between the primary and back-up relay according to the scenario that was being tested. To control the different setting groups, a SEL 2240 was used to perform the change according to the state of the grid under real-time testing. SEL 2240 has a software interface where all the logic can be set according to the output signals coming from RTDS in a feedback loop. As an example, if the microgrid is connected to the common coupling point, the central controller obtains the status of the switches from RTDS and then sends the correct setting group that the relays must be set. SEL 751 already has been configured with the 3 different setting groups and the controller is the one in charge to select which setting group must be actived.

In the third use case we did 2 different tests. In the first one, basic differential and overcurrent protection was implemented in RTDS software and then using the controller SEL 2240 again, it changed the settings groups according to 3 scenarios that we proposed (grid-connected, islanded, DER2 & DER4 off). Then a computer connected to a switch (LAN) was placed so we can replicated the same messages the controller sent to the relays in order to force change the ones sent by the controller. The computer already had GOOSE messaging algorithm implemented.

In the set up of use case 3, we tested the same implementation but instead of using a computer, we placed a raspberri pi in the LAN. Based on use case 2, using the same topology, remotely we managed to bypass the messages sent from the controller and sent fake setting groups in the relay, causing trip or leaving the microgrid unprotected from possible faults.

3.3 Data Management and Processing

Data from all the use cases was collected from the output files of RTDS, in most of the cases were current data but also some tripping and logic signal coming from the devices to the switches located in the microgrid were recorded.

From use case 1, the total data size was around 9 GB so we uploaded to private server cloud for further processing. This data will be used to feed machine learning-based algorithms for hard fault detection in microgrids.

For the other 2 cases, tripping signals and currents were recorded showing the unstable behaviour once cyber-attacks were inserted in the system.

4 Results and Conclusions

4.1 Discussion of Results

4.1.1 Simple Cyber-Attack approach

The tested cyber-attack is a data injection to the GOOSE protocol of the IEC 61850 standard. While data injection the parameter of protection was replaced from the proper to the false one by the attack side. Fig.6 illustrates a common configuration of the cyber-attack testing setup. The assumption of the tests is that a hacker gets access to Raspberry Pi connected to the local area network (LAN). During the cyber-attack test, two different protection applications were considered, each with a specific grid topology. Adaptive protection was tested within grid configuration illustrated in fig. 3; differential current protection is considered with a topology shown in fig.7. An initial stage of the attack is data collection and analysis. At the second stage when a hacker is familiar with data flows and able to define the most significant impact of attack a GOOSE message is replicated and starts to be sent with a sampling frequency two-five times higher than the sampling frequency of controller IED in adaptive protection case and protection IED in differential protection case to suppress the data flow containing proper information.

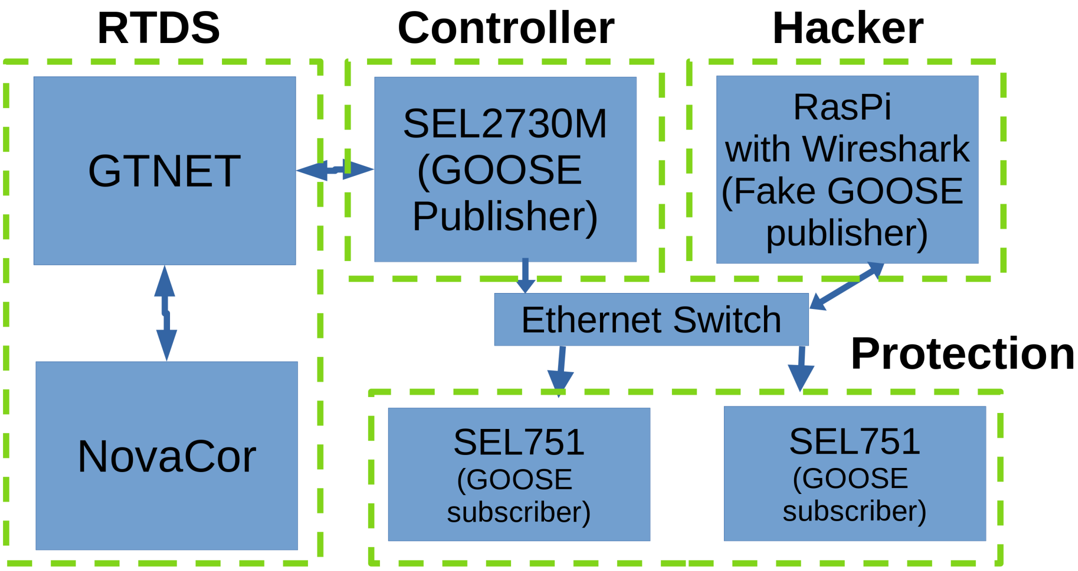
RTDS
Controller
Hacker
GTNET
SEL2730M (GOOSE Publisher)
RasPi with Wireshark (Fake GOOSE publisher)
Ethernet Switch
Protection
NovaCor
SEL751 (GOOSE subscriber)
SEL751 (GOOSE subscriber)

Figure 6: Cyber-attack testing environment

4.1.2 Differential protection

During the testing of cyber-attack at differential current protection, on-grid and off-grid configurations were tested. Different types of faults and attacks were also part of the testing. Fig. 8,9 illustrates examples of the operations without and with fault without cyber attacks.

Fig. 10,11 show tests of normal operation mode and fault operation with cyber-attack. The plots illustrate currents flow through the breakers of the fault line and voltages at the place of a fault. Therefore, for example from the fig. 11 is seen that with the fault at the line, breaker

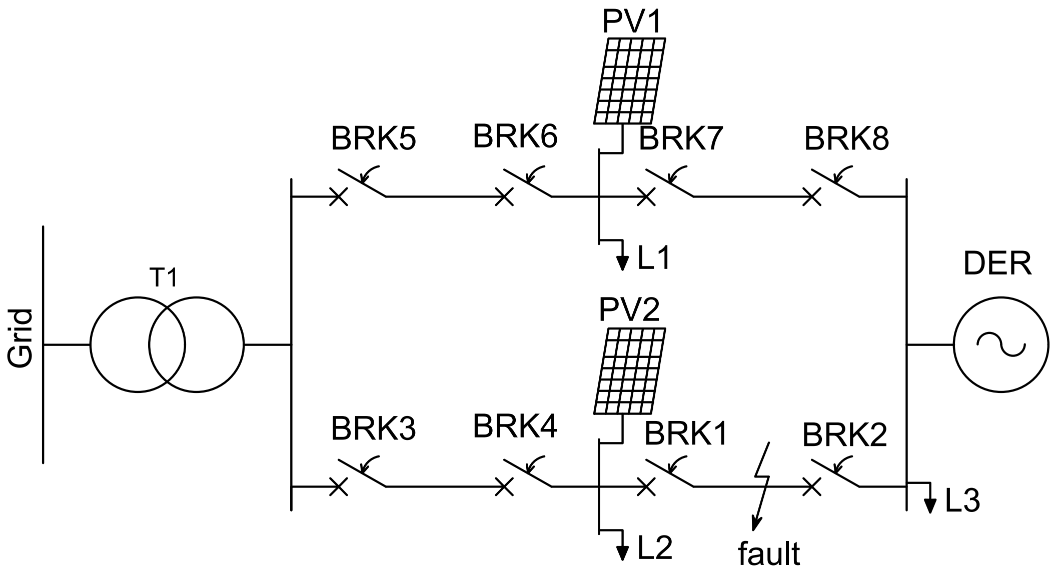

Figure 7: Differential protection testing topology

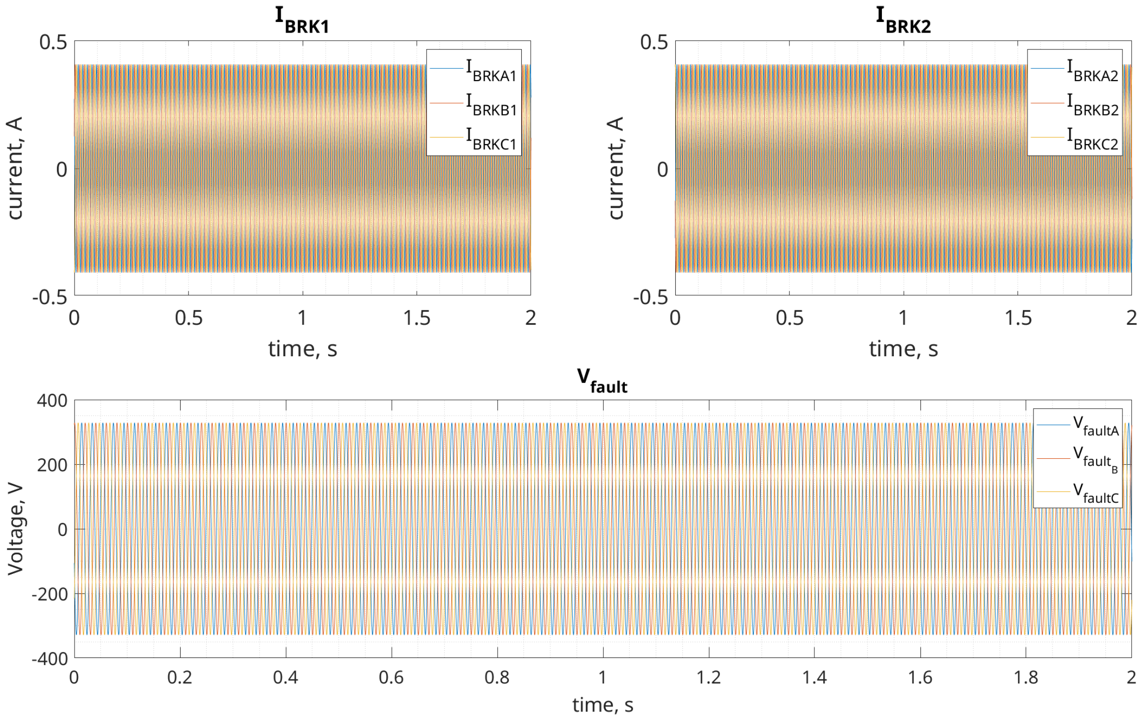

Figure 8: Normal operation of the grid, without cyber-attack

1 doesn't trip, and the three-phase current fault is not isolated from its side. Such operational state can damage primary power equipment and effect on end-users' appliances (Lagos, Papaspiliotopoulos, Korres, & Hatziargyriou, 2021).

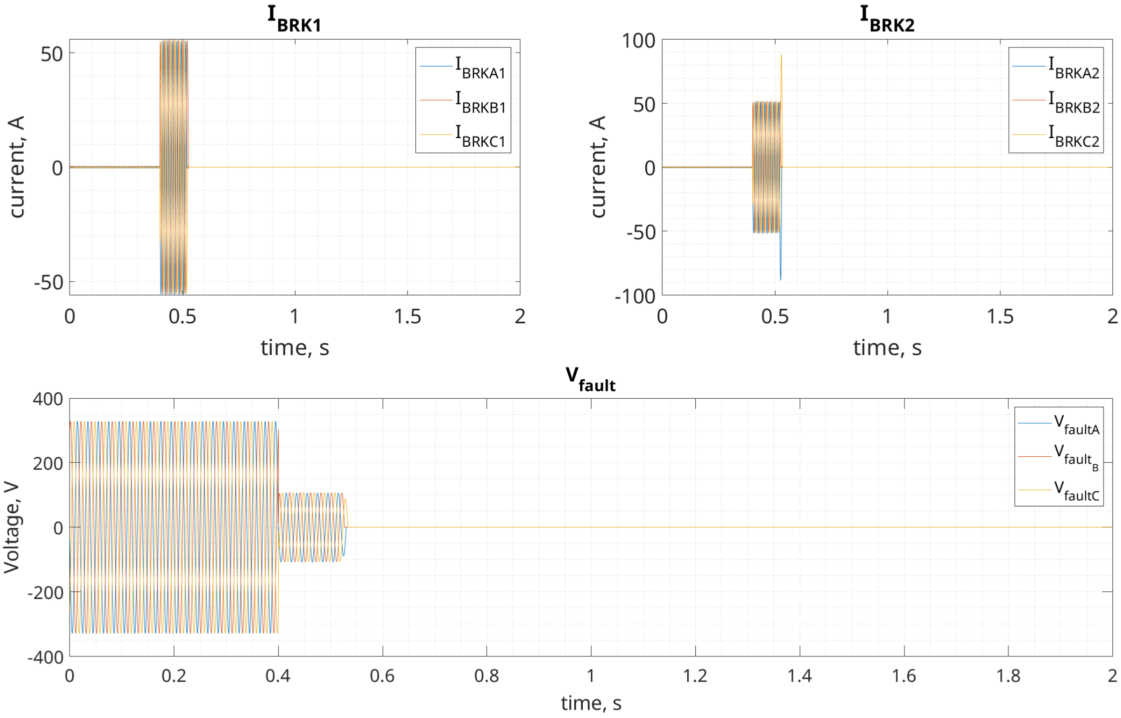

Figure 9: 3-phase fault on-grid operation, without cyber-attack

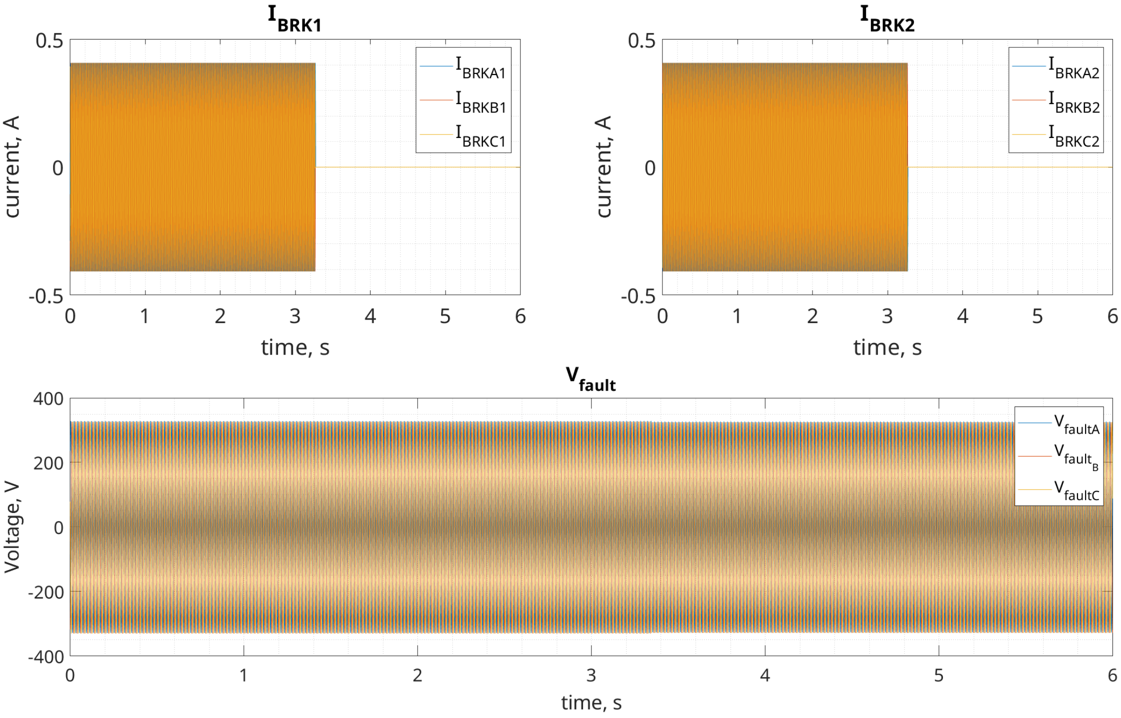

Figure 10: Normal operation of the grid, cyber-attack on both breakers

4.1.3 Adaptive protection during grid connected mode

During this mode, SW1 from Fig. 3 is closed and the microgrid is connected to the grid. Then we evaluate faults occurring in fault point F5 and the performace of the relays R9 and R7 and

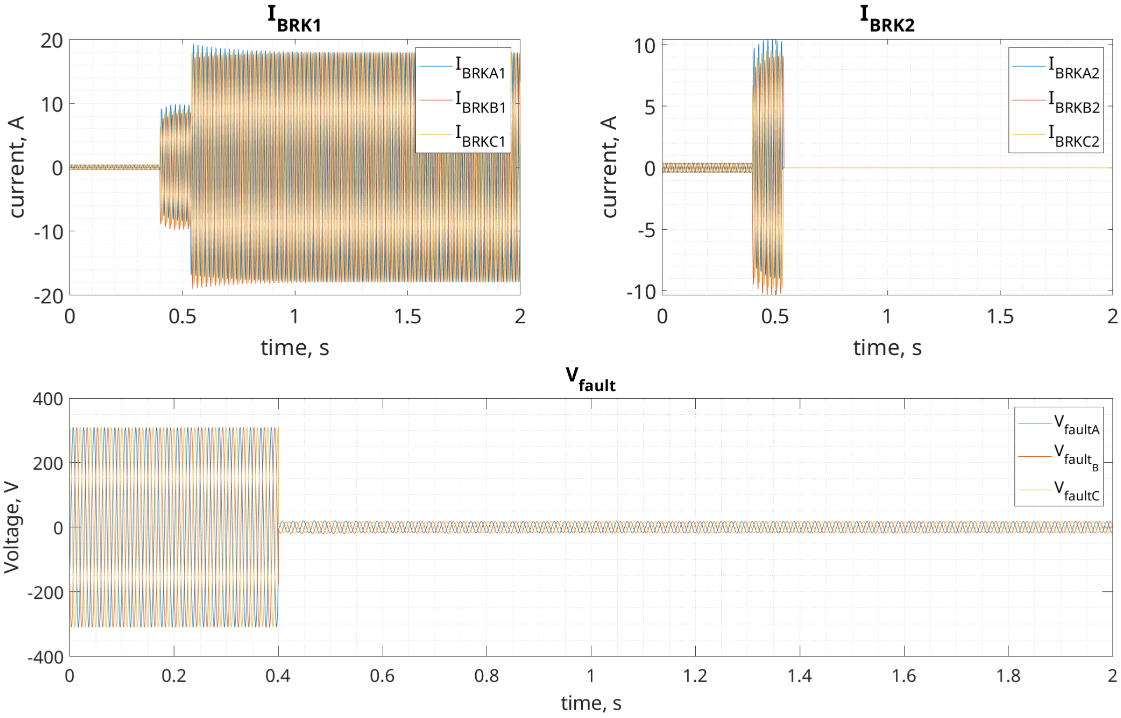

Figure 11: 3-phase fault off-grid operation, cyber-attack on breaker 4

its coordination are seen in Fig. 12

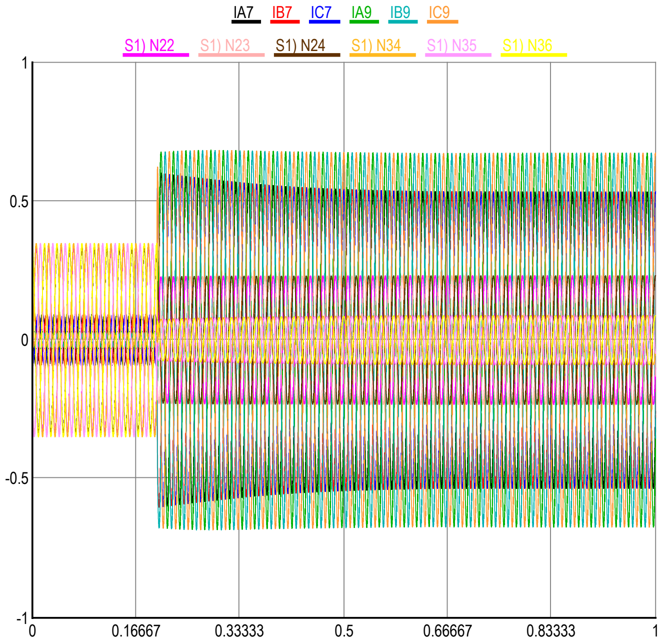

Figure 12: Performance of R9 and R7 after faults in F5

4.1.4 Adaptive protection during island mode

During island mode the settings change dramatically but the controller enables the setting group accordingly. A fault occurring in F5 under this setup have less in-feed current but we can see that R9 and R7 perform adequately, as seen in Fig. 13

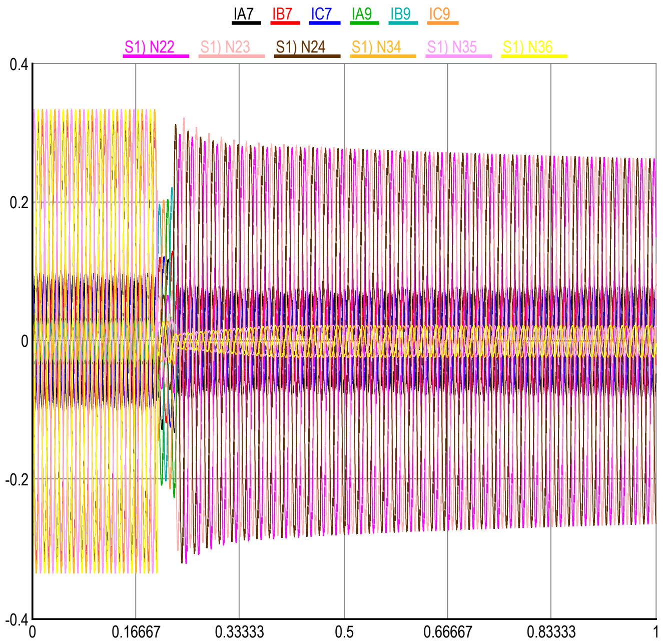

Figure 13: Performance of R9 and R7 after faults in F5

4.1.5 Adaptive protection during limited DER mode

During this scenario 2 DER were switched OFF and therefore lowering the current when a fault occurs. In Fig. 14, we can see that the relays (R7 and R9) maintain the microgrid protected even if the current is lowered.

4.1.6 Cyber-attack on during islanded mode

During islanded mode we tested the cyber-attack impact on the microgrid. We demonstrated that under normal operating conditions scenario, if a cyber-attack changes the settings group it can cause the tripping of certain switches in the grid by command of relays and cause instability. The effects of cyber-attack can be seen in Fig. 15.

The sampling window shown in Fig. 15 is big to the sequence of events during the occurrence of a cyber-attack. It is important to notice the vulnerability of centralized-based communication in adaptive protection. By attacking only one link and sending false data injection messages to the relays , an attacker is able to disconnect an entire microgrid. This could be avoided, by using distributed communication that allows custom made logics between the devices to change their group settings depending on scenario without relying on any standardized GOOSE messaging that can be imitated from a central controller.

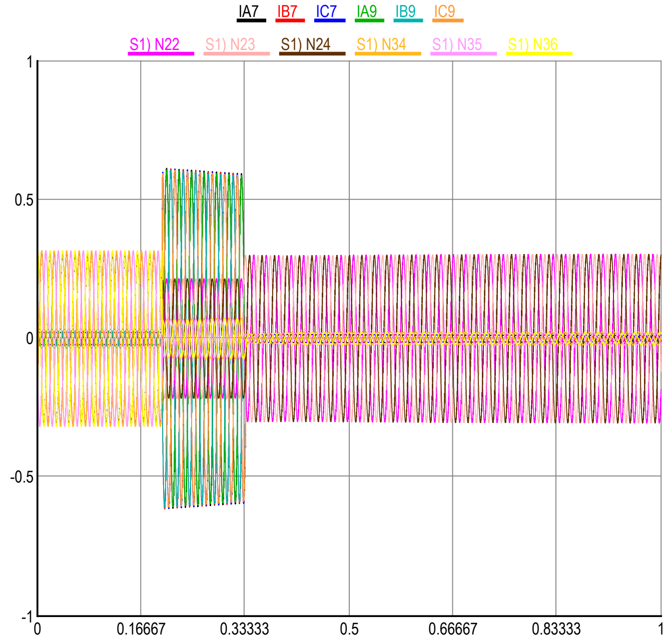

Figure 14: Performance of R9 and R7 after faults in F5

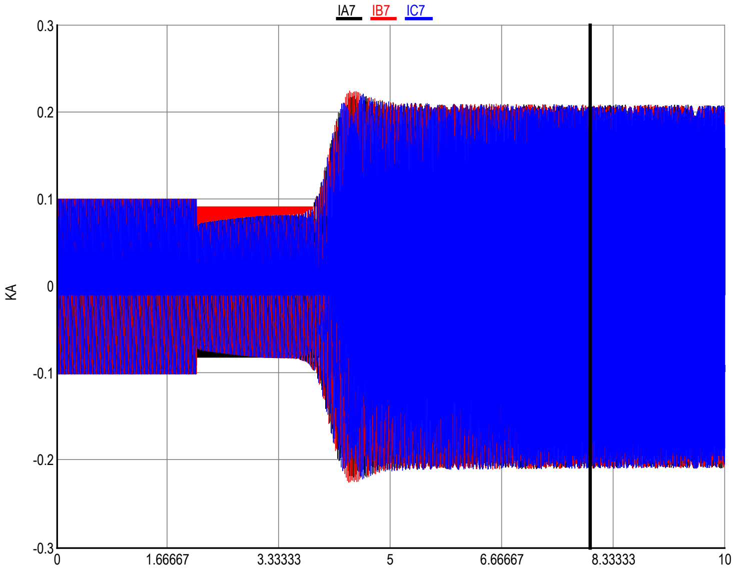

Figure 15: Current passing in R7 under normal operating condition and instability originated by cyber-attack

4.2 Conclusions

- Data was successfully collected that will be used in machine learning algorithms to perform hard fault detection in microgrids in the present of high resistance faults.
- We demostrated the applicability of adaptive protection to secure low voltage CIGRE benchmark microgrid independant of the scenario by changing to adequate setting suing a central controller.

- Relays coordinated during different scenarios and keep the microgrid protected from fault at all times by changing their settings according to the microgrid state.
- The impact of cyber-attacks in physical domain have tremendous impact in the electrical system as the system composed by one or multiple user can lose connection to electricity due to fake injection of protection setting to the relay causing the switches to open under normal operating conditions.
- The Lab Access in ICCS-NTUA provided the tools and all the infrastructure need to perform the tests. We were able to use additional hardware elements that provided more results in the research.
- Collaboration between instutions was extremely important as we were able to shares experiences and technical aspects fundamental to complete all the test in the time provided by the laboratory. conditions.
- HTD was extremely helpful as the team to which Lab Access was provided already prepared pre-work that could be done in home institution to facilitate and make more fluid the research carried out in the host institution. The comments in the revision from third party and home institution helped to improve the research.
- Time is a key factor for this kind of research as it might never be enough to perform the testing due to different unexpected reasons like loss of power in the laboratory. With good planning and time management these challenges can be tackled.

5 Open Issues and Suggestions for Improvements

- We would recommend more technical discussion rather than administrative before the travel time, so the schedule can be plan before hand in order to make the project work within the time limit of the research visit.
- During the time of stay we didn't face many issues, the timing and work from the host were more than enough to carry out the project during the Lab Access.

References

Beheshtaein, S., Cuzner, R., Savaghebi, M., & Guerrero, J. M. (2019, March). Review on microgrids protection. *IET Generation, Transmission & Distribution*, *13*(6), 743–759. Retrieved from https://doi.org/10.1049/iet-gtd.2018.5212 doi: 10.1049/iet-gtd.2018.5212

Gutierrez-Rojas, D., Nardelli, P. H. J., Mendes, G., & Popovski, P. (2021). Review of the state of the art on adaptive protection for microgrids based on communications. *IEEE Transactions on Industrial Informatics*, *17*(3), 1539-1552. doi: 10.1109/TII.2020.3006845

Habib, H. F., Lashway, C. R., & Mohammed, O. A. (2018). A review of communication failure impacts on adaptive microgrid protection schemes and the use of energy storage as a contingency. *IEEE Transactions on Industry Applications*, *54*(2), 1194-1207. doi: 10.1109/TIA.2017.2776858

Lagos, D., Papaspiliotopoulos, V., Korres, G., & Hatziargyriou, N. (2021). Microgrid protection against internal faults: Challenges in islanded and interconnected operation. *IEEE Power and Energy Magazine*, *19*(3), 20-35. doi: 10.1109/MPE.2021.3057950

Ustun, T. S., Ozansoy, C., & Zayegh, A. (2011). A microgrid protection system with central protection unit and extensive communication. In *2011 10th international conference on environment and electrical engineering* (p. 1-4). doi: 10.1109/EEEIC.2011.5874777

Disclaimer

This document contains material, which is copyrighted by the authors and may not be reproduced or copied without permission.

The commercial use of any information in this document may require a licence from the proprietor of that information.

Neither the Lab Access User Group as a whole, nor any single person warrant that the information contained in this document is capable of use, nor that the use of such information is free from risk. Neither the Lab Access User Group as a whole, nor any single person accepts any liability for loss or damage suffered by any person using the information.

This document does not represent the opinion of the European Community, and the European Community is not responsible for any use that might be made of its content.

Copyright Notice

© 2022 by the authors, the Lab Access User Group.

This project has received funding from the European Union's
Horizon 2020 research and innovation programme under
Grant Agreement No. 870620.