Field-ready implementation of fail-safe adaptive protection relay schemes

Christoph Mederer, Tobias Lorz, Johann Jaeger
Institute of Electrical Energy Systems
Friedrich-Alexander-Universität Erlangen-Nürnberg
Erlangen, Germany
christoph.mederer@fau.de, tobias.lorz@fau.de, johann.jaeger@fau.de

***Abstract*—Adaptive protection has been researched for many years. Numerous methods have been developed that all result in adaptive protection settings for changing grid conditions. However, implementing these settings on IEDs in the field is still lacking. This paper demonstrates how protection settings can be reliably adapted under practical conditions. Therefore, a laboratory setup is presented using real hardware consisting of multiple protection relays, a remote terminal unit and a real-time grid simulator. We guarantee a uniform protection scheme for all protection devices by implementing multiple safety measures. Implementing communication via IEC 61850 and the MQTT protocol this setup provides a standardized interface to include devices from multiple vendors to ensure interoperability. Simulating a substation of a real DSO our results show that adaptive protection can be reliably implemented, maintaining a unified protection scheme even under communication failures.**

***Index Terms*—adaptive protection, IEC 61850, fail-safe behavior, Hardware-in-the-Loop**

I. Introduction

Conventional protection uses a single setting set for diverse scenarios. As a result they are not able to keep up with the rapid change in the electrical energy system. Therefore, the concept of adaptive protection has been discussed for several decades [1]. A real online adaptive protection scheme is quite rarely implemented in the field up to now. A key challenge in deploying such schemes lies in the required communication infrastructure [2]. Consequently, many researchers rely on Hardware-in-the-Loop (HiL) setups that integrate real protection relays to reproduce realistic grid behavior. For example, [3] presents a HiL setup based on IEC 61850, where two setting groups (SGs) were activated depending on the simulated wind turbine infeed. The protection scheme used differential protection on one relay, while IEC 61850 communication employed Generic Object-Oriented Substation Events (GOOSE) to transmit the infeed state. The relay itself was not adjusted via IEC 61850, thus representing an offline adaptive protection approach limited to two predefined protection schemes. In [4], a HiL setup implemented multiple protection devices from different vendors. A parallel power transformer differential protection scheme was implemented, and communication between protection relays from two different manufacturers was established using IEC 61850. Focusing only on GOOSE, the study demonstrated interoperability between the two vendor devices. GOOSE messages were transmitted and received without errors. However, it was also acknowledged that conformance to the IEC 61850 standard alone does not guarantee interoperability across multiple vendors. No protection settings were directly adapted. The main objective was to verify cross-vendor communication, indicated by two LEDs on one intelligent electronic device (IED) lighting up when the other device issued a trip command. In [5], a HiL setup was presented consisting of two protection schemes. In the first, multiple IEDs at bay level communicated with a centralized protection and control device, whereas in the second, this central device acted as the sole protection unit receiving its input through merging units. Fixed parameter groups were defined for different clustered network scenarios, and the corresponding network configuration was transferred via GOOSE messages representing the state of the simulated circuit breakers. It was stated that the change of SGs requires about 100 ms. By implementing GOOSE communication, a fallback SG was introduced to be activated in case of communication failure. Detection of such a failure was achieved by monitoring the maximum time parameter, which ranged from 1 s to 60 s, and switching to the fallback group when the defined interval elapsed without receiving a GOOSE message.

Building upon these previous approaches, this work presents a setup capable of simultaneously adjusting the settings of multiple IEDs through a central remote terminal unit (RTU). Section II provides a detailed description of the setup. It consists of the RTU , four universal protection devices, and a real-time grid simulator (RTS). The implemented IEDs can be seen in Fig. 1. All components are time-synchronized. Using standard substation hardware makes the setup field-applicable. By creating a configuration file based on the IEC 61850 structure of the devices themselves, every writable object of the IEDs can be accessed and modified. Multiple safety measures are implemented to ensure a unified protection scheme across all devices, even in the event of communication failure. On the RTU, a docker-based container manages the application of the protection settings onto the IEDs using the

The authors gratefully acknowledge funding by the German Federal Ministry of Research, Technology and Space (BMFTR) within the Kopernikus Project ENSURE 'New ENergy grid StructURes for the German Energiewende'.

979-8-3315-8138-1

Fig. 1. Hardware setup of the implemented IEDs.

Message Queuing Telemetry Transport (MQTT) protocol and JavaScript Object Notation (JSON). The application running on the RTU is publicly available and can be adjusted for further use [6]. The work is finished with results to evaluate the general setup and the individual fallback levels. In the end a conclusion is drawn.

II. Laboratory Setup

A. General workflow and configuration

The general workflow is illustrated in Fig. 2. Each component of the laboratory setup can be located in the real world, starting with the generation of new protection settings for the system. As these settings are considered to provide improved protection performance, this work solely focuses on their application to the IEDs. The complete protection configuration is then published to an MQTT server. In practice, this step would happen in the control center of a distribution system operator (DSO). The RTU continuously monitors the specified MQTT topic and retrieves the JSON data as soon as it is published. The data is subsequently converted into IEC 61850 Manufacturing Messaging Specification (MMS) signals, which are written to the IEDs. Representing the bay, the IEDs interact with the RTS using IEC 61850 Sampled Values (SV) and GOOSE. Therefore the communication is based on the setup of a real, modern substation.

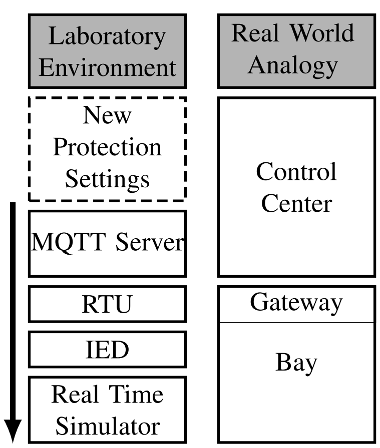

Fig. 2. Laboratory setup and analogy to real world.

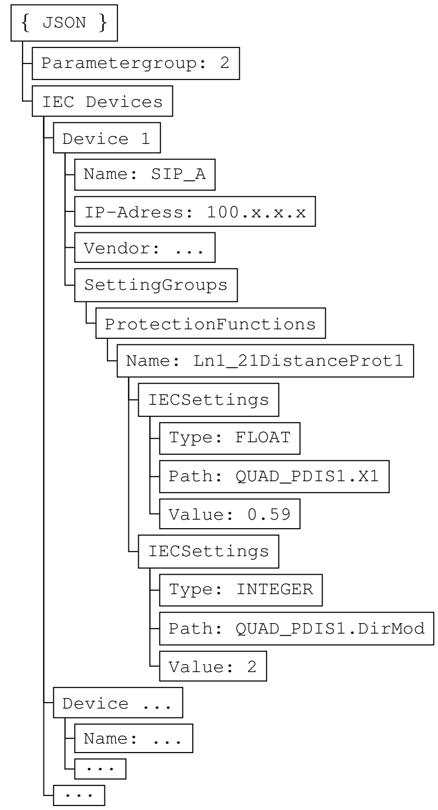

Fig. 3. Structure of the settings file.

B. Description of the protection setting structure

The new protection settings are saved within a JSON file. Using [7], one file is created for each IED. These files follow the IEC 61850 structure of the devices themselves. Consequently, the IEC addresses are taken directly from the IEDs, enabling a coherent write process. Since we aim to write to multiple IEDs, the individual files are combined into a single JSON file. By modifying the original structure of the individual files, the setting group of each device is placed at the top level of the JSON, ensuring a consistent protection scheme across all listed devices. Fig. 3 shows an exemplary JSON structure. For the IED SIP_A two example signals will be written. Multiple IEDs can follow. Each IED must support at least three distinct SGs: one for normal operation, one for writing, and one as a fallback in case of communication failure. The detailed write process is described in Section II-D. After successfully writing to all devices, each IED switches to the newly written SG. In case of communication failure, an adaptive protection scheme must fall back to a conventional configuration, which is stored in the third SG. This ensures a coherent protection scheme comparable to the one used before implementing adaptive protection.

C. MQTT Communication

MQTT was chosen due to its low overhead and ease of implementation. A local MQTT broker was established using Mosquitto. A Python script, based on the Paho MQTT library,

979-8-3315-8138-1

publishes the complete JSON file to the broker. The RTU subscribes to a dedicated topic and retrieves the file as soon as new protection settings are published.

D. Communication from RTU to IEDs

The RTU is capable of processing MQTT messages and transmitting IEC 61850 signals. However, these built-in features were not used. Writing signals to other IEDs is possible, but each signal must be created manually on the RTU and mapped to a dedicated MQTT topic for updating. Since the goal is to achieve an automated communication, this process is not feasible. Nevertheless, it is possible to include a so-called SIAPP. This is based on a docker container, allowing the creation of a fully configurable standalone software package that can be executed on the RTU. However, it must comply with hardware constraints. For instance, the container size must not exceed 350 MB. This approach enables multiple fallback levels. Additionally, a web interface was created to supervise the adapted settings. The libiec61850 was used to handle the communication between the RTU and the IEDs.

The following section describes the write process from the RTU to the IEDs. Upon receiving new settings, a check verifies that the JSON file contains the required top-level information. It is verified that SG ≥ 0 and that the parameter "IECDevices" exists. If so, the procedure continues, and the connection to the listed IEDs is monitored. The monitoring is described in detail in Section II-E. The RTU connects to the devices and creates multiple threads to establish communication with every IED. For each device, the currently active SG is queried to ensure that the procedure does not interfere with the active protection settings. If the SG targeted for writing differs from the active one, the process continues. Since communication is based on IEC 61850 MMS, each write request triggers a response from the IED, confirming whether the operation was successful. This allows the detection of failed write operations. The settings are not committed to the device after being written. The CnfEdit signal, which confirms and applies edited settings, is only set if all write operations for one device have been completed successfully. If a negative response occurs during the write process, the CnfEdit command is deliberately withheld, preventing any partial or inconsistent configuration from being applied. Since the number of protection settings to be changed may vary between devices, the system waits until each device has been successfully written. Afterwards, the SGs of all devices are switched. A communication failure during the switching of SGs is critical. To mitigate this, the switching command is sent in parallel to all devices. However, if the connection to an IED is lost during this process, different SGs could become active across devices. To prevent this, a two-sided fallback mechanism is implemented, which is explained in detail in the following section.

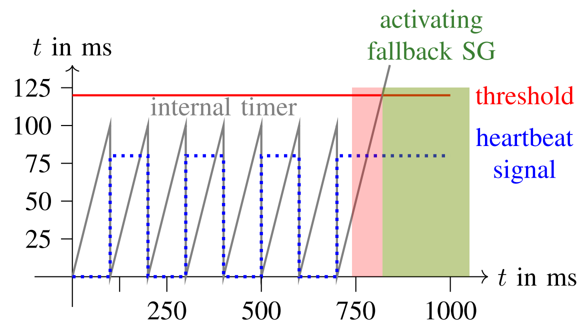

Fig. 4. Fallback mechanism on IED side.

E. Communication failure between RTU and IED

If the connection to any device is lost, the system switches back to the fallback SG. This SG contains conventional protection settings, ensuring that the implementation of adaptive protection remains at least equivalent to the status quo, even in case of communication failure. Since the device is no longer reachable through the RTU, a dedicated logic must be implemented on the IED itself. The general functionality is illustrated in Fig. 4. A GOOSE message is configured on the RTU and broadcast to all IEDs. Its value is updated periodically every 100 ms resulting in a heartbeat signal. On the IED level, a timer-based logic is implemented that resets whenever it detects a flank in the signal. If the timer exceeds a threshold of 120 ms, the IED activates its fallback SG independently. A communication error is depicted at $t = 740$ ms. The device switches to the fallback SG at $t = 820$ ms.

The IEDs do not communicate directly with each other. Therefore, the RTU monitors the connection to every device listed in the JSON centrally. It periodically attempts to connect to every device that is listed in the JSON. If one or more devices are not reachable for two consecutive 300 ms cycles, a switching command to the fallback SG is sent to all remaining reachable devices.

F. Communication failure between RTU and MQTT Server

Since the RTU constantly listens to the MQTT server, a communication loss can be detected nearly in an instant. In this case, each device receives a signal to switch back to the fallback SG. A reconnect process is implemented, and if the RTU successfully reconnects to the MQTT server, the SG is switched back to the previous configuration.

G. Simulation Case

The RTS simulates a 10 kV voltage level of a DSO in Germany. To emulate the communication between the IEDs and the RTS, IEC 61850 SV and GOOSE are implemented. Fig. 5 shows a simplified structure. All IEDs are located at a single substation, where the slack bus, representing the higher voltage level, is linked. Connected to the substation are several rings that could be operated either as closed rings

979-8-3315-8138-1

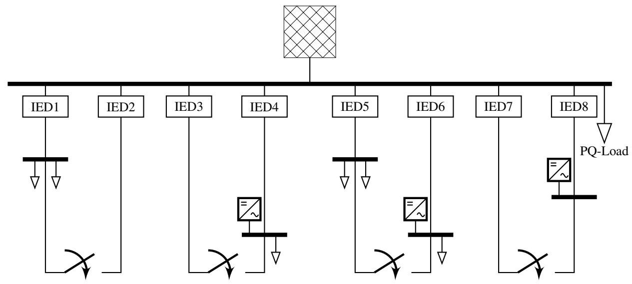

Fig. 5. Simplified network structure.

or as open branches. Each branch has a varying number of terminals, with each terminal supplying different amounts of loads, photovoltaic feed-in, and electric vehicle chargers. Due to the limited number of IEDs, only four different rings are simulated, while the remaining part of the network is summarized in one PQ load. As the slack provides the vast amount to the short circuit behavior the impact of this simplification is negligible. To reflect real operation as closely as possible, overcurrent-time protection and distance protection are used as protection functions, corresponding to the schemes applied in the actual substation. Due to the reduced number of IEDs, each IED, in contrast to the real setup, protects an entire ring or two branch circuits. Two instances of each protection function were configured on each device. Using SV, the substation voltage is broadcast to all IEDs, ensuring that they operate based on the same voltage reference. The current values are measured at each branch and sent to the respective protection devices. In total, 36 measured values were transmitted. GOOSE is used to communicate the trip decisions from the IEDs to the RTS to operate the circuit breakers when required.

III. Results

The timely behavior when writing new settings is evaluated. Afterwards, the two fallback mechanisms are examined. For changing a set of settings, $t = 0$ ms marks the moment when the RTU receives the new file and detects the active SG. Changing four settings per device took an average of 1.319 s over 10 test runs, ranging from 1.27 s to 1.394 s. Increasing the number of changed settings to 100 per device raised the average time to 2.863 s, ranging from 2.635 s to 3.537 s. In both cases, SG switching via IEC 61850 took approximately 400 ms of the total duration when the IED was fully configured which is significantly slower than the 100 ms stated in [4]. The IED's behavior during faults and SG switching could not be observed and may be vendor-specific. It can be concluded that the switching time depends on the number of preconfigured settings on the devices. A transition to specialized protection devices, such as distance relays, could reduce critical time due to fewer configurable parameters.

When switching between the normal and fallback SG, the exact moment of communication failure could not be reproduced in a time-synchronized manner. The analysis therefore focuses on the relative switching behavior of the IEDs, taking

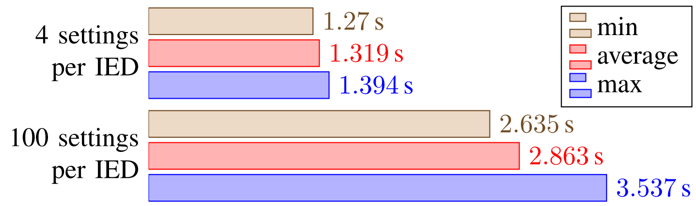

Fig. 6. Required time for changing settings.

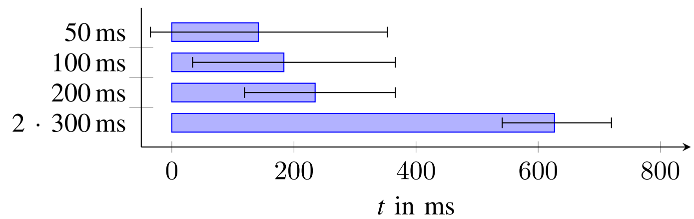

Fig. 7. SG switching behavior in reference to IED with communication failure.

the device that loses its connection as the reference. In Fig. 7 this behavior is shown for different connection times and cycles. Using two consecutive cycles of 300 ms, the reachable IEDs switch to the fallback SG 626 ms after the unreachable IED. Reducing the connection time and the cycle to one also reduces the average switching difference. In some cases, the reachable IEDs switch even faster than the unreachable one. However, further reducing this value can lead to unstable behavior when the connection experiences jitter. Switching back to the previous SG and switching the SG in case of an MQTT communication failure are both controlled centrally by the RTU for all IEDs. The resulting timing deviations are similar, averaging 57 ms.

IV. Conclusion

This work demonstrates a practical method for implementing adaptive protection using established hardware. A field-ready setup was built and tested that enables the centralized writing and switching of setting groups on multiple IEDs. The main functionality is implemented in a docker-based application on the RTU, which is publicly available and can be extended for further applications. The results show that adaptive protection can be realized with current IEDs and IEC 61850 services. The concept combines centralized coordination with local fallback mechanisms, ensuring a consistent protection scheme even under communication loss. The measurements indicate that setting group switching can be triggered simultaneously for all devices, but the actual switching times differ. Introducing additional logic on the IEDs, for example by allowing switching only after a defined timeout interval or at aligned time points, could reduce these deviations.

The present setup is limited to four IEDs, but the architecture can be extended to larger systems. Integrating devices from multiple vendors through their IEC 61850 data models could not be tested with the available hardware, but appears feasible based on the configuration used. Therefore, the presented setup provides a reproducible basis for practical adaptive protection implementations.

REFERENCES

[1] G. D. Rockefeller, C. L. Wagner, J. R. Linders, K. L. Hicks and D. T. Rizy, “Adaptive transmission relaying concepts for improved performance,” IEEE Trans. Power Delivery, vol. 3, no. 4, pp. 1446–1458, Oct. 1988

[2] K. Islam, D. Kim and A. Abu-Siada, “A review on adaptive power system protection schemes for future smart and micro grids, challenges and opportunities,” Electric Power Syst. Res., vol. 230, p. 110241, 2024

[3] S. Nomandela, M. E. S. Mnguni and A. K. Raji, “Systematic development and hardware-in-the-loop testing of an IEC 61850 standard-based monitoring and protection system for a modern power grid point of common coupling,” Energies, vol. 18, no. 19, p. 5281, 2025

[4] N. N. Shangase, “Interoperability challenges in multivendor IEC 61850 devices for parallel power transformer differential protection,” Int. J. Electr. Electron. Eng. Telecommun., vol. 13, pp. 45–57, Jan. 2024

[5] M. Pashaei, H. Rastegar, S. F. Zandrazavi, K. Kauhaniemi and H. Laaksonen, “Real-time hardware-in-the-loop approach for adaptive centralized protection schemes using clustering algorithms,” Expert Syst. Appl., vol. 255, p. 124707, 2024

[6] C. Mederer, “Field-ready implementation of fail-safe adaptive protection relay schemes”, GitHub, 2025. [Online]. Available: https://github.com/ChristophMed/Field-ready-implementation-of-fail-safe-adaptive-protection-relay-schemes.

[7] J. Vogelbacher, “writer-iec: Simple script for writing values to IEC servers,” GitHub, 2025. [Online]. Available: https://github.com/Jean28518/writer-iec.