Title: 5G-Based Fault Localization in Medium Voltage Underground Cables (FLUCCOM)

Author: Arman Ghaderi Baayeh

Date: 29.08.2024

Test Objectives

The main objective of these tests is to assess the feasibility and robustness of a novel 5G-based fault localization method designed for medium voltage underground cables. The tests will focus on validating the algorithm's resilience to communication latency, particularly when utilizing public communication networks instead of dedicated fiber optic links. This investigation is critical for benchmarking the performance of the proposed method as a reliable protection relay in distribution grids with a high penetration of inverter-based resources.

Purpose of Investigation *(PoI)*

The core purpose of investigation is summarized below:

- The tests will characterize the accuracy of the fault location method under varying communication latency conditions.
- They will verify the successful integration of the 5G communication module with the fault location algorithm.
- The tests will validate the reliability and robustness of the fault location method in medium voltage grids, especially under the influence of communication delays and in the presence of inverter-based resources and various fault scenarios.

Object under Investigation (*OuI*)

The following components of the platform are to be qualified by the tests:

- The embedded device implementing the fault localization algorithm.
- The 5G communication module and its integration with the protection algorithm.
- The RTDS for simulating transient waveforms and evaluating algorithm performance.

Function(s) under Investigation (*FuI*)

The functions specified by individual Objects under Investigation (OuI) are as follows:

- Fault detection and classification functions implemented on the embedded device.
- Communication functions and their capability to receive sample values from two channels.
- The fault location algorithm's ability to accurately identify fault positions under various scenarios.

Domain under Investigation (*DuI*)

The domain under investigation is power system protection. The tests will specifically focus on the system's performance under high penetration of inverter-interfaced renewable energy resources. The developed framework and test setup are designed to evaluate the impact of communication network characteristics, particularly latency, on the reliability of protection and fault location in medium voltage grids.

System under Test (*SuT*)

The following on-site and remote assets are included in the test-case:

<u>Simulation assets:</u>

- RSCAD for play backing simulated waveforms (on-site)
- Simulation tools MATLAB and Python (on-site)

<u>Hardware assets:</u>

- Real-time digital simulator (RTDS) for testing various fault scenarios (on-site)
- 5G test bed including merging units, network switch, and virtual private network. (on-site)
- Embedded device executing the fault location algorithm. (remote)

Functions under Test (*FuT*)

Three core functional components in OuI relevant for the operation of the SuT are tested:

- The fault location algorithm.
- Fault detection and classification functions.
- Communication unit of the embedded device.

Test criteria (TCR)

- Robustness of the protection algorithm in identifying internal faults under varying grid conditions, including high penetration of inverter-interfaced renewable energy sources.
- Sensitivity of the protection algorithm to communication latency.
- Fault location accuracy under various communication delay scenarios.

target metrics	variability attributes	quality attributes
• Fault Location Accuracy: The fault location error is measured as a percentage, ranging from 0% to 100%. An error of less than 2-3% is considered accurate, indicating reliable fault location performance. • Sensitivity of the Protection Algorithm: The protection algorithm must detect internal faults within one or two cycles of measurements. Sensitivity is evaluated by the algorithm's ability to quickly and accurately identify faults, ensuring timely protection. • **Impact of Communication Latency**: Communication latency is assessed by its effect on the protection algorithm's performance, particularly in detecting and responding to faults. An acceptable metric would involve the algorithm maintaining high accuracy and sensitivity despite latency, with minimal impact on fault detection times and error rates.	• **Uncontrolled Variability:** Factors such as network congestion, latency fluctuations, and inverter response, which cannot be directly controlled but must be accounted for in the testing process. • **Controlled Variability:** Factors such as communication latency (e.g., 5G network delays), fault types, fault location, and fault resistance, which can be manipulated to assess their impact on the protection algorithm's performance.	• **Sensitivity of Protection Algorithm**: The protection algorithm must accurately detect internal faults within one or two cycles, ensuring timely and reliable fault detection. • **Fault Location Accuracy**: The system must achieve a fault location error of less than 2-3% to meet the quality threshold. • **Successful Integration**: Pass/fail criterion based on the successful integration of components within the System under Test (SuT).