1 KIOS CoE – Sandboxing use-case 5 (SUC5) - Active distribution grid and microgrid

1.1 Description

With the increasing penetration of Distributed Energy Resources (DERs) in the distribution grid, active management of these variable and often intermittent resources has become essential. Active management of distribution grids can regulate generation and demand, ensure voltage stability, and manage congestion, enabling reliable, high-quality, and effective operation of modern distribution grids. Additionally, microgrid functionalities are required in certain cases, such as during faults or regional outages, to ensure the stand-alone operation of critical parts of the distribution grid. Active management systems facilitate smooth transitions between islanded (stand-alone) and grid-connected modes. In addition, automated control actions can be taken in each operating mode to ensure stable, efficient, and proper operation of distribution grids and microgrids.

This SUC involves the modeling of an MV distribution grid, with microgrid operating capabilities, as part of the digital twin within the real-time simulator. As depicted in Figure 1, the distribution grid includes three MV feeders, comprising a total of 15 distribution substations/buses. Each substation integrates PVs and load demand, modeled using synthesized data derived from real-life measurements. Additionally, each MV feeder includes a Battery Storage System (BSS), equipped with a Grid-Forming (GFM) inverter, enabling microgrid functionalities for operation in both grid-connected and islanding modes. Breakers are available to change the configuration of the distribution grid from radial to mesh or to enable the transition from grid-connected to islanding mode, if necessary. This setup allows the active distribution grid to function as a microgrid, operating independently from the main transmission grid. Islanding can be applied to the entire distribution grid or individually to each MV feeder, providing high flexibility and resilience in power management.

A microgrid controller is also modeled to receive measurements from each substation within the distribution grid/microgrid. The microgrid controller includes (a) an islanding and resynchronization controller and (b) a secondary controller. The islanding and resynchronization controller is responsible for smooth transitions between grid-connected (active distribution grid) mode and islanding (microgrid) mode with a minimum power disturbance. The secondary controller coordinates the flexible DERs (i.e., BSS with GFM inverters) within the microgrid. This coordination includes a power-sharing unit to regulate power exchange during grid-connected or islanded mode and a voltage-frequency (v-f) control scheme to maintain stability during stand-alone mode by keeping voltage and frequency close to nominal values.

It is essential for the microgrid controller to exchange measurements and set-points with the distribution grid emulated within the digital twin. Higher-level controllers, such as the DSO control center and/or a tertiary controller, need to communicate with the microgrid controller as well to send islanding trigger signals or provide reference values according to optimal scheduling of resources. As depicted in Figure 1, the tertiary controller provides active and reactive power references to the power-sharing unit during grid-connected mode and voltage and frequency references for the v-f control scheme of the secondary controller during islanding mode. The DSO gives the mode-transition command for the islanding and resynchronization controller.

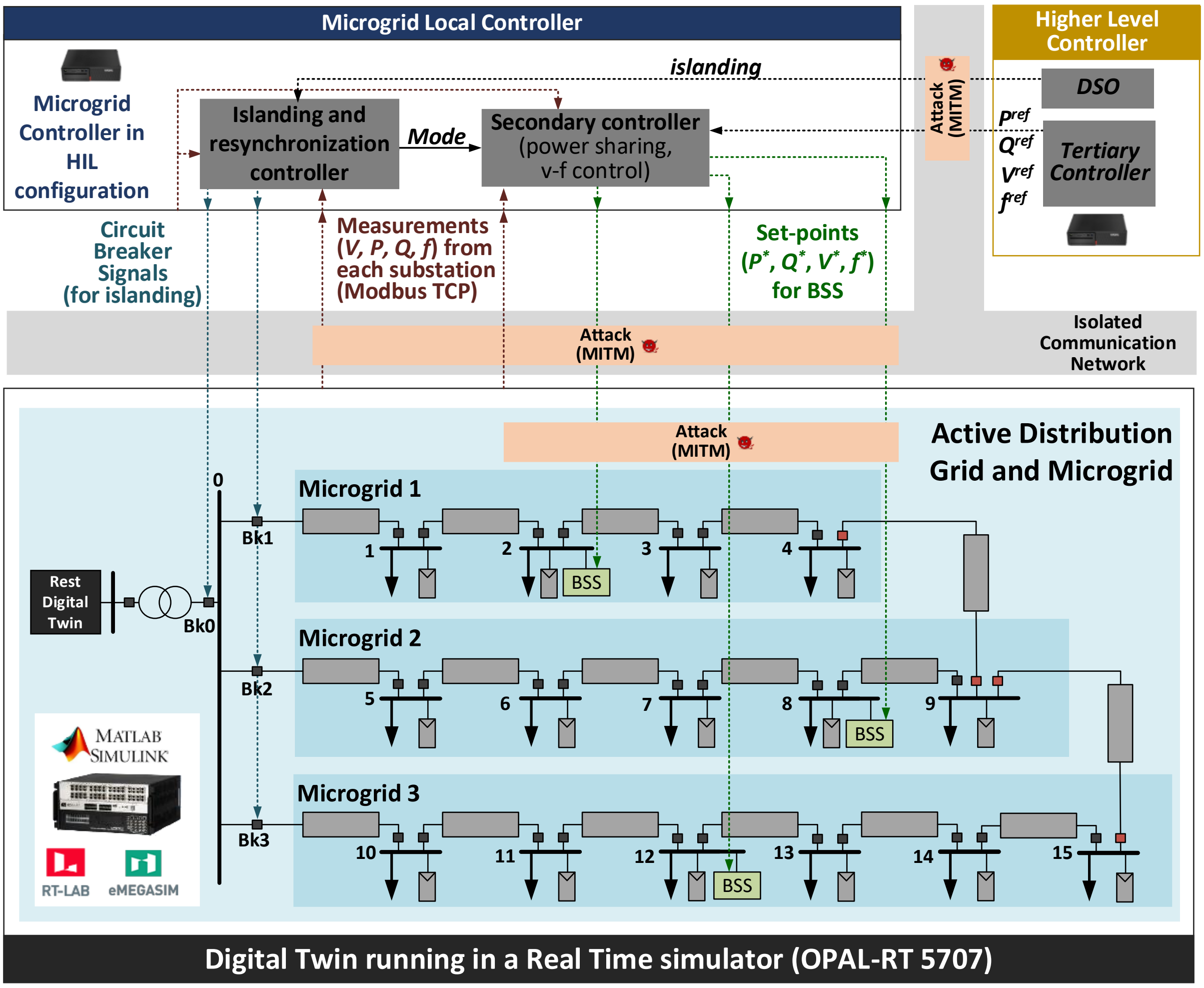

Figure 1 Testbed setup for investigating cyber-attack in active distribution grid and microgrid operation.

It the context of this sandboxing use case, various cyber-attack scenarios are investigated during the operation of the microgrid in either the grid-connected or the stand-alone mode (without examining the islanding transitioning), to further highlight the need for cyber-security solution in such active distribution grid and microgrid applications.

Within the framework of this SUC related to the operation of active distribution grids and microgrids, Modbus TCP communication is employed for data exchange. In this context, potential cyber-attacks include Man-In-The-Middle (MITM) attacks targeting the communication between the microgrid controller and either the higher-level controller (reference signals) or the active distribution grid/microgrid components (e.g., measurements from each substation, set-points to BSS). An FDI attack could manipulate the data of the reference values, set-points, or measurements exchanged in the local network. Consequently, such cyber-attacks can critically impact the operation of the active distribution grid or microgrid, as discussed in the following sub-section.

1.2 Attack scenarios

The attacks scenarios investigated in this SUC focus on MITM FDI attack, to compromise the integrity of data exchanged between different controllers within this SUC. A MITM with FDI attack on the set-points exchanged between the microgrid controller and the BSS will be investigated during grid-connected operation as active distribution grid, while a MITM with FDI on reference signals exchanged between higher-level and microgrid controller will be examined during islanding operation as microgrid. The attacks investigated in this SUC are summarized in Table 1.

Table 1: Attack Vector for SUC5

Attack Vector	Description
Attacked devices	• Set-points from the MG controller (Secondary controller) to the BSS primary controller. • Reference values from Higher Level Controller (Tertiary controller) sent to the MG Controller (Secondary controller).
Protocols	Modbus TCP
Type of attack	• MITM with FDI (during grid-connected mode operating as active distribution grid) • MITM with FDI (during islanding mode operating as microgrid)
Attack vector	Attacker should have access to local area network
Complexity	MITM and FDI (in both grid-connected and islanding mode): High complexity with precise signal value change in an offset approach
Privileges required	The attack is launched virtually within the digital twin level without requiring any privileges (e.g., administration rights) to access the device.
User interaction	None - There is no requirement for the attacker to authenticate to launch the attack.

1.3 Analysis of results

In this section, two specific scenarios (S1-S2) related to SUC5 are demonstrated and analysed, focusing on cyber-attacks targeting the communication channels between the microgrid local controller and either the higher-level controller or the inverter primary controller. These scenarios investigate MITM attacks involving FDI on the active power stet-points signals exchanged during grid-connected mode (S1), and on the frequency reference values exchanged during islanding mode (S2). For each scenario, an impact assessment is conducted to illustrate how these attacks can lead to power or frequency deviations during grid-connected or islanding mode, respectively.

1.3.1 SUC5/S1 – MITM with FDI cyber-attack during grid-connected operation

For the first scenario (S1), the active distribution grid is configured in grid-connected mode (Br0-Br3 are closed in Figure 1), with each MV feeder interconnected with the main grid. This scenario examines the operation of the GFM inverter of the BSS, connected at bus 2, during a MITM and FDI attack on the power set-point between the MG controller and the BSS primary controller. The specific FDI is virtually implemented within the digital twin environment, introducing an offset deviation on the power set-point (P^*) exchanged between the power-sharing unit of the secondary controller and the BSS primary controller of the GFM inverter. The objective is to disturb the active power exchange between the distribution grid and the main grid during grid-connected mode.

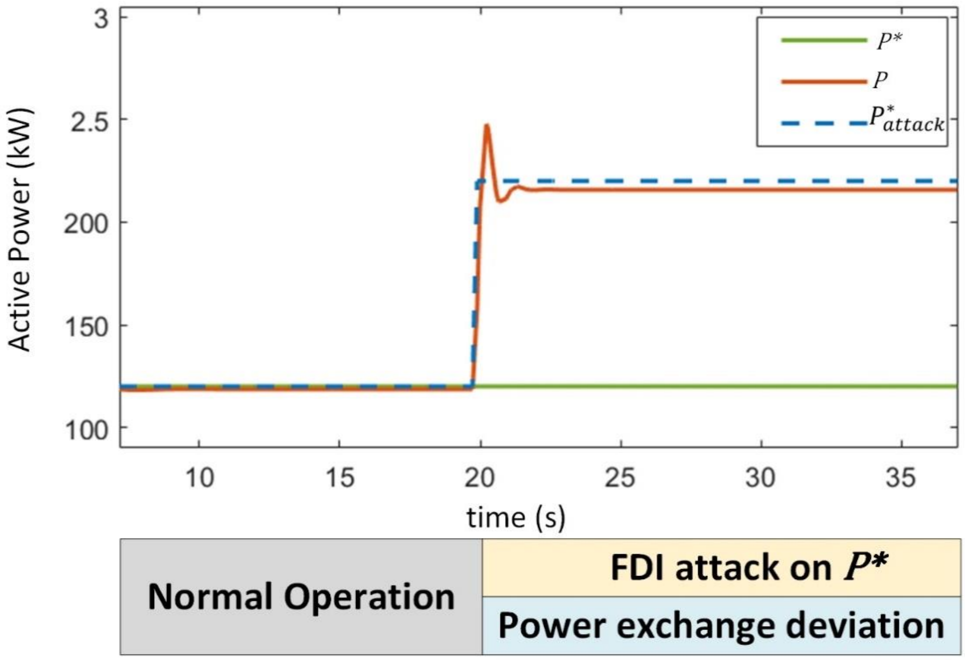

Figure 2: Active distribution grid operation during grid-connected mode, with an MITM-FDI attack on active power set-point P between microgrid local controller and BSS.*

In the case depicted in Figure 2, the active power operation (P) of each inverter-based BSS is regulated according to the set-points (P^*) generated by the power-sharing unit of the secondary controller (microgrid local controller), while considering the reference signals (P_{ref}) scheduled by the higher-level controller. During normal operation (before 20 s), the power injection of the BSS (connected at bus 2) is constant at 120 kW, as requested by the microgrid local controller. At 20 s, an MITM and FDI cyber-attack introduces a 100 kW offset deviation on the active power set-points (P^*) exchanged between the microgrid local controller and the BSS inverter controller. As a result, the BSS inverter changes its power injection to 220 kW according to the attacker-modified reference value (P^*_{attack}). This impacts the overall operation of the BSS, causing a significant deviation in the power exchange between the active distribution grid and the main grid.

The impact assessment of the first scenario (SUC5) indicates that a MITM and FDI cyber-attack, which deviates the power set-points by an offset, can cause significant power imbalance and deviation in the power exchanged between the active distribution grid and the main grid. If the attack causes an over-injection of power (i.e., the inverter injects more power than needed), it can lead to increased power export. Conversely, if the attack causes a power under-injection, it can lead to reduced power export or increased power import. Overall, such cyber-attacks can cause significant disturbances in power exchange within the active distribution grid. Therefore, it is crucial to safeguard smart grid applications against cyber-attacks.

1.3.2 SUC5/S2 – MITM with FDI cyber-attack under islanding operation

For the second scenario (S2), the active distribution grid shown in Figure 1 is configured in islanding mode (Br0 is open), with the three distribution feeders (Microgrid 1-3) equipped with BSS based on GFM inverters now interconnected (Br1-Br3 are closed) and operated as a single microgrid, disconnected from the main grid. The secondary controller (of the microgrid local controller) is responsible for monitoring and controlling the voltage and frequency of the entire microgrid through set-points (V^*, f^*) sent to the three GFM BSS inverters, while considering the reference signals (V_{ref}, f_{ref}) provided by a higher-level controller. In this scenario, a MITM and FDI cyber-attack introduces an offset deviation on the microgrid's frequency reference (f_{ref}) exchanged between the tertiary microgrid controller and the V-f control unit of the secondary controller. The objective is to disturb the operation of the entire microgrid system during islanding mode.

As presented in Figure 3, during normal operation (before 40 s), the microgrid frequency (f) follows the reference value of 50 Hz given by the tertiary controller (f_{ref}). The Proportional-Integral (PI) controller of the V-f control unit ensures that the microgrid frequency tracks the reference value in real-time, keeping the three feeders synchronized and compensating for any frequency deviations from the nominal values.

At 40 s, a MITM and FDI cyber-attack introduces a -0.5 Hz offset deviation on the reference frequency signal (f_{ref}) before it is received by the V-f unit of the secondary controller. As shown in Figure 3, although the tertiary controller continues to send the reference frequency of 50 Hz, this value is modified by the attacker, resulting in a new reference value (f_{ref_attack}) of 49.5 Hz. As the PI controller's reference input changes, the controller adjusts its output to minimize the frequency error between the measured frequency (f) and the attacked reference (f_{ref_attack}). Consequently, the microgrid frequency drops to 49.5 Hz, causing a constant deviation from the nominal frequency of 50 Hz and leading to frequency disturbance in the microgrid. If the attacker increases the frequency deviation, the microgrid's frequency stability will be seriously compromised. A similar response is expected in term of microgrid voltage operation, if the attacker deviates the voltage reference signals. In this case the voltage stability of the microgrid will be threatened as well.

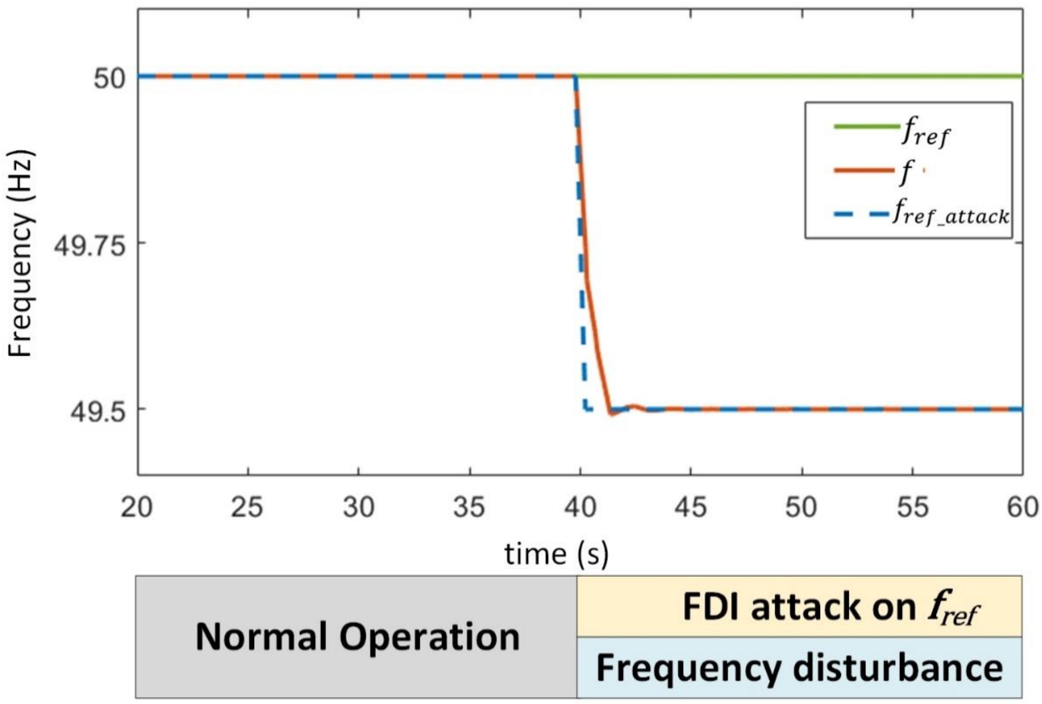

Figure 3: Microgrid operation during islanding mode, with an MITM-FDI attack on frequency reference signal f_{ref} between higher-level controller and microgrid local controller.

The impact assessment of this scenario indicates that the FDI attack on the frequency reference signal at the input of the secondary controller leads the entire microgrid to an underfrequency condition. The frequency deviation can cause critical frequency instability in the microgrid, with equipment and loads that depend on a stable 50 Hz frequency potentially malfunctioning or operating less efficiently, leading to disruptions in the power supply. Similarly, a cyber-attack on voltage reference signals can also threaten the voltage stability of the microgrid. Hence, it is important to safeguard the data exchange framework during islanding operation since the frequency and voltage stability of the microgrid is crucially affected.

1.4 Datasets

Section 1.3 illustrates two primary scenarios (S1-S2) concerning the operation of SUC5. These scenarios examine the functioning of an active distribution grid and microgrid system, along with the effects of certain cyber-attacks in this context. The demonstration of each scenario is detailed in selected time-series plots in Section 1.3, accompanied by an in-depth analysis of the processes and an impact assessment.

In this section, all data capture during the execution of each scenario is collected, including electrical measurements, reference and set-point signals. The datasets from each SUC5 scenario are made publicly available and can be accessed through the Zenodo repository. Further details regarding the dataset descriptions for the two scenarios (S1 and S2) of SUC5 can be found in Table 2 and Table 3, respectively.

Table 2: SUC5/S1 datasets

SUC5/S1	MITM with FDI cyber-attack in an active distribution grid (grid-connected)
Dataset description	This dataset is related to the operation of the fifth sandboxing use case (SUC5) described in the supporting document, which examines the operation of an active distribution grid, when the distribution grid is interconnected with the main grid. Specifically, this dataset corresponds to the first scenario (S1) of SUC5, where a MITM with FDI cyber-attack is virtually conducted within the sandboxing environment to introduce an offset deviation to the active power set-point allocated to BSS inverter controller from the secondary controller. More details about the scenario related to this dataset can be found in Section 1.3 of the supporting document. The dataset includes electrical measurements of the active power generated by the BSS inverter (connected at bus 2), and the active power set-point before and after the attack. The dataset is provided in the form of time-series measurements available as MATLAB (.mat) and CSV (.csv) files. The measurements were recorded from the real time simulator using the "OpWrite" block of the RT-LAB, with 1-millisecond time resolution.
Dataset purpose	• Analyse the operation a grid-connected feeder during healthy communication and under a MITM with FDI attack. • Impact assessment of cyber-attacks in such smart grid applications. • Test and evaluate cyber-security solutions to prevent the impact on power infrastructure.
Dataset type/format	• [ELECTRON_SUC5_S1_Grid-connected.mat] • [ELECTRON_SUC5_S1_Grid-connected.csv]
File size	1.460 KB
Data collection	Electrical measurements are extracted from the digital twin (running within the real-time simulators) of the sandboxing environment, using a block in the RT-LAB library named as 'OpWrite'.
Type of data	Electrical measurements of active power (in kW) injected by the BSS inverter (connected in bus 2), power set-point at the output of the secondary controller (in W), and the attacked power set-point received by the BSS (in kW).
Metadata and keywords	Renewable energy sources, battery storage system, active distribution grid, virtual power plant, cyber-attacks, man-in-the-middle, false data injection, Modbus TCP, electrical measurements, GFM inverter, secondary controller, tertiary controller, feeders, islanding, grid-connected, droop control.

Table 3: SUC5/S2 datasets

SUC5/S1	MITM with FDI cyber-attack in a microgrid (islanding mode)
Dataset description	This dataset corresponds to the second scenario (S2) of SUC5, where a MITM with FDI cyber-attack is virtually conducted within the sandboxing environment to introduce an offset deviation to the frequency reference signal, exchanged between the higher-level controller (tertiary controller) and the microgrid local controller (secondary V-f controller). More details about the scenario related to this dataset can be found in Section 1.3 of the supporting document. The dataset includes electrical measurements of the microgrid frequency, the reference frequency value generated by the tertiary controller, as well as the attacked frequency reference value. The dataset is provided in the form of time-series measurements available as MATLAB (.mat) and CSV (.csv) files. The measurements were recorded from the real time simulator using the “OpWrite” block of the RT-LAB, with 1-millisecond time resolution.
Dataset purpose	• Analyse the operation of the microgrid configuration during healthy communication and under MITM with FDI attack. • Impact assessment of cyber-attacks in such smart grid applications. • Test and evaluate cyber-security solutions to prevent the impact on power infrastructure.
Dataset type/format	• [ELECTRON_SUC5_S2_Islanding.mat] • [ELECTRON_SUC5_S2_Islanding.csv]
File size	4.671 KB
Data collection	Electrical measurements are extracted from the digital twin (running within the real-time simulators) of the sandboxing environment, using a block in the RT-LAB library named as ‘OpWrite’.
Type of data	Electrical measurements of frequency (in Hz) of the microgrid, frequency reference generated by the tertiary controller (in Hz), and attacked reference frequency (in Hz).
Metadata and keywords	Renewable energy sources, battery storage system, active distribution grid, virtual power plant, cyber-attacks, man-in-the-middle, false data injection, Modbus TCP, electrical measurements, GFM inverter, secondary controller, tertiary controller, feeders, islanding, grid-connected, droop control.