KIOS CoE – Sandboxing use-case 1 (SUC1) DER energy management and control

1.1 Description

This sandboxing use case focuses on advanced energy management and control applications for DERs, which are essential for optimizing their operation and achieving key objectives. These objectives include tracking the awarded power generation according to energy market clearing processes, avoiding intense power imbalances caused by intermittent weather-based RES, and increasing the profitability of DER owners. By leveraging real-time control strategies, the management system can dynamically adjust flexible DER operations to improve the overall response of aggregated DERs, based on both RES and Battery Storage Systems (BSS). Since this use case requires active control of an BSS and its operation can be severely affected in case of a cyber-attack, it is crucial to examine this scenario in a controlled and non-invasive environment enabled by the sandbox to avoid any disturbance to the actual power infrastructure.

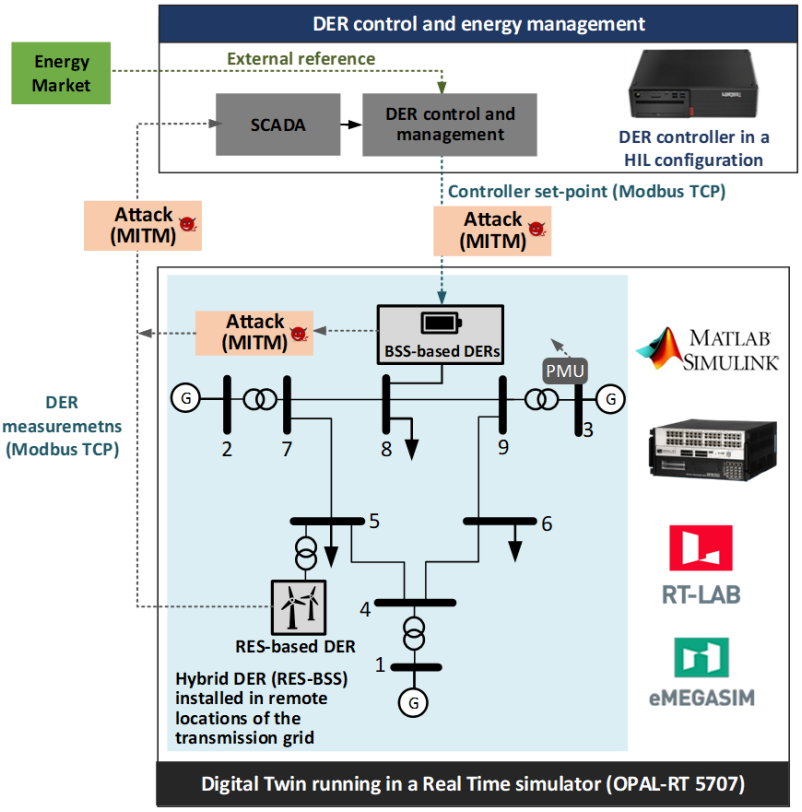

Figure 1: Testbed for DER energy management and control.

This sandboxing use case involves a RES (wind farm) and a flexible DER (BSS), which are remotely installed within the IEEE 9 bus transmission system, as illustrated in Figure 1. The entire system is emulated as a digital twin of a dynamic power system enhanced with DERs and runs in a real-time simulator (OPAL-RT 5707), as discussed in Section **Error! Reference source not found.**. The RES is i nstalled at bus 5 and is modelled as an inverter-based RES to replicate the operation of an actual 10.8 MW wind farm (6 x 1.8 MW wind turbines) located in Larnaca, Cyprus. Field measurements are received from the wind farm with a resolution of 30 seconds (through an IoT platform) and are fed into the real-time simulator to replicate the wind farm operation within the digital twin. The flexible DER is installed at bus 8 and is modelled as a 40 MVA inverter (in grid-following mode) combined

with a 40 MWh BSS. The BSS operation is regulated according to external set-points sent by the DER controller.

In this use case, the RES and the flexible DER are jointly managed, as a Virtual Power Plant (VPP), by a single energy market participant committed to delivering a constant active power to the grid on an hourly basis according to the market clearing results. To achieve this, a VPP-level DER controller is required to enable effective energy management of both the RES and the flexible DER (BSS). The DER controller is implemented as software running on a PC/Server connected in a real-time Control-HIL configuration with the power system digital twin, as presented in Figure 1. The DER controller is periodically executed every 5 seconds and has the following functionalities:

- **Receives measurements:** Receives measurements from RES operation (i.e., active P and reactive Q power) and from the flexible DER (i.e., active P, reactive Q power, and State of Charge - SOC) through Modbus TCP communication.
- **Monitoring:** Processes these measurements in a Supervisory Control and Data Acquisition (SCADA) system to monitor the VPP operation and the individual operation of RES and DER.
- **DER control and management:** Executes a DER control and management algorithm based on RES/DER measurements and external market obligation references (obtained through over-the-internet communication from the energy market portal) to determine the active power control set-point for the flexible DER. At this stage, the reactive power controller can also be executed to regulate overall reactive power injection according to Transmission System Operator (TSO) requests (to achieve voltage management).
- **Send set-points:** Sends active and reactive power set-points to the flexible DERs through Modbus TCP to regulate their operation and ensure controllable power injection when RES and DER are jointly considered as a VPP.

In this context, different cyber-attack scenarios have been examined (according to Section **Error! R eference source not found.**) to compromise the communication channels of the sandboxing use case and assess the impact on power domain operation. Specifically, MITM attacks have been both actually and virtually performed on the Modbus TCP communication channels established for receiving measurements from RES/DER and for sending set-points to flexible DER, as indicated in Figure 1. Complex MITM attacks combined with FDI have been conducted, with selected measurements and set-point values precisely altered using offset deviation, multiplicative alteration, stack at constant value, and replay attack approaches. Additionally, MITM with DoS attacks have been performed, where selected Modbus TCP connections between RES, flexible DER, and the VPP-level controller are dropped when the attack is launched.

The attack scenarios for this SUC are presented in Section 1.2. Selected attack scenarios are demonstrated in Section 1.3, where an impact assessment is also performed for those scenarios. Details about the datasets collected through SUC1 is provided in Section 1.4.

1.2 Attack scenarios

The attacks investigated in this SUC are summarized in Table 1. These scenarios focus on two primary types of MITM attacks: one involving FDI to compromise the integrity of measurements and set-points exchanged within SUC1, and another involving DoS to disrupt communication between RES-DERs and the DER controller. The targeted protocol for these attacks is Modbus TCP, a widely utilized protocol in smart grid applications.

Table 1: Attack Vector for SUC1

Attack Vector	• Description
Attacked devices	• Measurements from smart meters of RESs and DERs to DER controller. • Set-points sent to flexible DER inverters from DER controller.
Protocols	Modbus TCP
Type of attack	• MITM with FDI. • MITM with DoS.
Attack vector	Attacker should have access to local area network (of any RES and DER park)
Complexity	• MITM and FDI: High complexity with precise signal value change in an offset, multiplicative, stack at, and replay approach • MITM with DoS: Low complexity by dropping down (disrupting) the connection of the specific communication protocol.
Privileges required	The attack is launched either virtually within the digital twin or actually at the network 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, four selected scenarios (S1-S4) related to SUC1 are demonstrated and analysed, considering various cyber-attacks on communication channels between the RES, the flexible DER, and the DER's controller. The first three scenarios (S1-S3) examine MITM attacks with FDI on RES (wind farm) measurements, BSS measurements, and BSS set-points, respectively. The last scenario (S4) demonstrates the SUC1's operation under a MITM with DoS attack. For each scenario, an impact assessment is performed to show how these attacks can cause power deviations or power oscillations in the combined operation of RES and ES - hybrid system.

1.3.1 SUC1/S1 - MITM with FDI cyber-attack on wind farm measurements

The first scenario examines the operation of the hybrid DER system (RES-BSS) under a VPP framework when a MITM and FDI attack is conducted on wind farm measurements. This specific FDI attack (virtually implemented within the sandboxing) is characterized by high complexity, introducing an offset deviation on the wind farm measurements received by the DER controller (VPP-level controller) to disturb the operation of the hybrid DER system (Figure 2).

During normal operation (before 15:50 and after 15:52), the system is healthy and operating normally (no cyber-attack). Specifically, during the normal operation time interval, the RES (wind farm) generates 4 MW, and the flexible DER (BSS) discharges 1 MW to ensure that the hybrid DER (RES-BSS) successfully delivers 5 MW to the power grid, as required by the external reference according to the energy market clearing results.

In this scenario, a MITM and FDI attack is launched between 15:50 and 15:52. The cyber-attack maliciously introduces a 10 MW offset deviation on the measurements sent from the wind farm to the DER controller (VPP-level), as shown in the first plot of Figure 2. This attacked measurement affects the DER controller's response, causing an alteration to the set-point generated for the BSS. Consequently, the overall operation of the hybrid DER is impacted, as demonstrated in the second plot of Figure 2. During the attack, an inverse power deviation (-10 MW) is introduced to the power delivered by the combined RES and ESS plant. Thus, the attack deviates the power exchange from the requested 5 MW injection to a 5 MW absorption (-5 MW).

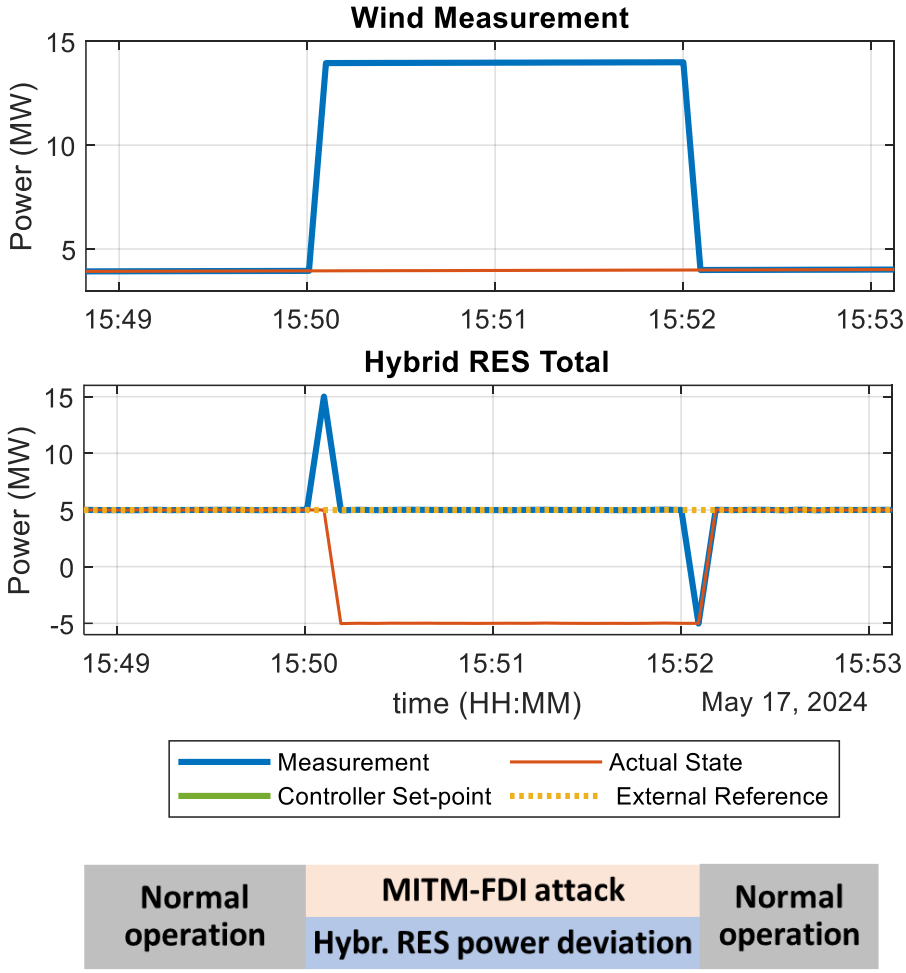

Figure 2: MITM and FDI attack causing offset deviation on wind farm measurements.

The impact assessment of this MITM and FDI cyber-attack in the context of SUC1 indicates that a malicious offset deviation of a wind farm measurement can cause a significant inverse power deviation in the power exchanged by the combined RES-ESS plant. Such attacks can result in undesired and intense power deviations from the market-awarded values, affecting the overall hybrid DER power operation and introducing power disturbances to the power system.

1.3.2 SUC1/S2 - MITM with FDI cyber-attack on BSS measurements

The second scenario examines the operation of the hybrid DER system (RES-BSS) when a MITM and FDI attack is conducted on BSS measurements. In this scenario, a virtual FDI attack of high complexity is implemented, introducing a multiplicative change on the BSS measurements before they are received by the DER controller at the VPP level to disrupt the operation of the hybrid DER system, as demonstrated in Figure 3.

During normal operation (before 05:40 and after 05:42), the hybrid DER functions correctly, providing the market-awarded power injection of 4 MW. During this period, the RES (wind farm) generates 6.46 MW, and the flexible DER (BSS) charges with 2.46 MW to match the market clearing

reference.

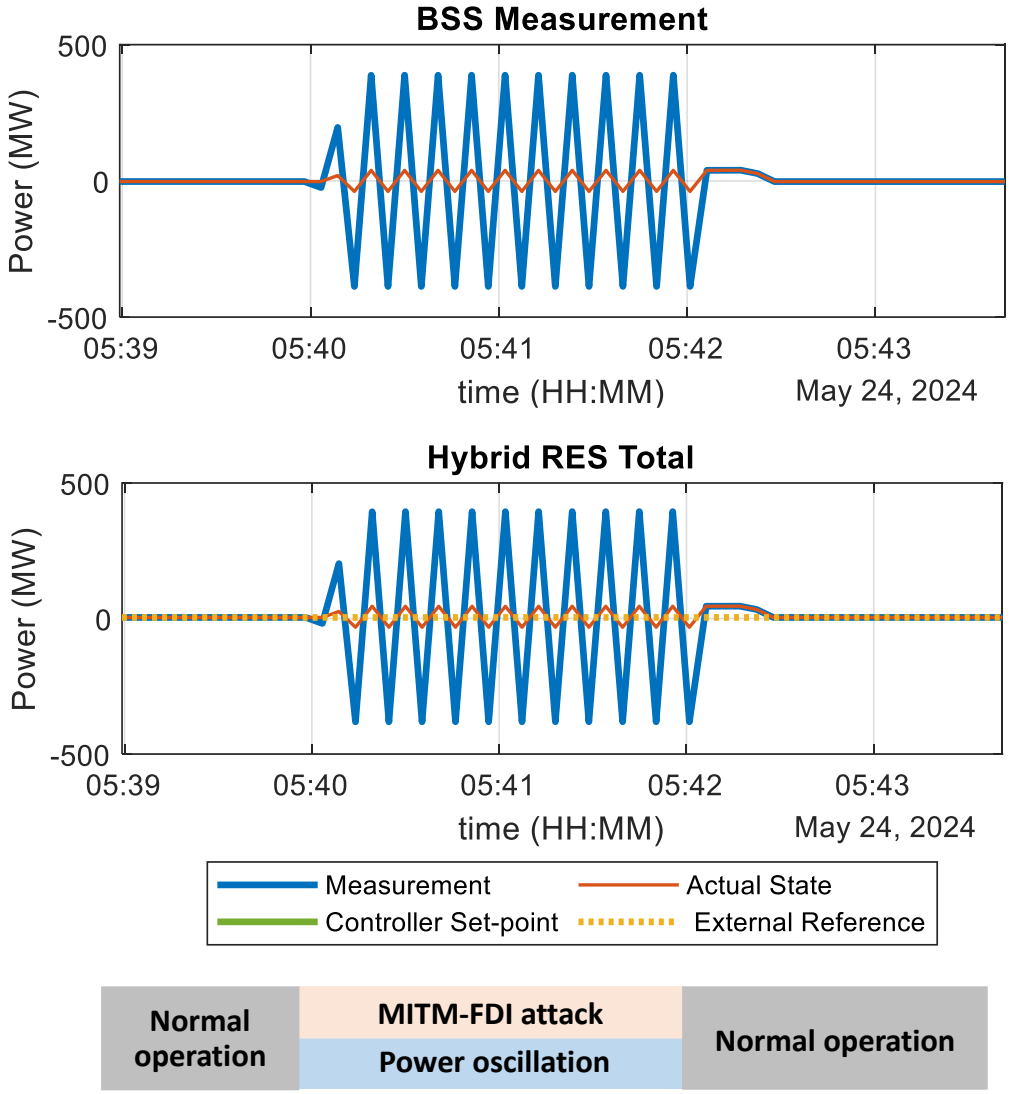

Figure 3: MITM and FDI attack causing multiplicative changes on BSS measurements.

A MITM and FDI cyber-attack is launched between 05:40 and 05:42, introducing a malicious multiplicative change (x10) on the BSS measurements sent to the DER controller (VPP level), as shown in the first plot of Figure 3. This attacked measurement affects the DER controller's response, causing the generation of extremely high set-points for the BSS, which forces the BSS to be saturated (charging or discharging) to the inverter's nominal power (±40 MW). This operation introduces an intense deviation between the external reference (market signal) and hybrid DER power injection, leading to the generation of new extremely high set-points in the opposite direction (from charging to discharging and vice versa). Consequently, the BSS oscillates between the upper (+40 MW) and lower (-40 MW) power operation points, limited by the BSS inverter's nominal power. Thus, the combined operation of the hybrid DER (RES-BSS) oscillates between 46.46 MW (injection) and -35.54 MW (absorption) during the attack, as presented in the second plot of Figure 3.

The impact assessment for the second scenario of SUC1 indicates that a MITM and FDI cyber-attack with a malicious multiplicative change in BSS measurements can cause intense power oscillation in

BSS operation. This results in severe power oscillation of the combined RES and BSS plant, introducing oscillating power disturbances to the power system that can affect the system stability.

1.3.3 SUC1/S3 - MITM with FDI cyber-attack on BSS set-points

While Scenarios S1 and S2 focus on MITM attacks on measurements, the third scenario of SUC1 emphasizes MITM with FDI attacks on set-points exchanged between the DER controller and the BSS. In this scenario, a FDI attack is implemented by replacing the active power set-point value (received by the BSS) with a constant value, effectively locking the BSS operation into a specific operating point and disrupting the overall operation of the hybrid DER system, as illustrated in Figure 4.

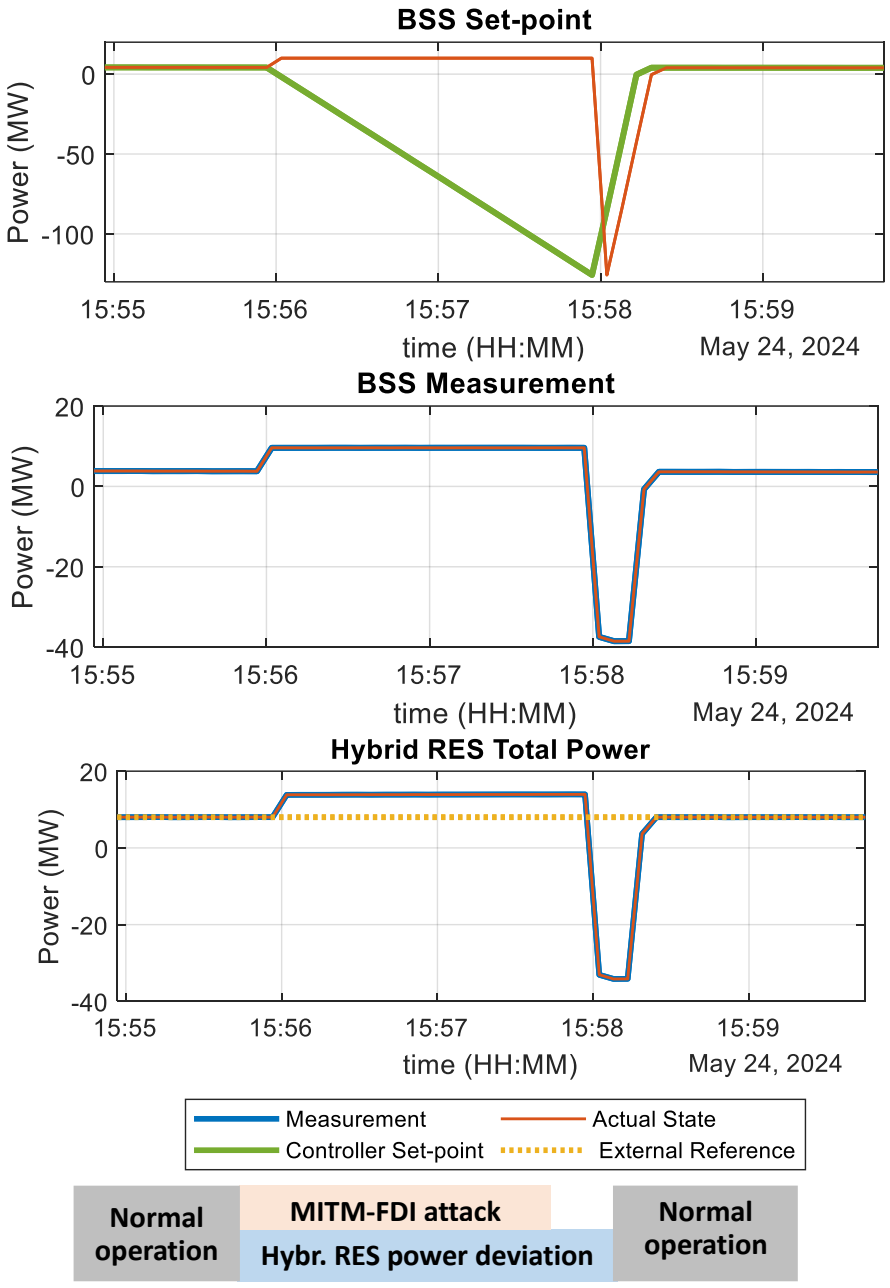

Figure 4: MITM and FDI attack stacking the BSS set-point to a constant value.

During normal operation without any cyber-attack (before 15:56 and after 15:58), the hybrid DER functions correctly, providing the market-awarded power injection of 8 MW. During this period, the

wind farm generates 4.2 MW, and the flexible DER (BSS) discharges 3.8 MW to meet the market external reference.

A MITM and FDI cyber-attack is launched between 15:56 and 15:58, setting the BSS set-point to a constant 10 MW, as shown in the first plot (red line) of Figure 4. As a result, the BSS changes its power injection to 10 MW according to the attacker-modified set-point, causing the hybrid DER injection to increase to 13.9 MW instead of the 8 MW required by the external market reference, as shown in the second and third plots of Figure 4. The deviation introduced by the attack between the market reference and the hybrid DER power injection forces the DER controller to change the BSS set-point to a large negative value in an attempt to compensate for the deviation imposed by the attacker. Consequently, when the cyber-attack is deactivated, the BSS power injection drops to the nominal negative value of the BSS inverter (-40 MW) for approximately 15 seconds, causing a significant disturbance in the operation of the hybrid DER.

The impact assessment of the third scenario of SUC1 indicates that a MITM and FDI cyber-attack that fixes the BSS set-point at a constant value can cause significant power deviation in the BSS and the hybrid DER operation during the attack. Additionally, an intense power deviation occurs for a transient period when the attack is deactivated. Such a cyber-attack causes power deviations and disturbances in the combined RES and BSS plant, ultimately affecting the overall operation of the power system.

1.3.4 SUC1/S4 - MITM with DoS cyber-attack

The final scenario of SUC1 focuses on a MITM combined with DoS attack that disrupts (drops) the Modbus TCP communication channel between the RES, BSS, and DER controller. This is implemented as an actual attack in the communication network of the sandboxing environment, following the description provided in Section **Error! Reference source not found.**. The MITM-DoS a ttack is indicated by the “Modbus Communication Lost” signal in the third plot of Figure 5, where 1 indicates that the attack is active and 0 indicates healthy communication conditions.

During healthy conditions (before 11:46:30 and after 11:54), the wind farm generates 4.8 MW, the BSS discharges 3.2 MW, and the hybrid DER delivers the 8 MW active power requested by the market external references.

When the MITM with DoS attack is launched between 11:46:30 and 11:54, the DER controller continues to use the previous inputs from the latest RES and BSS measurements. This is due to a debugging mechanism within the controller that considers the latest received values as inputs when communication is lost, preventing the controller from crashing. Consequently, the DER controller’s output signal (BSS set-point) remains constant and equal to the latest output before the attack, as shown in the first plot of Figure 5. Similarly, since communication between the DER controller and the BSS is disrupted during the attack, the internal set-point of the BSS inverter remains at the last healthy value, keeping the BSS power injection constant at the pre-attack level. However, this "freeze" operation of the BSS can affect the combined operation of the hybrid DER (RES and BSS) if wind power generation deviates or the external market reference changes. In Figure 5 (second plot), the external market reference changes from 8 MW to 4 MW at 11:50. Since the DoS attack is active during this time, the BSS cannot effectively adjust to the new reference point, and the hybrid RES and BSS plant fails to deliver the power requested by the energy market. Once the attack is deactivated and the Modbus TCP communication is re-established, the hybrid DER can follow the new reference signal again.

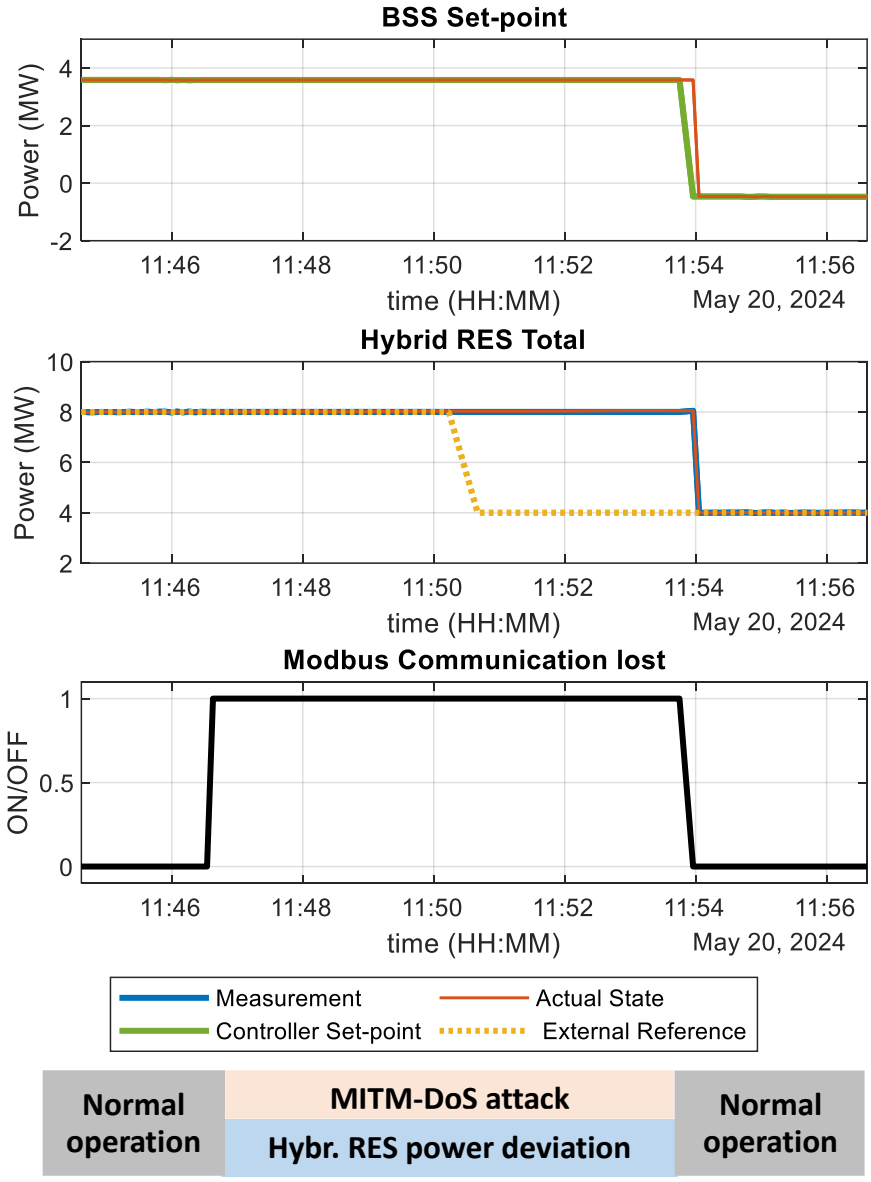

Figure 5: MITM with DoS attack distributing the Modbus TCP communication received and sent by the DER controller.

The impact assessment for the final scenario of SUC1 indicates that a MITM combined with DoS cyber-attack freezes the operation of the BSS at pre-attack values. Under such attacks, the BSS power injection remains constant and cannot respond to changes in RES generation or market external reference alterations. As a result, the hybrid DER power operation becomes uncontrollable.

1.4 Datasets

Four main scenarios (S1-S4) related to SUC1 operation have been demonstrated in Section 1.3. These scenarios explore the operation of a RES, a BSS, and their combined operation as a hybrid DER within a VPP framework under healthy conditions and various cyber-attacks targeting different communication channels. The demonstration of each scenario is presented through selected time-series plots in Section 4.3, accompanied by a detailed analysis of the processes involved and an impact assessment.

In this section, we have collected all the data captured during the execution of each scenario, including electrical measurements and network traffic. The datasets from each scenario of SUC1 are

made openly available and can be accessed through a Zenodo repository linked to this documentation.

Further details regarding the dataset descriptions for the four scenarios (S1-S4) of SUC1 can be found in Table 2 - Table 5, respectively.

Table 2: SUC1/S1 datasets

SUC1/S1	MITM with FDI cyber-attack on wind farm measurements
Dataset description	This dataset is related to the operation of the first sandboxing use case (SUC1) which examines the operation of a RES (wind farm) and a BSS as a combined hybrid DER within a VPP framework. Specifically, this dataset corresponds to the first scenario (S1) of SUC1, where a combined MITM and FDI cyber-attack is virtually conducted within the sandboxing environment to introduce an offset deviation to wind farm measurements received by the DER controller via the Modbus TCP communication protocol. More details about the scenario related to this dataset was described in the previous sections of this document. The dataset includes electrical measurements of the active power generation of the wind farm (attacked signal and actual state) and the BSS operation, as well as the set-point generated by the DER controller. The dataset is provided in the form of time-series measurements available as MATLAB (.mat) and CSV files. The measurements were recorded with a 5-second time resolution by the DER controller.
Dataset purpose	• Analyse the operation of RES, BSS and a hybrid DER configuration operating in a VPP approach during healthy communication and under MITM and 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_SUC1_S1_Pwind_Attack_Measurements.mat] • [ELECTRON_SUC1_S1_Pwind_Attack_Measurements.csv]
File size	17 KB, 43 KB
Data collection	This dataset was collected through the DER controller (executed in a Server PC installed within the sandboxing laboratory facilities) which is connected in the loop with the power system digital twin running in the real time simulator.
Type of data	Electrical measurements of active power (in kW) from RES and BSS and control set-point generated by the DER controller.
Metadata and keywords	Renewable energy sources, battery storage system, distributed energy resources controller, virtual power plant, cyber-attacks, man-in-the-middle, false data injection, Modbus TCP, electrical measurements.

Table 3: SUC1/S2 datasets

SUC1/S2	MITM with FDI cyber-attack on BSS measurements
Dataset description	This dataset is related to the operation of a sandboxing use case (SUC1) which examines the operation of a RES (wind farm) and a BSS as a combined hybrid DER within a VPP framework. Specifically, this dataset corresponds to the second scenario (S2) of SUC1, where a combined MITM and FDI cyber-attack is virtually conducted within the sandboxing environment to introduce a multiplicative change to BSS measurements received by the DER controller via the Modbus TCP communication protocol. More details about the scenario related to this dataset was provided in the description section of this sandboxing use-case. The dataset includes electrical measurements of the active power generation of the wind farm and the BSS operation (attacked signal and actual state), as well as the set-point generated by the DER controller. The dataset is provided in the form of time-series measurements available as MATLAB (.mat) and CSV files. The measurements were recorded with a 5-second time resolution by the DER controller.

Dataset purpose	• Analyse the operation of RES, BSS and a hybrid DER configuration operating in a VPP approach during healthy communication and under MITM and 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_SUC1_S2_Pbss_meas_Attack_Measurements.mat] • [ELECTRON_SUC1_S2_Pbss_meas_Attack_Measurements.csv]
File size	15 KB, 37 KB
Data collection	This dataset was collected through the DER controller (executed in a Server PC installed within the sandboxing laboratory facilities) which is connected in the loop with the power system digital twin running in the real time simulator.
Type of data	Electrical measurements of active power (in kW) from RES and BSS and control set-point generated by the DER controller.
Metadata and keywords	Renewable energy sources, battery storage system, distributed energy resources controller, virtual power plant, cyber-attacks, man-in-the-middle, false data injection, Modbus TCP, electrical measurements.

Table 4: SUC1/S3 datasets

SUC1/S3	**MITM with FDI cyber-attack on BSS set-points**
Dataset description	This dataset is related to the operation a sandboxing use case (SUC1) which examines the operation of a RES (wind farm) and a BSS as a combined hybrid DER within a VPP framework. Specifically, this dataset corresponds to the third scenario (S3) of SUC1, where a combined MITM and FDI cyber-attack is virtually conducted within the sandboxing environment to replace the BSS set-point (sent by the DER controller to the BSS) at a constant value (stack-at) via the Modbus TCP communication protocol. The dataset includes electrical measurements of the active power generation of the wind farm and the BSS operation, as well as the set-point generated by the DER controller (attacked signal and actual state). The dataset is provided in the form of time-series measurements available as MATLAB (.mat) and CSV files. The measurements were recorded with a 5-second time resolution by the DER controller.
Dataset purpose	• Analyse the operation of RES, BSS and a hybrid DER configuration operating in a VPP approach during healthy communication and under MITM and 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_SUC1_S3_Pbss_ref_Attack_Measurements.mat] • [ELECTRON_SUC1_S3_Pbss_ref_Attack_Measurements.csv]
File size	16 KB, 34 KB
Data collection	This dataset was collected through the DER controller (executed in a Server PC installed within the sandboxing laboratory facilities) which is connected in the loop with the power system digital twin running in the real time simulator.
Type of data	Electrical measurements of active power (in kW) from RES and BSS and control set-point generated by the DER controller.
Metadata and keywords	Renewable energy sources, battery storage system, distributed energy resources controller, virtual power plant, cyber-attacks, man-in-the-middle, false data injection, Modbus TCP, electrical measurements.

Table 5: SUC1/S4 datasets

SUC1/S4	**MITM with DoS cyber-attack**
Dataset description	This dataset is related to the operation of the use case (SUC1) which examines the operation of a RES (wind farm) and a BSS as a combined hybrid DER within a VPP framework. Specifically, this dataset corresponds to the fourth scenario (S4) of SUC1, where a combined MITM and DoS cyber-attack is conducted, as actual attack, in the

	isolated communication network of the sandboxing environment, disrupting the Modbus TCP communication exchanged between RES, BSS, and DER controller. More details about the scenario related to this dataset was provided in the description part of this document. The dataset includes electrical measurements of the active power generation of the wind farm and the BSS operation, as well as the set-point generated by the DER controller (attacked signal and actual state). In addition, the dataset includes the network communication traffic (related to Modbus TCP), as it is captured the WireShark software during the use case execution. The dataset is provided in the form of time-series electrical measurements available as MATLAB (.mat) and CSV files, recorded with a 5-second time resolution by the DER controller. In addition, the dataset includes network traffic packets captured as .pcapng files.
Dataset purpose	• Analyse the operation of RES, BSS and a hybrid DER configuration operating in a VPP approach during healthy communication and under MITM and 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_SUC1_S4_Modbus_MITM_Attack_Measurements.mat] • [ELECTRON_SUC1_S4_Modbus_MITM_Attack_Measurements.csv] • [ELECTRON_SUC1_S4_Modbus_Attack_Traffic.csv] • [ELECTRON_SUC1_S4_Modbus_Attack_Traffic.pcapng]
File size	11 KB, 80 KB, 56 KB
Data collection	This dataset was collected through: • the DER controller (executed in a Server PC installed within the sandboxing laboratory facilities) which is connected in the loop with the power system digital twin running in the real time simulator for the electrical measurements. • The WireShark software for capturing all the network traffic related to Modbus TCP communication.
Type of data	Electrical measurements of active power (in kW) from RES and BSS and control set-point generated by the DER controller. In addition, network traffic data related to Modbus TCP communication.
Metadata and keywords	Renewable energy sources, battery storage system, distributed energy resources controller, virtual power plant, cyber-attacks, man-in-the-middle, false data injection, Modbus TCP, electrical measurements, network traffic.

The above-mentioned datasets are made openly accessible and can be utilized by the wider scientific community to analyse the operation of modern power systems under various cyber-attack scenarios and to design new cyber-security solutions for safeguarding the operation of smart grids.