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

IEMI Test on a Complex Smart Grid Communication System (PETER)

Access Duration: 19/04/2022 to 09/07/2022

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:	Arash Nateghi (WIS Munster, Germany)

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:	[nnn]
Access Project Acronym:	PETER
Access Project Name:	IEMI Test on a Complex Smart Grid Communication System
User Group Leader:	Arash Nateghi (WIS Munster, Germany)
Document Identifier:	ERIGrid2-Report-Lab-Access-User-Project-PETER-final
Report Version:	vn.n
Contractual Date:	dd/mm/yyyy
Report Submission Date:	dd/mm/yyyy
Lead Author(s):	Arash Nateghi (WIS Munster) and Fernando Arduini (Fraunhofer INT)
Co-author(s):	
Keywords:	IEMI. Smart Grid. Communication System. Jamming Signals. Consequence Analysis. Nadir Frequency.
Status:	__ draft, _x_ final

Change Log

Date	Version	Author/Editor	Summary of Changes Made
08/12/2022	v1.0	Fernando Arduini (Fraunhofer INT)	Draft report template

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

The duration access was divided in two parts as the participants have different tasks. The access periods were the following:

Access Duration 1: 19/04/2022 to 19/05/2022 (Arash Nateghi – WIS Munster)
Access Duration 2: 15/06/2022 to 09/07/2022 (Fernando Arduini – Fraunhofer INT)

The respective report for each access is presented as follows:

- Access 1 (Arash Nateghi): *From page x to page x*
- Access 2 (Fernando Arduini): *From page x to page x*

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:	Arash Nateghi (WIS Munster, Germany)

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

Table of Contents

1 First List of Figures

List of Tables

Chapter 1

Lab Access 1 - Arash Nateghi (WIS Munster)

1 Introduction - Arash

The project Acronym is PETER (Pan- European Training, Research Education Network on Electromagnetic Risk Management) funded by the Marie- Sklodowska- Curie Actions (MSCA) within the Horizon 2020 program of the European Commission. The main objective of PETER project is to train 15 Early Stage Researchers (ESRs) on topics related to the development of high technology systems that maintain their reliability and safety throughout their life cycle, despite these systems being exposed to severe and complex Electromagnetic Interfere (EMI) threats.
Currently, the problem of EMI is addressed with a "rules-based" approach. This means that during the design phase for an electronic device, several directives/norms are prescribed, resulting in the standard application of several mitigation techniques (filtering, shielding, cable routing, etc.). But as the examples above show, such an approach suffers from some serious shortcomings when it comes to modern high-tech systems and highly critical applications such as medical systems and smart grid complex systems.
Because critical system safety is crucial and addressing the EMI issues requires evaluating failure probabilities that should be overlooked, rule-based approaches give a false sense of security when system reliability needs to be considered. Therefore, to ensure that people's safety is not compromised in this way, the PETER consortium has initiated a novel and much more robust "risk-based" approach to EMI management.
Both ESR 2 and ESR 15 are working closely together towards to give theoretical description of risk assessment methodologies, carrying out experimental analysis and model verification and work on risk management of the Smart Grid network of systems when Intentional Electromagnetic Interference (IEMI) attacks or threats cause disruptions to the system. The complex smart grid system includes the communication subsystem and application subsystems.
Each ESR focuses on one of the subsystems according to the requirements defined by its assigned Work Package (WP) 1 for ESR 2, which focuses on the communication system, and WP 4 for ESR 15, which focuses on case studies considering the application subsystem.
The main objective of ESR 2 for the laboratory access period is to assess the vulnerability of communications between the subsystems of a complex smart grid system to low-level radiated EMI signals.
The proposal reference number is 125, prepared by User Group (UG) leader ESR 2, Arash

Nateghi, from Defence Research Institute for Protection Technologies – ABC Protection (WIS) in collaboration with ESR15, Fernando Arduini from Fraunhofer Institute for Technological Trend Analysis (INT) both based in Germany.
The laboratory access provided by Research Director Knut Samdal from SINTEF Energi AS, part of the Norwegian National Smart Grid Laboratory (NSGL) in O.S. Bragstads Plass 2a, Gløshaugen, Trondheim, Norway. The EriGrid2 project support team members are Merkebu Zenebe Degefa, Santiago Sanchez Acevedo and Kjell Ljøkelsøy.
The start and end dates of ESRs participation are as follows: ESR2 from 04/19/2022 to 05/19/2022 and ESR15 from 06/09/2022 to 07/12/2022.

2 Methodology - Arash

Subsystems with different functions are available at the SINTEF Energy Research smart grid laboratory, e.g., Intelligent Electronic Devices (IEDs), Real Time Units (RTUs) and Measurement Units (MUs), which are crucial for sophisticated smart grid systems. The complex overall system structure used for this work is shown in Figure 2.1.

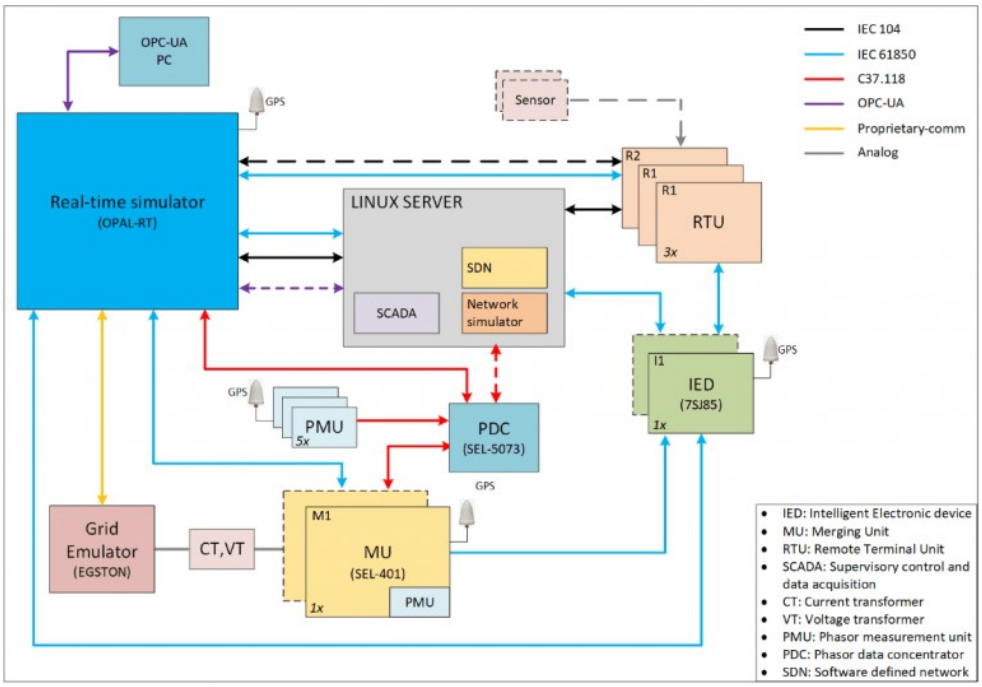


Figure 2.1: Smart-Grid complex communication system
(O'Toole, Moya, Rubin, Schnabel, & Wang, 2019).

As shown in Figure 2.1, smart grid system is a combination of four categories of physical hardware (IEDs, RTUs, MUs, and PMUs), real-time simulator (OPAL-RT), communication layers including protocols (IEC 104 and IEC 61850), and software components (HMI and SCADA systems). These four elements work together to provide visibility and operability for the SCADA (Supervisory Control and Data Acquisition) engineer. The communication structure of an infeed station consists of three levels of Process, Bay and Station levels as shown in Figure 2.2.

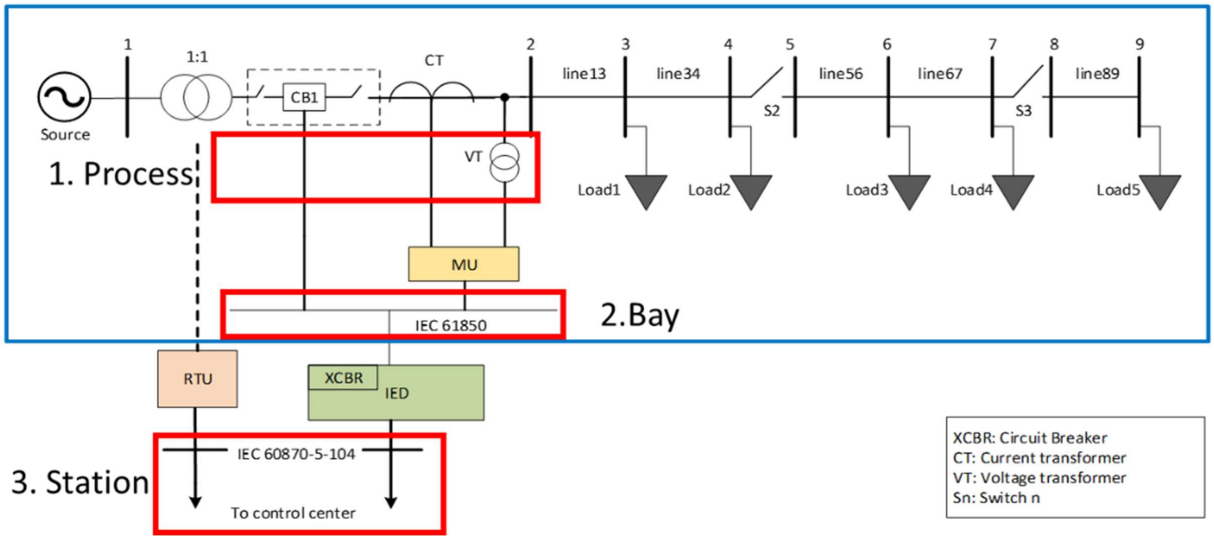


Figure 2.2: One-feeder substation with communication layers.

2.1 Test Plan

The process for assessing the vulnerability of the smart grid subsystems and the overall complex system to IEMI, shown in Figure 2.1, is to follow the standards for communication protocols such as IEC 104 and IEC 61850 and system setup. However, the nature of radiating IEMI signals, where the attacker does not follow any standard to avoid being detected by the system owners, goes beyond the ruled-based method and requires a risk-based approach for setting up the test plan, considering a different number of scenarios.
The steps to plan the measurement process were to take a device as a sub-system from the connected complex smart grid system, and physically position this device in a Faraday-Cage in one of the SINTEF's energy laboratories in collaboration with the Norwegian University of Science and Technology (NTNU).
The devices were positioned in the test environment by running two fibre optic cables from the smart grid lab to the Faraday-Cage without affecting the actual structure of the communication network.
Sweep period jamming (SPJ) signals (Nateghi, Schaarschmidt, Fisahn, & Garbe, 2021) with three different frequency ranges (100-200 MHz, 500 MHz-1 GHz and 1-3 GHz) were then radiated into the device under test (DUT). Next, the data transmission rate of the associated communication protocol, and the functionality of the DUT, as well as the causes of the radiated EMI signal to other devices were monitored.

2.2 Test Set-ups

Details on measurement setups for radiating the SPJ into complex smart grid subsystems given in Figure 2.2 are provided in the following subsections.

2.2.1 IED

IEDs are intelligent electronic devices used in smart grid communication systems and have built-in functions such as tap changer, flow sensor, temperature sensor, pressure sensor, Buchholz relay, pressure relief devices, automatic voltage regulator, trans-former cooling control and switching device control. For this work, the switching capability of the IED is used while the DUT is positioned in Faraday-Cage. The measurement setup for IEMI radiation in IED is shown in Figure 2.3.

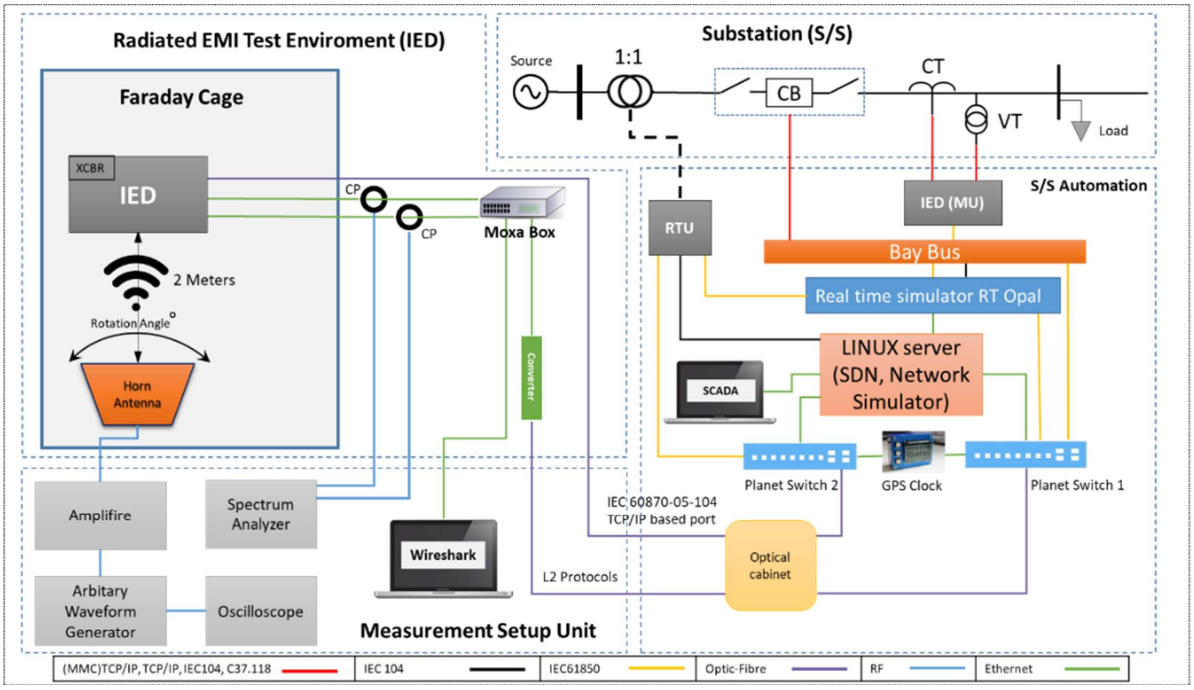


Figure 2.3: IED positioned in Faraday-Cage under IEMI test.

As can be seen from Figure 2.3, the two fibre-optic links from the substation automation environment in the smart grid lab connected to the radiated EMI test-bed where the Faraday Cage is located. The IED is connected to the Moxa box switch, which provides the connectivity and prepares the data collected from the IED via two connected Ethernet cables to be transmitted over via one of the fibre-optic links using appropriate protocol, IEC 60870-05-104. The second fibre-optic cable is connected directly to the IED, and the other head is connected to the second IED acting as a Measurement Unit (MU) via the appropriate switches for further coordination. The optical cabinet is used to maintain the speed of the data being transmitted from the IED in the Faraday-Cage over fibre-optic links, and each of the links is connected to the corresponding planet switch. The planet switches connect all devices including MUs, IEDs and RTUs to the server, network simulator, software defined network (SDN) and SCADA system, and the GPS clock connected to both switches synchronize all devices. After generating the SPJ signal by Matlab, an arbitrary wave generator is used in conjunction with an amplifier (with maximum of 250 W power gain for frequency range up to 1 GHz or 20 W power gain for frequencies above 1 GHz) and a horn antenna to radiate the jamming signal. The measurements are repeated 30 times for 20 seconds of duration for each criterion. The Current Probes (CPs) are used for monitoring the effect of coupled EMI into Ethernet wires connected to IED. The SCADA display provides a clear visibility of the operability of the IED, for example when switching on/off the circuit breaker of transformer 1, as shown in Figure 2.4.

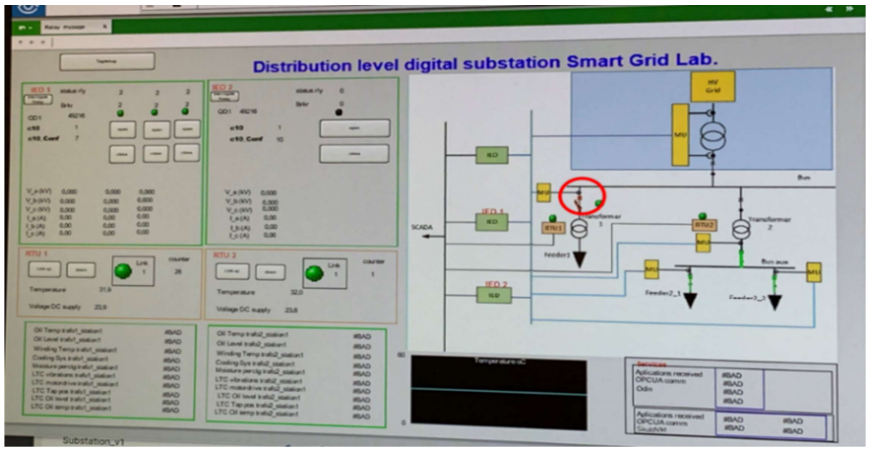


Figure 2.4: SCADA display for smart-grid lab.

2.2.2 MU

For IEMI's second experiment on a complex smart grid system, the measurement unit MU is positioned in the Faraday-Cage, as shown in Figure 2.5.

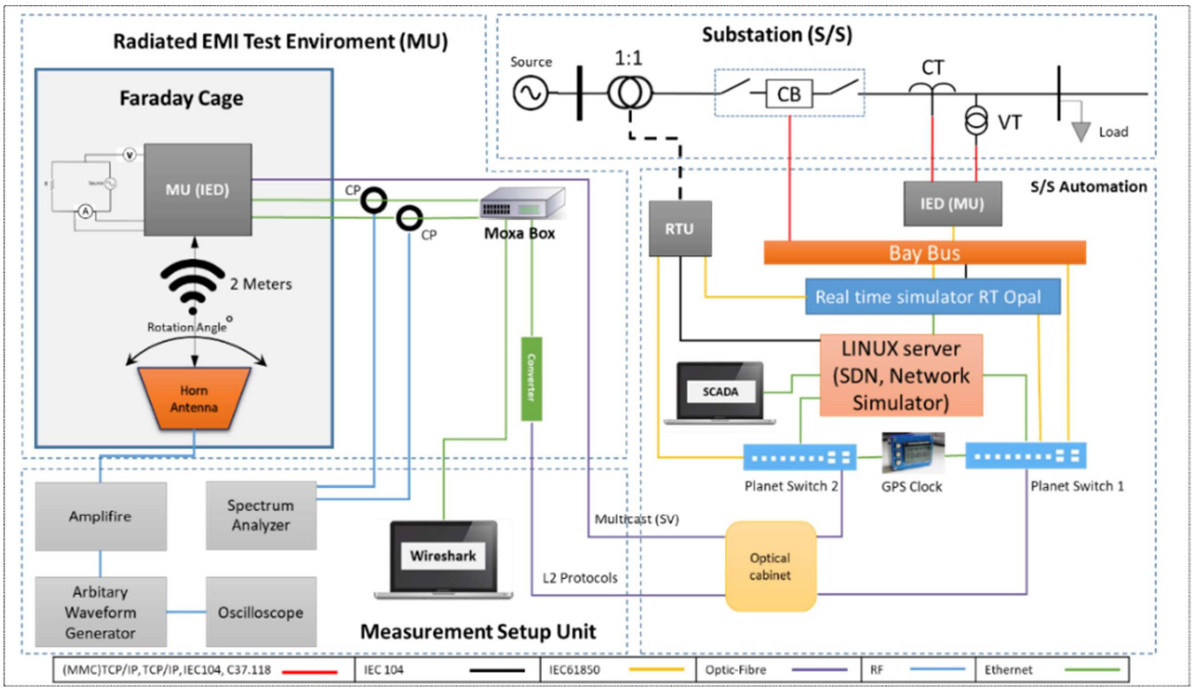


Figure 2.5: MU positioned in Faraday-Cage under IEMI test.

In Figure 2.5, the structure of the measurement setup is identical to the setup provided in previous Subsection, 2.2.1. For this experiment, the IED acts as MU and an auxiliary load is connected to the MU to measure and transmit the voltage and current readings to the other IED device. In addition to the communication protocols involved in this interconnected network structure, the sampled-values of IEC-81650 are an important value to be measured and evaluated before and after IEMI radiation.

2.2.3 RTU-1

Three different remote terminal units, RTUs, with different functionalities are chosen to be tested under IEMI attack in Faraday-Cage. The first RTU (RTU-1) deployed in this work is mainly used for multi-cast data transmission between different devices connected to the smart grid network system and it mainly transmits Goose messages. The measurement setup is shown in Figure 6. Only a single Ethernet cable is connected to the RTU-1 to transfer the appropriate da-ta using the associated protocol, as shown in Figure 6.

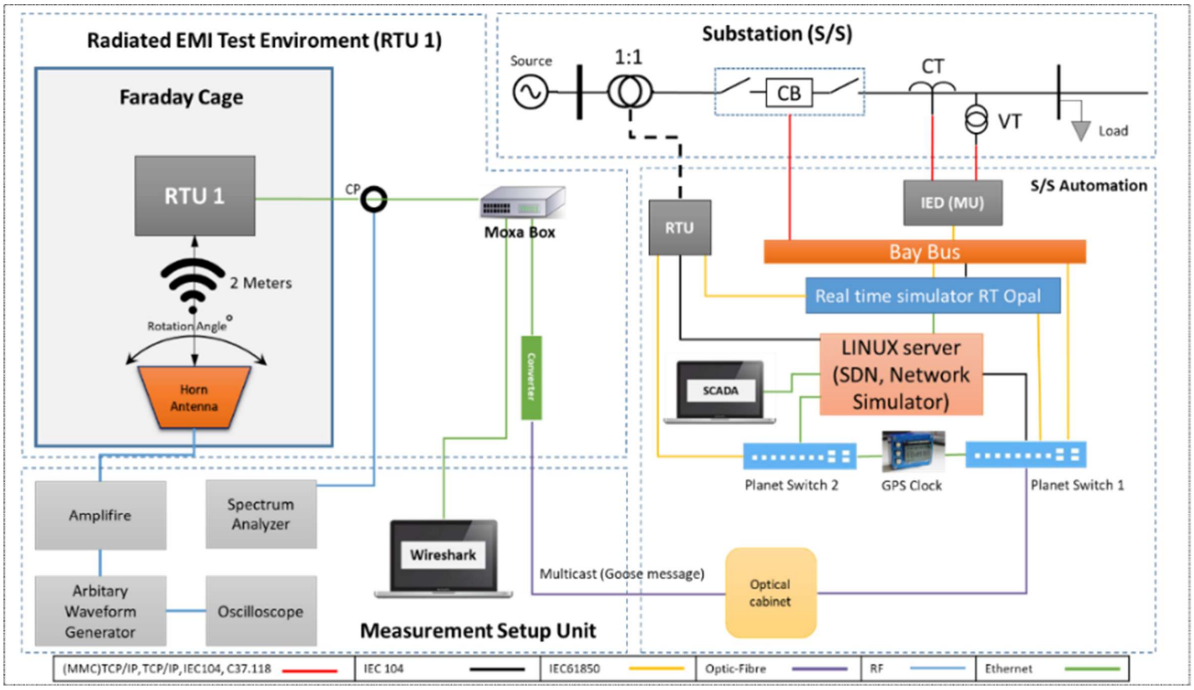


Figure 2.6: Measurement setup for RTU-1 positioned in Faraday-Cage.

2.2.4 RTU-2

The second RTU (RTU-2) is used to automate the smart grid system. This type of RTU is used to monitor and control geographically distributed substations that are not connected to a rest of the power supply network. The RTU-2 can store process data and transmit it to a control centre or master station via mobile radio or via the LAN network. The main protocol being studied is IEC 60870-5-14 when data for this experiment is transmitted over a single point connection to RTU-2 when IEMI is radiated, with the RTU-2 inside the Faraday-Cage as shown in Figure 7.

2.2.5 RTU-3

The third RTU deployed for this work is RTU-3, which provides automation for micro-grids with high performance and capable of many interfaces for complex tasks. For this experiment, RTU -3 is used as a communication gateway, which receives the da-ta from the IED and transmits the collected data to the SCADA system. RTU-3 sub-scribes to Goose messages from IED and uses IEC 104 protocol for sending the data to be used by human machine interface HMI and

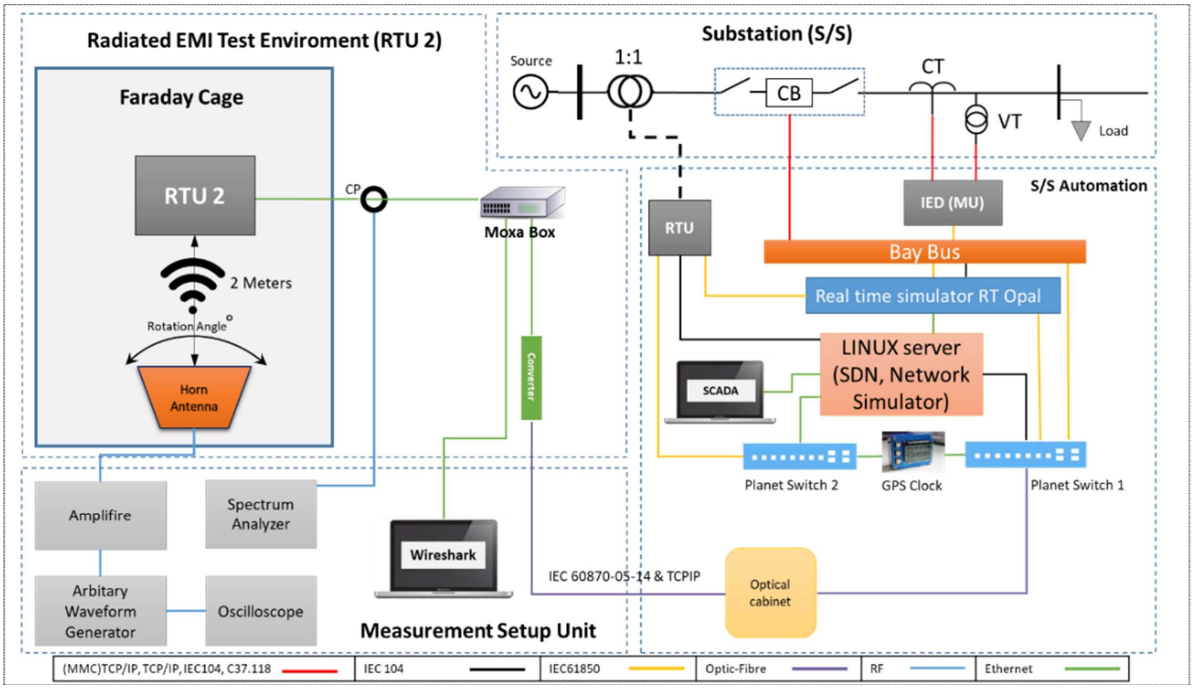


Figure 2.7: Measurement setup for RTU-2 positioned in Faraday-Cage.

a SCADA monitoring system. Figure 8 shows the layout of the measurement setup for RTU-3 in Faraday-Cage for IEMI radiation. In Figure 8, there are two Ethernet cable connections to RTU-3, which provides the functionality of a gateway to protect the data transmitted to critical parts of the system by enabling the embedded cyber-security application.

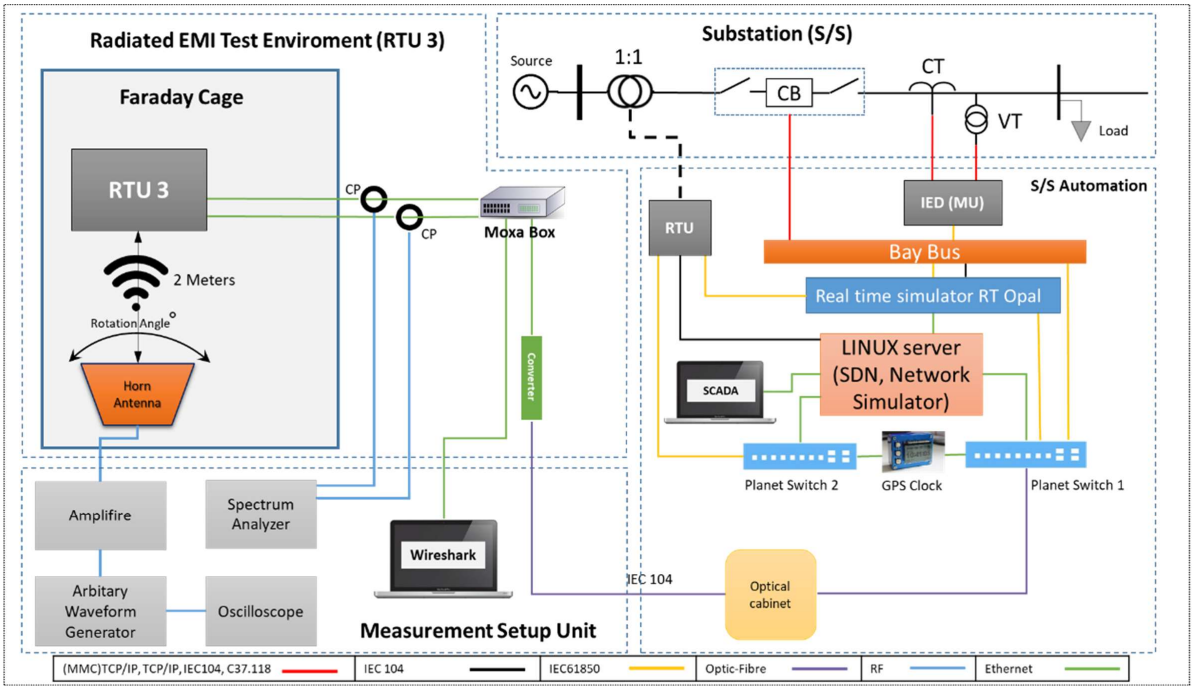


Figure 2.8: Measurement setup for RTU-3 positioned in Faraday-Cage.

2.3 Measurement data analysis

The susceptibility of the complex smart grid system considering the subsystems and the associated communication channels to radiated SPJ signals was assessed, and the methods of collecting and processing the required data are given in the following subsections.

2.3.1 Radiated SPJ into IED

For SPJ signal radiated into the IED positioned in the Faraday-Cage, the data-packet transmission-rate of IEC 60870-5-104 was monitored using Wireshark software considering different frequency intervals and power gain of IEMI. Table I illustrates the variables considered for this experiment.

Table 1.1: Frequency and power gain variables used for radiated IEMI into IED.

Frequency	Power Gain
100 to 200 MHz	0(%) of 250 W 35 (%) of 250 W
500 MHz to 1GHz	0(%) of 250 W 35 (%) of 250 W 55 (%) of 250 W
1 to 3 GHz	0(%) of 20 W 35 (%) of 20 W 55 (%) of 20 W 75 (%) of 20 W 100 (%) of 20 W

Due to the lack of a continuous incoming data packet transmission rate of the IED, the normal distribution of each scenario given in Table 1.1 is plotted using Python software and further explained below.

2.3.1.1 SPJ signal with frequency range of 100 - 200 MHz: From Figure 9 it can be seen that the 35 percent SPJ radiated into the IED reduces the probability of data transmission of the IEC 60870-5-104 protocol to around 0.15 with a mean value of 2.59 compared to 0 percent power gain with probability of around 0.85 at mean value of 3.5.

Due to the lack of access to a better designed antenna to propagate the SPJ within the 100 – 200 MHz frequency range, the power gain could not exceed 35 percent of 250 W.

2.3.1.2 SPJ signal with frequency range of 500 MHz - 1 GHz: As can be seen in Figure 10, the mean shifts to 3.8 when the power gain is 35 percent of 250 W compared to 0 percent and 55 percent power gain with mean values of 0.51 and 0.59, respectively. After increasing the power gain to 75 percent, the mean value is shifted to 4.1 and the standard deviation of the normal probability distribution has increased to 4.68 in compare with 1.3 in 0 and 55 percent power gain. After increasing the power gain to 75 percent, the mean value shifts to 4.1 and the standard deviation STD of the normal probability distribution has increased to 4.68, compared to 1.3 at 0 percent and 55 percent power gain.

Increasing the power gain of the radiated SPJ signal has caused the reduction in the probability of data packet transmission of the IEC 60870-5-104 protocol down to 0.09 when a power gain

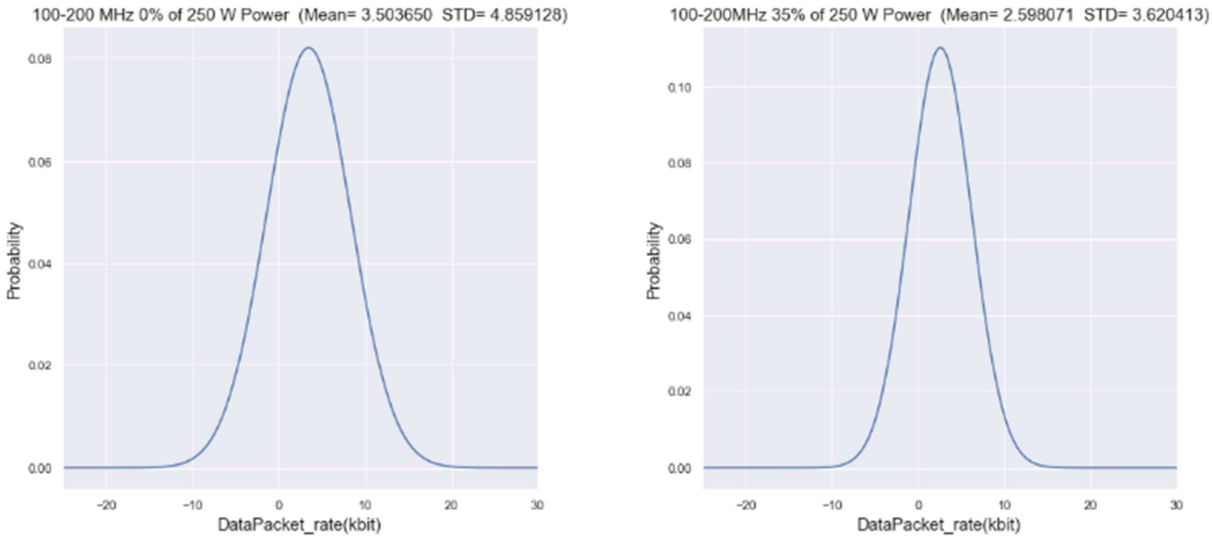


Figure 2.9: SPJ signal with frequency range of 100-200 MHz radiated into IED.

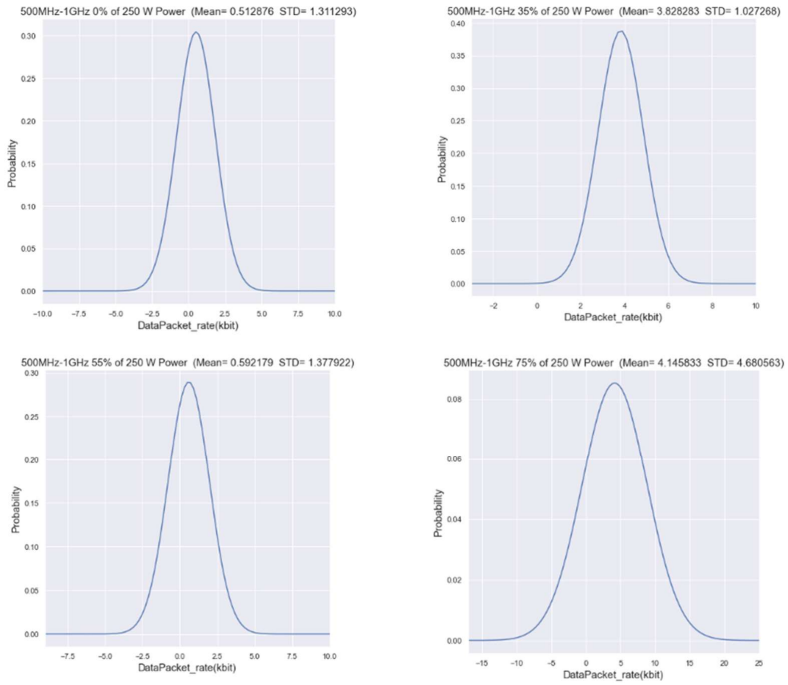


Figure 2.10: SPJ signal with frequency range of 500 MHz -1 GHz radiated into IED.

of 75 percent is applied. Upon visual inspection, the transformer circuit breaker, shown in Figure 11 below, opens and closes during EMI emissions in the 500MHz to 1GHz frequency range.

2.3.1.3 SPJ signal with frequency range of 1 - 3 GHz: As can be seen from Figure 12, by increasing the power gain of the SPJ signal with a frequency range of 1 - 3 GHz, the probability of data packet transmission of the IED using the IEC 60870 5 104 protocol has not changed significantly, the mean value is almost the same for all five scenarios.

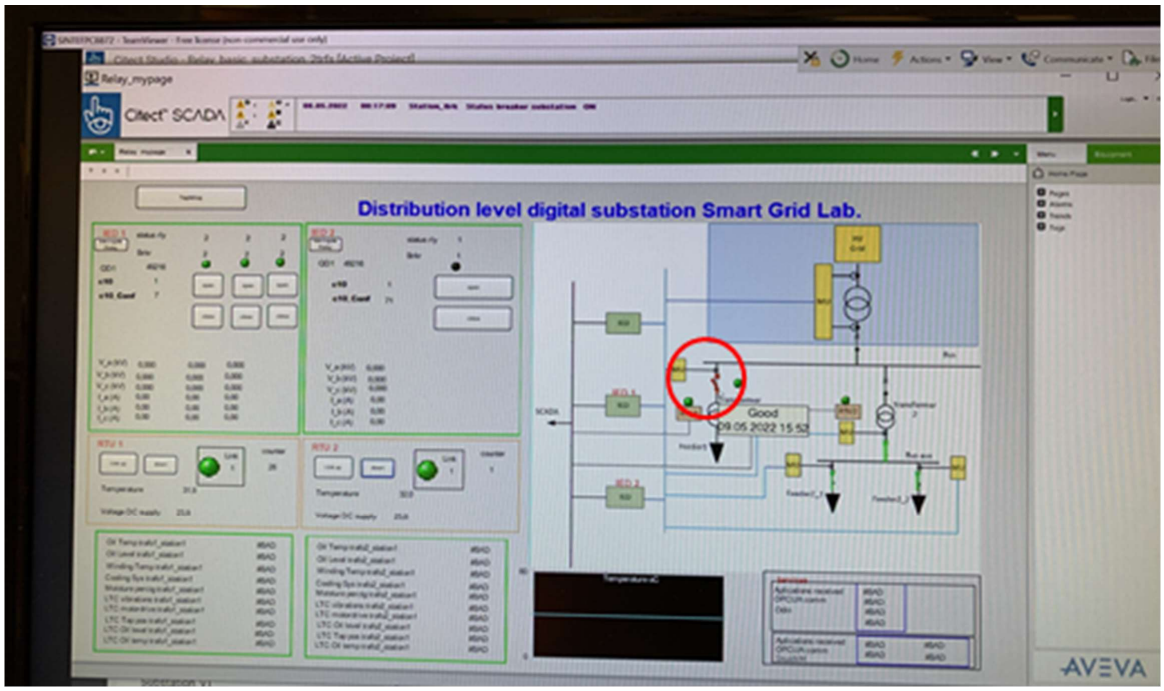


Figure 2.11: Transformer circuit breaker opens and closes during SPJ radiation.

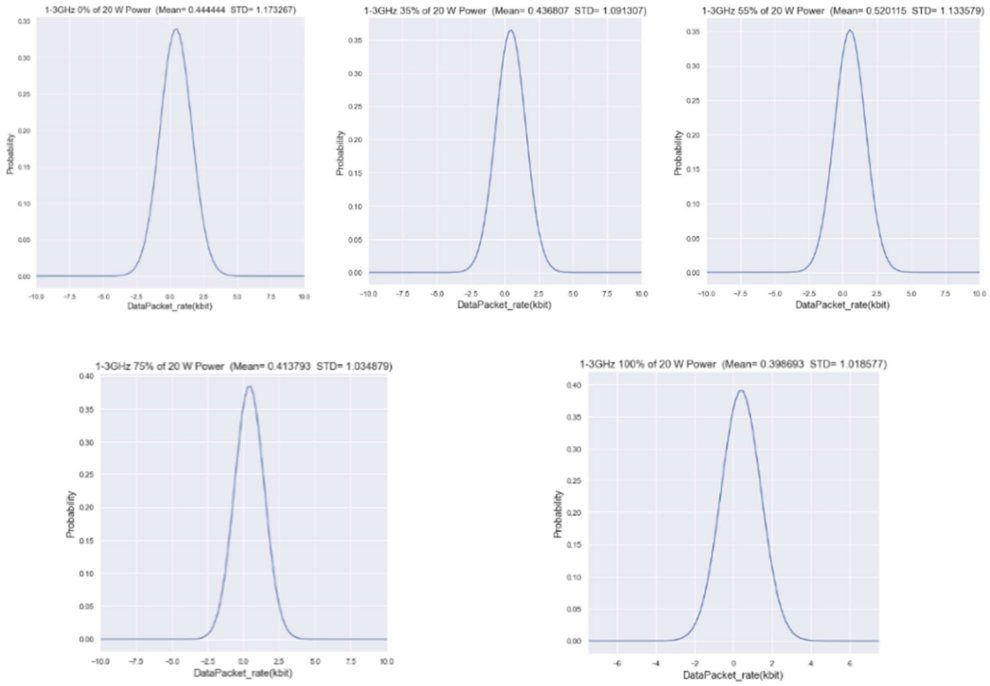


Figure 2.12: SPJ signal with frequency range of 1 - 3 GHz radiated into IED.

From all the different scenarios in Table I, the SPJ with a frequency range of 500MHz - 1GHz and a power gain of 75 percent of 250W can reduce the probability of the IED's data packet transmission the most. The SPJ signal with a frequency range between 100 - 200 MHz has more disruptive effects on the transmission of IED data packets compared to SPJ with 1 to 3 GHz because it targets the frequency range of the subsystems used in this experiment.

2.3.2 Radiated SPJ into MU

The MU positioned in Faraday-Cages, measures the voltage and current of the load using the integrated Voltage Transformer VT and Current Transformer CT. The SPJ signals given in Table II with different frequency and power gains are radiated into the DUT and Wireshark is used to monitor the data packet transmission rate of the IEC 61850 Sampled-Values transmitted to the other MU installed, as part of the complex smart grid system. The voltage and current readings transmitted from the MU under test and the second MU must match, and a fibre-optic connection is used to facilitate fast and accurate data transmission between two MUs. The Gaussian distribution of each scenario given in Table II is plotted using Python software and further explained below.

Table 1.2: Frequency and power gain variables used for radiated IEMI into MU.

Frequency	Power Gain
100 to 200 MHz	0(%) of 250 W 15 (%) of 250 W 25 (%) of 250 W 35 (%) of 250 W
500 MHz to 1GHz	0(%) of 250 W 35 (%) of 250 W 55 (%) of 250 W 75 (%) of 250 W
1 to 3 GHz	0(%) of 20 W 35 (%) of 20 W 55 (%) of 20 W 75 (%) of 20 W 100 (%) of 20 W

2.3.2.1 SPJ signal with frequency range of 100 - 200 MHz: As can be seen from Figure 13, the probability of the data packet transmission rate for the IEC 61850 Sampled-Values for all scenarios defined in Table II for the frequency range of 100 200 MHz is almost the same. The main reasons that the SPJ signal does not affect the MU data transmission rate is the use of a fiber-optic link used for data transmission and also the low efficiency of the antenna used for the 10 - 200MHz frequency range.

2.3.2.2 SPJ signal with frequency range of 500 MHz - 1 GHz: Figure 14 shows that although the fiber-optic link protects the data transmission of the IEC 61850 sample values, the 75 percent power amplification of the radiated SPJ signal has reduced the probability density PD of the transmitted data. The PD is about 0.0004 with a mean of 3875 compared to the other power gains with a PD of 0.0007 and a mean of about 3880 for the frequency range of 500MHz to 1GHz given in Table II.

In addition to monitoring the data transmission rate with Wireshark, the visual inspection of the DUT and SCADA system on the HMI was demonstrated. During radiation of SPJ with a frequency range of 500 MHz to 1 GHz only a voltage measurement was applied by VT, but some current induced in the system was recorded by the second MU when 35, 55 and 75 percent power gain of SPJ was applied as shown in Figure 15 below.

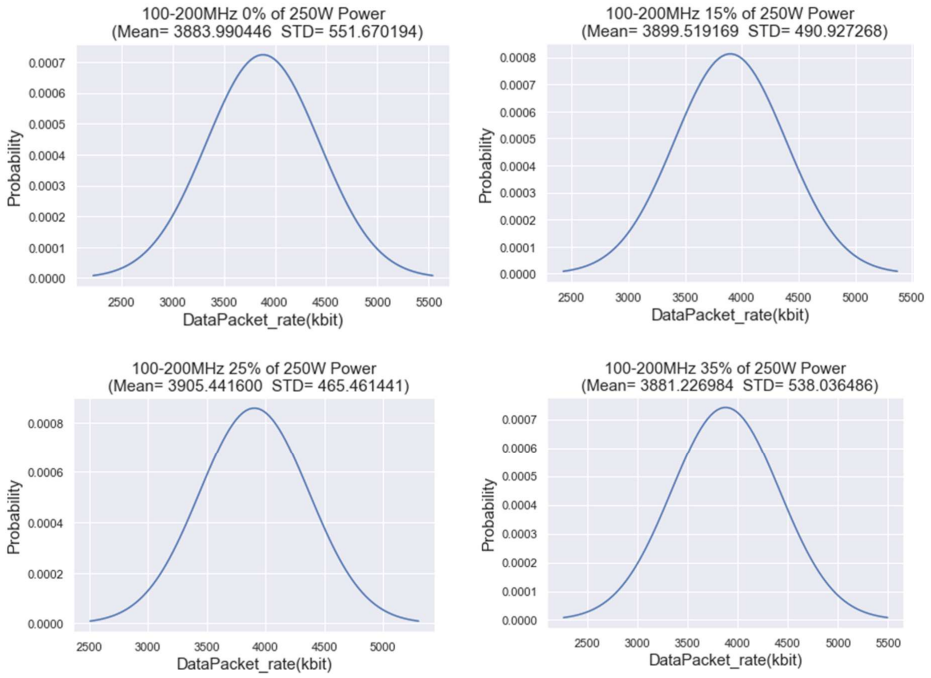


Figure 2.13: SPJ signal with frequency range of 100-200 MHz radiated into MU.

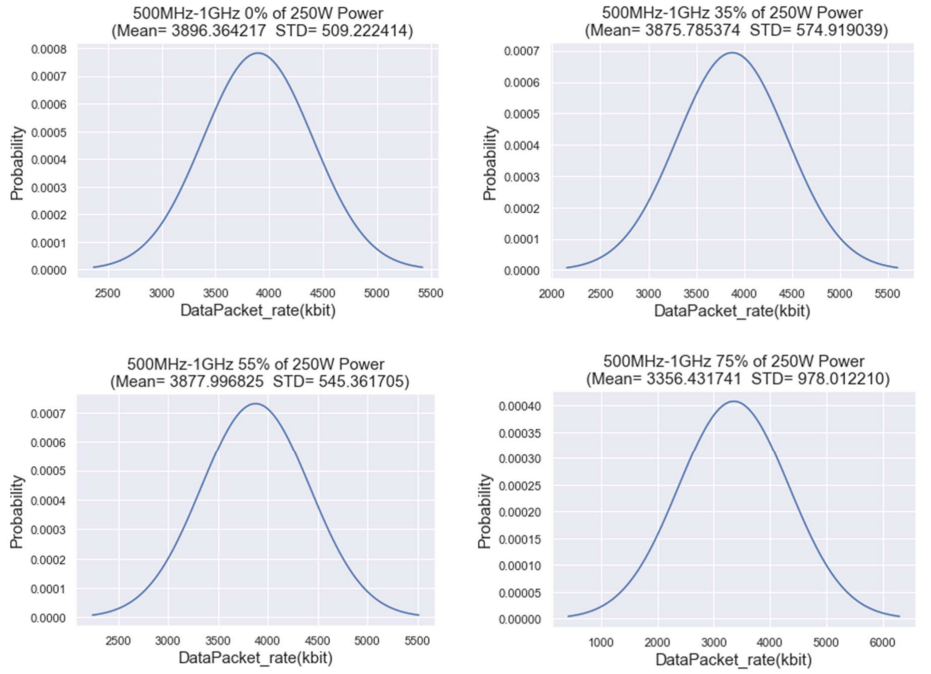


Figure 2.14: SPJ signal with frequency range of 500 MHz -1 GHz radiated into MU.

2.3.2.3 SPJ signal with frequency range of 1 - 3 GHz: The SPJ signal with a frequency range of 1 - 3 GHz has a minor impact on the data transmission of the IEC 61850 samples, as can be seen from Figure 16.

From visual inspection, when SPJ was applied with a frequency range of 1 - 3 GHz, the radiated current was induced in the MU, like SPJ with a frequency range of 500 MHz to 1 GHz. Although the VTs only measure the voltage of phases A and B, phase C also shows some induced voltage as can be seen in Figure 17.

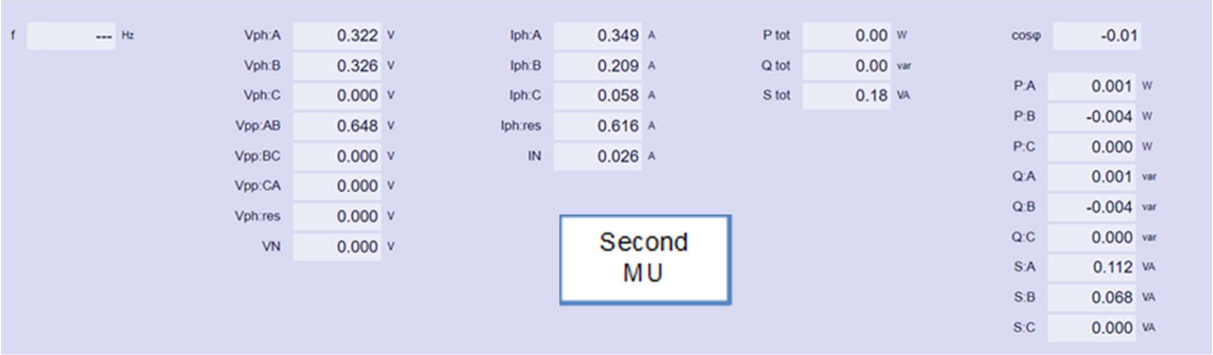


Figure 2.15: Current induced into the MU under test and recorded by second MU.

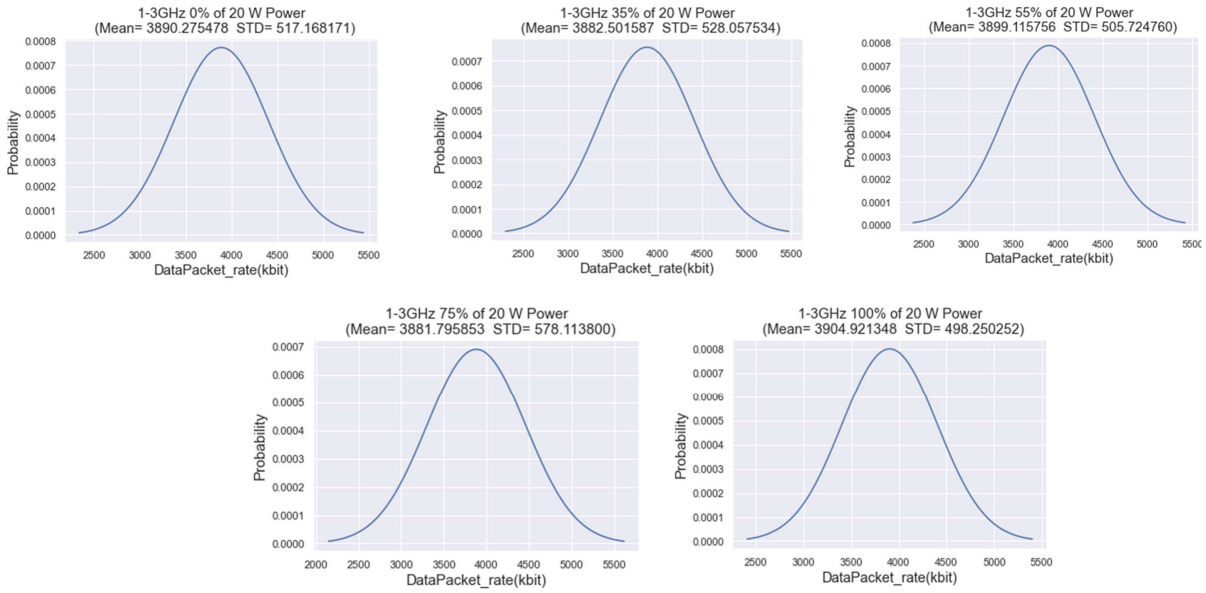


Figure 2.16: SPJ signal with frequency range of 1-3 GHz radiated into MU.

2.3.3 Radiated SPJ into RTU-1

The SPJ signals given in Table IIII with different frequency ranges and power gains are radiated into the RTU-1, which is positioned in a Faraday-Cage. The RTU-1 communicates with various devices as part of a complex smart grid system and only uses Goose messages to transfer the data. The packet rate behaviour of RTU-1's Goose messages is monitored with Wireshark

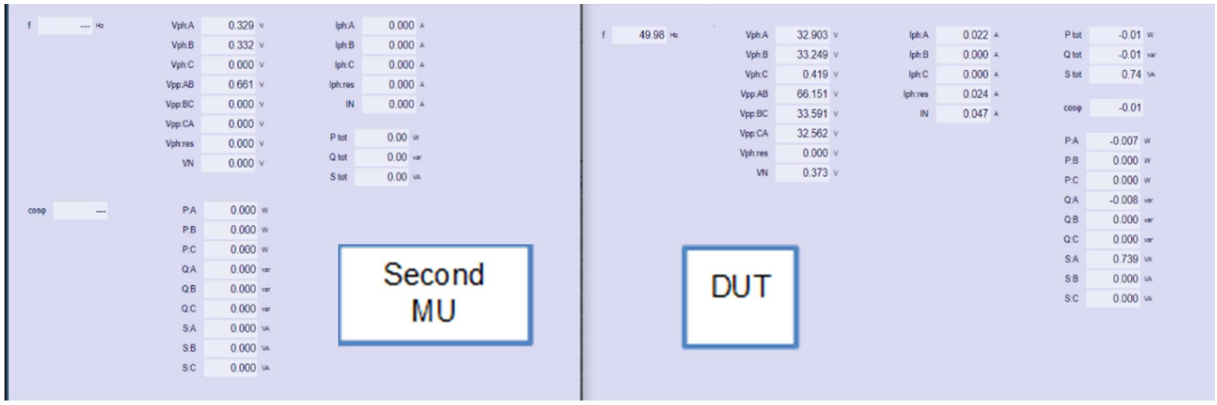


Figure 2.17: Voltage induced into DUT during SPJ radiation.

when radiating EMI signals in Table III, as explained below.

Table 1.3: SPJ signals with different frequency ranges and power gains radiated into RTU-1.

Frequency	Power Gain
100 to 200 MHz	0(%) of 250 W 15 (%) of 250 W 23 (%) of 250 W
500 MHz to 1GHz	0(%) of 250 W 15 (%) of 250 W 25 (%) of 250 W
1 to 3 GHz	0(%) of 20 W 35 (%) of 20 W 55 (%) of 20 W 75 (%) of 20 W 100 (%) of 20 W

The normal distribution of each scenario given in Table III is plotted using Python software and further explained below.

2.3.3.1 SPJ signal with frequency range of 100 - 200 MHz: Figure 18 shows that increasing the power gain of the SPJ signal from 0 to 23 percent reduces the PD density of the data packet transfer rate of the Goose messages of RTU-1 to about 0.12, compared to 0 percent power gain for a PD density of about 0.18.

In addition, the 23 percent of SPJ signal power gain is the limit where higher power gain causes the device to go into sleep mode for 20 minutes.

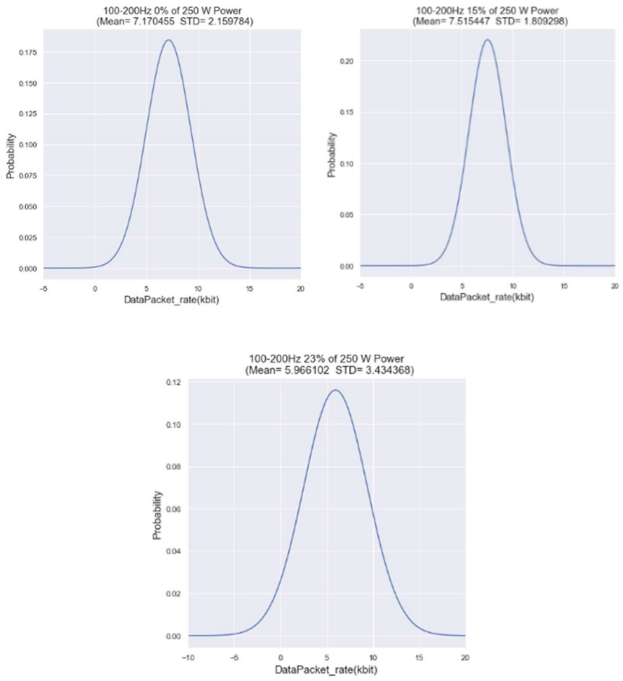


Figure 2.18: SPJ signal with frequency range of 100-200 MHz radiated into RTU-1.

2.3.3.2 SPJ signal with frequency range of 500 MHz - 1 GHz: From Figure 19 it can be seen that by radiating an SPJ signal with a frequency range of 500MHz to 1GHz, the mean value of the data packet transmission rate is reduced to about 0.54 with an STD of 0.49 when a 25 percent gain is applied, compared to a gain of 0 and 15 percent where the mean is about 7.5 and STD is about 2.1. Above 35 percent SPJ signal power gain will result in device shutdown and no Goose messages data packet is transmitted.

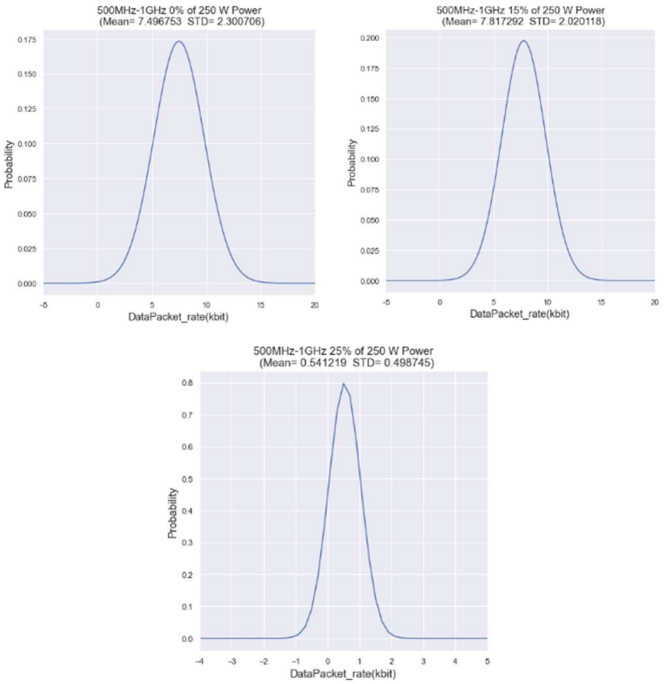


Figure 2.19: SPJ signal with frequency range of 500 MHz to 1 GHz radiated into RTU-1.

2.3.3.3 SPJ signal with frequency range of 1 - 3 GHz: The measurement results of the SPJ signal with a frequency range of 1 - 3 GHz radi-ated into the RTU-1 show that the DUT with the specified frequency range and power gains of 0, 35, 55, 75 and 100 percent of 20 W as shown in Figure 20.

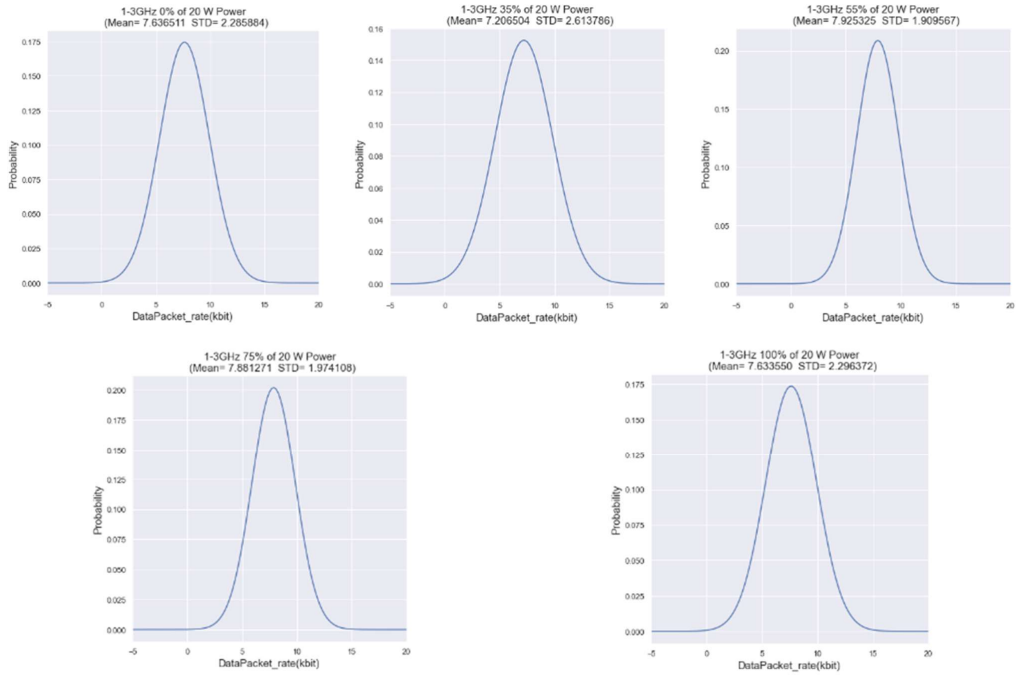


Figure 2.20: SPJ signal with frequency range of 1-3 GHz radiated into RTU-1.

2.3.4 Radiated SPJ into RTU-2

The second RTU (RTU-2) from different manufacturer of RTU-1 with different functionalities was placed in a Faraday-Cage and SPJ signals with different frequency ranges and power gains given in Table VI were radiated into the DUT. The data-packet transmission-rate of the IEC 60870-5-104 protocol is recorded using Wireshark software. The normal distribution of the associated protocol data packet transmission rate of each scenario given in Table VI is plotted using Python software, further explained below.

2.3.4.1 SPJ signal with frequency range of 100 - 200 MHz: From Figure 21, the radiated SPJ signal with a frequency range of 100 - 200 MHz and with different power gain amplitudes of 0, 15, 25 and 35 percent, the data transmission rate of the IEC 60870-5-104 protocol of RTU-2 is not affected significantly.

2.3.4.2 SPJ signal with frequency range of 500 MHz - 1 GHz: Due to a better antenna efficiency for radiating the SPJ signal within frequency range of 500 MHz - 1 GHz, the IEC 60870-5-104 mean and STD values of the data transfer rate of RTU 2 has droped for 55 percent to 0.38 and 1.57 respectively as it show below in Figure 22.

The 55 percent of SPJ is the point at which the data transfer rate of the IEC 60870-5-104 drops to zero above this limit.

Table 1.4: SPJ signals with different frequency ranges and power gains radiated into RTU-2.

Frequency	Power Gain
100 to 200 MHz	0(%) of 250 W 15 (%) of 250 W 25 (%) of 250 W 35 (%) of 250 W
500 MHz to 1GHz	0(%) of 250 W 35 (%) of 250 W 55 (%) of 250 W
1 to 3 GHz	0(%) of 20 W 35 (%) of 20 W 55 (%) of 20 W 75 (%) of 20 W 100 (%) of 20 W

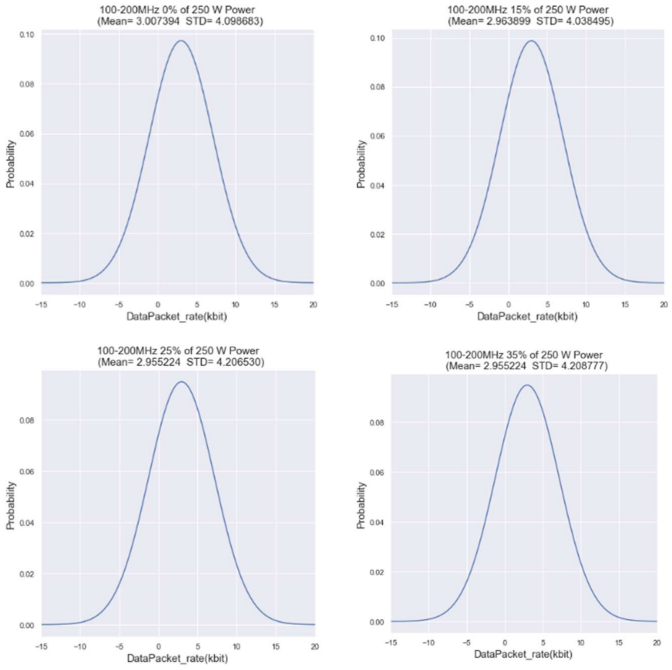


Figure 2.21: SPJ signal with frequency range of 100-200 MHz radiated into RTU-2.

2.3.4.3 SPJ signal with frequency range of 1 - 3 GHz: It can be seen from Figure 23 that the PD density of the data packet transmission rate of the IEC 60870-5-104 protocol was not affected enormously during the SPJ signal radiation with a frequency range of 1 to 3 GHz.

2.3.5 Radiated SPJ into RTU-3

The third RTU (RTU-3) is a multicasting device, which uses three different type of da-ta communication protocols of Goose messages, IEC 60870-5-104 and Internet.

The SPJ signals of different frequency ranges and power gains from Table V are radi-ated into RTU-3 positioned in Faraday-Cage and the data transmission behaviour of all three protocols are recorded for further analysis. The normal distribution of the associated protocols data

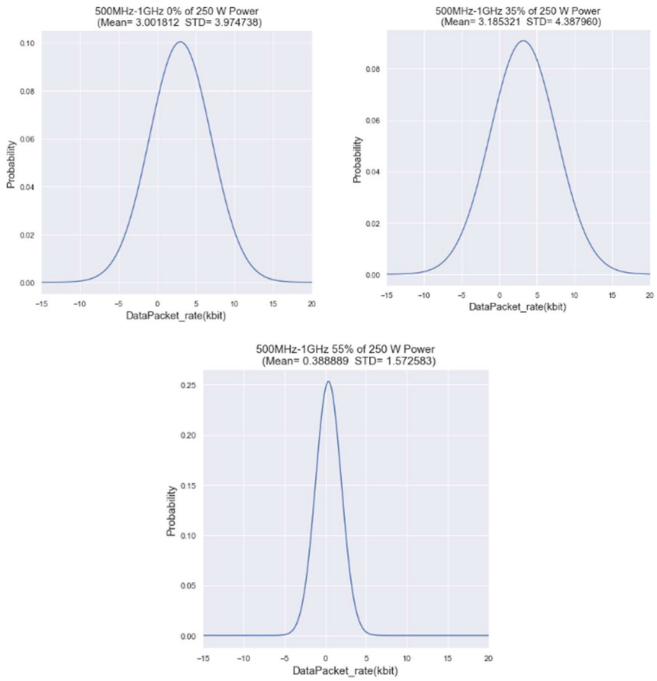


Figure 2.22: SPJ signal with frequency range of 500 MHz to 1 GHz radiated into RTU-2.

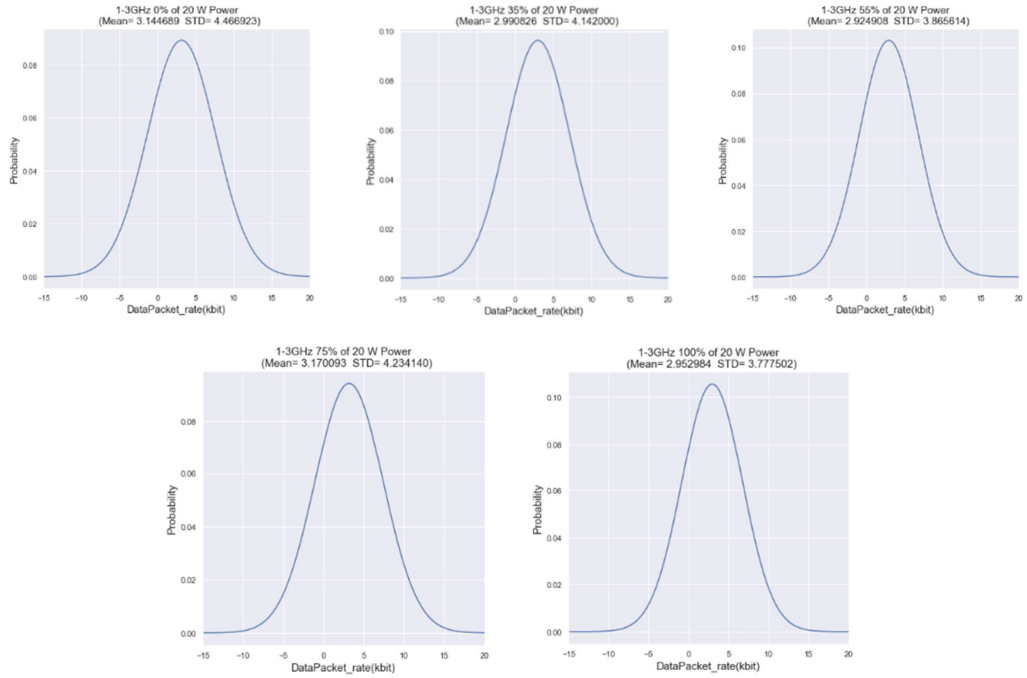


Figure 2.23: SPJ signal with frequency range of 1-3 GHz radiated into RTU-2.

packet transmission rate of each scenario given in Table V is plotted using Python software, further explained below.

2.3.5.1 SPJ signal with frequency range of 100 - 200 MHz for Goose messages: From Figure 24 the data transmission rate of Goose messages from RTU 3 is not sig-nificantly af-fected when a SPJ signal with a frequency range of 100 to 200 MHz is ra-diated into the DUT positioned in the Faraday-Cage.

Table 1.5: SPJ signals with different frequency ranges and power gains radiated into RTU-3.

Frequency	Power Gain
100 to 200 MHz	0(%) of 250 W 15 (%) of 250 W 25 (%) of 250 W 35 (%) of 250 W
500 MHz to 1GHz	0(%) of 250 W 35 (%) of 250 W 55 (%) of 250 W 75 (%) of 250 W
1 to 3 GHz	0(%) of 20 W 35 (%) of 20 W 55 (%) of 20 W 75 (%) of 20 W 100 (%) of 20 W

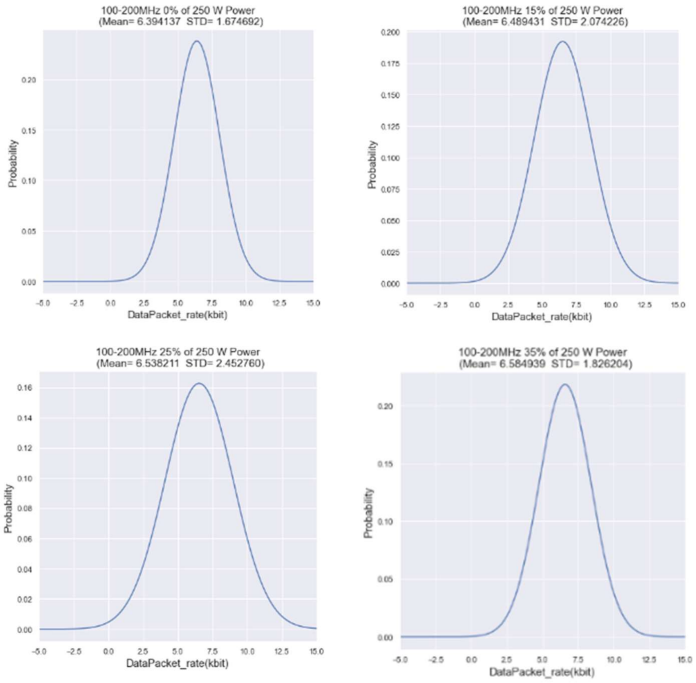


Figure 2.24: SPJ signal with frequency range of 100-200 MHz radiated into RTU-3.

2.3.5.2 SPJ signal with frequency range of 500 MHz - 1 GHz for Goose messages: From Figure 25 the data transmission rate of Goose messages from RTU-3 is not sig-nificantly af-fected when a SPJ signal with a frequency range of 500 MHz to 1 GHz is radiated into the DUT positioned in the Faraday-Cage.

2.3.5.3 SPJ signal with frequency range of 1 - 3 GHz for Goose messages: From Figure 26, apart from SPJ signal with 100 percent power gain, the rest of the scenarios defined for a frequency range of 1 to 3 GHz have a similar behaviour of the PD data transmission rate of the Goose messages. For this scenario, the mean and STD are shifted to around 9 and 4 respectively compared to the rest of the SPJ signal with mean and STD of 6.4 and 2.1 values. However, in this case there is no significant distortion of the data-packet transmission-rate of

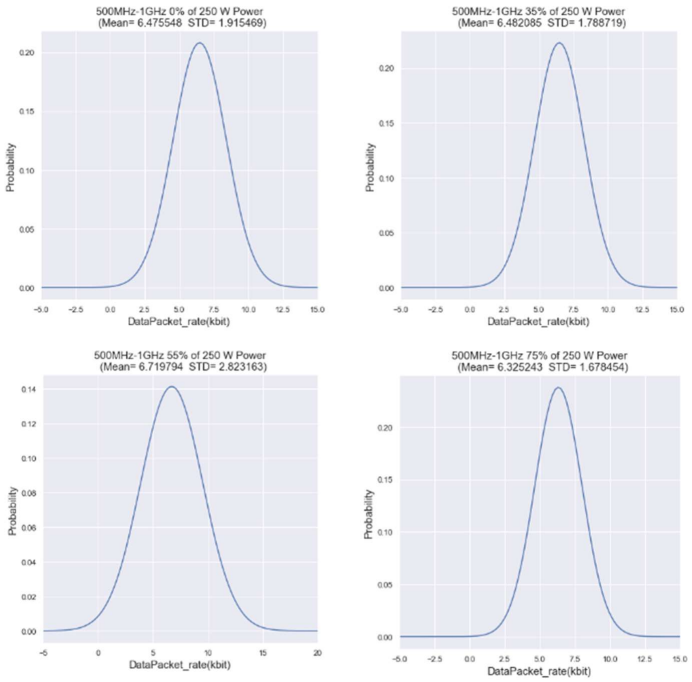


Figure 2.25: SPJ signal with frequency range of 500 MHz-1GHz radiated into RTU-3.

the Goose messages.

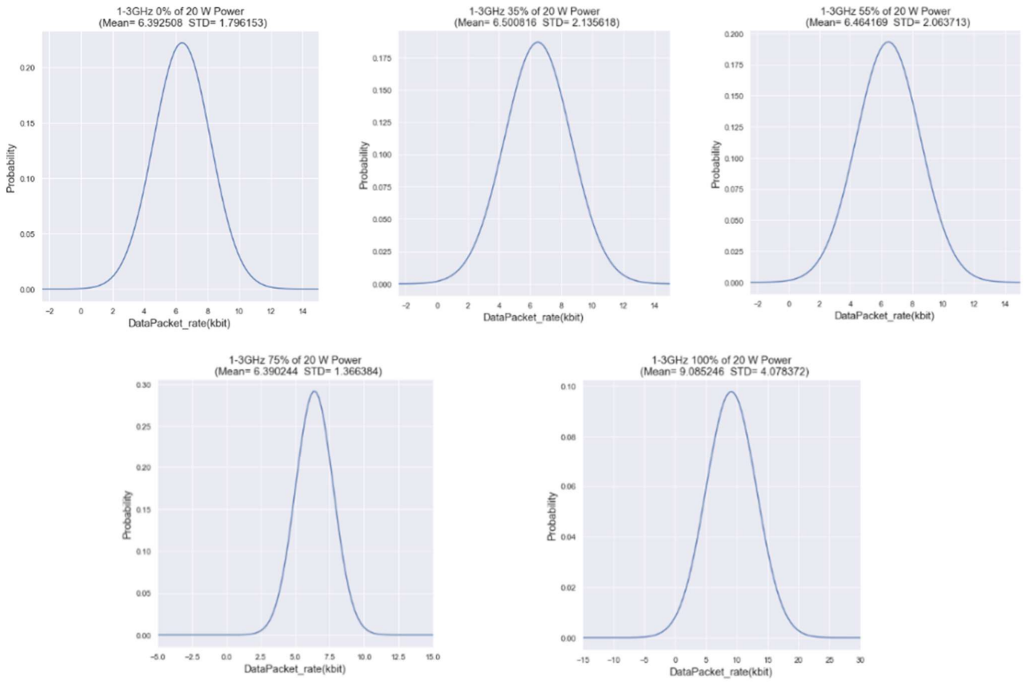


Figure 2.26: SPJ signal with frequency range of 1-3 GHz radiated into RTU-3.

2.3.5.4 SPJ signal with frequency range of 100 - 200 MHz for IEC 104: From Figure 27 the data transmission rate of IEC 60870-5-104 protocol of RTU-3 is not significantly affected when a SPJ signal with a frequency range of 100 to 200 MHz is radiated into the DUT positioned in the Faraday-Cage.

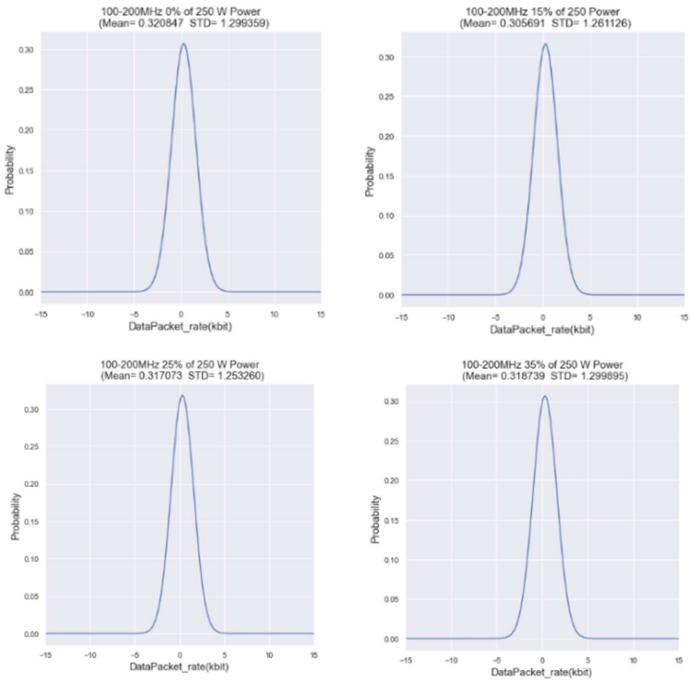


Figure 2.27: SPJ signal with frequency range of 100-200 MHz radiated into RTU-3.

2.3.5.5 SPJ signal with frequency range of 500 MHz - 1 GHz for IEC 104: It can be seen from Figure 28 that the data transmission rate of the RTU-3 with IEC 60870 5 104 protocol is not significantly affected when a SPJ signal with a frequency range of 500 MHz to 1 GHz and less than 75 percent power gain is radiated into the DUT positioned in the Faraday-Cage. The SPJ signal at 75 percent reduces the mean and STD values to approximately zero, which in this case means no data transmission for this protocol.

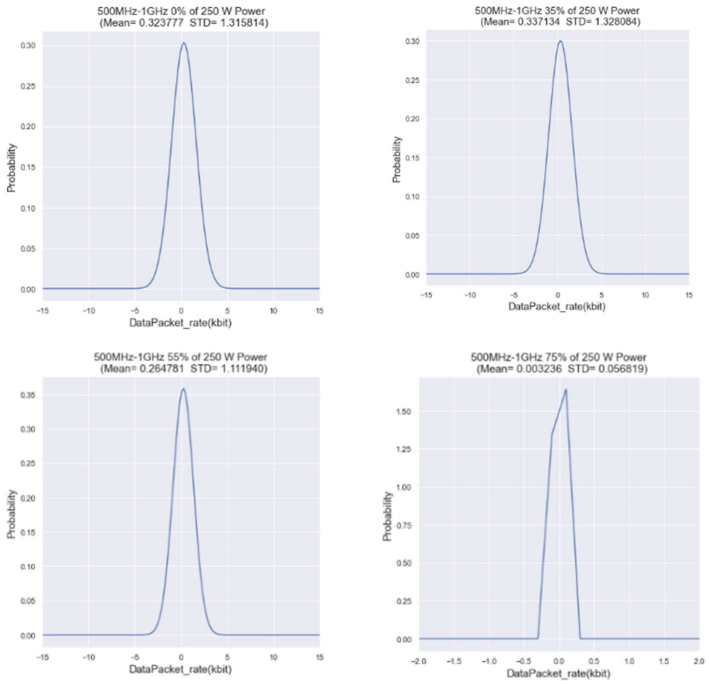


Figure 2.28: SPJ signal with frequency range of 500 MHz-1GHz radiated into RTU-3.

2.3.5.6 SPJ signal with frequency range of 1 - 3 GHz for IEC 104: From Figure 29 the data transmission rate of IEC 60870-5-104 protocol of RTU-3 is not affected when a SPJ signal with a frequency range of 1 to 3 GHz is radiated into the DUT positioned in the Faraday-Cage.

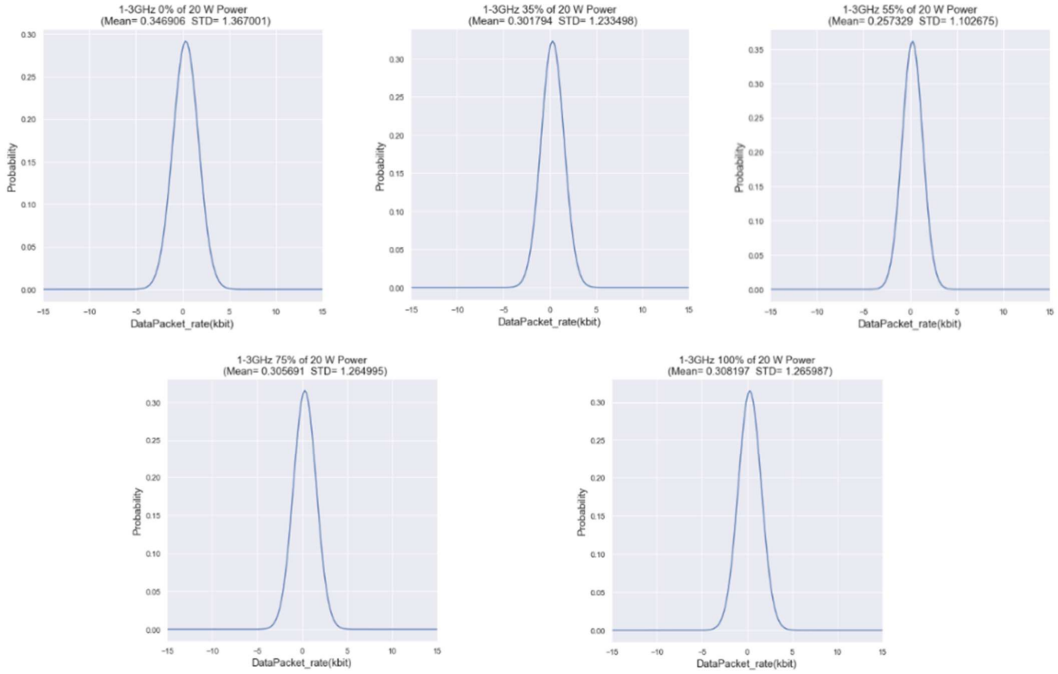


Figure 2.29: SPJ signal with frequency range of 1-3 GHz radiated into RTU-3.

2.3.5.7 SPJ signal with frequency range of 100 - 200 MHz for Internet: From Figure 30, radiation of the SPJ signal with 35 percent power gain into RTU-3 po-sitioned in Faraday-Cage reduces the mean value to approximately 0.79 for the Inter-net protocol.

The data -packet transfer-rate reduction of Internet protocol causes the disconnection of the DUT with Internet platform for visualising the behaviour of the device with relat-ed HMI.

2.3.5.8 SPJ signal with frequency range of 500 MHz - 1 GHz for Internet: As can be seen from Figure 31, the data transmission rate of the Internet protocol is significantly influenced by the SPJ signal radiated into the RTU-3 with 55 and 75 per-cent power amplification. The SPJ signals at 55 and 75 percent reduce the mean and STD values to approximately zero, which in this case means no data transmission for this protocol. From the visual inspection, the HMI of the RTU-3 is disconnected when 55 and 75 percent SPJ is applied.

2.3.5.9 SPJ signal with frequency range of 1 - 3 GHz for Internet: From Figure 32, apart from SPJ signal with 100 percent power gain, the rest of the scenarios defined for a frequency range of 1 to 3 GHz have a similar behaviour of the PD data transmission rate of the Internet protocol. For this scenario, the mean and STD are shifted to around 5.2 and 5.2 respectively compared to the rest of the SPJ signal with mean and STD of 3.6 and 3.2 values. However, in this case there is no significant distortion of the data-packet transmission-rate of the Internet protocol.

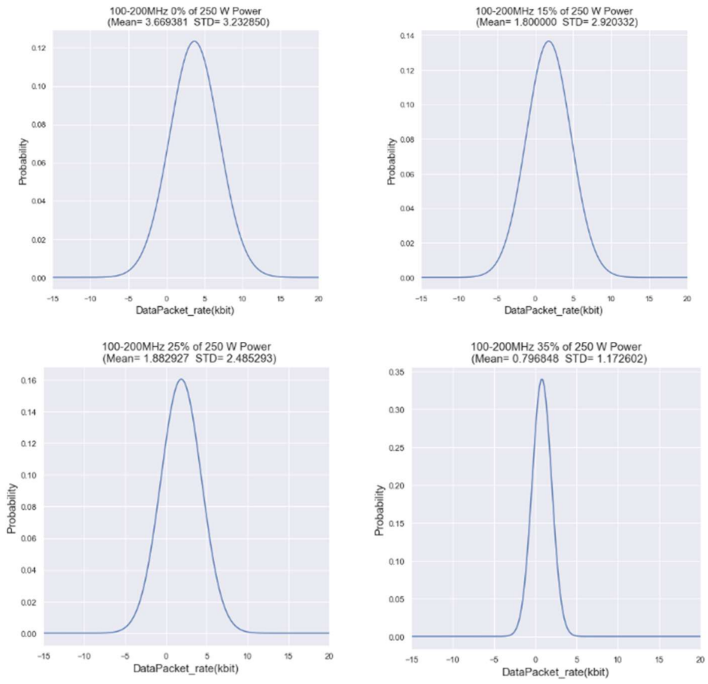


Figure 2.30: SPJ signal with frequency range of 100-200 MHz radiated into RTU 3.

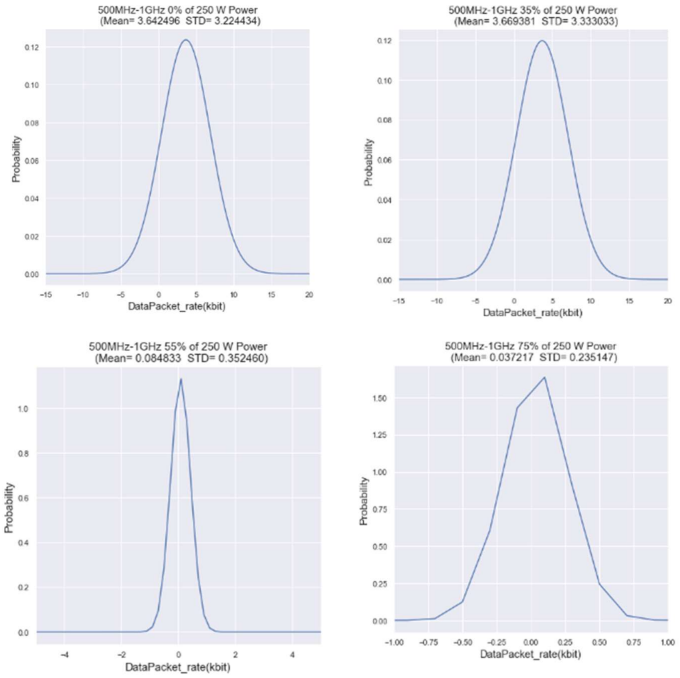


Figure 2.31: SPJ signal with frequency range of 500 MHz-1GHz radiated into RTU-3.

3 Discussion of Results by Aarsh

From the measurement results and after the data management carried out by ESR2 regarding the vulnerability assessment of the subsystems of the smart grid and the complex overall system, Table. 6 contains a summary of the results. Table. 6 compares the effects of IEMI radiation on the probability of data transmission rate for different DUTs with different frequency ranges and power gains. In addition, the behaviour of the subsystem and the overall system

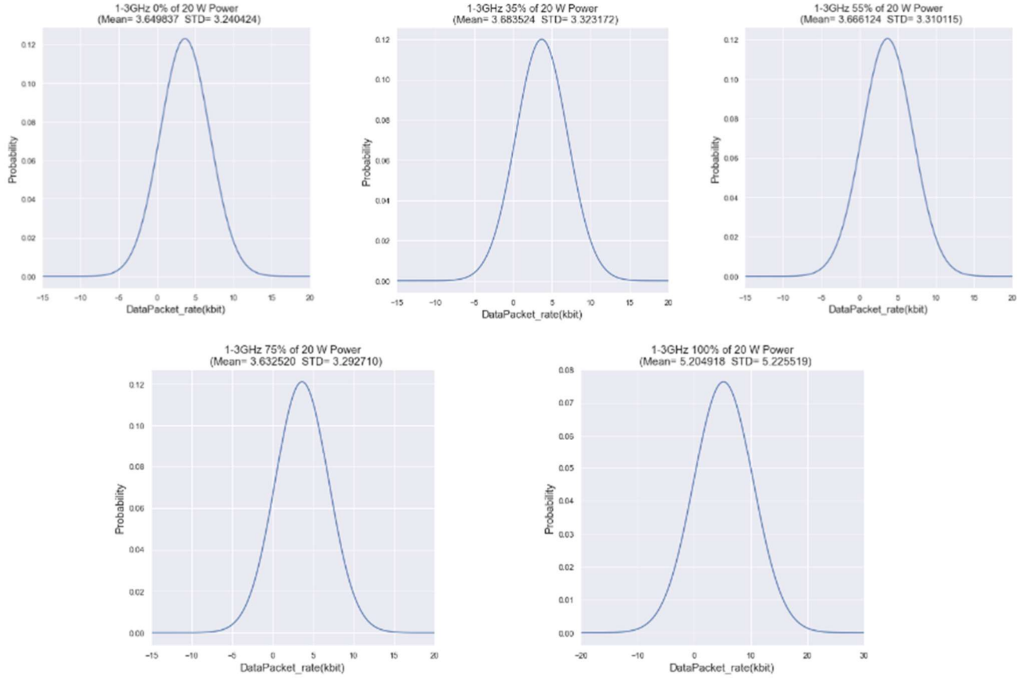


Figure 2.32: SPJ signal with frequency range of 1-3 GHz radiated into RTU-3.

are visually inspected and included in the summary. In the rightmost column, the severity of the disturbances on the DUT and the complex overall system is given according to the system setup described in section 3.

Table 6 shows that the severity of different subsystems of the complex smart grid system is not the same for the radiated IEMI with three different frequency ranges. It is also evident from visual inspection that IEMI radiation on one subsystem can cause failures for the other subsystems and the entire complex system.

4 Conclusion - Arash

To summarise, the use of smart grid communication devices such as radio modules, sensors, routers, and gateways that communicate via various communication channels and protocols over the Internet of Things IoT is rapidly increasing in decentralized energy management systems. In addition to environmental EMI, little expertise is required to design and build the source of intentional EMI disrupting communications links. This motivates wilful attackers to destroy the communication link and the IoT platform, especially when the energy management system of a critical infrastructure such as a smart grid is disrupted in the short or long term. The main objectives of this work within the PETER Project are to design different types of EMI sources and to setup a measurement procedure for propagating the EMI signal to different smart grid communication subsystems. Then, to monitor the effect of the coupled EMI signal on the subsystem as well as the overall system under attack and statistically test the susceptibility of the smart grid complex system to intentional low-power EMI. This experiment proves the vulnerability of the smart grid communication system to radiated IEMI, and just following the EMC/EMI standards will not be a complete solution to protect the system from malicious EMI attacks. The proposal to protect critical infrastructures like smart grid systems from intentional EMI attacks is to use the rule-based criteria as a foundation and demonstrate risk-based approach to protect the systems more adequately.

Table 1.6: DUTs (IED, MU, RTU1 RTU2) vulnerabilities to SPJ with different frequencies.

DUT Related Communication protocol	IEMI: SPJ frequency range	Radiated IEMI Power Max 250 W up to 1GHz Max 20 W for 1 to 3 GHz	Consequence (PMDTRR: Probability of Mean value Data transmission Rate (kbit/s))	Visual Inspection	Severity (1: Low 4: High)
IED IEC60870-5-104	100 to 200 MHz	35	PMDTR Increased by 37% Overloading data channel	No unusual behaviour	1
	500 MHz to 1GHz	75	PMDTR Reduced by 26% Blocking data channel	Transformer switch flicking on SCADA display but no loss of supply	3
	1 to 3 GHz	100	PMDTR not changed	No unusual behaviour	1
MU IEC61850 sample values	100 to 200 MHz	35	PMDTR not changed	No unusual behaviour	1
	500 MHz to 1GHz	75	PMDTR Reduced by 50% Blocking data channel	Current injection to other subsystems	3
	1 to 3 GHz	100	PMDTR not changed	Voltage injection to DUT and other subsystems	2
RTU1 Goose messages	100 to 200 MHz	23	PMDTR Reduced by 30% Blocking data channel	Sleep mode of the DUT for 20 minutes	4
	500 MHz to 1GHz	25	PMDTR Reduced by 100% Blocking data channel	DUT shootdown	4
	1 to 3 GHz	100	PMDTR not changed	No unusual behaviour	1
RTU2 IEC60870-5-104	100 to 200 MHz	35	PMDTR not changed	No unusual behaviour	1
	500 MHz to 1GHz	55	PMDTR Reduced by 100% Blocking data channel	DUT Stopped operating	4
	1 to 3 GHz	100	PMDTR not changed	No unusual behaviour	1

Table 1.7: DUT (RTU3 with different comm-protocols) vulnerabilities to SPJ with different frequencies.

DUT Related Communication protocol	IEMI: SPJ frequency range	Radiated IEMI Power Max 250 W up to 1GHz Max 20 W for 1 to 3 GHz	Consequence (PMDTRR: Probability of Mean value Data transmission Rate (kbit/s))	Visual Inspection	Severity (1: Low 4: High)
RTU3 Goose messages	100 to 200 MHz	35	PMDTR not changed	No unusual behaviour	1
	500 MHz to 1GHz	75	PMDTR not changed	No unusual behaviour	1
	1 to 3 GHz	100	PMDTR Reduced by 50% Blocking data channel	communication breakdown	3
RTU3 IEC 60870-5-104	100 to 200 MHz	35	PMDTR not changed	No unusual behaviour	1
	500 MHz to 1GHz	75	PMDTR Reduced by 100% Blocking data channel	communication breakdown	4
	1 to 3 GHz	100	PMDTR not changed	No unusual behaviou	1
RTU3 Internet	100 to 200 MHz	35	PMDTR close to zero	Disconnection of data	4
	500 MHz to 1GHz	75	PMDTR close to zero	Disconnection of data	4
	1 to 3 GHz	100	PMDTR Reduced by 30% Blocking data channel	communication delay	2

Chapter 2

Open Issues and Suggestions for Improvements by Arash

Dr Henning Taxt, the Energy system, Team Manager of SINTEF Energi AS, welcomed me, introduced me to the other team members and gave permission for access to the Smart Grid and Faraday Cage labs in SINTEF and NTNU. Dr Merkebu Zenebe Degefa introduced me to the rest of the team and provided the entire requirement during my stay at SINTEF. I worked closely with co-supervisor Dr Santiago Sanchez Acevedo, who supported me during the measurement set-up, where the installation of the new communication links had to be carried out, and during the demonstration of the measurements in the Faraday cage, in a different location than the smart grid laboratory. Co-supervisor Kjell Ljøkelsøy provided the equipment needed from zero to finish, from power cables to the spectrum analyser. Dr Martin Schaarschmidt and his team members Sven Fisahn and Joerg Radunz from WIS facilitated the transport of the measurement equipment needed from WIS, Germany, to SIN-TEF, Norway, to demonstrate the measurement at SINTEF throughout the month. List of measurement equipment is attached to Annex C. In addition, access to the lab was requested through the EriGrid.2 project. However, due to the requirements of the PETER project, SINTEF had to join the PETER project and ESr2's participation in SINTEF had to be counted as secondment in order to get the legal approval of the PETER project officer. A contract between the lead researcher ESR2 and SINTEF had to be signed in order to fulfil the legal and administrative requirements of the PETER project attached in Annex D. I want to thank all the SINTEF Energy system team members for their warm welcome and the incredible help and support, especially from Dr Henning Taxt, Dr Merkebu Zenebe De-gefa, Dr Santiago Sanchez Acevedo and Kjell Ljøkelsøy. I would like to say thank you to Dr Martin Schaarschmidt, Sven Fisahn and specially Joerg Radunz for facilitating the shipment of the measurement equipment from Germany to Nor-way.

Chapter 3

Lab Access 2 - Fernando Arduini (Fraunhofer INT)

1 Introduction

The electricity sector has been undergoing transformations toward the smart grid concept, which aims to improve the power system's robustness, efficiency, and flexibility. This transition has been achieved by the introduction of smart electronic devices (SEDs) and advanced automatic control and communication systems. Despite the benefits of such modernization, safety issues have emerged with significant concern among experts and entities worldwide. One of these issues is Intentional Electromagnetic Interference (IEMI), where offenders maliciously employ high-power electromagnetic sources to disrupt or damage electronic devices. Compared to a physical terrorist act intended to disrupt critical infrastructure (e.g., involving explosives), an IEMI attack can easily occur unnoticed and at a distance from the target system. Conversely, in contrast to a cyber-attack, in which a hacker may trigger alarms while attempting to bypass the firewalls of a system, an IEMI exposure typically does not leave any footprint on the affected system (Arduini, Lanzrath, Pusch, Suhrke, & Garbe, 2021).

In the context of IEMI, the risk is defined by the scenario involving an interference source and a target system, the consequence degree in case this scenario occurs, and its probability of occurrence. In the case of smart grids, several systems, interdependencies, and energy facilities are involved. Therefore, determining the consequences of successful IEMI attacks is very challenging (Lanzrath, Suhrke, & Hirsch, 2020). On the one hand, conducting susceptibility tests with High-Power Electromagnetic (HPEM) sources in real power infrastructures (e.g., substations) is impractical. It could trigger electrical equipment damage and even blackout events compromising the power supply of final consumers. On the other hand, carrying out susceptibility testing campaigns for "systems of systems" in HPEM lab facilities is also not always possible given the complexity of reproducing such systems realistically. For such purpose, the approach employed in recent studies is considering parts of the system in susceptibility tests and, based on the failures found, estimating what would happen at the system-of-systems level. To some extent, this estimation allows determining the degree of the risk consequence. However, as the power system has a dynamic and complex behavior, this approach may lead to underestimation or overestimation of the impact.

The role of ESR 15 in the PETER project is to propose an IEMI risk management methodology for complex systems represented specifically by smart grids. The idea behind a secondment

at SINTEF was to model a smart grid system in which IEMI failures at device-level could be emulated in a complex smart grid system for consequence analysis. As a requirement, this system needed to incorporate key power and communication smart grid elements operating in real-time for the emulation of device-level IEMI failures. These failures, in turn, refer to the most common effects found in IEMI test campaigns with smart grid devices. Given that, during the ESR's three-week secondment, a smart grid system was modeled, and the impact of Remote Terminal Units (RTUs) communication failures from different nodes of the system were evaluated based on the grid frequency response.

The following report aims to describe the smart grid system modeled using a Matlab/Simulink interface with the real-time simulator OPAL-RT. To this end, details about the power and communication elements are presented. Then, the NADIR frequency parameter, which is used as the impact analysis parameter, is described. Finally, the IEMI attack scenarios are detailed, and a discussion of the results is presented.

2 Cyber-physical system for IEMI impact analysis

A real-time smart grid was modelled in OPAL-RT. The OPAL-RT environment allows the integration of grid topologies modeled in Matlab/Simulink operating in real-time with physical and virtual smart grid devices, including Intelligent electronic devices (IEDs) and Ethernet switches. The cyber-physical smart grid in question was modelled in such a way that IEMI attacks could be emulated in real-time. Furthermore, the goal of such a system was to allow various system nodes, represented by IEDs, to be attacked for consequence evaluations as part of the risk management framework.

The following subsections describe the modelled electrical network as well as the SCADA system, including the communication and control systems.

2.1 Medium Voltage (MV) Distribution Network

The electrical network was modelled in Matlab/Simulink software. Figure 2.1 illustrates the implemented topology. It is based on the medium voltage distribution network proposed by the International Council for Large Electricity Systems (Cigre) (04.02, 2014). The network consists of a 110 kV sub-transmission system with a three-phase short-circuit level of 5000 MVA. The frequency reference of the system is given by the main Synchronous Generator (SC) connected on the 110 kV high voltage side. On the medium voltage side of 20 kV, there are 15 busbars. At busbar 9, a 6.67 MVA rated Wind Turbine (WT) was inserted. Likewise, an Energy Storage System (ESS) of 6.67 MVA was added at busbar 10. Both the WT and the ESS were represented by Voltage Source Converters (VSCs), which independently control the respective active and reactive powers. Under steady-state condition, the WT injects 1.5 MW into the grid while the ESS generation is null. Under frequency dip conditions, both WT and ESS inject active power into the system in order to withstand the network frequency oscillation. Protection elements have been inserted in some points of the system. These have an overvoltage function and are highlighted in yellow in the figure. Although these elements are not used in the analysis proposed in this report, their existence allows future investigations regarding the impact of IEMI failures in smart grids.

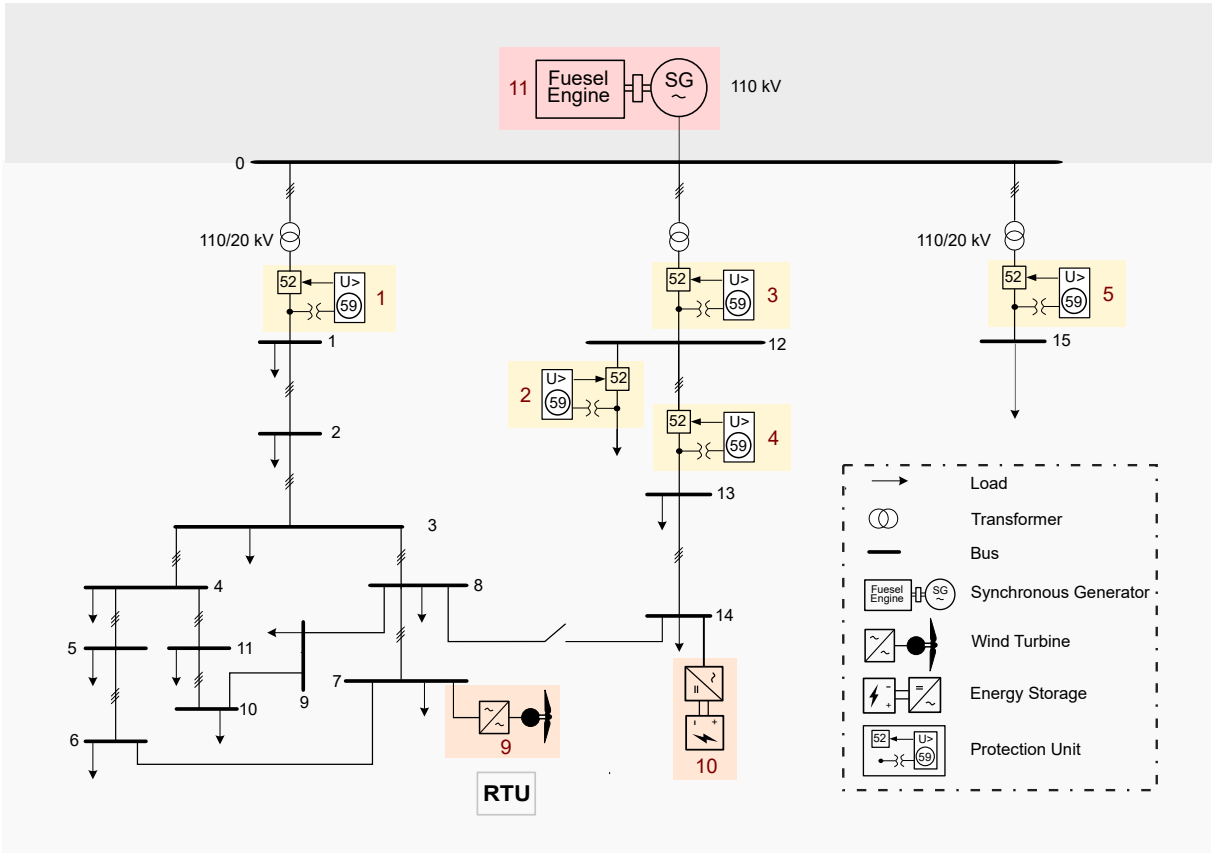


Figure 2.1: Modelled power system.

2.2 SCADA System

Figure 2.2 illustrates the communication architecture, which has been defined in accordance with IEC 61850 standard (Mackiewicz, 2006). In this framework, three levels are defined. The Process Level contains the Measurement Units (MUs) and Remote Terminal Units (RTUs) for current and voltage data acquisition, as well as circuit breaking capabilities. The Bay Level comprises the IEDs responsible for processing the process level devices data and making local control decisions. Finally, the Station Level is formed by the SCADA system. It comprises a Human Machine Interface (HMI) for monitoring and operating the system, a data storage for storing system events, as well as a controller for managing the network.

The individual devices on the different levels of IEEE 61850 have distinct communication requirements. On the Process Level, low latency times are required for the highest possible operating autonomy. This requirement does not pertain to the communication between the Bay and Station level. In the modelled architecture, the communication between the Process and Bay level devices is driven by GOOSE (Generic Object Oriented Substation Event) protocol. Similarly, the communication between IEDs and SCADA system is given by MMS (Manufacturing Messaging Specification) protocol. The mapping from one protocol to another is done by Ethernet Switches, represented by Communication Switches (CSs) in the figure.

A frequency support logic was implemented in an OPC Unified Architecture (UA) server to monitor and control the configured data points of the simulink model in real-time. Basically, this logic identifies system frequency drops and makes both the WT and the ESS to inject

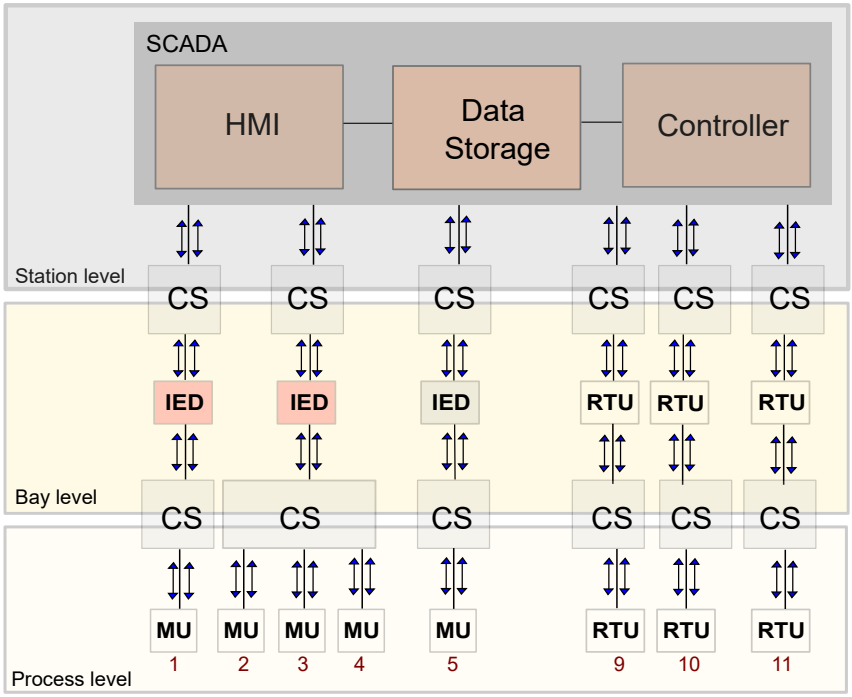


Figure 2.2: Modelled communication system according to the IEC 61850.

extra active power into the grid in order to increase the frequency levels during the transient period. The identification of a frequency drop is given by negative values of the rate of change of frequency (RoCoF), expressed by:

$$ROCOF = \frac{\omega - \omega_{(n-1)}}{T_s} \tag{3.1}$$

where ω is the actual speed of the synchronous generator, $\omega_{(n-1)}$ is the previous speed of the synchronous generator, and T_s is the sampling time.

In addition to the negative ROCOF condition, two other conditions are applied to ensure the effectiveness of the control. First, a minimum ROCOF value of 5e-4 is employed to prevent the WT and ESS references from changing in scenarios of negligible frequency oscillations. Second, the WT and ESS actuations are only allowed when ω is below an upper frequency threshold, defined by 1.01 p.u. When these three conditions are met, the reference signals of the RTU 9, which controls the WT, and the RTU 10, which controls the ESS, are changed in real-time to inject 10% and 15% more active power into the grid. The code for this control logic can be found in Appendix A.

2.3 Nadir frequency

The variable used to analyse the propagation effects of recurrent IEMI attacks was the system frequency. For this, the minimum frequency reached after a disturbance, known as NADIR frequency, was employed as a key metric. The disturbances, in turn, can be triggered by several events in which the generation level is disproportional to the system demand. These events include mainly losses of generating units and demand fluctuations (Ataee, Khezri, Feizi, & Bevrani, 2014).

Figure 2.3 indicates the NADIR frequency of the system containing only the primary control of the synchronous generator and the same system being supported by the WT and the ESS in a drastic load condition at t = 53s. On the one hand, for the system depending only on the primary control of the synchronous generator, the frequency, which is 50 Hz under nominal conditions, reaches a magnitude of 49.15 Hz (black curve). On the other hand, for the system being aided with the secondary control of the distributed elements, this same value is reduced to 49.10 Hz.

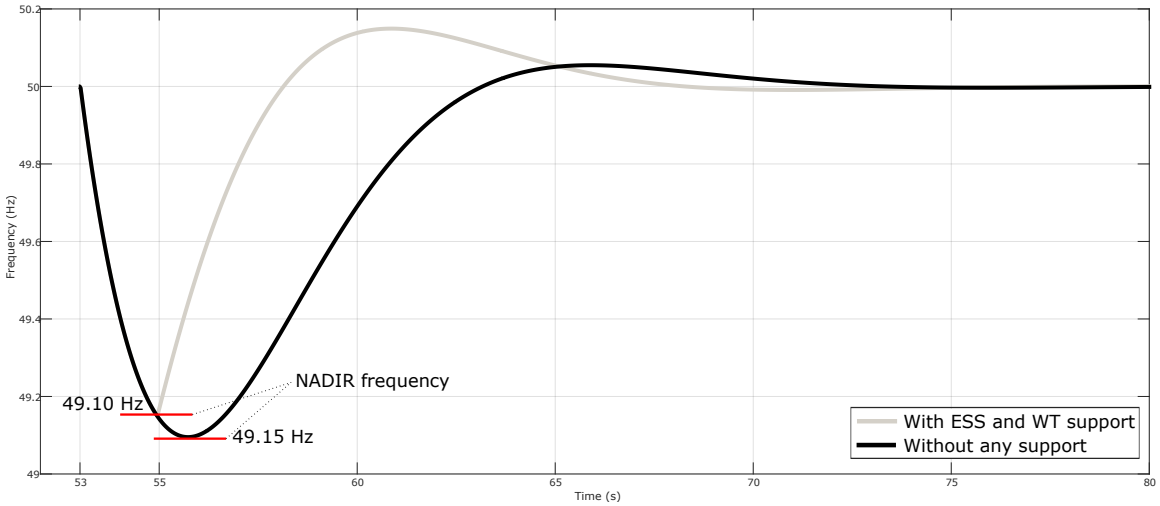


Figure 2.3: NADIR frequency

In view of this, the aim of this study is to investigate how IEMI attacks can impact the dynamics of smart grids that contain distributed elements for frequency support. Therefore, for all analyses presented in this report, the curve in black will represent the baseline scenario, in which the system does not suffer any attack.

2.4 Attack scenarios

Power system operation can be affected as a result of malfunctions of control and/or protection devices caused by IEMI. Based on the modeled smart grid, device-level IEMI effects can be emulated in the model to analyze the consequences at system-level. In the model described, we have as possible points of attack: the RTUs in charge of controlling the power management of the system; the MUs and IEDs responsible for protecting the power grid; and the station-level infrastructure formed by the SCADA system.

IEMI can cause severe impacts on the power system, especially during dynamic changes caused by load increase or decrease conditions, as well as occurrences of electrical faults. In this work, an analysis of the impact of IEMI during a load increase condition was carried out taking into account attacks to three facilities that integrate the network energy management: the main generation plant, which contains the synchronous diesel-based SG controlled directly by the RTU 11; the WT plant, whose wind turbine is managed by the RTU 9; and the ESS facility, whose battery system is controlled by the RTU 10.

For this purpose, the two most recurrent device-level effects for smart grid devices affected by high-power IEMI were tested. The first effect is the total device shutdown, in which the device stops performing its primary function. In the case of RTUs, this failure involves a complete interruption of the GOOSE message packet flow. The second effect is the intermittent interruption

of the device's communication channel, which can be achieved with constant or intermittent exposure of high-power interference signals. In this case, GOOSE packets from the affected RTUs are intermittently prevented from being transmitted.

GOOSE messages are grouped into Ethernet data packets and are exchanged in a publisher-subscriber mechanism, whose transmission occurs within a period of 4 milliseconds. Under this scheme, the same GOOSE message is retransmitted until a change occurs in the data set elements. At this time, a new message starts to be transmitted at high speed, containing the most updated data (Hou & Dolezilek, 2008). From the perspective of the energy management modelled for the smart grid, the GOOSE state number (stNum) parameter from the RTUs is incremented as the GOOSE data set's elements are changed to follow dynamic changes in the network. This implies that the communication link interruption due to an IEMI exposure is given by the non-changing stNum of the GOOSE messages of a respective RTU. In view of this, Figure 2.4 illustrates the IEMI effect of an RTU shutdown on stNum during a network load increase condition.

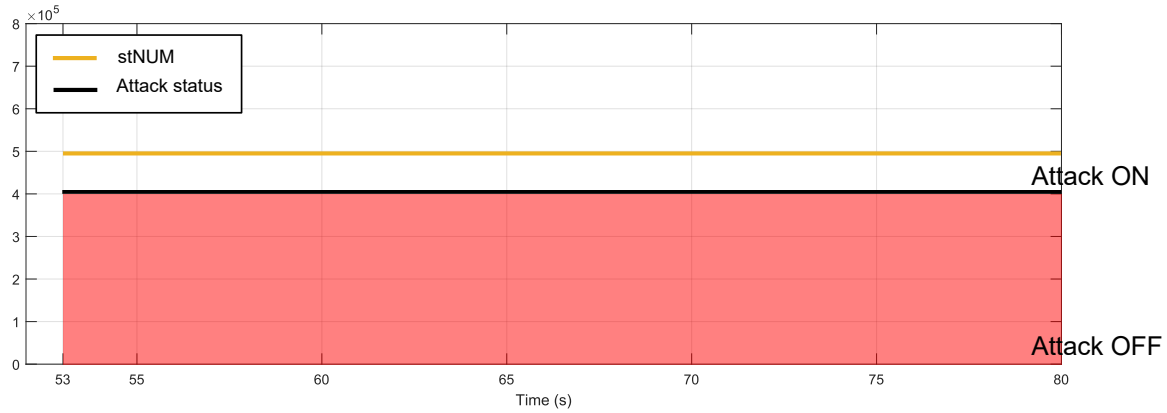


Figure 2.4: Effects of a shutdown failure on stNum

Similarly, Figure 2.5 illustrates the IEMI effect of intermittent communication interruption for the same load change condition. In this case, it is possible to observe that the parameter stNum is unchanged in the instants the RTU is being exposed to an attack. This attack, in turn, can be characterized by a duty cycle, which is given by the ratio of the ON attack condition duration (T_{on}) to the total attack period (T).

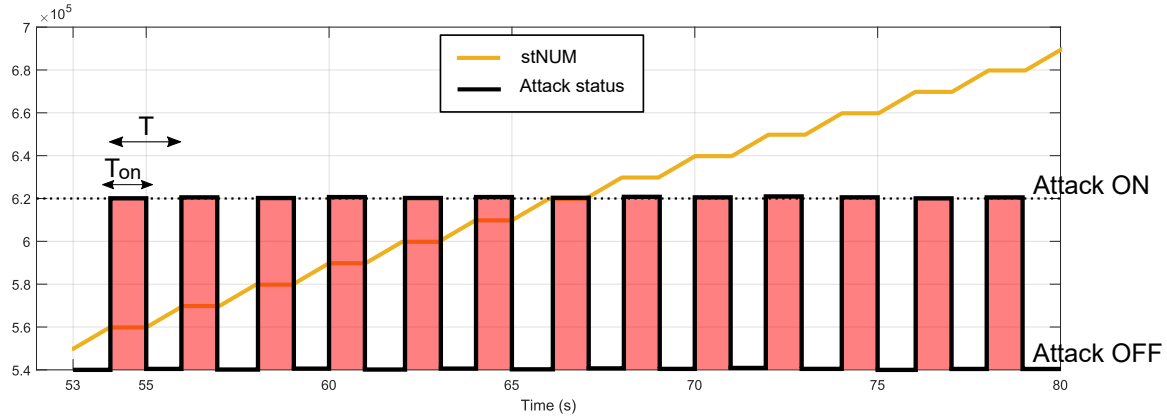


Figure 2.5: Effects of a shutdown failure on stNum

Attack scenarios were proposed to investigate the influence of device-level IEMI failures on the network NADIR frequency. Table 3.1 summarizes key information of the attack scenarios

Table 3.1: Attack Scenarios.

2* Attack Scenario	Target facility			2*Target device	2* Affected functionality	2*IEMI effect
	SG	WT	ESS			
1			x	RTU 10	Goose-based messages for Pess	Shutdown
2	x			RTU 11	Goose-based messages for Omega	Shutdown
3		x		RTU 9	Goose-based messages for Pwt	Shutdown
4	x	x	x	RTU 9, RTU 10, RTU 11	Goose-based messages for Pwt, Pess and Omega	Shutdown
5			x	RTU 10	Goose-based messages for Pess	Intermittent interruption of communication (DT = 60%)
6	x		x	RTU 10 and RTU 11	Goose-based messages for Pess and Omega	Intermittent interruption of communication (DT = 25%)
7	x		x	RTU 10 and RTU 11	Goose-based messages for Pess and Omega	Intermittent interruption of communication (DT = 40%)
8	x	x	x	RTU 9, RTU 10, RTU 11	Goose-based messages for Pwt, Pess and Omega	Intermittent interruption of communication (DT = 50%)
9	x	x	x	RTU 9, RTU 10, RTU 11	Goose-based messages for Pwt, Pess and Omega	Intermittent interruption of communication (DT = 50%)

that were implemented in the model. This information includes the target facilities, the smart grid devices and their respective affected functionalities, as well as the type of IEMI effect considered. For the attacks whose effect is given by intermittent interruption of communication, the duty cycle information of the attack is given to specify the scenario.

3 Results

The following subsections show the dynamic responses of the system under a load increase condition at t = 53 s. For each attack scenario, three graphs are presented. The first illustrates the stNum status of the RTUs 9, 10, and 11 that control WT, ESS, and SG, respectively. In

this graph, it is possible to identify the affected RTU, the type of IEMI effect (shutdown or intermittent communication failure), and the instants when the device is under the impact of the IEMI exposure.

On the one hand, for attack scenarios 1,2,3 and 4, the load change occurs when the respective RTU is already off due to a shutdown IEMI failure. This can be verified by the non-variation of stNUM in the whole simulation window. On the other hand, for attack scenarios 5, 6, 7, 8, and 9, the load change occurs when the device is under an intermittent attack effect, and the device may or may not be exposed at the beginning of the transient (53 s). In these cases, the stNUM is increasing, but it has some constant periods, which indicate the IEMI exposure instants. Attacks 8 and 9 have the same target devices and attack duty cycle, but the transient happens at different exposure times. In attack 8, the load change occurs when the communication of the RTU 9,10, and 11 are being interrupted, while in attack 9, the transient occurs at the period the devices are not being exposed.

The second graph shows the measured active power signals from the WT and the ESS, and the respective reference signals calculated by the controller responsible for the power management. These graphs show that both the measured and the reference signals are susceptible to response deviations due to interrupted GOOSE packets depending on the IEMI effect resulting from an attack. The deviation of these signals is given by comparing the responses with the scenario in which the system is not attacked, presented in section 2.3.

The third graph compares the dynamic frequency behavior of the system for the scenarios with and without the respective attack. In this graph, it is possible to visualize the degree of NADIR frequency degradation and how the signal returns to a steady-state after the transient at t = 53 s.

3.1 Attack Scenario 1

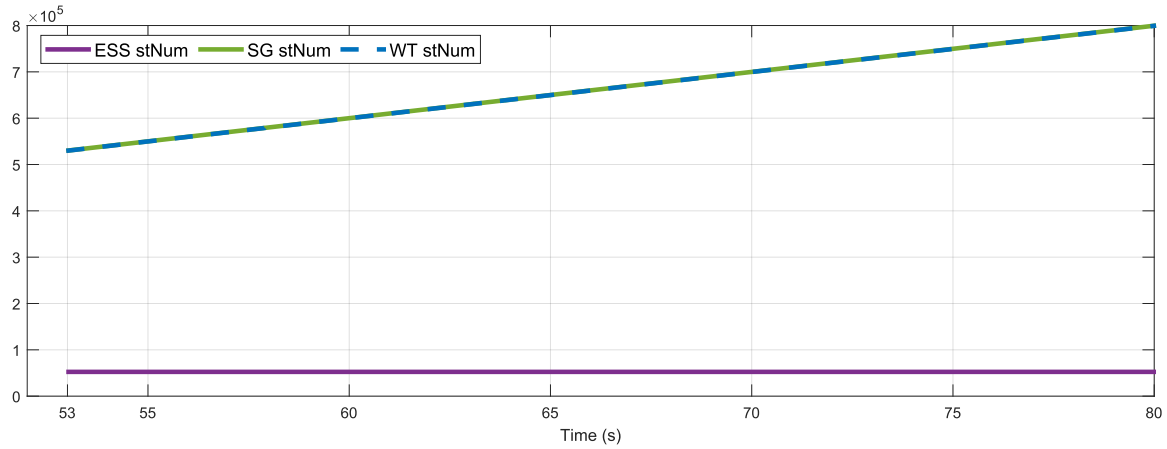


Figure 3.1: stNUM of controlled RTU's - Attack scenario 1.

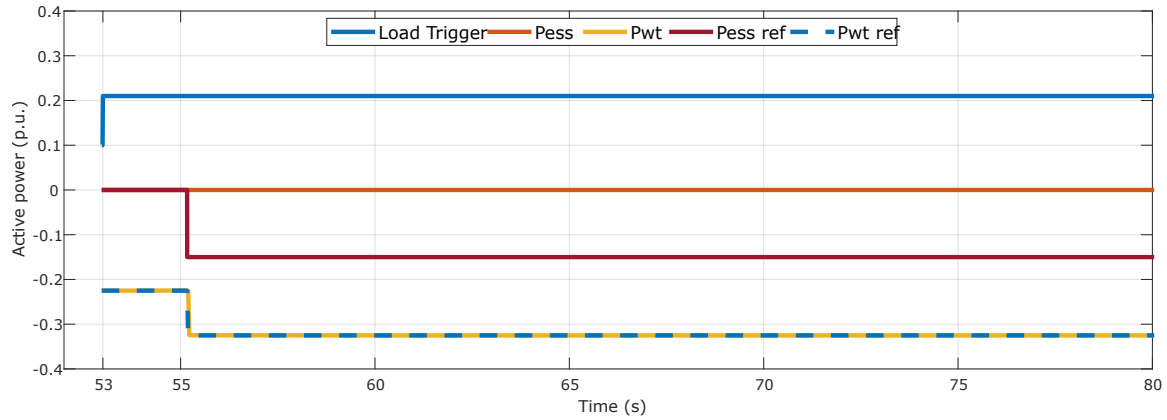


Figure 3.2: Active power reference and measurement signals - Attack scenario 1.

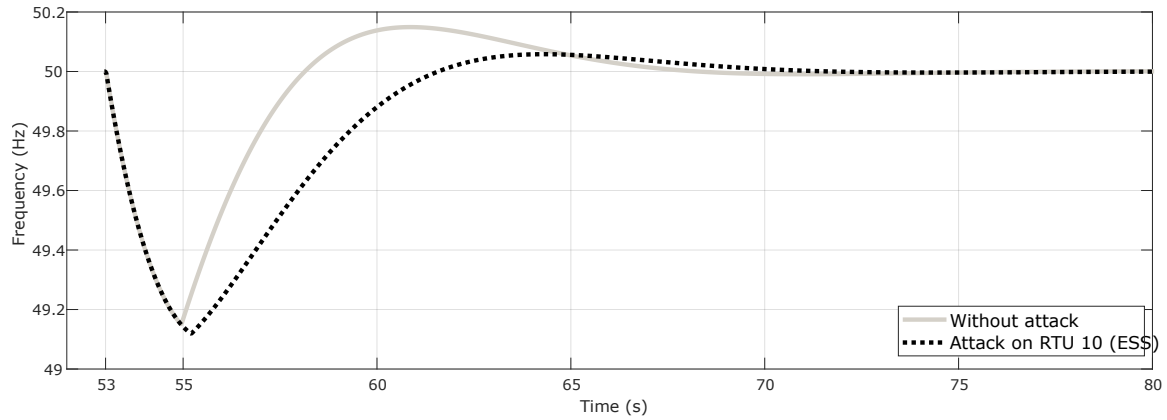


Figure 3.3: System frequency - Attack scenario 1.

3.2 Attack Scenario 2

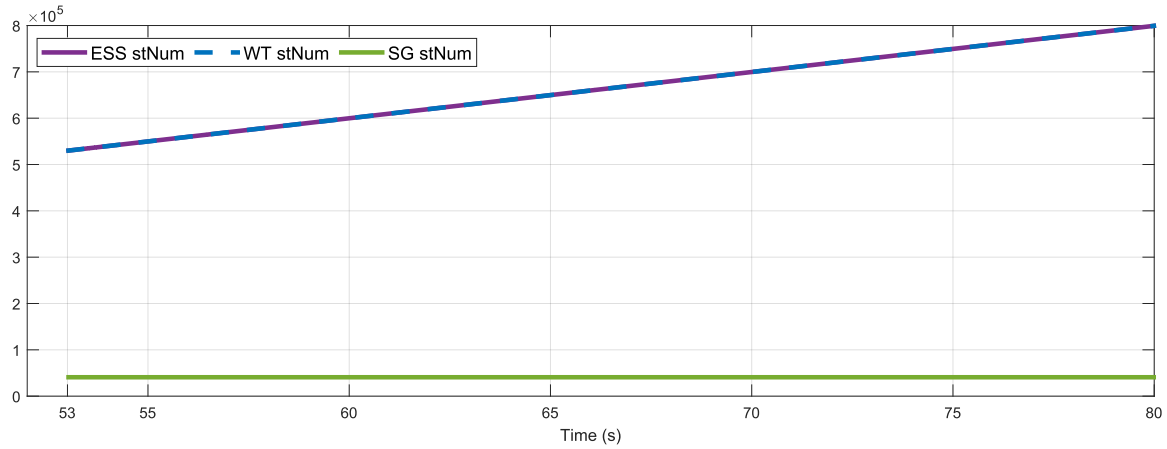


Figure 3.4: stNUM of controlled RTU's - Attack scenario 2.

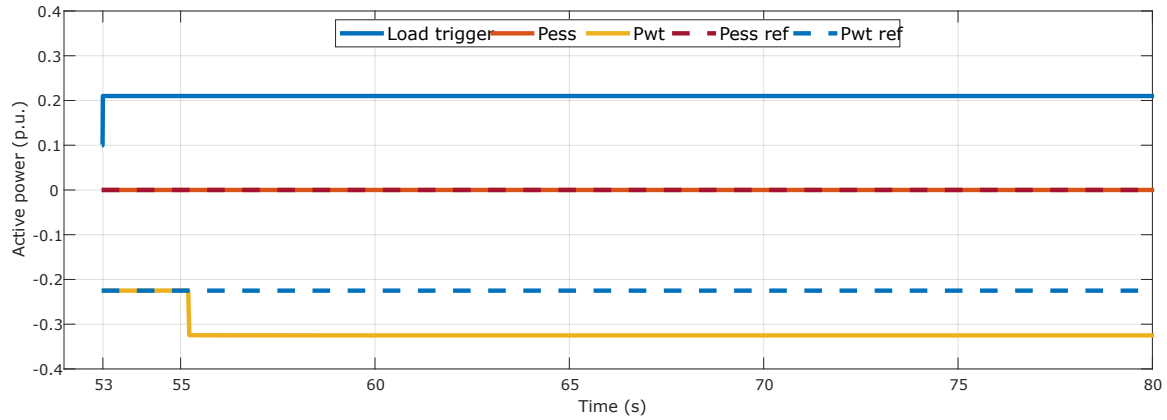


Figure 3.5: Active power reference and measurement signals - Attack scenario 2.

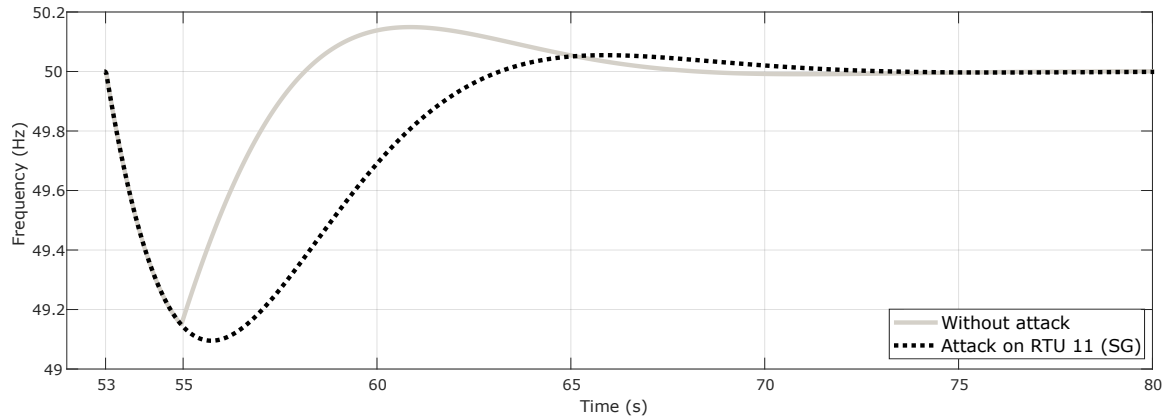


Figure 3.6: System frequency - Attack scenario 2.

3.3 Attack Scenario 3

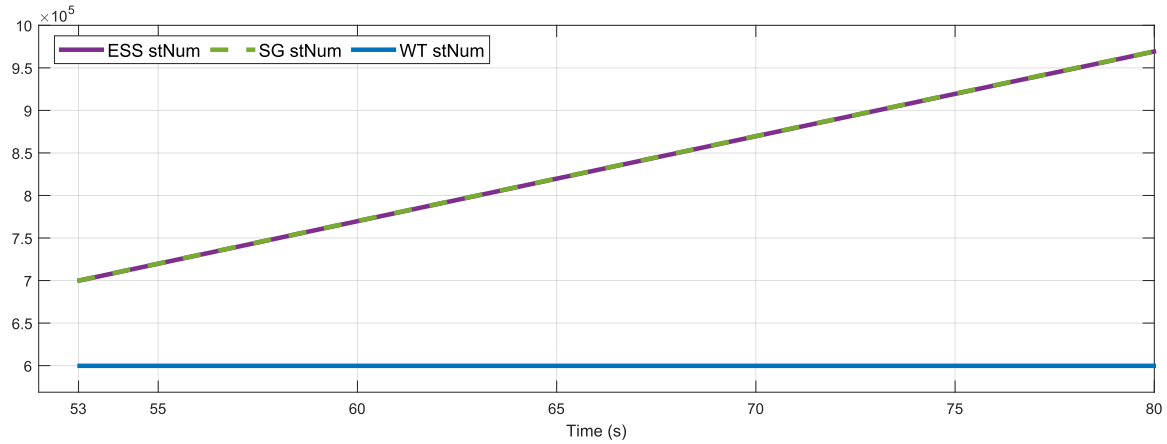


Figure 3.7: stNUM of controlled RTU's - Attack scenario 3.

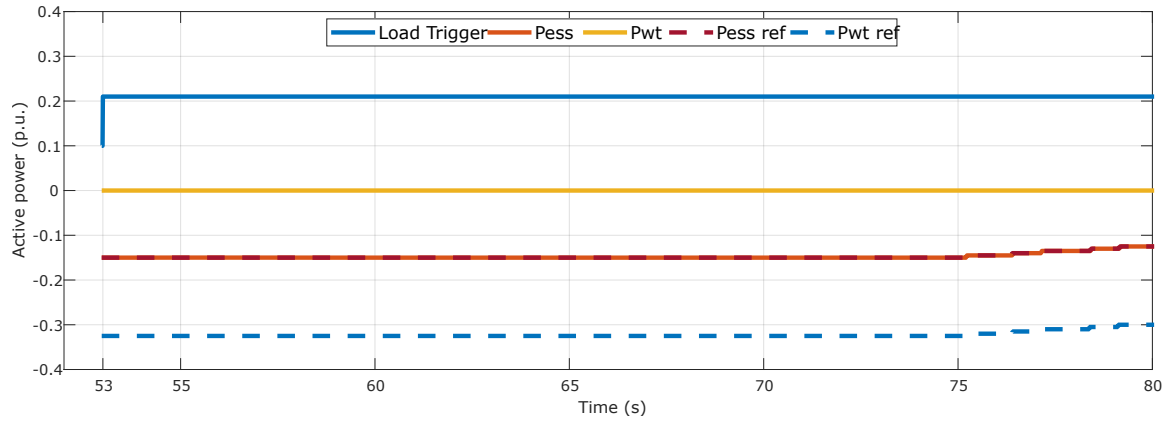


Figure 3.8: Active power reference and measurement signals - Attack scenario 3.

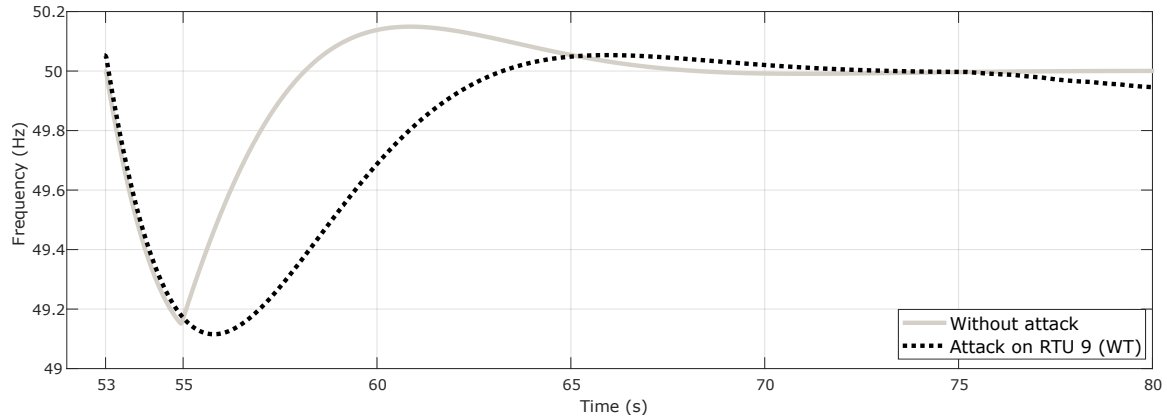


Figure 3.9: System frequency - Attack scenario 3.

3.4 Attack Scenario 4

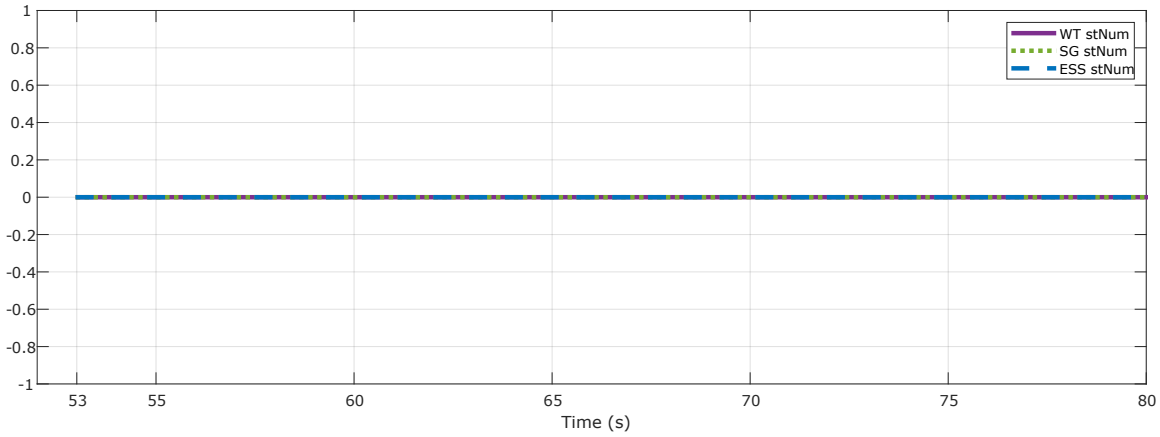


Figure 3.10: stNUM of controlled RTU's - Attack scenario 4.

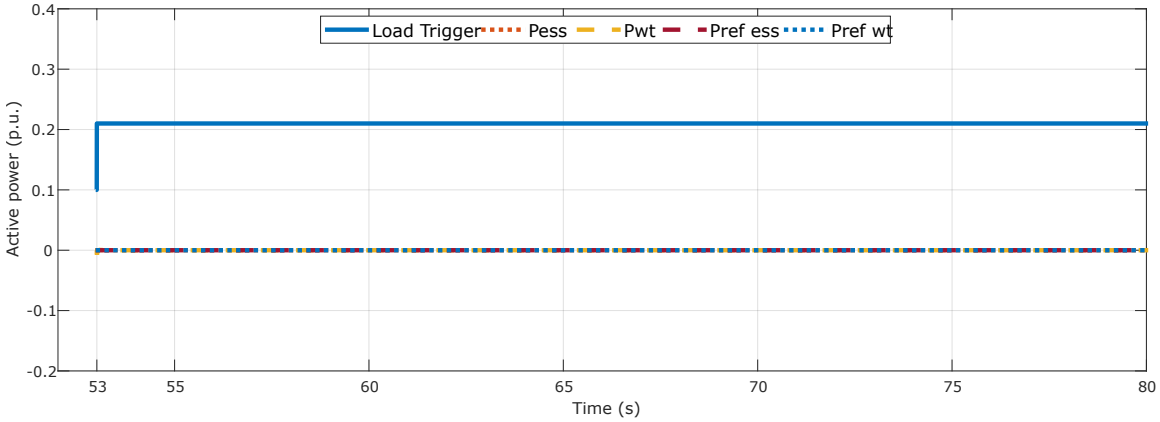


Figure 3.11: Active power reference and measurement signals - Attack scenario 4.

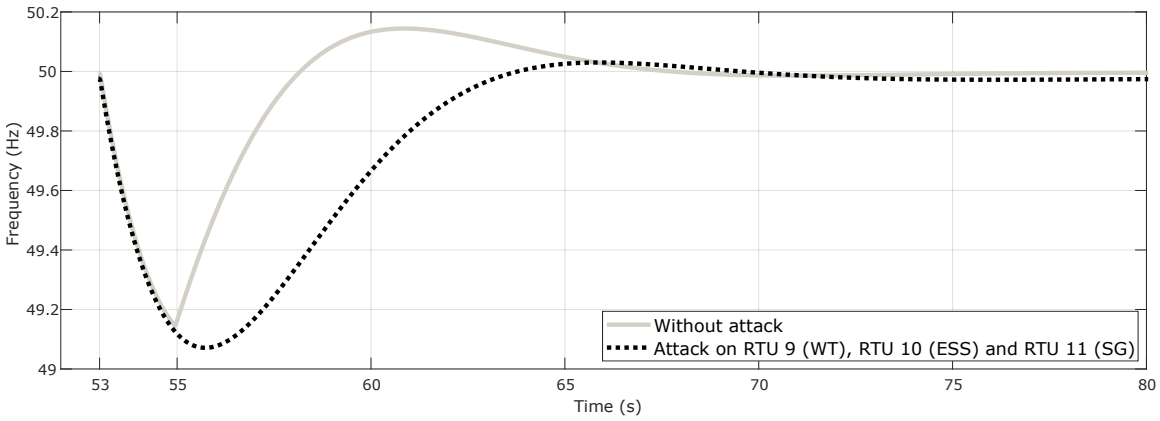


Figure 3.12: System frequency - Attack scenario 4.

3.5 Attack Scenario 5

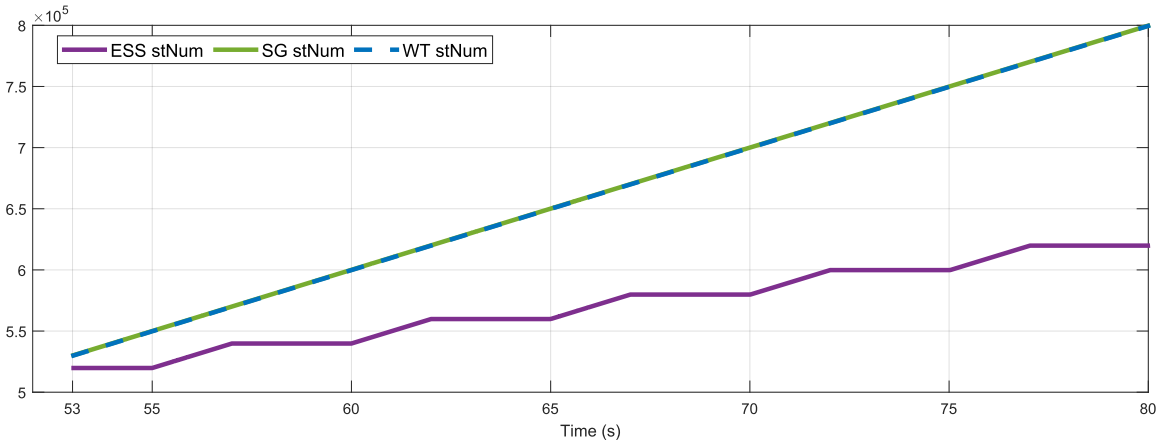


Figure 3.13: stNUM of controlled RTU's - Attack scenario 5.

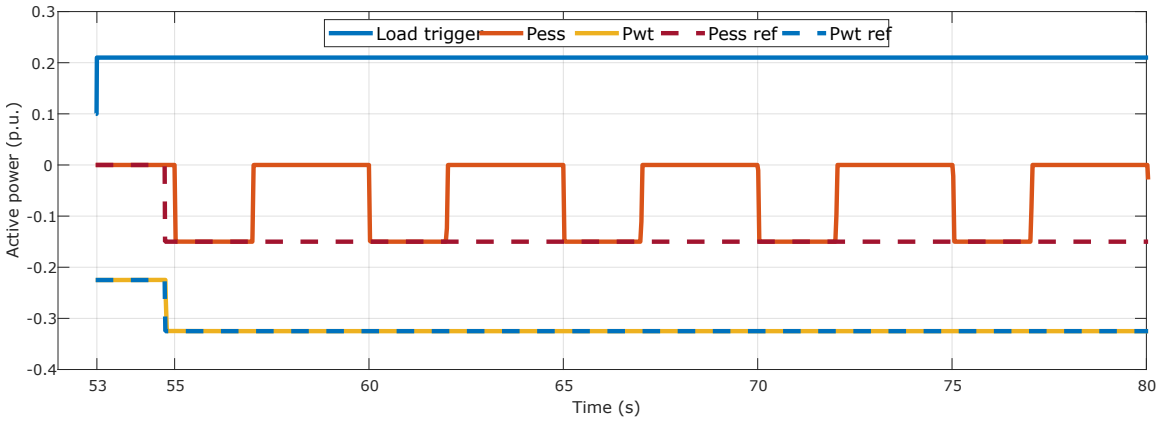


Figure 3.14: Active power reference and measurement signals - Attack scenario 5.

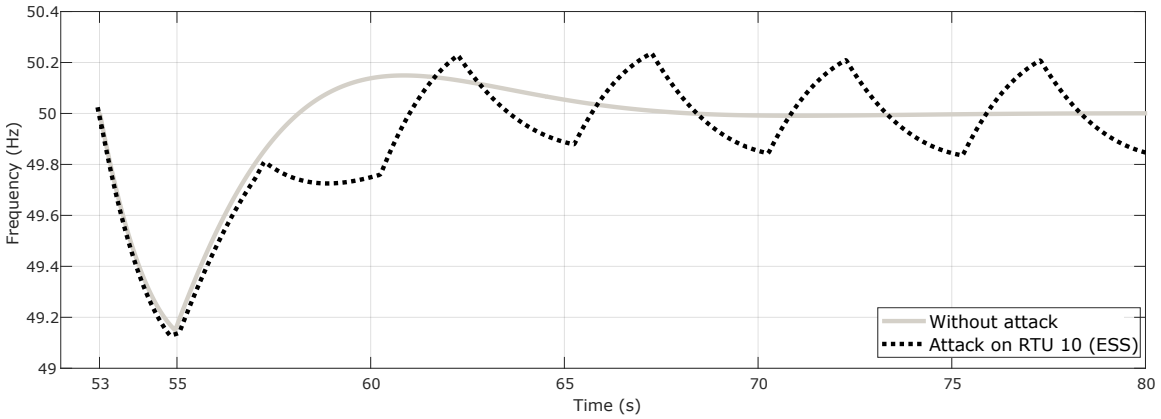


Figure 3.15: System frequency - Attack scenario 5.

3.6 Attack Scenario 6

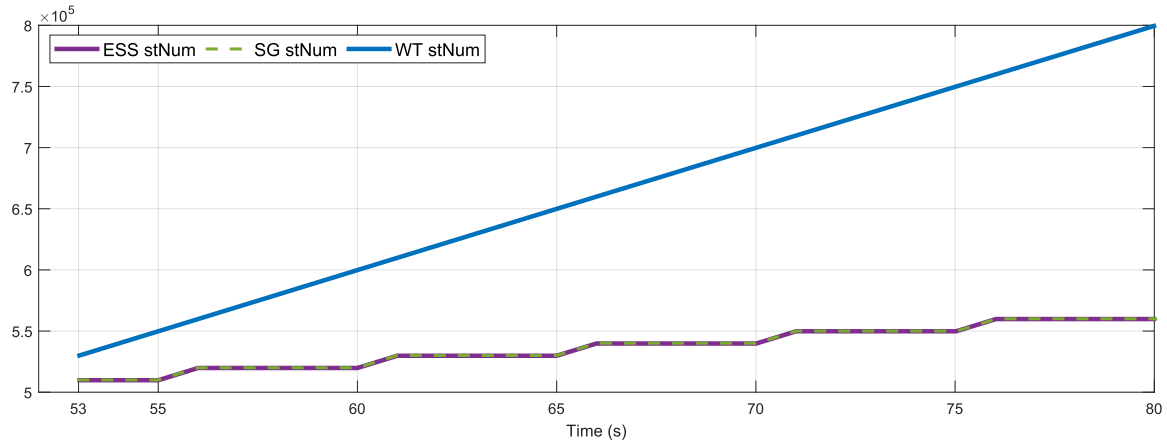


Figure 3.16: stNUM of controlled RTU's - Attack scenario 6.

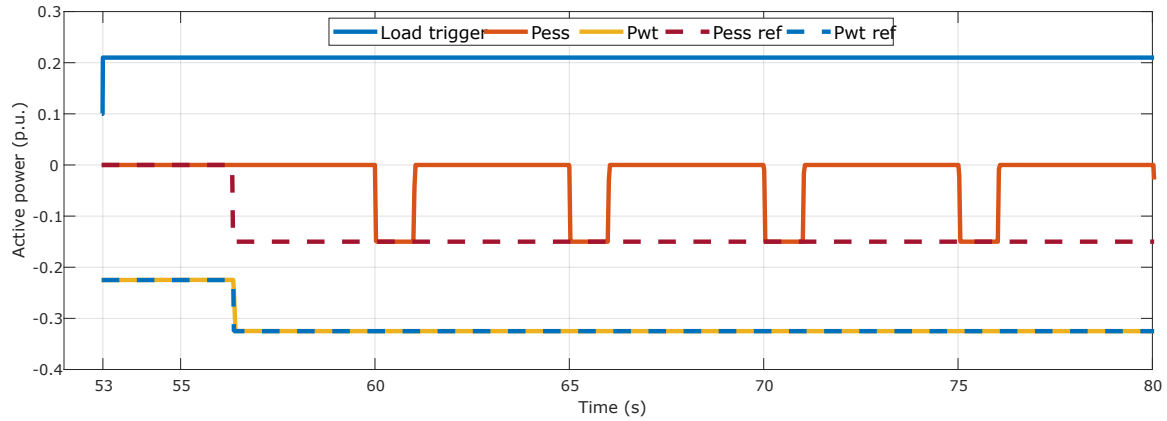


Figure 3.17: Active power reference and measurement signals - Attack scenario 6.

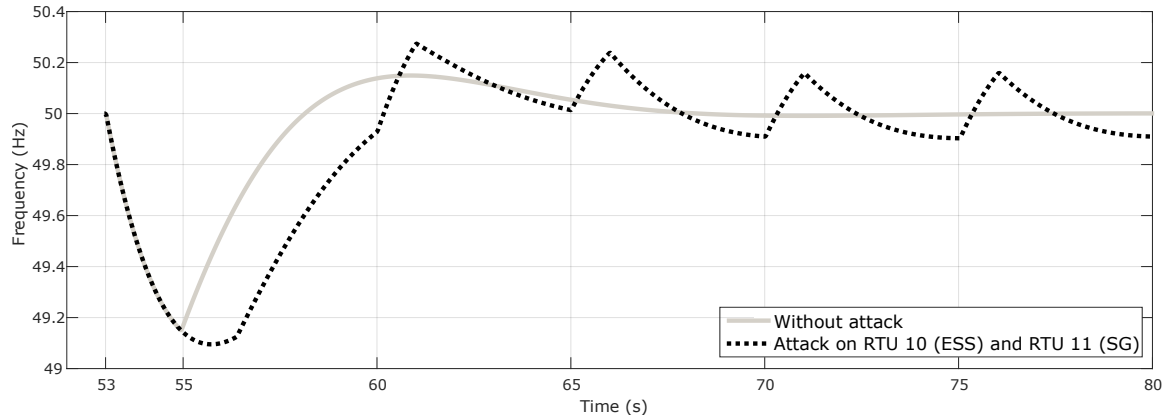


Figure 3.18: System frequency - Attack scenario 6.

3.7 Attack Scenario 7

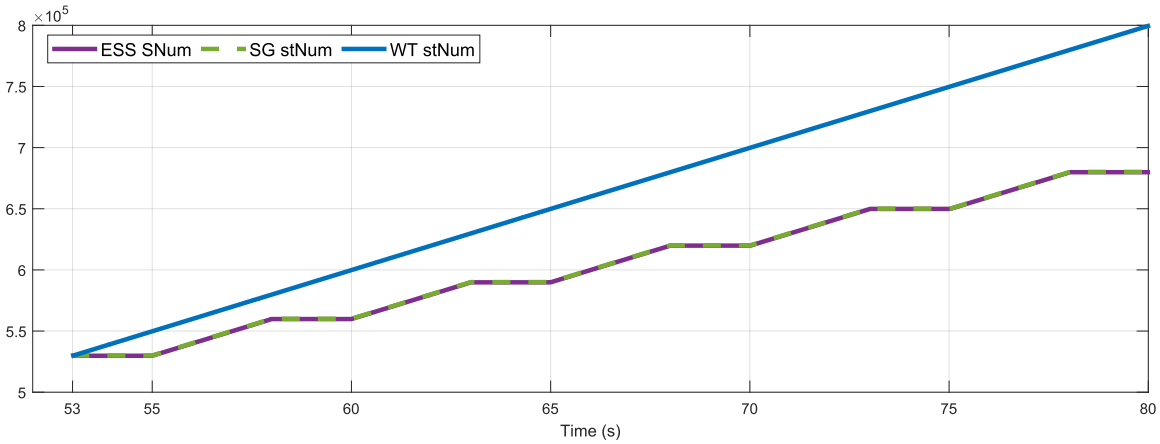


Figure 3.19: stNUM of controlled RTU's - Attack scenario 7.

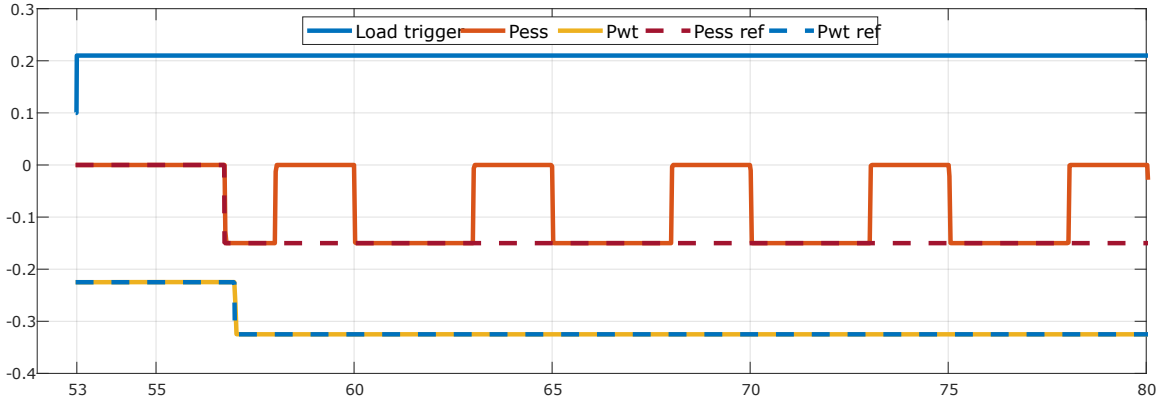


Figure 3.20: Active power reference and measurement signals - Attack scenario 7.

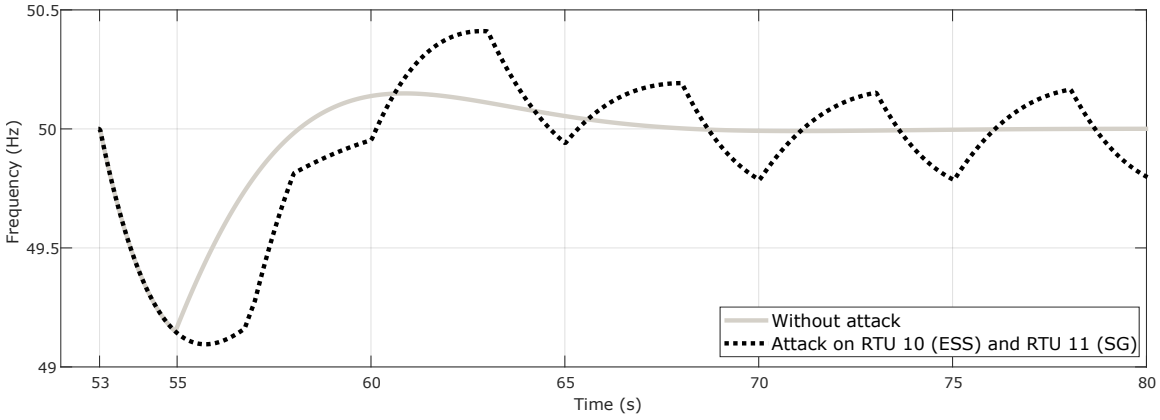


Figure 3.21: System frequency - Attack scenario 7.

3.8 Attack Scenario 8

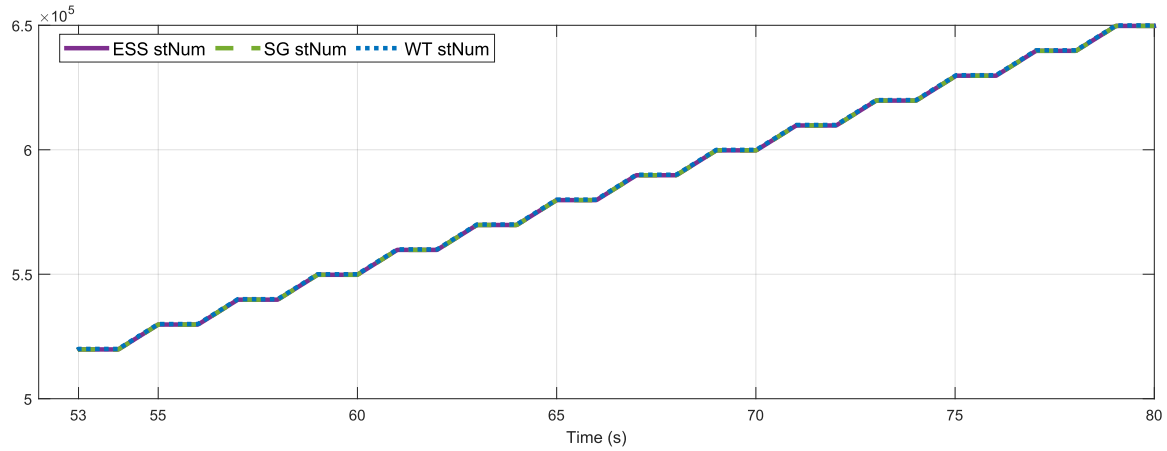


Figure 3.22: stNUM of controlled RTU's - Attack scenario 8.

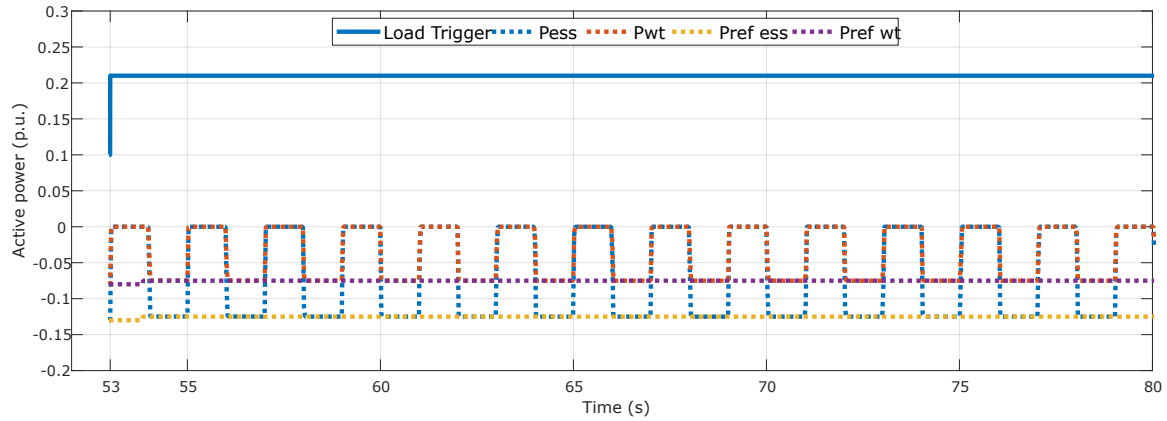


Figure 3.23: Active power reference and measurement signals - Attack scenario 8.

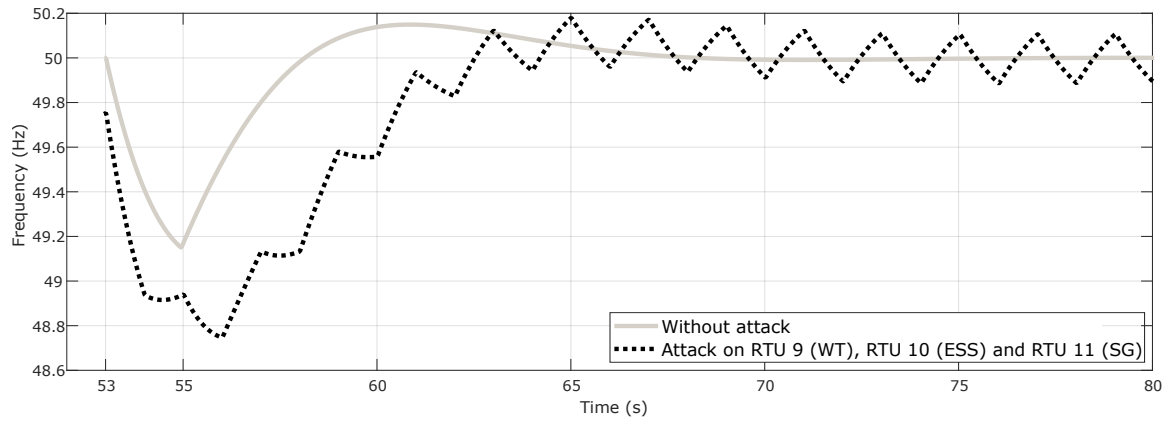


Figure 3.24: System frequency - Attack scenario 8.

3.9 Attack Scenario 9

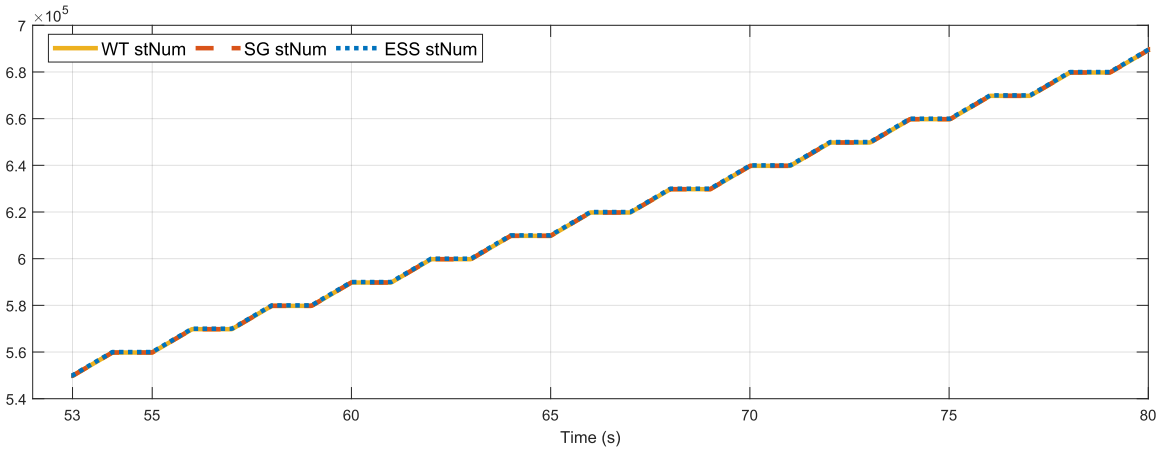


Figure 3.25: stNUM of controlled RTU's - Attack scenario 9.

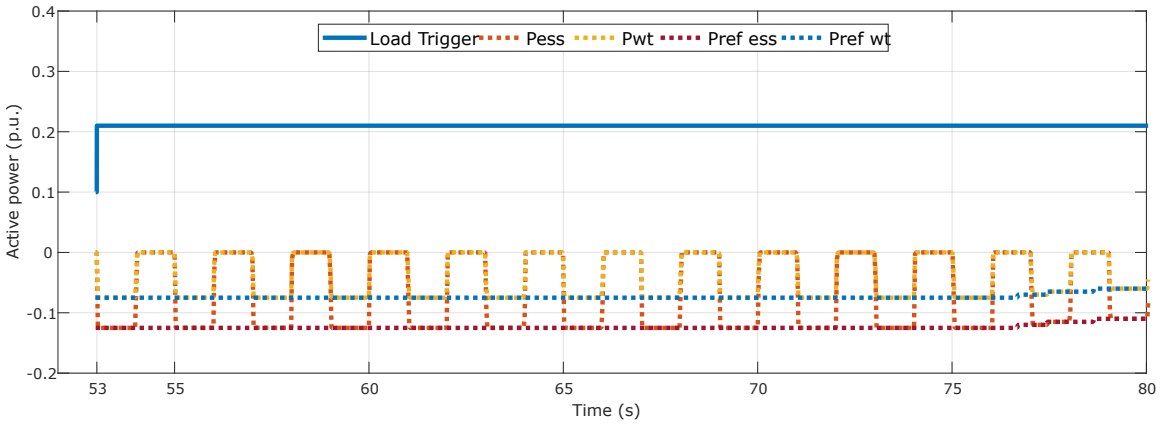


Figure 3.26: Active power reference and measurement signals - Attack scenario 9.

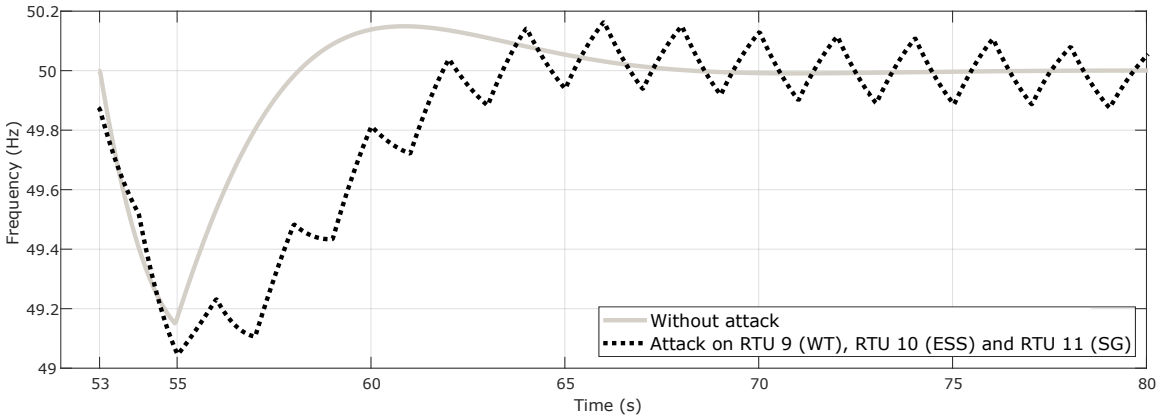


Figure 3.27: System frequency - Attack scenario 9.

Table 3.2: NADIR frequency values - Shutdown Failure Scenarios.

Attack Scenario	NADIR frequency (Hz)
Without attack	49,15
1	49,12
2	49,10
3	49,12
4	49,07

3.10 Comparative of the attack scenarios involving shutdown failure

.

Figure 3.28 compares the attack scenarios whose IEMI failure is given by the shutdown of the RTU device, where the goose messages are permanently interrupted. They are represented by attack scenarios 1, 2, 3 and 4. Additionally, Table 3.2 summarizes the NADIR frequency values for each case. It can be observed that all attack scenarios caused a worsening in the NADIR indicator in relation to the scenario without attack. Out of the scenarios involving single attacks, scenario 2, in which RTU 11 was affected, caused the worst frequency behavior. When all three RTUs were simultaneously affected by a shutdown failure (scenario 4), the NADIR frequency deteriorated even more, reaching 49.07 Hz. In all cases, although the attacks worsened the NADIR frequency, the shutdown failures only adversely influenced the frequency transient period. In all scenarios, it is observed that the frequency returned to the 50 Hz steady-state value in approximately 10 seconds.

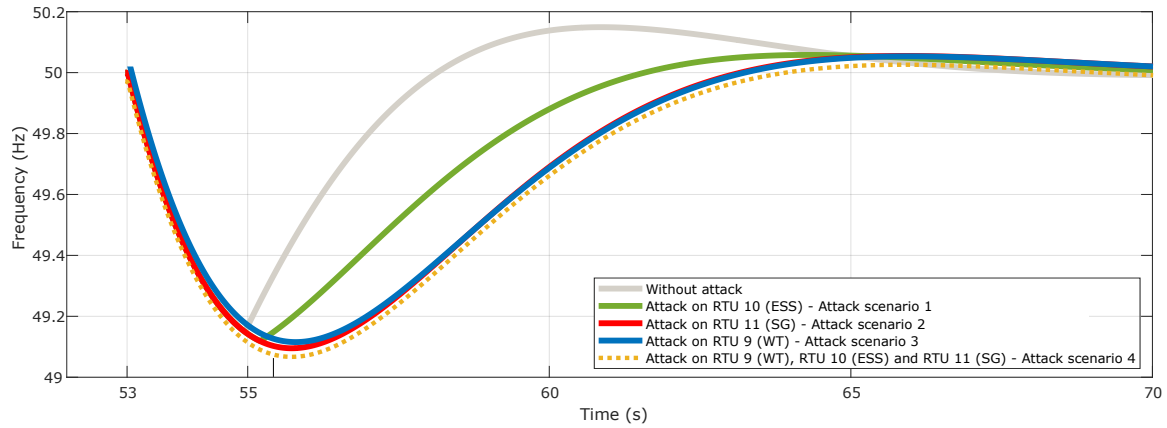


Figure 3.28: System frequency - Comparison for the shutdown failure.

3.11 Comparative of the attack scenarios involving intermittent communication failure

The frequency response of the attack scenarios where the failures emulated were the intermittent interruptions of goose messages are illustrated in Figure 3.29. Similarly, Table 3.3 summarizes the NADIR frequency of each scenario. In general, intermittency failures caused degradation of the frequency behavior both in steady and transient states. The more facilities attacked, the worse the NADIR frequency indicator. The frequency reached 48.75 when RTU

Table 3.3: NADIR Frequency Values - Intermittent Communication Failure Scenarios.

Attack Scenario	NADIR frequency (Hz)
Without attack	49,15
5	49,13
6	49,10
7	49,10
8	48,75
9	49,05

9 (WT), RTU 10 (ESS), and RTU 11 (SG) were targeted, 49.10 when RTU 10 (ESS) and RTU 11 (SG) were targeted, and 49.13 when only RTU 10 (ESS) was affected.

Comparing scenarios 6 and 7, where both RTU 10 (ESS) and RTU 11 (SG) were affected, it can be noticed that a higher duty cycle value led to higher frequency oscillations in transient and steady-state regimes, although the NADIR frequency values were comparable.

Regarding scenarios 8 and 9, where all facilities were targeted with an intermittent communication failure at the same duty cycle condition, it is observed that the frequency behavior is drastically sensitive to the instant the transient occurs during the IEMI exposure. In scenario 9, the load switching occurred when the IEMI exposure was enabled, while in scenario 8, the same transient started when the exposure was disabled. In both cases, the NADIR frequency was worse in scenario 8 since the fault had already caused a pre-transient condition where the frequency was below the 50 Hz rated value.

Besides the deterioration of the NADIR frequency, intermittency failures caused frequency oscillations on a steady-state basis. It, in turn, represents a power quality issue as frequency oscillations can stress synchronous generators and lead to over-temperature conditions.

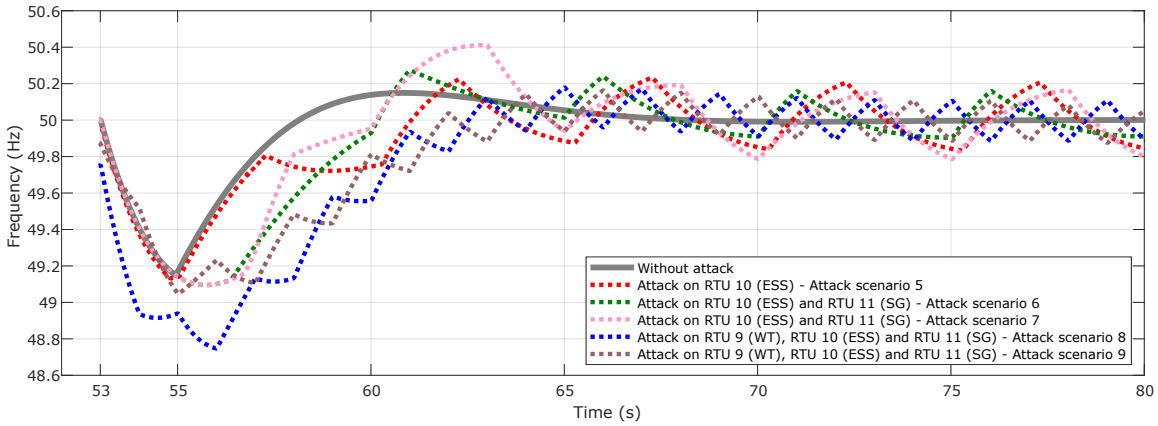
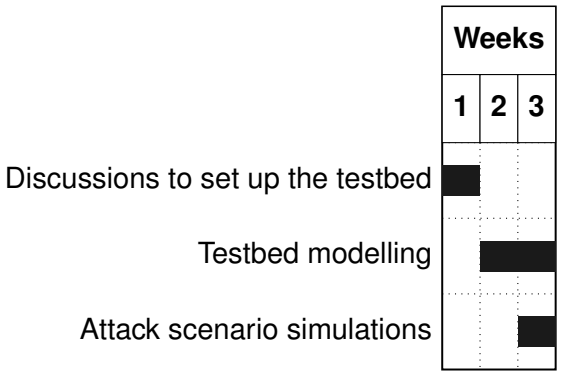


Figure 3.29: System frequency - Comparison for the intermittent communication failure

4 Activity Schedule

The secondment lasted 22 days, or approximately 3 weeks. Table 4.1 details the activity plan undertaken by the ESR. Each square of the table represents a week period.

Figure 4.1: Activity schedule.



5 Final considerations

Analyzing the consequences of IEMI attacks on energy infrastructures is essential for determining the risk. As part of the secondment of ESR 15 at SINTEF, a smart grid testbed for IEMI failure analysis was developed using a Matlab/Simulink interface with the real-time simulator OPAL-RT. The testbed in question consisted of a medium voltage electrical grid with control and protection elements managed by a SCADA system.

Based on attack scenarios simulated in the model, it has been shown that communication failures on RTUs due to IEMI can deteriorate the NADIR frequency of the system. Given the flexibility of the testbed developed, the model can be further exploited for analysis involving protection devices and the occurrence of multiple failures resulting from simultaneous IEMI attacks on the system.

References

04.02, C. T. F. C. (2014). *Benchmark systems for network integration of renewable and distributed energy resources.* International Council on Large Electric Systems Paris, France.

Arduini, F. R., Lanzrath, M., Pusch, T., Suhrke, M., & Garbe, H. (2021). A methodology for estimating the criticality of energy infrastructures in the context of iemi. In *2021 ieee international joint emc/si/pi and emc europe symposium* (pp. 743–748).

Ataee, S., Khezri, R., Feizi, M. R., & Bevrani, H. (2014). Investigating the impacts of wind power contribution on the short-term frequency performance. In *2014 smart grid conference (sgc)* (pp. 1–6).

Hou, D., & Dolezilek, D. (2008). Iec 61850–what it can and cannot offer to traditional protection schemes. *Schweitzer Engineering Laboratories, Inc*, *20080912*.

Lanzrath, M., Suhrke, M., & Hirsch, H. (2020). Hpem-based risk assessment of substations enabled for the smart grid. *IEEE Transactions on Electromagnetic Compatibility*, *62*(1), 173-185. doi: 10.1109/TEMC.2019.2893937

Mackiewicz, R. E. (2006). Overview of iec 61850 and benefits. In *2006 ieee power engineering society general meeting* (pp. 8–pp).

Nateghi, A., Schaarschmidt, M., Fisahn, S., & Garbe, H. (2021). Vulnerability of wireless smart meter to electromagnetic interference sweep frequency jamming signals. In *2021 ieee*

international joint emc/si/pi and emc europe symposium (p. 755-759). doi: 10.1109/EMC/SI/PI/EMCEurope52599.2021.9559200

O'Toole, Z., Moya, C., Rubin, C., Schnabel, A., & Wang, J. (2019). A cyber-physical testbed design for the electric power grid. In *2019 north american power symposium (naps)* (p. 1-5). doi: 10.1109/NAPS46351.2019.9000312

Appendix A. OPC-AU Frequency Support Logic Code

```
# -*- coding: utf-8 -*-
"""

server with OPCUA
in odin runs with python27
"""
from opcua import ua, Server
from random import randint, random
from math import floor
import time
import datetime

inpval = [1,1,1,1,1]    #initialization fro inputvalues to OPF

##OPCUA server configuration
server = Server()

url = "opc.tcp://192.168.10.107:4841"  #IP server(Skuld)
#url = 'opc.tcp://192.168.10.102:4841'  #IP server(Odin)
#url = "opc.tcp://192.168.2.155:4841"  #IP local server(Skuld)

server.set_endpoint(url)
server.set_server_name("ODIN_OPCUA")
server.set_security_policy([
                ua.SecurityPolicyType.NoSecurity,
                ua.SecurityPolicyType.Basic256Sha256_SignAndEncrypt,
                ua.SecurityPolicyType.Basic256Sha256_Sign])

name = "http://OPCUA_SERVER_ODIN"
addspace = server.register_namespace(name)


node = server.get_objects_node()

#variables for transmission
Param = node.add_object(addspace, "Parameters")
#Receiving parameters
Valrec1 = Param.add_variable('ns=4;i=2', "Valrec1",0,ua.VariantType.Float)
Valrec2 =  Param.add_variable('ns=4;i=3', "Valrec2",0,ua.VariantType.Float)
```

```
Valrec3 = Param.add_variable('ns=4;i=4', "Valrec3",0,ua.VariantType.Float)
Valrec4 =  Param.add_variable('ns=4;i=5', "Valrec4",0,ua.VariantType.Float)
Valrec5 =  Param.add_variable('ns=4;i=6', "Valrec5",0,ua.VariantType.Float)
#sending parameters
Vsend1 = Param.add_variable('ns=2;i=22',"Vsend1",0,ua.VariantType.Float)
Vsend2 = Param.add_variable('ns=2;i=23',"Vsend2",0,ua.VariantType.Float)
Vsend3 = Param.add_variable('ns=2;i=25',"Vsend3",0,ua.VariantType.Float)
Vsend4 = Param.add_variable('ns=2;i=24',"Vsend4",0,ua.VariantType.Float)


#Receiving vars
Valrec1.set_writable() #sets variable to be writable by clients
Valrec2.set_writable()
Valrec3.set_writable()
Valrec4.set_writable()
Valrec5.set_writable()
#sending vars
Vsend1.set_writable() #sets variable to be writable by clients
Vsend2.set_writable()
Vsend3.set_writable()
Vsend4.set_writable()


#Start Server
server.start()

vals_recv =[0,0,0,0,0]


try:
    print("Server OPCUA in ODIN started")
    cnt = 0
    lmt = 3
    dt = 0
    h = 1 #time execution
    w_k1 = 0
    w_k = 0
    dw =0
    flagw = False
    flagBES_out = False
    flagWT_out = False
    Pout = [-0.001*i for i in reversed(range(0,150,5))]
    Poutwt = [-0.001*i for i in reversed(range(0,100,5))]
    np = len(Pout)
    npwt = len(Poutwt)
    cnt_out = 0
    cnt_outwt = 0
    enableP = 0
    enablePwt = 0
    while True:
```

```
        ti = time.time()
        val1 = 0.001
        val2 = 0.21
        val3 = 0.23
        val4 = 0.32
        TIME = datetime.datetime.now()

        if cnt < lmt: #connectiong with scada initialize sned data first
            Valrec1.set_value(-1,ua.VariantType.Float)
            Valrec2.set_value(-1,ua.VariantType.Float)
            Valrec3.set_value(-1,ua.VariantType.Float)
            #Valrec4.set_value(0,ua.VariantType.Float)
            #Valrec5.set_value(0,ua.VariantType.Float)
            vals_recv[0] = Valrec1.get_value()
            vals_recv[1] = Valrec2.get_value()
            vals_recv[2] = Valrec3.get_value()
            print("received:", vals_recv)
            cnt+=1
        else: #get data value to the scada
            #get_variables from scada
            vals_recv[0] = Valrec1.get_value() #w speed
            vals_recv[1] = Valrec2.get_value() # enable P injection ES
            vals_recv[2] = Valrec3.get_value() # enable P injection WT
            vals_recv[3] = 0#Valrec4.get_value()
            vals_recv[4] = 0#Valrec5.get_value()
            print('I got = ',vals_recv)
            ########################################
            #Call here the SQL Database
            inpval = vals_recv
            ##method for frequency compensation
            w_k = vals_recv[0]

            enableP = vals_recv[1]
            enablePwt = vals_recv[2]

            dw = (w_k - w_k1)/h #evaluation rocof
            w_k1 = w_k      #delay for w

            ## Logic for ES power injection
            if dw < 0 and abs(dw)>5e-4 and w_k < 1.001:
                Pref = -0.15 * enableP
                Prefwt = -0.1 * enablePwt
                flagw = True
            else:
                Pref = 0
                Prefwt = 0
            if (flagBES_out and enableP == 1): #removing ES
                Pref = Pout[cnt_out]
                cnt_out += 1
                if cnt_out == np:
```

```
                    flagBES_out = False
                    cnt_out = 0
            if (flagWT_out and enablePwt == 1): #removing WT
                Prefwt = Poutwt[cnt_outwt]
                cnt_outwt += 1
                if cnt_outwt == npwt:
                    flagWT_out = False
                    cnt_outwt = 0
            if enableP == 0 and enablePwt == 0:
                flagw = False
            if enablePwt == 0:
               flagWT_out = False
            if enableP == 0:
                flagBES_out = False

################## MAP DATA to SEND to SCADA
            dsnd = [Pref,Prefwt,3,4]
            print("Im sending:", dsnd)
            ########################################
            #to write the variables to SCADA
            Vsend1.set_value(dsnd[0],ua.VariantType.Float) # Send Pref ES
            Vsend2.set_value(dsnd[1],ua.VariantType.Float) # Send Pref WT
            Vsend3.set_value(dsnd[2],ua.VariantType.Float)
            Vsend4.set_value(dsnd[3],ua.VariantType.Float)
            ################################################
            #Monitoring time execution receive--OPF--send
            tf = time.time()    #end_time of processing
            dt = tf-ti     #time processing the OPF and communications
            print("Time enlapse COMM %s" %dt)
        ######################################################
        #sendig parameters
        if cnt < lmt:
            Vsend1.set_value(val1,ua.VariantType.Float)
            Vsend2.set_value(val2,ua.VariantType.Float)
            Vsend3.set_value(val3,ua.VariantType.Float)
            Vsend4.set_value(val4,ua.VariantType.Float)
            print(val1,val2,val3,val4,TIME)
        if dt < h:
            a=0
        if flagw:
            time.sleep(30)
            flagw = False
            flagBES_out = True
            flagWT_out = True
        time.sleep(h)
        #time.sleep(floor(h-dt))
finally:
    server.stop()
    print("Server offline")
```